servicenow

Yokohama Sicherheitsmanagement

Zuletzt aktualisiert: 17.12.2025

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung.®ine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken
sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern. Andere Unternehmens- und
Produktnamen können Marken der jeweiligen Unternehmen sein,
denen sie zugeordnet sind.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Automatische Übersetzung

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsverzeichnis

Security Operations 6

Security Operations erkunden 8

Now Assist für Security Incident Response 15

Now Assist für Security Incident Response erkunden 18

Now Assist für Security Incident Response konfigurieren 21

Security Incidents mit Now Assist für Security Incident Response schließen 29

Anwendungsfälle von KI-Agent in Now Assist für Security Incident Responseverwenden 39

Anwendungen für die Angriffsoberflächenverwaltung 41

Vulnerability Response 43

Application Vulnerability Response 838

Container Vulnerability Response 1051

Konfigurations-Compliance 1129

Vulnerability Response Arbeitsbereiche 1398

Software-Stückliste 1602

Anwendungen zur Verwaltung von Sicherheitsfällen im Unternehmen 1644

Security Incident Response 1646

Threat Intelligence 3147

Sicherheitsstatus-Überwachung 3391

Sicherheitsstatus-Überwachung erkunden 3393

Arbeitsbereich Sicherheitsstatus-Überwachung verwenden 3409

Überwachung von Risikominderungssteuerungen mit Sicherheitsstatus-Überwachung 3428

Anwendungsfälle, Richtlinienbeispiele und unterstützte Service Graph Connectors in Sicherheitsstatus-Überwachung 3452

Integration von Cloud Security Posture Management mit Amazon Web Services 3466

Cloud Security Posture Management mit Microsoft Azure 3477

Cybersicherheits-Dashboard 3486

Benchmark-Punktzahlen aktivieren 3505

Legen Sie Ziele fest 3506

Security Simulation and Training Integration for Security Operations 3507

Risiko- und Compliance-Dashboard für GRC: Metrics 3509

Threat Intelligence-Sicherheitszentrum 3519

Threat Intelligence-Sicherheitszentrum erkunden 3521

Domänentrennung und Threat Intelligence-Sicherheitszentrum 3523

Richten Sie das Threat Intelligence-Sicherheitszentrum ein 3525

Zeigen Sie die Homepage des Threat Intelligence-Sicherheitszentrums an 3527

Integration von Threat Intelligence Security Center 3530

TISC-Integration mit SIR Workspace 3605

Administration 3605

Arbeiten mit Datenimporten 3649

Importieren Sie Threat Intelligence 3650

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analyst Workbench für Bedrohungen....3660
Threat Intelligence-Sicherheitszentrum Bibliothek....3676
MITRE-ATT&CK™ Repository....3808
Datenverwaltung und -speicherung....3816
Funktions-Flow zur TISC-Datenverarbeitung....3826
Data Loss Prevention Incident Response....3828
Data Loss Prevention Incident Response erkunden....3830
DLP IR Incident Response installieren und konfigurieren....3833
Verwaltung von DLP Incident Response....3834
Data Loss Prevention Incident Response Incident Management....3889
Eingehende Integration für Data Loss Prevention Incident Response....3913
DLP-Integrationen....3915
Security Operations allgemeine Funktionalität....3994
Erstellen und definieren Sie Filtergruppen in Security Operations....3996
Transformation freigegebener Daten....3998
Security Operations E-Mail-Verarbeitung....4002
Security Operations Feldzuordnung....4013
Security Operations Feldwerttransformationen....4017
Security Operations Zuordnung von Ergänzungsdaten....4019
Security Operations Anwenderdefinierte Eskalation....4021
Erstellen Sie domänengetrennte Eigenschaftsüberschreibungen....4023
Erstellen Sie eine Betriebssystemgruppe....4024
Richten Sie Sicherheits-Tag-Gruppen und Tags ein....4025
Sicherheitsanmerkungen....4029
Mit Security Support Common installierte Komponenten....4032
Modulzugriff nach Rolle für Security Operations-Anwendungen....4033
[store-future: BEGIN review]
[End]
Security Operations durchsuchen....4724
Referenzen zur Integration mit Security Operations....4724
Security Operations Workflow-Auslöser....4826
Orchestration für Security Operations....4828
Security Operations Szenarien und Beispiele....4829
[store-future: BEGIN review]
Reduzieren Sie die Zeit für Bedrohungsanalysen durch Automatisierung....4829
[store-future: BEGIN review]
[End]
Priorisieren Sie Schwachstellen mit hohem Profil....4835
[store-future: BEGIN review]
[End]
[End]
Security Operations und ServiceNow Store....4838
Laden Sie eine Anwendung zum ersten Mal von ServiceNow Store herunter....4838
Installieren Sie eine Security Operations -Integration....4844

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisiert eine zuvor aus dem heruntergeladene Anwendung ServiceNow Store..... 4848
Aktualisieren Sie Ihre Instanz von auf das nächste Familien-Release.....4849

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations

ServiceNow® Security Operations -Anwendungen importieren Incident-Daten aus Ihren Sicherheitstools in eine strukturierte Antwort-Engine. Diese nutzt intelligente Workflows, Automatisierung, Datenvisualisierungen und eine profunde Verbindung zur IT, um Bedrohungen basierend auf den Auswirkungen auf Ihre Organisation zu priorisieren und zu beheben.

Klicken Sie auf eine dieser Kacheln, um zu beginnen.

Security Operations-Anwendungen und ihre Arbeitsbereiche

Erfahren Sie, wie die Anwendungen Security Operations Ihnen helfen können, Ihren Sicherheitsstatus zu verbessern.

Now Assist für Security Incident Response

Erfahren Sie, wie Now Assist for Security Incident Response ServiceNow® Generative AI-Kompetenzen (GenAI) im Arbeitsbereich für Security Incident Response und in der Core-UI (UI16) unterstützt.

Anwendungen für die Angriffsoberflächenverwaltung

Erfahren Sie mehr über die Anwendungen in Vulnerability Response, mit denen Sie Schwachstellen auf Ihrer Cyberangriffsfläche identifizieren und beheben können.

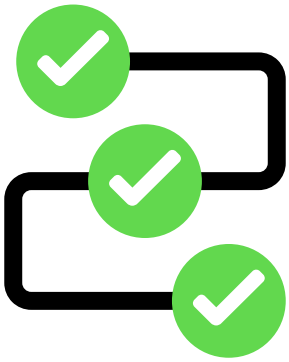
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen zur Verwaltung von Sicherheitsfällen im Unternehmen

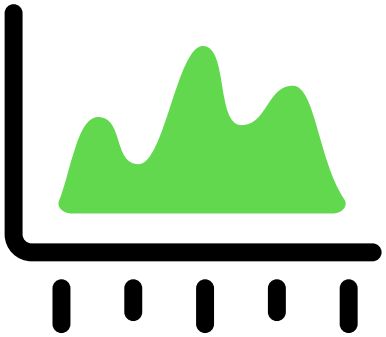
Erfahren Sie mehr über die Anwendungen in Security Incident Response, mit denen Sie kritische Security Incidents bei ihrer Entwicklung analysieren, isolieren und beheben können.

Anwendungen zur Kontrolle des Sicherheitsstatus



Erfahren Sie mehr über die Anwendungen, mit denen Sie Einblicke in Ihre allgemeine Sicherheitslage erhalten.

Cybersicherheits-Dashboard

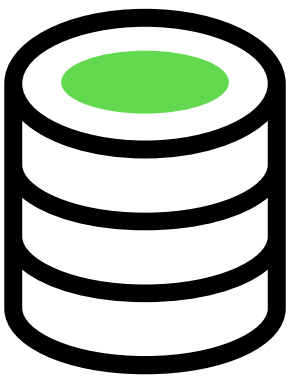


Erfahren Sie, wie das Cybersicherheits-Dashboard Daten aus den verschiedenen SecOps-Produkten in einem einheitlichen Dashboard konsolidiert.

Threat Intelligence-Sicherheitszentrum

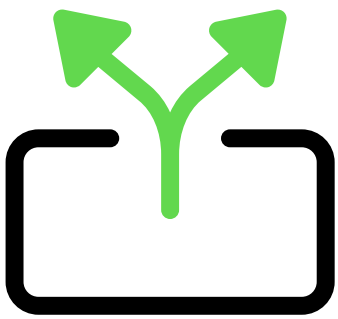
Erfahren Sie, wie die Plattform Threat Intelligence-Sicherheitszentrum (TISC) Technologielösungen für die Zusammenfassung und Verwaltung von Threat Intelligence bietet.

Reaktion auf Incident zur Vermeidung von Datenverlust



Erfahren Sie, wie Sie vertrauliche Informationen für Ihre Kunden verwalten und Ihre Kanäle für Datenverlust identifizieren und schützen können.

Gemeinsam genutzte Anwendungen von Security Operations



Erfahren Sie mehr über die Funktionen und Module, die allgemeine Funktionen für Security Operations bereitstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenarien und Beispiele von Security Operations

Erfahren Sie mehr darüber, wie Sie Security Operations -Anwendungen aus dem ServiceNow® Store abrufen und welche Szenarien für Anwendungen gelten, während Sie die -Produkte verwenden.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Security Operations erkunden

Schützen Sie Ihre Assets und Ihre Unternehmensumgebung mit ServiceNow Security Operations -Anwendungen und der Leistung des Now Platform®. Verbinden Sie Ihre Sicherheits- und IT-Teams, um Bedrohungen basierend auf den Auswirkungen auf Ihre Organisation zu priorisieren und zu lösen.

Security Operations – Übersicht

Die Anwendungssuite Security Operations hilft Ihnen, Ihre Assets zu schützen, indem Ihre allgemeine Sicherheitslage verbessert wird. Beispiel: Durch die Integration von Anwendungen wie Security Incident Response, Vulnerability Responseund Sicherheitsstatus-Überwachung mit Ihren vorhandenen Sicherheitstools können Ihre Security Operation Center (SOC)-Analysten, Manager und IT-Teams:

- Reagieren Sie auf sich schnell entwickelnde Cyber- und Sicherheitsbedrohungen
- Identifizieren, priorisieren und beheben Sie Schwachstellen
- Zeigen Sie Ihren gesamten Asset-Bestand an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

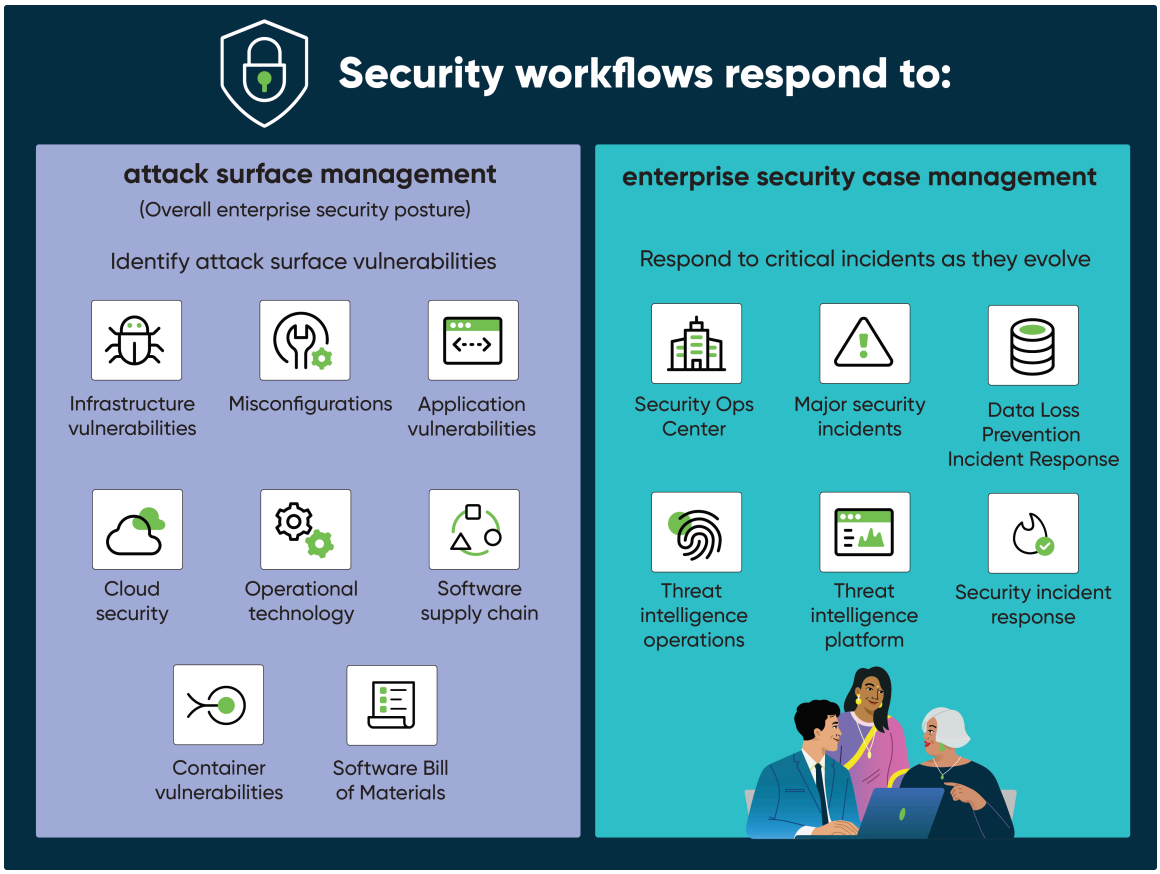
- Bestimmen Sie die allgemeine Abdeckung von Sicherheitstools
- Lösen Sie Security Incidents schneller mit intelligenten Workflows und ServiceNow Generative AI-Kompetenzen (GenAI). Weitere Informationen finden Sie unter Now Assist für Security Incident Response.

Security Operations -Anwendungen für -Workflows

Die Security Operations -Anwendungen fallen unter zwei große Kategorien für Security Operations -Workflows:

- Angriffsoberflächenmanagement: Anwendungen und Tools, mit denen Sie Ihre Schwachstellen antizipieren, verstehen und schließen können.
- Management von Sicherheitsfällen im Unternehmen: Anwendungen und Tools, mit denen Sie schnell auf kritische Incidents reagieren können.

Sicherheits-Workflows



Die beiden Kategorien von Security Operations-Anwendungen und die Anwendungsfälle, die Sie in Ihrer Unternehmensumgebung verwenden können.

Vorteile der Security Operations -Anwendungen

Zeigen Sie Security Operations -Anwendungen und -Daten mit Benutzeroberflächen (Arbeitsbereichen) der nächsten Generation an. Mit -Arbeitsbereichen können Sicherheitsanalysten, Manager des Security Operation Center (SOC) und Fehlerkorrekturspezialisten in Ihrer Organisation die folgenden Arten von Workflows von einem zentralen Ort aus überwachen und verwalten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- den Lebenszyklus von Security Incidents von der ersten Analyse bis zur Eindämmung, Beseitigung und Wiederherstellung.
- Die Schwachstellen, die sie am meisten interessieren, damit sie strategisch entscheiden können, welche Schwachstellen sie an IT-Teams zur Behebung senden.
- Wichtige Einblicke und wichtige Anwendungsfälle für die Abdeckung von Sicherheitstools und Asset-Hygiene, mit denen importierte Informationen zu Ihren Assets gemeldet und überwacht werden.

Anwendungen für die Angriffsoberflächenverwaltung

Anwendungen, mit denen Sie Bedrohungen antizipieren und Schwachstellen identifizieren können

Anwendung	Beschreibung	Anwender
Sicherheitsstatus-Überwachung	Gewinnen Sie Einblicke, wie gut Sicherheitstools bereitgestellt werden und Ihre Assets abdecken, basierend auf einem Asset-Bestand und importierten Daten. Service Graph Connectors und ServiceNow-Produkte wie Hardware Asset Management (HAM) und ITOM Discovery werden für Datenimporte unterstützt. Auf Richtlinien basierende Audits helfen Ihnen, die Korrektur von Kombinationen mit hohem Risiko zu priorisieren, z. B. Internetgefährdung und bekannte Schwachstellen. Erstellen Sie anwenderdefinierte Richtlinien und Einblicke, um die Compliance von Assets mit Ihren internen Konfigurationsstandards für Sicherheitstools zu überwachen.	• CISO • Informationssicherheitsanalyst • Security Operations Manager • IT-Betriebstechniker • Serviceverantwortlicher (Persona des Korrekturbesitzers)
Vulnerability Response	Schwachstellenscanner und Bewertungstools von Drittparteien helfen Ihnen, die Risiken zu identifizieren, die Schwachstellen für die	• CISO • Informationssicherheitsanalyst • Security Operations Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen, mit denen Sie Bedrohungen antizipieren und Schwachstellen identifizieren können (Fortsetzung)

Anwendung	Beschreibung	Anwender
	folgenden Arten von Assets darstellen: • Infrastruktur (Host) • Behälter • Anwendungen • Software-Stückliste Von diesen Tools identifizierte Schwachstellen stellen Risiken für die Sicherheits- und IT-Teams dar, die für die Wartung und den Schutz der Assets einer Organisation verantwortlich sind.	• IT-Betriebstechniker • Serviceverantwortlicher (Persona des Korrekturbesitzers)
Konfigurations-Compliance	Verifizieren Sie die Compliance mit Sicherheits- oder Unternehmensrichtlinien. Identifizieren, priorisieren und beheben Sie nicht konforme Konfigurationselemente mit Testergebnissen aus Drittpartei-SCA-Integrationen (Secure Configuration Assessment).	• CISO • Informationssicherheitsanalyst • Security Operations Manager • IT-Betriebstechniker • Serviceverantwortlicher (Persona des Korrekturbesitzers)

Anwendungen zur Verwaltung von Sicherheitsfällen im Unternehmen

Anwendungen, mit denen Sie auf kritische Sicherheitsverletzungen und Incidents reagieren können

Anwendung	Beschreibung	Anwender
Security Incident Response	Vereinfachen Sie den Prozess der Identifizierung kritischer Incidents, indem Sie leistungsstarke Workflow- und Automatisierungstools verwenden, die die Behebung beschleunigen. Integrieren Sie Ihre vorhandenen SIEM-Tools	• CISO • Informationssicherheitsanalyst • Security Operations Manager • Threat Intelligence-Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen, mit denen Sie auf kritische Sicherheitsverletzungen und Incidents reagieren können (Fortsetzung)

Anwendung	Beschreibung	Anwender
	(Security Information and Event Manager) mit den Anwendungen Security Incident Response und Security Operations, um Bedrohungsdaten aus verschiedenen Quellen zu importieren und automatisch priorisierte Security Incidents zu erstellen.	
Management schwerwiegender Sicherheits-Incidents	Die Funktionen zur Verwaltung schwerwiegender Security Incidents sind mit den vorhandenen Funktionen des Security Incident Response-Produkts kompatibel. Dies beinhaltet die Möglichkeit für einen Sicherheitsanalysten, einen Standard-Security Incident zu einem schwerwiegenden Security Incident zu eskalieren, sodass die neuen Produktfunktionen zur Unterstützung des Nachbesserungsprozesses verfügbar sind. Verfolgen Sie den Fortschritt eines schwerwiegenden Security Incident (Major Security Incident, MSI) von der Discovery bis zur Analyse. Lösungen vorschlagen, Security Incidents und den Abschluss heraufstufen und verknüpfen.	• CISO • Informationssicherheitsanalyst • Security Operations Manager • IT-Betriebstechniker • Serviceverantwortlicher (Persona des Korrekturbesitzers) • Generalrat
Reaktion auf Incident zur Vermeidung von Datenverlust	Mit Data Loss Prevention Incident Response (DLP IR) können Sie den Nachbesserungs-Workflow von DLP-Incidents aus mehreren Quellen, z. B. Endpunkt, Netzwerk, E-Mail und Cloud, überprüfen und verwalten. Mit der DLP-Anwendung können Sie Ihre Kanäle für	• CISO • Informationssicherheitsanalyst • Security Operations Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen, mit denen Sie auf kritische Sicherheitsverletzungen und Incidents reagieren können (Fortsetzung)

Anwendung	Beschreibung	Anwender
	Datenverlust identifizieren, darauf reagieren und sie schützen.	
Threat Intelligence	Ermöglicht es Antwortteams für Incidents, die Suche nach Bedrohungen und Korrelationen zu automatisieren. Die Integration mit MITRE ATT&CK ermöglicht Ihnen das Messen und Verstehen der Erkennungs- und Minderungsabdeckung und unterstützt Sie bei der Bedrohungssuche.	• CISO • Informationssicherheitsanalyst • Security Operations Manager • Threat Intelligence-Analyst
Threat Intelligence Security Center (TISC)	Sie können Threat Intelligence aus mehreren Quellen zusammenfassen, kuratieren und verwalten und eine Fallverwaltung für Threat Intelligence durchführen. Verfolgen Sie Kampagnen, operationalisieren Sie Threat Intelligence, und reagieren Sie auf umsetzbare Informationen.	• CISO • Informationssicherheitsanalyst • Security Operations Manager • Threat Intelligence-Analyst

Empfehlungen für weitere Themen

Wählen Sie eine Kachel aus, um mit den Security Operations Arbeitsbereichen zu beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich für Security Incident Response

Erfahren Sie mehr über den Arbeitsbereich für Security Incident Response

Arbeitsbereich des Schwachstellenmanagers

Erfahren Sie mehr über den Arbeitsbereich des Schwachstellenmanagers

Arbeitsbereich für Sicherheitsstatus-Überwachung

Erfahren Sie mehr über den Arbeitsbereich für Sicherheitsstatus-Überwachung

Arbeitsbereich der Schwachstellenbewertung

Erfahren Sie mehr über den Arbeitsbereich der Schwachstellenbewertung

Arbeitsbereich für IT-Korrekturen

Erfahren Sie mehr über den Arbeitsbereich für IT-Fehlerkorrekturen

Software-Arbeitsbereich für Stücklisten

Erfahren Sie mehr über den Software-Arbeitsbereich für Stücklisten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich für Threat Intelligence-Sicherheitszentrum (TISC).	Data Loss Prevention (DLP) Incident Response Workspace	Arbeitsbereich für das Management schwerwiegender Security Incidents (MSIM).
Erfahren Sie mehr über den TISC-Arbeitsbereich	Erfahren Sie mehr über den DLP-Arbeitsbereich	Erfahren Sie mehr über den MSIM-Arbeitsbereich

Problembehandlung und Hilfe

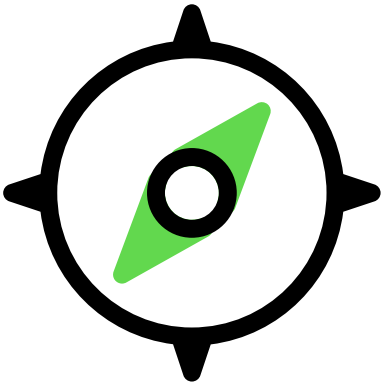
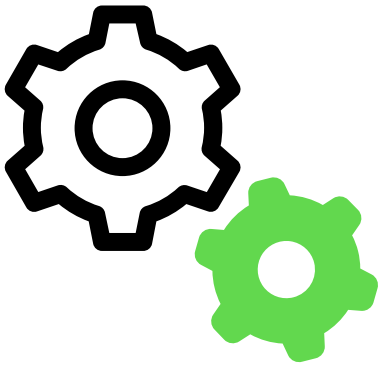
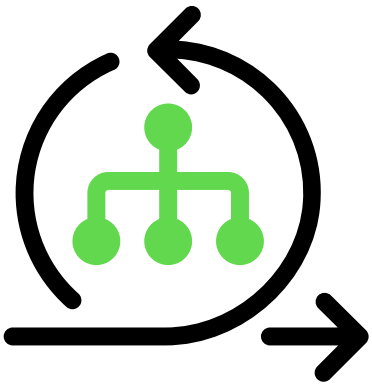
- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Now Assist für Security Incident Response

Sicherheitsanalysten können intelligente Workflows und Kompetenzen der generativen KI (ServiceNow) zur Lösung von Security Incidents nutzen. Sicherheitsmanager können mit der Anwendung Now Assist für Security Incident Response den Kontext von Security Incidents und Abschlussnotizen schnell in einem präzisen, leicht lesbaren Format überprüfen, Daten für Incident-Analysen anzeigen und sich die empfohlenen Korrekturschritte ansehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über Now Assist für Security Incident Response	Erfahren Sie, wie Sie die Kompetenzen für konfigurieren und aktivieren Now Assist für Security Incident Response	Erfahren Sie, wie Sie mit generativer KI und Abschlussnotizen für Security Incidents zusammenfassen und Abschlussnotizen für Security Incidents generieren Now Assist für Security Incident Response
	Verwenden Sie die KI-Agent-Sammlung von Security Incident Response Verwenden Sie die Anwendungsfälle von KI-Agents in Now Assist für Security Incident Response	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- Einige Now Assist -Produkte/-Funktionen sind derzeit für Kunden in FedRAMP-, NSC DOD IL5- oder Australia IRAP-geschützten Rechenzentren, für selbst gehostete Kunden oder in anderen eingeschränkten Umgebungen nicht verfügbar. Weitere Informationen finden Sie im Now Support Knowledge Base-Artikel KB0743854 . Achten Sie darauf, in zukünftigen Versionen nach Verfügbarkeitsaktualisierungen zu suchen.
- Einige Produkte/Funktionen Now Assist von sind derzeit nur für Kunden in bestimmten Regionen verfügbar. Weitere Informationen finden Sie in Artikel KB1699552 in der Now Support Knowledge Base. Achten Sie darauf, in zukünftigen Versionen nach Verfügbarkeitsaktualisierungen zu suchen.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

KI-Beschränkungen

Diese Anwendung nutzt künstliche Intelligenz (KI) und maschinelles Lernen, zwei sich schnell entwickelnde Studienbereiche, in denen Vorhersagen auf Grundlage von Datenmustern erstellt werden. Daher liefert diese Anwendung möglicherweise nicht immer präzise, vollständige und angemessene Informationen. Darüber hinaus gibt es keine Garantie dafür, dass diese Anwendung vollständig für Ihren Anwendungsfall trainiert und getestet wurde. Um diese Probleme zu minimieren, sind Sie dafür verantwortlich, Ihre Verwendung dieser Anwendung auf Genauigkeit, Schaden und Angemessenheit für Ihren Anwendungsfall zu testen und zu bewerten, die Ausgabe von Menschen beaufsichtigen zu lassen und sich bei der Entscheidungsfindung nicht ausschließlich auf KI-generierte Ergebnisse zu verlassen Zwecke. Dies ist besonders wichtig, wenn Sie diese Anwendung in Bereichen mit weitreichenden Auswirkungen wie Gesundheitswesen, Finanzen, Recht, Beschäftigung, Sicherheit und Infrastruktur einsetzen möchten. Sie erklären sich damit einverstanden, die Richtlinie zur zulässigen KI-Nutzung von ServiceNow einzuhalten, die von ServiceNow aktualisiert werden kann.

Datenverarbeitung

Bei dieser Anwendung müssen die Daten einzelner ServiceNow-Kundeninstanzen in eine zentrale ServiceNow-Umgebung übertragen werden, die sich in einer anderen Rechenzentrumsregion befinden kann als die, in der sich Ihre Instanz befindet, und möglicherweise an einen externen Cloud-Anbieter, z. B. Microsoft Azure. Diese Daten werden gemäß den internen Richtlinien und Verfahren von ServiceNow gehandhabt, einschließlich unserer Richtlinien, die über unser CORE-Compliance-Portal verfügbar sind.

Datenerfassung

ServiceNow sammelt und verwendet die Eingaben, Ausgaben und Ausgabenbearbeitungen dieser Anwendung, um ServiceNow-Technologien wie ServiceNow-Modelle und KI-Produkte zu entwickeln und zu verbessern. Darüber hinaus erfasst diese Anwendung Daten aus Security Incidents, Incidents, Change-Anforderungen, Problemen und angreifbaren Elementen. Kunden können der Datenerfassung für die Zukunft jederzeit widersprechen, wie auf der Now AssistAbwählseite beschrieben.

Weitere Informationen finden Sie in der Now Assist-Dokumentation .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response erkunden

Ihre Sicherheitsanalysten können intelligente Workflows und generative KI-Kompetenzen ServiceNow verwenden, um Security Incidents im Rahmen ihrer Arbeit mit der Anwendung Now Assist für Security Incident Response zu selektieren, zu untersuchen und zu schließen.

Now Assist für Security Incident Response – Übersicht

Mit Kompetenzen der generativen KI können Sicherheitsanalysten:

- Fassen Sie Details zu Security Incidents zusammen, und überprüfen Sie den Kontext schnell in einem präzisen, leicht lesbaren Format.
- Generieren Sie die empfohlenen nächsten Schritte für einen Security Incident.
- Generieren Sie Daten für die Analyse nach Incidents.
- Generieren Sie Abschlussnotizen.
- Korrelationseinblicke generieren

Sicherheitsanalysten können Ergebnisse, Incident-Details und Abschlussnotizen mit anderen Analysten, Managern und wichtigen Stakeholdern teilen.

Now Assist für Security Incident Response Anwender

Anwender

Anwender	Beschreibung
Sicherheitsanalysten und Manager	Zeigen Sie eine Vorschau der Detailinformationen zu Security Incidents an, sehen Sie sich die möglichen Auswirkungen an, und zeigen Sie die wichtigsten Korrekturmaßnahmen an, die bereits mit Zusammenfassungen von Security Incidents mithilfe von generativer KI durchgeführt wurden. Zusammenfassungen und empfohlene nächste Schritte (Aktionen) geben Analysten und Managern einen Vorteil bei ihren Untersuchungen und helfen beim Schließen von Security Incidents. Generative KI verwendet, um automatisch einen Entwurf von Abschlussnotizen zu generieren. Abschlussnotizen für Security Incidents werden schnell basierend auf Korrektur- und Eindämmungsaktivitäten erstellt und enthalten andere relevante Detailinformationen zu ihrem Abschluss.

Now Assist für Security Incident Response – Vorteile

Now Assist für Security Incident Response Funktionen

Leistung	Funktion	Anwender
Beschleunigen Sie die Selektierung von Security Incidents mit langen Aktivitätenströmen, indem Sie Arbeitsnotizen und kontextbezogene Informationen schnell in einem präzisen, leicht lesbaren Format überprüfen.	Generieren Sie Zusammenfassungen für Security Incidents, die die folgenden Informationen enthalten:	• Sicherheitsanalysten • Sicherheitsmanager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response Funktionen (Fortsetzung)

Leistung	Funktion	Anwender
	• Problem • Details • Beobachtungen • Wichtige getroffene Maßnahmen • Abschlussdetails	
Generiert automatisch einen Entwurf von Abschlussnotizen für einen Security Incident, wenn er zur Schließung bereit ist. Bevor sie den Security Incident schließen, können Analysten jeden Inhalt, der von der KI-Kompetenz generiert wird, ändern, indem sie ihn bearbeiten, entfernen oder eigene Notizen hinzufügen.	Generieren Sie Abschlussnotizen für Security Incidents	• Sicherheitsanalysten • Sicherheitsmanager
Generieren Sie auf Anforderung empfohlene nächste Schritte innerhalb des Workflows, um einen Security Incident zu schließen.	Generieren Sie empfohlene Aktionen für Security Incidents	• Sicherheitsanalysten • Sicherheitsmanager
Generieren Sie eine Nachfolgeanalyse, die eine Ursachenanalyse, eine Folgenabschätzung und gelernte Lektionen aus dem Workflow zum Schließen eines Security Incident enthält.	Generieren Sie Nachfolgeanalysen nach Incidents	• Sicherheitsanalysten • Sicherheitsmanager
Verbinden Sie aktuelle Incidents mit vergangenen Ereignissen, an denen dieselben betroffenen Anwender, Configuration Items (CIs) oder erkennbaren Elemente beteiligt sind.	Korrelationseinblicke generieren	• Sicherheitsanalysten • Sicherheitsmanager
Erfahren Sie schnell mehr über die Details eines Security Incident, indem Sie im Bereich Now Assist auf Zusammenfassungen und Abschlussnotizen zugreifen.	Greifen Sie auf die Zusammenfassung und die Abschlussnotizen der generativen KI im Bereich Now Assist zu. Geben Sie im Bereich Anforderungen für grundlegendere Informationen zu Security Incidents ein.	• Sicherheitsanalysten • Sicherheitsmanager
Passen Sie die generativen KI-Kompetenzen für Zusammenfassungen und Abschlussnotizen an Ihre Bedürfnisse an.	Kopieren Sie eine Kompetenz, ändern Sie die Auswahl zugehöriger Tabellenfelder, definieren Sie die Verfügbarkeit der Kompetenz, und wählen Sie aus, wo die Kompetenz angezeigt wird.	Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Now Assist für Security Incident Response finden Sie unter:

- Now Assist für Security Incident Response konfigurieren
- Fassen Sie einen Security Incident mit zusammen Now Assist für Security Incident Response
- Generieren Sie mit Abschlussnotizen für einen Security Incident Now Assist für Security Incident Response
- Generieren Sie Korrelationseinblicke mit Now Assist für Security Incident Response
- Generieren Sie mit empfohlene Aktionen für einen Security Incident Now Assist für Security Incident Response
- Generieren Sie mit eine Nachfolgeanalyse für einen Security Incident Now Assist für Security Incident Response
- Eingaben und Auslöser für Now Assist für Security Incident Response

Ergänzende Informationen für Now Assist für Security Incident Response

Verschaffen Sie sich einen schnellen Überblick über wichtige Informationen im Zusammenhang mit der Anwendung Now Assist für Security Incident Response.

Unterstützte Versionen

Version 2.0.1 von Now Assist für Security Incident Response unterstützt:

- veraltet UI (UI16): Security Incident Response Kernanwendung, v13.6.4
- Arbeitsbereich für Security Incident Response (SIR Workspace), v1.7.0
- Now Assist für Now Platform® v6.0.1

Unterstützte Anwenderoberflächen

Now Assist für Security Incident Response enthält die generativen KI-Kompetenzen, die in der folgenden Tabelle aufgeführt sind.

Now Assist für Security Incident Response unterstützte Schnittstellen und Kompetenzen

Schnittstelle	Funktionen
Security Incident Response	• Zusammenfassung von Security Incidents. • Generierung der empfohlenen nächsten Schritte für einen Security Incident • Generierung von Analysen nach Incidents, die Ursachenanalysen, Folgenabschätzungen und gelernte Lektionen umfassen. • Now Assist Bereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response unterstützte Schnittstellen und Kompetenzen (Fortsetzung)

Schnittstelle	Funktionen
	• Erstellung von Abschlussnotizen • Korrelationseinblicke aus dem Now Assist -Bereich.
Veraltet UI16	• Zusammenfassung von Security Incidents • Generierung der empfohlenen nächsten Schritte für einen Security Incident • Generierung von Analysen nach Incidents, die Ursachenanalysen, Folgenabschätzungen und gelernte Lektionen umfassen. • Now Assist Bereich. • Erstellung von Abschlussnotizen • Korrelationseinblicke aus dem Now Assist -Bereich.

Now Assist für Security Incident Response konfigurieren

Die Anwendung Now Assist für Security Incident Response wird in der Arbeitsbereich für Security Incident Response - und der veraltet -Core-UI (UI16) unterstützt. Sie können das geführte Setup in der Now Assist-Administrator -Konsole verwenden, um Now Assist für Security Incident Responsezu konfigurieren.

Konfiguration – Übersicht

Durch die Freigabe von Daten für das KI-Entwicklungsprogramm ServiceNow® stellen Sie relevante Daten bereit, um die Vorhersagegenauigkeit und die Anwender-Experience zu verbessern, Produkte an Ihre Geschäftsanforderungen anzupassen und „Halluzinationen“ für Ihre aktivierten Now Assist -Kompetenzen zu reduzieren.

Sie können die Datenfreigabe für eine Instanz vom ServiceNow Typ über die Konsole Now Assist-Administrator deaktivieren, wenn Sie nicht teilnehmen möchten. Weitere Informationen finden Sie unter Opt out of data sharing for Now Assist . Wiederholen Sie den Abwählvorgang für alle Instanzen, die die Funktion Now Assist verwenden.

Verwenden Sie die Now Assist-Administrator-Konsole, um Now Assist für Security Incident Response zu konfigurieren. Diese Konsole enthält alles, was Sie benötigen, um Anwendungen zu installieren und generative KI-Kompetenzen zu konfigurieren. Weitere Informationen finden Sie unter Configuring Now Assist settings and features .

In der folgenden Tabelle sind die Funktionen und Kompetenzen aufgeführt, auf die Sie über die Now Assist-Administrator-Konsole zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response Funktionen und Kompetenzen in der Now Assist-Administrator -Konsole

Now Assist-Technologieprodukt	Kompetenzen in Bezug auf Security Incidents
Now Assist für Security Incident Response	Zusammenfassung von Security Incidents **Hinweis:** Die Incident-Zusammenfassung unterstützt Security Incidents in jedem anderen Status als **Entwurf**.
	Lösungshinweise generieren.
	Empfohlene Aktionen für Security Incidents Die Kompetenz „Empfohlene Aktionen für Security Incidents“ unterstützt Security Incidents in jedem anderen Status als **Geschlossen** und **Abgebrochen**. **Hinweis:** Die Anwendung „KI-Suche“ muss aktiviert sein, damit die Kompetenz „Empfohlene Aktionen“ für Security Incidents funktioniert. Um zu überprüfen, ob die KI-Suche in Ihrer Instanz aktiviert ist, navigieren Sie zu **Alle** > **KI-Suche** > **Status der KI-Suche**. Wenden Sie sich an den Support, wenn auf der Seite angezeigt wird, dass die KI-Suche nicht aktiviert ist. Korrelationseinblicke unterstützen Security Incidents in allen Status.
	Generierung von Nachfolgeanalysen nach Incidents

1. Install Now Assist plugins .

   Installieren Sie die Anwendung Now Assist für Security Incident Response (sn_sec_gen_ai).

2. Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response

   Konfigurieren Sie eine Kompetenz, und überprüfen Sie ihre Details. Sie aktivieren eine Kompetenz aus dem Geführtes Setup.

Geführtes Setup verwenden, um Now Assist für Security Incident Responsezu implementieren

Geführtes Setup stellt eine Reihe von Aufgaben bereit, mit denen Sie Now Assist für Security Incident Response in Ihrer Instanz ServiceNow von konfigurieren können. Um Geführtes Setup für Now Assist für Security Incident Responsezu öffnen, navigieren Sie zu **Alle** > **Now Assist Admin** > **Funktionen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response.

Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response

Konfigurieren und überprüfen Sie die Details für eine Kompetenz in Geführtes Setup. Sie können eine Kompetenz aus Geführtes Setupaktivieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Now Assist Admin** > **Funktionen**.
2. Wählen Sie im Navigationsbereich **Technologie** aus, und wählen Sie **Security Operations** aus der Liste aus.
   Diese Security Incident-Kompetenzen werden auf der Karte „Security Incident“ angezeigt:
   - Empfohlene Aktionen für Security Incidents

     Die Anwendung „KI-Suche“ muss aktiviert sein, damit die Kompetenz „Empfohlene Aktionen“ für Security Incidents funktioniert. Um zu überprüfen, ob die KI-Suche in Ihrer Instanz aktiviert ist, navigieren Sie zu **Alle** > **KI-Suche** > **Status der KI-Suche**. Wenden Sie sich an den Support, wenn auf der Seite angezeigt wird, dass die KI-Suche nicht aktiviert ist.
   - Analyse nach Incident
   - Generierung von Korrelationseinblicken
   - Zusammenfassung von Security Incidents
   - Lösungshinweise generieren
3. Wählen Sie **Details anzeigen**.
   Sie können die in der Anwendung enthaltenen Kompetenzen nicht bearbeiten. Um die Standardeinstellungen zu bearbeiten, müssen Sie eine Kopie erstellen. Weitere Informationen zum Anpassen einer Kompetenz finden Sie unter Now Assist für Security Incident Response-Kompetenzen anpassen.
4. Wählen Sie **Kompetenz aktivieren** für die gewünschte Kompetenz aus.
5. Befolgen Sie die Schritte zum Konfigurieren und Aktivieren einer Kompetenz mit Geführtes Setup.

Hinweis:
Für einige Kompetenzen sind nicht alle unten aufgeführten Konfigurationsschritte erforderlich. Wählen Sie die einzigen Aufgaben aus, die im linken Bereich angezeigt werden, und befolgen Sie die Eingabeaufforderungen. Nachdem Sie die Aufgaben abgeschlossen haben, aktivieren Sie die Kompetenz.

a. Wählen Sie im Navigationsbereich **Eingabe wählen aus**, um die Eingaben oder Auslöser für die ausgewählte Kompetenz zu konfigurieren.

   Einige oder alle der folgenden Eingabevorlagen für die Kompetenz sind aufgelistet: **In Arbeit**, **Überprüfung**und **Geschlossen**. Die Vorlage **„In Arbeit“** ist ausgewählt.

   Möglicherweise möchten Sie für diese Eingabevorlagen ihre Standardeinstellungen beibehalten, bis Sie sich mit der Funktionsweise der -Kompetenzen für Now Assist für Security Operations vertraut gemacht haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für einige der Kompetenzen können Sie jedoch bestimmte zugehörige Tabellenfelder ändern, die Eingabeaufforderung für einen Security Incident testen, die Verfügbarkeit der Kompetenz definieren und auswählen, wo die Kompetenz angezeigt wird.

Wenn Sie Felder ändern möchten, wählen Sie nur die unterstützten Optionen aus den Listen aus, die als Teil Ihrer Eingabedaten bereitgestellt werden.

Wenn Sie die Eingaben oder Auslöser für eine Kompetenz ändern, bestimmen Sie, wie und wann eine Kompetenz verwendet wird. Sie können die Eingabedatenquelle einer Kompetenz nicht ändern. Die Datenquelle enthält die Tabellen und Felder, auf denen die Fähigkeit basiert. Sie können jedoch eine Kompetenz kopieren und anpassen. Weitere Informationen finden Sie unter Now Assist für Security Incident Response-Kompetenzen anpassen.

6. Wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt in Geführtes Setupfortzufahren.
7. **Wahlweise:** Testen Sie die Eingabeaufforderung für einen Security Incident-Datensatz.
8. Wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt in Geführtes Setupfortzufahren.
9. **Wahlweise:** Wählen Sie eine der folgenden Optionen aus, um die Verfügbarkeit zu definieren.
10. Wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt in Geführtes Setupfortzufahren.
11. Wählen Sie **Anzeige auswählen,** um zu bestimmen, wo die Kompetenz angezeigt werden soll.
12. Wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt fortzufahren.
13. **Wahlweise:** Fügen Sie Rollen hinzu, oder entfernen Sie sie.

    (Optional) Standardmäßig werden die Rollen sn_si.analyst und sn_si.manager hinzugefügt. Sie können die Ergebnisse aus der automatisierten Kompetenzgenerierung anzeigen. Sie können Rollen nur hinzufügen oder entfernen, wenn Sie Now Assist für Security Incident Response-Kompetenzen anpassensind.
14. Überprüfen Sie Ihre Auswahl, und wählen Sie **Aktivieren,** um die Konfiguration für die Kompetenz abzuschließen.
15. Wählen Sie **Zurück zu Security Incident**.
    Die Kompetenz wird im Abschnitt „Aktive Kompetenzen“ angezeigt.

Now Assist für Security Incident Response-Kompetenzen anpassen

Passen Sie einige der Eingabefelder einer generativen KI-Kompetenz an die Anforderungen Ihrer Umgebung an.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu **Alle** > **Now Assist Admin** > **Funktionen** Registerkarte der Konsole Now Assist-Administrator.
2. Wählen Sie im Navigationsbereich **Technologie** aus, und wählen Sie **Security Operations** aus der Liste aus.
   Diese Security Incident-Kompetenzen werden angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Empfohlene Aktionen für Security Incidents
- Analyse nach Incident
- Generierung von Korrelationseinblicken
- Zusammenfassung von Security Incidents
- Lösungshinweise generieren

3. Erstellen Sie eine Kopie einer Kompetenz, und passen Sie die Eingabefelder an.

a. Wählen Sie auf der Funktionskarte „Security Incident“ **Details anzeigen**.

b. Suchen Sie im Abschnitt „Aktive Kompetenzen“ nach der Kompetenz, die Sie kopieren möchten, und wählen Sie das Symbol „Weitere Aktionen“ ( ).

c. Wählen Sie **Kopie erstellen aus**.

d. Bestätigen Sie Ihre Auswahl im Modal.
Das geführte Setup wird angezeigt.

e. Geben Sie unter **Allgemeine Details**einen eindeutigen Namen und eine Beschreibung für die Kompetenz ein.

f. Fahren Sie mit dem nächsten Schritt fort, indem Sie **Speichern und fortfahren**auswählen.

g. Wählen Sie **Eingabe wählen aus**.

Wenn **„Eingabe wählen“** ausgewählt ist, werden die folgenden Eingabevorlagen für die Kompetenz aufgelistet: „In Arbeit“, „Überprüfen“ und „Geschlossen“. Die Vorlage „In Arbeit“ ist ausgewählt.

Sie können einige der Felder der Basiseingabetabelle, die Bedingungen und die zugehörigen Listen für die Vorlagen konfigurieren. Wählen Sie nur aus den zugehörigen Tabellen aus, die in den Listen für Ihre Eingabedaten unterstützt werden.

Sie können die Basiseingabetabelle [sn_si_incident] für Ihre Kopie der Kompetenz „Zusammenfassung von Security Incidents“ nicht ändern oder eine neue Datenquelle hinzufügen.

h. Ändern Sie die bearbeitbaren Felder in der Vorlage „In Arbeit“ mit dem Bedingungsgenerator und den Filterbedingungen weiter.

i. Fahren Sie mit dem nächsten Schritt in Geführtes Setup für die Vorlage In Arbeit fort, indem Sie **Speichern und fortfahren**wählen.

- **Eingabeaufforderung anpassen**: Bearbeiten Sie die Eingabeaufforderung, indem Sie die vordefinierten Abschnitte neu anordnen oder entfernen. Sie können die Eingabeaufforderung in einem Security Incident-Datensatz für jede Eingabevorlagenkonfiguration überprüfen und testen.
- **Verfügbarkeit definieren**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Kompetenz ist immer verfügbar	Die Kompetenz steht Benutzern jederzeit zur Verfügung.
Verfügbarkeit von Kompetenzen anpassen	Die Kompetenz ist nur verfügbar, wenn die Bedingungen erfüllt sind (Standard). Verwenden Sie den Bedingungsgenerator, um Ihre Bedingungen festzulegen.

- **Anzeige auswählen**:

Option	Beschreibung
Produktintern	Zeigt die Zusammenfassung der Security Incidents in allen Sicherheitsprodukten an. Now Assist Kompetenzen werden in Formularen und Arbeitsbereichen angezeigt.
Anwenderrollen	Wählen Sie das Erweiterungssymbol ( )
Now Assist-Bereich	Now Assist Kompetenzen sind im Bereich Now Assist verfügbar. **Hinweis:** Wenn diese Option nicht angezeigt wird, müssen Sie den Bereich Now Assist aktivieren. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

j. Wählen Sie **Vorlage speichern**, um Ihre Änderungen an der Vorlage In Arbeit zu speichern.

k. Wählen Sie die Vorlage Überprüfen aus.

l. Ändern Sie die bearbeitbaren Felder in den Vorlagen Überprüfen und Geschlossen mit Filterbedingungen weiter, wie in den vorherigen Schritten beschrieben.

m. Wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt in Geführtes Setupfortzufahren.

n. Wählen Sie **Vorlage speichern,** um Ihre Änderungen an einer Vorlage zu speichern.

o. Wählen Sie **Überprüfen und aktivieren aus,** um Ihre Kompetenz zu überprüfen und zusätzliche Änderungen vorzunehmen.

4. Wählen Sie **Aktivieren**.
   Ihre Kompetenz wird auf der Seite „Security Incident“ im Abschnitt „Alle verfügbaren Kompetenzen für Security Incident“ angezeigt.
5. Wählen Sie **Kompetenz aktivieren aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingaben und Auslöser für Now Assist für Security Incident Response

Sie können einige der Eingaben oder Auslöser für eine Kompetenz der generativen KI konfigurieren. Mit Eingaben oder Auslösern können Sie bestimmen, wie und wann eine Kompetenz verwendet wird.

Eingaben und Auslöser

Eingaben geben die für eine Kompetenz verwendeten Daten an. Zu den Eingaben gehören die Tabelle und die Felder, die zum Generieren der Zusammenfassung eines Security Incident verwendet werden. Ein Auslöser initiiert eine Aktion. Beispielsweise bestimmen Auslöser, wann das System eine Zusammenfassung generiert.

Sie können Eingaben und Auslöser ändern, aber Sie können nicht die Datenquelle einer Kompetenz ändern. Die Datenquelle enthält die Tabellen und Felder, auf denen die Fähigkeit basiert.

Kompetenz „Zusammenfassung von Security Incidents“.

Eingaben für die Kompetenz „Zusammenfassung des Security Incidents“ geben die Tabelle und die Felder an, die bei der Generierung einer Zusammenfassung des Security Incidents verwendet werden. In der folgenden Tabelle sind die Eingaben für die Kompetenz „Zusammenfassung von Security Incidents“ auf der Seite „Eingabe auswählen“ in der Konsole Now Assist-Administrator aufgeführt.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_incident].
Eingabefelder	• Kurzbeschreibung • Beschreibung • Status • Priorität • Arbeitsnotizen • Zusätzliche Anmerkungen
Zugehörige Eingabetabellen	• Betroffene CIs – Configuration Item • Betroffene Anwender – Anwender • Security Incident Response Aufgabe: Kurzbeschreibung • Status – Jeder andere Status als **„Abgebrochen“**. • Zugeordnete erkennbare Elemente: Befund des erkennbaren Elements ist böswillig oder verdächtig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kompetenz „Lösungshinweise generieren“

Eingaben für die Kompetenz „Lösungshinweise generieren“ geben die Tabelle und die Felder an, die verwendet werden, wenn die Lösungshinweise für einen Security Incident generiert werden. In der folgenden Tabelle sind die Eingaben für die Kompetenz „Lösungshinweise generieren“ von der Seite „Eingabe auswählen“ in der Konsole Now Assist-Administrator aufgeführt.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_incident].
Eingabefelder	• Kurzbeschreibung • Beschreibung • Arbeitsnotizen • Zusätzliche Anmerkungen

Kompetenz „Generierung von empfohlenen Aktionen für Security Incidents“.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_incident].

Kompetenz „Analyse nach Incidents generieren“.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_incident].

Kompetenz für die Generierung von Korrelationseinblicken

Ihre Korrelationseinblicke für einen Security Incident können Datensätze aus den folgenden Tabellen enthalten. Sie müssen jedoch berechtigt sein, auf diese Tabellen und Datensätze zuzugreifen.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_incident]. Configuration Item-Tabelle [cmdb_ci]. Incident-Tabelle [incident]. Tabelle „Change-Anforderung“ [change_request]. Problemtabelle [problem]. Tabelle für angreifbare Elemente [sn_vul_vulnerable_item].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabe	Beschreibung
	Ordnen Sie die Tabelle für erkennbare Elemente [sn_ti_observable] zu.

Security Incidents mit Now Assist für Security Incident Response schließen

Mit den von Now Assist für Security Incident Responseunterstützten generativen KI-Kompetenzen können Sicherheitsanalysten Security Incidents schnell aus ihrem Arbeitsablauf schließen.

Übersicht über Now Assist für Security Incident Response

Mit den Kompetenzen der generativen KI bei Now Assist für Security Incident Responsehaben Ihre Sicherheitsanalysten die Möglichkeit:

- Fassen Sie Details zu Security Incidents zusammen, und überprüfen Sie den Kontext schnell in einem präzisen, leicht lesbaren Format.
- Generieren Sie Abschlussnotizen (Lösung).
- Generieren Sie empfohlene Aktionen für einen Security Incident
- Generieren Sie Daten für die Analyse nach Incidents
- Generieren Sie Korrelationseinblicke, um die Untersuchung von Incidents zu beschleunigen.

Sicherheitsmanager und -analysten können von folgenden Stellen aus Zusammenfassungen von Security Incidents und Abschlussnotizen anfordern:

- Security Incident-Datensätze
- Security Incident Response Arbeitsbereich
- Bereich Now Assist.

Hinweis:
Die für einen Security Incident empfohlenen Aktionen und die Kompetenzen für die Analyse nach Incidents sind im Bereich Now Assist nicht verfügbar.

Sicherheitsmanager und -analysten können an folgenden Stellen empfohlene nächste Schritte und Nachfolgeanalysen von Incidents generieren:

- Security Incident-Datensätze
- Security Incident Response Arbeitsbereich

-Sicherheitsmanager und -analysten können im -Arbeitsbereich Security Incident Response nur aus generierten empfohlenen Aktionen aus Security Incidents Korrekturaufgaben erstellen.

1. Fassen Sie einen Security Incident mit zusammen Now Assist für Security Incident Response

   Generieren Sie eine Zusammenfassung für einen Security Incident, die das zugrunde liegende Problem, Incident-Details, zugehörige Listendaten (erkennbare Elemente) und bereits durchgeführte wichtige Aktionen enthält.

2. Generieren Sie mit empfohlene Aktionen für einen Security Incident Now Assist für Security Incident Response

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Generieren Sie mit eine Nachfolgeanalyse für einen Security Incident Now Assist für Security Incident Response
4. Generieren Sie Korrelationseinblicke mit Now Assist für Security Incident Response
5. Generieren Sie mit Abschlussnotizen für einen Security Incident Now Assist für Security Incident Response

   Generieren Sie automatisch die Abschlussnotizen für einen Security Incident.

6. Generative KI-Kompetenzen im Bereich Now Assist für Now Assist für Security Incident Responseanfordern

   Generieren Sie im Bereich Now Assist Zusammenfassungen und Abschlussnotizen.

   Hinweis:
   Die für einen Security Incident empfohlenen Aktionen und die Kompetenzen für die Analyse nach Incidents sind im Bereich Now Assist nicht verfügbar.

7. Now Assist für Security Incident Response-Kompetenzen anpassen

   Passen Sie die Eingabefelder einer Kompetenz an die Anforderungen Ihrer Umgebung an.

Fassen Sie einen Security Incident mit zusammen Now Assist für Security Incident Response

Mit der generativen KI-Kompetenz „Zusammenfassung von Security Incidents“ können Sie den Kontext eines Security Incidents nachvollziehen.

Vorbereitungen

Sie können einen Security Incident in der veraltet Core-UI (UI16) und in der Arbeitsbereich für Security Incident Responsezusammenfassen. Die Felder, die für die Eingabedaten verwendet werden, um einen Incident mithilfe von generativer KI zusammenzufassen, müssen mindestens 50 Wörter enthalten. Weitere Informationen zu den Eingabefeldern finden Sie unter Eingaben und Auslöser für Now Assist für Security Incident Response.

Erforderliche Rolle: sn_si.analyst, sn_si.manager oder sn_si.basic

Prozedur

1. Navigieren Sie in der Core-UI von veraltet zu **Alle** > **Security Incident** > **Incidents** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
2. Alternativ navigieren Sie zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
3. Wählen Sie auf der Registerkarte **Übersichtdie Option Zusammenfassen**aus.
   - Die generierte Zusammenfassung wird in einem Banner oben im Security Incident-Datensatz in veraltet Core UI16 angezeigt.
   - Die generierte Zusammenfassung wird auf der Registerkarte **Übersicht** in Arbeitsbereich für Security Incident Responseangezeigt.
4. **Wahlweise:** Wählen Sie aus den folgenden Optionen aus, nachdem die Zusammenfassung generiert wurde.

   (Optional) In von KI generierten Zusammenfassungen fehlen möglicherweise wichtige Details. Möglicherweise möchten Sie die Zusammenfassung auf Richtigkeit und Vollständigkeit überprüfen, bevor Sie fortfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Generieren Sie mit Abschlussnotizen für einen Security Incident Now Assist für Security Incident Response

Generiert automatisch einen Entwurf der Abschlussnotizen für einen Security Incident, wenn Sie ihn schließen. Der Entwurf kann bearbeitet werden und wird vor dem Schließen des Security Incidents überprüft. Er kann nach Bedarf verwendet oder geändert werden. Abschlussnotizen informieren andere Analysten, Manager und wichtige Stakeholder über die Lösung eines Security Incident.

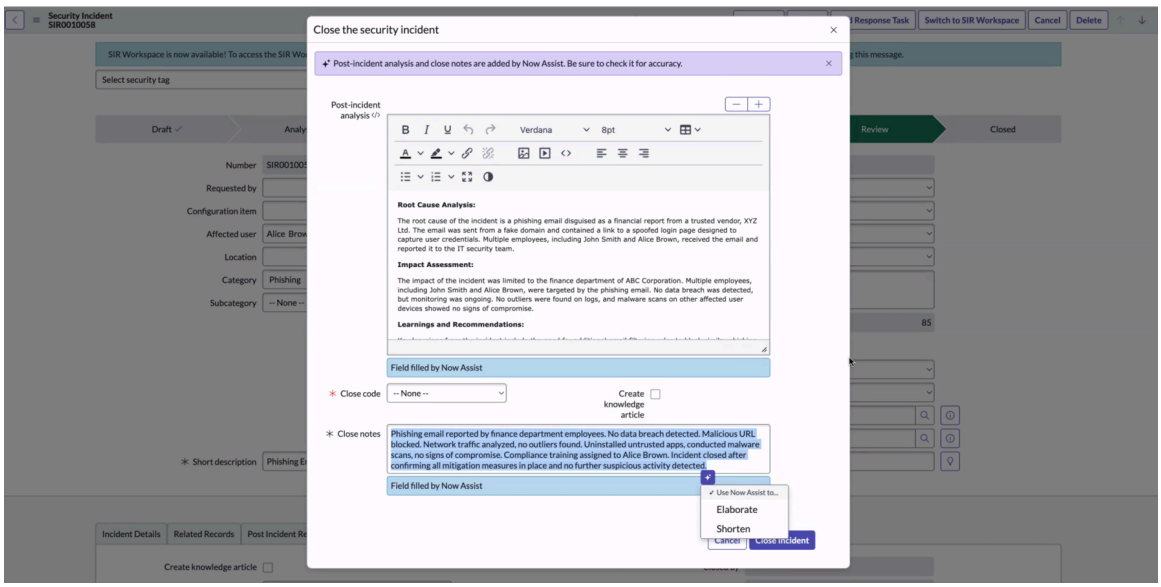
Vorbereitungen

Erforderliche Rolle: sn_si.analyst, sn_si.manager oder sn_si.basic

Prozedur

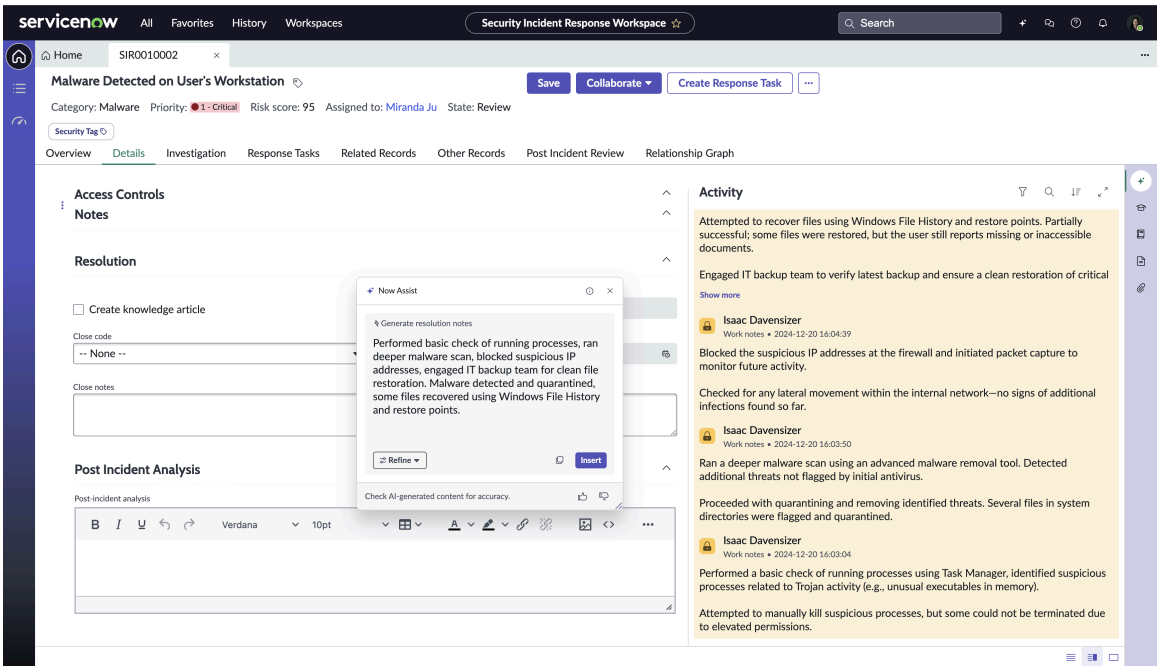
1. Navigieren Sie in der Core-UI von veraltet zu **Alle** > **Security Incident** > **Incidents** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
2. Alternativ navigieren Sie zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
3. Schließen Sie den Security Incident.

   Der folgende Screenshot zeigt die Lösungshinweise, die zum Schließen des Security Incident in Core-UI16 generiert wurden.

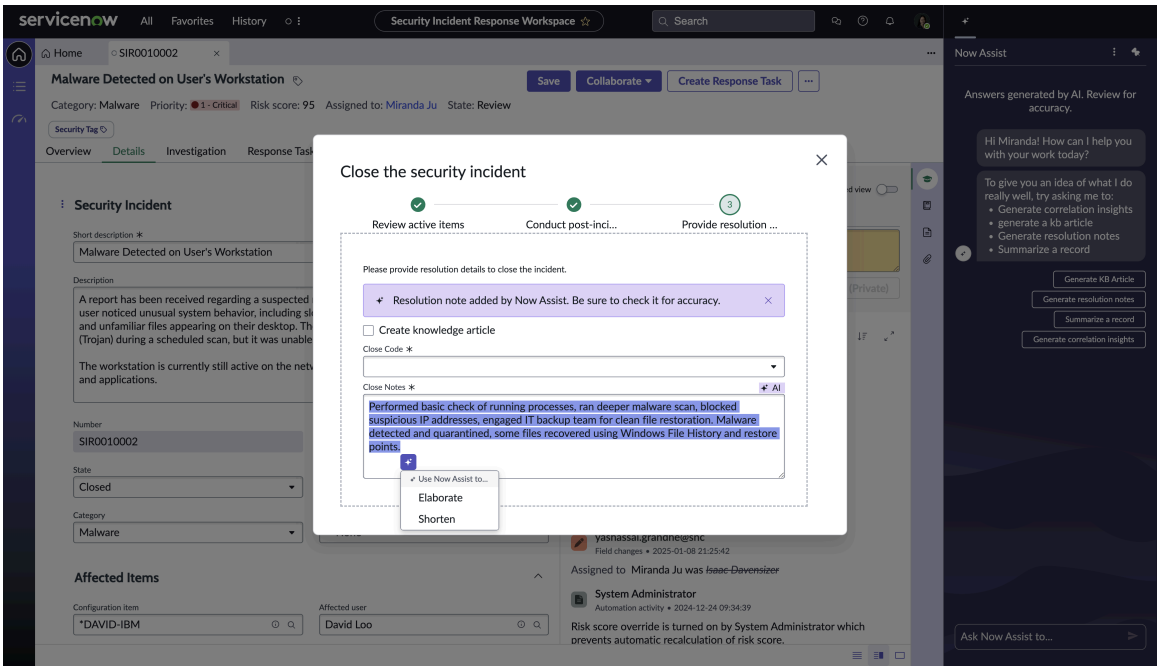


Automatisch generierte Lösungshinweise aus dem Security Incident Response-Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Bearbeiten Sie die mit dem Now Assist-Kontextmenü im Security Incident Response-Arbeitsbereich generierten Lösungshinweise.



Automatische Übersetzung

Generieren Sie mit empfohlene Aktionen für einen Security Incident Now Assist für Security Incident Response

Generieren Sie automatisch die nächsten Schritte, die Ihre Analysten ausführen können, um einen Security Incident im Security Incident Response-Arbeitsbereich zu schließen. Die empfohlenen Schritte basieren auf vorhandenen Security Incidents und Wissensartikeln.

Vorbereitungen

Die empfohlenen nächsten Schritte funktionieren für aktive Security Incidents in allen anderen Status als **Geschlossen** oder **Abgebrochen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anwendung „KI-Suche“ muss aktiviert sein, damit die Kompetenz „Empfohlene Aktionen“ für Security Incidents funktioniert. Um zu überprüfen, ob die KI-Suche in Ihrer Instanz aktiviert ist, navigieren Sie zu **Alle** > **KI-Suche** > **Status der KI-Suche**. Wenden Sie sich an den Support, wenn auf der Seite angezeigt wird, dass die KI-Suche nicht aktiviert ist.

Erforderliche Rolle: sn_si.analyst, sn_si.manager oder sn_si.basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
2. Wählen Sie in der kontextabhängigen Sidebar das Symbol **Empfohlene Aktionen** ( ).

3. Wählen Sie **Empfehlungen abrufen**aus.
4. Wählen Sie im Modal zum Überprüfen des KI-generierten Inhalts die Option **Ich bestätige aus**.
   Die generierten empfohlenen Aktionen werden in Karten angezeigt. Bis zu vier Referenzen für die Aktionen werden oben angezeigt. Diese Referenzen können eine beliebige Kombination aus Wissensartikeln (KB) oder Security Incidents (SIR#) sein.
5. Wählen Sie auf einer Karte eine aus.
6. **Wahlweise:** Wählen Sie im Bereich Empfohlene Aktionen das Aktualisierungssymbol, um die empfohlenen Aktionen erneut zu generieren.

   Die empfohlenen Aktionen bleiben eine Stunde lang im Cache. In folgenden Fällen können Sie die empfohlenen Schritte aktualisieren:

   - Sie sind der Meinung, dass Informationen im Zusammenhang mit dem Security Incident seit dem letzten Generieren der Aktionen geändert wurden.
   - Sie verlassen die Seite, melden sich ab, melden sich wieder an und kehren innerhalb von einer Stunde zum Security Incident zurück.

   Sie müssen die Aktionen ab Schritt 3 neu generieren, um sie nach einer Stunde anzuzeigen.
7. Wählen Sie auf einer Karte **Antwortaufgabe erstellen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Arbeitsbereich wird eine neue Registerkarte geöffnet. Die Felder **Kurzbeschreibung** und **Beschreibung** werden automatisch anhand der Details auf der ausgewählten empfohlenen Aktionskarte ausgefüllt.

8. Bearbeiten Sie das Formular nach Bedarf, und wählen Sie **Speichern**, um die Antwortaufgabe zu erstellen. Bis Sie den Wert in der Systemeigenschaft ändern, bleiben die beiden Optionen für alle von Ihnen generierten empfohlenen Aktionen **Details anzeigen** und **Antwortaufgabe erstellen**.
9. **Wahlweise:** Erstellen Sie eine Antwortaufgabe aus den empfohlenen Aktionen.
   Standardmäßig bietet Ihnen der Workflow die Möglichkeit, die empfohlenen Aktionen in Arbeitsnotizen von den Karten zu speichern. Wenn Sie die Möglichkeit haben möchten, eine Antwortaufgabe aus einer Aktionskarte zu erstellen, anstatt sie in Arbeitsnotizen zu speichern, müssen Sie das Feld Wert für die Systemeigenschaft **„Empfohlene SecOps-Aktion"** [sn_sec_ra.card_action_config] ändern.

   a. Navigieren Sie als Benutzer mit der Rolle „Security Incident Manager" [sn_si.manager] zu sys_properties.LIST.

   b. Suchen Sie die Systemeigenschaft „Empfohlene SecOps-Aktion" [sn_sec_ra.card_action_config], und öffnen Sie den Datensatz.

   c. Ändern Sie den Wert von „share_to_work_notes" in „create_task".

   d. Speichern Sie den Datensatz.

   e. Kehren Sie zum Security Incident-Datensatz zurück, und aktualisieren Sie die Seite.
   Die Aktionskarten bieten Ihnen die Optionen **Details anzeigen** und **Antwortaufgabe erstellen**.

Generieren Sie mit eine Nachfolgeanalyse für einen Security Incident Now Assist für Security Incident Response

Generiert automatisch eine Nachfolgeanalyse für einen Security Incident, die eine Ursachenanalyse, eine Folgenabschätzung sowie Lern- und Empfehlungsinformationen enthält.

Vorbereitungen

Sie müssen die Kompetenz „Nachfolgeanalyse nach Incident" aktivieren, wenn Sie möchten, dass die Nachfolgeanalyse nach dem Incident automatisch von Now Assist für Security Incident Responsegeneriert wird.

Wenn die Abschlussnotizen bereits vor dem Schließen des Security Incidents manuell ausgefüllt wurden, wird dieser Inhalt nicht von Now Assist für Security Incident Response überschrieben, wenn Analysten das Feld „Status" auf **Geschlossen**festlegen.

Erforderliche Rolle: sn_si.analyst, sn_si.manager oder sn_si.basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
2. Wählen Sie auf der Registerkarte **Details** im Feld Status die **Option Geschlossen aus**, um den Security Incident zu schließen.
   Das Modal Security Incident schließen wird geöffnet.
3. **Wahlweise:** Wählen Sie **Aktive Aufgaben überprüfen** aus, um alle aktiven Korrekturaufgaben zu überprüfen, die diesem Incident zugeordnet sind.

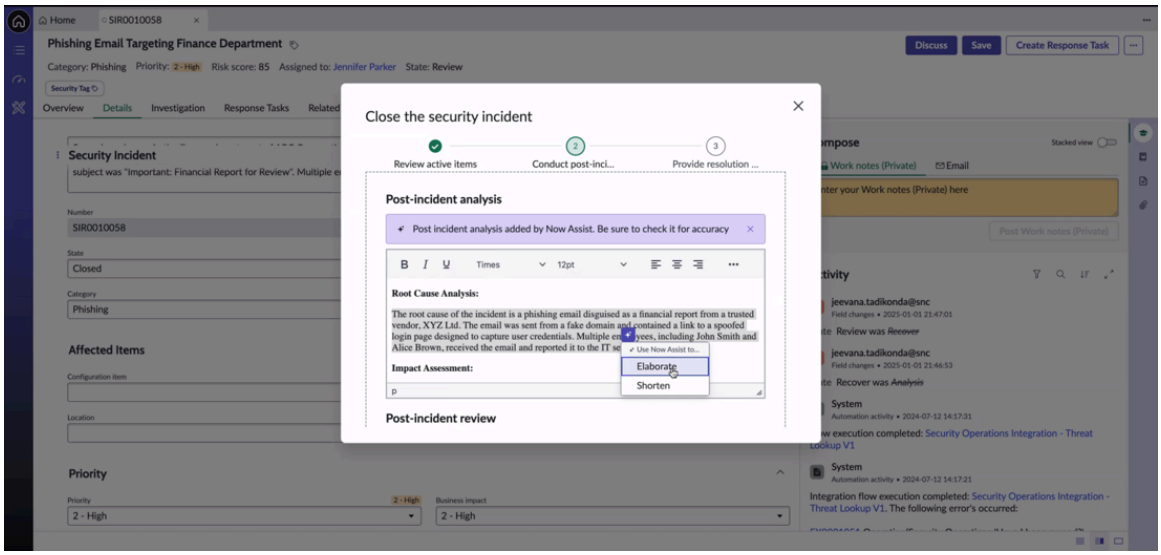
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine neue Registerkarte mit Datensätzen zur Überprüfung wird geöffnet. Verwenden Sie diese Option, um zu überprüfen, ob Sie zum Schließen des Security Incident bereit sind, da diese Aktion alle zugehörigen Workflows und Aktivitäten abbricht und den Incident für alle zugehörigen Korrekturaufgaben schließt.

4. Um die Nachfolgeanalyse des Incidents zu generieren, wählen Sie **Weiter**aus.
   Die Nachfolgeanalyse des Incidents wird im Modal mit drei Abschnitten angezeigt. Beachten Sie, dass das Now Assist-Symbol (✦) anzeigt, dass der Inhalt von Now Assist für Security Incident Responsegeneriert wird.
   - Analyse der zugrunde liegenden Ursache
   - Auswirkungsbewertung
   - Erkenntnisse und Empfehlungen

   Hinweis:
   Sie können das Now Assist-Kontextmenü in jeder der Optionen für die Nachfolgeanalyse von verwenden, die Ursachenanalyse/Auswirkungsbewertung/Lernergebnisse und Empfehlungen ausarbeiten oder kürzen und den Text ersetzen. **Mit der Option „Ausarbeiten“** können Sie dem vorhandenen Text weitere Informationen hinzufügen. **Durch das Kürzen** wird der ausgewählte Text prägnanter.

Der folgende Screenshot zeigt, wie das Now Assist-Kontextmenü verwendet wird, um den gewünschten Text für die Nachfolgeanalyse eines Incidents auszuarbeiten, zu kürzen und zu ersetzen.



5. Überprüfen Sie den Bericht auf Richtigkeit, und nehmen Sie die erforderlichen Änderungen vor.
6. **Wahlweise:** Wählen Sie **Bewertung durchführen** und **Bericht konfigurieren/Vorschau anzeigen,** um die Überprüfung nach dem Incident durchzuführen.
   Alle Änderungen, die Sie an der Überprüfung nach Incident vornehmen, werden eine Stunde lang gespeichert, wenn Sie diese Seite verlassen, um die Bewertung vorzunehmen oder eine andere Aktion auszuführen. Nach einer Stunde müssen Sie den Status für den Incident erneut auf **Geschlossen** setzen, um die Nachfolgeanalyse und Abschlussnotizen zum Incident neu zu generieren.
7. Wählen Sie **Weiter** aus, um die Lösungshinweise zu generieren.
   Die Lösungshinweise werden im Feld Abschlussnotizen angezeigt.
8. Wählen Sie einen aus der Liste für den Lösungscode aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie **Incident schließen aus**.
   Die Nachfolgeanalyse zum Incident wird im Feld Analyse nach dem Incident auf der Registerkarte Details und auf der Registerkarte Übersicht für Security Incidents im Security Incident Response-Arbeitsbereich gespeichert.

Korrelationseinblicke mit erkunden Now Assist für Security Incident Response

Sie wählen die Kriterien aus einem Security Incident aus, auf denen die Korrelationseinblicke basieren sollen.

Wichtige Hinweise zum Generieren von Korrelationseinblicken

- Sie können im Security Incident Response-Arbeitsbereich oder in der veraltet -UI (UI16) Korrelationseinblicke aus einem Security Incident-Datensatz in jedem Status generieren.
- Standardmäßig suchen Korrelationseinblicke nach übereinstimmenden Datensätzen aus den letzten 30 Tagen.
- Sie können die Werte für die Filter **Konfigurationselement**, **Betroffener Benutzer**und **Erkennbare Elemente** für Korrelationseinblicke auf der Registerkarte **Details** im Security Incident Response-Arbeitsbereich oder in den zugehörigen Listen **Konfigurationselemente**, **Betroffene Benutzer**und **Erkennbare Elemente** in der UI veraltet suchen und überprüfen (UI16).
- Ihre Suchkriterien und Ergebnisse werden im Bereich Now Assist angezeigt, bis Sie die Konversation zurücksetzen. Um Ihre Konversation zurückzusetzen, wählen Sie im Bereich das Zurücksetzen Now Assist - Menüsymbol ( ) und dann **Konversation zurücksetzen**aus.
- Sie müssen Zugriff auf die folgenden Tabellen haben, um diese Datensätze in den generierten Korrelationseinblicken anzeigen zu können:
  - Configuration Item-Tabelle [cmdb_ci].
  - Incident-Tabelle [incident].
  - Tabelle „Change-Anforderung“ [change_request].
  - Problemtabelle [problem].
  - Tabelle für angreifbare Elemente [sn_vul_vulnerable_item].
  - Ordnen Sie die Tabelle für erkennbare Elemente [sn_ti_observable] zu.
- Ihre Ergebnisse für Korrelationseinblicke basieren auf den Tabellen, auf die Sie Zugriff haben. Wenn Sie beispielsweise angreifbare Elemente (VIT) in den Ergebnissen für Korrelationseinblicke anzeigen möchten, müssen die Anwendung Vulnerability Response und die Lesezugriffsrolle (sn_vul.read_all) installiert sein.

Schritte zum Generieren von Korrelationseinblicken finden Sie unter Generieren Sie Korrelationseinblicke mit Now Assist für Security Incident Response.

Generieren Sie Korrelationseinblicke mit Now Assist für Security Incident Response

Generieren Sie Korrelationseinblicke im Bereich Now Assist, um vergangene Ereignisse mit dem Security Incident zu verbinden, an dem Sie arbeiten. Sie können die zugehörigen Informationen, die Sie generieren, verwenden, um zu vermeiden, dass Ihre Ermittlungen in Bezug auf betroffene Benutzer, Konfigurationselemente und erkennbare Elemente duplizieren, und helfen Sie Ihnen, den Incident, an dem Sie arbeiten, schneller zu lösen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Kompetenz „Generierung von Korrelationseinblicken“ muss aktiviert werden, bevor die Option **Korrelationseinblicke generieren** im Bereich Now Assist angezeigt wird.

Wenn der Bereich Now Assist nicht angezeigt wird, müssen Sie ihn aktivieren. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

Weitere Informationen zu Suchen nach Korrelationseinblicken finden Sie unter Korrelationseinblicke mit erkunden Now Assist für Security Incident Response.

Erforderliche Rolle: sn_si.analyst, sn_si.manager oder sn_si.basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
2. Alternativ können Sie in der veraltet UI (UI16) in der Tabelle „Security Incidents“ [sn_si_incident] nach einem Security Incident suchen und ihn öffnen.
3. Wählen Sie das Symbol Now Assist ( ) im oberen Header, um den Bereich Now Assist zu öffnen.
4. Wählen Sie **Korrelationseinblicke generieren**aus.

   Korrelationseinblicke werden generiert, wenn einer oder mehrere der folgenden Werte übereinstimmen. Im Bereich Now Assist werden die folgenden Filter angezeigt, auf denen Ihre Einblicke basieren. Es werden nur die Filter angezeigt, die Übereinstimmungen mit anderen Security Incidents aufweisen.

   Hinweis:
   Wenn kein Security Incident-Datensatz geöffnet ist, werden Sie aufgefordert, die Nummer für einen Security Incident-Datensatz einzugeben, nachdem Sie **Korrelationseinblicke generieren**gewählt haben.

   - **Configuration Item** (CI): Datensätze mit demselben CI, mit denen Sie potenzielle Schwachstellen in bestimmten Systemen identifizieren können. Ein Beispiel könnte der Laptop eines Benutzers sein.
   - **Betroffener Benutzer**: Frühere Incidents, die denselben Benutzer haben, damit Sie Muster wie häufige Phishing-Versuche oder mehrere nicht autorisierte Zugriffsversuche erkennen können. Ein Beispiel ist der Name eines bestimmten Benutzers.
   - **Erkennbare Elemente**: Datensätze, die durch gemeinsam genutzte erkennbare Elemente verknüpft sind, die auf potenzielle laufende Angriffe oder die wiederholte Verwendung einer schädlichen Infrastruktur hindeuten. Beispiele können IP-Adressen, URLs oder Datei-Hashes sein. Beachten Sie, dass Sie einen genauen Wert für ein erkennbares Element eingeben müssen, z. B. einen vollständigen Datei-Hash.

   Wenn für keinen dieser Filter übereinstimmende Daten vorhanden sind, werden keine angezeigt. Sie werden aufgefordert, dem Security Incident, an dem Sie arbeiten, einen dieser Werte hinzuzufügen, ihn zu speichern, Ihre Konversation im Bereich zurückzusetzen und es erneut zu versuchen.

5. Um Ihre Konversation zurückzusetzen, wählen Sie im Bereich das Symbol zum Zurücksetzen des Menüs Now Assist ( ) und dann **Konversation zurücksetzen**.
6. Wählen Sie einen Filter aus.

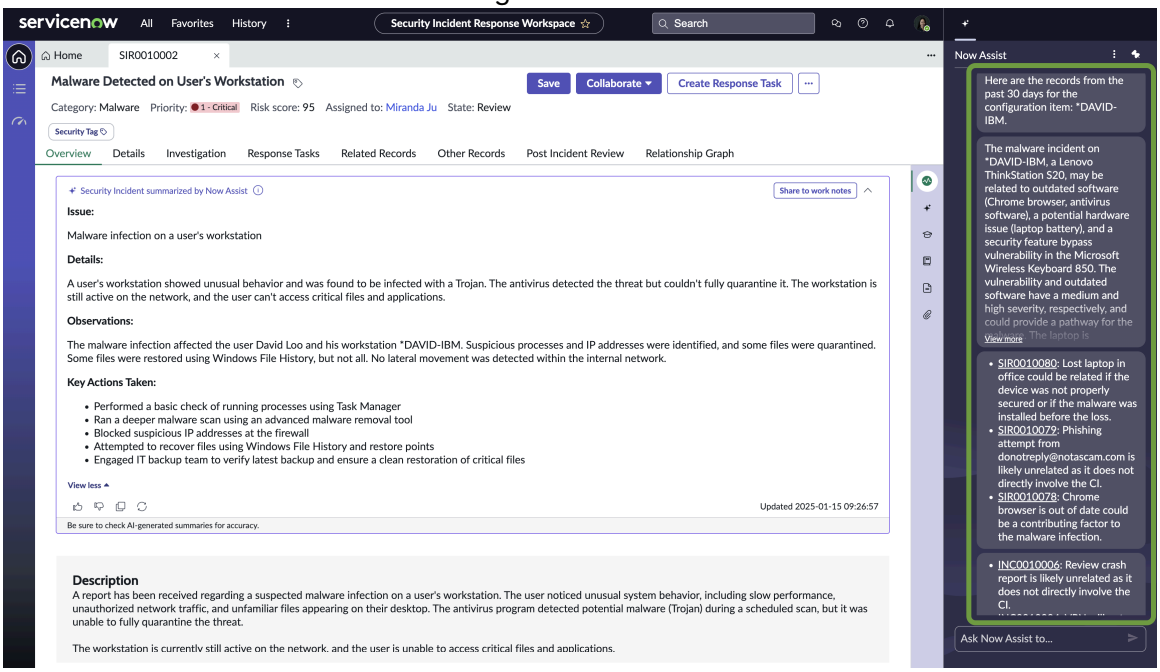
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übereinstimmende Ergebnisse werden im Bereich Now Assist angezeigt.

Im folgenden Beispiel wurde **Configuration item** angefordert. Die Suche hat eine allgemeine Zusammenfassung und Links zu Datensätzen zurückgegeben, die ein übereinstimmendes Konfigurationselement aufweisen.

Die Ergebnisse sind nach Datensatztyp gruppiert: Security Incident Record (SIR), Incident (INC), Change-Anforderung (CHG), Problem (PRB) und angreifbares Element (VIT).

- Der Filter Betroffene Benutzer gibt zurück: SIR-, INC- und CHG-Datensätze.
- Das Filterelement Configuration (Konfiguration) gibt zurück: SIR-, INC-, CHG-, PRB- und VIT-Datensätze.
- Der Filter für erkennbare Elemente gibt SIR-Datensätze zurück.



7. **Wahlweise:** Gehen Sie folgendermaßen vor, um das 30-Tage-Limit für die Abfrage zu ändern:
   a. Navigieren Sie als Benutzer mit der Rolle „Security Incident Manager“ [sn_si.manager] zu sys_properties.LIST.
   b. Suchen Sie die Systemeigenschaft Rückblickzeitraum für Korrelation [sn_sec_gen_ai.correlation_lookback_period], und öffnen Sie den Datensatz.
   c. Geben Sie im Feld **„Wert“** eine Zahl bis zu 360 ein.
   d. Speichern Sie den Datensatz.
   e. Kehren Sie zum Security Incident-Datensatz zurück, und aktualisieren Sie die Seite.

Generative KI-Kompetenzen im Bereich Now Assist für Now Assist für Security Incident Responseanfordern

Fordern Sie im Bereich Now Assist eine Zusammenfassung des Security Incidents oder Abschlussnotizen an.

Vorbereitungen

Unter Now Assist panel erfahren Sie, wie Sie den Bereich Now Assist aktivieren.

Erforderliche Rolle: si_analyst, si_manager oder sn_si.basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei einer Instanz an, auf der die Anwendung Now Assist für Security Incident Response installiert ist.
2. Navigieren Sie in der Core-UI von veraltet zu **Alle** > **Security Incident** > **Incidents** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
3. Alternativ navigieren Sie zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** und öffnen Sie einen Ihnen zugewiesenen Security Incident.
4. Wählen Sie im oberen Banner das Now Assist-Symbol ( ).

Anwendungsfälle von KI-Agent in Now Assist für Security Incident Responseverwenden

Verwenden Sie die KI-Agents Security Incident Response, um Ihre Aufgaben autonom zu erledigen.

Verfügbarer Anwendungsfall für KI-Mitarbeiter für Security Incident Response

Name des Anwendungsfalls	Beschreibung	Verfügbare KI-Agents
Schließen Sie den Security Incident	Dieser Anwendungsfall hilft den Sicherheitsanalysten, einen Security Incident mit natürlicher Sprache im Bereich Now Assist zu schließen.	Nachbearbeitungsgenerator für Security Incidents

Wichtig:
Standardmäßig sind alle Anwendungsfälle und KI-Agent-Datensätze schreibgeschützt.

Um einen Anwendungsfall zu ändern, müssen Sie zuerst Duplicate an agentic workflow und dann die folgenden Schritte ausführen:

- Aktivieren Sie den Anwendungsfall.
- Aktivieren Sie alle KI-Agents innerhalb des Anwendungsfalls.
- Bei Bedarf können Sie einen Auslöser hinzufügen, um den Anwendungsfall automatisch aufzurufen.

Möglicherweise sind mit der Anwendung Now Assist KI-Agents installiert, die nicht in Anwendungsfällen verwendet werden. Informationen zum Anzeigen aller für Sie verfügbaren Service Desk-Mitarbeiter finden Sie unter KI-Service Desk-Mitarbeiter suchen .

Security Incident Response Anwendungsfall „KI-Agent-Erfassung – Security Incident schließen“.

Mit dem Anwendungsfall Security Incident schließen können Sicherheitsanalysten einen Security Incident schließen.

Übersicht über Anwendungsfall „Security Incident schließen“.

Wenn Sie den Anwendungsfall „Security Incident schließen“ verwenden, brechen Sie die zugehörigen Antwortaufgaben ab, generieren Sie Lösungsnotizen, schließen Sie Notizen ab, schließen Sie Code und Analyse nach Incident (Post Incident Analysis, PIA) während

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

des Abschlusses eines Security Incident, geben Sie Feedback und passen Sie Inhalte in natürlicher Sprache über Now Assist an. Bereich.

Wenn Sie diesen Anwendungsfall ändern möchten, können Sie ihn duplizieren , die Einstellungen an Ihre spezifischen Bedürfnisse anpassen und stattdessen die duplizierte Version des Anwendungsfalls aktivieren.

Agent, der im Anwendungsfall „Security Incident schließen“ verwendet wird

Der Experte für den Nachbearbeitungsgenerator für Security Incidents wird im Anwendungsfall „Security Incident schließen“ verwendet.

Tools, die dem Anwendungsfall „Security Incident schließen“ zugeordnet sind

Die folgenden Tools sind einem KI-Agent zugeordnet, der im Anwendungsfall „Security Incident schließen“ verwendet wird.

Tools, die zum Schließen eines Security Incident zugeordnet sind

Tooltyp	Ausführungsmodus	Name	Beschreibung
Skripte	Autonom	Ruft Details zu Security Incidents ab	Tool zum Abrufen der Security Incident-Details aus der Security Incident-Nummer.
Skripte	Autonom	Ruft Abschlusscodewerte ab	Tool zum Abrufen verfügbarer Abschlusscodewerte für den Security Incident.
Skripte	Autonom	Schließt den Security Incident als falsch positiv	Tool, das verwendet wird, wenn der Incident als falsch positiv geschlossen wird.
Skripte	Autonom	Aktualisiert den Security Incident	Tool zum Aktualisieren eines Felds des Security Incident.
Subflow	Autonom	Generiert Abschlussnotizen	Tool zum Generieren von Abschlussnotizen für den Security Incident.
Subflow	Autonom	Generiert Nachfolgeanalysen nach Incidents	Tool zum Generieren der Nachfolgeanalyse für den Security Incident.

Auslöser für den Anwendungsfall „Security Incident schließen“.

Für diesen Anwendungsfall sind keine Auslöser vorhanden. Bei Bedarf können Sie einen Auslöser hinzufügen, um den Anwendungsfall automatisch aufzurufen.

Schließen Sie einen Security Incident

Chatten Sie mit einem KI-Mitarbeiter im Bereich Now Assist, um einen Security Incident zu schließen.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst oder sn_si.manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

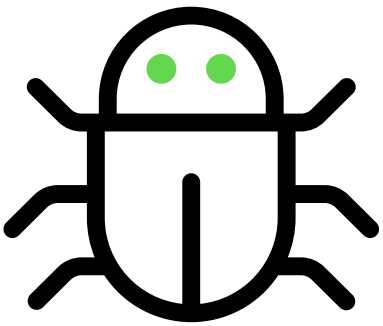
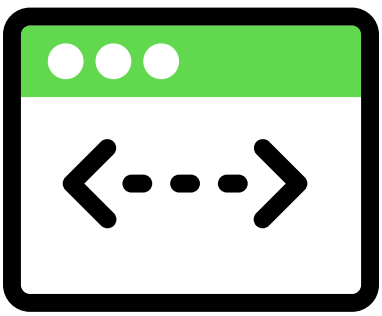
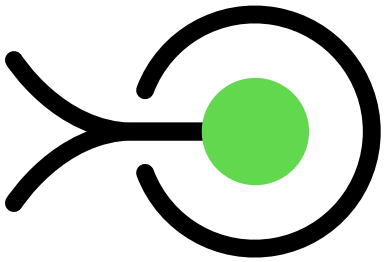
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie den Security Incident, den Sie schließen möchten, mithilfe des KI-Agenten.
3. Wählen Sie das Symbol Now Assist ( ).
   Der Bereich Now Assist wird angezeigt.
4. Schließen Sie den Security Incident, indem Sie eine der folgenden Optionen verwenden.

Anwendungen für die Angriffsoberflächenverwaltung

Vulnerability Response und andere Anwendungen, aus denen die Angriffsoberflächenverwaltung besteht, helfen Ihnen bei der Priorisierung Ihrer angreifbaren Assets und fügen Kontext hinzu, um Sie zu bestimmen, wenn geschäftskritische Systeme gefährdet sind. Mit der CMDB können Ihre Sicherheitsteams auch problemlos systemübergreifende Abhängigkeiten identifizieren und die geschäftlichen Auswirkungen von Changes oder Ausfallzeiten schnell bewerten.

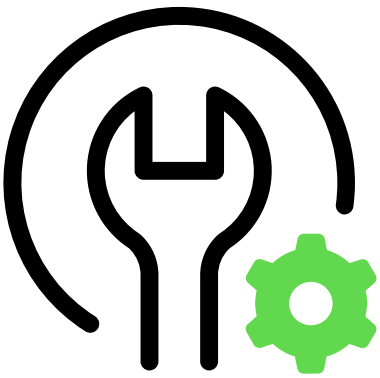
Vulnerability Response Anwendungen

Vulnerability Response	Application Vulnerability Response	Container Vulnerability Response
		
Erfahren Sie mehr über die Anwendung Vulnerability Response	Erfahren Sie mehr über die Anwendung Application Vulnerability Response	Erfahren Sie mehr über die Anwendung „Container Vulnerability Response“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Anwendungen (Fortsetzung)

Konfigurations-Compliance



Erfahren Sie mehr über die Anwendung Configuration Compliance

Software-Stückliste

Erfahren Sie mehr über die Software-Stücklisten-Anwendungen

Vulnerability Response Arbeitsbereiche

Arbeitsbereich des Schwachstellenmanagers

Erfahren Sie mehr über den Arbeitsbereich des Schwachstellenmanagers

Arbeitsbereich für IT-Korrekturen

Erfahren Sie mehr über den Arbeitsbereich für IT-Fehlerkorrekturen

Arbeitsbereich der Schwachstellenbewertung

Erfahren Sie mehr über den Arbeitsbereich der Schwachstellenbewertung

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community

Automatische Übersetzung

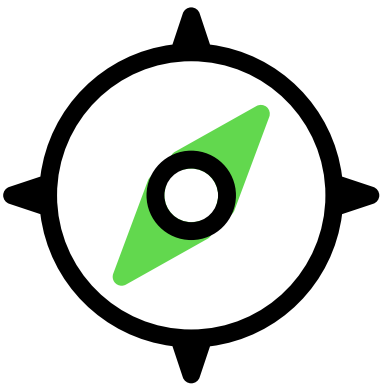
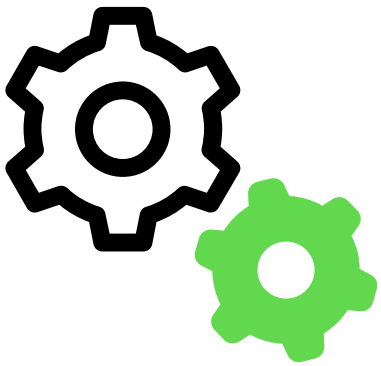
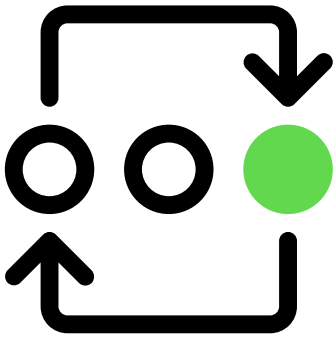
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Vulnerability Response

Die National Vulnerability Database (NVD) und andere Quellen sammeln Informationen zu bekannten Schwachstellen. Diese Schwachstellen können Schwachstellen in Software, Betriebssystemen, die von Malware ausgenutzt werden können, und andere Angriffe umfassen. Die Anwendung ServiceNow® Vulnerability Response unterstützt Sie bei der Nachverfolgung, Priorisierung und Behebung dieser Schwachstellen.

Vulnerability Response

Untersuchen	Einrichten und konfigurieren	integrieren
		
Erfahren Sie mehr über die Funktionen von Vulnerability Response	Installieren Sie Ihre Vulnerability Response-Anwendung, und richten Sie sie ein	Erweitern Sie Vulnerability Response durch die Integration mit anderen Anwendungen

Automatische Übersetzung

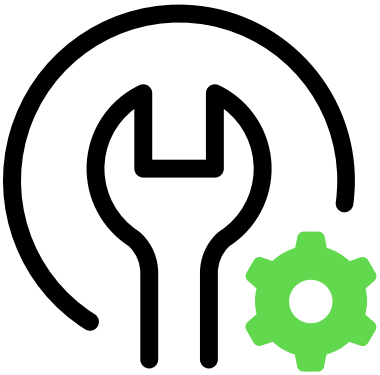
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response (Fortsetzung)

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

Erfahren Sie, wie Sie in den Arbeitsbereichen für Schwachstellenmanager, IT-Korrektur und Schwachstellenbewertung VITs überwachen, verwalten und beheben.

Beheben

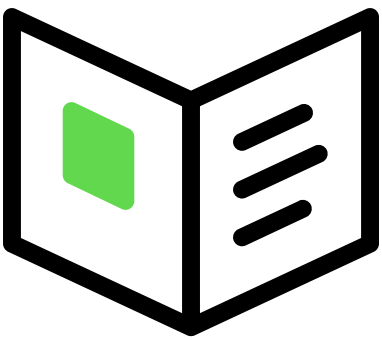


Verwenden Sie die Funktionen von Vulnerability Response, um Ihre Schwachstellen zu beheben und Ihre Assets zu schützen

Analytics und Reporting

Überwachen Sie den Korrekturfortschritt

Referenz



Erhalten Sie weitere Details zu Vulnerability Response-Versionshinweisen und -Komponenten sowie Referenzinformationen zu Feldern, Tabellen und Eigenschaften

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Die Anwendung Vulnerability Response erkunden

Die Anwendung ServiceNow® Vulnerability Response importiert und gruppiert angreifbare Elemente automatisch anhand von Regeln, mit denen Sie Schwachstellen schnell beheben können. Schwachstellendaten werden aus externen Quellen wie der National Vulnerability Database (NVD) und Integrationen von Drittanbietern abgerufen und mit von ServiceNow®entwickelten Anwendungen verarbeitet.

Sehen Sie sich eine Übersicht über Vulnerability Response an, in der angreifbare Elemente, Korrekturaufgaben und ihre Lebenszyklen definiert werden.

Übersicht über die typische Vulnerability Response innerhalb eines Unternehmens und die Vulnerability Response mit ServiceNow. Definiert angreifbare Elemente, Schwachstellen-Gruppen und deren Lebenszyklen.

Vulnerability Response und Ihre Unternehmensumgebung

In einer Enterprise-Umgebung verwenden Unternehmen normalerweise Schwachstellenscanner und Bewertungstools, um die Risiken zu identifizieren und zu verwalten, die Schwachstellen für ihre Assets darstellen. Von diesen Tools identifizierte Schwachstellen stellen Risiken für die Sicherheits- und IT-Teams dar, die für die Wartung und den Schutz der Assets einer Organisation verantwortlich sind. Einige Risiken umfassen unter anderem die folgenden Arten von identifizierten Schwachstellen:

- Abhängigkeit von veralteter Software oder falsch konfigurierten Systemen
- Ungesicherte Netzwerkprotokolle
- Abhängigkeit von fehlerhaften Softwarebibliotheken von Drittparteien
- Schlechte oder inkonsistente Systemadministrations-Hygiene
- Bilder des Baselinesystems, die nicht gehärtet sind

Da diese potenziellen Risiken offengelegt sind, stehen Sicherheits- und IT-Teams häufig vor Herausforderungen bei der Verarbeitung und Handhabung der Menge an Schwachstelleninformationen, die von ihren Scan- und Bewertungstools generiert werden. Insbesondere sind diese Teams überfordert, wenn sie eine große Anzahl identifizierter Schwachstellen verwalten und umsetzbare Antwortmaßnahmen entwickeln müssen, um die potenziellen Risiken zu minimieren, denen ihre Organisationen ausgesetzt sind.

Sie können diese Herausforderungen für Ihre eigene Sicherheitslage identifizieren, indem Sie die folgenden Fragen stellen:

- Welche identifizierten Schwachstellen sollten zuerst überprüft werden?
- Was bedeuten diese identifizierten Schwachstellen für unsere Organisation?
- Wer sollte für identifizierte Risiken verantwortlich sein und besitzen?
- Wer sollte praktisch sein und an der Lösung/Minderung dieser Risiken arbeiten?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wie können wir identifizierte Schwachstellen mit den vorhandenen Ressourcen effektiv mindern?
- Was sind die potenziellen unbeabsichtigten Ergebnisse der Reduzierung der identifizierten Schwachstellen?
- Welchen Prozess verfolgen wir, um Schwachstellen zu beheben, die unternommenen Schritte nachzuverfolgen und nachzuverfolgen, um sicherzustellen, dass unsere Aktionen funktioniert haben?
- Woher wissen wir, ob wir Fortschritte bei der Reduzierung unserer Gesamtrisikoposition machen?

Vulnerability Response, Security Operations und Now Platform®

Die Anwendung Vulnerability Response ist Teil der Security Operations- Suite. Zusammen helfen Ihnen diese Anwendungen, Ihre Assets zu schützen, indem Sie Ihren allgemeinen Sicherheitsstatus verbessern.

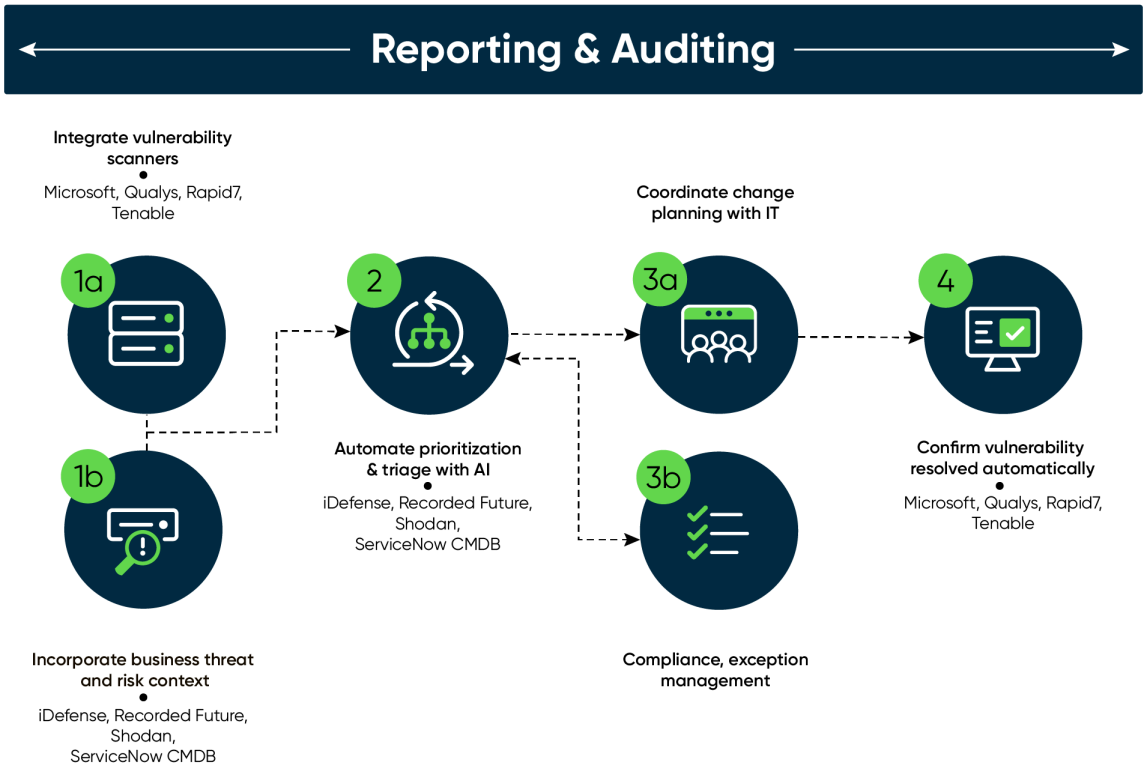
Die Anwendung ServiceNow Vulnerability Response hat zwei Hauptziele:

- Unterstützen Sie die Sicherheitsteams, die mit dem Umgang mit großen Mengen an Schwachstellendaten konfrontiert werden.
- Unterstützen Sie die Betriebsteams, die mit der Behebung von Schwachstellen beauftragt sind.

Auf diese Weise können Sie mit der Anwendung Vulnerability Response den Informationsfluss automatisieren – von der Integration über die Untersuchung bis zur Lösung.

Der Schwachstellenmanagement-Prozess in Now Platform® kann Prozesse, Daten, Berichterstellung und Automatisierung mit CMDBumfassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Integrieren Sie Scanner von Drittanbietern und ServiceNow® -Anwendungen mit der Anwendung Vulnerability Response, um bekannte Schwachstellendaten zu erfassen.
- Erweitern Sie Ihre erfassten Schwachstellendaten mit Exploit-, Threat Intelligence-, Risiko- und Geschäftskontext. Verwenden Sie diese Daten, um Patch- und Korrekturstrategien zu entwickeln.
- Importierte Schwachstellen aus dem NVD und Erkennungsdaten aus Drittanbieterprodukten werden mit den Assets in Ihrer CMDB abgeglichen. Eine Selektierung kann Folgendes umfassen: Erstellen von Korrekturaufgaben, die aus mehreren angreifbaren Elementen bestehen, d. h. Ihren Assets, für die ermittelte Schwachstellen vorhanden sind, Gruppieren dieser Aufgaben nach Kategorie, Priorisieren und Zuweisen an Teams.
- Nutzen Sie ein koordiniertes Change- und Ausnahmemanagement, um Schwachstellen zu beheben, die möglicherweise zusätzliche manuelle Eingriffe, mehr Zeit für die Lösung oder umfangreiche Untersuchungen erfordern.
- Bestätigen Sie, dass Schwachstellen automatisch durch Erkennungen Ihrer Scannerprodukte behoben und aktualisiert werden.

Wer in Ihrer Organisation möglicherweise Vulnerability Response verwendet

Vulnerability Response Benutzer teilen sich im Allgemeinen zwei Personae auf.

Schwachstellenanalyst

Die Persona des Schwachstellenanalysten befindet sich normalerweise in den Bereichen „Sicherheit“, „Risiko und Compliance“ oder „Verwaltung“. Diese Benutzer überwachen Schwachstellen und bestimmen, wann die Korrekturprozesse einzuleiten sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Der Schwachstellenanalyst verwendet Vulnerability Manager Workspace hauptsächlich zur Überwachung und Erstellung von Korrekturaufgaben.

Verantwortlicher für Korrektur

Die Persona des Korrekturbesitzers ist normalerweise ein Teil von IT Operations, DevOps/ Engineering oder ein Serviceverantwortlicher. Diese Benutzer führen die zur Behebung von Schwachstellen erforderlichen Korrekturaufgaben durch. Sie können Ausnahme- oder Change-Anforderungen einreichen, wenn kontrollierte Prozesse für die Wartung oder Entfernung von Assets erforderlich sind.

Wichtig:
Der Korrekturbesitzer arbeitet hauptsächlich innerhalb von IT Remediation Workspacean Korrekturaufgaben.

Application Vulnerability Response

Die Funktion Application Vulnerability Response (AVR) der Anwendung ServiceNow® Vulnerability Response importiert angreifbare Elemente (Application Vulnerable Items, AVITs) und kann gemäß den Regeln Anwendungsschwachstellen beheben. Es ist über ein separates Abonnement verfügbar. Die Dokumentation Application Vulnerability Response finden Sie unter Application Vulnerability Response erkunden.

Verfügbare Versionen

Ein Glossar mit Begriffen und weitere Referenzen, die neben Felddaten in den Formularen und Datensätzen in Vulnerability ResponseLinks, Artikel zur Problembehandlung und Wissensartikel enthalten, finden Sie unter Vulnerability Response Referenzinformationen.

Freigabeversion	Release-Hinweise
Vulnerability Response v23.0	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Installation von Vulnerability Response und unterstützten Anwendungen

Die Anwendung Vulnerability Response ist über den ServiceNow Storeverfügbar. Die Anwendung unterstützt andere ServiceNow -Anwendungen und Drittanbieterintegrationen, die Sie auch aus dem ServiceNow Storeherunterladen können. Weitere Optionen sind ebenfalls verfügbar, um das Basis-Setup zu erweitern.

Aufgaben für das grundlegende Setup

Die Anwendung Vulnerability Response ist als erster Schritt erforderlich. Weitere Informationen zur Installation von finden Sie unter Implementierungsprüfliste für die Anwendung Vulnerability Response und Anwendung Vulnerability Response installieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nach Abschluss der Installation können Sie Vulnerability Response mit dem Setup-Assistenten konfigurieren.

  Mit dem Setup-Assistenten können Sie Anwender und Gruppen für den Zugriff auf die Anwendung zuweisen, Zuweisungsregeln, Regeln für Korrekturaufgaben und Zieldaten erstellen oder bearbeiten und Risikorechner einrichten.

- Sie können auch eine oder mehrere unterstützte Drittanbieterintegrationen vom Setup-Assistenten auswählen, installieren und konfigurieren. Diese Integrationen rufen Schwachstellendaten von externen Systemen und Lieferanten ab. Weitere Informationen zur Funktionsweise von Integrationen und zu den von Vulnerability Responseunterstützten Integrationen finden Sie unter Vulnerability Response-Integrationen.
- Führen Sie vor der Implementierung von Drittanbieterintegrationen die geplante NVD-Integration und CWE-Aufgabe als Teil der Ersteinrichtung von Vulnerability Responseaus.

  Weitere Informationen zum Installieren, Konfigurieren und Anzeigen der NVD- und CWE-Bibliotheken finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien und Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus.

- Wählen Sie ggf. eine Analytics-Anwendung aus. Das Performance Analytics-Inhaltspaket für Vulnerability Response enthält Berichte, die alle Phasen des Vulnerability Management-Lebenszyklus abdecken.

  [Optional] Anwendung Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA].

- Wählen Sie ggf. eine Lösungsanwendung aus. Das Lösungsmanagement hilft Ihnen, die Schwachstellen in Ihrer Umgebung mit den Lösungen zu korrelieren, die sie beheben könnten. [Optional] Anwendung Solution Management for Vulnerability Response installieren.

  Hinweis:

  - Wenn die Anwendung Vulnerability Solution Management aktiviert ist, können Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration im Setup-Assistenten bearbeitet werden.

  - Vulnerability Solution Management erfordert ein separates Abonnement. Weitere Informationen finden Sie unter Vulnerability Solution Management.

- [Optional] Installieren Sie die App ServiceNow Agent und die Vulnerability Response App Mobile für Mobile Experience für Vulnerability Response.

Andere Setup-Aufgaben, die Sie ausführen können

Diese zusätzlichen Setupaufgaben ergänzen Ihre Basiskonfiguration und unterstützen die Remediation mit Optionen für die Berichterstellung, E-Mail-Benachrichtigungen, die Konfiguration der nativen Integration und die Arbeit mit angreifbaren Elementen. Die meisten dieser Aufgaben werden außerhalb des Setup-Assistenten ausgeführt. Weitere Informationen finden Sie unter Zusätzliche Setup- und Konfigurationsaufgaben für Vulnerability Response ..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Aufgaben außerhalb des Basis-Setups

Diese optionalen Konfigurationsaufgaben werden außerhalb des Setup-Assistenten durchgeführt, erfordern Codierungskenntnisse oder fortgeschrittene ServiceNow Kenntnisse und werden nicht als Teil der Basiskonfiguration betrachtet. Weitere Informationen finden Sie unter Erweiterte Konfigurationsaufgaben Vulnerability Response..

Vulnerability Response Personae und granulare Rollen

Bevor Sie Schwachstellen mit der Anwendung Vulnerability Response erfolgreich beheben können, müssen Sie Ihren Benutzern und Gruppen im Setup-Assistenten Personae und Rollen zuweisen.

Einer der ersten Konfigurationsschritte, die für die Anwendung Vulnerability Response erforderlich sind, ist das Zuweisen von Rollen zu Benutzern und Gruppen. Rollen definieren, was Benutzer und Gruppen in Vulnerability Response, Performance Analytics for Vulnerability Responseund allen Drittanbieterintegrationen mit Vulnerability Responsesehen und tun können.

Persona-Rollen weisen Sie vorhandenen Anwendern und Gruppen im Setup-Assistenten zu. Weitere Informationen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Hinweis:

Als Upgrade-Kunde können Sie Ihre vorhandenen Rollen für die Anwendung Vulnerability Response weiterhin verwenden. Der Zugriff für Anwender und Gruppen, denen vor v10.3 die Berechtigungen „sn_vul.vulnerability_read“ und „sn_vul.vulnerability_write“ und der Nachbesserungsbesitzer zugewiesen wurden, hat sich nicht geändert.

Um jedoch mehr Kontrolle darüber zu haben, was Benutzer und Gruppen in der Anwendung Vulnerability Response auf Aufgabenebene tun und sehen können, bevorzugen Sie möglicherweise die Verwendung von granularen Rollen. Weitere Informationen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Wenn Sie bereits Rollen mit dem Setup-Assistenten zugewiesen haben und granulare Rollenzuweisungen für alle Benutzer und Gruppen im Modul Benutzeradministration verwalten möchten, finden Sie weitere Informationen unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Persona-Rollen und granulare Rollen beginnen

Schlüsselbegriffe.

Rolle

Mit Rollen wird festgelegt, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können.

Gruppe

Eine Gruppe von Benutzern, die bestimmte Rollen und einen gemeinsamen Zweck teilen.

Persona-Rolle

Eine vorkonfigurierte Rolle in der -Anwendung, die aus mehreren granularen Rollen besteht. Die Persona-Rollen in Setup-Assistent, Schwachstellenadministrator, Schwachstellenanalyst, Korrekturbesitzer, Konfigurationselement-Manager und Ausnahmemanager entsprechen allgemeinen Berufsbezeichnungen für Manager, Analysten und Serviceverantwortliche in einer IT-Organisation oder einer Schwachstellenkorrekturgruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geerbte Rollen

Ein Begriff, der Rollen beschreibt, die Benutzer automatisch erwerben, wenn ihnen andere Rollen zugewiesen werden. Beispielsweise erben alle Benutzer oder Gruppen, denen die Persona-Rolle sn_vul.remediation_owner zugewiesen ist, auch die granularen Rollen sn_vul.read_assigned,sn_vul.write_assigned.

Zugriffssteuerungsliste (ACL)

Zugriffssteuerungslisten schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Um zu verhindern, dass Berichte verfügbar gemacht werden, legen Sie ab Vulnerability Response v16.5 die **Option Alle report_view-ACLs** auf *active=true*fest. Diese ACL stellt sicher, dass die geschützten Daten nur für autorisierte Anwender verfügbar sind.

Im Setup-Assistenten weisen Sie Gruppen und Anwender Persona-Rollen zu.

Hinweis:
Im Setup-Assistenten ist die Systemadministratorrolle (admin) für die Aufgaben im ersten Abschnitt erforderlich: Zuweisen von Rollen und Installieren von Integrationen. Nachdem Sie im Setup-Assistenten Persona-Rollen zugewiesen und Integrationen installiert haben, können Sie einen Benutzer oder eine Gruppe mit der Rolle sn_vul.vulnerability_admin zuweisen, um verbleibende Aufgaben im Setup-Assistenten abzuschließen und die Anwendung Vulnerability Response zu verwalten.

In der folgenden Tabelle sind die mit der Anwendung installierten Persona-Rollen Vulnerability Response aufgelistet.

Persona-Rollen für Vulnerability Response	Beschreibung
Zuweisen von sn_vul.vulnerability_admin: Schwachstellen-Administrator zu Anwendern oder Gruppen.	Benutzer mit dieser Rolle haben vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Benutzer mit dieser Rolle können alle VR-Anwendungen und Regeln konfigurieren und Drittanbieterintegrationen installieren.
Weisen Sie „sn_vul.vulnerability_analyst - Schwachstellenanalyst“ Anwendern und Gruppen zu.	Anwender und Gruppen mit dieser Rolle können alle Datensätze für die VI-Korrektur anzeigen und aktualisieren.
Zuweisen von sn_vul.remediation_owner: Korrekturbesitzer zu Anwendern und Gruppen.	Benutzer und Gruppen mit dieser Rolle beheben Schwachstellen, die ihnen oder einer Gruppe, der sie angehören, zugewiesen werden. Gruppen oder Anwender mit dieser Rolle können die ihnen oder einer Gruppe, der sie angehören, zugewiesenen Datensätze anzeigen und aktualisieren.
Weisen Sie sn_vul.ci_manager Benutzern und Gruppen zu.	Benutzer und Gruppen mit dieser Rolle verwalten die erneute Klassifizierung von nicht abgeglichenen Konfigurationselementen (Configurations Items, CI), die nicht in der Configuration Management Database (CMDB) gefunden wurden.
Weisen Sie Lesezugriff auf bestimmte Bereiche in der Anwendung nach Aufgabe zu.	Weisen Sie beispielsweise sn_vul.read_all zu, damit ein Benutzer alle VR-Datensätze anzeigen kann. Für Lesezugriff zum Anzeigen von Regeln für Korrekturaufgaben weisen Sie „sn_vul.read_group_rules“ zu. Anwender und

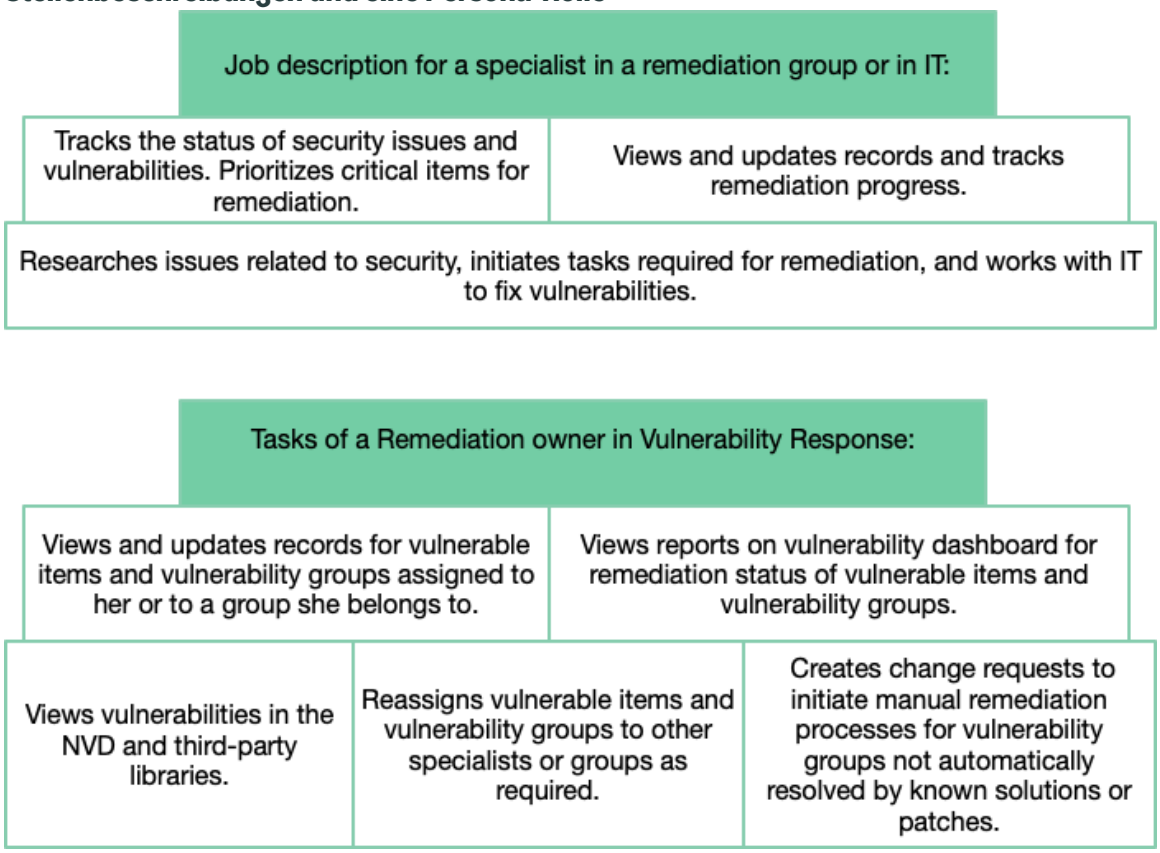
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rollen für Vulnerability Response	Beschreibung
	Gruppen mit dieser Rolle aktualisieren keine Datensätze.

Granulare Rollen und Persona-Rollen

Eine Möglichkeit, sich über Persona-Rollen Gedanken zu machen, besteht darin, zu überlegen, inwiefern sich ihre Beschreibungen auf Stellenbeschreibungen für verschiedene IT- oder Schwachstellenkorrektur-Positionen in Ihrer Organisation beziehen können. Die folgende Abbildung zeigt eine mögliche Stellenbeschreibung für einen Fehlerkorrekturspezialisten in der IT und wie sich die mit dieser Stelle verknüpften Aufgaben auf die Aufgaben einer Persona-Rolle für Korrekturbesitzer in der Anwendung Vulnerability Response beziehen.

Stellenbeschreibungen und eine Persona-Rolle



Sowohl die Stellenbeschreibung als auch die Persona-Rolle des Korrekturbesitzers können als eine Reihe von Korrekturaufgaben definiert werden. In der obigen Abbildung befinden sich eine Stellenbeschreibung und eine Persona-Rolle in grünen Blöcken über den Aufgaben, die sie beschreiben. In diesem Beispiel entsprechen einige der typischen Stellenanforderungen für einen Spezialisten in einer Korrekturgruppe direkt den Aufgaben, aus denen die Persona des Korrekturverantwortlichen in Vulnerability Responsebesteht: Datensätze überprüfen und aktualisieren, Korrekturstatus von Schwachstellen verfolgen, Elemente für die Korrektur priorisieren, und wenden mit der IT Korrekturen und Patches an.

Manchmal entsprechen die Aufträge in Ihrer Organisation jedoch möglicherweise nicht direkt den Aufgaben, aus denen eine der fünf Persona-Rollen in der Anwendung Vulnerability Response besteht. Aus verschiedenen Gründen, z. B. zum Schutz vertraulicher Daten oder zur Einhaltung von Vorschriften, müssen Sie den umfassenden Zugriff einschränken, den einige Persona-Rollen Ihren Benutzern und Gruppen gewähren. Umgekehrt müssen Sie Benutzern und Gruppen mehr Zugriff gewähren, damit sie ihre Aufgaben ausführen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mithilfe granularer Rollen können Sie Rollen einfach anpassen und den Zugriff steuern, den Benutzer und Gruppen auf Vulnerability Response, Performance Analytics for Vulnerability Responseund Integrationen von Drittanbietern haben.

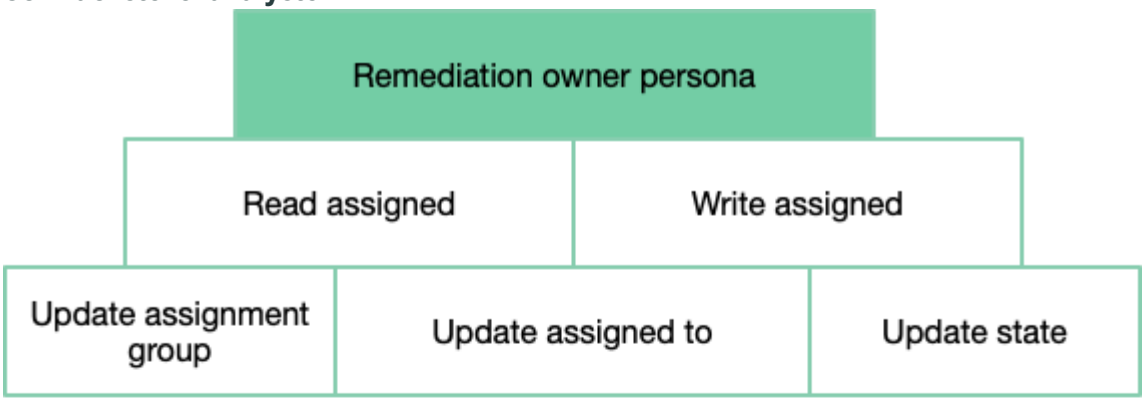
Die granularen Rollen definieren die Aufgaben

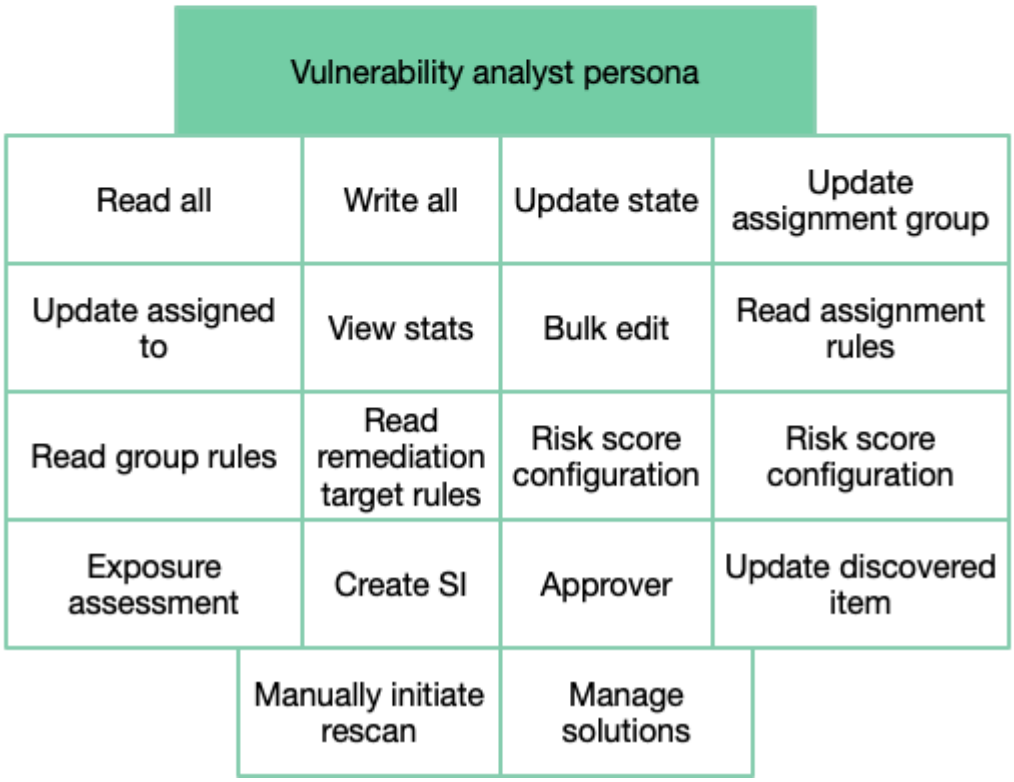
Die Namen der granularen Rollen in Vulnerability Response beschreiben normalerweise, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Beispiel: In der vorherigen Abbildung verfügen Benutzer und Gruppen mit zugewiesener Persona des Korrekturbesitzers über die granularen Rollen sn_vul.read_assigned und sn_vul.write_assigned. Mit diesen granularen Rollen können Benutzer oder Gruppen angreifbare Elemente und ihnen zugewiesene Korrekturaufgabendatensätze anzeigen und aktualisieren. Um Beschreibungen bestimmter granularer Rollen anzuzeigen, navigieren Sie als Benutzer mit der Systemadministratorrolle zu **Anwenderadministration** > **Rollen** und suchen Sie die gewünschte Rolle. Rollen, die automatisch geerbt werden, wenn eine Rolle zugewiesen wird, werden aufgelistet. Wenn eine Rolle von anderen Rollenzuweisungen abhängt, werden außerdem alle erforderlichen Rollen aufgelistet.

In der folgenden Abbildung sind die granularen Rollen der Persona des Verantwortlichen für die Korrektur und des Schwachstellenanalysten dargestellt. Beachten Sie, dass die Persona des Korrekturbesitzers die Berechtigungen „read_all“ und „write_all“ der Persona des Schwachstellenanalysten nicht enthält. Die granularen Rollen „read_all“ und „write_all“ sind erforderlich, damit Benutzer und Gruppen alle Datensätze für angreifbare Elemente und Korrekturaufgaben lesen und bearbeiten können. Um diese Rollen anzupassen, fügen Sie einfach granulare Rollen hinzu, oder entfernen Sie sie, um den Zugriff zu erweitern oder einzuschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Granulare Rollen und Personas für Korrekturverantwortlichen und Schwachstellenanalysten





Wenn Sie möchten, dass Ihre Benutzer und Gruppen mehr Zugriff haben, als die Persona-Rollen zulassen, können Sie den Benutzern und Gruppen granulare Rollen hinzufügen. Umgekehrt können Sie granulare Rollen entfernen, wenn Sie den Zugriff für bestimmte Benutzer und Gruppen auf Aufgabenebene einschränken möchten.

Hinweis:
Zum Zuweisen und Bearbeiten granularer Rollen im Benutzeradministrationsmodul ist die Systemadministratorrolle erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Granulare Rollen im Benutzeradministrationsmodul

Ein Beispiel für die Verwaltung granularer Rollen für einen Benutzer oder eine Gruppe finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Informationen zum Zuweisen von Persona-Rollen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Vulnerability Response Übersicht über Zuweisungsregeln

Definieren Sie die Kriterien, nach denen angreifbare Elemente (VITs) automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

Die Standardzuweisungsregel **An CI-Supportgruppe zuweisen**ist im Basissystem enthalten, die der **CI-Supportgruppe**angreifbare Elemente zuweist. Die Regel „An CI zuweisen-Supportgruppe“ weist eine VIT der Supportgruppe zu, die für das Configuration Item (CI) festgelegt ist, das der VIT zugeordnet ist.

Hinweis:
Manuell erstellte Zuweisungen werden durch die Zuweisungsregeln nicht neu bewertet.

Zuweisungstyp (**Manuell** oder **Regel)** ist im VIT-Formular und in der Listenansicht verfügbar. Jede VIT, die ursprünglich durch eine Regel zugewiesen wurde, anschließend manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel.

Verwenden Sie Zuweisungsregel- und Zuweisungstypinformationen, um Fälle zu identifizieren, in denen die Zuweisungsregeln keine richtige Übereinstimmung für den beabsichtigten Empfänger gefunden haben. Sie können die Informationen auch verwenden, um zu ermitteln, welche Regeln die meisten Neuzuweisungen hatten.

Die von Zuweisungsregeln festgelegten Zuweisungsgruppen werden von **Korrekturaufgabenregeln** verwendet, um Besitzer zu Korrekturaufgaben (VULs) zuzuweisen.

Hinweis:
Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Zuweisungsregeln verfügbar zu machen, müssen Sie die Rapid7 InsightVM Asset List-Integration vor den anderen Rapid7 InsightVM Integrationen ausführen.

Die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.

Angreifbare Elemente werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, angreifbare Elemente mit Zuweisen **mit zuzuweisen**:

- Anwendergruppe : Mit dieser Option können Sie eine der vorhandenen Anwendergruppen Now Platform® auswählen.
- Anwendergruppenfeld : Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle cmdb_ci verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder angezeigt:
  - Keine: Gibt an, dass für dieses Pflichtfeld kein Standardwert vorhanden ist
  - Konfigurationselement: Genehmigungsgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurationselement: Zuweisungsgruppe
- Konfigurationselement: Supportgruppe

- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Kenntnisse in der Codierung oder fortgeschrittenen ServiceNow. Weitere Informationen zur Verwendung des Skript-Editors zum Definieren komplexer Bedingungen finden Sie im KB-Artikel KB0965240 .

Führen Sie zuerst Regeln mit hoher Priorität aus (Elemente, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist oder bei denen ein VIT von der Compliance-Abteilung behandelt werden sollte). Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist und Sie wissen, wer dafür verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel zum Zuweisen von VITs an die Gruppe, die festlegt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt.

Bewertungsprozess für Zuweisungsregeln

Zuweisungsregeln werden verwendet, um eine VIT zu bewerten und zuzuweisen, wenn eine neue VIT geöffnet, also importiert, manuell erstellt oder erneut geöffnet wird. Sofern Sie Zuweisungsregeln nicht manuell erneut anwenden, nachdem sich der VIT oder sein Status geändert hat, wird ein VI einmal ausgewertet.

Der folgende Prozess wird für jede neue, aktualisierte oder erneut geöffnete VIT verwendet:

- Für jede Zuweisungsregel für Schwachstellen wird die VIT mit dem Zuweisungsfilter verglichen, wobei die Regel niedrigster Ordnung zuerst ist.
- Wenn die Bedingung erfüllt ist, wird die VIT einer Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung mit allen anderen Regeln finden, wird die VIT der Standardzuweisungsgruppe zugewiesen, sofern eine Standardregel vorhanden ist.

  Sobald das angreifbare Element zugewiesen wurde, verwendet die entsprechende Regel für Korrekturaufgaben die Zuweisung als eines ihrer Kriterien, um die angreifbaren Elemente in eine Korrekturaufgabe zu platzieren. Siehe Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

Hinweis:
Die Standardregel ist die Regel mit dem höchsten Wert für die Ausführungsreihenfolge. Eine abschließende Regel, die ein gutes Ausweichkontakt-Element darstellt, ist active=true. Wenn keine Standardregel vorhanden ist, bleibt die VIT nicht zugewiesen, wenn die Regel für Korrekturaufgaben die Zuweisung vornimmt.

Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie die Schaltfläche **Changes übernehmen** auf der Listenseite für Zuweisungsregeln, um alle geänderten Regeln für alle aktiven offenen VIs mit Ausnahme der manuell zugewiesenen Regeln erneut auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn die geplante Aufgabe *Reapply all vulnerability assignment rules* vor der ersten Verwendung **von Änderungen anwenden**nicht ausgeführt wurde, werden alle Zuweisungsregeln für alle offenen VITs mit Ausnahme der manuell zugewiesenen VIs ausgeführt. Danach werden bei allen nachfolgenden Verwendungen von **Changes übernehmen** nur die geänderten Regeln und alle abhängigen Regeln erneut ausgeführt. Änderungen an einer Regel können dazu führen, dass eine VIT einer anderen unveränderten Regel entspricht. Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

Die geplante Aufgabe [*Reapply all vulnerability assignment rules*] ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle Regeln auf alle offenen VITs mit Ausnahme der manuell zugewiesenen angewendet. Sie kann **Täglich**, **Wöchentlich**, **Monatlich**, **Regelmäßig**, **Einmal**oder **Bei Bedarf**ausgeführt werden. Je nachdem, wie viele aktive VIs Sie in Ihrer Umgebung haben, denken Sie daran, das Feld **Ausführen** nach der ersten Ausführung entsprechend zu setzen, um Auswirkungen auf die Leistung zu vermeiden.

Upgrade-Kunden sollten in den Versionshinweisen Vulnerability Response Informationen zu den Auswirkungen dieser Funktion auf vorhandene VITs lesen.

Wichtig:
Als Schwachstellenadministrator und -analyst können Sie die aktuellen Zuweisungen für ausgewählte angreifbare Elemente unter Vulnerability Manager Workspaceabrufen. Diese Methode ist effizienter als das Ausführen der Zuweisungsregeln für alle angreifbaren Elemente in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Wenn sich die Zuweisungsgruppe in einer Zuweisungsregel ändert, können die angreifbaren Elemente automatisch neu bewertet und neu gruppiert werden, indem die Systemeigenschaft sn_vul.rerun_task_rules und die Business-Regel Mit Korrekturaufgaben verknüpfen aktiviert werden.

So aktivieren Sie die Systemeigenschaft:

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Öffnen Sie die Systemeigenschaft sn_vul.rerun_task_rules.
3. Setzen Sie den **Wert** im Feld Wert auf true.

Wenn die Systemeigenschaft auf „true“ festgelegt ist und die Zuweisungsregeln erneut angewendet werden, wird die Verknüpfung der angreifbaren Elemente mit den Korrekturaufgaben aufgehoben, bei denen die Bedingung nicht mehr übereinstimmt.

Hinweis:
Standardmäßig ist die Systemeigenschaft sn_vul.rerun_task_rules auf „false“ festgelegt.

Um die Neugruppierung angreifbarer Elemente zu automatisieren, müssen Sie die Geschäftsregel „Korrekturaufgaben verknüpfen“ aktivieren.

So aktivieren Sie die Geschäftsregel:

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
2. Geschäftsregel Link zu Korrekturaufgaben öffnen.
3. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Geschäftsregel zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beim Aktivieren gruppiert die Business Rule die angreifbaren Elemente neu, indem sie in die entsprechende Gruppe verschoben oder eine Gruppe erstellt wird, wenn sie nicht unter einer vorhandenen Gruppe gruppiert werden können.

Hinweis:

- Die angreifbaren Elemente werden aus den Gruppen entfernt, ohne die Gruppen zu löschen.
- Es werden nur die Elemente entfernt, die mithilfe von Regeln für Korrekturaufgaben oder Korrekturmaßnahmen erstellt wurden.
- Die Neugruppierung erfolgt nur dann automatisch, wenn sich die Zuweisungsgruppe im Rahmen einer Zuweisungsregel ändert, und nicht, wenn sie manuell geändert wird.

Die Umgruppierung in Arbeitsbereichen wird für Korrekturaufgaben durchgeführt, die aus einer Korrekturmaßnahme erstellt werden.

Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben

Konfigurieren Sie Korrekturaufgaben (VULs), damit Analysten und Korrekturspezialisten angreifbare Elemente (VI) organisieren und massenweise analysieren können. Die Kriterien, nach denen Korrekturaufgaben erstellt werden, sind so konfiguriert, dass Sie angreifbare Elemente nicht manuell Korrekturaufgaben zuweisen müssen. Mit Korrekturaufgaben können Sie den Fortschritt überwachen und den Nachbesserungsprozess effizienter gestalten.

Nachverfolgung der Anzahl der Zurückstellungen für angreifbare Elemente und Korrekturaufgaben

Verfolgen Sie, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Eine regelmäßige Aufgabe, **Anzahl der Zurückstellungen festlegen**, wird täglich ausgeführt, um die Anzahl der Datensätze zu erfassen, die mehr als einmal in der Spalte Anzahl der Zurückstellungen zurückgestellt wurden. Datensätze werden in den Modulen „Mehrere Zurückstellungen“ für VR, AVR und CVR angezeigt.

Angreifbare Elemente werden automatisch aktualisiert

Hinweis:

Die Automatisierung der Aktualisierung von angreifbaren Elementen gilt nur für Korrekturaufgaben, die mit dem Bedingungsfilter oder der Filtergruppe erstellt wurden. Die Automatisierung gilt nicht für VIs, die manuell hinzugefügt oder mithilfe von Regeln für Korrekturaufgaben gruppiert wurden.

Wenn das Kontrollkästchen **Zugehörige angreifbare Elemente automatisch aktualisieren** aktiviert ist, werden der Aufgabe automatisch neue VIs hinzugefügt, die den Filterkriterien für Korrekturaufgaben entsprechen. Angreifbare Elemente in der Korrekturaufgabe, die nicht mehr den Filterkriterien entsprechen, werden automatisch aus der Aufgabe entfernt.

Wenn die Korrekturaufgabe den Status **Offen** verlässt, wird das Kontrollkästchen standardmäßig deaktiviert. Wenn angreifbare Elemente unabhängig vom Status weiterhin der Korrekturaufgabe hinzugefügt werden sollen, deaktivieren Sie die Geschäftsregel *`Set auto refresh vulnerable items`*.

Sie können das Kontrollkästchen manuell im Status „Wird untersucht“ erneut aktivieren. **Zugehörige angreifbare Elemente automatisch aktualisieren** ist nicht deaktiviert, wenn die Korrekturaufgabe in den Status **„Warten auf Implementierung“** wechselt. Sobald sich der Status „Warten auf Implementierung“ befindet, können der vorhandenen Aufgabe keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

neuen angreifbaren Elemente hinzugefügt oder vorhandene angreifbare Elemente entfernt werden.

Hinweis:
Wenn eine Korrekturaufgabe manuell erstellt wird und VIs mit dem **Bedingungsfilter** oder **der Filtergruppe**hinzugefügt werden, ist das Kontrollkästchen deaktiviert. Sie können das Kontrollkästchen aktivieren oder nicht.

Angreifbare Elemente werden manuell aktualisiert

Wenn Sie bei manuell erstellten Korrekturaufgaben mit einem Filter **für Filtergruppen** oder **Bedingungen** auf der Seite **„Korrekturaufgabe“** auf den zugehörigen Link Zugehörige angreifbare Elemente **aktualisieren** klicken, werden alle angreifbaren Elemente hinzugefügt, die den Filterkriterien entsprechen. Elemente, die den Kriterien nicht mehr entsprechen, werden entfernt. Diese Aktion ermöglicht eine sofortige Aktualisierung der Liste der angreifbaren Elemente und wird verwendet, unabhängig davon, ob das Kontrollkästchen **Zugehörige angreifbare Elemente automatisch aktualisieren** aktiviert ist oder nicht.

Manuell erstellte Korrekturaufgaben mit den Filtertypen **Bedingung** oder **Filtergruppe** werden einmal pro Stunde aktualisiert.

Die Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Elemente automatisch gruppiert und zugewiesen werden. Die Standardregel **Vulnerability**ist im Basissystem enthalten und sammelt angreifbare Elemente auf Grundlage ihrer Schwachstellen. Sie können jedoch nach jedem anderen Wertesatz in Spalten gruppieren, auf die über das VI zugegriffen werden kann. Diese Werte können die Supportgruppe für Konfigurationselemente (CI), den Schwachstellenschweregrad usw. umfassen.

Sie können eine beliebige Anzahl von Bedingungen erstellen. Sobald Sie eine Gruppe nach Auswahl festgelegt haben, wird eine weitere Zeile angezeigt. Sie können bis zu sechs **„Gruppieren nach** “-Auswahlen auswählen. Sie können auch die Gruppenzuweisung automatisieren. Siehe Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

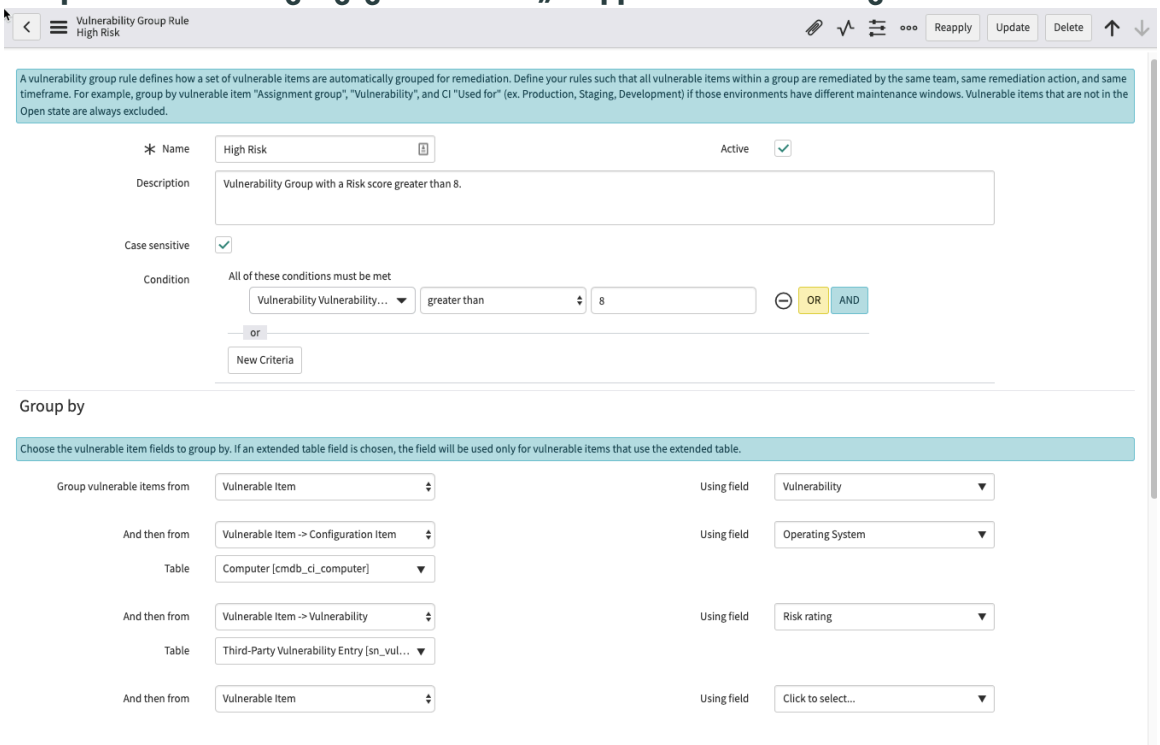
Hinweis:
Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Regeln für Korrekturaufgaben verfügbar zu machen, müssen Sie die Rapid7 InsightVM Asset-Listenintegration vor den anderen Rapid7 InsightVM -Integrationen ausführen.

Sie können Ihre angreifbaren Elemente beispielsweise nach der Kostenstelle des angreifbaren CI oder nach dem Angriffsvektor der Schwachstelle gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit niedrigem Schweregrad oder für CIs mit geringem Risiko festlegen. Sie können eine andere Aufgabenregel für kritische Server und Schwachstellen mit Exploits festlegen – angreifbare Elemente, die das Unternehmen einem höheren Risiko aussetzen.

Für angreifbare Elemente, die das Unternehmen einem höheren Risiko aussetzen, können andere Regeln verwendet werden. Der Name der Korrekturaufgabe wird an die Korrekturaufgabenregel „ **Gruppieren nach** “-Werte angehängt, um die Kurzbeschreibung des neuen Datensatzes zu erstellen. Weitere Informationen zu verfügbaren Feldern finden Sie unter Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für den Bedingungsgenerator für „Gruppieren nach“-Einträge



Wenn ein neues angreifbares Element erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Schwachstellenregeln anhand dieser Kriterien ausgewertet. Ein VI wird nur einmal automatisch ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete AE verwendet:

- Für jede Regel für Korrekturaufgaben wird der VI mit dem Regelfilter für Korrekturaufgaben verglichen.

- Für jede Regel, bei der die Bedingung der Regel für Korrekturaufgaben erfüllt ist, ruft die Regel die Daten aus der **Auswahlgruppe nach** Auswahl im AE ab. Es erstellt einen Gruppennamen und ein Feld. In diesem Fall, **Hohes Risiko: QID-32342:***Zusammenfassung von `QID-3242`* (Name: Schwachstellen-ID:Schwachstellenzusammenfassung).

  Hinweis:
  Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

  Die Regel prüft, ob eine übereinstimmende Korrekturaufgabe vom Typ **„Offen** “ vorhanden ist, die der gleichen Zuweisungsgruppe wie das VI zugewiesen ist.

  - Wenn die Aufgabe gefunden wird, wird das VI zur vorhandenen Aufgabe im Status **Offen** hinzugefügt.
  - Wenn keine Aufgabe im Status „ **Offen“** gefunden wird, erstellt die Regel eine Aufgabe **mit hohem Risiko: QID-32342**, weist sie derselben Zuweisungsgruppe wie das AE zu und platziert das AE in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Bedingungen der Korrekturaufgabenregel verglichen wird, bevor sie in eine Korrekturaufgabe aufgenommen wird, können zu viele Regeln die Leistung beeinträchtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig verwenden die Regeln für Korrekturaufgaben beim Gruppieren der Elemente die von den **Zuweisungsregeln** für das angreifbare Element festgelegte Zuweisungsgruppe und weisen die Korrekturaufgabe entsprechend den angreifbaren Elementen zu.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln im Modul **„Zuweisungsregeln“** gesteuert. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn eine Aufgabenregel gelöscht wird, können Sie im Formular oder in der Listenansicht alle von dieser Regel erstellten **offenen** Aufgaben löschen. Aufgaben, die sich nicht im **Kontrollkästchen** befinden, werden ausgeschlossen.

Die Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Regel für Korrekturaufgaben ändern möchten, klicken Sie auf der Seite für die Regel für **Korrekturaufgaben** auf die Schaltfläche Erneut anwenden, um die geänderte Regel für alle aktiven **offenen** Korrekturaufgaben erneut auszuführen, die von dieser Regel erstellt wurden. Es löscht Korrekturaufgaben basierend auf der geänderten Regel automatisch und erstellt sie neu.

Wichtig:
Als Schwachstellenadministrator und -analyst können Sie die Regeln für Korrekturaufgaben für ausgewählte angreifbare Elemente im Vulnerability Manager Workspacebewerten. Diese Methode ist effizienter als die erneute Anwendung der Regeln für Korrekturaufgaben in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Vulnerability Response Korrekturzielregeln

Korrekturzielregeln definieren den erwarteten Zeitrahmen für die Korrektur von angreifbaren Elementen (VI, Vulnerable Items), ähnlich wie SLAs einen Zeitrahmen für die Korrektur der Schwachstelle selbst bieten. Wenn ein Asset beispielsweise PCI-Daten (Kreditkartendaten) enthält, muss die Schwachstelle für dieses Element gemäß PCI DSS innerhalb von 30 Tagen behoben werden.

Schwachstellenmanager können Korrekturzielregeln erstellen, indem sie Folgendes definieren:

- Das Nachbesserungsziel
- Das Erinnerungsziel
- Die Empfänger der Erinnerung und der Benachrichtigung – Wer benachrichtigt werden soll, wenn die angreifbaren Elemente (VIs) das Erinnerungs- oder Korrekturzieldatum überschritten haben und nicht korrigiert wurden.

Schwachstellenanalysten und -manager können das Zieldatum für die Nachbesserung im Formular für angreifbare Elemente und in den Listenansichten anzeigen, sofern sich die angreifbaren Elemente nicht im Status **„Zurückgestellt“**, **„Gelöst“**oder **„Geschlossen“** befinden. Korrekturzielregeln werden beim Import ausgeführt und erneut ausgeführt, wenn ein VI erneut geöffnet wird.

Das **Zieldatum der Korrektur** ist in der VI-Listenansicht als Punkte wie folgt farbcodiert:

- Angreifbare Elemente, deren Benachrichtigungsdatum noch nicht erreicht wurde, werden grün angezeigt.
- Angreifbare Elemente, deren Korrekturzieldatum näher rückt, werden orange angezeigt.
- Angreifbare Elemente, deren Nachbesserungszieldatum verstrichen ist, werden rot angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pro Korrekturzielregel wird eine Zusammenfassungs-E-Mail gesendet, wenn mindestens ein AEs sich dem Korrekturzieldatum nähert oder das Korrekturzieldatum verstrichen ist.

Korrekturzielregeln können deaktiviert oder gelöscht werden

Wenn eine Regel deaktiviert wird, werden die aktuellen Korrekturzieldaten für die VIs gelöscht, auf die sie angewendet wurde. Wenn ein AE eine aktive Regel erfüllt, wird diese Regel angewendet. Andernfalls hat das AE keine Regel oder kein Zieldatum, und sein Status ist **Kein Ziel**.

Wenn Regeln gelöscht werden, werden das **Zieldatum der Korrektur** und zugehörige Felder für geschlossene, zurückgestellte oder gelöste VIs beibehalten. Das **Zieldatum der Korrektur** und zugehörige Felder für nicht geschlossene VIs werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

Szenario für Korrekturzielregel

Wenn mehrere Korrekturzielregeln auf dasselbe angreifbare Element angewendet werden, wird die restriktivste Regel angewendet.

Hinweis:
Korrekturziele werden aus dem Datum **von „Zuletzt geöffnet“** plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.

Ab V17.1 werden Korrekturziele anhand des **Ziels ab (Datum)**berechnet. Der Standardwert bleibt **Datum der letzten Öffnung**.

Beispiel: Wenn ein angreifbares Element die Bedingung für zwei Korrekturzielregeln erfüllt:

Szenario: Angreifbares Element wurde zuletzt am 01.03.2018 um 10:00:00 geöffnet.

- Korrekturzielregel 1: Zuletzt geöffnet am 03.07.2018; Korrekturziel ist 15 Tage seit dem letzten Öffnen; Das berechnete Zieldatum der Korrektur ist der 16.03.2018 10:00:00.
- Korrekturzielregel 2: Zuletzt geöffnet am 10.03.2018; Korrekturziel ist 10 Tage seit dem letzten Öffnen; Das berechnete Zieldatum der Korrektur ist der 11.03.2018 10:00:00.

In diesem Szenario gilt die Korrekturzielregel 2 für das angreifbare Element, da sie über das restriktivere Datum verfügt. 10 Tage seit der ersten Identifizierung des angreifbaren Elements im Vergleich zu 15 Tagen.

Hinweis:
Sobald die Korrekturzielregel definiert ist, werden Korrekturzieldaten von der geplanten Aufgabe *`Evaluate remediation targets`* berechnet.

Über die geplante Aufgabe „Korrekturziele auswerten“

`Evaluate remediation targets` wird einmal täglich um 4:00:00 ausgeführt.

Es durchläuft alle aktiven Schwachstellenregeln, beginnend mit den Regeln mit dem frühesten Korrekturzieldatum. Es untersucht alle angreifbaren Elemente, die:

- befinden sich nicht im Status **„Geschlossen“**, **„Zurückgestellt“**oder **„Gelöst“**.
- Hat kein Korrekturzieldatum.
- Ein Korrekturzieldatum aufweisen, das nach dem Datum in der Korrekturzielregel liegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Evaluate remediation targets fügt ein Korrekturzieldatum hinzu. Wenn keines vorhanden ist oder wenn eine Regel zu einem früheren Datum als dem im Datensatz angegebenen führt, wird das vorhandene Zieldatum aktualisiert. Abschließend werden die Felder **Korrekturziel** und **Korrekturstatus** im Formular für angreifbare Elemente aktualisiert.

Sobald *Evaluate remediation targets* ausgeführt wird, werden verfügbare Benachrichtigungen gesendet.

Evaluate remediation targets löscht die Korrekturfelder im AE und sendet keine Benachrichtigungen mehr.

Wenn die Eigenschaft *sn_sec_cmn.evaluate_targetmissed_records* aktiviert ist, wird verhindert, dass die geplante Aufgabe *Remediation Target Rules* verfehlte AEs bewertet. Diese Eigenschaft ist standardmäßig aktiviert.

Korrekturzielregeln werden erneut angewendet

Wenn Sie eine Korrekturzielregel ändern, klicken Sie auf die Schaltfläche **Changes übernehmen** auf der Listenseite für Korrekturzielregeln, um alle geänderten Regeln für alle aktiven offenen AEs mit Ausnahme der Status **Geschlossen**, **Zurückgestellt** oder **Gelöst erneut** auszuführen. Je nachdem, wie viele VIs Sie haben, kann dies einige Zeit dauern.

Hinweis:

Wenn die geplante Aufgabe *Evaluate remediation targets* ausgeführt wird, können Sie keinen Prozess zum erneuten Anwenden initiieren. Wenn jedoch bereits ein Prozess zum erneuten Anwenden ausgeführt wird und die regelmäßige Aufgabe, die durch ihn ausgelöst wurde, ausgeführt wird, werden sie parallel ausgeführt.

Die Prozesse zum erneuten Anwenden in Vulnerability Response und Application Vulnerability Response sind unabhängig und können parallel ausgeführt werden.

Wichtig:
Als Schwachstellenadministrator und -analyst können Sie das neueste Nachbesserungszieldatum für ausgewählte angreifbare Elemente unter Vulnerability Manager Workspaceabrufen. Diese Methode ist effizienter als die Ausführung der Korrekturzielregeln für alle angreifbaren Elemente in der UI klassisch, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Zugehörige Informationen

Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln

Zeigen Sie den Nachbesserungszielstatus eines angreifbaren Elements Vulnerability Response an

Erstellen oder bearbeiten Sie Benachrichtigungen für Korrekturziele

Gruppen und Regeln für die Schwachstellenklassifizierung

Klassifizierungsgruppen automatisieren die Klassifizierung von Werten einer Tabelle basierend auf den in der Gruppe definierten Klassifizierungsregeln. Die Bedingung für jede Regel wird der Reihe nach ausgewertet, und die erste Übereinstimmungsregel wird verwendet.

Das Vulnerability Response-Basissystem enthält die folgenden beiden Klassifizierungsgruppen, die erkannte Elemente bzw. Schwachstellen klassifizieren:

- Klassifizierung erkannter Elemente
- Klassifizierung von Schwachstelleneinträgen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Schwachstellen und erkannte Elemente importiert werden, werden die Klassifizierungsregeln für Schwachstellen in den jeweiligen Gruppen ausgeführt. Basierend auf den in der Regel festgelegten Bedingungen werden die Datensätze in der entsprechenden Klassifizierungsgruppe klassifiziert. Sie können diese Regeln erstellen, bearbeiten, löschen oder erneut auf eine vorhandene Schwachstelle anwenden.

Hinweis:

- Für eine ausgewählte Tabelle kann nur eine aktive Klassifizierungsgruppe vorhanden sein.
- Sobald Sie eine Gruppe erstellt haben, können Sie sie nicht löschen.

Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie eine Klassifizierungsregel, Wenden Sie eine Regel auf eine vorhandene Schwachstelle an und Deaktivieren oder löschen Sie eine Klassifizierungsregel.

ML-Lösungen (maschinelles Lernen) für Vulnerability Response

Empfehlungen für die Zuweisung von Schwachstellen nutzt ServiceNow® Predictive Intelligence und maschinelles Lernen, um Zuweisungsgruppen für angreifbare Elemente (VIs) und Korrekturaufgaben (VULs oder RTs) zu empfehlen. Sie können die Zeit reduzieren, die Sie für die Identifizierung der Verantwortlichen für nicht oder falsch zugewiesene Schwachstellenergebnisse verwenden. Außerdem können Sie eine vom System generierte Konfidenzpunktzahl anzeigen, die bewertet, ob die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist.

Die Fähigkeiten Predictive Intelligence werden in Vulnerability Response verwendet, um eine bessere Arbeits-Experience zu bieten, indem ein Lösungsdefinitionsmodell erstellt und trainiert wird, das die Zuweisungsgruppe basierend auf vorhandenen Daten vorhersagen kann.

Weitere Informationen hierzu finden Sie unter Predictive Intelligence .

Empfehlungen für die Zuweisung von Schwachstellen

Mit der Anwendung Empfehlungen für die Zuweisung von Schwachstellen (com.snc.vulnerability.recom) kann das System mithilfe von Vulnerability Response Empfehlungen in ServiceNow Predictive Intelligencezuweisen. Dieses Plugin erfordert:

- Vulnerability Response (com.snc.vulnerability)
- Predictive Intelligence (com.glide.platform_ml)

Weitere Informationen hierzu finden Sie unter Predictive Intelligence .

Vertrauensbewertungen

Verwenden Sie die Anwendung Empfehlungen für die Zuweisung von Schwachstellen, um die Konfidenzpunktzahl zu generieren, die das Konfidenzniveau der empfohlenen Zuweisungsgruppen für die ausgewählten RTs oder VIs angibt. Die Vertrauensbewertung bewertet, ob das System davon ausgeht, dass die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist. Es werden bis zu 10 Empfehlungen angezeigt. Diese Empfehlungen basieren auf der höchsten Wahrscheinlichkeit für erfolgreiche Zuweisungen. Die erste Empfehlung in der Liste bedeutet, dass das System die richtige Zuweisungsgruppe hat.

Auf einer Skala von 0 bis 100 gibt die Konfidenzpunktzahl für jede Zuweisungsgruppe die Wahrscheinlichkeit an, dass ein VI oder RT zu dieser bestimmten Gruppe gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Predictive Intelligence

Klassifizierungslösung erstellen und trainieren

Eine Ähnlichkeitslösung erstellen und trainieren

Clustering-Lösung erstellen und trainieren

Erweiterte Einstellungen für ML-Lösungen konfigurieren

CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Vulnerability Response automatisch Hostdaten, um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. Dies geschieht mithilfe von **CI-Suchregeln**. Diese Regeln werden verwendet, um Configuration Items (CIs) zu identifizieren und dem Datensatz des angreifbaren Elements hinzuzufügen, um die Korrektur zu unterstützen.

Navigieren Sie ab Version 19.0 zu **Security Operations** > **CMDB** > **Suchregeln** um die Liste in Ihrer Instanz zu finden.

Beim Importieren von Assets wird zuerst eine Suche in der Liste **„Erkannte Elemente“** anhand von Drittpartei-IDs durchgeführt, um Übereinstimmungen mit Configuration Items (CIs) aus vorherigen Importen zu finden. Wenn eine Übereinstimmung mit der Host-ID gefunden wird, wird diese als Feld **Configuration item (Konfigurationselement)** im Datensatz des angreifbaren Elements verwendet.

Sie können sehen, wie importierte Assets mithilfe der Liste **Erkannte Elemente** CIs zugeordnet werden. Wenn keine Übereinstimmung gefunden wird oder das Feld „Host-ID“ leer ist, verwenden die Regeln die Informationen des anderen Hosts, um zu versuchen, das CI korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein Platzhalter-CI erstellt und als **nicht abgeglichenes CI**gekennzeichnet. Weitere Informationen zum Umgang mit diesen CIs finden Sie unter Nicht abgeglichene CIs.

CI-Suchregeln können domänengetrennt sein und sind quellenspezifisch. Jede Quelle kann mehrere Bereitstellungen haben.

Hinweis:
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellenquellenintegration gemeinsam genutzt. Wenn eine Regel gelöscht oder geändert wird, wirken sich die Löschung oder Änderungen auf alle Bereitstellungen der Schwachstellenintegration aus.

Wenn versucht wird, eine Übereinstimmung zu finden, besteht der erste Schritt in der Lieferanten-ID-Suche nach einer genauen Übereinstimmung zwischen Quelle, Quellinstanz und Lieferanten-ID. Dann werden Suchregeln der Reihe nach von der niedrigsten zur höchsten ausgeführt und angehalten, wenn eine Regel nur ein einziges CI als Übereinstimmung zurückgibt. Wenn eine Regel so erstellt wird, dass mehr als ein CI zurückgegeben wird, wird nur die erste Übereinstimmung verwendet.

Hinweis:
Um einen Abgleich mit Netzwerkelementen auf niedriger Ebene zu vermeiden, wenn es sich bei einem übereinstimmenden CI um eines der folgenden Elemente handelt: `dscy_Switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic`oder `cmdb_ci_ip_address`, wird das übergeordnete CI zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Systemeigenschaft zum Ausschließen von CI-Klassen ist verfügbar. Diese Eigenschaft ist mit einem Upgrade nicht verfügbar. Upgrade-Informationen und Anweisungen zum Festlegen der Eigenschaft finden Sie unter CI-Klassen ignorieren.

Um das Auffinden von Übereinstimmungsproblemen zu erleichtern, wird bei einer Übereinstimmung die CI-Suchregel, mit der sie gefunden wird, dem Datensatz „Erkanntes Element“ im Feld **„CI-Übereinstimmungsregel“** hinzugefügt. Suchregeln werden zuerst anhand des niedrigsten **Reihenfolgewerts** ausgewertet.

Die CI-Suchregeln werden mit den entsprechenden Integrations-Plugins geliefert.

Einige der Qualys CI-Suchregeln sind:

- QUALYS-HOST-ID
- FQDN
- NetBIOS
- DNS
- IP

Einige der Rapid7 CI-Suchregeln sind:

- MAC-Adresse
- FQDN
- HostName
- IP

Einige der Tenable.io-CI-Suchregeln sind:

- FQDN
- NETBIOS
- HOSTNAME
- MAC-Adresse
- DNS

Hinweis:
Die Tenable.io-CI-Suchregeln priorisieren und füllen die nicht leeren Netzwerkschnittstellenwerte (FDQN, IPV4 und MacAddress) gegenüber den regulären FDQN-, IPV4- und MacAddress-Werten für ein erkanntes Element aus. Wenn diese Werte für die Netzwerkschnittstelle leer sind, werden die regulären Werte für FDQN, IPV4 und MacAddress für ein erkanntes Element ausgefüllt.

Einige der Tenable.sc-CI-Suchregeln sind:

- MAC-Adresse
- FQDN
- NETBIOS

Hinweis:
Einmal entfernte Regeln können nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden. Die Logik, die zum Iterieren und Abgleichen von CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie alle anwenderdefinierten CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln**. Unter Schritte zum Verhindern von doppelten oder verwaisten Datensätzen nach dem Ausführen von Vulnerability Response CI-Suchregeln finden Sie weitere Informationen zum Verhindern des Duplikats von verwaisten Elementen, zum Löschen von Daten und zum Bereinigen von Daten.

Hinweis:
Informationen zum CI-Abgleich finden Sie unter KB0998706 .

Aktualisierte CI-Suchregeln werden erneut angewendet

Wenn Sie eine CI-Suchregel ändern, klicken Sie auf der Listenseite „CI-Suchregeln“ **auf Änderungen anwenden,** um alle Regeln für die erkannten Elemente erneut auszuführen, die:

- Wurden mit den aktualisierten Regeln abgeglichen
- Werden von keiner Regel abgeglichen

Wenn sich das Configuration Item (CI) nach dem erneuten Anwenden der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Die betroffenen Erkennungen und angreifbaren Elemente werden ebenfalls aktualisiert. Weitere Informationen finden Sie unter CI-Suchregeln erneut auf ausgewählte erkannte Elemente anwenden.

Nicht klassifizierte Hardware

Wenn ein Asset in den Configuration Management Database (CMDB) nach CI-Suchregeln keine Übereinstimmung findet, wird das Asset als nicht klassifizierte Hardware bezeichnet.

Wenn Daten aus ServiceNow -Integrationen importiert werden, verwendet Vulnerability Response automatisch Hostdaten, um nach Übereinstimmungen in CMDBzu suchen. Die CI-Suchregeln werden verwendet, um Configuration Items (CIs) zu identifizieren und dem Datensatz des angreifbaren Elements hinzuzufügen, um die Nachbesserung zu unterstützen. Wenn die Assets nicht in CMDBzu finden sind, führt die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) ihre eigenen Identifizierungsregeln aus, die für die Hardwareklasse und alle untergeordneten Elemente definiert sind, und erstellt ein CI unter einer nicht klassifizierten Hardwareklasse. Wenn Discovery dieses Asset findet, wird die vorhandene nicht klassifizierte Hardware nicht neu klassifiziert, sondern es wird ein CI erstellt. Dies liegt daran, dass die Identifizierungsregel auf dem Namen des Hardware-CI basiert.

Wenn die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

Die folgenden Auszüge zeigen die IRE-Nutzlast zum Erstellen von CIs in nicht klassifizierter Hardware über Vulnerability Response bzw. Discovery.

```
"className": "cmdb_ci_unclassed_hardware",

"values": {
      "name": "asset01.company.com",//from NetBios,
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123"
   }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"settings": {
      "updateWithoutSwitch": true
   }
```

```
"className": "cmdb_ci_cmdb_ci_win_server"

"values": {
      "name": "asset01",
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123",
      "os_domain": "company"
   }

"settings": {
      "updateWithoutSwitch": false
   }
```

In diesem Fall wird das vorhandene nicht klassifizierte Hardware-CI nicht in Windows-Server neu klassifiziert, sondern es wird ein neues CI unter Windows-Server erstellt. Der Grund dafür ist, dass die Identifizierungsregel auf dem Namen des Hardware-CI basiert. Wenn Sie die Nutzlasten beachten, ist der Name in der Nutzlast von Vulnerability Response mit FQDN/NETBIOS identisch, es ist jedoch nur der Hostname für die Nutzlast von Discovery.

Zugehörige Informationen

Klassifizieren Sie nicht klassifizierte Hardware neu

Nicht abgeglichene CIs

Configuration Items (CIs) werden beim Import automatisch mit CIs in Configuration Management Database (CMDB) abgeglichen. Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Das Modul listet die Configuration Items ohne Übereinstimmung auf.

Wenn Sie der Meinung sind, dass ein nicht abgeglichenes CI zu einer vorhandenen Klasse in der CMDB gehört, überprüfen Sie Ihre CI-Suchregeln. Andernfalls sollten Sie das Configuration Item erneut klassifizieren.

Hinweis:
Der Standardfilter für diese Liste ist auf **Nicht abgeglichen**festgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Wenn die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

Zugehörige Informationen

Nicht abgeglichene Konfigurationselemente anzeigen und neu klassifizieren

Nicht übereinstimmende erkannte Elemente abstimmen

Schritte zum Verhindern von doppelten oder verwaisten Datensätzen nach dem Ausführen von Vulnerability Response CI-Suchregeln

Vorhandene Konfigurationselemente werden dedupliziert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt

Sie können Configuration Items (CIs) in Configuration Management Database (CMDB) mithilfe der API Identification and Reconciliation Engine (IRE) erstellen. Durch die Verwendung der IRE-API zum Erstellen von CIs können Sie verhindern, dass doppelte CIs erstellt werden, und Sie können CI-Attribute abgleichen, indem Sie zulassen, dass nur autorisierende Datenquellen in CMDBschreiben.

Eine CI-Klasse (Tabelle) ist der ursprüngliche Tabellenname in der Instanzdatenbank. CMDB enthält Basissystemklassen, in denen Daten zu CIs gespeichert werden.

IRE für CI-Erstellung verwenden

Vor Vulnerability Response v12.2, wird, wenn kein übereinstimmendes CI gefunden wird, entweder in der Liste „Erkannte Elemente“ oder in CMDBein CI in der Klasse der nicht abgeglichenen CIs (sn_sec_cmn_unmatched_ci) erstellt. Weitere Informationen finden Sie unter Nicht abgeglichene CIs.

Wenn IRE ab v24.0.6 von Vulnerability Responseauf Ausnahmen stößt, die die Erstellung von CIs verhindern, werden die Einzelheiten dieser Ausnahmen im Feld „Zusätzliche Informationen“ aufgezeichnet. Durch Überprüfen der Details in diesem Feld können Sie die Ursache ermitteln und die erforderlichen Korrekturen implementieren, um sicherzustellen, dass das CI erfolgreich erstellt wird.

Ab Vulnerability Response v12.2 bis v18.0: Wenn bei Anwendung der CI-Suchregeln keine Übereinstimmung gefunden wird, werden die Asset-Informationen an IRE gesendet, und es wird ein CI in einer der Klassen *„Nicht klassifizierte Hardware“* und *„Unvollständige IP identifiziertes Gerät“* erstellt. Ab Vulnerability Response v18.0 ist die neue Klasse *Cloud-Ressource* ebenfalls enthalten. Weitere Informationen zum Konfigurieren der Kategorisierung von nicht abgeglichenen Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets aktualisieren.

CMDB CI-Klassen

Hinweis:
Um die neuen Klassen zu verwenden, aktivieren Sie das Plugin CMDB CI Class Models. Andernfalls werden CIs in der nicht abgeglichenen CI-Klasse erstellt.

Wenn der Host, den Sie von einem Drittanbieterscanner importiert haben, nicht in der Liste „Erkannte Elemente“ oder in CMDBgefunden werden kann, wird er vonin einer der folgenden neuen CMDB CI-Klassen erstellt.

CMDB CI-Klassen

CMDB CI-Klasse	Beschreibung
Unvollständige IP-Identifizierung des Geräts (*cmdb_ci_incomplete_ip*)	In dieser Tabelle wird ein CI erstellt, wenn nur die IP-Adresse in den vom Scanner empfangenen Hostinformationen verfügbar ist.
Nicht klassifizierte Hardware (*cmdb_ci_unclassed_hardware*)	Das CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen eine der folgenden Informationen verfügbar ist: • Hostname • IP-Adresse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CMDB CI-Klassen (Fortsetzung)

CMDB CI-Klasse	Beschreibung
	• DNS • NETBIOS • MAC-Adresse **Hinweis:** Wenn die MAC-Adresse verfügbar ist, wird der Netzwerkadaptereintrag erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft. Wenn sowohl die IP-Adresse als auch die MAC-Adresse verfügbar sind, wird auch das IP-Adressen-CI erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft.
Cloud-Ressource (*cmdb_ci_cmp_resource*)	CI wird in dieser Tabelle erstellt, wenn *Cloud Resource ID* in den vom Scanner empfangenen Hostinformationen verfügbar ist. **Hinweis:** Wenn der Asset-Typ einer Scannerintegration auf *Hybrid* und die Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* auf „false“ festgelegt ist, werden die CIs in der Klasse *„Nicht klassifizierte Hardware“* erstellt, nicht jedoch in der Klasse *„Cloud-Ressource“*.

Wenn die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

In folgenden Fällen verwendet das System automatisch eine nicht abgeglichene CI-Klasse:

- Das CMDB CI-Klassen-Plugin ist nicht aktiviert.
- IRE löst beim Erstellen eines CI eine Ausnahme aus.

Weitere Informationen finden Sie unter Nicht abgeglichene CIs.

Zugehörige Informationen

Store-App „CMDB CI Class Models“

Identification and Reconciliation Engine (IRE)

CI-Klasse für nicht abgeglichene Cloud-Assets aktualisieren

Ab Vulnerability Response v20.0 können Sie die nicht abgeglichenen Cloud-Assets aus den Scannern Qualys, Rapid7 und Tenable mithilfe der Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* als *nicht klassifizierte Hardware* kategorisieren.

Diese Systemeigenschaft mit dem Standardwert „false“ ist im Lieferumfang des Basissystems enthalten. Klassifiziert die nicht abgeglichenen Cloud-Assets in eine Klasse

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nicht klassifizierter Hardware (*cmdb_ci_unclassed_hardware*) oder *einer Cloud-Ressource* (*cmdb_ci_cmp_resource*) für die Integrationen, die sowohl Infrastruktur- als auch Cloud-Assets einbeziehen.

Ab Vulnerability Response v20.0 wird in der Tabelle „Drittpartei-Integrationen“ (sn_sec_int_integration) die Spalte „Asset-Typ“ hinzugefügt, um die Integrationen zu identifizieren, die sowohl Infrastruktur- als auch Cloud-Assets unterstützen. Die Spalte „Asset Type“ (Asset-Typ) enthält den Wert *Hybrid* für die Scanner, die sowohl Infrastruktur- als auch Cloud-Assets einbeziehen. Qualys, Rapid7- und Tenable-Integrationen haben beispielsweise den Wert *Hybrid* in der Spalte Asset Type (Asset-Typ).

- Bei der Neuinstallation von Vulnerability Response v20.0 und höher werden alle nicht abgeglichenen Cloud-Assets in folgende Kategorien eingeteilt:
  - Standardmäßig*nicht klassifizierte Hardwareklasse*.
  - *Cloud-Ressourcen* -Klasse, wenn Sie die Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* in trueändern.
- Für Upgrades auf Vulnerability Response v20.0:
  - Wenn in der Klasse *„Cloud-Ressource“* Assets vorhanden sind, wird die Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* auf „wahr“ festgelegt, damit die nicht abgeglichenen Cloud-Assets weiterhin der Klasse *„Cloud-Ressource“* (*cmdb_ci_cmp_resource*) hinzugefügt werden.
  - Andernfalls wird die Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* auf „false“ festgelegt, sodass die nicht abgeglichenen Cloud-Assets in der Klasse *„Nicht klassifizierte Hardware“* kategorisiert werden.

Hinweis:
Wenn Sie den Wert der Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* ändern, stellen Sie sicher, dass Sie nicht abgeglichene Configuration Items in der zuvor als Ziel festgelegten CI-Klasse löschen, und wenden Sie die Suchregeln erneut an. Weitere Informationen darüber, wie Sie die vorhandenen CIs löschen und CI-Suchregeln erneut anwenden, damit die neuen CIs in der richtigen Klasse erstellt werden, finden Sie unter KB1533376 .

Erkannte Elemente

Assets werden automatisch Configuration Items (CIs) in Configuration Management Database (CMDB) zugeordnet, wenn sie mithilfe von **CI-Suchregeln**importiert werden. Erkannte Elemente geben Ihnen Einblick in die Zuordnung der Asset-Identifizierung zu CIs in CMDB.

Erkannte Elemente werden **als abgeglichen**, **nicht abgeglichen**oder **neu klassifiziert**betrachtet. Identifizierte CIs befinden sich im Status **Abgeglichen**.

Um das Auffinden potenzieller Übereinstimmungsprobleme zu erleichtern, wird im Feld „CI-**Übereinstimmungsregel“ die CI-Suchregel angezeigt, die dem CI** entspricht.

Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Das Modul listet nicht abgeglichene Konfigurationselemente auf. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Eine Beschreibung der Felder in Erkannte Elemente finden Sie unter Formularfelder „Erkannte Elemente“.. Weitere Informationen zum Abgleich nicht übereinstimmender erkannter Elemente und zum erneuten Anwenden von CI-Suchregeln auf ausgewählte erkannte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elemente finden Sie unter Nicht übereinstimmende erkannte Elemente abstimmen bzw. Wenden Sie die CI-Suchregeln erneut auf ausgewählte erkannte Elemente an.

CI-Changes für erkannte Elemente

Wenn sich ein Configuration Item (CI) für ein erkanntes Element (DI) ändert, werden die betroffenen Erkennungen und angreifbaren Elemente (VIs) aktualisiert. Die Risikopunktzahl, Zuweisungsregeln, Gruppenregeln und die Korrekturzielregel werden neu ausgewertet.

Ab v24.0.6 von Vulnerability Responsekönnen Sie die Aktualisierungen für ein CI in der Tabelle „Erkanntes Element“ anzeigen. Informationen wie das vorherige CI, das aktualisierte CI und den Benutzer, der die Änderungen vorgenommen hat, sind in der zugehörigen Liste Audit-Verlauf dokumentiert.

Wenn ein VI mit derselben Schwachstelle und demselben CI vorhanden ist, werden die Erkennungen mit dem vorhandenen VI aktualisiert und das aktuelle VI wird mit dem Substatus `ungültiges` CIgeschlossen. Arbeitsnotizen werden aus folgenden Gründen hinzugefügt:

- Wenn Erkennungen von einem VI in ein anderes verschoben werden.
- Wenn ein doppeltes AEs geschlossen wird

Wenn Sie das CI für das vorhandene VI nicht aktualisieren möchten, legen Sie die Eigenschaft `sn_sec_cmn.update_on_ci_change` auf `false`fest. Wenn sich dann ein CI ändert, wird ein neues VI erstellt und das vorhandene als `ungültiges`CI geschlossen.

Der Standardwert der Eigenschaft `sn_sec_cmn.update_on_ci_change` ist `true`.

Erkannte Elemente werden erneut ausgewertet

Wenn neue Daten zu einem erkannten Element empfangen werden, wird das erkannte Element nicht sofort erneut ausgewertet. Beim Empfang neuer Daten wird die Option *`reevaluate_ci`* standardmäßig auf *`true`* festgelegt.

Die regelmäßige Aufgabe *`Re-apply CI Lookup Rules on the Changed Discovered items`* wertet alle erkannten Elemente aus, deren Quelldaten vom Scanner geändert werden. Er verarbeitet die erkannten Elemente erneut und aktualisiert die angreifbaren Elemente, die sich auf das erkannte Element beziehen, dessen Quelldaten sich geändert haben. Der Wert dieser regelmäßigen Aufgabe ist standardmäßig *`On Demand`*.

Hinweis:
Sie können diese geplante Aufgabe auch täglich ausführen.

Vulnerability Response Korrekturaufgabe und Status angreifbarer Elemente

Mit der Anwendung Vulnerability Response können Sie das Statusmodell verwenden, um den Status einer Korrekturaufgabe jederzeit anzuzeigen. Wenn Sie wissen, wie die einzelnen Status miteinander in Beziehung stehen und sich gegenseitig beeinflussen, können Sie bestimmen, wann und wie Sie Ihre angreifbaren Elemente (VIs) korrigieren sollten.

Status der Korrekturaufgaben

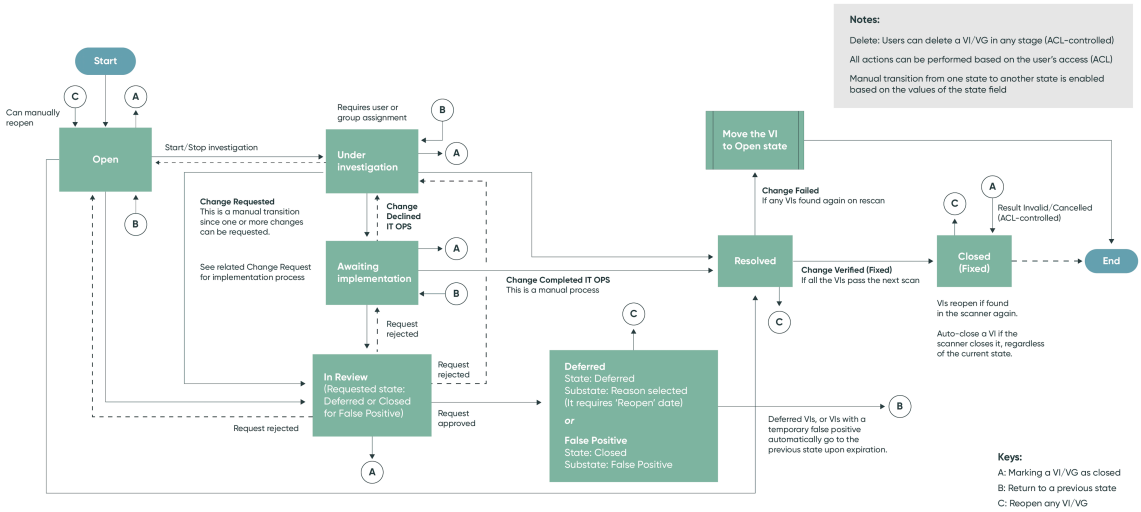
Komplexe Anwendungsfälle können manchmal dazu führen, dass ein angreifbares Element einen anderen Status aufweist als seine Korrekturaufgabe. Wenn Sie wissen, wie Status funktionieren, können Sie dieses Verhalten erklären und können bei der Erstellung von Korrekturaufgaben und beim Erstellen oder Bearbeiten von Regeln für Korrekturaufgaben helfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v23.0 von Vulnerability Responseist der Workflow **„Statusgenehmigung für angreifbares Element“** veraltet und wird durch den Flow „Statusgenehmigung für Schwachstellenelement“ im Flow Designer ersetzt.

Korrekturaufgaben haben viele mögliche Status, wie im folgenden Diagramm dargestellt.

Vulnerability Response-Status-Flow



Hinweis:
Jedes Aufgabenformular enthält die Schaltflächen **Verfolgen** und **Aktualisieren**, die bei ServiceNow -Aufgaben standardmäßig verwendet werden.

Weitere Informationen zu den Status von Korrekturaufgaben und den Aktionen, die Sie im jeweiligen Status ausführen können, finden Sie unter Vulnerability Response Status der Korrekturaufgaben.

Weitere Informationen zu Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente finden Sie unter Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente.

Weitere Informationen zu Korrekturaufgaben und VI-Status finden Sie unter Korrekturaufgaben und Status angreifbarer Elemente.

Weitere Informationen zum Status von Korrekturaufgaben für AEs in mehreren Gruppen finden Sie unter Status der Korrekturaufgabe für angreifbare Elemente (VIs) in mehreren Gruppen.

Berechnung und Anzeige des Alters von angreifbaren Elementen

Das Alter der angreifbaren Elemente wird in der Anwendung Vulnerability Response mit weiteren Details angezeigt.

Das Alter der angreifbaren Elemente (VI) wird im Format „Tage/Stunden/Minuten“ in der Spalte „Alter“ in der Listenansicht der angreifbaren Elemente und in den Feldern „Alter“ und „Alter geschlossen“ in den VI-Datensätzen (VIT) angezeigt. Das Alter wird in höherwertigen Ziffern angezeigt und kann Ihnen dabei helfen, die folgenden Aktivitäten genauer durchzuführen:

- Konfigurieren Sie Regeln im Modul „Regeln für automatische Löschung“, um bestimmte VI-Datensätze nach Tagen/Stunden/Minuten gezielt anzusprechen und zu löschen. Das Entfernen von Datensätzen mit höherer Genauigkeit kann Ihre Leistung verbessern, insbesondere wenn Sie eine große Anzahl von VI-Datensätzen in Ihrer Instanz haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie in Performance Analytics Berichte mit spezifischeren Details für die Anwendung Vulnerability Response an.
- Erstellen Sie Filter, die nur die gewünschten AEs identifizieren.
- Listenansichten kürzen, um nur die gewünschten VIs anzuzeigen.
- Einfacheres Dot-Walking.

Eine geplante Aufgabe hat das Alter berechnet und alle aktiven AEs aktualisiert. In Instanzen mit einer großen Anzahl von VI-Datensätzen kann dieser Prozess langsam sein und die Leistung beeinträchtigen. AE-Alter wird bei Bedarf effizienter berechnet und mit signifikanteren Ziffern in einer erweiterten Altersspalte angezeigt. Die erweiterte Spalte „Alter“ wird automatisch hinzugefügt, wenn Sie die Anwendung Vulnerability Response installieren oder aktualisieren.

Hinweis:
Wenn Sie ein Upgrade durchführen und das AE-Alter nicht in der Listenansicht der angreifbaren Elemente und in den Feldern „Alter“ und „Alter geschlossen“ für aktive AE-Datensätze (VIT) im Format „Tage/Stunden/Minuten“ (9 Tage, 18 Stunden, 29 Minuten) angezeigt wird , ist die Altersspalte in Ihrer Instanz nicht aktuell. Weitere Informationen zur Behebung dieses Problems nach einem Upgrade finden Sie unter KB0749231 .

Die Altersspalte und die Felder können nicht bearbeitet werden. Ein Schwachstellenmanager mit der Berechtigung sn_vul.vulnerability_read oder der Persona des Schwachstellenadministrators kann diesen Wert anzeigen, und IT-Korrekturbesitzer mit der Rolle sn_vul.remediation_owner können ihn für die ihnen zugewiesenen Datensätze anzeigen.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

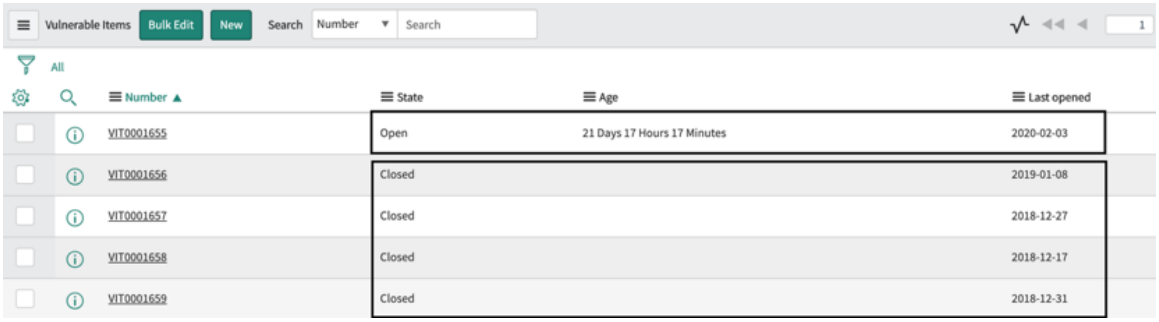
Das AE-Alter wird wie in den folgenden Abbildungen dargestellt angezeigt.

Liste der angreifbaren Elemente

Wie in der folgenden Abbildung dargestellt, wird in der Liste „Angreifbare Elemente“ in der Spalte „Alter“ das Alter in Tagen/Stunden/Minuten (21 Tage 17 Stunden 17 Minuten) nur für aktive AEs angezeigt. Aktive VIs sind VIs in anderen Status als „Geschlossen“. Dieser Alterswert stellt die Anzahl der Tage dar, die das AE aktiv war.

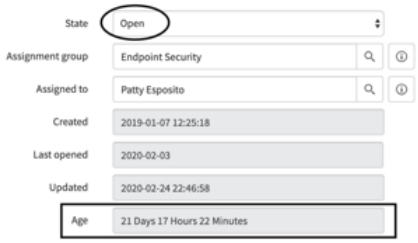
Für VIs im Status „Geschlossen“ wird das Alter nicht angezeigt. Bei VIs, die sich zuvor im Status „Geschlossen“ befanden und dann erneut geöffnet wurden, gibt der Wert die Anzahl der Tage an, die das AE seit dem Datum der letzten Öffnung aktiv war.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

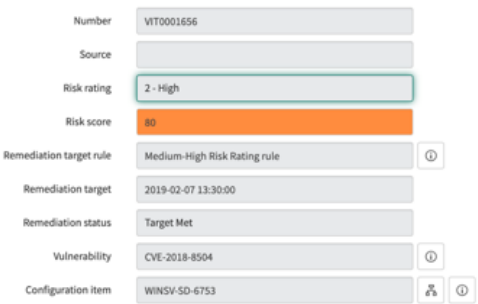


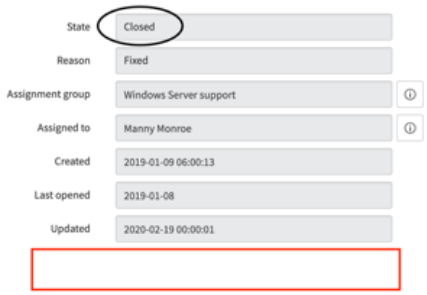
Alter in AE-Datensätzen

In den VI-Datensätzen ist der Wert der Spalte „Alter“ in der Listenansicht für aktive AEs im Feld „Alter“ sichtbar.



Der Wert der Spalte „Alter“ wird für VI-Datensätze im Status „Geschlossen“ nicht angezeigt.



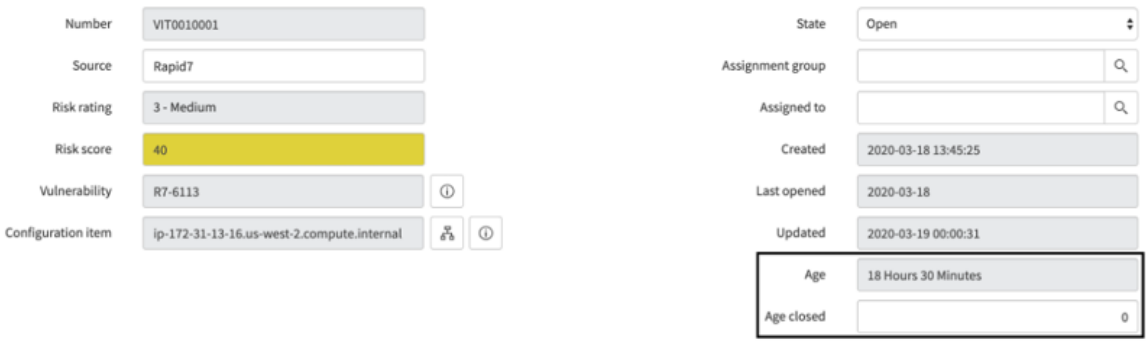


Alter der Liste der angreifbaren Elemente und der VI-Datensätze, wenn ein VI aktualisiert wird

Wenn sich ein AE im Status „Geschlossen“ befindet, wird das Feld „Alter“ nicht angezeigt. Wenn der AE auf „Geschlossen“ wechselt, wird der Wert in Anzahl der Tage aus der Spalte „Alter“ im Feld Alter geschlossen (9) angezeigt (siehe folgende Abbildung). Dieser Wert gibt an, wie viele Tage das AE aktiv war, bevor es in den Status „Geschlossen“ geändert wurde. In der folgenden Abbildung war dieses VI beispielsweise 9 Tage, 18 Stunden und 29 Minuten lang aktiv, im geschlossenen Datensatz wird jedoch nur die Anzahl der Tage (9) angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn dieses AE erneut geöffnet wird und der AE-Status zurück in „Offen“ wechselt, wird das Feld „Alter geschlossen“ auf 0 zurückgesetzt. Da das AE wieder aktiv ist, wird das Alter in Tagen/Stunden/Minuten in der Listenansicht im Alter angezeigt Spalte und auf das Feld Alter in der VIT.



Weitere Informationen zum Anpassen der Berechnungen „Alter“ und „Alter geschlossen“ finden Sie im Artikel KB1703270 .

Zuweisungen von angreifbaren Elementen und Korrekturaufgaben werden entfernt

Sie können die Felder **Zugewiesen an** und **Zuweisungsgruppe** für angreifbare Elemente direkt aus den Datensätzen für angreifbare Elemente (VIT) und Korrekturaufgaben löschen, von denen Sie feststellen, dass sie Ihnen oder Ihren Gruppen möglicherweise nicht korrekt zugewiesen sind.

Übersicht

Ab v16.5 können Korrekturbesitzer die Datensätze für die Neuzuweisung mit der Schaltfläche **Zuweisung** aufheben in den Anwendungen Vulnerability Response und Application Vulnerability Response aktualisieren.

Anwendungsfall

Wenn Sie feststellen, dass VIs nicht in Ihrem Korrekturbereich liegen, oder wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen nicht korrekt zugewiesen wurden, sollten Sie sich oder Ihre Gruppen möglicherweise aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** auf Schwachstellen entfernen Datensätze für Elemente und Korrekturaufgaben.

Heben Sie die Zuweisung des Moduls auf

Die Schaltfläche **„Zuweisung aufheben“** wird für die folgenden Datensätze in jedem anderen Status als „Geschlossen“ oder „Gelöst“ angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Korrekturaufgaben (VULs) sowohl in der klassischen Umgebung als auch in den Vulnerability Response -Arbeitsbereichen. Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, werden die Felder **Zugewiesen an** und **Zuweisungsgruppe** für alle zugehörigen VIs ebenfalls gelöscht.
- Angreifbare Elemente (VITs) in der klassischen -Umgebung und in den -Arbeitsbereichen Vulnerability Response.
- Angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs)

Alle Datensätze, die Sie mit der UI-Schaltfläche oder manuell aktualisieren, werden im Modul Nicht zugewiesen unter den jeweiligen Modulen angezeigt.

Informationen zum erneuten Zuweisen von Datensätzen mithilfe der UI-Aktion *`Unassigned`*] finden Sie unter Entfernen Sie Zuweisungen von angreifbaren Elementen.

Massenbearbeitung

Sie können die Zuweisungsfelder für mehrere VIs in einer Liste löschen. Nachdem Sie die VIs und **Massenbearbeitung**ausgewählt haben, aktivieren Sie im angezeigten Dialogfeld das Kontrollkästchen **Zuweisung** aufheben.

Systemeigenschaft und Benachrichtigungen

Wenn Sie ein Administrator mit der Rolle sn_vulc.vulnerability_admin sind und für einen Datensatz auf **„Zuweisung aufheben“** klicken, löst die Systemeigenschaft *`sn_vul.unassign_vr.approval_required`* standardmäßig den Genehmigungs-Flow aus und erstellt einen Status-Change-Genehmigungsdatensatz im Überprüfungsstatus. Außerdem wird eine Genehmigungsanforderung für den Genehmiger ausgelöst, der wird in der Liste **Meine Genehmigungen** angezeigt.

Hinweis:
Als Schwachstellenadministrator können Sie die Systemeigenschaft *`sn_vul.unassign_vr.approval_required`* auf **„false“** festlegen, um den Genehmigungsprozess zu deaktivieren.

- Wenn der Genehmiger die Anforderung genehmigt, löscht *`sn_vul.default_assignment_group`* den Inhalt der Felder **Zugewiesen an** und **Zuweisungsgruppe** und füllt das Feld **Zuweisungstyp** mit **Nicht zugewiesen**aus. Als Schwachstellenadministrator können Sie den Wert in der Systemeigenschaft *`sn_vul.default_assignment_group`* ändern, sodass die Zuweisungsfelder gelöscht und dann eine bestimmte Gruppe zugewiesen wird. Wenn ein Benutzer beispielsweise für einen Datensatz auf **die Option zum Aufheben der Zuweisung** klickt und Sie ihn zur Überprüfung an eine bestimmte Gruppe weiterleiten möchten, können Sie im Wertfeld der Systemeigenschaft eine System-ID für die Gruppe Ihrer Wahl hinzufügen.

  Hinweis:
  Wenn Sie diesen Wert ändern, werden Benachrichtigungen für alle nicht zugewiesenen VIs, AVITs und CVITs an die von Ihnen angegebene Gruppe gesendet.

- Wenn der Genehmiger Ihre Anforderung ablehnt, wird der Grund für die Ablehnung auf der Registerkarte **Notizen** angezeigt.

Wenn alternativ *`sn_vul.default_assignment_group`* nicht für eine bestimmte Gruppe konfiguriert ist, werden Benutzer, die Sie der Benutzergruppe „Benachrichtigung für die Zuweisung aufheben“ hinzufügen, benachrichtigt, wenn die Zuweisung von Datensätzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aufgehoben wird. Die Systemeigenschaft *sn_vul.default_assignment_group* bestimmt die Benachrichtigungen an diese Gruppe.

Der Zuweisungstyp – **Manuell**, **Regel**oder **Nicht zugewiesen**– ist in den VI-Datensätzen und in der Listenansicht verfügbar. Der Zuweisungstyp **Nicht zugewiesen** wird für Datensätze angezeigt, nachdem die Felder **Zugewiesen an** und **Zuweisungsgruppe** durch die Systemeigenschaft der Funktion gelöscht wurden.

Überwachen Sie Ihre Zuweisungsregeln mit der geplanten Aufgabe für diese Funktion

Eine tägliche regelmäßige Aufgabe zählt die Datensätze beim Übergang zum Zuweisungstyp **Nicht zugewiesen**. Mit dieser Anzahl können Schwachstellenanalysten Zuweisungsregeln überwachen und anpassen, die basierend auf Zuweisungsregeln mit einer höheren Anzahl nicht zugewiesener AEs möglicherweise keine gute Leistung erbringen.

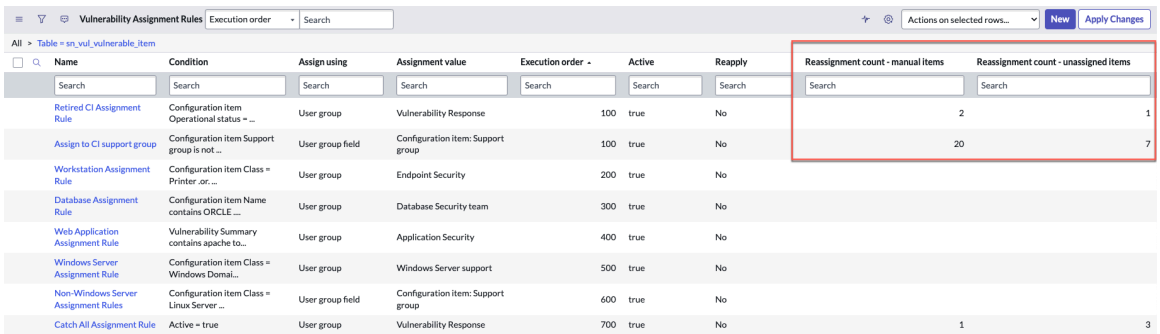
Die geplante Aufgabe *Reassignment count for assignment rules* wird täglich ausgeführt und ermittelt die Gesamtzahl der AEs, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen wurden.

Die von diesem Auftrag gesammelten Anzahlen gelten für die angreifbaren Elemente und die eindeutigen Zuweisungsregeln für Vulnerability Response und Application Vulnerability Response. Die Anzahl wird nach Zuweisungsregel in jeder Zuweisungsregelliste für jedes Modul angezeigt.

Die Aufgabe zählt auch alle Datensätze, deren Zuweisung manuell aufgehoben wurde. Sowohl die manuellen Anzahlen als auch die von dieser Funktion erfassten Anzahlen werden in der Liste „Regeln für die Zuweisung von Schwachstellen“ in zwei Spalten veröffentlicht: *Reassignment count - manual items* und *Reassignment count - unassigned items*.

1. Um diese Anzahlen anzuzeigen, navigieren Sie als Schwachstellen-Administrator zu **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Klicken Sie auf das Zahnradsymbol oben rechts in der Liste, und wählen Sie *Reassignment count - manual items*und *Reassignment count - unassigned items* für die Anzeige aus.
3. Jedes VI, das ursprünglich von einer Regel zugewiesen wurde, anschließend aber automatisch oder manuell neu zugewiesen wurde, enthält in der Listenansicht einen Verweis auf die ursprüngliche Regel.

Das folgende Beispiel zeigt die Anzahl der Neuzuweisungen für zwei Zuweisungsregeln.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners

Sicherheitsrisiko-Rechner automatisieren die Berechnung der Anfangswerte für die Felder von angreifbaren Elementen. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste passende Rechner wird verwendet.

Schwachstellen-Rechner

Das -Basissystem Vulnerability Response enthält zwei Schwachstellen-Rechner, die die Basis-**Risikopunktzahl** für das angreifbare Element festlegen.

- **Standardrisikorechner**
- **Schwachstellenschweregrad**

Schwachstellen-Rechner können so erstellt werden, dass sie angreifbare Elemente anhand beliebiger Kriterien priorisieren und ihre Auswirkungen mithilfe von Bedingungsfiltern bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle, die Klasse des Konfigurationselements (Configuration Item, CI) oder das Alter des angreifbaren Elements handelt, können Sie zusätzliche Schwachstellen-Rechner erstellen, um andere Felder für angreifbare Elemente festzulegen. Oder Sie können die vorhandenen Schwachstellen-Rechner anpassen. Ein Rechner kann so geschrieben werden, dass er jeden Satz von Prioritäten widerspiegelt. Siehe Erstellen Sie einen Vulnerability Response -Rechner und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

Darüber hinaus können Sie Attribute in „configuration_item“ [cmdb_ci] in der Configuration Management Database (CMDB) verwenden, um die Logik für Ihre Vulnerability Response-Risikorechner zu erstellen. Wenn Sie beispielsweise feststellen, dass in Ihrer Organisation nach außen gerichtete CIs angreifbarer sind und möglicherweise eine sofortige Korrektur erfordern, können Sie für diese CIs Attribute wie z. B. `Internet Facing` zuweisen. Dieses und andere Attribut sind in den Versionshinweisen zum Common Service Data Model für das Orlando-Familienrelease aufgeführt. Aktuelle Informationen und Anleitungen zu CMDBfinden Sie in den folgenden Themen:

- Konzeptionelles Modell des Common Service Data Model
- CMDB-Schemamodell

Jeder Rechner enthält eine Liste von Rechnerregeln, wobei eine Bedingung bestimmt, wann sie angewendet wird. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel der Reihe nach ausgewertet, und die erste passende Rechnerregel wird verwendet.

Der Rechner für **den Schwachstellenschweregrad** berechnet die **Risikopunktzahl** für angreifbare Elemente anhand des normalisierten Schwachstellenschweregrads.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Pro Zielfeld (**Risikopunktzahl**) kann jeweils nur ein Rechner aktiv sein. **Der Schwachstellenschweregrad** ist standardmäßig deaktiviert.
- Ab v23.0 von Vulnerability Responsewird bei jeder Aktualisierung der Risikopunktzahl für eine VIT der Abschnitt **„Hinweise“** mit den folgenden Details aktualisiert:
  - Name der Rechnergruppe
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, werden dem Namen die Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, klicken Sie auf eine beliebige Regel, und aktivieren Sie das Kontrollkästchen **Erweiterte Ansicht**. Wählen Sie im Dropdown-Feld **Werttyp** die gewünschte Option aus. Wenn Vorlage ausgewählt ist, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn Skript ausgewählt ist, können Sie entweder das vorhandene Skript hinzufügen oder aktualisieren.

    Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes` hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v25.0.3 von Vulnerability Responseist die Systemeigenschaft standardmäßig deaktiviert. Wenn Sie die Option aktivieren, können Sie nur dann alle Änderungen im Zusammenhang mit der Risikopunktzahl anzeigen.

Alle aktivierten Schwachstellen-Rechner legen die ausgewählten Felder jedes Mal fest, wenn ein angreifbares Element erstellt wird, wenn ein zugehöriges CI oder eine zugehörige Schwachstelle geändert wird oder wenn der zugehörige Link **Risikowert berechnen** in einem angreifbaren Element verwendet wird. Beispielsweise wird die Risikopunktzahl für Datensätze zu angreifbaren Elementen automatisch aktualisiert, wenn der Schweregradwert für eine importierte Schwachstelle aktualisiert wird. Nachdem ein Schwachstellenimport eine Schwachstellenpunktzahl aktualisiert hat, wird für diese Schwachstelle die Kennzeichnung „Neu berechnen“ aktiviert. Die Risikopunktzahlen für die angreifbaren Elemente, für die die Neuberechnungskennzeichnung (wahr) mit dieser Schwachstelle aktiviert ist, werden neu berechnet.

Wenn Sie in einem vorhandenen angreifbaren Element auf den zugehörigen Link **Risikopunktzahl berechnen** klicken und einer der Rechner aktiviert ist, wird das Feld **„Risikopunktzahl“** im angreifbaren Element aktualisiert.

Hinweis:

- Der zugehörige Link **Risikopunktzahl berechnen** ist nur sichtbar, wenn mindestens ein Schwachstellen-Rechner aktiviert ist.
- Ab v22.0 von Vulnerability Responsekönnen Sie die Risikopunktzahl für ein angreifbares Element in Vulnerability Manager Workspace und IT Remediation Workspace aktualisieren, indem Sie in der zugehörigen Datensatzansicht auf die Schaltfläche **Risikopunktzahl berechnen** klicken.
- Ab Version 23.0 von Vulnerability Responsewerden bei jeder Änderung der Risikopunktzahl für eine VIT die folgenden Details im Abschnitt „Hinweise“ der VIT dokumentiert:
  - Name der Rechnergruppe
  - Name des Rechners
  - Feldwerte mit ihrer Gewichtung und ihrem Beitrag zur Risikopunktzahl
  - Endgültige Risikopunktzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln des Schwachstellen-Rechners

Der **Standardrisiko-Rechner** des Basissystem-Rechners enthält die Regel**Standardrisikoregel**, eine spezielle Regel des Schwachstellen-Rechners, die als **Risikoregel**bezeichnet wird. Es berechnet **die Risikopunktzahl** basierend auf mehreren Werten:

- Schwachstellenschweregrad
- Exploit-Informationen
- Relevanz
- Externe Gefährdung des CI mit der Schwachstelle
- EPSS-Punktzahlen

Sie können die Werte anpassen, die in der **Standardrisikoregel** verwendet werden sollen, und festlegen, wie viel Gewichtung jeder dieser Werte erhalten soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der Basis-**Risikopunktzahl**zählt.

Sie können die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.

Ein Beispiel dafür, wie Risikopunktzahlen für Risikoregel-Rechner bestimmt werden, finden Sie unter Beispiel für die Berechnung der Risikopunktzahl für Vulnerability Response.

Zuweisen eines Gewichtungsprozentsatzes

Sie können auch einen Gewichtungsprozentsatz (0–100) auf Feldwertebene zuweisen. Sie können beispielsweise jedem Schweregrad (Keine bis Kritisch) einen Gewichtungsprozentsatz zuweisen.

Wenn die Schweregradgewichtung für die Risikoregel 50 beträgt und die folgenden Gewichtungswerte für den Schweregrad zugewiesen sind:

Schwachstellenschweregrad	Risikopunktzahl
Kritisch	100
Hoch	50
Mittel	20
Keine	0

Wenn der Schweregrad „Kritisch“ ist, beträgt die entsprechende Gewichtung 50. Bei einem hohen Schweregrad beträgt die entsprechende Gewichtung 25, bei einem mittleren Schweregrad eine Gewichtung von 10. Wenn der Schweregrad „Keine“ ist, ist die entsprechende Gewichtung 0. Weitere Informationen finden Sie unter Beispiel für die Berechnung der Risikopunktzahl für Vulnerability Response.

Regeleinstellungen des Schwachstellen-Rechners

Jede Regel hat eine Einstellung **für Reihenfolge**. Das erste Element, das den Bedingungen entspricht, aktualisiert jedoch das Feld **Risikopunktzahl** im angreifbaren Element. Weitere Informationen zu den Regeleinstellungen des Schwachstellen-Rechners finden Sie unter Erstellen Sie einen Vulnerability Response -Rechner. Rechnerregeln ohne Skript haben in der Regel weniger Auswirkungen auf die Leistung als Rechnerregeln mit Skript.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Rechner **für den Schwachstellenschweregrad** des Basissystems enthält Rechnerregeln, die jedem Schweregrad („Keine“ bis „Kritisch“) einen Wert (0–100) für **die Risikopunktzahl** basierend auf dem Schweregrad zuweisen. **Dem Schweregrad „Unbekannt“** wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden, und wie **beim Standardrisikorechner**können neue Rechnerregeln oder neue Risikoregeln erstellt werden.

Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen wird basierend auf Faktoren wie Schweregrad, Kritikalität, Exploit-Informationen usw. eine Risikopunktzahl und Bewertung zugewiesen. Die Geschäftsregel *`Update Risk Rating from Risk Score`* in der Tabelle der angreifbaren Elemente ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert waren.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Ab Version 18.0 von Vulnerability Response,

- Die Risikoeinstufungstypen werden in der Basistabelle als vr_risk_rating bereitgestellt. Diese Typen werden als Teil der Geschäftsregel in jeder Tabelle übergeben, in der die Risikoeinstufung berechnet wird.
- Das Skript wird so geändert, dass Sie die Einträge in den Tabellenwerten für Risikopunktzahlgewichtungen für die Berechnung der Risikoeinstufung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, müssen Sie die Bezeichnungen für die neue Risikoeinstufung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Risikopunktzahlgewichtungen“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn ein Configuration Item (CI) von ohne Internetzugriff in mit Internetzugriff geändert wird.
- Wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittparteieinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer Known Exploit Vulnerability (KEV) verknüpft sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable-Schwachstellenintegration und Tenable-Risikoregel

Die Tenable-Risikoregel ist mit Tenable Vulnerability Integrationverfügbar. Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in Vulnerability Responseverwendet wird. Die Tenable-Risikoregel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisiko-Rechners in den Schwachstellen-Rechnern von Vulnerability Responseinstalliert.

Diese Risikoregel ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten.

Vulnerability Response Erkennungen von angreifbaren Elementen durch Integrationen von Drittparteien

Zeigen Sie alle Informationen an, die von Drittparteiscans in Ihrer Instanz Now Platform® gesammelt werden. Zeigen Sie die zurückgegebenen Ergebnisse der Scans bei Erkennung und angreifbare Elemente in Ihrer Instanz an, da diese Ergebnisse auf den Scannern angezeigt werden.

Übersicht

Die Anwendung Vulnerability Response unterstützt Drittanbieterintegrationen, die Daten zu angreifbaren Elementen aus Ihrer Unternehmensumgebung abrufen. Detaillierte Daten zu Erkennungen, also einzelnen, unterschiedlichen Vorkommen von Schwachstellen, die von den Scannern Ihrer Drittanbieterintegrationen gemeldet werden, werden importiert und sowohl im Erkennungs-Datensatz als auch im Datensatz für angreifbare Elemente in Ihrer Now Platform-Instanz angezeigt.

Drittanbieterintegrationen rufen Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, die von den Scannern gemeldet werden. Erkennungsdaten werden mit angreifbaren Elementen gekoppelt, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn kein VI gefunden wird, wird ein neues erstellt. Erkennungen werden nur durch Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden wurden.

In früheren Versionen von Vulnerability Responsehat die Erkennung angreifbarer Elemente die Beziehung zwischen einem CI (Asset) in Ihrer Umgebung und einer importierten Schwachstelle von einem Drittanbieterscanner zu einem eindeutigen angreifbaren Element in Ihrer Now Platform-Instanz erstellt.

Die Granularität der ursprünglichen, vom Scanner bereitgestellten Daten bleibt erhalten. Bei Erkennungen werden die Erkennungsdaten mit angreifbaren Elementen gekoppelt. Wenn während einer Erfassung kein angreifbares Element gefunden wird, wird ein neues VI erstellt.

Ab Version 21.1.2 von Vulnerability Responsewird eine Systemeigenschaft `sn_vul.show_last_open_detection` im Basissystem bereitgestellt. Standardmäßig ist der Wert dieser Eigenschaft auf „false“ festgelegt, und das aktuelle Verhalten der Zusammenfassung der Werte von der ersten Erkennung bis zum VI bleibt unverändert. Wenn sie jedoch auf „true“ festgelegt ist, wird ein VI nach einer Erfassung automatisch mit der letzten offenen Erkennung aktualisiert. Die Felder wie IP-Adresse, SSL, Port, Protokoll, NetBIOS und Nachweis werden für die VI-Erkennungen aktualisiert. Bei Bedarf können Sie die Erkennungsfelder anpassen, die aktualisiert werden sollen, indem Sie das DetectionBase -Skript ändern.

Um die Werte für die letzte offene Erkennung anzuzeigen, navigieren Sie in der VI-Formularansicht zur Registerkarte **Letzte offene Erkennung**. Um alle im letzten Jahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

geöffneten VIs mit den letzten offenen Erkennungswerten zu aktualisieren, können Sie bei Bedarf die geplante Aufgabe *Update Last Open Detection Value To VITs* ausführen. Diese regelmäßige Aufgabe wird auch im Basissystem bereitgestellt.

Hinweis:
Wenn ein Configuration Item (CI) für ein erkanntes Element geändert wird, werden die entsprechenden Updates auch in den Erkennungen berücksichtigt. Daher können die Erkennungen von einem VI in ein anderes verschoben werden. Basierend auf dieser Änderung und dem Wert der Eigenschaft *sn_vul.show_last_open_detection* werden die Werte der Erkennungen für die Quell- und Ziel-VIs zusammengefasst.

Unterstützte Versionen von Vulnerability Response

Weitere Informationen zum Installieren oder Aktualisieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren.

Unterstützte Drittanbieterintegrationen

Für die Erkennung angreifbarer Elemente ist eine unterstützte Drittanbieterintegration mit Ihrer Anwendung Vulnerability Response erforderlich. Die folgenden Drittanbieterintegrationen werden von der Anwendung Vulnerability Response für die Erkennung angreifbarer Elemente unterstützt:

- Qualys-Host-Erkennungsintegration
- Rapid7-Data Warehouse:
  - Integration angreifbarer Elemente
  - Integration zur Lösung von angreifbaren Elementen
- Rapid7 Vulnerable Item Resolution Integration (InsightVM)
  - Integration mit einer Einblick-VM
  - Integration angreifbarer Elemente – API
- Tenable Vulnerability Integration
- Microsoft Defender Threat and Vulnerability Management

Diese Drittanbieterintegrationen sind mit einem von ServiceNow Storegetrennten Abonnement verfügbar. Weitere Informationen zu diesen Integrationen finden Sie unter Vulnerability Response-Integrationen und Security Operations und ServiceNow Store, um Informationen zum Erhalt von -Berechtigungen zu erhalten.

Um sicherzustellen, dass der Scanner Ihrer Drittpartei für den Import konfiguriert ist, lesen Sie die Anwendung Rapid7 Integration for Security Operations installieren und konfigurieren und Qualys Vulnerability Integration installieren.

Schlüsselbegriffe für die Erkennung angreifbarer Elemente

Schwachstelle

Daten zu Schwachstellen in Software, Betriebssystemen und Assets, die aus internen und externen Quellen importiert wurden. Diese Daten werden importiert und mit vorhandenen Assets (Konfigurationselemente, CIs) verglichen, die in der CMDB aufgeführt sind.

Angreifbares Element

Ein angreifbares Element wird erstellt oder aktualisiert, wenn eine importierte Schwachstelle mit einem CI in der CMDB übereinstimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung

Ein einzelnes, eindeutiges Vorkommen einer Schwachstelle, das von einem Scanner gemeldet wird, der in der Umgebung Now Platform als angreifbares Element erkannt wird. Eine Erkennung enthält angereicherte Daten zu einer Schwachstelle und den entsprechenden angreifbaren Elementen. Diese Daten werden im Erkennungsdatensatz (VID#) und in der Listenansicht für angreifbare Elemente angezeigt, die die folgenden Details enthält:

- Zuerst gefunden (Daten)
- Zuletzt gefunden (Datum)
- DNS-Name
- Net-BIOS-Name
- IP-Adresse
- Port
- Protokoll
- Nachweis
- SSL
- Mal gefunden

Hinweis:
Das Hinzufügen einer Business-Regel in der Erkennungstabelle wirkt sich auf die Leistung der Erfassung aus.

Erkennungsschlüssel

Eine Kombination von Feldern mit Hashwert, die eine Möglichkeit bieten, eine Erkennung zu identifizieren und an ein angreifbares Element zu binden. Erkennungsschlüssel sind integrationsspezifisch.

Erkennungsschlüsselkonfigurationen

Scanner	Schwachste	Port	Protokoll	Asset-ID	Nachweis	NIC
Qualys-IDs	Ja	Ja	Ja	Ja	Nein	NA
Tenable	Ja	Ja	Ja	Ja	Nein	NA
Rapid7	Ja	Ja	Ja	Ja	Ja (Groß-/Kleinschreibung wird nicht beachtet)	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn der Erkennungsschlüssel nicht angegeben ist oder für Versionen vor Vulnerability Response 14.0 verwendet wird, ist der Erkennungsschlüssel eine Kombination aus Schwachstelleneintrag, Port, Protokoll, Asset-ID und Nachweis.
- Ab v19.0 von Vulnerability Responsewird eine neue Erkennungsschlüssel-NIC für Rapid7 InsightVMhinzugefügt, die standardmäßig aktiviert ist. Vorhandene Erkennungen ohne NIC werden mit der ersten eingehenden NIC in der Nutzlast von Rapid7aktualisiert. Der Erkennungsschlüssel wird bei der Erkennung einschließlich der NIC neu berechnet und gefüllt. Neue Erkennungen werden erstellt, wenn ähnliche Erkennungen mit unterschiedlichen NIC-Werten erkannt werden. Für diese Daten wird kein Rollup in der Tabelle der angreifbaren Elemente durchgeführt. Der NIC-Wert wird in einer neuen Spalte in den Tabellen sn_vul_detection_key_config und sn_vul_detection gespeichert.

De duplizieren

Prozess, der von der Anwendung Vulnerability Response zum Reduzieren einzelner Erkennungen in einem einzigen VI verwendet wird, wenn die Daten bestimmte hartcodierte Kriterien erfüllen.

Externe AE-ID

Der Wert, der im Feld „Externe ID“ der VI-Tabelle gespeichert ist. Dieser Wert ist ein Hash, der aus der Kombination von Schlüsseln innerhalb eines AE besteht, der darstellt, was ihn in der Anwendung einzigartig macht. Er besteht aus einem CI und einem angreifbaren Eintrag.

Öffnen Sie gelöste angreifbare Elemente erneut

Angreifbare Elemente, die in Ihrer Instanz Now Platform auf **„Gelöst“** gesetzt wurden, aber durch die nachfolgenden Integrationsausführungen nicht in den **Status „Geschlossen“/ „Behoben“** versetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Geschlossene VIs mit dem Substatus „ **Repariert** “ oder **„Veraltet“** werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIs mit der neuen Schwachstelle abgeglichen werden können.

Gemäß der Skripteinbindung `DetectionBase`, Methode `_shouldReOpenVI()`wird die VIT, die zuvor mit dem Substatus **Fest**, **Veraltet**oder **CI Außer Betrieb genommenGeschlossen**war, erneut geöffnet, und die Erkennung wird der vorhandenen VIT zugeordnet.

Angenommen, das Datum der Schließung eines VIT liegt nach dem Datum „last_found“ einer Erkennung. Sie erwarten, dass diese VIT-Datensätze geschlossen bleiben. Wenn Sie jedoch sehen, dass eine zuvor geschlossene VIT erneut geöffnet wird, bedeutet dies, dass die VIT durch eine frühere Erkennung geschlossen wurde und die Schwachstelle bei einem späteren Scan erneut gefunden wurde. Wenn eine neue Erkennung gefunden wird, die mit der geschlossenen VIT übereinstimmt, die dieselbe Schwachstelle im Configuration Item der VIT aufweist, wird die VIT erneut geöffnet.

Für Rapid7 -Erkennungen ist auf der Rapid7-Konfigurationsseite in Ihrer -Instanz jetzt eine Option verfügbar, um gelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden VIs, die auf **„Gelöst“** gesetzt, aber dann nicht von nachfolgenden Scans auf **„Geschlossen“/„Behoben“** gesetzt wurden, nach der von Ihnen eingegebenen Anzahl von Tagen zurück in den Status „ **Offen“** geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Scanner bei Erkennungen Qualys vom Typ weiterhin AEs findet, die auf **„Gelöst“** festgelegt wurden, dann aber durch nachfolgende Scans nicht in den **Status „Geschlossen“/„Behoben“** übergingen, werden diese AEs zurück in den Status „Offen **“ verschoben**, wenn das zuletzt gefundene Datum nach dem Gelöst-Datum liegt.

Zeigen Sie Erkennungsdaten an

Sie können die Daten, die aus Erkennungen von angreifbaren Elementen importiert wurden, im VI-Datensatz anzeigen. Weitere Informationen finden Sie unter Zeigen Sie Vulnerability Response Erkennungsdaten für angreifbare Elemente an und Überprüfen Sie Vulnerability Response die Erkennungsdaten für angreifbare Elemente in Integrationsausführungsdatensätzen (VINTRUN)..

Vulnerability Solution Management

Korrelieren Sie die Schwachstellen in Ihrer Umgebung automatisch mit den Lösungen, die sie beheben könnten. Identifizieren Sie die Korrekturmaßnahmen, die für Ihre Schwachstellen gelten, und priorisieren Sie sie entsprechend der maximalen Reduzierung des Schwachstellenrisikos.

Vulnerability Solution Management

Sicherheits- und IT-Teams wenden häufig einen erheblichen Teil ihrer Zeit auf die Recherche von Schwachstellenergebnissen auf, um die effektivsten Behandlungsmethoden für ihre Umgebung zu identifizieren. Angesichts des Umfangs und der Komplexität von Schwachstellen in großen Organisationen ist die Übertragung von Schwachstellenergebnissen in Korrekturaufgaben ein manueller, langwieriger und fehleranfälliger Prozess.

Mit Vulnerability Solution Managementkönnen Sie Ihre Schwachstellenergebnisse automatisch mit den Lösungen korrelieren, die sie beheben. Identifizieren Sie die Softwarepatches, Konfigurationsupdates und andere Steuerungen, die die größten Auswirkungen für Ihre Organisation haben, ohne manuellen Aufwand.

Vulnerability Solution Management-Anforderungen

Vulnerability Solution Management ist eine Funktion, die in der Anwendung Vulnerability Response verfügbar ist. Vulnerability Solution Management erfordert ein separates Abonnement.

Weitere Informationen zum Abrufen von Berechtigungen für Anwendungen von ServiceNow Storefinden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab. Unter Anwendung Solution Management for Vulnerability Response installieren finden Sie weitere Informationen zur Installation der Anwendung, nachdem Sie sie auf Ihre Instanz heruntergeladen haben.

Nach der Installation bietet Ihnen Vulnerability Solution Management Zugriff auf die Lösungsdaten Microsoft Security Response Center und Red Hat innerhalb von Vulnerability Response.

Hinweis:

Sie können beide Lösungsanwendungen im Setup-Assistenten konfigurieren. Weitere Informationen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

Integration der Microsoft Security Response Center-Lösung Weitere Informationen zu den importierten Lösungen finden Sie unter und Red Hat Solution Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen

Stellen Sie für die aktuelle Version von Vulnerability Solution Managementsicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben.

Release-Version von Vulnerability Solution Management	Kompatible Versionen von Vulnerability Response	Release-Hinweise
Vulnerability Solution Management v10.3	Vulnerability Response v18.0	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Über Lösungen und Ersatzlösungen

Ein veraltetes Update ist ein vollständiger Ersatz für ein oder mehrere vorherige Releases. Beispielsweise kann ein Service Pack ein Hotfix-Update ersetzen. Lösungen beziehen sich auf Schwachstellen. Lösungen können sich auch auf andere Lösungen in einer Ersetzungskette beziehen. Lösungen beheben Schwachstellen in vorhergehenden Lösungen und sind kumulativ. Vulnerability Solution Management ordnet Schwachstellen aus vorhergehenden Lösungen automatisch Ersatzlösungen zu. Wenn eine ältere Schwachstelle gefunden wird, kann sie mit einer beliebigen höheren Ersatzlösung behoben werden. Die höchste Ersatzlösung wird jedoch bevorzugt, da sie am kumulativsten ist.

Potenzielle Lösungen vs. bevorzugte Lösungen

Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben könnte. Schwachstellen haben oft viele potenzielle Lösungen. Eine bevorzugte -Lösung ist die Einzellösung, die auf die Korrektur einer Schwachstelle oder eines angreifbaren Elements (VI) abzielt. Sie teilt die Absicht mit und ermöglicht detailliertere Bereitstellungsmetriken.

Bevorzugte Lösungen

Vulnerability Solution Management legt automatisch die effektivste Lösung (**Bevorzugte Lösung**) für die erkannte Schwachstelle basierend auf der höchsten Ersatzlösung fest, wenn nur eine einzige Ersatzlösung mit der höchsten Ersatzlösung vorhanden ist. Wenn für die Schwachstelle mehr als eine höchste Ersatzlösung vorhanden ist, wird kein Wert festgelegt. In Vulnerability Responseist eine **bevorzugte Lösung** die Lösung Microsoft Security Response Center oder Red Hat mit der höchsten Ersatzlösung, die aus den mit der Schwachstelle verknüpften Lösungen abgeleitet ist.

Werte**für die bevorzugte Lösung** können für das angreifbare Element oder die Schwachstelle festgelegt werden. Wenn sie direkt für die Schwachstelle festgelegt wird, erben alle angreifbaren Elemente, die der Schwachstelle zugeordnet sind, diese Lösung. Ändern Sie die Werte für die **bevorzugte Lösung** für mehrere angreifbare Elemente mithilfe der Massenbearbeitungsfunktion. Bei der Massenbearbeitung wird nur die **bevorzugte Lösung** für das angreifbare Element aktualisiert, da das Festlegen der **bevorzugten Lösung** auf der Ebene des Schwachstelleneintrags die **bevorzugte Lösung** für alle neuen VIs in Zukunft festlegen würde. Die Massenbearbeitung gilt nur für aktuelle angreifbare Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn für eine Schwachstelle mehrere Ersatzlösungen mit höchster Priorität vorhanden sind, werden die Werte **für Bevorzugte Lösung** auf Schwachstellenebene gelöscht, da diese Lösung vom betroffenen Asset abhängt. Wenn für eine Schwachstelle mehrere Ersatzlösungen mit höchster Priorität vorhanden sind, legen Sie eine **Bevorzugte Lösung** für das angreifbare Element fest. Sie können mithilfe der **Suchliste** im Formular **„Angreifbares Element“** eine andere Lösung festlegen.

Alle bevorzugten Lösungen für die angreifbaren Elemente in einer Korrekturaufgabe befinden sich in einer zugehörigen Liste im **Korrekturaufgaben-** Datensatz.

Nicht alle Lösungsimporte führen zu vollständigen Datenaktualisierungen. Der Ersetzungsprozess wird aktualisiert, wenn:

- Ein angreifbares Element wird erstellt.
- Daten haben sich an einem aktiven VI geändert.

Hinweis:
Ab v22.0 von Vulnerability Responsewerden die Lösungen in den beiden oben genannten Fällen nicht mehr in die Warteschlange gestellt.

- Für einen Drittparteieintrag mit dem CVE wird eine neue Zuordnung erstellt.
- Neue Lösungsdaten wurden seit dem letzten Import freigegeben, eine vorhandene Lösung wird aktualisiert.

Ab v24.0.6 von Vulnerability Responsekönnen Sie neben Lieferantenlösungen auch Lösungen von Scannern erfassen. Zur Erstellung der Lösungen werden die Korrekturdaten von Scannern wie Tenable, Qualysund Microsoft TVM genutzt. Diese Scannerlösungen werden mit den folgenden Integrationen importiert:

- Tenable.sc Plugin-Integration
- Tenable.io Plugin-Integration
- Qualys Knowledge Base (Auffüllen)
- Microsoft TVM Machine Vulnerabilities Integration (vollständiger Import)
- Microsoft TVM – Integration von Computer-Schwachstellen (Delta-Import)

Wenn die Schwachstellen-Integrationen ausgeführt werden, wird vor der Verarbeitung von Drittanbietereinträgen eine Nutzlast von Korrekturinformationen erstellt. Bei Tenable- und Qualyswerden Korrekturdaten auf Einstiegsebene der Schwachstelle oder Drittpartei empfangen. Umgekehrt werden für Microsoft TVM Lösungen auf Erkennungsebene erstellt, was ein direktes Auffüllen der bevorzugten Lösungen für die angreifbaren Elemente ohne weitere Verarbeitung ermöglicht. Diese Lösungen werden basierend auf diesen Korrekturinformationen erstellt und nach Bedarf verarbeitet. Bei der Verarbeitung wird die bevorzugte Lösung für die Schwachstellen ausgefüllt und ein Rolldown für die angreifbaren Elemente durchgeführt. Die bevorzugte Lösung wird in der folgenden Reihenfolge ausgefüllt:

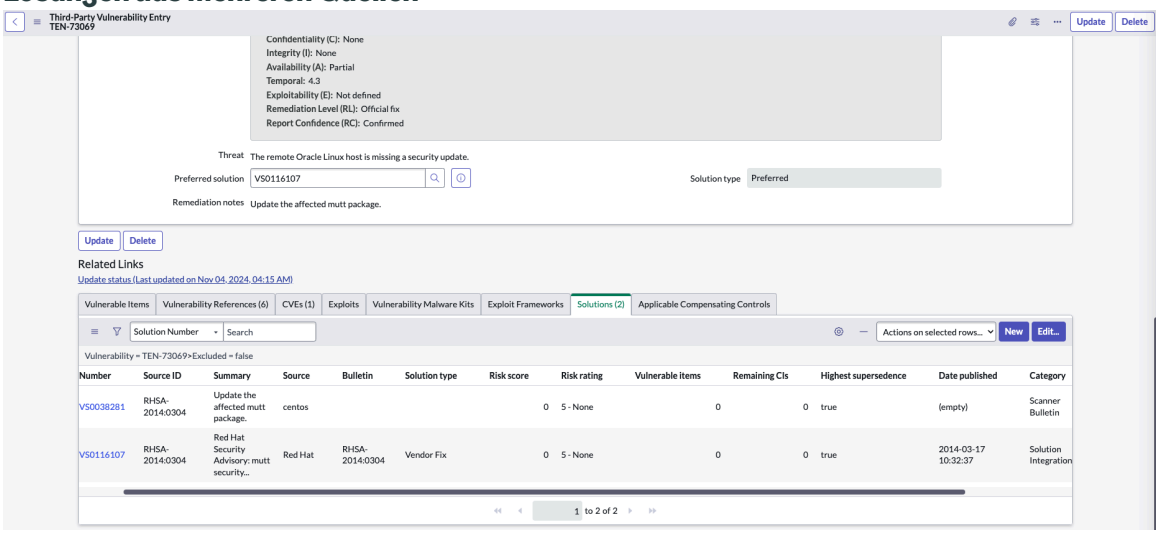
- Manuelle Auswahl: Wenn Sie eine Lösung manuell auswählen, wird sie nicht überschrieben.
- Lieferantenlösungen (Microsoft-, RedHat-, CVRF- und CSAF-Importe): Wenn Sie eine Lösung nicht manuell auswählen, wird die Lieferantenlösung automatisch ausgewählt.
- Aktuelle Lösungen (falls aktiviert): Wenn für eine Schwachstelle mehrere höhere Ersatzlösungen verfügbar sind, bleibt das Feld für die **bevorzugte Lösung** leer. Wenn Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in solchen Fällen die Eigenschaft *sn_vul.latest_solutions*aktivieren, wird die neueste höhere Ersatzlösung des Lieferanten als bevorzugte Lösung eingetragen.

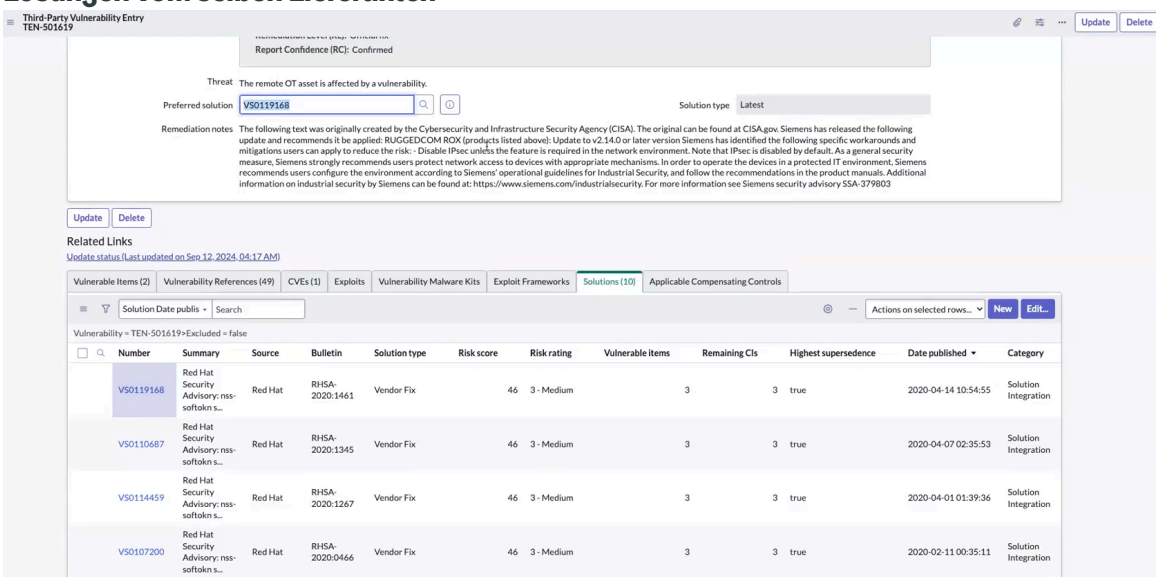
- Scanner-Bulletin-Lösungen (falls aktiviert): Wenn Sie eine Lösung nicht manuell auswählen oder keine Lieferantenlösungen verfügbar sind, wird das Feld **Bevorzugte Lösung** mit den Scannerlösungen ausgefüllt, sofern eine einzelne Scannerlösung vorhanden ist. Sie müssen die Eigenschaft *sn_vul.populate_scanner_solutions* aktivieren, um die Scannerlösungen auszufüllen.

Lösungen aus mehreren Quellen



Dieses Beispiel veranschaulicht die Auswahl einer Lösung, wenn mehrere Lösungen aus verschiedenen Quellen verfügbar sind. In diesem Fall gibt es zwei Lösungen für eine Schwachstelle – eine von einem Lieferanten und eine von einem Scanner. Da die Lösung VS0116107 von einem Lieferanten, z. B. Redhat, mit einer höheren Präferenz empfangen wird, wird sie als bevorzugte Lösung ausgewählt.

Lösungen vom selben Lieferanten

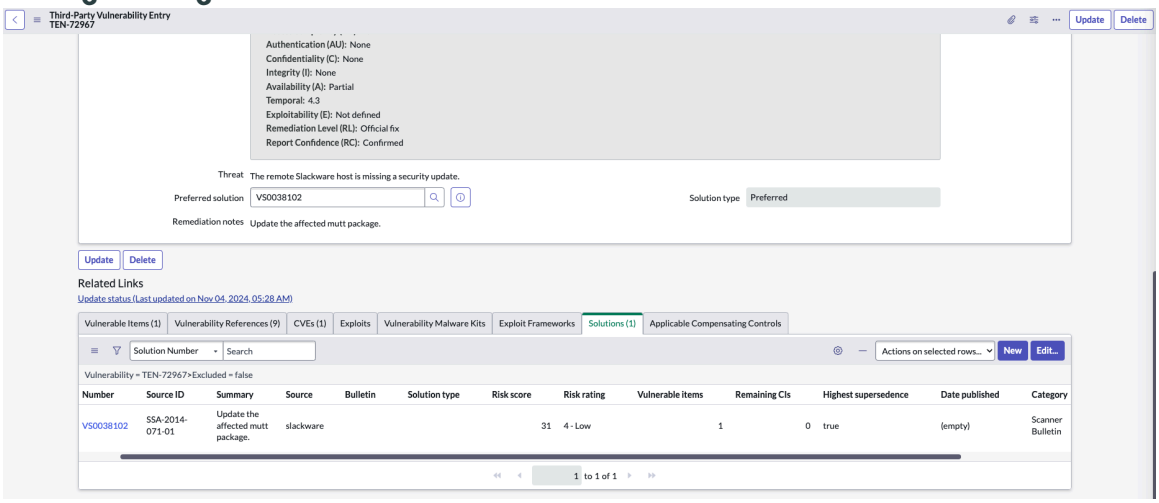


Dieses Beispiel veranschaulicht die Auswahl einer Lösung, wenn mehrere Lösungen vom selben Lieferanten verfügbar sind, in diesem Fall Redhat. Wenn die Eigenschaft *sn_vul.latest_solutions* aktiviert ist und keine anderen Lieferantenlösungen für eine bestimmte Schwachstelle verfügbar sind, werden diese Lösungen verarbeitet, wobei die bevorzugten Lösungen für die Schwachstellen und anschließend für angreifbare Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gefüllt werden. Wenn Sie die Eigenschaft *sn_vul.latest_solutions*aktivieren, wird die neueste Lösung als bevorzugte Lösung ausgewählt.

Lösungen vom gleichen Scanner



Dieses Beispiel veranschaulicht die Auswahl einer Lösung, wenn nur eine Scannerlösung von den Scannern verfügbar ist. Wenn die Eigenschaft *sn_vul.populate_scanner_solutions* aktiviert ist, werden die Lösungen verarbeitet, wobei die bevorzugten Lösungen für die Schwachstellen und anschließend für die angreifbaren Elemente ausgefüllt werden. Wenn mehrere Scannerlösungen vorhanden sind, bleibt das Feld **Bevorzugte Lösung** aufgrund der Mehrdeutigkeit leer.

Verbesserung des Lösungsmanagements und der Leistungsoptimierung

Lösungen werden von verschiedenen Integrationen empfangen, einschließlich Microsoft und Redhat. Ersteres bietet monatliche Updates und erstellt eine Kette von Abhängigkeiten, um die bevorzugte Lösung für Schwachstellen nachzuverfolgen. Andere Integrationen folgen diesem Updateformat jedoch nicht, und für sie muss keine Abhängigkeitskette erstellt werden. Zuvor wurde eine Verarbeitungslogik verwendet, die das Erstellen eines Diagramms umfasst, um den Vorrang aufrechtzuerhalten und die höchsten Ersatzlösungen zu identifizieren. Diese Lösungen wurden als bevorzugte Lösung für die Schwachstellen vorgeschlagen. Da das Erstellen des Diagramms jedoch zeitaufwändig ist, werden die anderen Integrationen von diesem Prozess ausgeschlossen. Zur Verbesserung der Leistung wird ab v22.0 von Vulnerability Responsedie Methode *Utility.processNonGraphSolutions()* in der geplanten Aufgabe *Process Vulnerability Solutions Metrics Queue* aufgerufen. Diese Methode verarbeitet Lösungen aus anderen Integrationen als Microsoft.

Zweitens werden die Lösungen mithilfe der regelmäßigen Aufgabe *Process Vulnerability Solutions Metrics Queue*aus verschiedenen Quellen in die Warteschlange gestellt. Diese geplante Aufgabe umfasst das Rollup von Lösungen aus NVD-Einträgen für Einträge von Drittparteien, das Ausfüllen bevorzugter Lösungen für Schwachstellen und das Aktualisieren der Korrekturstatusmetriken für die Lösungen. In den folgenden Szenarien müssen nur die Korrekturstatusmetriken aktualisiert werden:

- Wenn sich die bevorzugte Lösung für die Schwachstellen ändert
- Wann die VITs erstellt oder gelöscht werden
- Wenn ein VIT-Import abgeschlossen ist

Obwohl sich die Lösungen in der Warteschlange befinden, um nur die Korrekturstatusmetriken zu aktualisieren, versuchen sie dennoch, ein Rollup für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösungen aus NVD-Einträgen für Einträge von Drittanbietern durchzuführen und die bevorzugten Lösungen auszufüllen. Um diesen Prozess zu optimieren, wird in der Tabelle der Schwachstellenlösungen die Spalte **Update-Status** eingeführt. Wenn die Korrekturstatusmetriken für Lösungen aktualisiert werden müssen, ohne dass ein Rollup oder das Ausfüllen bevorzugter Lösungen erforderlich ist, werden die Lösungen nicht mehr in die Warteschlange gestellt. Stattdessen wird die Spalte **Update-Status** direkt als true aktualisiert. Dieser Ansatz ermöglicht die Behandlung von Fällen, in denen nur die Korrekturstatusmetriken aktualisiert werden müssen, was zu Zeit- und Ressourceneinsparungen führt. Sobald die Verarbeitung der Lösungen in der Warteschlange abgeschlossen ist, werden in der geplanten Aufgabe Lösungen identifiziert, für die für die Aktualisierung der Status true festgelegt ist. Dann werden sie durch diese Lösungen iteriert, wobei die Anzahlen berechnet und die Korrekturstatusmetriken entsprechend aktualisiert werden. Dieser Schritt spielt eine wichtige Rolle bei der Verbesserung der Leistung der geplanten Aufgabe, da die Anzahl der Lösungen, die in die Warteschlange gestellt werden müssen, reduziert wird. Um Metriken für den Korrekturstatus anzuzeigen, navigieren Sie zur Tabelle „Schwachstellenlösung“ [sn_vul_solution], und wählen Sie eine Schwachstellenlösung aus. Wählen Sie dann die Registerkarte **Korrekturstatus** aus. Die Registerkarte enthält die folgenden Felder:

Metriken für den Korrekturstatus

Feld	Beschreibung
Bevorzugte Lösungsziele: Korrekturstatus für VIs, für die dies die bevorzugte Lösung ist	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
AEs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
CIs insgesamt	Anzahl der CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Behobene AEs in Prozent	Abschluss in Prozent für die Korrektur angreifbarer Elemente (VIs, Vulnerable Items) Gilt für VIs, für die diese Lösung bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Behobene CIs in Prozent	Abschluss in Prozent für CI-Korrektur. Gilt für VIs, für die diese Lösung bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken für den Korrekturstatus (Fortsetzung)

Feld	Beschreibung
Bevorzugte Lösungsziele (einschließlich „Zurückgestellt“): Korrekturstatus für AEs, einschließlich „Zurückgestellt“, für die dies die bevorzugte Lösung ist	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
AEs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
CIs insgesamt	Anzahl der CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird.
Behobene AEs in Prozent	Abschluss in Prozent für die Korrektur angreifbarer Elemente (VIs, Vulnerable Items) Gilt für VIs, für die diese Lösung bevorzugt wird.
Behobene CIs in Prozent	Abschluss in Prozent für CI-Korrektur. Gilt für VIs, für die diese Lösung bevorzugt wird.
Potenzielle Lösungsziele: Korrekturstatus für alle VIs mit einer Schwachstelle im Zusammenhang mit dieser Lösung	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Potenzielle Lösungsziele (einschließlich „Zurückgestellt“): Korrekturstatus für alle VIs, einschließlich „Zurückgestellt“, mit einer Schwachstelle im Zusammenhang mit dieser Lösung	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt.

Drittens muss sichergestellt werden, dass eine bevorzugte Lösung für Schwachstellen und VITs verfügbar ist, um die Schwachstellen zu beheben. In Situationen, in denen für eine Schwachstelle mehrere höhere Ersatzlösungen vorhanden sind, wird eine bevorzugte Lösung aufgrund von Mehrdeutigkeit nicht ausgefüllt. Zur Bewältigung dieses Szenarios

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird ein Ansatz implementiert, der das Ausführen der Verarbeitungslogik und das Ausfüllen der bevorzugten Lösung umfasst, wenn sie verfügbar ist. In Fällen, in denen es nur eine höhere Ersatzlösung gibt, wird diese als bevorzugte Lösung eingetragen. Wenn mehrere höhere Ersatzlösungen vorhanden sind, bleibt das Feld für die bevorzugte Lösung leer. Das Ziel besteht jedoch darin, die höchste Ersatzlösung, die als neueste veröffentlicht wird, als bevorzugte Lösung anzugeben. Um dies zu erreichen, wird eine Systemeigenschaft *sn_vul.latest_solutions* eingeführt. Standardmäßig ist diese Eigenschaft auf „false“ gesetzt. Wenn Sie die Funktion zum Ausfüllen der neuesten Lösungen als bevorzugte Lösung aktivieren möchten, wenn keine bevorzugte Lösung verfügbar ist, können Sie diese Eigenschaft aktivieren. Nach der Aktivierung wird die Spalte **„Lösungstyp“** in der Schwachstellentabelle mit den folgenden Optionen aktualisiert:

- Bevorzugt: Wenn die bevorzugte Lösung ausgefüllt ist
- Aktuell: Wenn keine bevorzugte Lösung verfügbar ist, wird die neueste Lösung aus dem Satz der höchsten Ersatzlösungen basierend auf dem Wert des Veröffentlichungsdatums ausgewählt. Das Feld, das als aktuelle Lösung ausgewählt werden soll, kann mit der Systemeigenschaft *sn_vul.latest_solutions* angepasst werden. Standardmäßig ist der Wert auf „Veröffentlichungsdatum“ festgelegt, er kann jedoch in „zuletzt geändert“ geändert werden, um die Lösung basierend auf der zuletzt geänderten Spalte in den Lösungen auszuwählen.
- Manuell: Wenn der bevorzugte Lösungstyp manuell aktualisiert wird. Die Priorität für diesen Lösungstyp ist die höchste.

In bestimmten Szenarien kann sich die bevorzugte Lösung für ein angreifbares Element (VIT) von der bevorzugten Lösung für die entsprechende Schwachstelle unterscheiden. Dies tritt auf, wenn die bevorzugte Lösung manuell auf einer VIT und nicht auf der Schwachstelle aktualisiert wird. In solchen Fällen wird das Feld **Lösungstyp** in der VIT ausgeblendet.

Was Vulnerability Solution Management tut

- Ordnet neue angreifbare Elemente (VITs) und Korrekturaufgaben während Integration der Microsoft Security Response Center-Lösung des Imports von und Red Hat Solution Integration automatisch Lösungen zu.

  MSRC Lösungen sind dem aktuellen Bulletin zugeordnet, in dem die Lösung angezeigt wird.

- Ordnet angreifbare Elemente und Korrekturaufgaben automatisch Lösungen zu, wenn Schwachstellen-Datensätze manuell Lösungen zugeordnet werden.

  Hinweis:
  Angreifbare Elemente, die manuell einer anderen Lösung zugewiesen wurden, werden nicht automatisch mit Lösungsänderungen auf Schwachstellenebene aktualisiert.

- MSRC: Erstellt während des Imports Ersatzketten, die Sie in der zugehörigen Liste der Lösung anzeigen können.
- Gibt an, ob eine Lösung eine höchste Ersatzlösung ist oder nicht.
- Listet die Lösungsrisiko **-Punktzahl** auf, die jeder Lösung zugeordnet ist, um Ihnen die größten Möglichkeiten zur Risikoreduzierung zu bieten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwaltet **den Korrekturstatus** für Lösungen in Datensätzen **von Drittanbietern für Schwachstelleneinträge**, **Korrekturaufgaben**und **Schwachstellenlösungen,** damit Sie den Fortschritt der Korrektur nachverfolgen können.

  Sie enthält:

  - Anzahlen der angreifbaren Elemente nach behobenem Prozentsatz für die VIs mit bevorzugten Lösungen, mit und ohne VIs im Status „Zurückgestellt“.
  - Configuration Item (CI) zählt nach Prozent korrigiert für die VIs mit Bevorzugte Lösungen, mit und ohne VIs im Status „Zurückgestellt“.
  - Anzahlen der angreifbaren Elemente nach behobenem Prozentsatz für die VIs mit potenziellen Lösungen, mit und ohne VIs im Status „Zurückgestellt“.
  - Konfigurationselemente zählen nach Prozent korrigiert für die VIs mit Bevorzugte Lösungen, mit und ohne VIs im Status „Zurückgestellt“.

Verwendungsmöglichkeiten Vulnerability Solution Management

- Erstellen Sie Lösungen, die Schwachstellen zugeordnet sind, und zeigen Sie sie an, oder löschen Sie sie, um Schwachstellenlösungen nachzuverfolgen, die nicht von Lösungsinhalten von Drittparteien abgedeckt werden. Die Lösungsintegration mit dem Rapid7 Data Warehouse wird nicht unterstützt.
- Ordnen Sie einem Lösungsdatensatz Schwachstellen von Drittparteien und NVD-Einträge zu.
- Entfernen Sie angreifbare Elemente und Korrekturaufgaben, und ordnen Sie sie erneut einer Lösung zu.
- Zeigen Sie die **bevorzugte Lösung,** die für eine bestimmte Schwachstelle gilt, in den Formularen für Schwachstellen und angreifbare Elemente an.
- Zeigen Sie die zugehörige Liste **„Bevorzugte Lösungen“** auf Korrekturaufgabenformularen an, in denen alle Lösungen aufgelistet sind, die von mindestens einem aktiven AEs in dieser Gruppe bevorzugt wurden.
- Zeigen Sie die **Korrekturstatusdetails** für eine Lösung an, die die Risikoreduzierung zeigen, die mit der Bereitstellung der **bevorzugten Lösung** für Schwachstellen, angreifbare Elemente, Korrekturaufgaben und Lösungsformulare verbunden ist.
- Zeigen Sie im Lösungsformular Schwachstellen an, die für eine bestimmte Lösung gelten.
- MSRC: Zeigen Sie die Ersatzlösungen für eine bestimmte Lösung für eine Schwachstelle an, um das neueste Update zum Bereitstellen oder ein früheres, fokussierteres und effizienteres Update zu finden.
- Zeigen Sie Listen von Lösungen an, die nach verschiedenen Merkmalen sortiert sind.
  - Alle: Lösungen sortiert nach Veröffentlichungsdatum und Nummer.
  - MSRC: Höchste Ersatzlösung: Lösungen mit aktiven, nicht zurückgestellten angreifbaren Elementen. Sortiert nach **Höchste Ersatzlösung**, **Veröffentlichungsdatum**und **Nummer**.
  - Mit angreifbaren Elementen: Lösungen mit aktiven, nicht zurückgestellten angreifbaren Elementen. Sortiert nach **Höchste Ersatzlösung** oder **Bevorzugt**, **Risikopunktzahl**und **Anzahl**. Bei Bereitstellung bieten die Top-Einträge in der Liste die größte Risikoreduzierung für die Assets in Ihrer Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikopunktzahl und Risikobewertung des Lösungsdatensatzes

Hinweis:
Risikopunktzahl und **Risikobewertung** des Lösungsdatensatzes unterscheiden sich von den Feldern, die für Schwachstellen, angreifbare Elemente und Korrekturaufgaben verwendet werden.

Die **Risikopunktzahl** des Lösungsdatensatzes ist eine gewichtete Berechnung, die auf der **Risikopunktzahl** des angreifbaren Elements und der Anzahl aktiver angreifbarer Elemente basiert, bei denen diese Lösung die **potenzielle Lösung**ist. Die **Risikopunktzahl** der Lösung gibt eine Schätzung der Risikoreduzierung an, die durch die Lösung erwartet wird.

Die **Risikopunktzahl** des Lösungsdatensatzes wird wie folgt berechnet:

- Zunächst werden 85 % der höchsten oder maximalen **Risikopunktzahl** eines aktiven angreifbaren Elements mit dieser potenziellen Lösung berechnet.
- Die **Risikopunktzahl** des Lösungsdatensatzes tabelliert dann die Gesamtzahl der angreifbaren Elemente mit dieser potenziellen Lösung. Für jeden Bereich der Anzahl der angreifbaren Elemente addieren sie einige Punkte und erhalten so eine Gesamtsumme.
  - 0–09 angreifbare Elemente fügen keine Punkte hinzu
  - 10–99 angreifbare Elemente fügen 5 Punkte hinzu
  - 100–999 angreifbare Elemente fügen 10 Punkte hinzu
  - 1000 und mehr angreifbare Elemente fügen 15 Punkte hinzu

  Beispiel: Für eine **Risikopunktzahl** eines angreifbaren Elements von 80 würde die **Risikopunktzahl** des Lösungsdatensatzes bei 68 beginnen. Wenn es insgesamt 200 aktive angreifbare Elemente mit dieser potenziellen Lösung gäbe, wäre die endgültige **Punktzahl für das** Lösungsrisiko 78.

Die **Risikobewertung** des Lösungsdatensatzes unterteilt die **Risikopunktzahl** des Lösungsdatensatzes in Bereiche von Kritisch bis Keine. **Die Risikobewertung** der Lösung bewertet die Risikoreduzierung für die angreifbaren Elemente, die von dieser Lösung korrigiert werden.

Bis VR v16.1 wurde die resultierende Lösungsrisiko **-Punktzahl durch Risikobewertungen** in die folgenden Bereiche unterteilt:

- 1 – Kritisch (Lösungsrisiko **-Punktzahl**über 90)
- 2 – Hoch (70–89 **Risikopunktzahl**für Lösungsdatensatz)
- 3 – Mittel (30–69 **Risikopunktzahl**für Lösungsdatensatz)
- 4 - Niedrig (1–29 **Risikopunktzahl**für Lösungsdatensatz)
- 5 – Keine (0 Lösungsdatensatz – **Risikopunktzahl**)

Ab VR v16.1 wird die resultierende Lösungsrisiko **-Punktzahl** für Solution Management durch Risikobewertungen in die folgenden Bereiche unterteilt:

- 1 – Kritisch (Lösungsrisiko **-Punktzahl**über 90)
- 2 – Hoch (70–89 **Risikopunktzahl**für Lösungsdatensatz)
- 3 - Mittel (40–69 **Risikopunktzahl**für Lösungsdatensatz)
- 4 - Niedrig (1–39 **Risikopunktzahl**für Lösungsdatensatz)
- 5 – Keine (0 Lösungsdatensatz – **Risikopunktzahl**)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

Zeigen Sie den Fortschritt der Statusbereitstellung eines aktuellen Patch-Zyklus für das höchste Ersatzmodul an, sortiert nach Datum.

Zeigen Sie mit dem Modul „Mit angreifbaren Elementen“ die Lösungen mit dem höchsten Wert an, sortiert nach Risikopunktzahl.

Lösungslisten vermitteln wichtige Lösungsdetails, Risikopunktzahlen und Bereitstellungsmetriken. Verwenden Sie für die Priorisierung **die Risikopunktzahl** und die Anzahl der aktiven AEs. Erfahren Sie, welche Lösungen im aktuellen Patch-Zyklus nicht vorankommen. Dies kann ein Hinweis darauf sein, dass eine erforderliche Bereitstellung versäumt wurde.

Hinweis:
Fügen Sie **%VIs remedied(percent_nd_pref_vis_remediated)** aus dem Menü **„Listenspalten personalisieren“** für den Korrekturfortschritt im Formular „Schwachstellenlösungen“ hinzu.

Integration der Microsoft Security Response Center-Lösung

Überprüfen und implementieren Sie die von Integration der Microsoft Security Response Center-Lösungbereitgestellten Korrekturlösungen.

Integration der Microsoft Security Response Center-Lösung ist in der Funktion Vulnerability Solution Management von Vulnerability Responseenthalten und über ein separates Abonnement verfügbar. Unter Vulnerability Solution Management finden Sie weitere Informationen darüber, wie Vulnerability Response Lösungen integriert.

Microsoft Security Response Center untersucht Berichte über Sicherheitsschwachstellen, die sich auf Microsoft-Produkte und -Services auswirken, und stellt Lösungsinformationen bereit, um das Management von Sicherheitsrisiken zu erleichtern. Lösungen sind bekannte Korrekturen, die aus dem Produkt Integration der Microsoft Security Response Center-Lösung in Ihr Microsoft Security Response Center importiert werden.

Integration der Microsoft Security Response Center-Lösung enthält Einstiegspunkte für das Produkt Microsoft Security Response Center, die als geplante Aufgaben aufgerufen werden. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren. Geplante Aufgaben werden automatisch und in der angegebenen Reihenfolge ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Stellen Sie für die aktuelle Version der Lösungen Vulnerability Solution Management und Microsoft Security Response Center sicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben.

Weitere Informationen zum Installieren und Konfigurieren von Vulnerability Solution Management und Lösungsintegrationen finden Sie unter Anwendung Solution Management for Vulnerability Response installieren und Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Release-Version von Vulnerability Response	Version von Vulnerability Solution Management	Release-Hinweise
Vulnerability Response v15.0	v10.3	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Rollen

Integration der Microsoft Security Response Center-Lösung -Aufgaben betreffen die folgenden Rollen.

- sn_vul.vulnerability_admin oder sn_vul.admin (veraltet): Kann Datensätze lesen, schreiben und löschen.
- sn_vul.vulnerability_write: Kann Datensätze lesen und schreiben.
- sn_vul.vulnerability.read: Kann Datensätze lesen.
- sn_vul.remediation_owner: Kann interne Notizen zu Datensätzen lesen und schreiben, die der Fehlerkorrekturspezialistengruppe oder einer Person zugewiesen sind. (In der Rolle itil enthalten.)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Integration der Microsoft Security Response Center-Lösung

Um Integration der Microsoft Security Response Center-Lösunganzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.

Die folgende Integration ist im Basissystem enthalten.

Integration der Microsoft Security Response Center-Lösung

Integration	Beschreibung
Integration der Microsoft Security Response Center-Lösung	Ruft Lösungen und Zuordnungen aus der National Vulnerability Database (NVD) ab, um Lösungen mit Schwachstellen, angreifbaren Elementen und Korrekturaufgaben zu verknüpfen. **Hinweis:** Integration der Microsoft Security Response Center-Lösung bietet keine Lösungen vor 2016.

Lösungen

Informationen zum Anzeigen importierter Lösungen in einer Liste finden Sie unter Zeigen Sie eine Lösung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Red Hat Solution Integration

Sie können die von Red Hat Solution Integration bereitgestellten vorgeschlagenen Korrekturlösungen in der Anwendung Vulnerability Response überprüfen und implementieren.

Red Hat Solution Integration ist in der Funktion Vulnerability Solution Management von Vulnerability Responseenthalten und über ein separates Abonnement verfügbar. Unter Vulnerability Solution Management finden Sie weitere Informationen darüber, wie Vulnerability Response Lösungen integriert.

Red Hat Solution Integration untersucht Berichte über Sicherheitsschwachstellen, die Produkte und Services Red Hat von betreffen, und stellt Informationen zur Lösung bereit, um das Management von Sicherheitsrisiken zu erleichtern. Lösungen, die als Remediationen bezeichnet werden, werden aus Red Hat Solution Integration in Ihren Red Hatimportiert.

Ab Version 21.0 von Vulnerability Responseüberträgt Red Hat Nutzlasten im CSAF-Format (Common Security Advisory Framework) und nicht mehr im CVRF-Format (Common Vulnerability Reporting Framework). CSAF, ein XML-basierter Standard, unterscheidet sich sowohl in der Struktur als auch im Format von CVRF. Um dieser Änderung Rechnung zu tragen, wurde ein neuer CSAF-Parser entwickelt. Dieser Parser interpretiert das CSAF-Format und extrahiert die erforderlichen Felder, um die Tabellen entsprechend zu füllen.

Hinweis:
Standardmäßig erhalten Sie die Nutzlast im CSAF-Format.

Die folgenden Auszüge zeigen das Integrationsskript zum Analysieren der von Red Hat empfangenen Nutzlast im CSAF- bzw. CVRF-Format.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(true);
})(integrationProcessGr);
```

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(false);
})(integrationProcessGr);
```

Red Hat Solution Integration enthält Einstiegspunkte für das Red Hat-Produkt und wird als regelmäßige Aufgabe aufgerufen. Die geplante Aufgabe vereinfacht den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellenmanagementsystemen synchronisiert. Er wird automatisch ausgeführt. Sie können die geplante Aufgabe auch manuell ausführen.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Stellen Sie für die aktuelle Version der Lösungen Vulnerability Solution Management und Red Hat sicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben.

Weitere Informationen zum Installieren und Konfigurieren von Vulnerability Solution Management und Lösungsintegrationen finden Sie unter Anwendung Solution Management for Vulnerability Response installieren und Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

Release-Version von Vulnerability Response	Version von Vulnerability Solution Management	Release-Hinweise
Vulnerability Response v15.0	v10.3	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Rollen

Red Hat Solution Integration -Aufgaben betreffen die folgende Rolle:
sn_vul.configure_rhsa_integration

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Red Hat Solution Integration

Um Red Hat Solution Integrationanzuzeigen, navigieren Sie zu **Vulnerability Response** > **Administration** > **Integrationen**.

Die folgende Integration ist im Basissystem enthalten.

Red Hat-Integration

Integration	Beschreibung
Red Hat Solution Integration	Ruft Lösungen und Zuordnungen aus der National Vulnerability Database (NVD) ab, um Lösungen mit Schwachstellen, angreifbaren Elementen und Korrekturaufgaben zu verknüpfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösungen

Informationen zum Anzeigen importierter Lösungen in einer Liste finden Sie unter Zeigen Sie eine Lösung an.

Rapid7 Lösungsmanagement

Lösungen sind bekannte Korrekturen, die entweder aus dem Data Warehouse Rapid7oder Rapid7 InsightVM Rapid7 in Ihr Rapid7 Vulnerability-Integration importiert werden. Das Data Warehouse importiert sowohl Lösungen als auch Ersatzlösungen. Mit Rapid7 InsightVMerhalten Sie Lösungen als Teil der Rapid7 Vulnerable Item Integration – API.

Ab Version 21.0 von Vulnerability Responseändert sich die Art und Weise, wie Lösungen von Rapid7 InsightVMerstellt werden. Anstatt sich auf die Felder **„solution_summary“**, **„solution_fix“**oder **„solution_type“** zu verlassen, erstellt Rapid7 InsightVM jetzt Lösungen mit der vom Scanner bereitgestellten Lösungs-ID. Selbst wenn diese Felder leer sind, wird eine Lösung erstellt, sofern eine Lösungs-ID verfügbar ist.

Um importierte Lösungen als Liste anzuzeigen, navigieren Sie zu **Rapid7** > **Lösungen**.

Wenn das Plugin Vulnerability Solution Management aktiviert ist, bietet die neueste Version von Rapid7 Vulnerability-Integration die folgenden wichtigen Funktionen für Lösungen:

- Das Lösungsmanagement Rapid7 für wird zum Lösungsmanagement für Schwachstellen verschoben.
- Eine neue Integration von Rapid7 Prerequisite Solution Management für das Data Warehouse wird eingeführt. Die Integration ruft die erforderliche Lösung aus dem Data Warehouse Rapid7 ab.
- Die zugehörige Liste Rapid7 (Lösung) zu Drittparteieinträgen (TPE) wird ausgeblendet.
- Die zuvor importierten Daten können im neuen Datenmodell angezeigt werden. Rapid7-Lösungen, Lösungsersetzung und Zuordnung der Schwachstellenlösung werden erneut importiert, und das Feld **Importieren seit** wird auf leer gesetzt. Das Feld wird in Lösungsmanagement ausgefüllt.
- Die Erkennungen werden aktualisiert, um das Lösungsfeld auszufüllen. Erkennungen zeigen die Lösungen als Teil von Vulnerability Solution Management an.
- Rapid7 erhält eine höhere Priorität gegenüber anderen Lösungen, wenn die bevorzugte Lösung auf TPE für das Data Warehouse Rapid7 festgelegt wird.
- Die Lösungen führen ein Rollup zu angreifbaren Elementen (VI) aus Erkennungen für Rapid7 InsightVMdurch.

Hinweis:
Wenn Sie das Plugin Vulnerability Solution Management nicht aktiviert haben, funktioniert die Anwendung unverändert.

Vulnerability Solution Management

Wenn Sie das Plugin Vulnerability Solution Management aktiviert haben, werden die Lösungen Rapid7 für das Data Warehouse Rapid7 und Rapid7 InsightVM in die Tabelle „Schwachstellenlösungen“ [sn_vul_solution] gefüllt. Wenn Sie jedoch das Plugin Vulnerability Solution Management nicht aktiviert haben, funktioniert Rapid7 Vulnerability-Integration unverändert und importiert die Lösungen in die anwenderdefinierte Tabelle [sn_vul_r7_solution].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Tabelle der Schwachstellenlösungen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Schwachstellenlösungen** Hier können Sie die Lösungen verschiedener Lieferanten anzeigen und vergleichen. Um importierte Lösungen in der anwenderdefinierten Tabelle anzuzeigen, navigieren Sie zu **Alle** > **Rapid7 Vulnerability-Integration** > **Lösungen**.

Hinweis:
Nach Quelle gruppieren, um Lösungen basierend auf Lieferanten anzuzeigen.

Rapid7 Prequired Solution Management integration

Wenn Sie das Plugin Vulnerability Solution Management aktiviert haben, wird ein Korrekturskript ausgeführt und ändert die Reihenfolge der Integrationen. Die neue Rapid7 Prerequisite Solution Integration für das Data Warehouse Rapid7 ordnet die Lösungen den erforderlichen Lösungen zu. Die Integrationen werden in der folgenden Reihenfolge ausgeführt:

1. Rapid7 Lösungsintegration
2. Rapid7 Voraussetzungslösung
3. Rapid7 Ersatz für Lösungsintegration
4. Rapid7 Integration der Schwachstellenlösungszuordnung
5. Rapid7 VI-Lösungsintegration (ab v19.0 von Vulnerability Response)

Hinweis:
Wenn Sie die Integrationen manuell ausführen, beginnen Sie mit Rapid7 -Lösungsintegration. Ändern Sie die Next-Integrationskette in der Rapid7 Integration nicht. Die Sequenz wird in der Spalte Next Integration (Nächste Integration) definiert.

Zugehörige Liste Rapid7 (Lösungen) auf TPE

Wenn Sie das Plugin Vulnerability Solution Management aktiviert haben, haben Sie folgende Möglichkeiten:

- Sie können die TPEs anzeigen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Drittpartei**.
- Die zugehörige Liste Lösungen (Rapid7), die in älteren Releases verfügbar war, kann nicht angezeigt werden.
- Sie können die Rapid7-bezogenen Lösungen in der zugehörigen Liste Lösungen zusammen mit Lösungen aus anderen Quellen wie RedHat, Microsoft (MSRC) usw. anzeigen.

Wenn Sie das Plugin Vulnerability Solution Management nicht aktiviert haben, geschieht Folgendes:

- Die Funktionalität zugehöriger Listen bleibt unverändert.
- Sie können die zugehörige Liste Lösungen (Rapid7) anzeigen.
- Die zugehörige Liste Lösungen wird ausgeblendet.

Bevorzugte Lösung für TPE und VIs

Rapid7 ruft die Lösung aus dem Data Warehouse auf der Drittpartei-Eintragsebene (TPE) ab und für Rapid7 InsightVM die Lösung aus dem Data Warehouse auf der Erkennungsebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für ein Data Warehouse Rapid7 wird die Lösung auf folgende Weise verwaltet:

- Die bevorzugte Lösung wird basierend auf der Schwachstellen- und Lösungszuordnung für das TPE festgelegt.
- Wenn die Schwachstelle von Rapid7 eine höchste Ersatzlösung von Rapid7hat, wird sie als bevorzugte Lösung festgelegt, unabhängig von anderen Lösungen von Lieferanten, die mit dieser Schwachstelle verbunden sind.
- In allen anderen Fällen bleibt der Flow der bevorzugten Lösung unverändert. Weitere Informationen zum Standardverhalten bevorzugter Lösungen finden Sie unter Vulnerability Solution Management.

Für Rapid7 InsightVMwird die Lösung auf folgende Weise verwaltet:

- Die bevorzugte Lösung ist ein Rollup von Erkennungen zu VIs.
- Wenn eine einzelne Erkennung und Lösung von Rapid7vorhanden ist, wird ein Rollup für die Lösung bis zum AE durchgeführt.
- Wenn mehrere Erkennungen vorhanden sind und alle dieselbe Lösung von Rapid7haben, wird ein Rollup für die Lösung bis zum VI durchgeführt.
- Wenn mehrere Erkennungen mehrere Lösungen von Rapid7haben, wird die neueste Lösung bis zum VI zusammengefasst.

Ab v19.0 von Vulnerability Responsewird die bevorzugte, von Rapid7 Data Warehouse generierte Lösung direkt in angreifbare Elemente eingetragen, indem Rapid7 unter Umgehung von Vulnerability Solution Managementausgeführt wird. Dieser Change stellt sicher, dass jegliche Ungewissheit hinsichtlich möglicher Lösungen für diese angreifbaren Elemente beseitigt wird.

Um diese direkte Auffüllung über Rapid7zu erreichen, werden die folgenden Schritte ausgeführt:

- Eine neue Integration, Rapid7 VI Solution Integration, wird eingerichtet und in den vorhandenen Workflow von Rapid7 Vulnerability Integration integriert.
- Eine neue Tabelle [sn_vul_r7_rapid7_vi_solution_import] wird erstellt.
- Eine neue Transformationszuordnung Rapid7 VI-Lösungstransformation wird erstellt.
- Die Skripteinbindung Rapid7AssetsImportProcessor wird geändert, um die Verarbeitung von Lösungen auszuschließen, die von Rapid7 innerhalb von Vulnerability Solution Managementgeneriert wurden.

Nach Ausführung der Rapid7 VI-Lösungsintegration werden die von Rapid7 abgerufenen unverarbeiteten Daten in der neu erstellten Tabelle gespeichert. Anschließend wird die Rapid7 VI-Lösungstransformation ausgelöst, die diese Daten verarbeitet und die bevorzugte Lösung direkt in die Tabelle der angreifbaren Elemente eingetragen.

Hinweis:
Die Rapid7 VI Solution Integration füllt die bevorzugte -Lösung ausschließlich aus, wenn das Plugin Vulnerability Solution Management „ installiert wurde.

Ab v22.0 von Vulnerability Responsewerden die Lösungen von Rapid7 bei Ausführung der geplanten Aufgabe *`Process Vulnerability Solutions Metrics Queue`*nicht mehr in die Warteschlange gestellt. Diese geplante Aufgabe umfasst das Rollup von Lösungen aus NVD-Einträgen für Einträge von Drittparteien, das Ausfüllen bevorzugter Lösungen für Schwachstellen und das Aktualisieren der Korrekturstatusmetriken für die Lösungen. In den folgenden Szenarien müssen nur die Korrekturstatusmetriken aktualisiert werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn sich die bevorzugte Lösung für die Schwachstellen ändert
- Wann die VITs erstellt oder gelöscht werden
- Wenn ein VIT-Import abgeschlossen ist

Obwohl sich die Lösungen in der Warteschlange befinden, um nur die Korrekturstatusmetriken zu aktualisieren, versuchen sie dennoch, ein Rollup für Lösungen aus NVD-Einträgen für Einträge von Drittanbietern durchzuführen und die bevorzugten Lösungen auszufüllen. Um diesen Prozess zu optimieren, wird in der Tabelle der Schwachstellenlösungen die Spalte **Update-Status** eingeführt. Wenn die Korrekturstatusmetriken für Lösungen aktualisiert werden müssen, ohne dass ein Rollup von Lösungen aus NVD-Einträgen in Einträge von Drittparteien oder das Ausfüllen bevorzugter Lösungen erforderlich ist, werden sie nicht mehr in die Warteschlange gestellt. Stattdessen wird die Spalte **Update-Status** direkt als true aktualisiert. Dieser Ansatz ermöglicht die Behandlung von Fällen, in denen nur die Korrekturstatusmetriken aktualisiert werden müssen, was zu Zeit- und Ressourceneinsparungen führt. Sobald die Verarbeitung der Lösungen in der Warteschlange abgeschlossen ist, werden in der geplanten Aufgabe Lösungen identifiziert, für die für die Aktualisierung der Status true festgelegt ist. Dann werden sie durch diese Lösungen iteriert, wobei die Anzahlen berechnet und die Korrekturstatusmetriken entsprechend aktualisiert werden. Dieser Schritt spielt eine wichtige Rolle bei der Verbesserung der Leistung der geplanten Aufgabe, da die Anzahl der Lösungen, die in die Warteschlange gestellt werden müssen, reduziert wird.

Lösungsersetzungskette, die aus Rapid7 Data Warehouse für eine Schwachstelle importiert wird

Sie können die Ersatzlösungen für eine Lösung anzeigen, indem Sie eine Schwachstellenlösung und die zugehörige Liste Ersatzlösungen auswählen. Sie können die vorhergehenden Lösungen anzeigen, indem Sie die zugehörige Liste Vorangehende Lösungen auswählen. Wenn Sie eine Lösung an das TPE anhängen, wird die Ersatzlösung dieser Lösung an dieses TPE angehängt.

Ändern Sie die maximale Tiefe der Lösungsersetzungskette in einem Diagramm anhand der Systemeigenschaft

Die im Datenmodell Rapid7 empfangene Lösungsersetzungskette ist zu lang, um das Diagramm während des Ausfüllens der bevorzugten Lösung zu erstellen. Um die Tiefe der Kette einzuschränken, wird eine Systemeigenschaft namens `sn_vul.max_recursion_depth` mit einem Wert von 500 erstellt. Wenn die Kettentiefe mehr als 500 beträgt, wird der Rest der Kette ignoriert. Um die maximale Tiefe der Kette zu ändern, navigieren Sie zur Tabelle [sys_properties], und ändern Sie den Wert der Eigenschaft.

Die Anwendung Rapid7 wird aktualisiert

Wenn Sie das Upgrade des Plugins Rapid7 Vulnerability-Integration durchführen und das Plugin Vulnerability Solution Management noch nicht aktiviert haben, funktioniert die Anwendung unverändert.

Unabhängig davon, ob Sie das Plugin Vulnerability Solution Management vor oder nach dem Upgrade der Anwendung Rapid7 aktivieren, bleibt das Feld **Importieren seit** für die folgenden Integrationen leer:

- Rapid7 Subsinging Solution Integration
- Integration der Rapid7-Schwachstellenlösungszuordnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rapid7-Lösungsintegration

Hinweis:
Ab der nächsten Integrationsausführung wird die Tabelle der Schwachstellenlösungen mit Daten gefüllt.

Für Rapid7 InsightVMwerden die Daten auf Erkennungsebene empfangen. Wenn die -Integration Rapid7 InsightVM ausgeführt wird, werden die Lösungen in die Tabelle der Schwachstellenlösungen importiert.

Generisches Framework zur Erfassung von Daten von beliebigen Lösungsanbietern

Ein generisches Framework für die Integration von Lösungsinformationen ist verfügbar, um die Erfassung von Daten in verschiedenen Dateiformaten von Lösungsanbietern zu unterstützen. Diese Formate beschleunigen den Informationsaustausch und die Verarbeitung und erleichtern die gemeinsame Nutzung kritischer sicherheitsbezogener Informationen in einem standardisierten Berichtsformat.

Folgende Dateiformate werden unterstützt:

Common Vulnerability Reporting Framework (CVRF)

Das Common Vulnerability Reporting Framework (CVRF) ist eine XML-basierte Sprache. Wichtige Anbieter wie Oracle, Red Hat, Ciscound MicrosoftMicrosoft Azure Event Hubs unterstützen das CVRF-Format.

Common Security Advisory Framework (CSAF)

Das Common Security Advisory Framework (CSAF) ist ein Open-Source-Standard, der JSON-basierte strukturierte, maschinenlesbare Sicherheitswarnhinweise bereitstellt. Wichtige Anbieter wie Siemens, Red Hat, Trefferarchi und Näher unterstützen das CSAF-Format.

Das von CVRF oder CSAF unterstützte Lösungsmanagement umfasst die folgenden Schlüsselfunktionen:

- Konfiguration über den Setup-Assistenten
- Unterstützung für den Import von CVRF- oder CSAF-Daten über Dateiimport
- Unterstützung für den Import von CVRF- oder CSAF-Daten über die CVRF- - oder CSAF-URL -URL
- Unterstützung für den Import von CVRF- oder CSAF-Daten über Hinweise
- Zuordnung von Lösungen zu zugehörigen Schwachstellen

Das Plugin Vulnerability Response übernimmt die Aktualisierung der Metrikstatus der erstellten Lösung.

Weitere Informationen zur Konfiguration der Lösungsanbieter finden Sie unter Konfigurieren Sie die Anbieter von Schwachstellenlösungen.

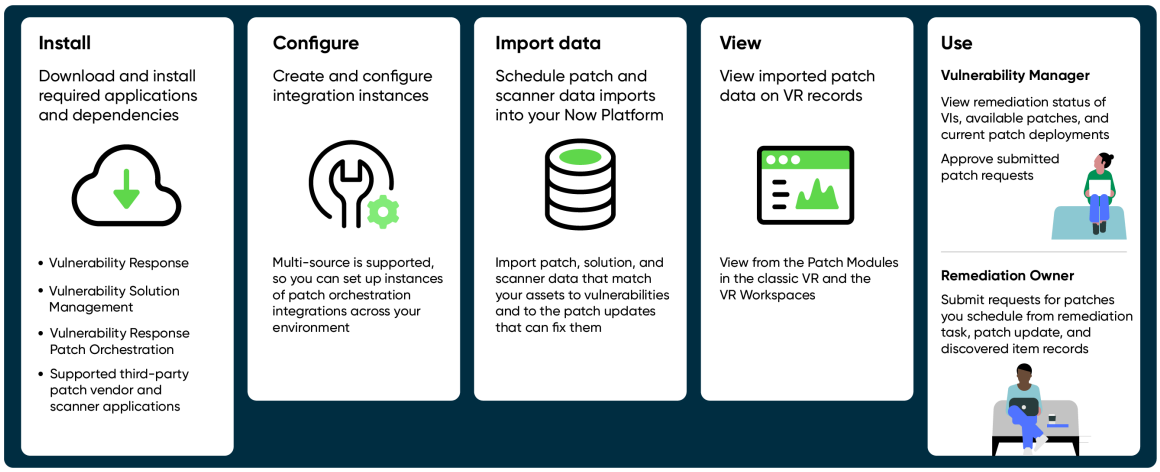
Patch-Orchestrierung mit Vulnerability Response

Sie können Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen Ihrer Assets mit -Patch-Orchestrierung mit Vulnerability Responseverwalten. Vulnerability Response Patch Orchestration und die Patch Orchestration Integrationen sind unter ServiceNow® Storeverfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Patch-Orchestrierung mit verstehen Vulnerability Response

Bei der Patch-Orchestrierung mit Vulnerability Response werden Daten aus geplanten Importen von Lösungsintegrationen von Drittanbietern, Patch-Lieferanten und Schwachstellen-Scannern verwendet. Diese Daten werden in der Anwendung Vulnerability Response korreliert. Mit dieser Datenorganisation können Sie die Schritte des Korrekturzyklus für Schwachstellen abschließen. Beginnen Sie mit der Identifizierung von Schwachstellen, wenden Sie dann Patches und Updates an, und schließen Sie schließlich angreifbare Elemente mithilfe von Scannerdaten von Drittanbietern – alles aus Ihrer Instanz Now Platform®.



Die Patch-Orchestrierung mit Vulnerability Response wird sowohl in der klassischen Umgebung als auch in den Arbeitsbereichen Vulnerability Response unterstützt.

Informationen zur Patch-Orchestrierung in den Arbeitsbereichen finden Sie unter Patchen Sie die Orchestrierung mit den -Arbeitsbereichen Vulnerability Response ..

Mit der Patch-Orchestrierung in Vulnerability Responsekönnen Schwachstellenmanager, Analysten und IT-Korrekturspezialisten die folgenden Korrekturaufgaben ausführen:

- Sehen Sie sich weiteren Kontext und Informationen zu den Arten von Patches und den Lieferanten an, aus denen ihre Lösungen bestehen (Patches).
- In den -Arbeitsbereichen Vulnerability Response oder in der klassischen Umgebung können Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Nachbesserung von Schwachstellen aus Datensätzen anzeigen und überwachen.
- Stellen Sie Patches, die von Drittpartei-Lösungsanbietern unterstützt werden, für deren Windows, CentOS, macOS, Oracleund andere Assets in regelmäßigen, geplanten Intervallen bereit. Sie können Patches außerhalb der Geschäftszeiten planen, um Konflikte mit Mitarbeitern bei der Arbeit zu vermeiden.
- Verwenden Sie importierte Erkennungsdaten, die von Drittanbieterscannern bereitgestellt werden, um Assets zu identifizieren, die Schwachstellen aufweisen und nicht gepatcht wurden oder durch geplante Patches nicht erfolgreich aktualisiert wurden.
- Initiieren und planen Sie verfügbare Patches für Assets, für die Updates von Patch-Updates, Korrekturaufgaben und erkannten Elementdatensätzen in der Anwendung Vulnerability Response erforderlich sind.
- Überwachen Sie Patch-Bereitstellungen mit einem optionalen Genehmigungsprozess für Patch-Anforderungen, die von Ihren Korrekturspezialisten übermittelt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtige Begriffe

Konfigurationselement bzw. Configuration Item (CI)

CIs sind die vorhandenen Assets, die in Ihrer Configuration Management Database (CMDB) aufgeführt sind.

Angreifbares Element (VI)

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht. Angreifbare Elemente (VITs) werden nach bestimmten Kriterien, die Korrekturaktionen für VIs angeben, in Korrekturaufgaben oder Listen gruppiert.

Instanz

Bezieht sich auf einen eindeutigen Account einer Lösungsanbieteranwendung. Beispielsweise kann jeder Benutzeraccount eine Instanz in der Anwendung HCL BigFix sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für eine Instanz Now Platform®.

Lösung

Im Kontext dieser Integration gibt es zwei Arten von Lösungen: potenzielle und bevorzugte. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben kann. Schwachstellen haben oft viele potenzielle Lösungen. Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte, erkannte Schwachstelle.

Patch

Software-Updates, die Schwachstellen beheben. Patch-Lieferanten verwenden ihre eigenen Namen für Patches, z. B. In der Anwendung HCL BigFix werden Patches als Fixlets bezeichnet.

Bevorzugter Patch

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Sobald Patches bereitgestellt wurden, werden sie den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und beheben sie.

Bereitstellung

Für die Zwecke dieser Integration bedeutet Bereitstellung, wenn Sie einen Patch auf einen Computer anwenden, initiieren oder planen.

Die Bereitstellung in Now Platform kann sich auch auf eine Integration beziehen, die mehrere Quellen unterstützt. Das Vorhandensein einer einzelnen Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie in Ihrer Umgebung über mehrere Bereitstellungen eines Drittanbieter-Scanners oder einer Lösungsanbieter-Integration verfügen.

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

- Die Anwendung Vulnerability Response und die Abhängigkeits-Plugins „Security Support Common“ und „Security Support Orchestration“.
- Vulnerability Solution Management.
- Vulnerability Response Patch Orchestration-Anwendung verfügbar in ServiceNow® Store.
- Eine unterstützte Patch-Lieferantenanwendung einer Drittpartei, z. B. „The Vulnerability Response Patch Orchestration Integration with HCL BigFix“ oder „The Vulnerability Response Patch Orchestration Integration with Microsoft SCCM“.
- Unterstützte Scanner-Integrationen von Drittanbietern mit Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rollen

Benutzer benötigen Rollen, die für die Patch-Orchestration-Integration spezifisch sind, die Sie verwenden, um in der Anwendung Vulnerability Response Daten anzuzeigen und Patches zu planen. Weitere Informationen finden Sie in den Konfigurationsinformationen für die unten aufgeführten unterstützten Integrationen, die Sie verwenden.

- Informationen zur Integration der HCL BigFix Patch Orchestration in mit Vulnerability Response und Integration der Vulnerability Response Patch Orchestration mit Microsoft SCCM.
- In den Arbeitsbereichen Vulnerability Response und in der klassischen Umgebung wird die Rolle sn_vul_patch_orch.read_patch, mit der Benutzer Daten anzeigen, aber nicht bearbeiten können, von den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt.

  Die Rollen, die Sie zum Konfigurieren der Verbindungen zu den Patch-Anbietern und zum Planen von Patches zuweisen müssen, sind integrationsspezifisch. Weitere Informationen finden Sie unter Konfigurieren Sie die Integration der Patch-Orchestration-Integration Vulnerability Response mit HCL BigFix und Vulnerability Response Patch Orchestration mit MS SCCM konfigurieren.

Es gibt einen Übermittlungs- und Genehmigungsprozess für Patch-Anforderungen, die in den Anwendungen enthalten sind. Standardmäßig ist in der Anwendung Vulnerability Response Patch Orchestration in Ihrer Instanz Now Platform eine Systemeigenschaft aktiviert [**sn_vul_patch_orch.patch_approval_required**].

Diese Systemeigenschaft ist aktiviert, sodass geplante Patch-Bereitstellungen zur Überprüfung und Genehmigung an Benutzer übermittelt werden, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind. Wenn Sie möchten, dass Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Genehmigung planen, können Sie die Eigenschaft [**sn_vul_patch_orch.patch_approval_required**] deaktivieren. Möglicherweise möchten Sie Genehmigungen aktiviert lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen. Wenn Sie die Systemeigenschaft „Genehmigung“ deaktivieren, kann jeder Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

Weitere Informationen und Anleitungen zum Deaktivieren dieser Systemeigenschaft finden Sie im Konfigurationsthema für Ihre unterstützte Integration.

- Konfigurieren Sie die Integration der Patch-Orchestration-Integration Vulnerability Response mit HCL BigFix.
- Konfigurieren Sie die Integration von Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM.

Planen Sie Patches aus Vulnerability Response -Datensätzen

Korrekturspezialisten können Patch-Updates zur Behebung angreifbarer Elemente planen und den Korrekturfortschritt von Datensätzen in der Anwendung Vulnerability Response aus überwachen.

Sie können Patches von den folgenden Datensätzen aus planen:

- Patch-Update
- Nachbesserungsaufgabe
- Erkanntes Element

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze, die die Anzahl aktiver AEs in zusammenfassen Vulnerability Response

Um potenzielle Leistungsprobleme beim Aufrollen aller Patches für alle Schwachstellen zu vermeiden, ändert die geplante Aufgabe, die Änderungen aufnimmt, nur die Anzahl der aktiven VIs. Für diese Anzahländerungen und zugehörigen Daten wird ein Rollup für die folgenden Datensätze in der Anwendung Vulnerability Response durchgeführt:

- VIT (angreifbares Element)
- RT (Korrekturaufgabe)
- Schwachstellenlösung
- Patch-Update

Weitere Informationen zum Anzeigen von Patch-Daten und zum Anzeigen von Patch-Daten in Datensätzen sowie zum Anzeigen von Patches ohne Lösungen finden Sie in den folgenden Themen.

- Patchen Sie Daten und Status-Rollup für die Patch-Orchestrierung in Vulnerability Response.
- Anzeigen von Patch-Daten und Planen von Patches in Vulnerability Response.
- Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Massenbearbeitung von angreifbaren Elementen mit Patches

Sie können angreifbare Elemente in der klassischen Umgebung, die Patches aus der klassischen Umgebung enthalten, massenweise bearbeiten. Weitere Informationen zur Funktionsweise der Massenbearbeitung finden Sie unter Führen Sie eine Massenbearbeitung von angreifbaren Elementen in durch Vulnerability Response. Die bevorzugten Patches für alle für die Massenbearbeitung ausgewählten VIs. Diese Bearbeitungsoption funktioniert nur, wenn allen ausgewählten VIs bevorzugte Patches zugeordnet sind.

Übersicht über Ausnahmeverwaltung

Wenn Ihre Organisation eine veröffentlichte Richtlinie, einen Standard oder eine Leitlinie für das Schwachstellenmanagement oder die Sicherheit nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT), die nicht gemäß der Richtlinie behoben werden können.

Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen anerkennen und ihnen zustimmen, wenn die Schwachstelle nicht behoben wird.

Lebenszyklus einer Ausnahme

Definition einer Ausnahme

Eine Ausnahme ist eine Anforderung, die Nachbesserung eines VI oder RT für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Ausnahme wird angefordert

Als Korrekturbesitzer können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für ein VI oder RT beantragen. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wechselt das AE oder RT in den Status „ **Zurückgestellt“**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Ausnahmeanforderung wird genehmigt

VIs oder RTs, die nicht sofort behoben werden können, werden von Schwachstellenanalysten überprüft, auf Risiken geprüft und zur Zurückstellung genehmigt, bis sie behoben werden können. Das Genehmigen einer Ausnahmeanforderung kann ein zweistufiger Workflow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger hinzu.

Hinweis:

- Ab Vulnerability Response v15.0 wird der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert, wenn Sie die VR-Anwendung zum ersten Mal bereitstellen. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

  Sobald eine Ausnahmeanforderung für ein AE oder RT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

  - Erneut öffnen
  - Löschen
  - Aktualisieren Sie das Feld **Zuweisung an** oder **Zuweisungsgruppen**
- Ab v23.0 von Vulnerability Responseist der Workflow **„Genehmigung des Ausnahmeregelstatus“** veraltet und wird durch den Flow „Genehmigung einer Ausnahmeregel“ im Flow Designer ersetzt.

Verfolgen Sie eine Ausnahmeanforderung

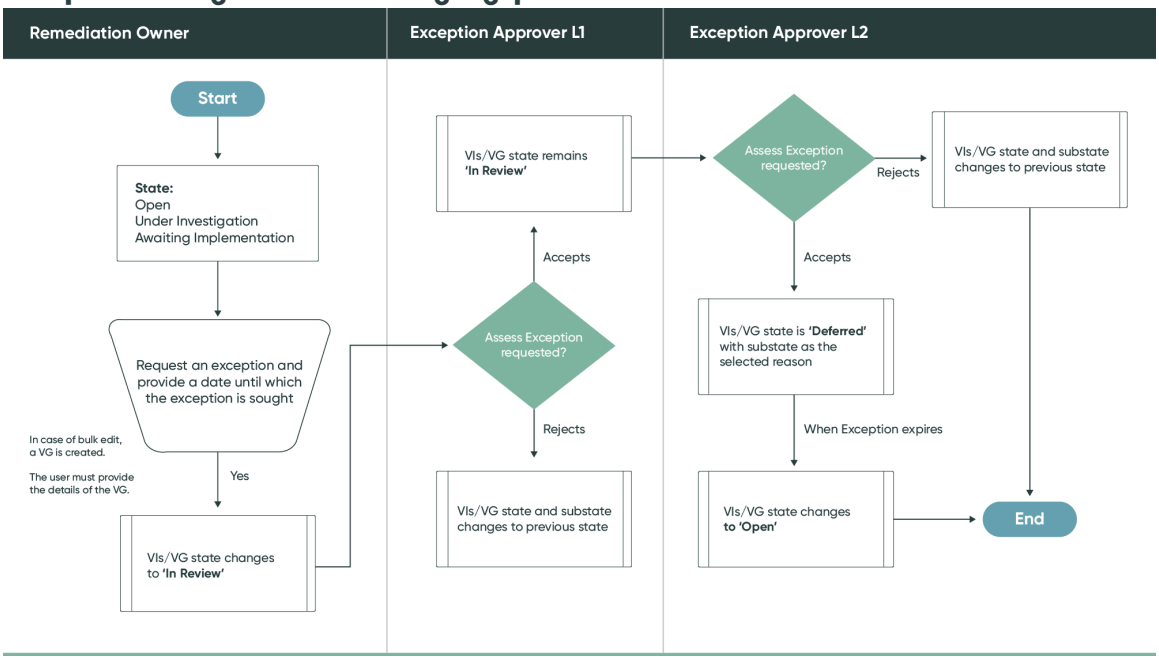
Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status mithilfe der Registerkarte **Change-Genehmigungen** im VI oder RT nachverfolgen. Wenn eine Aktion für eine RT ausgeführt wird, können Sie den Status der einzelnen AEs in dieser RT nicht nachverfolgen.

Ablauf einer Ausnahmeanforderung

Wenn eine Ausnahmeanforderung für ein bestimmtes VI oder RT abläuft, wird das betroffene VI oder RT in den Status **„Offen“** versetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Exception Management-Genehmigungsprozess vor VR v15.0



Wenn ein einzelnes VI oder alle VIs in einem RT den nächsten Scan bestehen, ändern sich die VIs und gegebenenfalls das Feld RT- **Status** in **Geschlossen** mit dem Substatus **Fest**.

Mehrere Zurückstellungen

Verfolgen Sie, wie oft ein Datensatz oder eine Korrekturaufgabe zurückgestellt wurde. Die regelmäßige Aufgabe `set deferral counts` wird täglich ausgeführt, um die Anzahl der Datensätze zu erfassen, die in der Spalte Anzahl der Zurückstellungen im Modul Mehrere Zurückstellungen für VR mehr als einmal zurückgestellt wurden. Alle Anzahlen für Datensätze, die einer Korrekturaufgabe zugeordnet sind, werden gesammelt und veröffentlicht, wenn eine Korrekturaufgabe mehr als einmal zurückgestellt wird.

Zugehörige Informationen

Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace

Fordern Sie eine Ausnahme in an IT Remediation Workspace

Ausnahme anfordern mit GRC: Richtlinien- und Compliance-Management in IT Remediation Workspace

Übersicht über Ausnahmeregeln

Mit Ausnahmeregeln für Vulnerability Response können Sie den Zurückstellungsprozess für angreifbare Elemente (VIs) automatisieren. Fordern Sie eine Ausnahme für die angreifbaren Elemente (VIs) an, die nicht sofort behoben oder zurückgestellt werden können, indem Sie die betroffenen Schwachstellen, Konfigurationselemente (CIs) oder VIs identifizieren. Übereinstimmende VIs basierend auf der Regel zurückstellen, wenn das System sie durch Automatisierung des VI-Zurückstellungsprozesses identifiziert

Es werden Ausnahmeregeln in Ihrer Organisation verwendet

Verwenden Sie Ausnahmeregeln, um neue und vorhandene VIs automatisch für einen bestimmten Zeitraum zurückzustellen, wenn sie der genehmigten Regelbedingung entsprechen. Die Automatisierung minimiert das Risiko des Fehlens von Servicelevel-Vereinbarungen und erleichtert die Verwaltung mehrerer Elemente, da manuelle Eingriffe entfallen.

Zurückstellungsregeln unterstützen die Reihenfolge, d. h. die Regel mit der höchsten Priorität wird zuerst ausgeführt. Wenn eine Regel mit hoher Priorität auf ein AE

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angewendet wird, werden nachfolgende Regeln nicht erneut darauf angewendet, auch wenn die Bedingung mit dem AE übereinstimmt.

Hinweis:

- Sie können Regeln nur erstellen, wenn Sie in der Konfiguration der Ausnahmeverwaltung Vulnerability Response auswählen. Details finden Sie unter Konfigurieren Sie die Ausnahmeverwaltung für Vulnerability Response.
- Wenn AEs von einer Ausnahmeregel zurückgestellt werden, werden sie in die neu erstellte Korrekturaufgabe für die Zurückstellung kopiert. Die VIs sind weiterhin Teil der RTs, zu denen sie zuvor gehörten.

Der Lebenszyklus einer Ausnahmeregel sieht wie folgt aus:

- Erstellen einer Ausnahmeregel
- Die Anforderung einer Ausnahmeregel wird genehmigt
- Ausnahmeregel aktivieren
- Eine Ausnahmeregel wird zurückgestellt
- Ablauf einer Ausnahmeregel

Erstellen einer Ausnahmeregel

Sie können eine Ausnahmeregel erstellen, um die AEs, die den definierten Bedingungen entsprechen, automatisch für den angegebenen Zeitraum zurückzustellen. Nachdem Sie eine Ausnahmeregel erstellt haben, senden Sie sie zur Genehmigung.

Die Anforderung einer Ausnahmeregel wird genehmigt

Das Genehmigen einer Ausnahmeregelanforderung ist ein zweistufiger Prozess. Wenn nur der Genehmiger der ersten Ebene vorhanden ist, kann die Ausnahmeregel durch eine einzige Genehmigung bewertet und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann die Genehmigung einer Ausnahmeregel nicht genehmigt werden. Nachdem die Regel genehmigt wurde, wird eine Korrekturaufgabe (Remediation Task, RT) erstellt. Weitere Informationen finden Sie unter Antrag auf Ausnahmeregel genehmigen.

Hinweis:

Ab Vulnerability Response v15.0 wird der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert, wenn Sie die VR-Anwendung zum ersten Mal bereitstellen. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Nachdem die Anforderung einer Ausnahmeregel genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Abbrechen
- Löschen

Ausnahmeregel aktivieren

Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe im Status „Zurückgestellt“ erstellt. Ab dem Datum „Gültig ab“ wird die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausnahmeregel für alle VIs ausgeführt, die erstellt werden, und auch für diejenigen, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden.

Hinweis:
Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wird am „Gültig ab“-Datum einmalig eine geplante Aufgabe für die vorhandenen Daten ausgeführt.

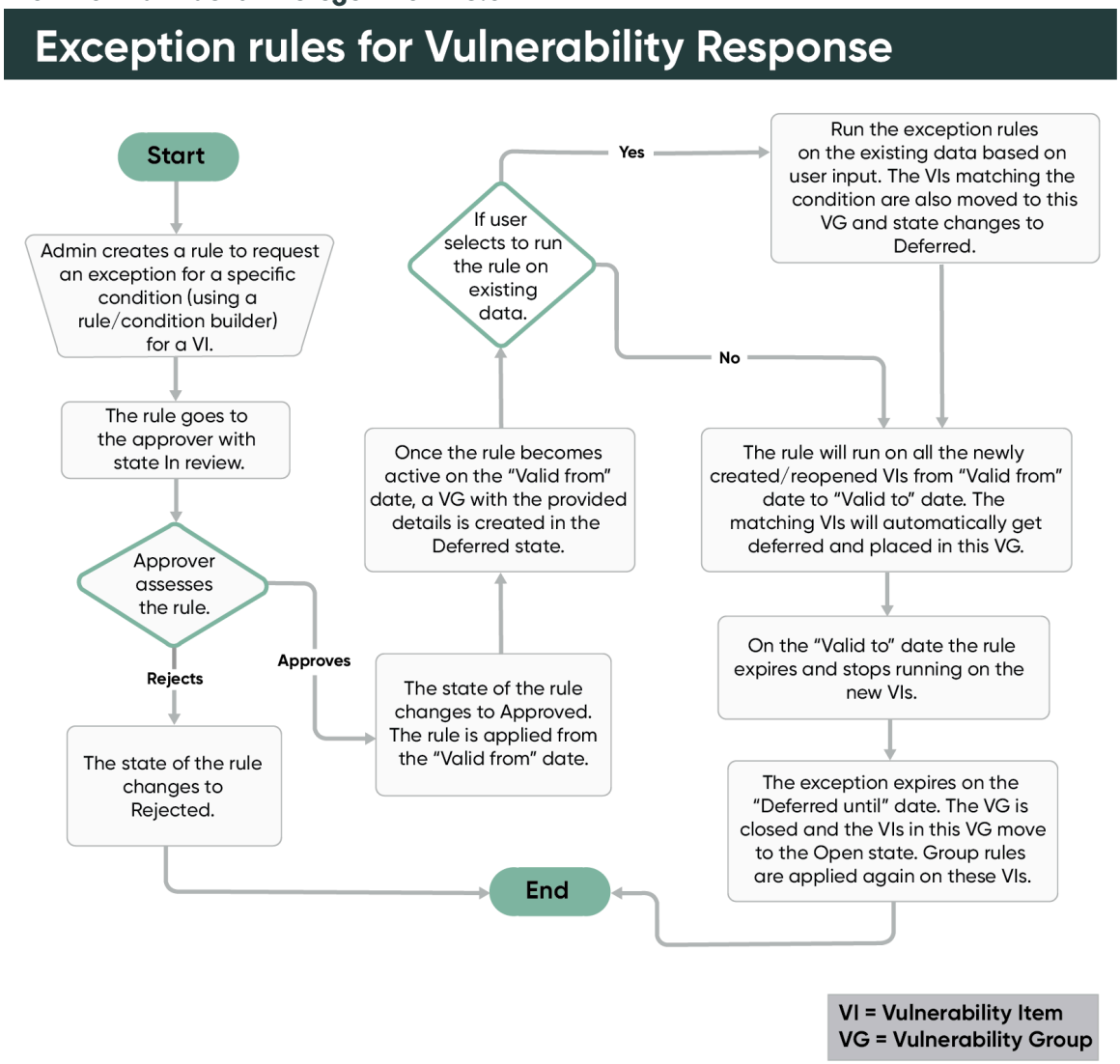
Eine Ausnahmeregel wird zurückgestellt

Sie können AEs, die den in dieser Ausnahmeregel definierten Bedingungen entsprechen, bis zu dem für die Regel definierten Datum „Zurückgestellt bis“ zurückstellen. An diesem Datum wird die Korrekturaufgabe geschlossen, die Sie für die Ausnahmeregel erstellt haben, und alle AEs in dieser Gruppe kehren in den Status „Offen“ zurück. Gruppenregeln werden erneut auf sie angewendet, um sie den erforderlichen RTs zuzuweisen.

Ablauf einer Ausnahmeregel

Nachdem die Ausnahmeregel abgelaufen ist, wird sie für neue oder erneut geöffnete VIs nicht mehr ausgeführt. Das zugeordnete RT bleibt bis zum Datum „Zurückgestellt bis“ im Status „Zurückgestellt“.

Workflow für Ausnahmeregeln vor v15.0



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über Ausschlussregeln

Ausschlussregeln bieten eine Möglichkeit, Erkennungen zu filtern oder von der Umwandlung in angreifbare Elemente (VITs) während des Erfassungsprozesses in Vulnerability Responseauszuschließen.

Diese Regeln können für verschiedene Szenarien eingerichtet werden, z. B.:

- Schwachstellen mit niedrigem Schweregrad oder Risiko, die keine sofortige Korrektur erfordern, werden ausgeschlossen.
- Verbesserung des Nachbesserungsprozesses durch Priorisierung der kritischsten VITs für Maßnahmen.
- Reduzieren der Verarbeitungszeit während des Datenimports durch Ausschließen eines Prozentsatzes der Erkennungen von der VIT-Konvertierung.

Während des Prozesses der Datenerfassung gibt es unterschiedliche Ansätze für den Umgang mit neuen und vorhandenen Erkennungen.

- Für neue Erkennungen:
  - Wenn eine neue Erkennung die Bedingungen einer Ausschlussregel nicht erfüllt, wird mit den VITs eine Erkennung erstellt.
  - Wenn eine neue Erkennung die Bedingungen einer Ausschlussregel erfüllt, wird die Regel mit der Erkennung verknüpft, es wird jedoch keine VIT erstellt. Füllen Sie die entsprechende Ausschlussregelreferenz im Erkennungsdatensatz aus. Die Spalte „Ausschlussregel“ wird im Erkennungsdatensatz entsprechend mit der Referenz zur Ausschlussregel gefüllt.
- Für vorhandene Erkennungen:
  - Wenn die Erkennung die Bedingungen einer Ausschlussregel nicht erfüllt, wird der normale Workflow fortgesetzt.
  - Wenn eine vorhandene Erkennung mit den Bedingungen einer Ausschlussregel übereinstimmt, behält die dieser Erkennung zugeordnete VIT ihren aktuellen Status bei, die Regel wird jedoch der Erkennung zugeordnet.
    Der Status der VIT wird durch den Wert gesteuert, der in der Eigenschaft `sn_vul.close_vit_with_excluded_detections` definiert ist. Standardmäßig ist der Wert in dieser Eigenschaft auf False festgelegt. Wenn der Wert auf „Falsch“ festgelegt ist, werden die Erkennungen unter einer VIT ausgeschlossen, und der Status der VITs bleibt im aktuellen Status. Wenn der Wert jedoch auf true festgelegt ist, können die folgenden Szenarien eintreten:
    - Wenn jede Erkennung unter einer VIT ausgeschlossen wird, wird der Status der VIT auf Geschlossen (excluded) aktualisiert.

      Hinweis:
      Ab v22.1.2 von Vulnerability Response wurde ein neuer Substatus namens „Ausgeschlossen“ hinzugefügt,

    - Wenn eine Erkennung als Geschlossen markiert wird, während die verbleibenden ausgeschlossen werden, wird die VIT als Geschlossen – Fest festgelegt.
    - Wenn für die VIT offene Erkennungen vorliegen, bleibt die VIT im Status Offen.

Zugehörige Informationen

Erstellen Sie eine Ausschlussregel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Falsch positiv – Übersicht

Ein falsch positives Ergebnis ist ein Zustand, bei dem der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, in Tatsächlich jedoch keine Schwachstelle vorliegt. Dafür kann es mehrere Gründe geben, z. B. falsche Klassifizierung, falsche Logik oder falscher Algorithmus im Scanner. Der für die Korrektur Verantwortliche kann angreifbare Elemente (VIs) oder Korrekturaufgaben (RTs) als falsch positive Meldungen kennzeichnen.

Wichtig:
Sie können die angreifbaren Host-Elemente in einem Massenvorgang in Vulnerability Manager Workspaceals falsch positiv markieren. Weitere Informationen dazu, wie Sie angreifbare Host-Elemente massenweise als falsch positiv kennzeichnen, finden Sie unter Massenbearbeitung für falsch positive Werte im Arbeitsbereich des Schwachstellenmanagers.

Lebenszyklus eines falsch positiven Elements

Bedeutung von „falsch positiv“.

Der Scanner gibt manchmal eine Warnung aus, wenn in Tatsächlich keine Schwachstelle vorliegt. Wenn beispielsweise ein Configuration Item außer Betrieb genommen wurde, der Scanner jedoch immer noch ein damit zusammenhängendes Problem auslöst, markieren Sie es als falsch positiv.

wird als falsch positiv markiert

Weitere Informationen zum Markieren eines VI oder RT als falsch positiv finden Sie unter Als falsch positiv markieren.

Mit dem falsch positiven arbeiten

Sobald ein VI oder RT als falsch positiv markiert ist, wird der Status in Geschlossen aktualisiert und der Substatus in Falsch positiv geändert. Die folgenden Aktionen können ausgeführt werden:

- Erneut öffnen
- Löschen
- Aktualisieren Sie das Datum im Feld **Bis**. Dieses Datum wird dann als Ablaufdatum für das falsch positive Ergebnis verwendet.

Hinweis:
Wenn die Genehmigung nicht erfolgt, wird der VI oder RT in den vorherigen Status zurückversetzt.

Falsch positives Ergebnis wird genehmigt

Der Genehmiger kann das falsch positive Ergebnis in seinem Genehmigungs-Workflow genehmigen.

Hinweis:

Ab Vulnerability Response v15.0 wird der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert, wenn Sie die VR-Anwendung zum ersten Mal bereitstellen. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Falsch positives Element wird erneut geöffnet

Ein VI oder RT in einem falsch positiven Substatus kann jederzeit erneut geöffnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Falsch positives Ergebnis wird nachverfolgt

Verwenden Sie den Abschnitt **„Statusänderungsgenehmigungen“,** um den Status der falsch positiven Meldungen nachzuverfolgen. Nach der Genehmigung wird der Status des VI oder RT auf „Geschlossen“ aktualisiert, und der Grund wird auf „Falsch positiv“ festgelegt.

Ablauf eines falsch positiven Werts

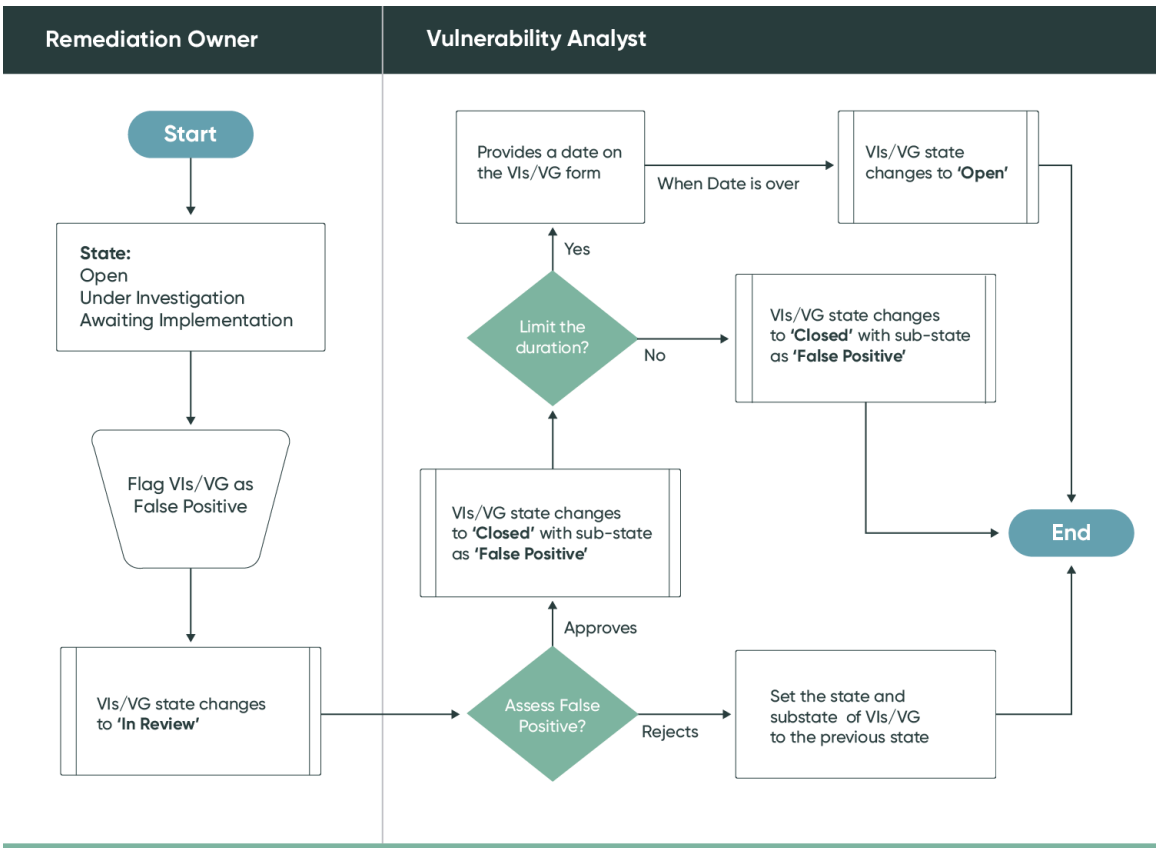
Nur der falsch positive Genehmiger kann ein Bis-Datum für das falsch positive Ergebnis festlegen, damit das VI oder RT abläuft. Außerdem können nur falsch positive Meldungen ablaufen, für die der Genehmiger ein Bis-Datum angegeben hat. Dieses Datum kann angegeben werden, nachdem das falsch positive Ergebnis genehmigt wurde.

Ein falsch positives Ergebnis ohne Bis-Datum ist ein dauerhaft falsch positives Ergebnis. Nachdem das falsch positive Feld abgelaufen ist, wird der Status des AE oder VR zurück in „Offen“ geändert.

Hinweis:

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Falsch positiver Genehmigungsprozess vor v15.0



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Genehmigungsprozess erfolgt automatisch, wenn alle VIs den nächsten Scan bestehen. Die VIs werden unabhängig vom aktuellen Status automatisch geschlossen. Die Felder AEs oder, falls zutreffend, RT **State** ändern sich in **Geschlossen** mit dem Substatus **Fest.**

Weitere Informationen finden Sie unter Falsch positives Ergebnis wird markiert und genehmigt.

Zugehörige Informationen

Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an

Watchdog für Vulnerability Response

Der Watchdog wird verwendet, um Tabellen basierend auf den von Ihnen angegebenen Bedingungen nachzuverfolgen. Beispielsweise können damit Details zu Integrationsausführungsfehlern in Vulnerability Responseprotokolliert werden.

Sie können sich über diese Fehler benachrichtigen lassen. Basierend auf dieser Benachrichtigung können Sie die Remediation planen. Die Standard-Watchdogs sind:

- Integrationsausführung fehlgeschlagen: Wenn der Status der Integrationsausführung auf Abgeschlossen und der Substatus auf Fehlgeschlagen festgelegt sind, werden Benutzer und Benutzergruppen benachrichtigt, wenn die Bedingung eine Anzahl größer als 0 zurückgibt, die Integrationsausführung also fehlschlägt.
- Integrationen mit langer Ausführungszeit: Skript, mit dem überprüft wird, ob die Integrationsausführung die festgelegte Zeit überschreitet. Dieser Watchdog benachrichtigt Sie proaktiv, wenn sich der Abschluss der Integrationsausführung verzögert.
- Überlappende regelmäßige Ausführungen: Skript zum Überprüfen der wiederkehrenden Integrationsausführungen, die während des bevorstehenden Vorkommens noch ausgeführt werden. Es generiert einen Link, der die Liste dieser Integrationen enthält.

Überwachungsprotokoll

Der Watchdog verfügt über ein Überwachungsprotokoll, das angibt, wie oft die Bedingung erfüllt wurde.

Übersichts-Dashboard

Verwenden Sie das Dashboard „Übersicht“, um den Watchdog in den letzten 30 Tagen zu überwachen. Sie können mehrere Widgets erstellen, um andere von Ihnen überwachte Watchdog-Themen nachzuverfolgen.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Bericht

Name	Beschreibung
WatchDog-Fehler der letzten 30 Tage	Alle Bedingungen wurden in den letzten 30 Tagen erfüllt.

Weitere Informationen finden Sie unter Konfigurieren Sie den Watchdog und Fehlerbehandlung für Erkennungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Change Management für Vulnerability Response

Als IT-Korrekturbesitzer können Sie Change-Anforderungen (CHG) direkt aus Korrekturaufgaben (RT) in der Anwendung Vulnerability Response erstellen und verwalten. Change-Anforderungen helfen Ihnen, Change-Aktivitäten für Ihre Assets zu initiieren und nachzuverfolgen, damit Sie Ihre Korrekturaufgaben und die entsprechenden angreifbaren Elemente korrigieren können.

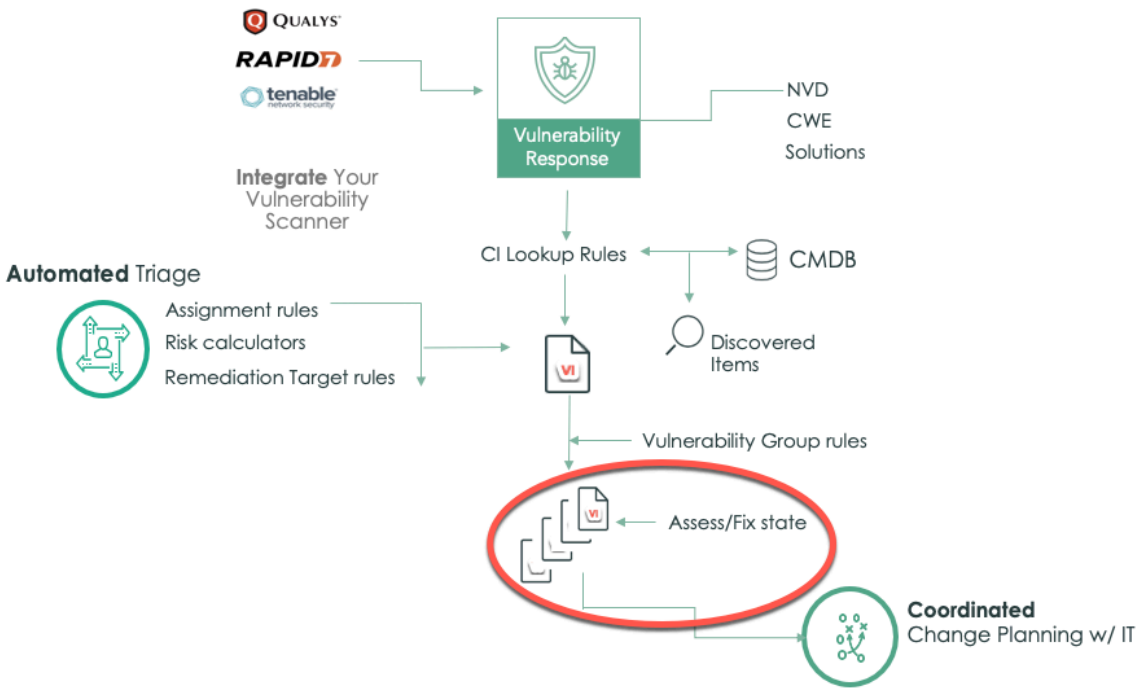
Change-Anforderungen und Schwachstellen-Workflow

Wenn Sie mit der Anwendung Vulnerability Response nicht vertraut sind, finden Sie weitere Informationen unter Die Anwendung Vulnerability Response erkunden.

Die folgende Abbildung zeigt den Informationsfluss für Vulnerability Response, von der Einrichtung der Integration (Scanner) über die automatisierte Selektierung bis hin zur Untersuchung.

Change-Anforderungen und Change-Management sind Teil des Nachbesserungsprozesses (Status „Bewerten“/„Korrektur“) im Workflow Vulnerability Response, der in der folgenden Abbildung dargestellt ist. In dieser Phase können Sie Change-Anforderungen verwenden, um die Nachbesserung von Schwachstellen zu initiieren und nachzuverfolgen. Sie können Change-Anforderungen direkt aus der Korrekturaufgabe erstellen und verwalten und Untersuchungs- und Korrekturaufgaben auflisten, die Lösungen für betroffene Assets für die Configuration Items (CI) in Ihrer CMDB enthalten.

Change-Anforderungen in Vulnerability Response



Wann Change-Anforderungen in Vulnerability Response verwendet werden sollen

Als IT-Korrekturbesitzer können Sie Change-Anforderungen aus einer Korrekturaufgabe erstellen, wenn ein manueller und kontrollierter Prozess jeglicher Art zum Ändern oder Entfernen von unterstützten Konfigurationselementen (Configuration Items, CI) in Ihrer CMDB erforderlich ist. Wenn Sie Change-Anforderungen direkt aus einem Korrekturaufgaben-Datensatz erstellen und verwalten, können Sie Schwachstellen schnell untersuchen und beheben. Die AEs einer gelösten Korrekturaufgabe können beim nächsten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

geplanten Scan in Ihrer Now Platform gescannt und verifiziert und an die automatisierte Selektierung des Workflows Vulnerability Response zurückgegeben werden. Zu den manuellen Eingriffen, die möglicherweise Change-Anforderungen erfordern, gehören beispielsweise die folgenden:

- Ein Software-Patch, eine Korrektur oder eine andere Aufgabe der IT, die für angreifbare Elemente vor der RT-Lösung erforderlich ist.
- Sie stellen fest, dass eine Teilmenge der angreifbaren Elemente in einer Korrekturaufgabe weitere Untersuchungen oder eine Neuzuweisung an eine andere Abteilung erfordert.
- Sie bestimmen, dass eine Teilmenge angreifbarer Elemente in einer RT mit einer großen Anzahl angreifbarer Elemente in eine neue Korrekturaufgabe verschoben werden kann.
- Sie können einer vorhandenen Change-Anforderung eine Korrekturaufgabe zuordnen, um die Duplizierung von Korrekturaufgaben zu vermeiden.

Arten von Change-Anforderungen für ein RT

Die Anwendung Vulnerability Response nutzt die drei Arten von Service-Changes, die vom Produkt ITSM Change-Management in Ihrer Instanz Now Platform® unterstützt werden – Standard, Notfall und Normal. Die Art des Change, den Sie auswählen, bestimmt, welches Statusmodell aufgerufen wird und welcher Change-Prozess befolgt werden muss. Change-Anforderungen erfassen die detaillierten Informationen über den Change, z. B. den Grund, die Priorität, das Risiko, den Typ und die Kategorie des Change. Siehe Change-Typen .

Als Vulnerability Response IT-Korrekturbesitzer haben Sie die folgenden Möglichkeiten, um normale, standardmäßige und Notfall-Change-Anforderungen direkt aus einer Korrekturaufgabe zu erstellen:

- Sie können Change-Anforderungen erstellen, die vorab ausgefüllte Informationen aus der Korrekturaufgabe enthalten, um den Prozess zu optimieren und Zeit zu sparen.
- Sie können einer vorhandenen Change-Anforderung eine Korrekturaufgabe zuordnen, um zu vermeiden, dass Change-Anforderungen doppelte Change-Anforderungen erstellen, die ähnliche Informationen und angreifbare Elemente gemeinsam nutzen.
- Mithilfe einer Reihe von Bedingungen können Sie eine Teilmenge angreifbarer Elemente herausfiltern und eine Korrekturaufgabe aufteilen. Die von Ihnen ausgewählten Elemente werden automatisch in ein neues RT verschoben.

Sie können angreifbare Elemente anhand von Werten aus beliebigen Feldern einer Korrekturaufgabe filtern und die Change-Anforderung nur auf diejenigen Elemente anwenden, die Ihren Filterkriterien entsprechen.

Zugehörige Informationen

Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Teilen Sie eine Korrekturaufgabe auf

Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

Bewertung des Gefahrenpotenzials von Software mit Software Asset Management (SAM Foundation)

Verwenden Sie die Anwendung ServiceNow® Schwachstellenbewertung Bewertung des Gefahrenpotenzials, um die Gesamtanzahl der installierten Software für ein bestimmtes Softwarepaket in Ihren Assets zu bestimmen. Bei Verwendung mit der Anwendung ServiceNow® Software Asset Management (SAM) Foundation können Sie Ihre Gefährdung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bewerten, angreifbare Elemente erstellen und die Nachbesserung für die erkannte angreifbare Software verwalten.

Wichtig:
Sie können die Bewertung des Gefahrenpotenzials nach Common Vulnerabilities and Exposures (CVE) und Software durchführen, um die zusätzlichen Funktionen im Arbeitsbereich für die Schwachstellenbewertung zu nutzen. Weitere Informationen finden Sie unter Erkunden Sie den Arbeitsbereich der Schwachstellenbewertung.

Bestimmen Sie Ihr Risiko für angreifbare Software, indem Sie die angreifbaren Softwareinformationen (Herausgeber, Produkt, Edition und Version) angeben, ohne die Common Vulnerabilities and Exposures-Datenbank (CVE) zu verwenden. Bewerten Sie Fälle von Zero-Day-Schwachstellen (aktueller Tag) für Software für die folgenden Fälle:

- Wenn für Produkte noch keine CVE-Daten vorliegen.
- Wenn eine Verzögerung zwischen dem Zeitpunkt besteht, zu dem eine Schwachstelle öffentlich bekannt wird, und der Aktualisierung der CVE-Daten mit der Schwachstelle im NVD.
- Wenn Sie zwischen den geplanten Prüfungen Ihres Schwachstellenscanners etwas über die Schwachstelle erfahren.

Mit der Anwendung Bewertung des Schwachstellenrisikos können Sie, wenn Sie den Herausgeber und das Produkt der angreifbaren Software kennen, anhand der Datensätze, die die in Ihrem Netzwerk installierte Software auflisten, die von der Anwendung SAM Foundation erstellt wurde, Ihr Risiko für potenziell schädliche Software einschätzen Pakete bei Bedarf.

Wenn Sie das Ausmaß Ihres Gefahrenpotenzials für diese Art von Schwachstelle kennen, können Sie proaktiv reagieren, indem Sie eine rote Warnung implementieren und die Software deinstallieren oder Ihr Security Operations Center (SOC) informieren, dass nach einem bestimmten Patch gesucht werden soll. Sie können angreifbare Elemente erstellen und dem Korrekturspezialisten Aufgaben zur weiteren Korrektur der Untersuchung zuweisen. Zeigen Sie die Liste der Korrekturaufgaben (VUL) an, um sicherzustellen, dass die gewünschten angreifbaren Elemente erstellt und der VUL ordnungsgemäß zugeordnet wurden.

Zugehörige Informationen

Konfigurieren Sie die Bewertung des Gefahrenpotenzials für Schwachstelle .

Bewerten Sie Ihre Gefährdung durch angreifbare Software

Schwachstellen-Krisenmanagement

Erstellen und verfolgen Sie kritische Schwachstellenereignisse mithilfe des VCM-Workflows (Vulnerability Crisis Management). Erstellen Sie Schwachstellenbewertungsdatensätze, erfassen Sie Schlüsselattribute der Schwachstelle, um das Risiko zu berechnen, führen Sie Bewertungen durch, um das Gefahrenpotenzial zu identifizieren, und beziehen Sie Stakeholder ein, um eine koordinierte und schnelle Reaktion auf Schwachstellen zu ermöglichen.

Verwalten von Schwachstellen-Krisenereignissen

Das Schwachstellen-Krisenmanagement ist ein vollständiger Workflow zur Behandlung von Schwachstellen-Krisenereignissen mit den folgenden Fähigkeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Identifizieren Sie angreifbare Konfigurationselemente effizient, indem Sie kritische Schwachstellen mit dem Softwareinstallationsbestand aus dem Bestand Software Asset Management und Software Bill of Materials (SBOM), vom Scanner gemeldeten Schwachstellen und Configuration Management Database (CMDB)korrelieren.
- Konvertieren Sie Bewertungsergebnisse zur Korrektur in angreifbare Elemente.
- Initiieren Sie einen schwerwiegenden Security Incident, um eine schnelle und koordinierte Reaktion auf die Bedrohung sicherzustellen.
- Interagieren Sie mit Teams im gesamten Unternehmen, und arbeiten Sie zusammen, um eine einheitliche Reaktion auf Schwachstellen zu ermöglichen.
- Stellen Sie funktionsübergreifenden Stakeholdern und beteiligten Teams regelmäßige Statusberichte bereit, um Transparenz und Kommunikation während der Krise aufrechtzuerhalten.

Vulnerability Crisis Management mit dem Arbeitsbereich für Schwachstellenbewertung

Hinweis:
Ab v1.0.1 von Vulnerability Crisis Management ist die Anwendung als separates Abonnement im Store verfügbar. Sie können vom Arbeitsbereich der Schwachstellenbewertung nur dann auf Vulnerability Crisis Management zugreifen, wenn Sie über eine differenzierte Berechtigung verfügen oder die Anwendung aus dem Store installiert haben. Zuvor war das Plugin „Vulnerability Emergency Response“ im Plugin „Vulnerability Emergency Response“ enthalten. Ab v3.2.2 wurde das Plugin „Vulnerability Emergency Response“ in Bewertung des Schwachstellenrisikos umbenannt.

Wird eine Schwachstelle von Interesse identifiziert, erstellt der Schwachstellenereignismanager einen Schwachstellenbewertungsdatensatz mit Informationen zur Threat Intelligence-Quelle, den Schwachstellenmerkmalen und den betroffenen Produkten. Diese Informationen werden für weitere Auswirkungs- und Risikoanalysen verwendet.

Nachdem der Datensatz für eine Schwachstelle von Interesse erstellt wurde, wird eine Risikobewertung durchgeführt. Diese Bewertung umfasst die strukturierte Risikobewertung, die Überprüfung des Datensatzes und die Beobachtungen des Analysten, der die Aufgabe ausführt. Die anfängliche Risikopunktzahl für eine Schwachstelle von Interesse wird anhand der Attribute berechnet, die zum Zeitpunkt der Ereigniserstellung verfügbar sind. Die Risikopunktzahl für die Bewertung kann sich ändern, wenn zusätzliche Informationen verfügbar werden. Verwenden Sie die Risikopunktzahl, um die potenziellen Auswirkungen der Ausnutzung zu bestimmen und Antwortprioritäten festzulegen.

Nachdem die Bewertung für eine relevante Schwachstelle erstellt und festgestellt wurde, dass ein Risiko für die Infrastruktur der Organisation darstellt, können Sie die Bedrohung weiter analysieren, indem Sie die Risikobewertung mit einer eingehenden Bewertung des Gefahrenpotenzials mit dem Softwareinstallationsbestand von Software Asset Management, Software Bill of Materials aktualisieren. (SBOM)-Bestand, vom Scanner gemeldete Schwachstellen und Configuration Management Database (CMDB). Betroffene Configuration Items und Anwendungen werden automatisch durch eine Bewertung identifiziert. Zusätzliche betroffene Elemente können manuell hinzugefügt werden.

Sobald die Bewertung abgeschlossen ist, können angreifbare Elemente oder angreifbare Anwendungselemente für die Gefahrenpotenzial-Ergebnisse erstellt werden, denen noch kein angreifbares Element zugeordnet ist. Der Risikopunktzahl-Rechner für angreifbare Elemente kann genutzt/konfiguriert werden, um die Risikopunktzahl für angreifbare Elemente anzupassen, die mit Datensätzen der Schwachstellenbewertung verknüpft sind. Dem Schwachstellenbewertungsdatensatz können die Gefährdungsstufe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und die Ereignispriorität zugewiesen werden. Je nach Ereignispriorität kann der Schwachstellenereignis-Manager die Schwachstellenbewertung mit einem schwerwiegenden Security Incident vorschlagen, heraufstufen oder verknüpfen.

Verwenden Sie Management schwerwiegender Sicherheits-Incidents, um Nachbesserungsaktivitäten nachzuverfolgen und zu verwalten, laufende Security Incidents zu verknüpfen, Ad-hoc-Aufgaben zu erstellen, betroffene Teams einzubeziehen, Statusberichte zu senden und mithilfe der in Management schwerwiegender Sicherheits-Incidentsverfügbaren Zusammenarbeitsintegrationen zusammenzuarbeiten.

ServiceNow® Software Asset Management und Software Bill of Materials (SBOM) Bewertungs-Verarbeitungslogik

Anhand der Daten Software Asset Management werden die von NVD für das CVE stammenden CPEs und anschließend die Discovery-Modelle mithilfe der Zeichenfolgen-Abgleichlogik abgerufen. Nach dem Abrufen der Discovery-Modelle wird ein Scan auf zugehörige Installationen ausgeführt, die zugehörigen Konfigurationselemente werden abgerufen und die Tabelle „Betroffene Konfigurationselemente“ ausgefüllt. Sie können weitere Details wie Herausgeber, Produkt, Version und Edition angeben. Basierend darauf werden alle übereinstimmenden Discovery-Modelle und die Softwareinstallationen für den Datensatz abgerufen. Anschließend werden die zugehörigen Configuration Items abgerufen und die Tabelle „Betroffene Configuration Items“ wird neu gefüllt.

Für SBOMwird die zugehörige Software für das CVE aus der zugehörigen (m2m)-Tabelle (zwischen CVE und Software) abgerufen. Nach dem Abrufen der Softwaredetails werden die zugehörigen SBOM-Komponenten identifiziert, indem das Produkt und die Version aus der SBOM-Komponente mit dem Produkt und der Version der identifizierten Software abgeglichen werden.

Nachdem die zugehörigen Komponenten gefunden wurden, werden die Entitäten abgerufen, die sich auf die Komponenten beziehen. Das Produktmodell aus den -Entitäten und das zugehörige CI (falls gefunden) werden abgerufen, und das Konfigurationselement wird in der Tabelle „Betroffene Konfigurationselemente“ gespeichert. Wenn das Konfigurationselement keine angreifbaren Elemente enthält, können Sie es zum Erstellen des angreifbaren Elements verwenden. Wenn kein Configuration Item gefunden wird, wird das Produktmodell in der Tabelle „Betroffene Softwaremodelle“ gespeichert und kann zum Erstellen angreifbarer Anwendungselemente verwendet werden.

Weitere Informationen zur Verwendung des Workflows „Schwachstellen-Krisenmanagement“ finden Sie unter Arbeitsbereich der Schwachstellenbewertung verwenden.

Zugehörige Informationen

Schwachstellenbewertung erkunden

Erkunden Sie den Arbeitsbereich der Schwachstellenbewertung

Registerkarte „Bewertung“.

Domain Separation und Vulnerability Response

Die Domänentrennung wird in Vulnerability Response unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Umfasst alle Aspekte des **Basis** -Supports.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Vulnerability Response

Mit Domain Separation können Sie VR-Verfahren (Vulnerability Response) für den gesamten Kundenstamm standardisieren, um die Betriebskosten zu senken und die Servicequalität zu erhöhen.

Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt sind und niemals für andere Clients verfügbar sind.

Unterstützung für Domain Separation in Vulnerability Response nach Versionsreleases

Release	Support-Stufe	Notizen
Orlando	Standard	
Paris	Standard	
Quebec	Standard	
Rom	Standard	
San Diego	Standard	
Tokio	Standard	
Utah	Standard	
Vancouver	Standard	
Washington DC	Standard	

Die Domänentrennung für die Anwendung Vulnerability Response deckt die folgenden Produktfunktionen ab:

- Erfasst die angreifbaren Elemente von Drittanbieterscannern (z. B. Qualys, Rapid 7 oder Tenable) in der richtigen Domäne. Die Daten werden in derselben Domäne erfasst wie der Integrationsbenutzer, dessen Anmeldeinformationen für die Integration verwendet werden.
- Scannt bestimmte Assets von Vulnerability Response in der Domäne, von der sie angefordert wurden, erneut.
- Verwendet den CMDB-CI-Suchprozess, um sicherzustellen, dass die CI-Informationen von den Scannern mit den CIs in CMDB der Domäne des Integrationsbenutzers übereinstimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Berechnet Risikopunktzahlen auf der Ebene des angreifbaren Elements gemäß dem Risikopunktzahl-Rechner, der in derselben Domäne wie der Integrationsbenutzer definiert ist.
- Korrekturzielregeln werden für angreifbare Elemente gemäß den Korrekturzielregeln ausgeführt, die in derselben Domäne wie der des Integrationsbenutzers definiert sind.
- Regeln für Korrekturaufgaben können in derselben Domäne wie die Domäne des Integrationsbenutzers definiert werden und bleiben.
- Korrekturaufgaben, die mit den Regeln für Korrekturaufgaben erstellt wurden, bleiben in derselben Domäne, in der die Gruppenregeln erstellt werden.
- Der Zurückstellungs-Workflow durchläuft den Genehmigungsprozess in derselben Domäne, für die die Zurückstellung angefordert wird.
- Berichte und Dashboards zeigen die Status der angreifbaren Elemente an, z. B. Alter des angreifbaren Elements, offene angreifbare Elemente nach CI, Schwachstellen nach Auswirkung und Status des Korrekturzieldatums in der Domäne, zu der es gehört.
- Wissen aus Scannern von Drittparteien oder der National Vulnerability Database (NVD) kann in der globalen Domäne erfasst werden, und Daten können von mehreren Clients gemeinsam genutzt werden.

Hinweis:
In allen oben genannten Fällen gelten die übergeordneten Prinzipien der Transparenz in getrennten Domänentrennung in der NOW Platform.

Weitere Informationen zum Erstellen und Unterstützen von domänengetrennten Importen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration und Erstellen und unterstützen Sie mehrere Domänen im Framework für Hintergrundaufträge.

Anwendungsfälle

Die Anwendung Vulnerability Response verwaltet den Lebenszyklus eines angreifbaren Elements durchgängig. Die folgenden Anwendungsfälle berücksichtigen die Domänentrennung:

- **Nehmen Sie** angreifbare Elemente (Schwachstellen in Asset) aus Ihrer Drittanbieterintegration auf.
  - Erfassen Sie Daten aus mehreren Instanzen
  - Deduplizieren Sie das angreifbare Element
  - Mit CMDB-CI abgleichen
- **Anreicherung** von angreifbaren Elementen mit Risikopunktzahlen und Korrekturzieldaten
  - Asset-Ergänzung (CMDB)
  - Ergänzung von Risikopunktzahl und Korrekturzieldatum
- **Gruppieren Sie** angreifbare Elemente, und weisen Sie die Korrekturaufgabe zu
  - Gruppiert automatisch die angreifbaren Elemente
  - Korrekturaufgabe automatisch zuweisen
- **Beheben**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Korrekturaufgaben
- Umfassender Korrekturlebenszyklus
- Zurückstellungs-Workflow

- **Messen Sie** die Sicherheitslage der Organisation und das Programm für Schwachstellenmanagement
  - Schwachstellen-Trend, angreifbarstes Asset, Schwachstelle nach Alter
  - Korrekturstatus nach Korrekturzieldatum

Setup

Das Einrichten von Domain Separation für Vulnerability Response erfordert keine zusätzlichen Schritte. Alle Vulnerability Response -Tabellen erwerben die Spalte „Domäne“, nachdem die Instanz domänengetrennt wurde. Sie können Importdaten von Schwachstellenintegrationen in bestimmte Domänen leiten. Weitere Informationen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration.

Domänengetrennte Daten

Daten können domänengetrennt sein. Das bedeutet:

- Das von Drittanbieterscannern erfasste angreifbare Element bleibt in derselben Domäne wie die Domäne des Integrationsbenutzers und ist von keiner anderen Domäne aus zugänglich.
- Schwachstellen, angreifbare Elemente (Instanzen) oder Assets in einer Domäne können nicht in anderen Domänen angezeigt werden.
- Der Risikobewertungsalgorithmus, die Korrekturaufgabenregeln und die Korrekturzielregeln können von niemandem außerhalb der Domäne angezeigt werden.
- Schwachstelleninformationen aus dem NVD können in der globalen Domäne vorhanden sein und für alle Kunden freigegeben werden.
- Korrekturaufgaben in einer Domäne können nicht in einer anderen Domäne angezeigt werden.
- Zurückstellungs-Workflows, die in einer Domäne erstellt wurden, sind in einer anderen Domäne nicht sichtbar.
- Alle E-Mail-Benachrichtigungen sind in der Domäne enthalten, zu der sie gehören.

Hinweis:

Die in der Instanz verfügbaren Vorlagen für geplante Importe sind standardmäßig auf „Domäne: global“ festgelegt. Um Konflikte zu vermeiden, wenn mehrere Domänen in Instanzen vorhanden sind, passen Sie die folgende Vorgehensweise an:

- Verteilen Sie die in der -Instanz verfügbaren Importvorlagen auf die Anzahl der an der Integration beteiligten Domänen.
- Aktualisieren Sie die Domäne des Importvorlagendatensatzes auf die sys_id der Zieldomäne.
- Erstellen Sie bei Bedarf Importvorlagen für jede Domäne.
- Stellen Sie sicher, dass jede Domäne über 2 Importvorlagen verfügt.
- sn_vul_sched_import_pool: Diese Tabellendatensätze sollten domänengetrennt sein, wenn Domain Separation in der Instanz vorhanden ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie Schwachstellenanalysten ihre eigenen Anwendungsdaten verwalten

- Analysten erstellen ihre eigenen Regeln für die Anwendungsinstallation, für die Verwaltung von Anwendungen mit mehreren Quellen und für die CI-Suche.
- Analysten können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Analysten können ihre eigenen Workflows für Zurückstellungen und Change-Management erstellen.
- Analysten können eigene Regeln für Korrekturaufgaben und Risikobewertungslogik erstellen, um Schwachstellen genau zu priorisieren, Korrekturaufgaben automatisch zuzuweisen und sie der richtigen Zuweisungsgruppe zuzuweisen.
- Domänenbenutzer erstellen ein manuelles angreifbares Element und schließen es dann.

Geschäftslogik und -prozesse, die nach Instanzbesitzern domänengetrennt werden können

- Vulnerability Response Benutzer und Gruppen
- Vulnerability Response-Integrationen
- Setupkonfiguration abschließen (Anwender- und Gruppenverwaltung, Anwendungsinstallation, Anwendungsverwaltung mit mehreren Quellen, CI-Suchregeln, Regeln für Korrekturaufgaben, Risikorechner, Korrekturzielregeln usw.)
- Vollständiger Korrekturlebenszyklus einschließlich Zurückstellung
- Regelmäßige Aufgaben

Zugehörige Informationen

Domänentrennung für Service Provider

Service-Mapping in Vulnerability Response

Service Mapping hilft Unternehmen, ein umfassendes Verständnis Ihrer IT-Infrastruktur und der Beziehungen zwischen verschiedenen Komponenten zu erlangen. Sie ermöglicht die automatische Erkennung und Zuordnung von Services, Anwendungen und Infrastrukturkomponenten und bietet eine visuelle Darstellung der Abhängigkeiten und Beziehungen.

In Vulnerability Responsestellt die regelmäßige Aufgabe `Set related CI services` Verbindungen zwischen den betroffenen Business-Services und den Configuration Items (CIs) her, die den angreifbaren Elementen (VITs) zugeordnet sind. Der Verknüpfungsprozess findet statt, sobald der Integrationsimport abgeschlossen ist und zu einem bestimmten Zeitpunkt. Um die Leistung dieser geplanten Aufgabe zu verbessern, wurden ab v21.1.2 von Vulnerability Responsemehrere Changes implementiert. Diese sind:

- Berechnung der Risikopunktzahl: Zur Berechnung von Risikopunktzahlen wird die geplante Aufgabe `Set related CI services` verwendet. Nach der Verarbeitung des CI speichert dieser Auftrag die erforderlichen Daten in der Tabelle „Zugehörige Services“ [sn_vul_m2m_ci_services]. Zuvor beinhaltete die Risikoberechnung in Konfigurations-Complianceden direkten Zugriff auf die `CIUtils` der Configuration Management Database (CMDB) Application Programming Interface (API), um während des Imports Services für jedes Testergebnis abzurufen. Der aktuelle Prozess verlässt sich jedoch auf die Ausgabe der geplanten Aufgabe aus der Tabelle „Zugehörige Services“ [sn_vul_m2m_ci_services], um die Risikopunktzahl in Konfigurations-Compliancezu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

berechnen. Darüber hinaus wurde der Basissystem-Rechner so geändert, dass er die Tabelle „Zugehörige Services“ [sn_vul_m2m_ci_services] verwendet.

- Größe der Services: Der Servicewert in der Systemeigenschaft *sn_sec_cmn.services_affected_by_CI_max_size*, der sich auf die geplante Aufgabe *Set related CI services* bezieht, wird von 1000 auf 500 verringert.
- Servicetiefe: Die Tiefe in der Systemeigenschaft *sn_sec_cmn.services_affected_by_CI_max_depth*, die sich auf die geplante Aufgabe *Set related CI services* bezieht, wird von 10 auf 5 reduziert. Der Servicewert wird ebenfalls von 1000 auf 500 verringert.
- Ausschluss von Klassen CMDB : Die Systemeigenschaft *sn_sec_cmn.ignoreCIClassForService* wurde eingeführt, um die Konfiguration von Klassen CMDB zu ermöglichen, für die die Serviceberechnung übersprungen werden soll. Im Basissystem ist diese Eigenschaft für *cmdb_ci_unclassed_hardware*, *cmdb_ci_incomplete_ip*, *sn_sec_cmn_unmatched_ci* festgelegt, da diese Klassen von Vulnerability Response erstellt werden und möglicherweise keine Servicezuordnung aufweisen. Zuvor basierte die Serviceberechnung auf der VIT. Die Logik wurde jedoch geändert, um stattdessen das erkannte Element zu verwenden. Das erkannte Element wird zur Berechnung des Services verwendet, der dann dem CI in derselben Tabelle zugeordnet wird.
- Geplante Aufgabe für vollständige Aktualisierung von Services: Eine geplante bedarfsgesteuerte Aufgabe *Full refresh-related CI services for VI*wurde eingeführt, um eine vollständige Aktualisierung von Services durchzuführen. Wenn Sie ein Upgrade auf v21.0 von Vulnerability Responsedurchführen, wird der Auftrag *Set related CI services* zunächst länger ausgeführt, da die Basistabelle erkannte Elemente anstelle von angreifbaren Elementen verwendet. Daher muss der Auftrag alle erkannten Elemente verarbeiten, die innerhalb der letzten 90 Tage gescannt wurden. Wenn Sie außerdem häufigere Serviceaktualisierungen benötigen, können Sie dies durch die Planung wöchentlicher regelmäßiger Aktualisierungen oder die Durchführung einer vollständigen Aktualisierung berücksichtigen. Wenn Sie Aktivitäten durchgeführt haben, die zu Änderungen an den mit Ihren CIs verknüpften Services geführt haben, und Sie möchten, dass Vulnerability Response diese Änderungen widerspiegelt, können Sie bei Bedarf die geplante Aufgabe *Full refresh related CI services for VI*ausführen. Dieser Auftrag verwendet alle erkannten Elemente, die in den letzten 90 Tagen erfasst wurden, und aktualisiert die zugehörigen Services entsprechend.

Zugehörige Informationen

Service Mapping

CIUtils - Global

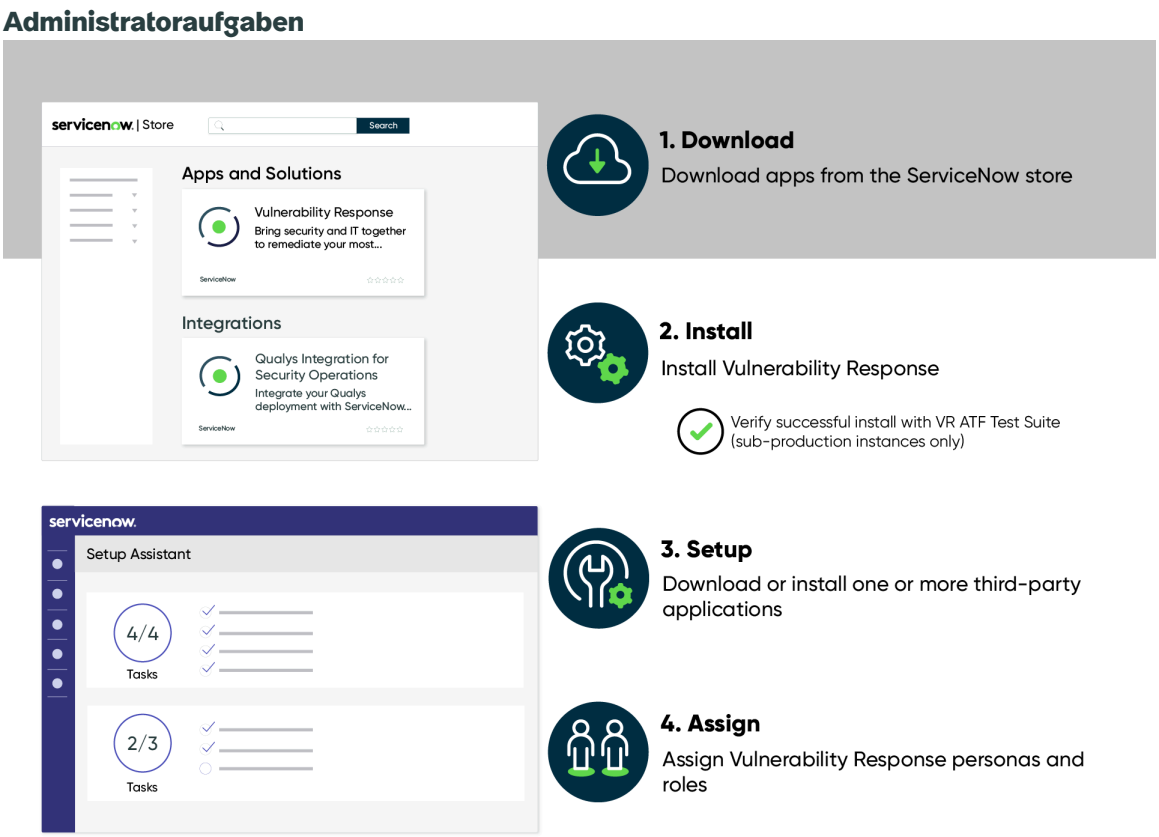
Vulnerability Response – Implementierung

Führen Sie die in den folgenden Abbildungen dargestellten Schritte aus, um die Anwendung Vulnerability Response aus dem ServiceNow Storeherunterzuladen, in Ihrer Instanz Now Platform® von zu installieren und mit dem Setup-Assistenten zu konfigurieren.

Ein Installations- und Konfigurationsbeispiel für die Installation des Basissystems, der Anwendung Vulnerability Response und der Scanner-Anwendung eines Drittanbieters, der Anwendung Qualys, ist in den folgenden Abbildungen dargestellt. Erforderliche Rollen und obligatorische Aufgaben sowie optionale Schritte werden ebenfalls aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weitere Informationen zu den einzelnen Schritten in den folgenden Abbildungen sowie eine Prüfliste mit Links zu unterstützender Dokumentation finden Sie unter Implementierungsprüfliste für die Anwendung Vulnerability Response.
- Sie können die Konzepte und die Reihenfolge der in diesem Beispiel dargestellten Schritte auf die Installation und Konfiguration anderer unterstützter Anwendungen für Vulnerability Responseerweitern. Eine Liste der unterstützen Anwendungen finden Sie unter Installation von Vulnerability Response und unterstützten Anwendungen.
- Die Administratorrolle ist erforderlich, um die Anwendung Vulnerability Response und die Anwendung Qualys Vulnerability, die in diesem Beispiel verwendet werden, herunterzuladen und zu installieren.
- Die Administratorrolle weist Benutzern und Gruppen auch die Persona „Schwachstellenadministrator“ [sn_vul.vulnerability_admin] und andere Persona-Rollen Vulnerability Response zu.



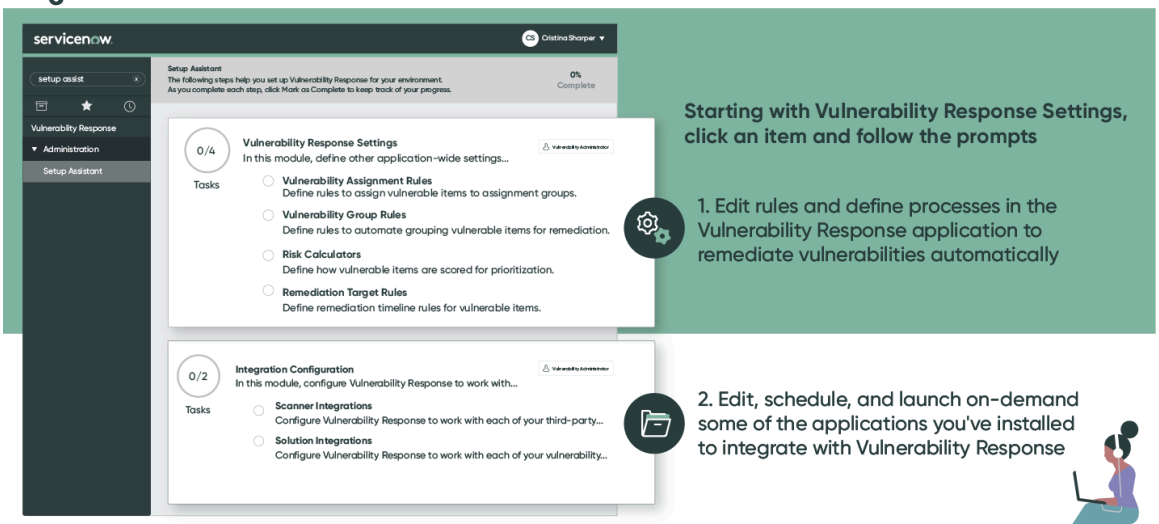
Die Rolle sn_vul.vulnerability_admin konfiguriert die Anwendungen Vulnerability Response und Qualys im Setup-Assistenten und überprüft die erwarteten Ergebnisse.

Befolgen Sie die Schritte und Eingabeaufforderungen im Setup-Assistenten, beginnend mit dem Abschnitt „Einstellungen für Vulnerability Response“, um mit der Installation und Konfiguration fortzufahren. Wenn Sie diese Einstellungen überprüfen, können Sie die -Prozesse von Vulnerability Response verstehen und überprüfen, während Sie mit der Einrichtung Ihrer Umgebung fortfahren.

Erforderliche Rolle: sn_vul.vulnerability_admin oder alternativ admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgaben des Schwachstellenadministrators



Roles required: sn_vul.vulnerability_admin or admin

Überprüfen Sie die Beschreibungen, Standardeinstellungen und Demodaten, die Sie mit den Anwendungen in den folgenden Abschnitten installiert haben:

- Zuweisungsregeln für Schwachstellen – weisen angreifbare Elemente (VIs) automatisch der entsprechenden Zuweisungsgruppe zu.
- Regeln für Korrekturaufgaben: Gruppieren angreifbare Elemente (VIs) automatisch, wenn sie basierend auf bestimmten Bedingungen importiert werden.
- Risiko-Rechner: Der Standard-Risiko-Rechner ist aktiviert.
- Korrekturzielregeln: Definieren Sie Korrekturzeitleisten für VIs und Korrekturaufgaben (RTs).
- Überprüfen und bearbeiten Sie die Einstellungen für die von Ihnen installierten Drittanbieteranwendungen und installierten Lösungen, und definieren Sie Bedingungen für Ihre Datenimporte. Geben Sie Ihre Drittpartei-Accountinformationen ein, und konfigurieren Sie Importeinstellungen, Zeitpläne, CI-Suchregeln (Configuration Item, Konfigurationselement) und andere Einstellungen.

Weitere Informationen finden Sie unter Implementierungsprüfliste für die Anwendung Vulnerability Response.

Weitere Informationen zur Anpassung oder Implementierung der Anwendung Vulnerability Response finden Sie unter KB1000704 .

Vulnerability Response installieren

Bevor Sie die Anwendung Vulnerability Response in Ihrer Instanz Now Platform ausführen, müssen Sie die Berechtigung von erhalten und die Anwendung von ServiceNow Storeherunterladen, sie in Ihrer Instanz Now Platform installieren und einige Installationsschritte im Setup-Assistenten ausführen.

Vorbereitungen

Hinweis:

Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

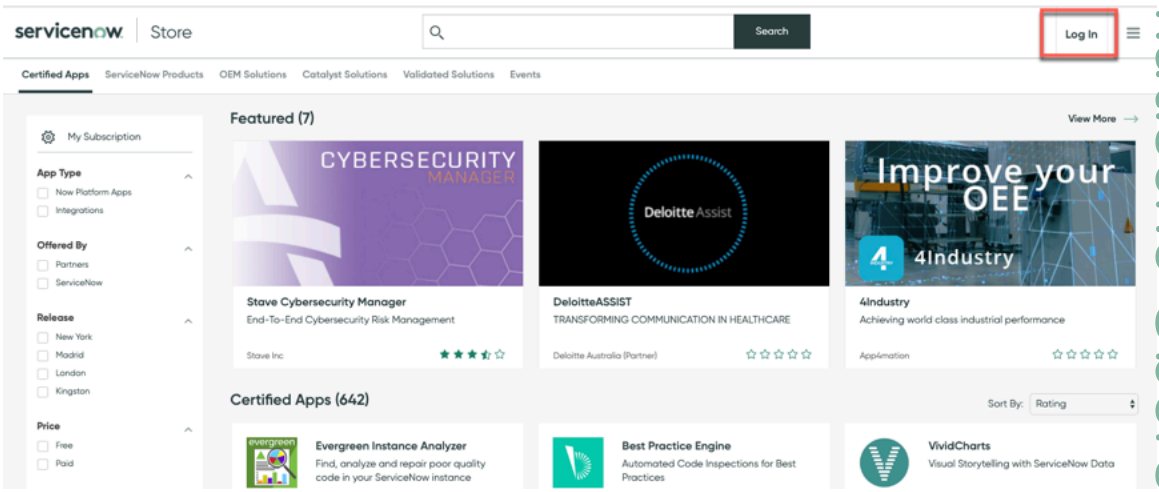
- Vergewissern Sie sich, dass Ihrer Instanz die erforderlichen Rollen ServiceNow zugewiesen sind.
- Die Administratorrolle ist für die Installation und das Zuweisen von -Rollen erforderlich.

Erforderliche Rolle: Administrator

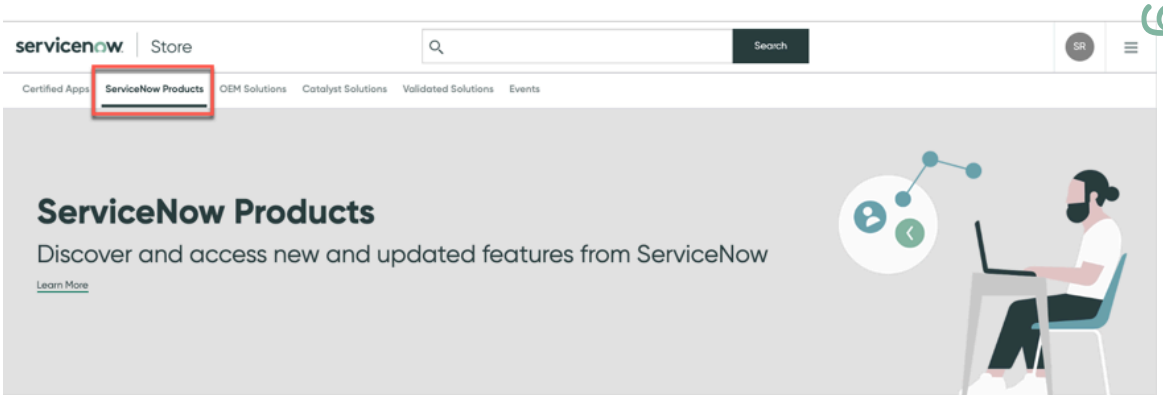
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Um die Berechtigung zu erhalten und die Kernanwendung Vulnerability Response herunterzuladen, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite **auf Anmelden**.



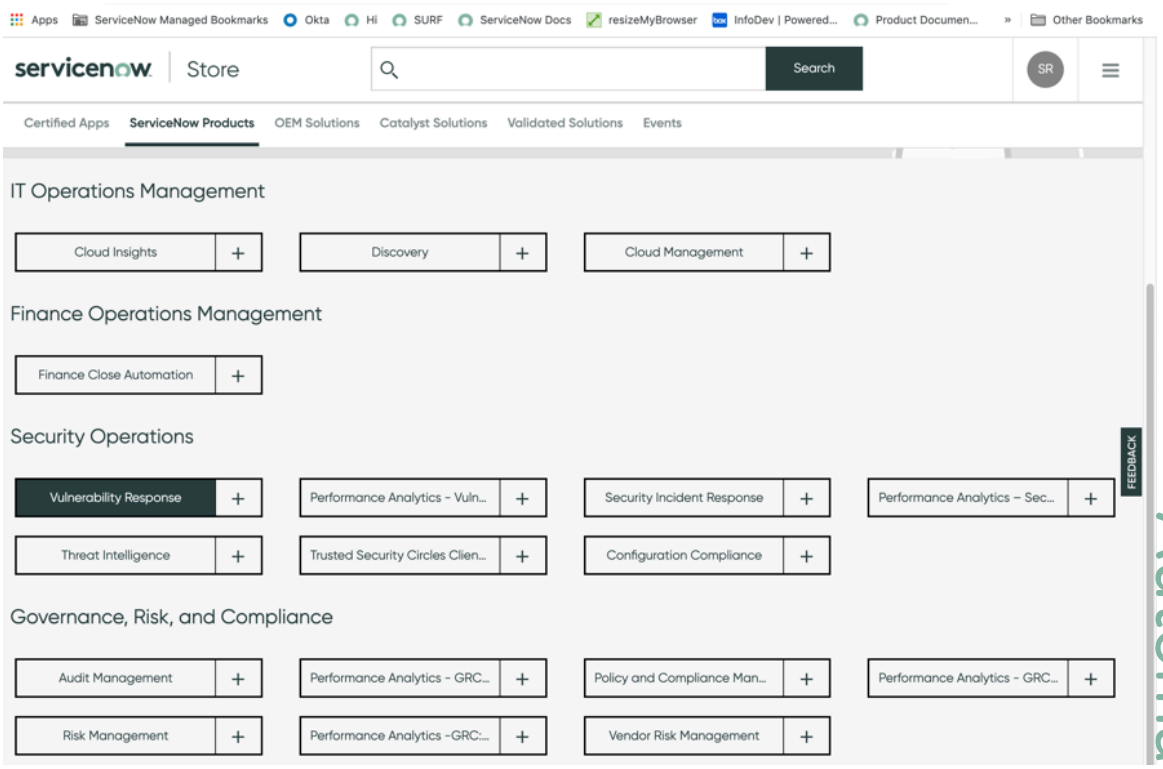
3. Geben Sie im angezeigten Dialogfeld Ihre HI-Anmeldeinformationen ein, und klicken Sie auf **Anmelden**.
4. Klicken Sie auf der angezeigten Seite auf die Registerkarte **ServiceNow-Produkte**, wenn sie nicht ausgewählt ist.



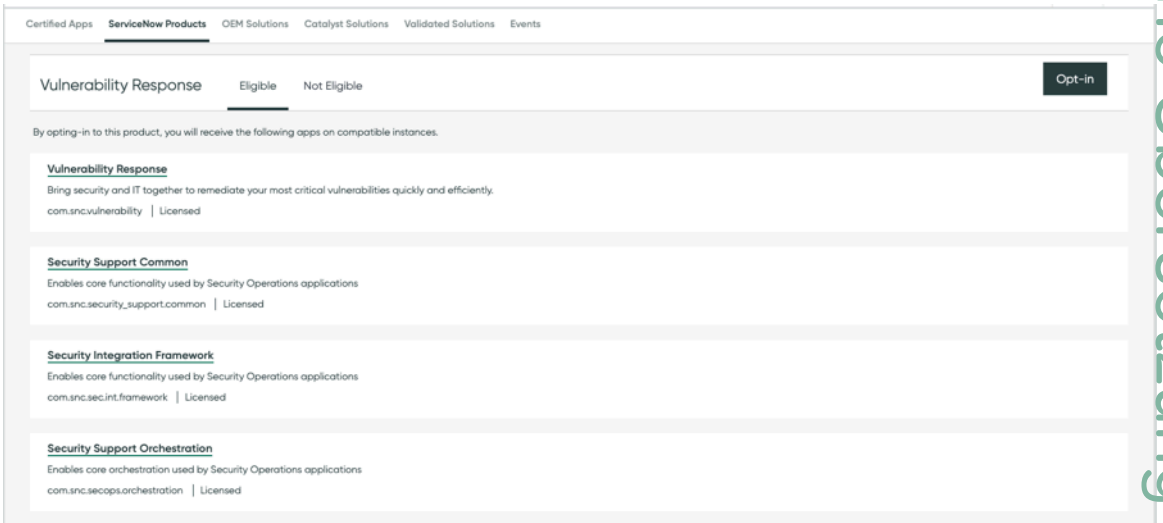
5. Um die zugeordneten Anwendungen anzuzeigen, für die Sie mit der Anwendung Vulnerability Response berechtigt sind, klicken Sie auf der Seite mit der Produktliste auf das Produkt **Vulnerability Response**.

Automatische Übersetzung

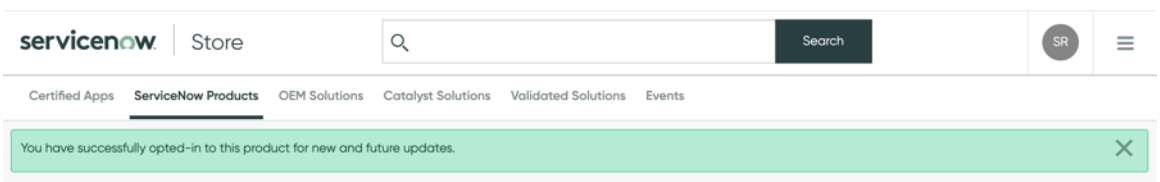
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Registerkarte Berechtigt werden alle Anwendungen aufgelistet, für die Sie berechtigt sind, wenn Sie sich anmelden. Klicken Sie auf einen Link, um weitere Informationen zu einer Anwendung zu erhalten.



6. Um die Kernanwendung Vulnerability Response zu erhalten, klicken Sie auf **Aktivieren**.
7. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Eingabeaufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.
   Es wird eine Meldung angezeigt, dass Sie sich erfolgreich für die Anwendung entschieden haben.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

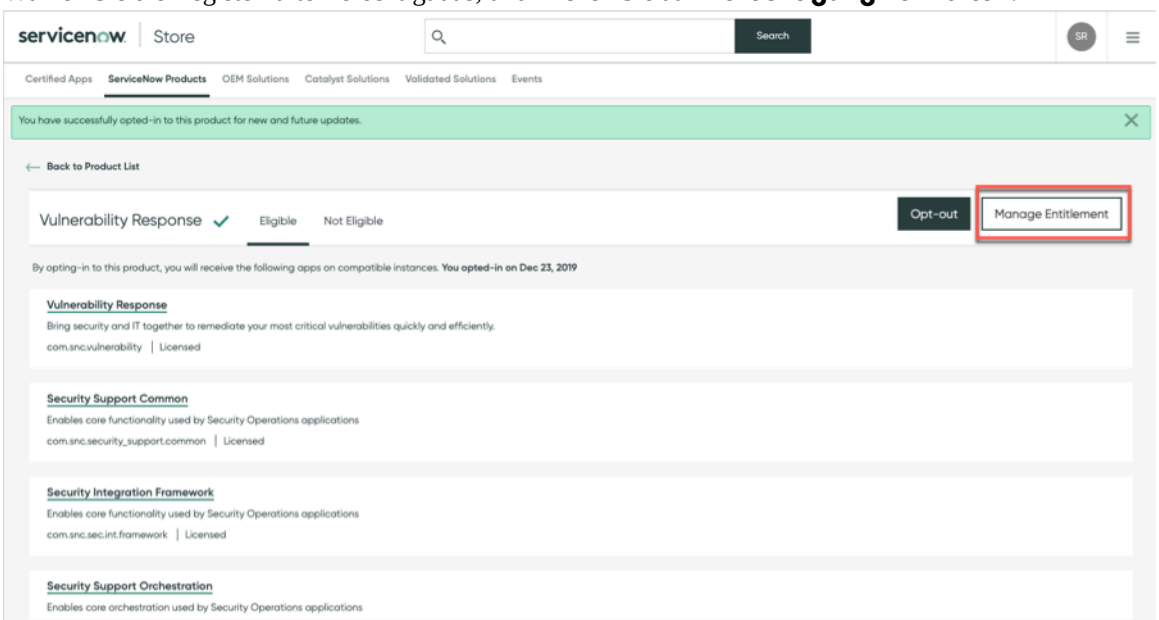
Wenn die Registerkarte ServiceNow Produkte ausgewählt und angezeigt ist, ersetzt ein grünes Häkchen das Pluszeichen rechts neben der Anwendung Vulnerability Response (siehe folgende Abbildung).

Nachdem Sie die Nutzungsbedingungen für eine der Anwendungen auf der Registerkarte **ServiceNow-Produkte** akzeptiert und Berechtigungen für eine der Anwendungen auf der Registerkarte Produkte von ServiceNow verwaltet haben, können Sie auf der Seite Produktliste auf das Pluszeichen (+) klicken, um Berechtigungen zu erhalten und die anderen Anwendungen zu aktivieren Seite mit einem einzigen Klick.

8. Fahren Sie mit Schritt 10 fort, um die Anwendung in Ihrer Instanz Now Platform zu installieren.
9. **Wahlweise:** Um Ihre Berechtigung für die Anwendung Vulnerability Response in anderen Instanzen Now Platform zu verwalten, führen Sie alternativ die folgenden Schritte aus.

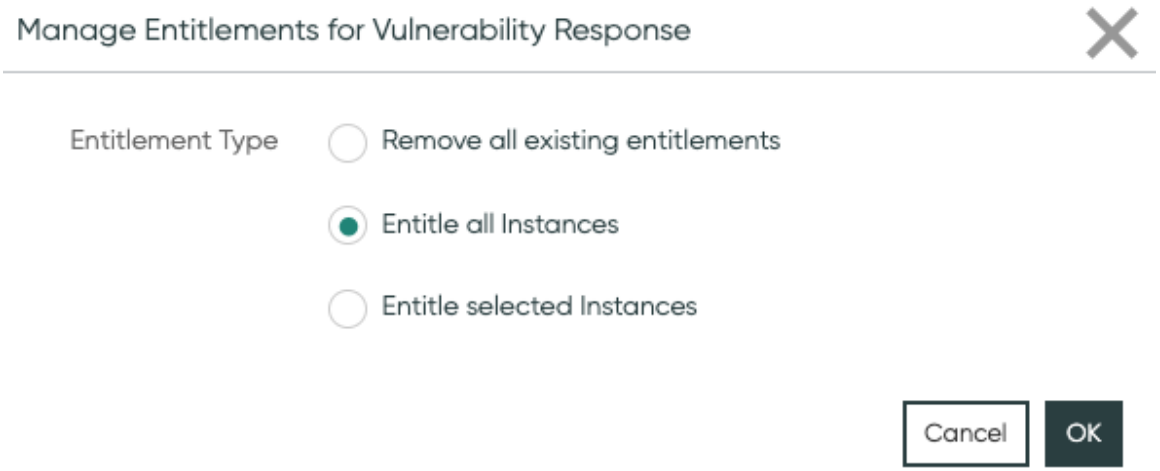
   a. Wenn die Schaltfläche Berechtigung verwalten nicht angezeigt wird, klicken Sie auf die Anwendung Vulnerability Response in der Produktliste, um sie anzuzeigen.

   b. Wählen Sie die Registerkarte Berechtigt aus, und klicken Sie auf **Berechtigung verwalten**.



   c. Wählen Sie im angezeigten Dialogfeld „Berechtigungen für Vulnerability Response verwalten“ eine Option aus:

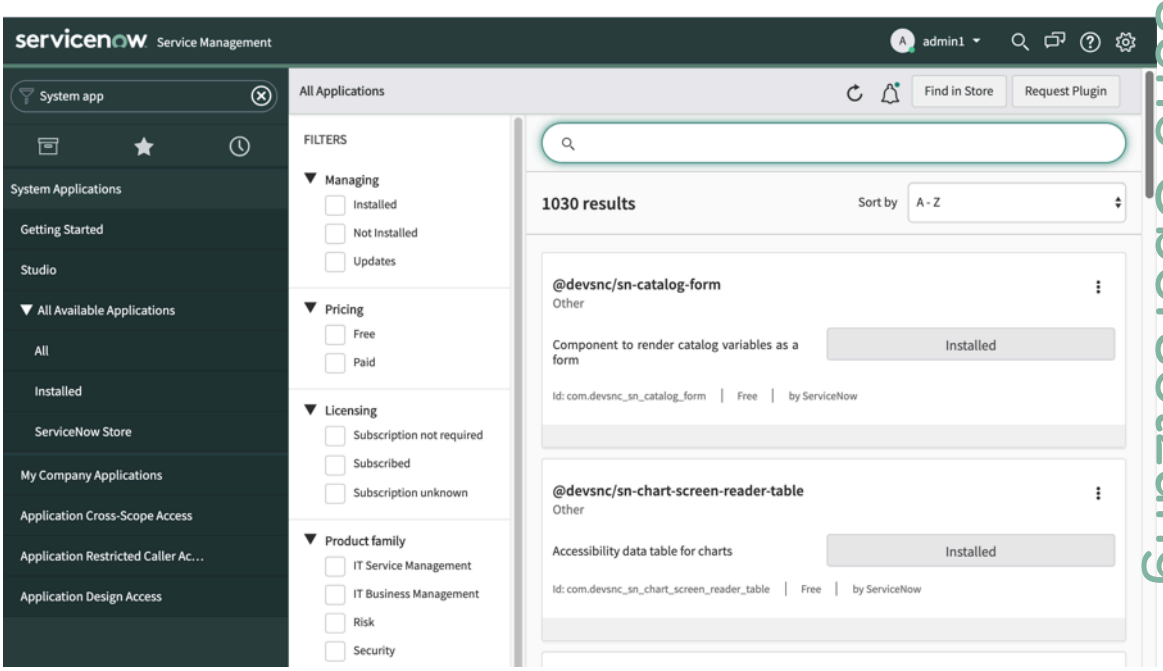
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Klicken Sie auf **OK** oder **Abbrechen,** um fortzufahren.
Sie können nun Plugins aktivieren und die Anwendung auf Ihren Now Platform Instanzen installieren.

10. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Vulnerability Response installieren möchten.

11. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



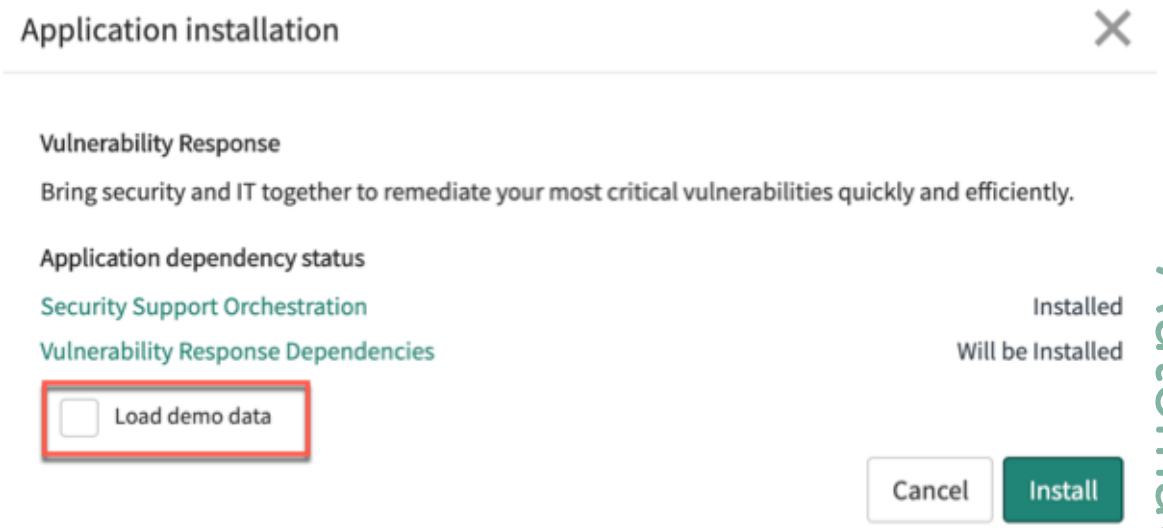
12. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Vulnerability Response (sn_vul), wählen Sie in der Auswahlliste eine Version aus, und klicken Sie auf **Installieren**.
Das Dialogfeld „Anwendungsinstallation“ wird angezeigt. Alle Abhängigkeiten, die installiert werden, werden angezeigt.

13. **Wahlweise:** Wenn Sie Demodaten wünschen, aktivieren Sie das Kontrollkästchen Demodaten laden, und klicken Sie auf **Installieren**.

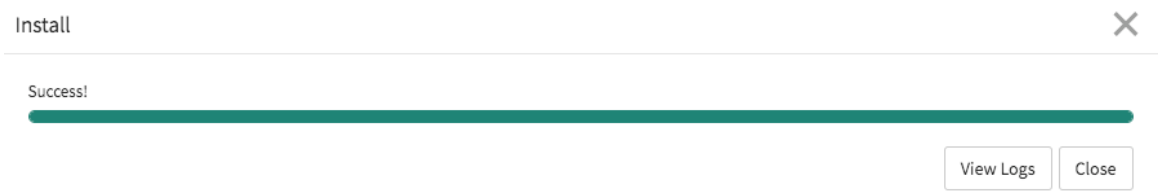
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie das Kontrollkästchen **Demodaten laden** nicht aktivieren, können die Demodaten nicht später über den **Anwendungsmanager** installiert werden. Informationen zur Installation oder erneuten Installation von Demodaten nach der Erstinstallation finden Sie im Artikel Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] in der Knowledge Base Now Support.

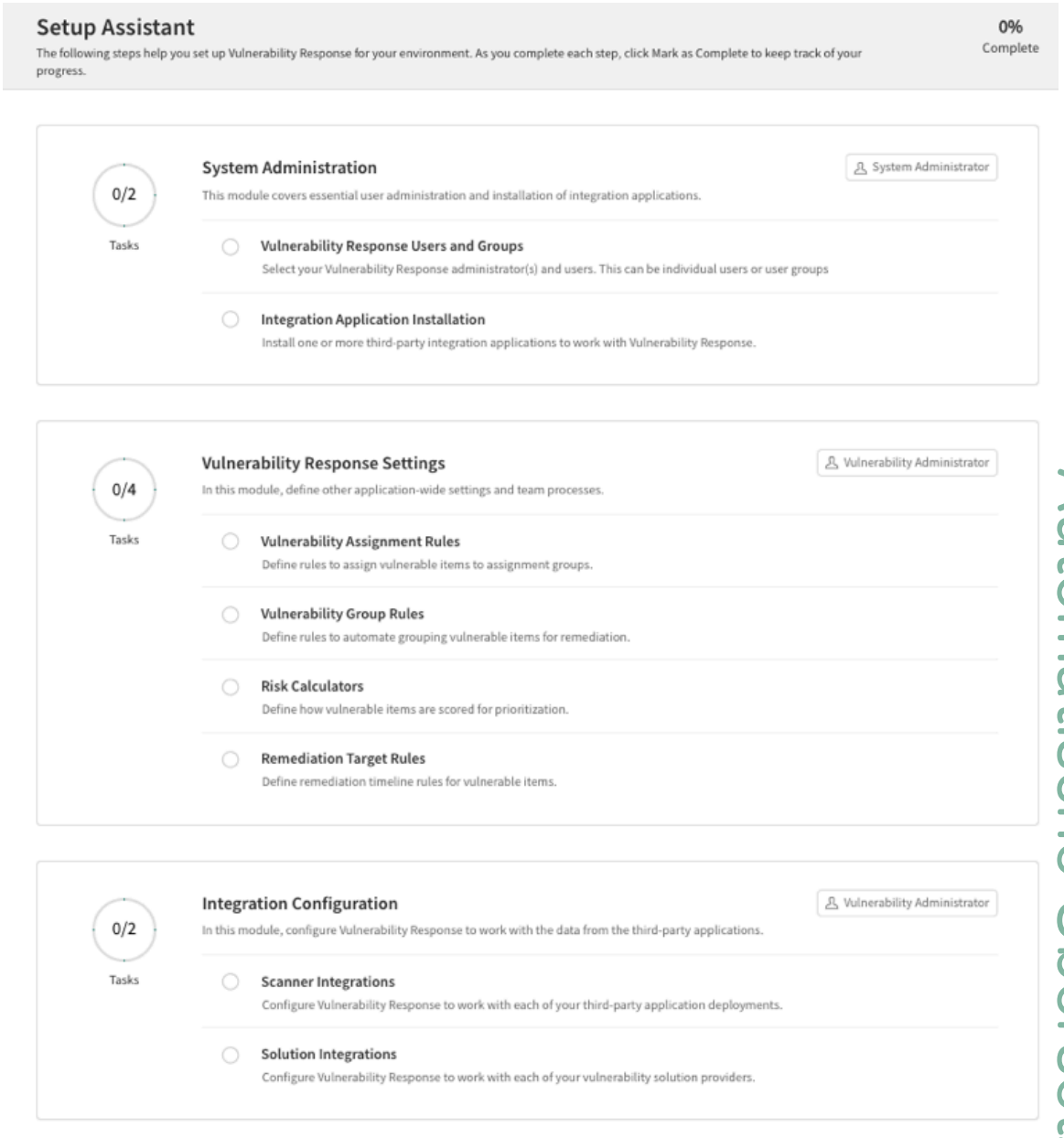


Diese Installation kann einige Zeit in Anspruch nehmen. Nachdem die Anwendung erfolgreich installiert wurde, wird im Dialogfeld „Installieren“ eine Meldung angezeigt.



14. Klicken Sie auf **Schließen**.
15. Nachdem die Installation erfolgreich abgeschlossen wurde, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



16. Befolgen Sie die Anweisungen auf den Formularen in den einzelnen Abschnitten.

Nächste Maßnahme

Weitere Informationen zu Einstellungen für Vulnerability Response, zur Installation von Anwendungen, zur Konfiguration, zu Integrationen, Gruppenregeln, Risikorechnern und Korrekturzielregeln finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

Mit Vulnerability Response installierte Komponenten

Bei der Aktivierung der Anwendung Vulnerability Response werden mehrere Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und regelmäßige Aufgaben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie gefilterte Listen für mit einer Anwendung installierte Komponenten an

Ab v24.0.6 von Vulnerability Responsesind die am häufigsten verwendeten Systemeigenschaften jetzt in der Anwendung Vulnerability Response zugänglich. Um diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Vulnerability Response**Eigenschaften**.

Filtern Sie die Tabelle „Anwendungsdateien“, damit nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert wurden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert werden, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie diese Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator **sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **AND**und dann aus. **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Hinweis:
Rollen, geplante Aufgaben und Tabellen für Application Vulnerability Response finden Sie unter Mit Application Vulnerability Response installierte Komponenten.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_prisma.configure_prisma_integration	Sichert die CRUD- und report_view-Vorgänge in der Tabelle „sn_vul_prisma_hosts_import“ und den Vorgang „report_view“ in der Tabelle „sn_vul_prisma_host_attrb“.	
sn_vul.view_manager_workspace	Ansichten Vulnerability Manager Workspace.	
sn_vul.delete	Löscht Quelldatensätze und angreifbare Elemente. Vor v23.0 hatte die Administratorrolle die Berechtigung zum Löschen der Quelldatensätze.	• sn_vul_cmn.delete • sn_vul.delete_vulnerable_items
sn_vul_cmn.delete	Löscht Quelldatensätze.	
sn_vulc.bulk_edit	Führt einen Massenbearbeitungsvorgang für Testergebnisse durch.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul.app_bulk_edit	Führt einen Massenbearbeitungsvorgang für angreifbare Anwendungselemente (Application Vulnerable Items, AVITs) durch.	sn_vul.app_write_all
sn_vul_container.container_bulk_edit	Führt einen Massenbearbeitungsvorgang für angreifbare Container-Elemente (CVITs) durch.	sn_vul_container.write_all
sn_vul_cisa.configure_intelligence_integration	Konfiguriert Intelligence-Integrationen.	
Schwachstellenmanager und leitende Analysten [sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)]	Aktualisieren Sie Eigenschaften und Schwachstellen-Integrationen. Die Rolle sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) ist für die Verwaltung Vulnerability Response von erforderlich, einschließlich Schwachstellen-Integrationen, Regeln für Korrekturaufgaben, Rechnern, Regeln und Aufgaben für Korrekturzielen, Berichten und der Konfiguration von Drittanbieterintegrationen.	• sn_vul.vulnerability_write • sn_vul.c iso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (wenn die Qualys-Schwachstellenintegration installiert ist.) • sn_vul_r7.admin (wenn die Rapid7 Vulnerability Integration installiert ist.) • sn_vul_shodan.admin (wenn die Shodan Exploit-Integration installi ist.) • sn_vul.configure_nvd_integration (wenn die NVD-Integrationen installiert sind.) • Treemap_admin (wenn die Anwendung „Performance Analyti installiert ist.)
Patch-Orchestrierung	Konfiguriert unterstützte Patch-Lieferanten-Integrationen von Drittparteien Zeigen Sie Patch-Daten und Patch-Datensätze an, und wenden Sie sie an.	• sn_vul_patch_orch.configure_patc Patches konfigurieren und anwenden. • sn_vul_patch_orch.read_patch Kann Patch-Datensätze und Date anzeigen. • sn_vul_bigfix.configure_integration Konfiguriert die Anwendung „BigFix Patch Orchestration Integration“. Diese Rolle enthält die granularen Rollen „sn_vul_bigfix.read_integration“ ur „connection_admin“, mit denen de

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
		Benutzer eine Verbindung zur Bigl Konsole herstellen kann. • sn_vul_sccm.configure_integration Diese Rolle enthält die granularen Rollen „sn_vul_sccm.read_integration“ und „connection_admin“, die es dem Anwender ermöglichen, eine Verbindung zur SCCM-Konsole herzustellen. • sn_vul_bigfix.read_integration Benutzer mit dieser Rolle können die Datensätze der Anwendungen Vulnerability Response und BigFix Patch Orchestration Integration sowie die Patch-Orchestrationsda anzeigen (schreibgeschützt). • sn_vul_sccm.read_integration Benutzer mit dieser Rolle können die Datensätze der Anwendung Vulnerability Response und die Microsoft SCCM Patch Orchestration Integration-Anwendung und die Patch Orchestration-Daten anzeigen (schreibgeschützt).
Schwachstellenanalysten [sn_vul.vulnerability_write]	Die Rolle sn_vul.vulnerability_write ist für die Verwaltung von Korrekturaufgaben und angreifbaren Elementen sowie für die Überwachung des Korrekturfortschritts erforderlich.	• sn_vul.read_all • sn_sc_cmn.write • sn_vul_qualys.user (wenn die Qual Schwachstellenintegration installie ist.) • sn_vul_shodan.write (wenn die Shodan Exploit-Integration installi ist.)
V19.0: Manager für Schwachstellenereignisse [sn_vul_analyst.vul_event_manager]	Die Rolle sn_vul_analyst.vul_event_manager wird verwendet, um die Auswirkungen einer neuen Schwachstelle oder Software zu bewerten oder eine Zero-Day-Schwachstelle hinzuzufügen, um die betroffenen Assets zu identifizieren und angreifbare Elemente (VIs) zu erstellen.	• sn_sec_cmn.read • canvas_user • sn_vul_analyst.emergency_respon • sn_vul.manage_exposure_assessm

Automatisierte Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
Andere [sn_vul.read_all] Die Rolle sn_vul.vulnerability_read ist veraltet.	Die Rolle sn_vul.read_all ist für alle Personen erforderlich, die Einblick in das Schwachstellenmanagement benötigen. Zum Beispiel IT- und Sicherheitsverantwortliche oder andere Personen, die einen Drilldown von allgemeinen Dashboards zu den Elementen durchführen möchten, aus denen die Visualisierungen des Dashboards bestehen. **Wichtig:** Ab v24.0.6 von Vulnerability Responsehat die Rolle sn_vul.read_all die Berechtigung zum Zugriff auf Vulnerability Manager Workspace.	• sn_sec_cmn.read • sn_vul_qualys.read (wenn die Qual Schwachstellenintegration installie ist. • sn_vul_shodan.read (wenn die Shodan Exploit-Integration installie ist.) • pa_viewer (wenn die Anwendung „Performance Analytics“ installiert ist.) • sn_vul_tenable.read_integration (wenn die Tenable-Schwachsteller Integration installiert ist.) • sn_vul.view_manager_workspace
sn_vul.read_assigned	Zeigen Sie angreifbare Elemente, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind, in der klassischen Anwenderoberfläche und in IT Remediation Workspacean. **Wichtig:** Ab v24.0.6 von Vulnerability Responsehat die Rolle sn_vul.read_assigned die Berechtigung, auf IT Remediation Workspacezuzugreifen.	sn_vul.view_rem_workspace
VR-Systemimportadministrator [sn_vul.vr_import_admin]	Systembenutzer, der ausgeführt wird. Führt geplante Aufgaben aus. **Hinweis:** Dieser Anwender ist der standardmäßige Ausführen-als-Anwender für jeden Integrationsdatensatz. Nicht ändern.	• import_admin • sn_vul.vulnerability_write
Korrekturbesitzer [sn_vul.remediation_owner]	Zeigen Sie Berechtigungen für angreifbare Elemente und Korrekturaufgaben an, die Ihnen oder Ihrer Gruppe zugewiesen sind, und aktualisieren Sie sie. Kann alle Schwachstellen	Enthalten in der Rolle itil.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	und Lösungen anzeigen. Hat Schreibzugriff auf das**Feld „Interne Notizen“** im Lösungsdatensatz.	
CISOs und Schwachstellenmanager [sn_vul.vulnerability_cso]	Zeigen Sie das CISO-Dashboard in Performance Analytics für Vulnerability Response an.	• sn_vul.c iso_read • sn_vul.read_all
Falsch positiver Genehmiger [sn_vul.false_positive_approver]	Genehmigt/ablehnt falsch positive Anforderungen ab.	sn_vul.view_manager_workspace
Ausnahmegenehmiger [sn_vul.exception_approver]	Genehmigt/ablehnt Ausnahmeanforderungen ab.	sn_vul.view_manager_workspace

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Füllen Sie gespeicherte OOTB-Filter für das Host- und App-Modul aus	Migriert Module im Zusammenhang mit dem Host- und App-Modul.
Gespeicherte OOTB-Filter für CC-Modul ausfüllen	Migriert Module im Zusammenhang mit dem CC-Modul.
Füllen Sie gespeicherte OOTB-Filter für das Containermodul aus	Migriert Module im Zusammenhang mit dem Containermodul.
Hostbezogene gespeicherte Filter aktualisieren	Aktualisiert alle Zusammenfassungsdaten, die sich auf gespeicherte Filter des Host-Moduls beziehen.
CC-bezogene gespeicherte Filter aktualisieren	Aktualisiert alle Zusammenfassungsdaten, die sich auf die gespeicherten Filter des CC-Moduls beziehen.
Aktualisieren Sie die gespeicherten Filter im Zusammenhang mit dem Container	Aktualisiert alle Zusammenfassungsdaten, die sich auf gespeicherte Filter des Containermoduls beziehen.
Aktualisieren Sie die App-bezogenen gespeicherten Filter	Aktualisiert alle Zusammenfassungsdaten, die sich auf gespeicherte Filter des App-Moduls beziehen.
Löst die Zusammenfassungserstellung und -ausführung für gespeicherte Filter aus	Erstellt, aktualisiert, führt und aktualisiert die Zusammenfassungen im Zusammenhang mit dem gespeicherten Filter.
Version 19.0 von Vulnerability Response und v4.0 von Veracode Vulnerability Integration	Die Veracode-CWE-Integration ruft Veracode -spezifische Common Weakness Enumeration-Daten (CWE) ab, um Informationen zu Bedrohungen und Korrekturempfehlungen zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	Die Veracode-SBOM-Integration erfasst Release-, Versions- und Schwachstelleninformationen aus Veracode für die Komponenten in Ihren Softwareprojekten. Die Integration generiert SBOMs im JSON-Format „CycloneDx“ und lädt sie in Ihre -Instanz Die Veracode-Kategorieintegration ruft erweiterte Kategoriedaten aus Veracodeab. Mit der DevOps-Integration Veracode können DevOps-Anwender Zusammenfassungsdetails für Schwachstellen-Scans von Drittparteien ohne SecOps-Lizenz anzeigen. JSON-basierte APIs für die folgenden Veracode-Integrationen: Angreifbares Anwendungselement, Scan-Zusammenfassung, Anwendungsliste. Die XML-basierten API-Versionen dieser Integrationen sind veraltet.
Ordnen Sie der automatischen Ausnahmeregel vorhandene AEs zu	Ordnet die automatische Ausnahmeregel automatisch vorhandenen AEs zu.
Angreifbare Erkennungen automatisch schließen	Schließt automatisch die veralteten angreifbaren Erkennungen basierend auf der in der Tabelle „sn_vul_auto_close_config“ definierten Konfiguration.
Version 16.1: Integrationen mit HCL BigFix-Sammlung, Fixlet und Aktionen.	Verwalten Sie Patches und Patch-Bereitstellungen für Schwachstellen mit Patches aus dem Produkt HCL BigFix.
Zugehörige Anzahlen für alle Lösungen berechnen	Standardmäßig inaktiv. Verarbeitet Lösungsdaten einmal pro Nacht statt kontinuierlich. Ab v22.0 können Sie diese Aufgabe nur bei Bedarf ausführen. Da diese geplante Aufgabe alle Lösungen verarbeitet, kann dies die Leistung beeinträchtigen. Daher wird empfohlen, diesen Auftrag nur einmal auszuführen, wenn die Lösungsdaten beschädigt sind.
Berechnen Sie die Anzahl der zugehörigen VIs für Schwachstelle und Korrekturaufgabe	Erfasst manuelle und VI-Importänderungen für den Tag. Gleicht Schwachstellen- und Lösungsbeziehungen ab und berechnet die Gesamtsummen neu. Lösungsdaten werden in die Warteschlange gestellt und separat von der geplanten Aufgabe **der Warteschlange für Schwachstellenlösungsmetriken** verarbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Überprüfen Sie die Zeitüberschreitung bei MID-Server	Pingt den MID-Server an und nach 30 Sekunden tritt ein Fehler auf.
V19.0: Überprüfen Sie das potenzielle Schwachstellenrisiko	Verarbeitet die Delta-CVEs, die Software und die Delta-Installationen, um das Risiko zu erhalten.
Überprüfen Sie den Ausführungsstatus „WaitComplete“.	Markiert eine Integrationsausführung als abgeschlossen, sobald verifiziert wurde, dass sie vollständig abgeschlossen ist.
Überprüfen Sie den Ablauf der Zurückstellung für angreifbare Elemente und Gruppen	Sendet Benachrichtigungen, wenn angreifbare Elemente oder Schwachstellen abgelaufen sind (und wenn sie in einer Woche ablaufen). Überprüft, ob eine Ausnahmeregel für ein zurückgestelltes AEs gilt, und aktualisiert die Felder **„Grund“** und „ **Bis“** gemäß der Ausnahmeregel. Der Status des AE bleibt bis zum spätesten Ablaufdatum zurückgestellt.
Abbrechen von VITs schließen, denen kein CI zugeordnet ist	Schließt automatisch angreifbare Elemente, denen kein Configuration Item (CI) zugeordnet ist und die seit drei Tagen nicht mehr aktualisiert wurden. Status wird auf „Geschlossen/Abgebrochen“ festgelegt.
VI beim Löschen des Exp-Datensatzes schließen	Schließt ein VI, wenn es gelöscht wird.
Integration von Compliance-Ergebnissen	Importiert Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Zitaten mit autoritativen Quellen zur Verarbeitung in der Anwendung Configuration Compliance.
Integration der Auffüllung von Compliance-Ergebnissen	Als Teil einer verketteten Integrationsausführung mit Tenable.io Assets Integration importiert Konfigurationsbewertungsdaten für ignorierte Assets, die erkannt werden (importiert durch Assets-Integration).
CR-Statussynchronisierung	Das Skript passt alle vorhandenen Korrekturaufgaben an CHG-Beziehungen an, sodass sie synchronisiert werden. Aktiviert die zukünftige Synchronisierung.
Version 15.0 Integration von Scan-Anmeldeinformationen	Importiert und speichert sie sicher vorübergehend Tenable.io Anmeldeinformationen, die für den Zugriff auf den Scanner für erneute Scans bei Bedarf verwendet werden.
CWE Comprehensive 2000 Integration	Schwachstellen-Integration, die Schwachstelleninformationen aus dem Common Weakness Enumeration-Datensatz (CWE) abruft, der von der MITRE Incident kuratiert wird.
V18.0: Veraltete Split-Aktionsdatensätze löschen	Täglicher Auftrag zum Bereinigen veralteter Datensätze in Zwischentabellen für aufgeteilte Aufgaben.
Deaktivieren Sie VR-Lösungen, wenn die Lösungsanwendung nicht aktiv ist	Deaktiviert und blendet die Funktion Vulnerability Solution Management aus, wenn die Anwendung Solution Management for Vulnerability Response nicht installiert ist.
Bewerten Sie die Korrekturziele	Legt für alle angreifbaren Elemente Korrekturzieldaten fest oder aktualisiert sie. Bestimmt den Status von Korrekturzieldaten anhand von Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
• Korrektur der Erkennungen für aktualisierten Schlüssel für Rapid7 • Korrektur der Erkennungen für aktualisierten Schlüssel für Qualys • Die Erkennungen für einen aktualisierten Schlüssel für Tenable werden korrigiert	Bereinigt Erkennungsdaten automatisch durch eine integrationsspezifische geplante Aufgabe, die nach dem Upgrade auf Vulnerability Responseausgelöst wird.
Version 16.1: Generiert einen Korrektur-Digest	Dieser Auftrag generiert automatisch einen E-Mail-Digest für alle Anwender in der Anwendergruppe „Korrekturbesitzer“. Die Aufgabe ist standardmäßig aktiviert.
V19.0: Von CISA ausgenutztes CVE in Risikokonfiguration einfügen	Fügt CISA-CVEs in die Risikokonfigurationstabelle ein, um das Risiko zu berechnen.
V18.0: Klassische Korrekturaufgaben in einheitliche Korrekturaufgabe einfügen	Einmalige geplante Aufgabe zum Einfügen aller in der klassischen Anwenderoberfläche erstellten Korrekturaufgaben in die einheitliche Korrekturaufgabe (sn_vul_remediation_task).
Integration der Microsoft Security Response Center-Lösung	Vulnerability Solution Management -Integration, die Lösungen von Microsoft Security Response Centerabruft.
Version 16.1: Integrationen für Microsoft SCCM-Sammlung, Patch-Update und Bereitstellungen	Verwalten Sie Patches und Patch-Bereitstellungen für Schwachstellen mit MicrosoftMicrosoft Azure Event Hubs SCCM-Patches.
Gedrosselten Integrationsprozess aufnehmen	Erstellt den Integrationsprozess für Shodan Exploit-Integration.
Text für betroffene Produkte ausfüllen	Nach dem Upgrade werden von vorhandenen Lösungen verarbeitet, um den Text der betroffenen Produkte auszufüllen. Dieser Auftrag wird nur einmal ausgeführt.
Füllen Sie die neue CR-Anzahlspalte aus	Füllt die neue Spalte für die CR-Anzahl für Kunden automatisch mit vorhandenen Daten in der Tabelle für Korrekturaufgaben [sn_vul_vulnerability] aus.
Warteschlange für Metriken der Schwachstellenlösung verarbeiten	Verarbeitet die Lösungsdaten in der Warteschlange durch: • Rollup von Lösungen aus NVD-Einträgen auf Einträge von Drittparteien • Ausfüllen bevorzugter Lösungen für Schwachstellen, und • Die Korrekturstatusmetriken für die Lösungen werden aktualisiert Darüber hinaus verarbeitet es auch die Lösungen, die für die Statusaktualisierung markiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	Hinweis: Wenn Sie nur Rapid7verwenden, können Sie diese geplante Aufgabe deaktivieren, um die Leistung zu verbessern.
Füllen Sie die Datensätze in der Zuordnungstabelle für Schwachstellenlieferanten aus Füllen Sie Datensätze in der Zuordnungstabelle für Schwachstellenlieferanten für Rapid7-Schwachstellen aus	Fügt Datensätze in die Zuordnungstabelle für Schwachstellenlieferanten für vorhandene Schwachstellen ein.
Öffnen Sie zurückgestellte Schwachstellen-Gruppen erneut	Öffnet zurückgestellte Korrekturaufgaben erneut, wenn das Aufschubdatum verstrichen ist.
Alle Zuweisungsregeln für Schwachstellen erneut anwenden	Wertet Zuweisungsregeln für alle **offenen** AEs neu aus.
Version 16.5: Anzahl der Neuzuweisungen für Zuweisungsregeln	Wird täglich ausgeführt und postet die Gesamtzahl der AEs und Korrekturaufgaben, deren Zuweisung von dieser Funktion für eine bestimmte Zuweisungsregel aufgehoben wurde.
Red Hat Solution Integration	Vulnerability Solution Management -Integration, die Lösungen von Red Hat Security Advisoryabruft.
V17.1: Doppelte VITs in Korrekturaufgabe aktualisieren und beheben	Findet doppelte angreifbare Elemente für die Elemente in der Korrekturaufgabe, für die „Doppelte VIs automatisch aktualisieren“ aktiviert ist.
Aktualisieren Sie die zugeordneten angreifbaren Elemente für die auf der Regel für Korrekturaufgaben basierende Korrekturaufgabe	Aktualisiert die Korrekturaufgabe mit angreifbaren Elementen, die den Kriterien Filtergruppe und Bedingungsgruppen entsprechen.
Reparieren Sie fehlerhafte angreifbare Elemente, die zuletzt geöffnet und geschlossen wurden	Repariert vorhandene UI-Daten, die durch zuvor behobene Fehler beschädigt wurden.
Rechner erneut ausführen	Wendet die Rechner auf alle angreifbaren Elemente an, die von der Änderung betroffen sind. Dies löst eine Neuberechnung der kumulativen Risikopunktzahlen der Korrekturaufgabenaus. **Hinweis:** Das erneute Ausführen von Rechnern kann je nach Umgebung viel Zeit in Anspruch nehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Abgebrochene Integrationsimportsätze wiederholen	Versucht abgebrochene Integrationsimportsätze erneut. Versucht es fünfmal, bevor ein Fehler zurückgegeben wird.
Wiederholen Sie Integrationsprozesse	Wiederholt Integrationsprozesse. Versucht es fünfmal, bevor ein Fehler zurückgegeben wird.
Rollup der Werte von angreifbaren Elementen zu Schwachstelle und Gruppe	Berechnet die Risikopunktzahl, die Anzahl der angreifbaren Elemente und den Korrekturzielstatus für Korrekturaufgabenmithilfe des Rollup-Rechners. **Hinweis:** Ab v23.0 von Vulnerability Responsewird die regelmäßige Aufgabe erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade beinhaltet die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.
Führen Sie den Schweregradrechner nach der Heraufstufung des Schwachstelleneintrags aus	Führt den Schweregradrechner aus, nachdem eine zuvor fehlende Schwachstelle mit ihrer Punktzahl und anderen Daten von einem Drittanbieter aktualisiert wurde, z. B. Qualys Cloud Platform, Rapid7 Nexpose. **Hinweis:** Ab v25.0.3 von Vulnerability Responsewird die geplante Aufgabe erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade beinhaltet die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.
V19.0: Führen Sie eine Bewertung des Gefahrenpotenzials für konfigurierte CVEs durch	Berechnet das Risiko für alle CVE-Datensätze in der Risikokonfigurationstabelle.
V19.0: Softwarerisiko ausführen	Berechnet das Risiko für alle Softwaredatensätze in der Risikokonfigurationstabelle.
Geplanter Schwachstellen-Datenquellenprozessor	Überprüft die Importwarteschlange auf zu verarbeitende Einträge und weist basierend auf den verfügbaren Ressourcen einen geplanten Importauftrag zu.
Geplante Bereinigung von Anhängen des Prozesses für Schwachstellenintegration	Entfernt XML-Anhänge für die Integration, sobald sie 14 Tage alt sind. Diese Aufbewahrungszeit ist nicht konfigurierbar.
Zeitüberschreitungsprüfung für geplante Schwachstellenintegration	Bricht Integrationsausführungen ab, die mehr als 60 Minuten dauern.
Legen Sie zugehörige CI-Services für AE fest	Sobald der Integrationsimport abgeschlossen ist, werden die betroffenen Business Services zu einem bestimmten Zeitpunkt mit CIs verknüpft, die mit angreifbaren Elementen verbunden sind. Weitere Informationen finden Sie unter Service-Mapping in Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Legen Sie die Anzahl der Zurückstellungen fest	Erfasst die Anzahl der Zurückstellungen eines angreifbaren Elements, eines angreifbaren Anwendungselements, eines angreifbaren Containerelements oder einer Korrekturaufgabe.
Löst die nächste Integration aus	Löst die nächste Integration in einer verketteten Integrationsausführung aus.
Vorlagenintegration	Beim erneuten Scannen wird ein einzelner Vorlagendatensatz an Tenable.io gesendet.
Aktualisiert nicht gruppierte angreifbare Elemente	Bestimmt, ob sich ein angreifbares Element in einer Korrekturaufgabe befindet , und fügt es der Liste **„Nicht gruppierte angreifbare Elemente“** hinzu oder entfernt sie daraus. **Hinweis:** Diese Aufgabe wird nach dem Upgrade ausgeführt und kann je nach Datensatz sehr lange dauern.
Schwachstelle in VG aktualisieren	Aktualisiert das Feld **„Schwachstelle“** in der Tabelle „Korrekturaufgabe“ (sn_vul_vulnerability) nach dem Upgrade. Dieser Auftrag wird einmal ausgelöst und ist danach inaktiv.
Vorlage für Schwachstellenimport	Engine, die die Importwarteschlange verarbeitet. Einer von 10
Geschlossenes Update für Vulnerability Response-Alter	Aktualisiert die Spalte „Alter geschlossen“ in der VI-Tabelle.
Anzahl der Vulnerability Response-CIs	Berechnet die Anzahl der CIs, die in den letzten 30 Tagen von Drittanbieter-Scannern gescannt wurden.
Vulnerability Response-Risiko- und Korrekturstatus-Upgrade	Aktualisiert die Risikobewertung für Daten, wenn Sie ein Upgrade durchführen.
v20.0: Ablaufdatum für Risikominderung	Überprüft, ob Ausgleichssteuerungen für ein angreifbares Element und eine Korrekturaufgabe abgelaufen sind. Wenn sie abgelaufen sind, wird die Risikopunktzahl auf die ursprüngliche Risikopunktzahl zurückgesetzt und eine E-Mail-Benachrichtigung gesendet, dass die Ausgleichssteuerungen abgelaufen sind. Versendet auch eine E-Mail-Benachrichtigung, wenn Ausgleichssteuerungen festgelegt werden, die innerhalb von 7 Tagen ablaufen sollen.

Installierte Tabellen

Tabelle	Beschreibung
v24.0.6 Import von Prisma-Hosts [sn_vul_prisma_hosts_import]	Importsatztabelle für die Hosts.
v24.0.6 Prisma-Hostattribute [sn_vul_prisma_host_attrb]	Asset-Attributtabelle für die Hostintegration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
v22.0 sn_vul_cmn_auto_close_rule	Schließt veraltete Erkennungen automatisch basierend auf Filterbedingungen.
sn_vul_cmn_ws_saved_filter	Speichert die Daten des gespeicherten Filters.
sn_vul_licensing_usage	Enthält das doppelte Asset, das unvollständige IP-Asset, die Gesamtanzahl der Scanner-Assets und die endgültige Nutzung.
sn_vul_m2m_entry_compersating_control	Stellt die Zuordnung zwischen Schwachstelleneinträgen und Ausgleichssteuerungen dar.
v21.0 Rapid7 Scan Engine [sn_vul_r7_scan_engine]	Speichern Sie die Datensätze, die von der Scan Engine importiert wurden, um Assets während eines Scans zu erkennen und auf Schwachstellen zu überprüfen.
v21.0 Import von Rapid7 Scan Engine [sn_vul_r7_scan_engine_import]	Wird von der Rapid7 Scan Engine-Integration verwendet, um Importdaten vor der Verarbeitung bereitzustellen.
Version 19.0: [sn_vul_veracode_cwe_import]	Erweitert die Veracode-Kategorietabelle für CWE-Korrekturempfehlungen.
Version 19.0: [sn_vul_veracode_category_import]	Speichert importierte Kategoriedaten.
Version 19.0: [sn_vul_veracode_sbom_import]	Speichert importierte SBOM-Daten, die aus Veracode stammen.
V17.1: Nachweis zum VI-Schlüssel hinzufügen sn_vul_Proof_key_vulnerability]	Rapid7-Schwachstellen, für die Nachweise im VI-Schlüssel enthalten sein müssen. Ab v24.0.6 von Vulnerability Responsewird die Spalte „Regulärer Ausdruck zur Aufteilung von Tenable-VITs“ hinzugefügt. Sie speichert den von einem Benutzer eingegebenen regulären Ausdruck, der zum Analysieren des Nachweises aus der Nutzlast verwendet wird.
Bewertete angreifbare Elemente [sn_vul_m2m_exp_sw_vi]	Weist einer Zuweisungsgruppe während der Erstellung der Korrekturaufgabe eine Korrekturaufgabe zu.
Zuweisungsregel sn_vul_vgr_assignment_rule	Weist einer Zuweisungsgruppe während der Erstellung der Korrekturaufgabe eine Korrekturaufgabe zu. Vor v15.0: Weist einer Zuweisungsgruppe während der Erstellung der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	Korrekturaufgabe] eine Korrekturaufgabe zu.
Change-Anforderung zuordnen [sn_vul_action_associate_cr]	Bereitstellungstabelle, die zur Verarbeitung neuer Korrekturaufgaben-CHG-Zuordnungen verwendet wird. Vor v15.0: Bereitstellungstabelle zur Verarbeitung neuer VG-CHG-Zuordnungen.
Asynchrone angreifbare Elemente Auftrag sn_vul_async_vi_job]	Enthält Hintergrundaufträge, die angreifbare Elemente verarbeiten. Es wird nur ein Auftragstyp unterstützt. Massenbearbeitung von Schwachstellen verwendet.
Typ des Auftrags für asynchrones angreifbares Element sn_vul_async_vi_job_type	Enthält die Typen von Hintergrundaufträgen und verweist auf das entsprechende Skript. Hat nur einen Prozessor, den **VulnerabilityBulkEditProcessor**
Veraltete Erkennungen automatisch schließen sn_vul_auto_close_config]	Speichert die Konfiguration für das automatische Schließen veralteter Erkennungen.
Granularität angreifbarer Elemente konfigurieren sn_vul_action_vi_granularity_config]	Speichert das UI-Formular, das zum Aktivieren oder Deaktivieren von „Port einschließen“ auf der Konfigurationsseite im Modul „VI-Granularität konfigurieren“ verwendet wird.
Change-Anforderungen erstellen sn_vul_action_create_cr]	Wird verwendet, um Change-Anforderungen aus einer Korrekturaufgabe zu erstellen.
Angreifbare Elemente erstellen [sn_vul_action_create_vi]	Eine Bereitstellungstabelle, die als Platzhalter für Informationen verwendet wird. Diese Tabelle speichert keine Datensätze.
Sammlung [sn_vul_patch_orch_collection]	Speichert Sammlungsdaten aus verschiedenen Instanzen.
CWE sn_vul_cwe	Katalog der Common Weakness and Enumeration-Softwareschwachstellen (CWE).
Anwendbare CWE-Plattform [sn_vul_cwe_m2m_cwe_platform]	Enthält die importierten anwendbaren CWE-Plattformdaten.
CWE-Kategorie	Enthält die importierten CWE-Kategoriedaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_vul_cwe_category]	
Häufige CWE-Konsequenz [sn_vul_cwe_consequenz]	Enthält die importierten allgemeinen CWE-Konsequenzdaten.
Externe CWE-Referenz sn_vul_cwe_reference	Enthält die importierten externen CWE-Referenzdaten.
Beispiel für CWE-Beobachtung [sn_vul_m2m_cwe_cve]	Enthält die importierten CWE-CVE-Daten.
CWE-Plattform sn_vul_cwe_platform	Enthält die importierten CWE-Plattformdaten.
Externe CWE-Referenz sn_vul_cwe_reference	Enthält die importierten CWE-bezogenen externen Referenzdaten.
CWE-Beziehung [sn_vul_m2m_cwe_relation]	Enthält die importierten CWE-Beziehungsdaten.
CWE-Ansicht sn_vul_cwe_view	Enthält die importierten CWE-Ansichtsdaten.
CWE-Schwäche sn_vul_cwe_weakness	Enthält die importierten CWE-Schwachstellendaten.
Version 16.1: Gerätesammlung [sn_vul_patch_orch_m2m_src_ci_collection]	Speichert Sammlungsdaten zu erkannten Elementen.
Version 16.1: Geräte-Update [sn_vul_patch_orch_m2m_src_ci_update]	Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in Datensätzen für erkannte Elemente angezeigt werden.
Übereinstimmung Discovery-Modell verwundbare Softw [sn_vul_discovery_model_software_match]	Ergänzt den Abgleich von angreifbarer Software mit einem Discovery-Modell.
Konfiguration für Ausnahmeverwaltung	Speichert die Konfigurationseinstellungen für die Ausnahmeverwaltungsfunktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vul_exception_config	
Ausnahmeregel sn_vul_auto_exception_rule	Enthält den Satz von Regeln, die für die Ausnahmeverwaltung ausgewertet wurden.
Exploit sn_vul_exploit	Enthält die Definitionen von Exploits: öffentlich verfügbarer Code, der eine Schwachstelle ausnutzt.
Exploit-Framework sn_vul_exploit_framework	Enthält die Namen von Exploit-Frameworks: vollständige Softwarepakete, die viele Exploits ausführen können.
Verfügbar gemachte Discovery-Modelle [sn_vul_m2m_exp_sw_model]	Speichert die Zuordnung zwischen dem Discovery-Modell und Schwachstellenbewertung Bewertung des Gefahrenpotenzials.
Bewertung des Gefahrenpotenzials [sn_vul_exp_by_sw]	Speichert die Datensätze für die Bewertung des Gefahrenpotenzials.
V19.0: Risikomanifest sn_vul_analyst_exposure_manifest	Manifesttabelle für die Delta-Verarbeitung.
Einträge zum Gefahrenpotenzial von Schwachstellen sn_vul_m2m_entry_exp]	Speichert die Zuordnung zwischen Schwachstelle (sn_vul_entry) und Bewertung des Gefahrenpotenzials.
Malware-Kit [sn_vul_malware_kit]	Enthält die Details von Malware-Kits: vorgefertigte Tools, die das Ausführen eines Exploits oder einer Reihe von zugehörigen Exploits ohne zusätzliche Codierungs- oder Konfigurationsarbeit erleichtern
Fehlende Asset-Tabelle [sn_vul_tenable_missing_asset]	Enthält temporäre Asset-IDs für ignorierte Compliancebewertungsdaten für Konfigurationen mit nicht abgeglichenen Assets.
Update der Microsoft Response Center-Lösung sn_vul_msrc_update	Enthält den Zeitpunkt der letzten Aktualisierung der Lösungsdaten durch Microsoft. Wird für den Vergleich mit dem nächtlichen Import verwendet, um die Delta-Daten zum Download zu bestimmen.
Microsoft Security Response Center Lösungsimport sn_vul_msrc_solution_import	Wird von der Integration der Microsoft Security Response Center-Lösung verwendet, um Importdaten vor der Verarbeitung bereitzustellen.
Integration der Microsoft Security Response Center-Lösung [sn_vul_msrc_integration]	Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_integration] für Integration der Microsoft Security Response Center-Lösung.
Nationale Verwundbarkeit – Datenbankeintrag [sn_vul_nvd_entry]	Dokumentierte Schwachstelle aus der US-Schwachstellendatenbank (National Vulnerability Database) des NIST.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
NVD-CVSS-Import [sn_vul_nvd_cvss_import]	Enthält Bereitstellungsdaten, die während des NVD-Imports noch nicht in das Schema Vulnerability Response transformiert wurden.
Version 16.1 [sn_vul_patch_orch.patch_approval_required]	Wenn Patch-Bereitstellungen über eine Patch-Integration geplant werden, werden Anforderungen zur Überprüfung und Genehmigung an Benutzer übermittelt, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind. Diese Eigenschaft ist standardmäßig aktiviert.
Version 16.1: Patch-Bereitstellung [sn_vul_patch_orch_deployment]	Speichert Informationen über bereitgestellte Patches für Sammlungen und CIs.
Version 16.1: Patch-Update sn_vul_patch_orch_update	Speichert Informationen zu den Patches, die auf verschiedenen Instanzen verfügbar sind.
Version 16.1: Potenzieller Patch [sn_vul_patch_orch_m2m_vuln_patch]	Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zum Beheben einer Schwachstelle verwendet werden können.
V19.0: Potenzielles Schwachstellenrisiko sn_vul_analyst_m2m_pot_exp_sw_model	Risikobewertungstabelle für CVE.
Produktkategorie sn_vul_product_category	Enthält die importierten Produktkategoriedaten.
Red Hat Security Advisory [sn_vul_rhsa_update]	Vergleicht die Lösungen Red Hat mit dem nächtlichen Auftrag, um die Delta-Daten für den Import zu bestimmen.
Red Hat Lösungsimporte sn_vul_rh_solution_import	Wird von Red Hat Solution Integration verwendet, um Importdaten vor der Verarbeitung bereitzustellen.
Red Hat Solution Integration sn_vul_rh_integration	Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_integration] für Red Hat Solution Integration.
Zugehörige Business-Services sn_vul_m2m_ci_services	Verknüpft CIs mit Business-Services, um die Suche nach betroffenen Services zu ermöglichen. Enthält eine Kennzeichnung, die angibt, ob sie von Service-Mapping hinzugefügt wurde.
V18.0: Anzahl der Korrekturmaßnahmen sn_vul_daily_count_re	Tägliche Anzahl der Korrekturmaßnahmen. Diese Tabelle wird täglich aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
V18.0: Datensatz der Korrekturmaßnahme sn_vul_remediation_effort_record]	Verfolgt den Korrekturfortschritt für Korrekturmaßnahmen (RE). Enthält Verweise auf die REs.
Korrekturzielregel sn_vul_ttr_rule	Definiert den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Elements. Erweitert die Anwendungsdatei.
V18.0: Korrekturaufgabe sn_vul_remediation_task]	Speichert alle Korrekturaufgaben für VR, AVR, CVR und Testergebnisgruppen. Besteht aus Informationen, die sich auf die Datensätze der Tabelle [sn_vul_vulnerability] beziehen. Benutzer, die in der Listenansicht der Tabelle [sn_vul_vulnerability] keine Datensätze anzeigen können, können die Informationen zu diesen Datensätzen in der Listenansicht der Tabelle [sn_vul_remediation_task] einsehen. Diese Tabelle ist für die Benutzer im Arbeitsbereich des Schwachstellenmanagers oder im Arbeitsbereich für IT-Korrekturen zugänglich
REST-Integration sn_vul_rest_integration	Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_integration] für REST-basierte Integrationen.
SAM NVD-Schwachstellenerkennung sn_vul_sam_config]	Enthält, welche CIs und Schwachstellen mit SAM NVD überwacht werden und ob die SAM NVD-Schwachstellenerkennung aktiviert ist oder nicht.
Geplanter Importpool [sn_vul_sched_import_pool]	Sammlung von Datensätzen für geplante Importsätze, die den gleichzeitigen Import von Datenquellen erleichtern.
Wählen Sie Angreifbares Element [sn_vul_action_select_vi]	Basisbereitstellungstabelle, die zum Umgang mit der Aufteilung der VG, zum Erstellen von CHGs und zum Zuordnen von CHGs verwendet wird
Setup-Status [sn_vul_setup_status]	Nur intern: Wird vom Setup-Assistenten verwendet. Wann immer der Setup-Assistent geöffnet wird, zeigt er den Status der Schritte Abgeschlossen an. Der Prozentsatz in der rechten oberen Ecke stammt aus dieser Tabelle.
Schweregradzuordnung [sn_vul_severity_map]	Enthält die Zuordnungen vom Quellschweregrad zum normalisierten Schweregrad.
Zuordnung für Lösungsscanner	Ordnet Lieferant, Scanner und Stichwörter für den Ausschluss oder Einschluss zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_vul_solution_scanner_mapping]	
Korrekturaufgabe aufteilen sn_vul_action_split_vg]	Bereitstellungstabelle für die Aufteilung von Korrekturaufgaben.
Eintrag für Drittpartei-Schwachstelle [sn_vul_ third_party_entry]	Dokumentierte Schwachstelle aus einer Drittanbieterquelle.
[sn_vul_tenable_io_template]	Ein Vorlagendatensatz wird an Tenable.io gesendet und dann während des erneuten Scannens für Elemente importiert, die Tenable.io als Quelle haben.
Manifest aktualisieren sn_vul_update_manifest	Liste von Korrekturaufgaben, die aktualisiert wurden und eine Neuberechnung durch den Rollup-Rechner erfordern.
V17.1: Nutzung nach CI-Klassen [sn_vul_licensing_usage_by_ci_classes]	Enthält die nach CI-Klasse aggregierte Verwendungsanzahl.
Anzahl der VR-Konfigurationselemente [sn_vul_vr_configuration_item_count]	Enthält den gleitenden kumulativen Durchschnitt für 90 Tage von Configuration Items, die aus Drittanbieterintegrationen importiert wurden.
Zuweisungsregel für Schwachstellen sn_vul_assignment_rule	Enthält den Satz von Regeln, die zum Festlegen der Zuweisungsgruppe auf VIs ausgewertet wurden.
Schwachstellen-Rechner sn_vul_calculator_group	Enthält die Regeln des Schwachstellen-Rechners. Die Reihenfolge der Rechner bestimmt, welcher Rechner zuerst ausgewertet wird, und in jedem Rechner wird höchstens eine Rechnerregel verwendet.
Regel des Schwachstellen-Rechners sn_vul_calculator]	Enthält die Regeln für alle Rechner. Für jeden Rechner werden die Rechnerregeln der Reihe nach überprüft. Der erste Rechner, der die Bedingung erfüllt, verwendet die Werte innerhalb dieser Regel.
Schwachstellen-CVEs sn_vul_m2m_entry_cve]	Verknüpft Daten von NVD Common Vulnerability Exposures (CVE) mit angreifbaren Einträgen.
Importwarteschlangeneintrag Schwachstellen-Datenquelle [sn_vul_ds_import_q_entry]	Warteschlange für Anhänge, bevor sie von einer Datenquelle verarbeitet werden. Wird von Schwachstellen-Integrationen verwendet.
Schwachstelleneintrag sn_vul_entry	Dokumentierte Schwachstelle.
Schwachstelleneintrags-Scan sn_vul_entry_scan	Speichert die Beziehung zwischen einem Scan und einem Schwachstelleneintrag.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Schwachstellen-Exploit-Framework sn_vul_m2m_framework_vul]	Enthält die Beziehung zwischen Exploit-Frameworks und Schwachstellen.
V19.0: Bewertung des Schwachstellenrisikos sn_vul_analyst_sam_config	Konfigurationstabelle der Risikobewertung für CVE.
Konfiguration der Schwachstellengranularität sn_vul_granularity_config]	Speichert und verwaltet den Status des Ein- oder Ausschlussports für das Modul „VI-Granularität konfigurieren“.
Korrekturaufgaben sn_vul_vulnerability	Sammlung von angreifbaren Elementen, die zur Korrektur organisiert wurden.
Change-Anforderungen für Korrekturaufgaben [sn_vul_m2m_vg_change_request]	Speichert die Zuordnung von Korrekturaufgaben und CHG-Anforderungen.
Korrekturaufgabenelemente [sn_vul_m2m_vul_group_item]	Zuordnung von Korrekturaufgaben und angreifbaren Elementen.
Regeln für Korrekturaufgaben sn_vul_grouping_rule	Enthält die Regeln, die die Kriterien definieren, mit denen Gruppen automatisch für einen Satz angreifbarer Elemente erstellt werden.
Integration von Sicherheitslücken sn_vul_integration	Planbarer Datensatz zum Importieren von Schwachstellendaten aus einer externen Quelle. Erweitert die geplante Skriptausführung.
Datenquelle Sicherheitslückenintegration sn_vul_int_data_src	Datenquelle, die mit einer Schwachstellenintegration verwendet werden soll.
Schwachstellenintegrationsprotokoll [sn_vul_integration_log]	Zeichnet Protokollinformationen auf, die von der Ausführung der Schwachstellenintegration ausgegeben werden.
Integrationsprozess für Schwachstellen sn_vul_integration_process	Einzelnes Prozessvorkommen für eine Schwachstellenintegration.
Warteschlange für Schwachstellenintegration sn_vul_integration_queue	Stellt die Importanforderungen für eine Integrationsausführung in die Warteschlange, wenn alle Datenquellen verwendet werden.
Ausführung der Schwachstellen-Integration	Aufrufe von Schwachstellenintegrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vul_integration_run	**Hinweis:** Wenn eine Integrationsausführung ausgeführt wird, kann sich im Backlog nur eine Integration im Status „Bereit“ befinden.
Statistiken zur Ausführung von Schwachstellenintegrationen sn_vul_integration_stats	Speichert die Aufgliederung jedes Schritts (z. B. REST-API-Zeit, VI-Erstellungszeit usw.) für eine Integrationsausführung
Aufgabe für angreifbares Element [sn_vul_m2m_item_task]	Angreifbare Elemente, die Problemen, Changes und Security Incidents zugeordnet sind.
Schwachstellen-Malware-Kit [sn_vul_m2m_malware_kit_vul]	Enthält die Beziehungen zwischen Schwachstellen und Malware-Kits.
Erforderliche Schwachstellenlösung [sn_vul_m2m_solution_prerequisite]	Enthält die quellenspezifischen Voraussetzungen für die Anwendung einer Lösung, falls verfügbar.
Schwachstellenquotengrenze sn_vul_rate_limit]	Definiert eine Quotenbegrenzung, die für einen Scanner verwendet werden soll.
Verwundbarkeitsreferenz sn_vul_reference	Externe Referenzen für bekannte Schwachstellen.
Status der Schwachstellenkorrektur [sn_vul_m2m_ttr_status]	Status des angreifbaren Elements im Vergleich zur nächsten angewendeten Korrekturzielregel.
Regel zum Schwachstellenrisiko sn_vul_calc_risk	Spezialisierte Rechnerregel, die mit den Risikopunktzahl-Rechnern verwendet wird. Verwendet Gewichtungen, die angeben, welche Werte, bezogen auf ein AE, zur Berechnung der Risikopunktzahl verwendet werden.
Rechner für Schwachstellen-Rollup sn_vul_rollup	Liste der Rechner für Schwachstellen-Rollup.
Schwachstellen-Scan sn_vul_scan	Schwachstellen-Scan. Enthält, was mit welchem Scanner gescannt werden soll, und eine Zusammenfassung der Scan-Ergebnisse.
Konfigurationselement für Schwachstellen-Scan [sn_vul_m2m_scan_configuration_item]	Ordnet CMDB-CIs zu, die sich in der Warteschlange zum Scannen befinden.
Warteschlangeneintrag für Schwachstellen-Scan [sn_vul_scan_q_entry]	Scandatensatz in der Warteschlange zum Scannen oder Verarbeiten. Erleichtert die Anforderungen innerhalb der angegebenen Quotengrenzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Quelle des Schwachstellen-Scans sn_vul_m2m_scan_source	Ordnet Quellen einem Scan-Datensatz zu und kennzeichnet alle Datensätze, die sich in der Warteschlange zum Scannen befinden.
Aufgabe des Schwachstellen-Scans [sn_vul_m2m_scan_vulnerability]	Ordnet Schwachstellenaufgaben für die Quellen eines Scan-Datensatzes zu.
Schwachstellenscanner [sn_vul_scanner]	Definiert für Scans zu verwendende Scanner von Drittparteien.
Quotenbegrenzung des Schwachstellenscanners [sn_cmn_scanner_rate_limit]	Ordnet einen Scanner einer Quotenbegrenzung zu.
Verwundbare Software [sn_vul_m2m_entry_software]	Enthält Zuordnungen zwischen Schwachstellen und angreifbarer Software.
Schwachstellenlösung sn_vul_solution	Enthält die Beziehungsdaten zwischen der Schwachstelle und den möglichen Lösungen dafür. Ab v24.0.6 von Vulnerability Responsewird dieser Tabelle eine neue Spalte mit dem Titel „Scanner-Bulletin“ hinzugefügt.
Schwachstellenlösung [sn_vul_m2m_vulnerability_solution]	Verknüpft die Tabelle „Schwachstelleneintrag“ (sn_vul_entry) mit der Tabelle „Schwachstellenlösung“ (sn_vul_solution).
Sicherheitsrisikostatus Change-Genehmigung sn_vul_change_approval	Verfolgt den Genehmigungsprozess für Schwachstellen.
Ersatzlösung für Schwachstelle [sn_vul_m2m_solution_supersedence]	Enthält die quellenspezifische Beziehung zwischen Lösungen.
Schwachstellenupdatemanifest [sn_vul_vuln_update]	Enthält eine Liste von Schwachstellen, deren Rollup-Daten aktualisiert werden müssen, nachdem ihre angreifbaren Elemente aktualisiert oder geschlossen wurden oder bei denen sich die Risikopunktzahl geändert hat.
Schwachstellenzuordnung für Lieferanten [sun_vul_vulnerability_vendor_mapping]	Enthält eine Liste von Schwachstellen und deren Lieferanten.
Angreifbares Element [sn_vul_vulnerable_item]	Enthält das Auftreten einer Schwachstelle für ein Konfigurationselement.
Erkennung von angreifbarem Element	Enthält die Erkennungen angreifbarer Elemente aus Drittanbieterintegrationen.

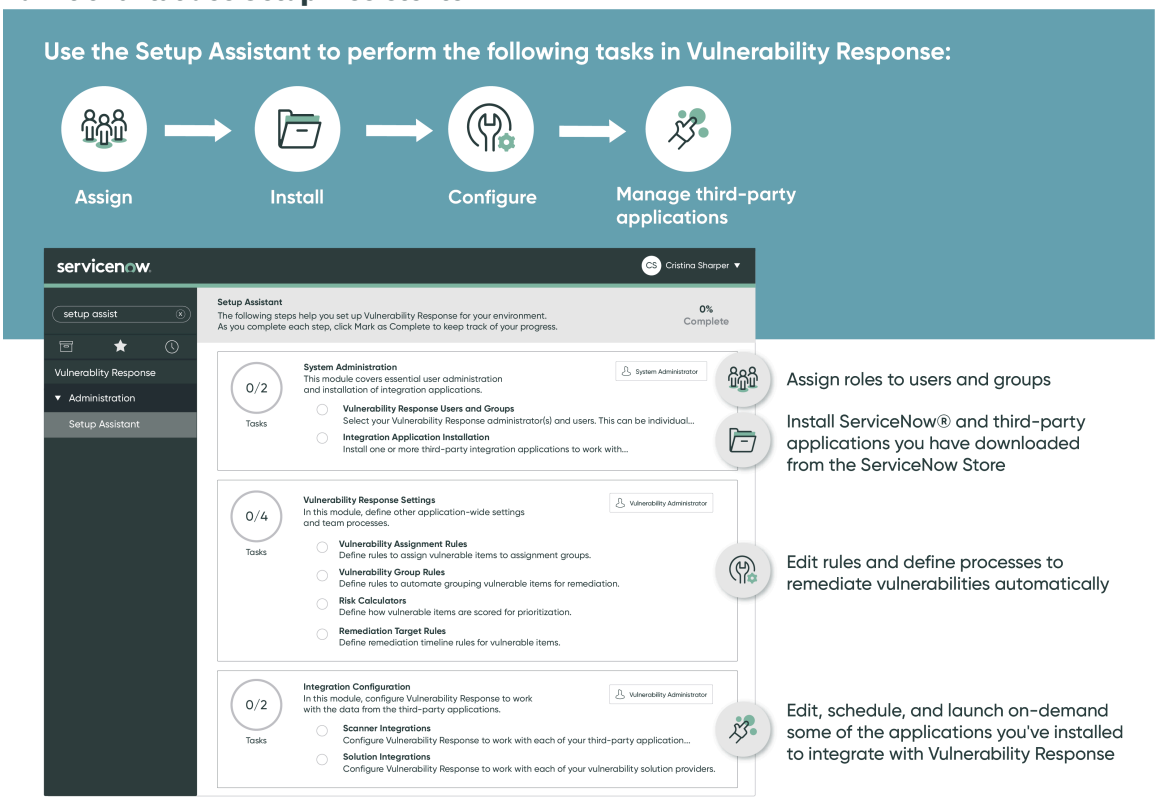
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vul_detection	
Software mit Schwachstellen [sn_vul_software]	Software, die bekanntermaßen bestimmte Schwachstellen aufweist.

Vulnerability Response mit dem Setup-Assistenten konfigurieren

Der Setup-Assistent führt Sie durch die Einrichtung von Vulnerability Response und bestimmten Drittanbieterintegrationen für Ihre Umgebung. Der Setup-Assistent bietet fast alles, was Sie zum Installieren und Einrichten Ihrer Umgebung benötigen, damit Sie Vulnerability Responseverwenden können.

Funktionalität des Setup-Assistenten



Now Platform® roles: admin and vulnerability admin

Zur Verwendung des Setup-Assistenten sind zwei verschiedene Now Platform® Rollen erforderlich: Administrator und Schwachstellen-Administrator.

Lesen Sie die folgenden Abschnitte, um die Anweisungen und Eingabeaufforderungen im Setup-Assistenten zu ergänzen.

Systemadministration: Weisen Sie Benutzer und Gruppen zu und installieren Sie Integrationsanwendungen

Erforderliche Rolle: admin

Eine Liste der Anwender und Integrationen ist vor Beginn dieser Aufgaben beim Schwachstellenmanager anzufordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.
2. Im ersten Abschnitt, Systemadministration, weist der Administrator Anwendern und Gruppen Rollen zu und installiert unterstützte Integrationen.

   Weisen Sie Anwendern und Gruppen im Setup-Assistenten Personae und Rollen Vulnerability Response zu.

   Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

3. Weisen Sie im Setup-Assistenten Rollen zu.
   - Weisen Sie Anwendern oder Gruppen die Rolle „sn_vul.admin“ zu.
   - Weisen Sie die Rolle „sn_vul.admin“ für die Verwaltung und Konfiguration von Vulnerability Response zu, einschließlich Schwachstellen-Integrationen, Regeln für Korrekturaufgaben, Rechnern und Regeln für die Korrekturzeit.
   - Weisen Sie die Rolle sn_vul_vulnerability_write für die Erstellung und Aktualisierung von Korrekturaufgaben und angreifbaren Elementen zu.

     Hinweis:
     Alle anderen Benutzer erhalten nur für Korrekturaufgaben, die ihnen zugewiesen sind, automatisch Schreibzugriff.

   - Weisen Sie die Rolle sn_vul_vulnerability_read zu, um Korrekturaufgaben, angreifbare Elemente und andere Schwachstelleninformationen anzuzeigen.

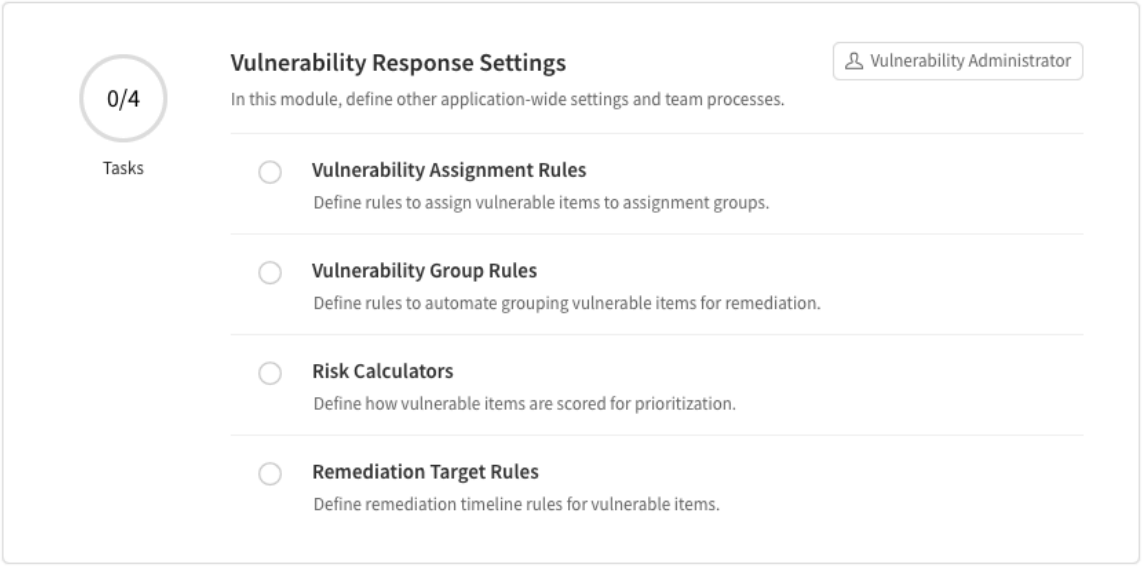
     Hinweis:
     Anwendern mit der Rolle itil wird automatisch die Rolle sn_vul.remediation_owner gewährt, mit der sie Korrekturaufgaben, zugewiesene angreifbare Elemente, Schwachstelleneinträge und Lösungen in der Anwendung Vulnerability Response in ihrer -Instanz und in der Anwendung Mobile Agent anzeigen können. Es ist keine zusätzliche Zuweisung erforderlich.

4. Installieren Sie Integrationsanwendungen von Drittparteien.
   - Unter Installation von Vulnerability Response und unterstützten Anwendungen und Vulnerability Response-Integrationen finden Sie weitere Informationen zu Anwendungen, die von Vulnerability Responseunterstützt werden.
   - Weitere Informationen zur Verwendung des Setup-Assistenten zum Installieren unterstützter Apps finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.

Vulnerability Response-Einstellungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In den Vulnerability Response-Einstellungen legt der Schwachstellenadministrator anwendungsweite Einstellungen sowie Regeln für Vulnerability Responsefest. Alternativ kann der Administrator diese Aufgaben ausführen.

1. Erstellen Sie Zuweisungsregeln für Schwachstellen.

Erstellen Sie Regeln, die die automatische Zuweisung von zu lösenden Korrekturaufgaben definieren. Mindestens eine Regel ist im Lieferumfang des Basissystems enthalten. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Hinweis:

Die Funktion zum erneuten Anwenden erfordert eine Baselineanwendung der Regeln. Sobald Ihre Regeln erstellt sind, aktivieren Sie die geplante Aufgabe *`Reapply all vulnerability assignment rules`*, um sie nach Belieben auszuführen. Andernfalls müssen Sie alle Regeln erneut auf alle offenen VIs anwenden, bevor Sie sie ändern.

Wenn der Auftrag abgeschlossen ist, legen Sie das Feld **Ausführen** in der geplanten Aufgabe entsprechend Ihrer Umgebung fest. Abhängig von der Anzahl Ihrer aktiven AEs kann deren tägliche Auswertung und Aktualisierung nicht unerhebliche Auswirkungen auf die Leistung haben. Erwägen Sie bei größeren Umgebungen eine Aktualisierung einmal pro Woche oder sogar einmal im Monat.

Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

2. Erstellen Sie Regeln für Korrekturaufgaben.

Erstellen Sie Regeln, die die automatische Erstellung von Korrekturaufgaben für die Lösung definieren. Mindestens eine Regel (**Schwachstelle)** ist im Lieferumfang des Basissystems enthalten. Sie können die Regeln aus dem Formular oder der Listenansicht erneut anwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn eine Gruppenregel gelöscht wird, können Sie im Formular oder in der Listenansicht alle **offenen** Gruppen löschen, die von dieser Regel erstellt wurden. Gruppen, die sich nicht im Status **„Offen“** befinden, werden ausgeschlossen.
- Weitere Informationen zum Erstellen von Regeln für Ihre Umgebung finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.
- Unter Die Anwendung Vulnerability Response erkunden finden Sie weitere Informationen zur Verwendung von Vulnerability Response zum Beheben von Schwachstellen.

3. Risikorechner erstellen und aktivieren.

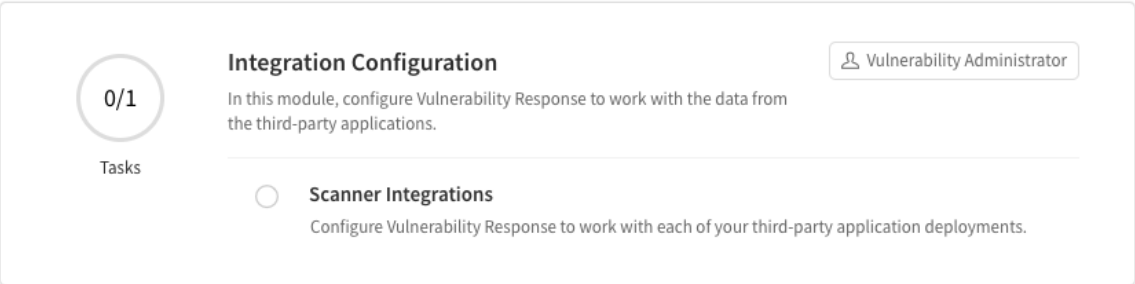
   Aktivieren Sie Risikorechner, die definieren, wie angreifbare Elemente für die Priorisierung bewertet werden. Mehrere Risikorechner sind im Lieferumfang des Basissystems enthalten. Informationen zum Erstellen oder Bearbeiten von Risikorechnern für Ihre Umgebung finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.

4. Erstellt Korrekturzielregeln.

   Erstellen Sie Korrekturzielregeln für Korrekturkategorien. Mindestens eine Regel ist im Lieferumfang des Basissystems enthalten. Weitere Informationen zum Erstellen von Regeln für Ihre Umgebung finden Sie unter Vulnerability Response Korrekturzielregeln.

Integrationskonfiguration

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin.



Im Abschnitt Integrationskonfiguration konfigurieren, planen, bearbeiten und starten Sie bei Bedarf die folgenden Integrationen von Drittpartei-Schwachstellenscannern und, wenn die Anwendung Solution Management for Vulnerability Response installiert ist, die Lösungsanbieter.

- Weitere Informationen zum Konfigurieren von Qualys Vulnerability Integrationfinden Sie unter Qualys Vulnerability Integration mit dem Setup-Assistenten konfigurieren.
- Die Konfiguration der Anwendung Vulnerability Response Integration with Tenable wird unterstützt. Siehe Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten.
- Nach der Installation der Anwendung Vulnerability Solution Management wird die Option **Lösungsintegrationen** unter **Scannerintegrationen**angezeigt. Klicken Sie auf **Lösungsintegrationen,** um in diesem Abschnitt des Setup-Assistenten Ihre installierten Anbieter von Schwachstellenlösungen zu konfigurieren. Red Hat Solution Integration und Integration der Microsoft Security Response Center-Lösung werden unterstützt.

  Weitere Informationen zu installierten Lösungen finden Sie unter Vulnerability Solution Management. Weitere Informationen zur Installation finden Sie unter Anwendung Solution Management for Vulnerability Response installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Konfigurieren Ihrer installierten Lösungen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

- Wenn eine Integration aus mehreren Quellen stammt, können Sie mehrere Bereitstellungen derselben Drittparteiintegration bereitstellen.
- Die Einstellungen aus der ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

Hinweis:
Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Daten aus jeder Drittanbieterintegration sind eindeutig identifiziert und in einer einzigen Instanz von Vulnerability Responseverfügbar.

Hinweis:
Mehrere Schwachstellen-Integrationen für Rapid7 InsightVM sind im Setup-Assistenten nicht verfügbar. Informationen zum Konfigurieren und Erstellen mehrerer Rapid7 InsightVM -Integrationen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration.

Zusätzliche Aufgaben

Unter Zusätzliche Setup- und Konfigurationsaufgaben für Vulnerability Response . finden Sie weitere Informationen zu Setupaufgaben, die nicht im Setup-Assistenten enthalten sind.

Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu

Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten Gruppen oder Anwendern zu.

Vorbereitungen
Wenn Sie in Vulnerability Response bereits mit dem Setup-Assistenten Persona-Rollen zugewiesen haben und weitere Informationen zum Bearbeiten und Verwalten Ihrer granularen Rollen und Rollenzuweisungen im Modul Benutzeradministration wünschen, lesen Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Responsenach.

Als Upgrade-Kunde können Sie Ihre vorhandenen Rollen für die Anwendung Vulnerability Response weiterhin verwenden. Der Zugriff für Anwender und Gruppen, denen in früheren Versionen von Vulnerability Response die Berechtigungen sn_vul.vulnerability_read und sn_vul.vulnerability_write und die Rollen für Korrekturbesitzer zugewiesen sind, hat sich nicht geändert.

Um jedoch mehr Kontrolle darüber zu haben, was Benutzer und Gruppen in der Anwendung Vulnerability Response auf Aufgabenebene tun und sehen können, bevorzugen Sie möglicherweise die Verwendung von Personas und granularen Rollen.

Wenn Sie die Persona-Rolle sn_vul.vulnerability_admin noch nicht mit dem Setup-Assistenten zugewiesen haben, führen Sie die folgenden Schritte aus, um sie zuzuweisen. Nach der Zuweisung ist der Schwachstellenadministrator mit dieser Persona-Rolle berechtigt, die Aufgaben des Setup-Assistenten nach dem ersten Abschnitt auszuführen und Regeln und Drittanbieterintegrationen in der Anwendung Vulnerability Response zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Übersicht über Persona-Rollen und granulare Rollen finden Sie unter Vulnerability Response Personae und granulare Rollen.

Wenn Sie ein Upgradekunde sind, verwenden Sie die folgende Tabelle als Referenz.

Vor v10.3	Ab v10.3
Wenn Sie sn_vul.admin zugewiesen haben	Möglicherweise möchten Sie Benutzern oder Gruppen „sn_vul.vulnerability_admin – Schwachstellenadministrator“ zuweisen. Benutzer mit dieser Rolle haben vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Benutzer mit dieser Rolle können alle VR-Anwendungen und Regeln konfigurieren und Drittanbieterintegrationen installieren.
Wenn Sie sn_vulnerability_write für Benutzer und Gruppen zugewiesen haben.	Unter Umständen möchten Sie Benutzern und Gruppen „sn_vul.vulnerability_analyst – Schwachstellenanalyst“ zuweisen. Anwender und Gruppen mit dieser Rolle können alle Datensätze für die VI-Korrektur anzeigen und aktualisieren.
Wenn Sie sn_vul.remediation_owner zugewiesen haben	Möglicherweise möchten Sie Anwendern und Gruppen „sn_vul.remediation_owner – Korrekturbesitzer“ zuweisen. Benutzer und Gruppen mit dieser Rolle beheben Schwachstellen, die ihnen oder einer Gruppe, der sie angehören, zugewiesen werden. Gruppen oder Anwender mit dieser Rolle können die ihnen oder einer Gruppe, der sie angehören, zugewiesenen Datensätze anzeigen und aktualisieren.
Wenn Sie sn_vul.admin für die Verwaltung von nicht abgeglichenen Configuration Items (CI) zugewiesen haben	Unter Umständen möchten Sie Anwendern und Gruppen den CI-Manager sn_vul.ci zuweisen. Anwender und Gruppen mit dieser Rolle verwalten nicht abgeglichene Configuration Items (CIs), die nicht in der Configuration Management Database (CMDB) gefunden wurden. Gruppen oder Anwender mit dieser Rolle aktualisieren erkannte Elemente.
Wenn Sie sn_vul.admin für Zurückstellungen und Ausnahmegenehmigungen zugewiesen haben.	Möglicherweise möchten Sie Anwendern und Gruppen „sn_vul.exception_approver - Ausnahmegenehmiger“ zuweisen. Benutzer und Gruppen mit dieser Rolle genehmigen Ausnahmen, Zurückstellungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vor v10.3	Ab v10.3
	und Abschlüsse von Korrekturaufgaben und angreifbaren Elementen. Ab v20.0 wird die granulare Rolle sn_vul.read_all für diese Rolle entfernt, sodass Sie auf die Ihnen und Ihrer Gruppe zugewiesenen angreifbaren Elemente und Korrekturaufgaben zugreifen können, anstatt auf alle angreifbaren Elemente und Korrekturaufgaben.
Wenn Sie sn_vul.vulnerability_read zugewiesen haben, um Einblick in das Schwachstellenmanagement zu gewähren.	Unter Umständen möchten Sie bestimmten Bereichen in der Anwendung Lesezugriff nach Aufgabe zuweisen. Weisen Sie beispielsweise sn_vul.read_all zu, damit ein Benutzer alle VR-Datensätze anzeigen kann. Für Lesezugriff zum Anzeigen von Regeln für Korrekturaufgaben weisen Sie „sn_vul.read_group_rules“ zu. Anwender und Gruppen mit dieser Rolle aktualisieren keine Datensätze.

Um die granularen Rollen anzuzeigen, die ein Benutzer oder Gruppen mit einer Persona-Rolle standardmäßig erben, navigieren Sie zu **Alle** > **Anwenderadministration** > **Rollen**. Suchen Sie die gewünschte Rolle, und klicken Sie darauf, um den Datensatz zu öffnen. Auf der Registerkarte Enthält Rollen werden alle granularen Rollen der Persona-Rolle sowie alle geerbten Rollen aufgelistet.

Unter Umständen möchten Sie sich vergewissern, dass Sie alle erforderlichen Benutzer und Gruppen erstellt haben, bevor Sie im Setup-Assistenten Rollen zuweisen. Alternativ können Sie zum Hinzufügen neuer Benutzer und Gruppen aus dem Setup-Assistenten auf den Link **Benutzeradministration** im Formular klicken, das in der folgenden Abbildung dargestellt wird.

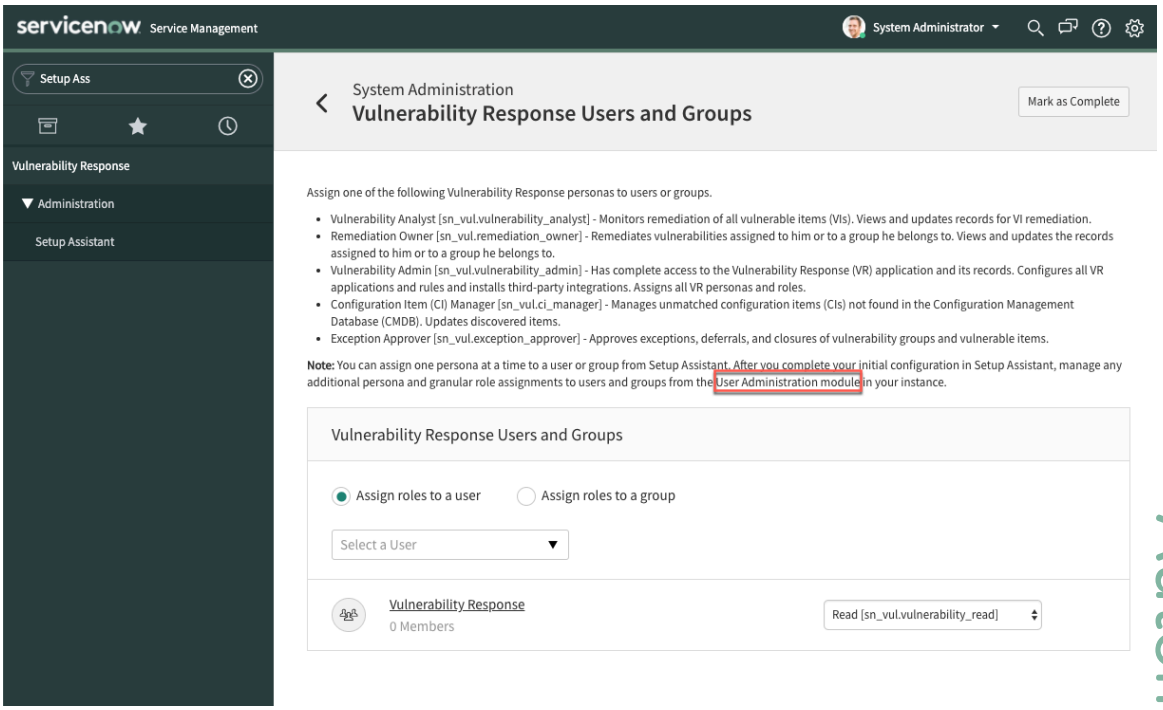
Im folgenden Beispiel wird beschrieben, wie ein Benutzer mit der Schwachstellen-Administratorpersona zugewiesen wird, um den Zugriff auf die Anwendung Vulnerability Response einzuschränken. Normalerweise können Sie Gruppen andere Persona-Rollen als sn_vul.vulnerability_admin zuweisen.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration Setup-Assistent**.
   Die Seite „Setup-Assistent“ wird angezeigt.
2. Klicken Sie auf Vulnerability Response Anwender und Gruppen.
   Die Seite „Systemverwaltung – Vulnerability Response-Anwender und -Gruppen“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie Rollen einem Anwender zuweisen aus, und wählen Sie einen vorhandenen Anwender aus der Liste aus.

   Sie können nur einen Anwender oder eine Gruppe mit einer Persona-Rolle zuweisen.

   Nachdem Sie auf der rechten Seite des Formulars einen Benutzer oder eine Gruppe ausgewählt haben, wird die Standardpersona Korrekturbesitzer [sn_vul.remediation_owner] standardmäßig zugewiesen und bleibt in der Liste angezeigt, bis Sie sie ändern.

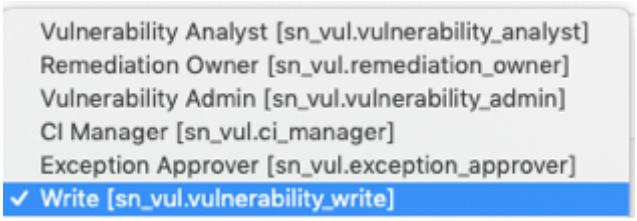
   Hinweis:
   Wenn Sie ein Upgrade auf eine neuere Version von Vulnerability Response durchführen und die Rolle sn_vul.vulnerability_read oder sn_vul.vulnerability_write vor dem Upgrade einem Benutzer oder einer Gruppe zugewiesen haben, wird sie zusammen mit den neuen Persona-Rollen angezeigt (siehe folgende Abbildung). .

   Als Upgrade-Kunde können Sie Ihre vorhandenen Rollen für die Anwendung Vulnerability Response weiterhin verwenden. Der Zugriff für Anwender und Gruppen, denen vor v10.3 die Berechtigungen „sn_vul.vulnerability_read“ und „sn_vul.vulnerability_write“ und der Nachbesserungsbesitzer zugewiesen wurden, hat sich nicht geändert.

   Beachten Sie, dass für vorhandene Benutzer oder Gruppen, denen derzeit die Rollen sn_vul.vulnerability_read oder sn_vul.vulnerability_write zugewiesen sind, diese Rollen zusammen mit den Persona-Rollen in der Liste angezeigt werden. Sobald Sie eine Persona-Rolle zugewiesen haben, ist die alte Rolle in Zukunft nicht mehr verfügbar. Wie in der folgenden Abbildung dargestellt, wird beispielsweise die Rolle „Schreiben“ [sn_vul.vulnerability_write] nicht mehr als Option für diesen Benutzer oder diese Gruppe angezeigt, nachdem ihm bzw. ihr eine der Persona-Rollen zugewiesen wurde.

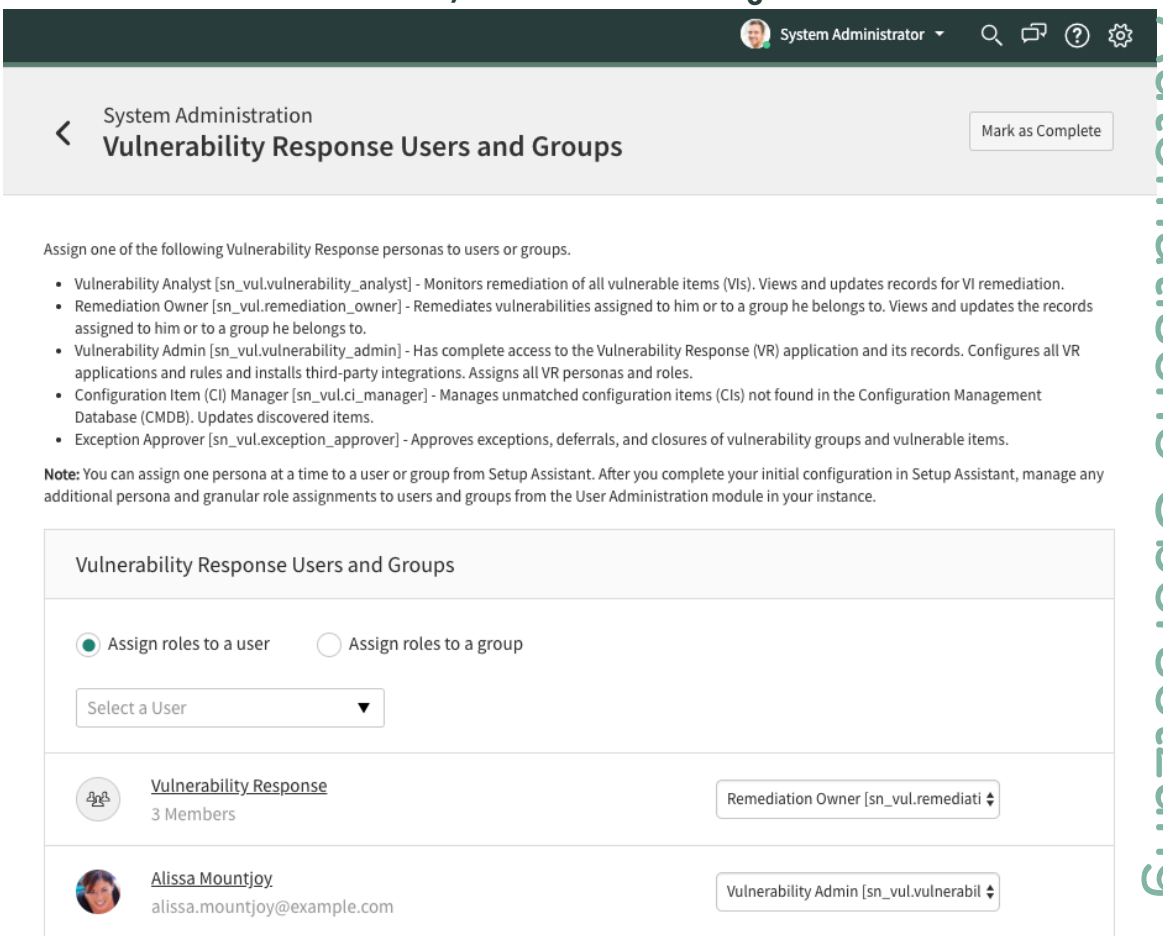
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie in der Liste rechts im Formular **den Eintrag Schwachstellenadministrator [sn_vul.vulnerability_admin]**aus.
   Es wird eine Nachricht angezeigt, die anzeigt, dass der Benutzer oder die Gruppe erfolgreich mit der Persona zugewiesen wurde.

Persona des Korrekturbesitzers, die einer Gruppe zugewiesen ist, und Persona des Schwachstellenadministrators, die einem Benutzer zugewiesen ist



5. Verwenden Sie die Beschreibungen der oben aufgeführten Persona-Rollen und weisen Sie den verbleibenden Persona-Rollen weiterhin Benutzer und Gruppen zu: Korrekturbesitzer, Schwachstellenanalyst, CI-Manager und Ausnahmegenehmiger.
   Sie haben die Zuweisung von Persona-Rollen zu Anwendern und Gruppen mit dem Setup-Assistenten erfolgreich abgeschlossen.
6. **Wahlweise:** Um die Anwender in einer Gruppe im Setup-Assistenten zu bearbeiten, gehen Sie wie folgt vor.

   a. Klicken Sie bei angezeigter Gruppe im Formular auf den Namen der Gruppe, die Sie bearbeiten möchten.
   Der Gruppendatensatz wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Klicken Sie bei ausgewählter Registerkarte Gruppenmitglieder auf **Bearbeiten**.
Das Formular „Mitglieder bearbeiten“ wird angezeigt

c. Verwenden Sie den Slushbucket, um Benutzer auszuwählen oder zu entfernen.

d. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern und zum Gruppendatensatz zurückzukehren.

e. Klicken Sie auf **Aktualisieren**, um zum Setup-Assistenten zurückzukehren.

f. Klicken Sie auf der Seite „Setup-Assistent“ auf **Vulnerability Response-Anwender und -Gruppen,** um mit der Konfiguration im Setup-Assistenten fortzufahren.

Nächste Maßnahme

Fahren Sie als Systemadministrator mit der Konfiguration von Vulnerability Response im Setup-Assistenten fort. Beachten Sie, dass Sie nach Abschluss des ersten Abschnitts einen Benutzer, dem Sie die Persona-Rolle des Schwachstellen-Administrators zugewiesen haben, die Aufgaben im Setup-Assistenten ausführen lassen können. Weitere Informationen zum Verwalten granularer Rollen und Beispiele finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Verwalten Sie Personas und granulare Rollen für Vulnerability Response

Nachdem Sie die erstmalige Zuweisung von Persona-Rollen mit dem Setup-Assistenten abgeschlossen haben, verwalten Sie zusätzliche granulare Rollenzuweisungen zu Anwendern oder Gruppen über das Modul „Benutzeradministration“ in Ihrer Instanz.

Vorbereitungen

Wenn Sie die Ersteinrichtung und Konfiguration für Vulnerability Response mit dem Setup-Assistenten noch nicht abgeschlossen oder Benutzern und Gruppen Persona-Rollen zugewiesen haben, navigieren Sie zu **Vulnerability Response** > **Administration** > **Setup-Assistent**. Weitere Informationen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Wichtige Begriffe und eine Übersicht über Persona-Rollen finden Sie unter Vulnerability Response Personae und granulare Rollen.

Eine Persona-Rolle ist eine vorkonfigurierte Rolle in der -Anwendung, die aus mehreren granularen Rollen besteht. Die Persona-Rollen in Setup-Assistent, Schwachstellenadministrator, Schwachstellenanalyst, Korrekturbesitzer, Konfigurationselement-Manager und Ausnahmemanager entsprechen allgemeinen Berufsbezeichnungen für Manager, Analysten und Serviceverantwortliche in einer IT-Organisation oder einer Schwachstellenkorrekturgruppe.

Wenn Sie möchten, dass Ihre Benutzer und Gruppen mehr Zugriff haben, als eine der Rollen zulässt, können Sie den Benutzern und Gruppen granulare Rollen hinzufügen. Umgekehrt können Sie granulare Rollen entfernen, wenn Sie den Zugriff für bestimmte Benutzer und Gruppen auf Aufgabenebene einschränken möchten. Außerdem können Sie anwenderdefinierte Rollen erstellen, die Ihren Anforderungen entsprechen.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um granulare Rollen für Anwender und Gruppen zu verwalten, wählen Sie eine aus, um fortzufahren.

   Die Namen der granularen Rollen in Vulnerability Response beschreiben normalerweise, was Benutzer tun und sehen können. Um Beschreibungen bestimmter granularer Rollen anzuzeigen, navigieren Sie zu **Alle** > **Anwenderadministration** > **Rollen** und suchen Sie die gewünschte Rolle. Rollenbeschreibungen, Rollen, die beim Zuweisen einer Rolle automatisch geerbt werden, und alle Rollen, die von anderen Rollen abhängen, sind ebenfalls aufgelistet.

2. Führen Sie die folgenden Schritte aus, um einem Anwender oder einer Gruppe eine granulare Rolle zuzuweisen oder zu entfernen.
   Angenommen, Sie möchten einem IT-Manager eine Rolle zuweisen, die es ihm ermöglicht, Datensätze anzuzeigen, aber nicht zu aktualisieren oder zu bearbeiten. Um Datensätze in Vulnerability Response, Performance Analytics for Vulnerability Responseund für alle Drittanbieterintegrationen anzuzeigen, weisen Sie diesem Anwender die granulare Rolle sn_vul.read_all zu.

   a. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**.

   b. Suchen Sie den Anwender, und klicken Sie in der Spalte Name auf den Datensatz, um ihn zu öffnen.
   Der Datensatz des Benutzers wird angezeigt.

   c. Wenn dies nicht ausgewählt ist, wählen Sie die Registerkarte Rollen.
   Die dem Benutzer derzeit zugewiesenen Rollen werden angezeigt.

   d. Klicken Sie auf **Bearbeiten**.
   Das Formular „Mitglieder bearbeiten“ wird angezeigt.

   e. Geben Sie im Feld Sammlung des Slushbucket den Namen der Rolle ein, falls Sie ihn kennen, oder geben Sie `*sn_vul` ein, um nur die für Vulnerability Response verfügbaren granularen Rollen anzuzeigen.

   f. Suchen Sie sn_vul.read_all, und verschieben Sie sie in die Rollenliste.

   Hinweis:
   Verwenden Sie den gleichen Prozess, um bestimmte granulare Rollen von Benutzern im Slushbucket zu entfernen, indem Sie die Rolle aus der Liste „Rollen“ in die Liste „Sammlung“ verschieben.

   g. Klicken Sie auf **Speichern**.
   Der Benutzerdatensatz wird mit der neuen granularen Rolle angezeigt.

   h. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Liste „Benutzer“ zurückzukehren.
   Sie haben einem Anwender die Berechtigung zum Lesen, aber nicht Aktualisieren von Datensätzen in Vulnerability Response, Performance Analytics for Vulnerability Responseund für Drittanbieterintegrationen erteilt.

3. Führen Sie die folgenden Schritte aus, um eine Gruppe so zu bearbeiten, dass nur bestimmte Mitglieder über erweiterten Zugriff mit detaillierteren Rollen verfügen.
   Angenommen, Sie möchten bestimmten Anwendern in der Gruppe „Korrekturbesitzer“ (sn_vul.remediation_owner) erlauben, angreifbare Elemente manuell zu erstellen, möchten diese Berechtigung jedoch nicht auf alle Anwender in der Gruppe erweitern. Die Berechtigung zum manuellen Erstellen angreifbarer Elemente wird von der granularen Rolle sn_vul.create_vulnerable_items

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gewährt. Führen Sie die folgenden Schritte aus, um diese Berechtigung nur ausgewählten Anwendern aus dieser Gruppe zu erteilen.

a. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**.

b. Suchen Sie die Gruppe Korrekturbesitzer, und klicken Sie in der Spalte Name auf die Gruppe, um den Datensatz zu öffnen.
Der Gruppendatensatz wird angezeigt.

c. Wenn dies nicht ausgewählt ist, wählen Sie die Registerkarte Gruppenmitglieder.
Die aktuellen Mitglieder der Gruppe werden angezeigt.

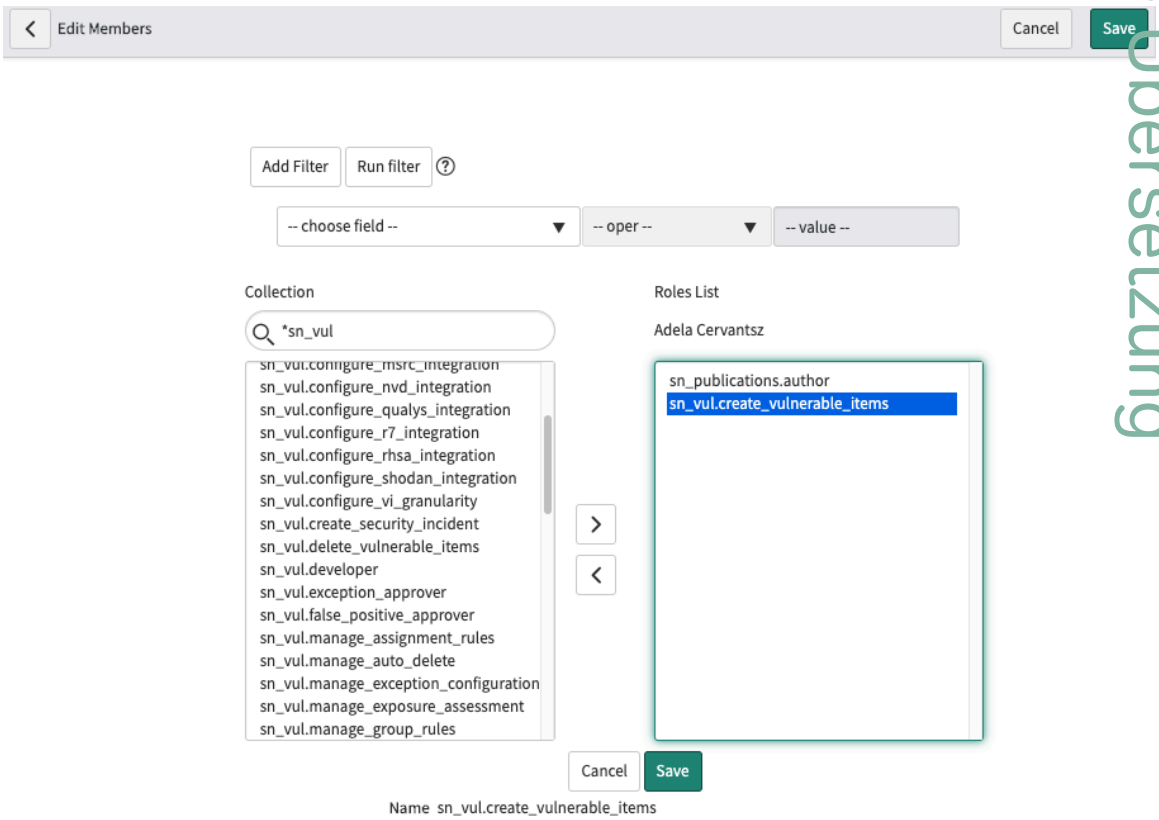
d. Klicken Sie auf einen Namen aus der Liste, der Sie die granulare Rolle zuweisen möchten, und öffnen Sie den Datensatz.

e. Scrollen Sie im Datensatz zur Registerkarte Rollen, und wählen Sie sie aus.
Die dem Benutzer zugewiesenen Rollen werden angezeigt.

f. Klicken Sie auf **Bearbeiten**.
Das Formular „Mitglieder bearbeiten“ wird angezeigt.

g. Geben Sie im Feld Sammlung den Namen der Rolle ein, falls Sie ihn kennen, oder geben Sie `*sn_vul` ein, um alle für Vulnerability Response verfügbaren granularen Rollen anzuzeigen.

h. Suchen und verschieben Sie sn_vul.create_vulnerable_items in die Rollenliste.



i. Klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Benutzerdatensatz wird mit der neuen granularen Rolle angezeigt.

j. Klicken Sie auf den Zurückpfeil, um zur Ansicht der Benutzer im Datensatz für die Gruppe Korrekturbesitzer zurückzukehren

k. Klicken Sie in der Liste, der Sie diese granulare Rolle zuweisen möchten, auf Namen, öffnen Sie die Datensätze, und verwenden Sie den Slushbucket, um die Rolle zuzuweisen.

l. Nachdem Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Gruppenliste zurückzukehren.
Sie haben einigen Anwendern in der Gruppe „Korrekturbesitzer“ (sn_vul.remediation_owner) die Berechtigung erteilt, angreifbare Elemente manuell zu erstellen.

4. Führen Sie die folgenden Schritte aus, um eine neue Rolle nur mit von Ihnen ausgewählten granularen Rollen zu erstellen.
Angenommen, Sie möchten eine Rolle für einen Compliance-Auditor erstellen. Diese Rolle arbeitet eng mit Governance, Risk, and Compliance (GRC) zusammen, und die Aufgabe erfordert die folgenden Berechtigungen und Aufgaben innerhalb von Vulnerability Response:

- Verwaltet Nachbesserungsfristen für angreifbare Elemente und Schwachstellen-Gruppen
- Genehmigt Ausnahmeanforderungen zum Verlängern von Fristen oder zum Zurückstellen der Remediation
- Verwaltet die Bereinigung älterer angreifbarer Elemente mit automatischer Löschung
- Definieren Sie Risikopunktzahlen
- Liest alle Datensätze in Vulnerability Response, kann sie jedoch nicht bearbeiten.

a. Navigieren zu **Alle** > **Anwenderadministration** > **Rollen**.

b. Klicken Sie in der Liste Rollen auf **Neu**.

c. Füllen Sie die Felder im Rollendatensatz aus.

Erstellen Sie einen Namen, wählen Sie die Anwendung aus, die diesen Datensatz enthält, und geben Sie eine Kurzbeschreibung für Ihre neue Rolle ein. Weitere Informationen zu den anderen Feldern im Formular finden Sie unter Rollen erstellen

Hinweis:
Wenn Sie einen Namen für Ihre neue Rolle erstellen, möchten Sie möglicherweise einen Namen verwenden, der in der Rollenliste leicht zu erkennen ist und die Funktionalität der Rolle beschreibt. Für dieses Beispiel bevorzugen Sie möglicherweise einen Titel wie „Compliance Auditor – GRC-VR“.

d. Klicken Sie auf **Absenden**.
Die Liste „Rollen“ wird angezeigt.

e. Suchen Sie Ihre neue Rolle, und klicken Sie darauf, um den Datensatz zu öffnen.

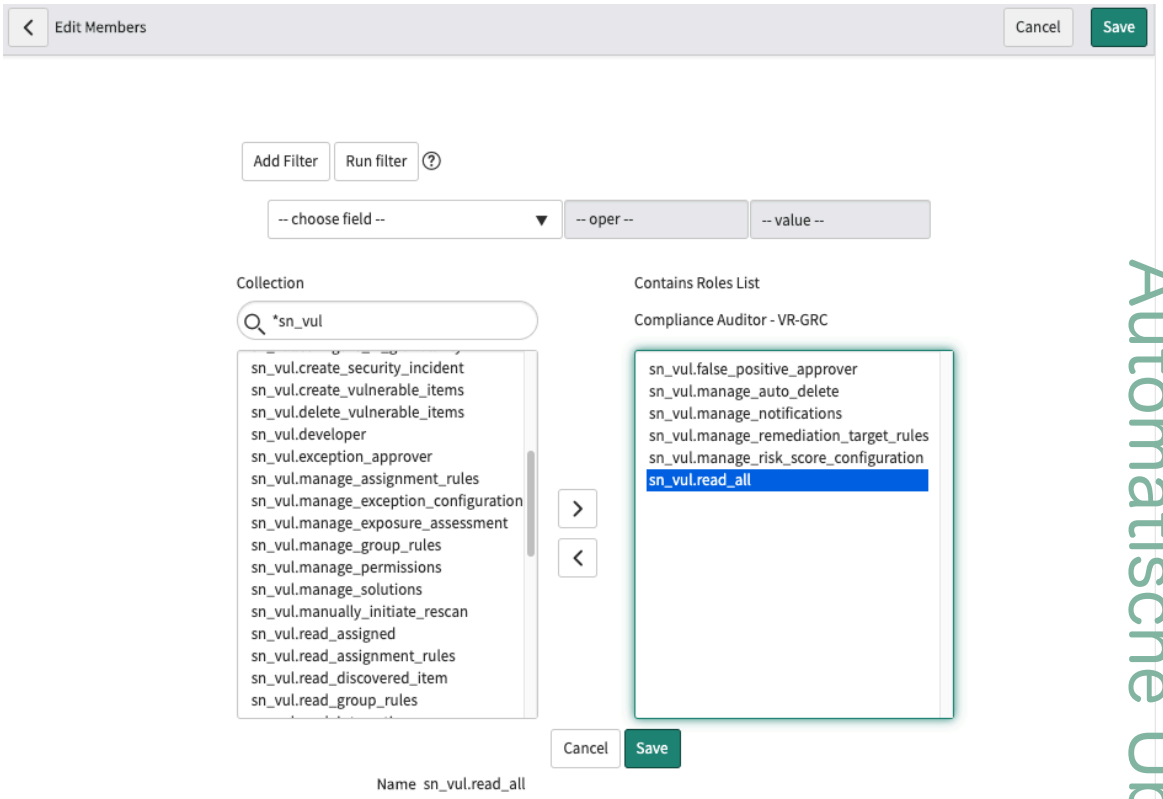
f. Klicken Sie auf **Bearbeiten**.
Das Formular „Mitglieder bearbeiten“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Verwenden Sie den Slushbucket, um Ihrer neuen Rolle granulare Rollen hinzuzufügen.

In diesem Beispiel werden die erforderlichen Rollen für diese neue Rolle in der rechten Spalte in der folgenden Abbildung angezeigt.

Um nur die granularen Rollen für Vulnerability Response anzuzeigen, geben Sie im Feld Sammlung den Text *sn_vulein.



h. Klicken Sie auf **Speichern**.
Der Datensatz für Ihre neue Rolle wird angezeigt. Beginnen Sie mit der Registerkarte Enthält Rollen und bearbeiten Sie die Rolle nach Bedarf.

i. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
Ihre neue Rolle wird in der Liste „Rollen“ angezeigt.

Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten

Installieren Sie die Integrationsanwendungen von Drittparteien, für die Sie berechtigt sind, in Vulnerability Response mit dem Setup-Assistenten.

Vorbereitungen

Der Setup-Assistent unterstützt die Installation der meisten Integrationsanwendungen von Drittparteien mit Vulnerability Response. Für einige Anwendungen müssen Sie jedoch mit der Konfiguration fortfahren, die Sie über Konfigurationsmodule in Ihrer Instanz installieren. Unter Vulnerability Response-Integrationen finden Sie eine Liste der Anwendungen, die von Vulnerability Responseunterstützt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

- Nach der Installation bietet die Funktion Vulnerability Solution Management von Vulnerability Response Zugriff auf Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration im Setup-Assistenten.
- Vulnerability Solution Management ist über ein separates Abonnement verfügbar. Unter Vulnerability Solution Management finden Sie weitere Informationen darüber, wie Vulnerability Response Lösungen integriert.

Bevor Sie Anwendungen von Drittanbietern über den Setup-Assistenten installieren und aktivieren können, führen Sie die folgenden Aufgaben aus, um eine reibungslose Installation zu gewährleisten:

Aufgaben einrichten	Beschreibung
Vergewissern Sie sich, dass Sie gültige Berechtigungen ServiceNow für die Integrationsanwendungen haben, die Sie installieren möchten.	Navigieren zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz, um Berechtigungen zu überprüfen. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Weitere Informationen zum Abrufen von Berechtigungen für eine Anwendung Security Operations aus ServiceNow Storefinden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab.
(Optional) Wenn die Anwendung noch nicht installiert und aktiviert ist, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren.	Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren und konfigurieren.
Wenn dies noch nicht installiert und aktiviert ist, müssen Sie Schwachstellendaten mit der geplanten Aufgabe „NVD-Integration und CWE“ aktivieren und importieren, bevor Sie die Scanner-Anwendung eines Drittanbieters ausführen, um Daten zu importieren.	Führen Sie die NVD- und CWE-Integrationen im Rahmen der Ersteinrichtung von Vulnerability Response und bevor Sie Schwachstellendaten mit dem Scannerprodukt eines Drittanbieters in Ihre Instanz importieren. Weitere Informationen finden Sie unter Grundlagen zu NVD-Integrationen.
Stellen Sie sicher, dass Sie alle Setupaufgaben abgeschlossen haben, die für die Integrationen von Drittparteien für Vulnerability Responseerforderlich sind.	Überprüfen Sie alle erforderlichen Setup-Aufgaben für jede Integration, die Sie unter Vulnerability Response-Integrationeninstallieren möchten.

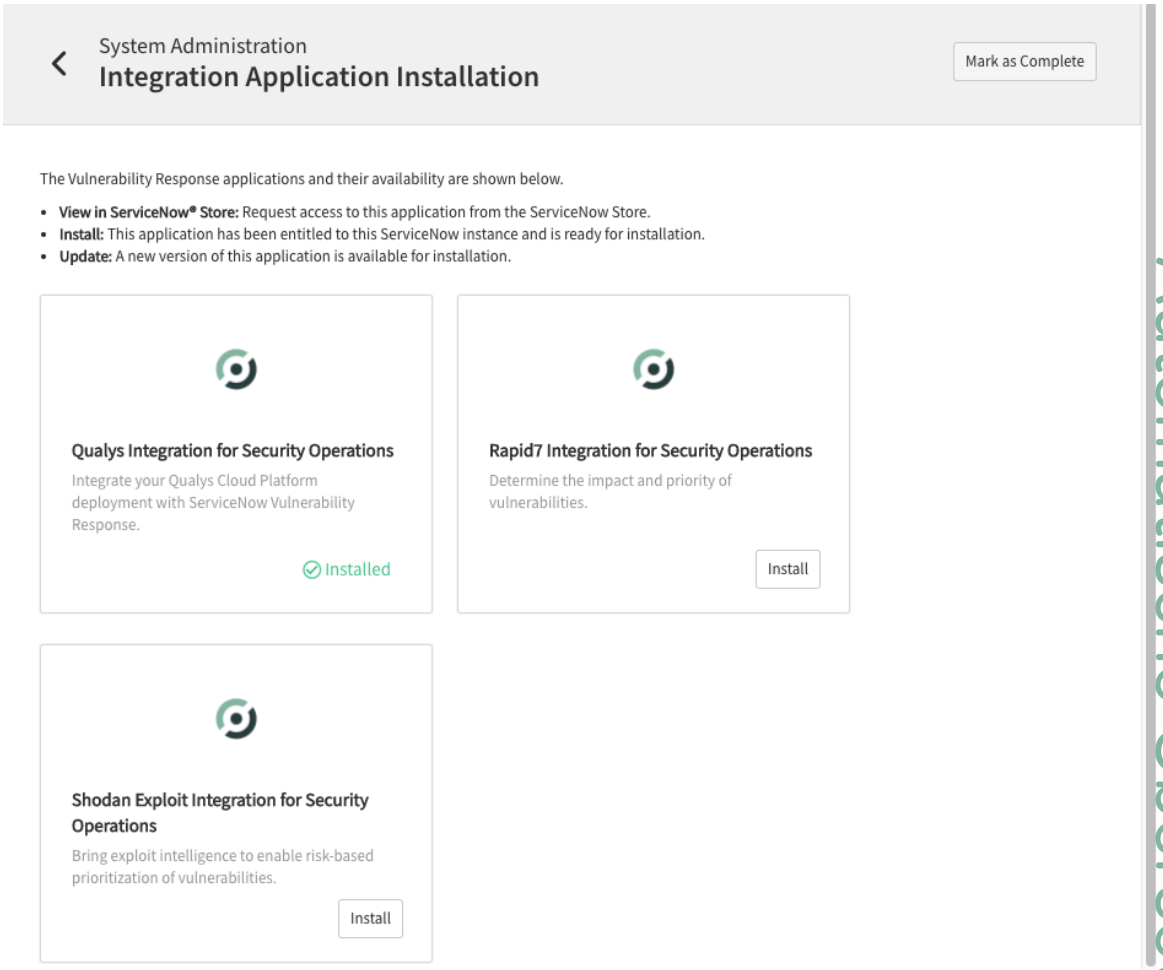
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Systemverwaltung** > **Installation der Integrationsanwendung**.

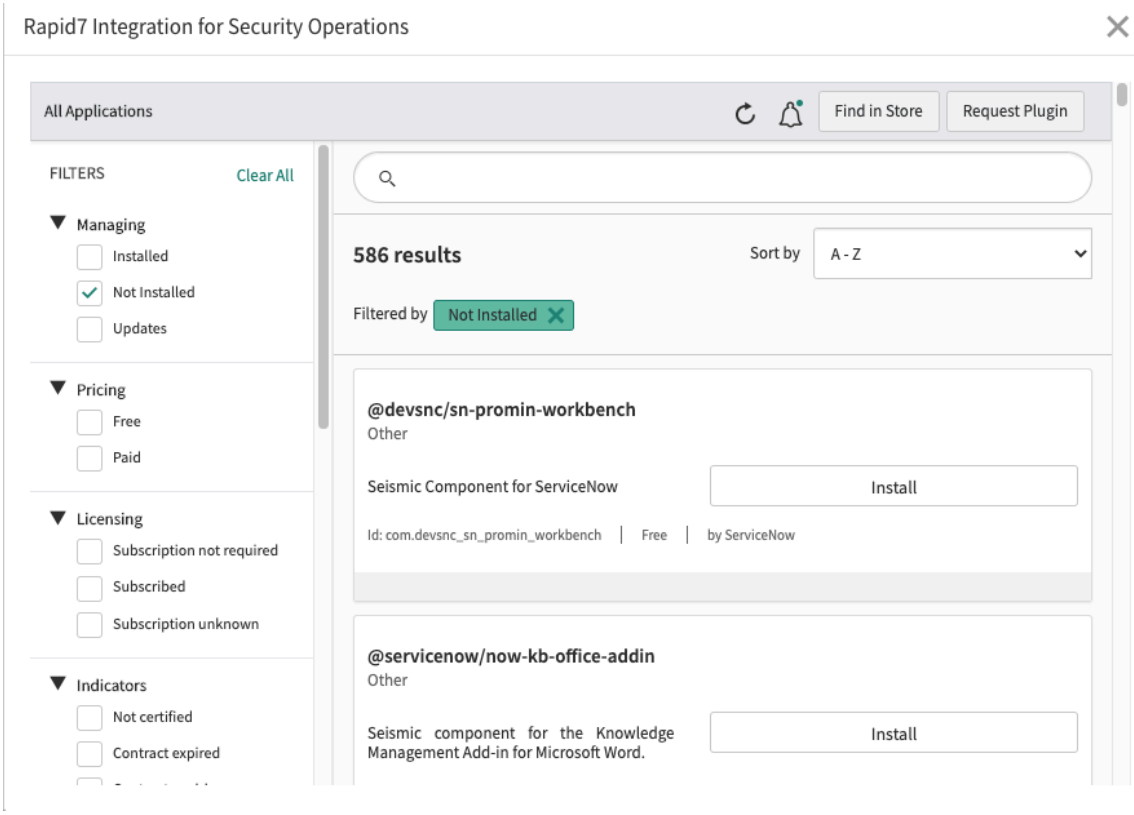
   Nach einigen Minuten werden die Anwendungen angezeigt, für die Sie berechtigt sind und die zur Installation in Ihrer Instanz von verfügbar sind.



2. Suchen Sie die Anwendung, die Sie installieren möchten, und klicken Sie auf der Anwendungskachel **auf Installieren**.
   Das Dialogfeld „Alle Anwendungen“ wird mit dem Namen der Anwendungskachel angezeigt, auf die Sie geklickt haben, z. B. Rapid7 Integration for Security Operations, (siehe folgende Abbildung).

Automatische Übersetzung

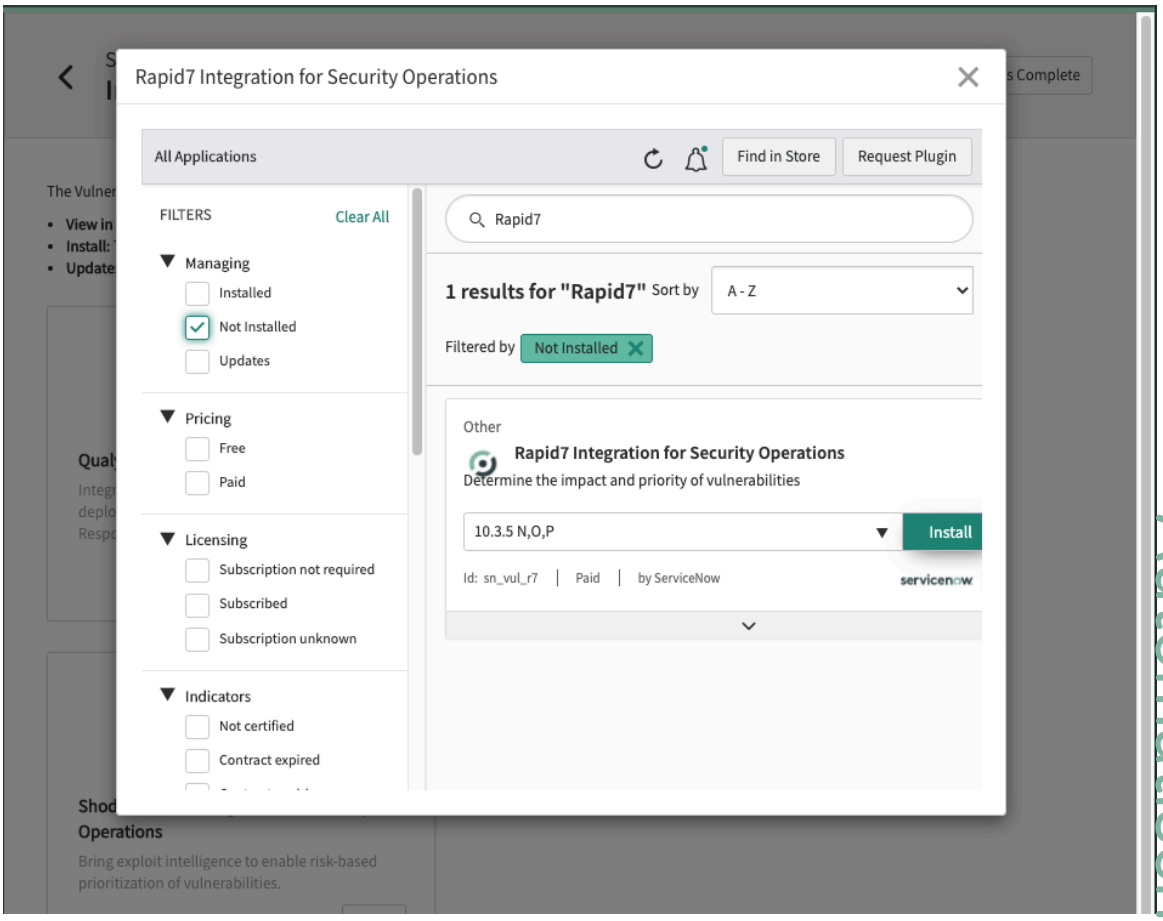
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Suchen Sie die Anwendung, wählen Sie in der Auswahlliste eine Version aus, und klicken Sie auf **Installieren**.

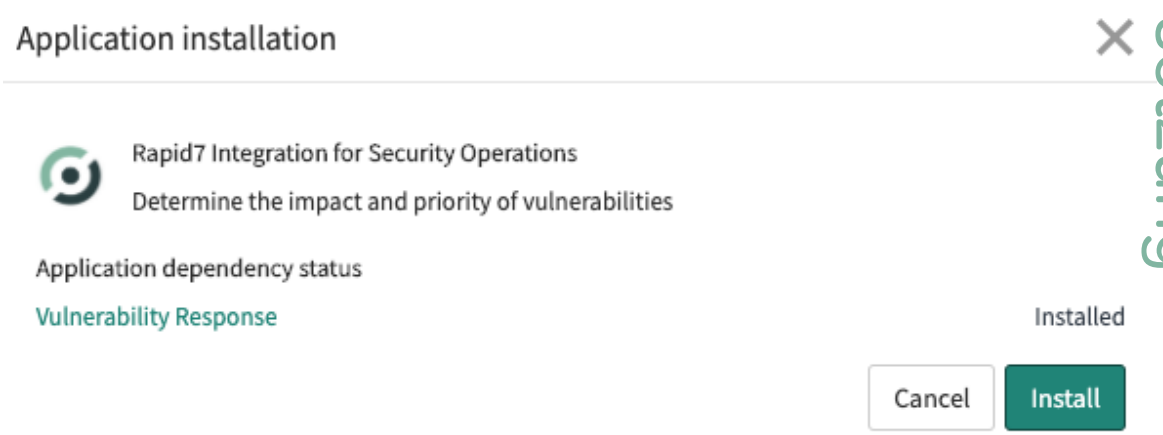
   Wenn ein Update für die Anwendung verfügbar ist, wird die Schaltfläche **Aktualisieren** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Dialogfeld „Anwendungsinstallation“ wird der Status der Anwendungsabhängigkeit angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.

4. Klicken Sie im Dialogfeld „Anwendungsinstallation“ auf **Installieren**.



Im Dialogfeld „Installieren“ wird angezeigt, wenn die Installation erfolgreich abgeschlossen wurde.

5. Schließen Sie das Dialogfeld.
Die Seite „Alle Anwendungen“ wird angezeigt, die zeigt, dass Ihre Anwendung erfolgreich installiert wurde.

Nach der Installation und Aktivierung können Sie die folgenden Anwendungen und installierten Lösungen direkt im Abschnitt „Integrationskonfiguration“ des Setup-Assistenten konfigurieren, planen und starten:

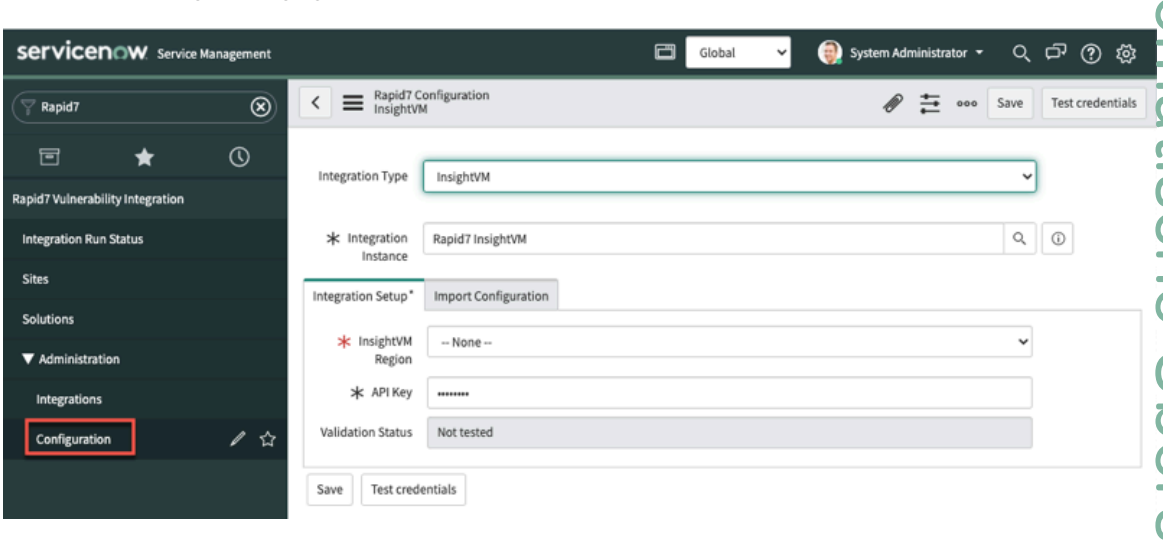
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Qualys Vulnerability Integration
- Vulnerability Response Integration with Tenable.
- Die Integration der Microsoft Security Response Center-Lösung
- Die Red Hat Solution Integration
- Integration der Microsoft Security Response Center-Lösung
- Die Microsoft Defender Threat and Vulnerability Management Integration

Navigieren Sie für andere Anwendungen, die oben nicht aufgeführt sind, direkt zum Konfigurationsmodul der Anwendung, um mit der Konfiguration fortzufahren und die erforderlichen Anmeldeinformationen von Drittparteien einzugeben. Die folgende Abbildung zeigt beispielsweise den Speicherort der Konfiguration und das Modul für die Anwendung Rapid7.

Weitere Informationen zum Konfigurieren bestimmter Anwendungen finden Sie in der Produktdokumentation zur Installation und Konfiguration nach Produktnamen, die für die einzelnen Anwendungen angegeben ist.



Nächste Maßnahme
Fahren Sie mit der Konfiguration Ihrer Anwendung im Setup-Assistenten fort, wenn Ihre Anwendung unterstützt wird.

Wenn die Konfiguration Ihrer Anwendung im Setup-Assistenten nicht unterstützt wird, navigieren Sie direkt zum Konfigurationsmodul der Anwendung, um mit der Konfiguration fortzufahren. Informationen zum Anzeigen unterstützter Anwendungen im Setup-Assistenten finden Sie unter Installation von Vulnerability Response und unterstützten Anwendungen.

Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien

Wenn noch nicht installiert, laden Sie die NVD-Integration herunter, führen Sie sie aus und führen Sie die geplante CWE-Aufgabe als Teil Ihres ersten Setups von Vulnerability Response und bevor Sie Schwachstellendaten mit einem Scannerprodukt eines Drittanbieters in Ihre Instanz importieren. Vulnerability Response Integration with NVD ist unter ServiceNow Storeverfügbar.

Erfassung von CWE- und NVD-Daten

Importierte Daten aus den NVD- und CWE-Integrationen werden verwendet, um die Schwachstellendaten in Ihrer Instanz anzureichern und Sie zu entscheiden, ob die Korrektur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für eine Schwachstelle, ein angreifbares Element oder eine Korrekturaufgabe eskaliert werden soll. Nach dem ersten Import können Sie Bibliotheksdatensätze bei Bedarf aktualisieren oder eine regelmäßige Aufgabe konfigurieren, um die Datensätze regelmäßig zu aktualisieren. Vulnerability Response speichert sie unter **Libraries**.

Das Common Vulnerability Bewertungssystem (CVSS), das in NVD- und Drittpartei-Einträgen enthalten ist, erfasst die Hauptmerkmale einer Schwachstelle. Vulnerability Response verwendet CVSS-Daten, um einen normalisierten Wert zu erstellen, der den Schweregrad der Schwachstelle widerspiegelt. Wenn der Schweregrad berechnet wird, ermöglicht die Schwachstelle ein besseres Verständnis des Risikos, das von dieser Schwachstelle für Ihre Organisation ausgeht. Der Schweregrad hilft Ihnen, die Nachbesserung von Schwachstellen zu bewerten und zu priorisieren.

Wenn dies Ihre erste Installation von Vulnerability Responseist oder bevor Sie zum ersten Mal Daten mit einem Scannerprodukt eines Drittanbieters erfassen:

1. Führen Sie einen ersten Import von CWE-Daten mit der CWE Comprehensive 2000 Integration durch.

   Weitere Informationen finden Sie unter Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus. Sie führen CWE-Aktualisierungen **bei Bedarf** standardmäßig über den Integrationsdatensatz durch und müssen sie konfigurieren, wenn sie als geplante Aufgabe ausgeführt werden sollen.

   Hinweis:
   Planen Sie die Ausführung des CWE-Updates vor dem Update der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**.

2. Stellen Sie sicher, dass die Anwendung Vulnerability Response Integration with NVD installiert ist und Daten aus der API-Integration der National Vulnerability Database des NIST (Nur CVE) oder der API-Integration der National Vulnerability Database des NIST (Nur CVE und CPE) erfolgreich importiert wurden.

   Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Nach der Installation wird die Integration der NIST National Vulnerability Database Integration – API (nur CVE) standardmäßig aktiviert. Sie wird täglich ausgeführt. Weitere Informationen finden Sie unter Grundlagen zu NVD-Integrationen und Installieren Sie die -Integration Vulnerability Response mit der US-Schwachstellendatenbank (National Vulnerability Database) des NIST.

3. Drittpartei-Bibliotheken werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

Importierte Schwachstellendaten und angreifbare Elemente werden angezeigt

Die folgenden Bibliotheken sind verfügbar:

Bibliotheken	Beschreibung
NVD	Liste der von NVD gefundenen Schwachstellen, einschließlich Sicherheitsprüflisten, sicherheitsbezogener Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits.
CWE	Liste der von der Community entwickelten Software-Schwachstellentypen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bibliotheken	Beschreibung
	Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Common Weakness Enumerations“ eskalieren, er dient nur zur Referenz.
Drittpartei	Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs.

Zugehörige Informationen

Zeigen Sie Schwachstellenbibliotheken Vulnerability Response an

Anwendung Solution Management for Vulnerability Response installieren

Bevor Sie die Funktion Solution Management for Vulnerability Response von Vulnerability Response in Ihrer -Instanz verwenden können, müssen Sie die Installation der Anwendung Vulnerability Solution Management abschließen. Diese Anwendung ist als separates Abonnement im ServiceNow Storeverfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Führen Sie diese Setupaufgaben aus, um eine reibungslose Installation zu gewährleisten.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration sind die Lösungsanwendungen, die nach der Installation von Solution Management for Vulnerability Response in Vulnerability Solution Managementverfügbar sind.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Solution Management for Vulnerability Response erfordert die Anwendung Vulnerability Response. Stellen Sie für die aktuelle Version von Vulnerability Solution Managementsicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben. Weitere Informationen finden Sie unter KB0856498 – Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen . Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass Sie berechtigt sind, auf die Anwendung zuzugreifen.	Um zu überprüfen, ob Sie berechtigt sind, für die Anwendung Vulnerability Solution Management berechtigt sind, navigieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wie Sie Berechtigungen für die Anwendung Vulnerability Solution Management von ServiceNow Store abrufen und in Ihre Instanz Now Platform herunterladen, erfahren Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab.
Stellen Sie sicher, dass Ihre NVD-Datensätze für die letzten 10 Jahre aktuell sind.	Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.
Stellen Sie sicher, dass Ihre Drittpartei-Schwachstellen auf dem neuesten Stand sind.	Informationen zu Schwachstellenintegrationen von Drittparteien finden Sie unter Vulnerability Response-Integrationen.
Vergewissern Sie sich, dass Ihrer Instanz die erforderlichen Rollen Now Platform zugewiesen sind.	Die folgenden Rollen sind für die Installation und Überprüfung der erwarteten Ergebnisse erforderlich: Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response. • Der Systemadministrator [admin] installiert die Anwendung. Wenn dies noch nicht geschehen ist, weist der Administrator die Rolle des Schwachstellen-Administrators [sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)] zu. • Der Schwachstellenadministrator überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: „admin“ zur Installation der Anwendung Vulnerability Solution Management und „vulnerability admin“ zur Konfiguration der Anwendung.

Prozedur

1. Navigieren Sie zum ServiceNow Store.
2. Klicken Sie auf **Anmelden**, und geben Sie Ihre HI-Anmeldeinformationen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die Registerkarte **ServiceNow-Produkte**, um die verfügbaren ServiceNow -Produkte anzuzeigen.
4. Klicken Sie auf das Pluszeichen (**+**) neben **Vulnerability Solution Management,** um alle zugehörigen Anwendungen anzuzeigen, für die Sie berechtigt sind.
5. Klicken Sie **auf Aktivieren,** um zu überprüfen, ob Sie die Berechtigung zum Zugriff auf Vulnerability Solution Management für die Anwendung haben.
6. Wenn Sie bereits über die -Berechtigung verfügen, fahren Sie mit Schritt 10 fort, um die Anwendung in Ihrer Instanz Now Platform zu installieren.
7. Aktivieren Sie das Kontrollkästchen, und klicken Sie bei der Eingabeaufforderung auf **Akzeptieren**, um den Nutzungsbedingungen zuzustimmen.
   Es wird eine Meldung angezeigt, dass Sie sich erfolgreich für die Anwendung entschieden haben.
8. **Wahlweise:** Klicken Sie auf Berechtigung verwalten, wenn Sie Ihre Berechtigung für Vulnerability Solution Management in anderen Now Platform -Instanzen verwalten möchten.

   Hinweis:
   Wenn die Schaltfläche **Berechtigung verwalten** nicht angezeigt wird, klicken Sie in der Produktliste auf die Anwendung **Vulnerability Solution Management,** um sie anzuzeigen.

   a. Option wählen

   b. Klicken Sie auf **OK** oder **Abbrechen,** um fortzufahren.
      Sie können nun Plugins aktivieren und die Anwendung in Ihren Instanzen installieren.

9. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Vulnerability Solution Management installieren möchten.
10. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
11. Suchen Sie die Anwendung Vulnerability Solution Management (sn_vul_solution), und klicken Sie auf **Installieren**.
    Im Dialogfeld „Anwendungsinstallation“ wird der Status des Anwendungsabhängigkeits-Plugins angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.
12. Klicken Sie auf **Installieren**.
    Diese Installation kann einige Zeit in Anspruch nehmen. Nachdem die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden, wird im Dialogfeld „Installieren“ eine Meldung angezeigt.

    Der Schwachstellenadministrator kann die Anwendung jetzt im Setup-Assistenten konfigurieren.

13. Klicken Sie auf **Schließen**.

    Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration sind die Lösungsanwendungen, die nach der Installation von Solution Management for Vulnerability Response in Vulnerability Solution Managementverfügbar sind.

    Zeigen Sie die Schwachstellenlösungen an, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen**. Weitere Informationen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Nachdem Sie die Anwendung und die verfügbaren Lösungen konfiguriert haben, überprüfen Sie mithilfe der Tabelle „Schwachstellenlösung“ [sn_vul_m2m_vulnerability_solution], ob CVEs und Lösungen übereinstimmen.

Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA].

Bevor Sie die Anwendung Performance Analytics for Vulnerability Response verwenden können, müssen Sie die Berechtigung von erhalten und die Anwendung von ServiceNow Storeherunterladen, in Ihrer Instanz Now Platform® von installieren und einige Installations- und Konfigurationsschritte ausführen. Die PA-Anwendung wird nicht als Teil der Anwendung Vulnerability Response installiert. Sie ist als separates Abonnement verfügbar.

Vorbereitungen

Wenn Sie die Anwendung bereits in Ihrer -Instanz haben und auf eine neuere Version der Anwendung aktualisieren, fahren Sie in den folgenden Schritten mit Schritt 8 fort, um mit der Aktualisierung und Konfiguration fortzufahren.

Führen Sie bei einer Neuinstallation vor der Installation die folgende Setupprüfliste durch. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Um sicherzustellen, dass Plugins und Anwendungen installiert und aktiviert sind, navigieren Sie zu **Alle** > **Subscription Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Vergewissern Sie sich, dass das Plugin „Vulnerability Response Dependencies“ (com.snc.vul_dep) installiert und aktiviert ist.	**Vulnerability Response-Abhängigkeiten** Dieses Plugin enthält alle Abhängigkeits-Plugins, die zur Unterstützung der Anwendung erforderlich sind. Um sicherzustellen, dass das Plugin installiert und aktiviert ist, soll die Anwendung in Ihrer Instanz zu navigieren **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**. Wenn Sie aufgefordert werden, andere Abhängigkeits-Plugins zu aktualisieren, klicken Sie auf die Links in den Dialogfeldern und befolgen Sie die Anweisungen, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

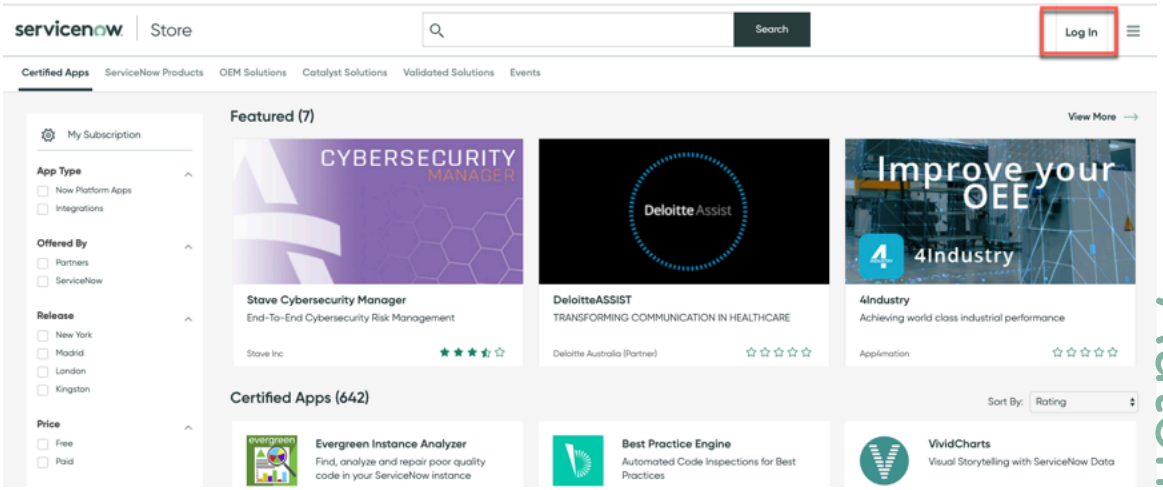
Setupaufgaben	Beschreibung
Vergewissern Sie sich, dass die Anwendung ServiceNow Vulnerability Response (sn_vul) installiert und aktiviert ist.	**Vulnerability Response** Um sicherzustellen, dass das Plugin installiert und aktiviert ist, soll die Anwendung in Ihrer Instanz zu navigieren **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**. Wenn Sie aufgefordert werden, andere Abhängigkeits-Plugins zu aktualisieren, klicken Sie auf die Links in den Dialogfeldern und befolgen Sie die Anweisungen, um fortzufahren. Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Wenden Sie sich an ServiceNow, um Einzelheiten zu erfahren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen. Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der Performance Analytics-Administrator [pa_admin] oder der Systemadministrator [admin] installiert die Anwendung und überprüft die erwarteten Ergebnisse. • Der Schwachstellenadministrator [sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse mithilfe der PA-Dashboards. • Der Verantwortliche für die Korrektur [sn_vul.remediation_owner] überwacht Change-Management-Aufgaben und liest und aktualisiert zugewiesene Datensätze. Die Rolle sn_vul.remediation_owner wird auch automatisch zugewiesen, wenn einem Benutzer die Rolle itil zugewiesen wird.
Stellen Sie sicher, dass die Anwendungen Performance Analytics und Vulnerability Response kompatibel sind.	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Erforderliche Rolle: admin oder pa_admin

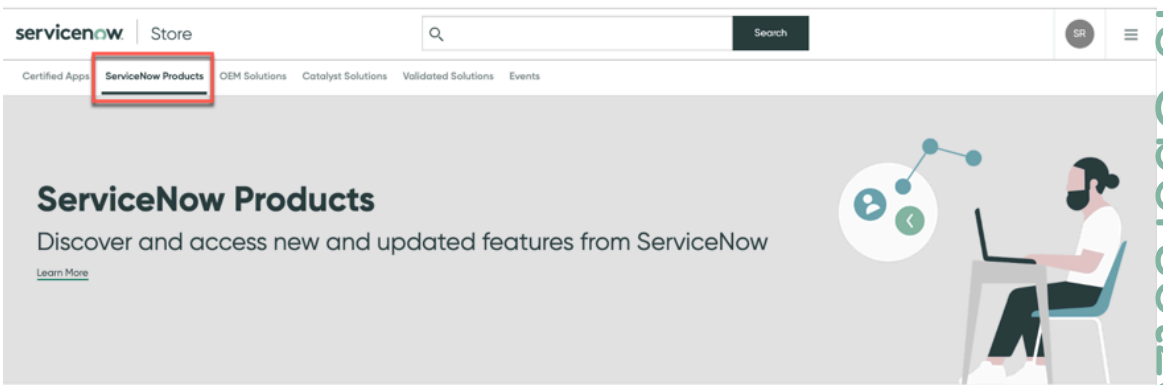
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

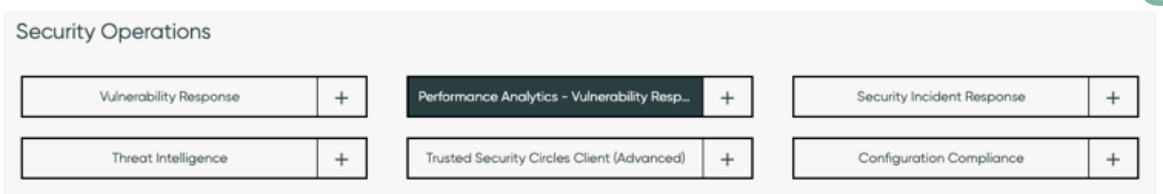
1. Um die Berechtigung zu erhalten und die Anwendung in Ihrer Instanz Now Platform herunterzuladen, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite **auf Anmelden**.



3. Geben Sie im angezeigten Dialogfeld Ihre HI-Anmeldeinformationen ein, und klicken Sie auf **Anmelden**.
4. Klicken Sie auf der angezeigten Seite auf die Registerkarte **ServiceNow-Produkte**, wenn sie nicht ausgewählt ist.



5. Klicken Sie auf der Seite mit der Produktliste auf **Performance Analytics - Vulnerability Response**.

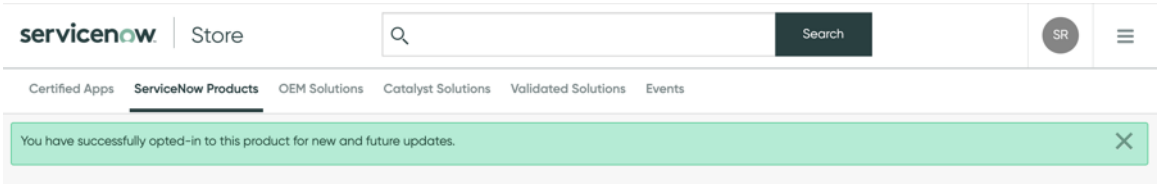


6. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
   Eine Seite mit der Schaltfläche Aktivieren wird angezeigt.
7. Um die Anwendung Performance Analytics for Vulnerability Response zu erhalten, klicken Sie auf **Aktivieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Eingabeaufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.

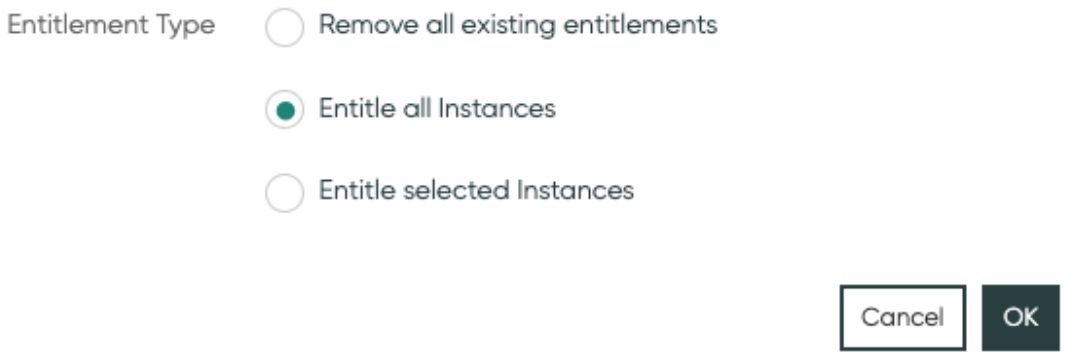


9. **Wahlweise:** Alternativ können Sie die folgenden Schritte ausführen, um Ihre Berechtigungen für die Anwendung in anderen Now Platform -Instanzen zu verwalten.

   a. Wenn die Schaltfläche Berechtigung verwalten nicht angezeigt wird, klicken Sie auf die Anwendung Performance Analytics for Vulnerability Response in der Produktliste, um sie anzuzeigen.

   b. Wählen Sie die Registerkarte Berechtigt aus, und klicken Sie auf **Berechtigung verwalten**.

   c. Wählen Sie im angezeigten Dialogfeld „Berechtigungen für Vulnerability Response verwalten“ eine Option aus:

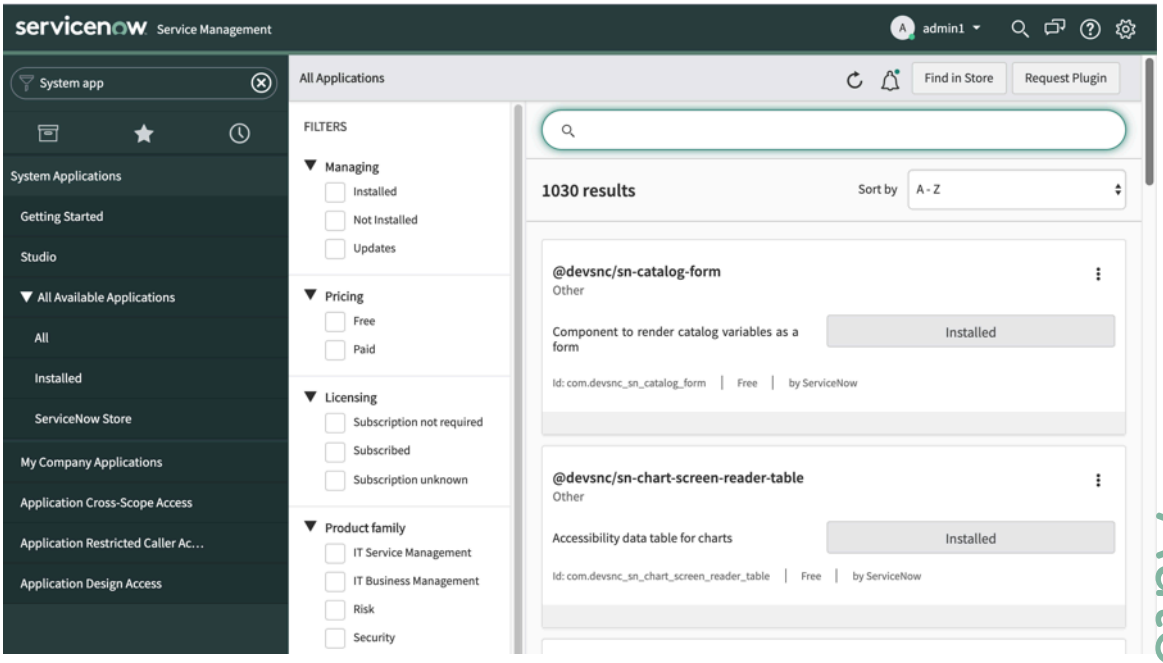


   d. Klicken Sie auf **OK** oder **Abbrechen,** um fortzufahren.
   Sie können nun Plugins aktivieren und die Anwendung auf Ihren Now Platform Instanzen installieren.

10. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Vulnerability Response installieren möchten.
11. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



12. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Performance Analytics - Inhaltspaket - Vulnerability Response (sn_vul_analytics), und klicken Sie auf **Installieren**.

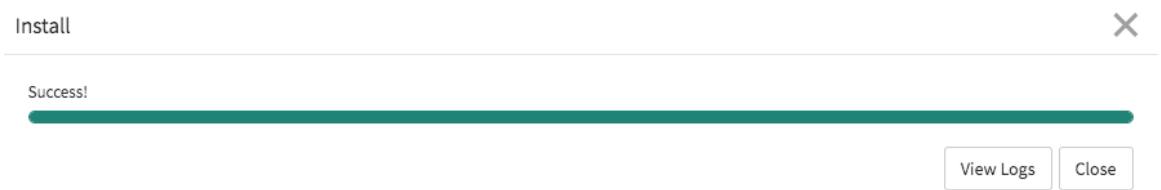
    Hinweis:
    Wenn Sie auf eine neue Version aktualisieren, wählen Sie die gewünschte Version aus der Auswahlliste aus.

    und klicken Sie auf **Aktualisieren**.
    Das Dialogfeld „Anwendungsinstallation“ wird angezeigt. Alle Abhängigkeiten, die automatisch mit der Anwendung installiert werden, werden ebenfalls angezeigt.

13. **Wahlweise:** Wenn Sie Demodaten wünschen, aktivieren Sie das Kontrollkästchen Demodaten laden, und klicken Sie auf **Installieren**.

    Hinweis:
    Wenn Sie das Kontrollkästchen **Demodaten laden** nicht aktivieren, können die Demodaten nicht später über den **Anwendungsmanager** installiert werden. Informationen zur Installation oder erneuten Installation von Demodaten nach der Erstinstallation finden Sie im Artikel Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] in der Knowledge Base Now Support.

    Diese Installation kann einige Zeit in Anspruch nehmen. Nachdem die Anwendung erfolgreich installiert wurde, wird im Dialogfeld „Installieren“ eine Meldung angezeigt.



14. Klicken Sie auf **Schließen**.

15. **Wahlweise:** Wenn Sie mit einer großen Anzahl aktiver angreifbarer Elemente in Ihrer Umgebung rechnen, können Sie die Standardeinstellung für die maximale Anzahl gesammelter Datensätze ändern, geplante Aufgaben aktivieren und Sammlungszeiten außerhalb der Geschäftszeiten festlegen.

Automatische Übersetzung

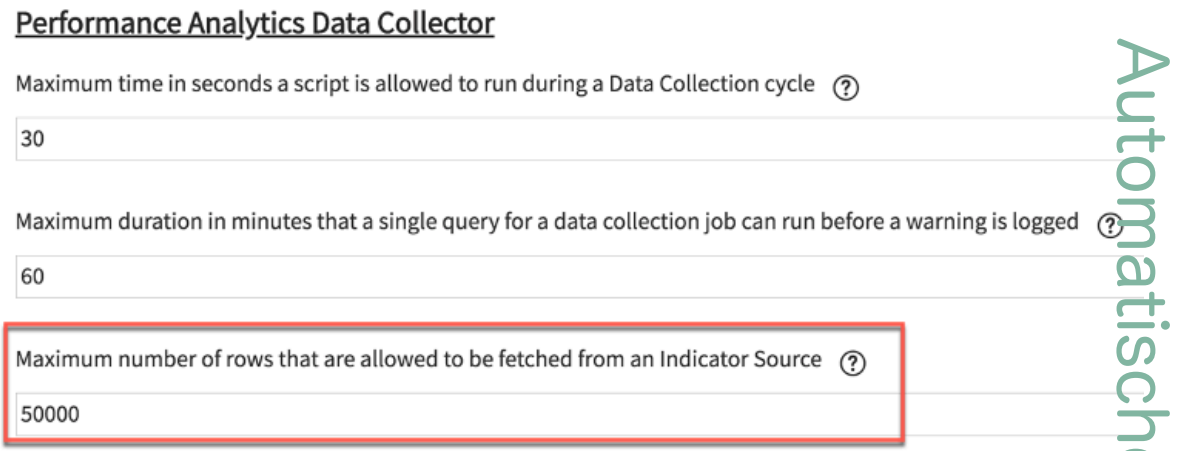
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie die folgenden Schritte aus, um diese und andere Einstellungen für die Anwendung nach der Installation zu ändern.

a. Navigieren zu **Alle** > **Performance Analytics** > **Administratorkonsole**.

b. Klicken Sie auf der Kachel Erweiterte Konfiguration auf den Link **Performance Analytics-Eigenschaften**.

c. Scrollen Sie auf der Seite [Performance Analytics] der Administratorkonsole zum Abschnitt Performance Analytics Data Collector (Datensammler für Performance Analytics).
Die Standardeinstellung (50.000 Datensätze) wird für die maximale Anzahl von Zeilen angezeigt, die von einer Indikatorquelle abgerufen werden dürfen.



d. Möglicherweise möchten Sie diese Anzahl auf einen Wert erhöhen, der etwa 20 % über der Gesamtanzahl der in Ihrer Umgebung erwarteten aktiven angreifbaren Elemente (VIs) liegt.

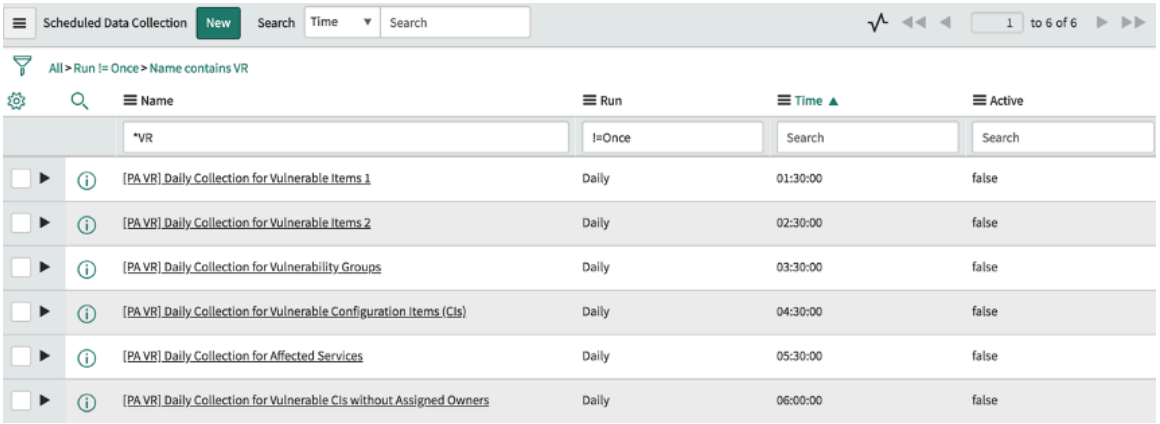
e. Klicken Sie auf **Speichern**.

f. Um geplante Aufgaben zu aktivieren, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge**.
Die Liste Geplante Datensammlung wird angezeigt. In der Spalte „Aktiv“ sind die geplanten Aufgaben deaktiviert, die standardmäßig in der Spalte „Anwendung“ für „Performance Analytics – Inhaltspaket – Vulnerability Response“ aufgeführt werden (falsch).

Hinweis:
Eine geplante Aufgabe für die Verlaufsdatensammlung wird in der Liste der Aufgaben nicht angezeigt. Bei großen Datenmengen möchten Sie möglicherweise mit der Erfassung von Daten und Trends beginnen, indem Sie Ihre täglichen Aufgaben aktivieren, wenn Sie Performance Analytics für die Anwendung Vulnerability Response einrichten.

Automatische Übersetzung

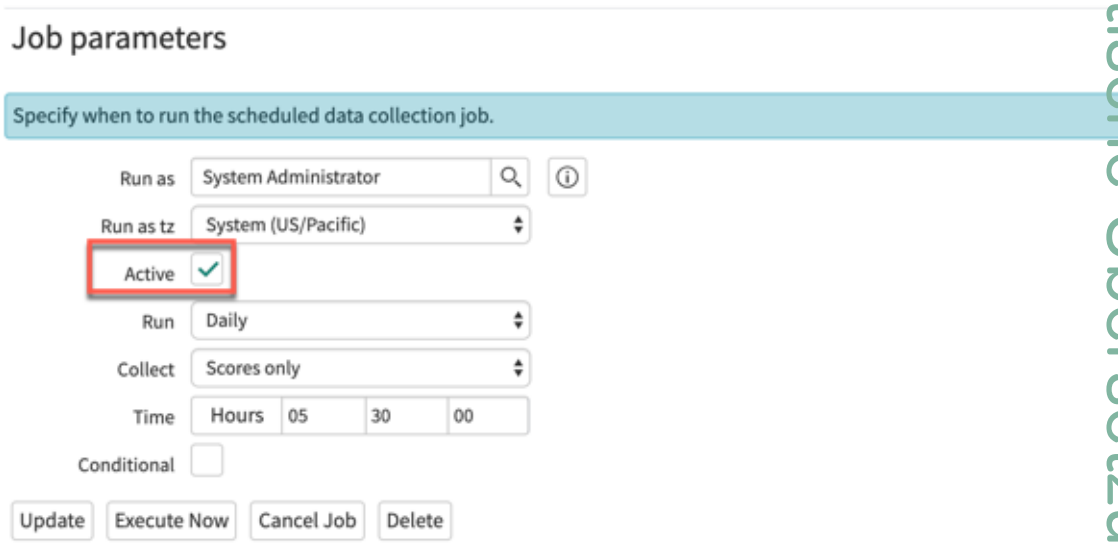
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



g. Klicken Sie in der Spalte Name auf einen Link, um einen PA_VR-Auftragsdatensatz zu öffnen.

h. Wenn Felder nicht bearbeitet werden können, klicken Sie auf den Link **hier,** um sie zu bearbeiten.

i. Klicken Sie im Abschnitt mit den Auftragsparametern auf das Kontrollkästchen Aktiv, um einen Auftrag zu planen.
Die Felder Zeit werden angezeigt.



j. Geben Sie die Startzeit für den Auftrag ein.
Wenn Sie mit einem großen Volumen rechnen, ziehen Sie es möglicherweise vor, Sammlungszeiten außerhalb der Geschäftszeiten festzulegen. Wenn Sie in Ihrer Umgebung 10 Millionen aktive AEs oder mehr erwarten, wenden Sie sich an Ihren ServiceNow® – Implementierungspartner, um weitere Informationen zum Einrichten Ihrer Datensammlungsumgebung zu erhalten.

Weitere Informationen zu den für die Datensammlung verwendeten -Indikatoren finden Sie unter Performance Analytics -Indikatoren für Vulnerability Response [PA] anzeigen.

k. Nachdem Sie alle gewünschten Aufträge aktiviert haben, klicken Sie auf **Aktualisieren**.
Die Liste Geplante Datensammlung wird angezeigt. Weitere Informationen finden Sie unter Performance Analytics-Eigenschaften .

Automatische Übersetzung

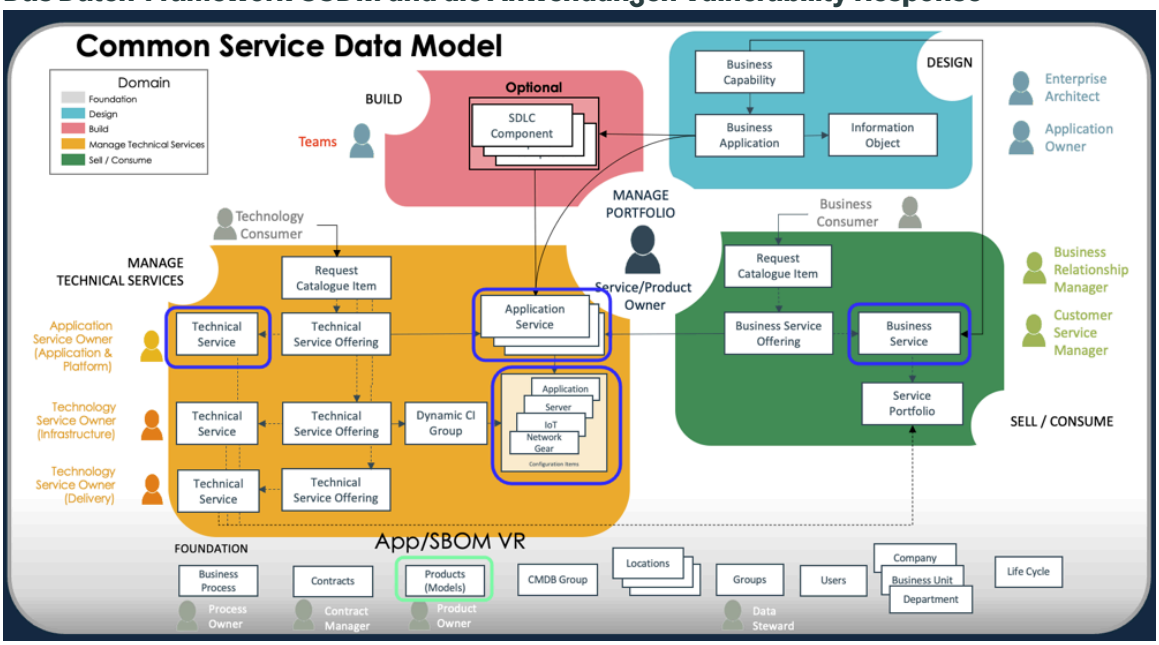
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Navigieren zu **Vulnerability Response** > **Übersicht** um das Dashboard anzuzeigen.

Vulnerability Response -Anwendungen und -Tabellen CSDM.

Die Anwendungen Vulnerability Response, Application Vulnerability Response, Schwachstellenintegrationen von Drittanbietern und Software Bill of Materials verwalten die Tabellen CSDM (tragen Daten zu diesen bei). Diese Anwendungen verwenden auch Daten aus Tabellen CSDM, die andere Anwendungen generieren. Mehrere ServiceNow -Produkte profitieren daher von diesen Security Operations -Anwendungen und fügen ihnen einen Mehrwert hinzu.

Das Daten-Framework CSDM und die Anwendungen Vulnerability Response



CSDM Tabellen, auf die von Vulnerability Response, Application Vulnerability Response, Schwachstellenintegrationen von Drittanbietern und den Anwendungen Software Bill of Materials verwiesen wird

Wenn Assets von Schwachstellenscannern (Integrationen) von Drittparteien importiert werden, werden sie in Vulnerability Response eingefügt und in bestimmten Tabellen dargestellt:

- Host Vulnerability Response Erkannte Elemente.
- Von Cloud und Container Vulnerability Response erkannte Images
- Application Vulnerability Response Erkannte Anwendungen (Produktmodell)

Im Rahmen der Suche nach einem CMDB-Konfigurationselement (CI) Security Operations wird eine Suche durchgeführt, um einen (CI-)Datensatz aus importierten Daten mit vorhandenen Datensätzen in der CMDB abzugleichen.

Jeder spezifische CI-Datensatz kann nicht erkennbare Attribute enthalten, z. B. Supportgruppe oder Klassifizierung, die im CI ausgefüllt werden und als Eingabe für die Zuweisungsregeln für angreifbare Elemente verwendet werden können. Diese Attribute können aus Synchronisierungen mit dem Common Service Data Model (CSDM) basierend auf vorgelagerten technischen Serviceangeboten ausgefüllt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie zugehörige CSDM-Objekte für Vulnerability Response, Application Vulnerability Response, Schwachstellenintegrationen von Drittanbietern und Software Bill of Materials nutzen möchten, müssen Sie geskriptete Regeln verwenden.

Um beispielsweise angreifbare Elemente zur Korrektur mithilfe von Zuweisungsregeln für angreifbare Elemente automatisch zuzuweisen, können Sie eine Regel erstellen, die Klassifizierungswerte von Konfigurationselementen nutzt, wenn sie für importierte Schwachstelleneinträge aktualisiert werden. In diesem Fall benötigen Sie eine geskriptete Regel, um den gewünschten Zielwert vom zugehörigen CSDM-Objekt abzufragen.

Nachfolgend finden Sie ein Beispiel für eine geskriptete Abfrage, mit der Sie feststellen können, ob ein CI Java enthält und an einen Schwachstelleneintrag gebunden ist.

Scripted (query)

Vulnerability Response, Application Vulnerability Response, Schwachstellenintegrationen von Drittanbietern und Software Bill of Materials Anwendungen verweisen auf die folgenden Tabellen. Weitere Informationen finden Sie in der Abbildung zum Daten-Framework CSDM und Vulnerability Response -Anwendungen.

- Die Produktmodelltabelle [cmdb_model] (referenziert durch Application Vulnerability Response und Software Bill of Materials).
- Tabelle „Anwendungsmodell“ [cmdb_application_product_model] (referenziert durch Application Vulnerability Response und Software Bill of Materials).
- Die Configuration Item-Tabelle [cmdb_ci].
- Die Tabelle „Business-Service“ [cmdb_ci_service_business].
- Tabelle „Service“ [cmdb_ci_service].
- Tabelle „CMDB-Gruppe“ [cmdb_group].
- Tabelle „Dynamische CI-Gruppe“ [cmdb_ci_query_based_service].

CSDM Tabellen, die von den Vulnerability ResponseAnwendungen , Application Vulnerability Response, Schwachstellenintegrationen von Drittanbietern und den Anwendungen Software Bill of Materials verwendet werden

1. Tabelle „Produktmodell“ [cmdb_model] (verwendet von Application Vulnerability Response und Software Bill of Materials).
2. Tabelle „Anwendungsmodell“ [cmdb_application_product_model] (verwendet von Application Vulnerability Response und Software Bill of Materials).
3. Die Configuration Item-Tabelle [cmdb_ci].
4. Geschäftsanwendung [cmdb_ci_business_app] (verwendet von Application Vulnerability Response und Software Bill of Materials).
5. Business-Service [cmdb_ci_service_business]
6. Technischer Service [cmdb_ci_service_technical].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie Software Bill of Materials -Dateien hochladen, versuchen die SBOM-Anwendungen, alle von Ihnen hochgeladenen Produktmodelle und Geschäftsanwendungen mit bereits in Ihrer CMDB vorhandenen Produktmodellen und Geschäftsanwendungen abzugleichen. Sie können Anwendungsservices oder Geschäftsanwendungen mit einem Produktmodell verknüpfen.

Produkte, die den Anwendungen Vulnerability Response, Application Vulnerability Response, Schwachstellenintegrationen von Drittanbietern und den Anwendungen Software Bill of Materials Mehrwert hinzufügen

Die Verwendung der Vulnerability Response -Anwendungen mit den folgenden ServiceNow -Produkten kann Ihrer Organisation zugutekommen.

Schwachstellenscanner und Integrationen von Drittparteien

Importierte Schwachstellen aus der National Vulnerability Database (NVD) und Erkennungsdaten von Drittanbieter-Scannern werden mit den Assets in Ihrer CMDB abgeglichen. Wenn eine importierte Schwachstelle mit einem vorhandenen Asset übereinstimmt, wird ein angreifbares Element erstellt. Angreifbare Elemente werden automatisch in zu korrigierenden Aufgaben gruppiert, mit Risikobewertung für den Geschäftskontext bewertet, priorisiert und den entsprechenden Teams zur Korrektur zugewiesen. Weitere Informationen und eine Liste der Integrationen finden Sie unter Vulnerability Response-Integrationen.

CWE Comprehensive 2000 und NVD Integrations

Importierte Daten aus den Integrationen NIST National Vulnerability Database (NVD) und Common Weakness Enumeration (CWE) werden verwendet, um die Schwachstellendaten in Ihrer Instanz zu ergänzen und Sie zu entscheiden, ob die Korrektur für eine Schwachstelle, ein angreifbares Element oder eine Korrekturaufgabe eskaliert werden soll. Siehe Grundlagen zu NVD-Integrationen und Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus, um weitere Informationen zu erhalten.

Produkte, die von der Integration mit profitieren Software Bill of Materials

Sicherheitsstatus-Überwachung

Sicherheitsstatus-Überwachung ermöglicht es Cybersicherheitsteams, Einblick in den gesamten Bestand von Unternehmens-Assets zu erhalten und ihre allgemeine Sicherheitslage zu bestimmen. Richtlinien in SSÜ können Ihnen dabei helfen, angreifbare Assets zu erkennen, die Sie mit den Vulnerability Response -Anwendungen importieren, um Lücken bei der Abdeckung von Sicherheitstools zu finden.

Governance, Risk und Compliance

Verbinden Sie Sicherheit und IT mit einem integrierten Risikoprogramm, das kontinuierliche Überwachung, Priorisierung und Automatisierung bietet.

DevOps

Schützen Sie Ihre Umgebungen während Softwareentwicklungszyklen mit GitHub-Aktionen, die Sie über Ihre GitHub-Umgebung initiieren, vor potenziell schädlichen Komponenten. Laden Sie SBOM-Dateien aus Ihren GitHub-Repositorys in Now Platform hoch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen oder bearbeiten Sie Vulnerability Response -Zuweisungsregeln

Nachdem Sie Ihre erste Bewertung von Zuweisungsregeln mit dem Setup-Assistenten abgeschlossen haben, können Sie Regeln erstellen, um angreifbare Elemente automatisch basierend auf Filterbedingungen zuzuweisen. Diese Regeln weisen angreifbare Elemente zu, wenn sie importiert oder manuell erstellt werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem enthält eine Zuweisungsregel für Schwachstellen, **Der CI-Supportgruppe zuweisen**, die angreifbare Elemente der gleichen Zuweisungsgruppe wie die CI-Supportgruppe zuweist. Diese Regel kann mithilfe von Filterbedingungen geändert werden, oder Sie können eine neue Regel erstellen. Mit Zuweisungsregeln definieren Sie die Zuweisungsbedingungen und die Reihenfolge der Ausführung. Sobald ein VI eine Regelbedingung erfüllt, wird die Zuweisungssuche beendet.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Öffnen Sie die Regel **An CI-Supportgruppe zuweisen**, oder klicken Sie auf **Neu**.
3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

Zuweisungsregel für Schwachstellen

Feld	Beschreibung
Name	Name der Gruppenregel.
Aktiv	Gibt an, ob die Zuweisungsregel aktiv ist.
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Regeln mit hoher Priorität, Elemente, die einer besonderen Behandlung bedürfen, bei denen das Risiko kritisch ist oder bei denen ein VI von der Compliance mit Vorschriften und Gesetzen gehandhabt werden sollte, damit sie zuerst ausgeführt werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist, und Sie wissen , wer dafürverantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um der Gruppe VIs zuzuweisen, die bestimmt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt.
Beschreibung	Beschreibung der Zuweisungsregel.
Bedingung	
Vorschau	Zeigt an, wie viele Ergebnisse diese Abfrage zurückgeben wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedingungsfelder	Bedingungen, die erfüllt werden müssen. **Hinweis:** Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Zuweisungsregeln verfügbar zu machen, müssen Sie die Rapid7 InsightVM Asset List-Integration vor den anderen Rapid7 InsightVM Integrationen ausführen. Die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.
Neues Kriterium	Fügt weitere Bedingungsfilterfelder zur Auswahl hinzu.
Zuweisen mit	Um die Zuweisung von anhand dieser Regel erstellten Gruppen zu automatisieren, wählen Sie eine der verfügbaren Optionen aus. ○ Anwendergruppe: Wählen Sie eine Anwendergruppe aus der Suchtabelle aus. ○ Anwendergruppenfeld: Wählen Sie ein Anwendergruppenfeld aus dem Dropdown-Menü aus. ○ Skript: Erstellen oder bearbeiten Sie ein Skript. **Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert das Fachwissen ServiceNow.

4. Klicken Sie auf **Absenden**.
   Neue oder aktualisierte Regeln werden beim nächsten Import bewertet.

Hinweis:

Die Funktion zum erneuten Anwenden erfordert eine Baselineanwendung der Regeln. Sobald Ihre Regeln erstellt sind, aktivieren Sie, falls noch nicht geschehen, die geplante Aufgabe `Reapply all vulnerability assignment rules`, um nach Belieben auszuführen. Sie wendet alle Regeln auf alle offenen VIs an, mit Ausnahme der manuell zugewiesenen. Je nachdem, wie viele aktive VIs Sie in Ihrer Umgebung haben, denken Sie daran, das Feld **Ausführen** nach der ersten Ausführung entsprechend zu setzen, um Auswirkungen auf die Leistung zu vermeiden.

Wenn Sie diese geplante Aufgabe nicht ausgeführt haben und versuchen, die Schaltfläche **„Änderungen anwenden“** im Formular „Zuweisungsregeln“ zu verwenden, müssen Sie dies dann ausführen. Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

Erstellen Sie eine Vulnerability Response -Zuweisungsregel mit ML

Verwenden Sie das folgende Skript, um eine Ausweichkontakt-Zuweisungsregel für angreifbare Elemente zu erstellen, die ML-Empfehlungen von Predictive Intelligence verwendet, um sie automatisch zur Korrektur zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Anwendung Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response muss installiert und aktiviert sein. Diese Anwendung ist unter ServiceNow Storeverfügbar.

Eine Klassifizierungslösung muss definiert, aktiv und trainiert sein. Sie verwenden dieses Modell, um die geeignete Zuweisungsgruppe für angreifbare Elemente (VI) vorherzusagen, wenn Ihre Zuweisungsregeln keine richtige Übereinstimmung für die beabsichtigten Empfänger gefunden haben.

Diese Regel hilft Ihnen möglicherweise, die Anzahl der nicht zugewiesenen AEs zu reduzieren, nachdem andere Zuweisungsregeln bereits abgeschlossen wurden.

Siehe Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response installieren und Erstellen und trainieren Sie eine Lösungsdefinition für Vulnerability Response, um weitere Informationen zu erhalten.

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Möglicherweise möchten Sie diese Aufgabe nur ausführen, wenn Sie über fortgeschrittene Codierungserfahrung verfügen oder über fundierte Kenntnisse über Now Platform, seine Funktionen von Predictive Intelligence und die Funktionsweise von Zuweisungsregeln verfügen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Wählen Sie **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response -Zuweisungsregeln.
4. Wählen Sie in der Auswahlliste Zuweisen mit die Option **Skript**aus.
5. Kopieren Sie im Editor das folgende Skript, und fügen Sie es ein.

```
   /*
   * Catch-all assignment rule using ML recommendation
   * NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
   * Classification Solution must be active and trained
   */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
   var ARU = new sn_vul.AssignmentRecommendationUtils();
   ARU.initialize();

   var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
   /*
   *returns object containing array of predictions
   *payload structure:
   *
   {
      "predictions": [
         {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
            "name": "Windows Server support ",
            "confidence_score": "57.54"
        },
        ...
    ],
    "exception": ""
}
*/
var viPredictionArray = viPredictionObj['predictions'];
var topPredictionObj = viPredictionArray.shift();

return topPredictionObj['sys_id'];
}
```

6. Wählen Sie **Absenden**.

Nächste Maßnahme

Überprüfen Sie Vulnerability Response Übersicht über Zuweisungsregeln, um allgemeinere Informationen über Zuweisungsregeln und die geplante Aufgabe *`Reapply all vulnerability assignment rules`* zu erhalten.

Erstellen Sie eine Vulnerability Response -Zuweisungsregel für den Servicesupport

Verwenden Sie das folgende Skript, um eine Regel zu erstellen, die angreifbare Elemente basierend auf den betroffenen Geschäftsservices zur Korrektur zuweist.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Möglicherweise möchten Sie diese Aufgabe nur ausführen, wenn Sie über fortgeschrittene Codierungserfahrung verfügen oder über profunde Kenntnisse über Now Platform und die Funktionsweise von Zuweisungsregeln verfügen.

Mit dieser Regel werden VIs danach zugewiesen, wie genau sie mit den in Ihrer CMDB aufgeführten Geschäftsservices übereinstimmen. Wenn keine zugehörigen Services, Abteilungen oder Supportgruppen übereinstimmen, werden der Schwachstellenanalystengruppe VIs zugewiesen.

Diese Regel hilft Ihnen möglicherweise, die Anzahl der falsch zugewiesenen oder nicht zugewiesenen VIs zu reduzieren, nachdem andere Zuweisungsregeln bereits abgeschlossen wurden.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Wählen Sie **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response -Zuweisungsregeln.
4. Wählen Sie in der Auswahlliste Zuweisen mit die Option **Skript**aus.
5. Kopieren Sie im Editor das folgende Skript, und fügen Sie es ein.

```
/*
Assigns Vulnerable Item based on related Business Service
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Assigns to default Vulnerability Analyst group if no related Business Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
   var ci = vitGR.getValue('cmdb_ci');
   var defaultAssignmentGroup = 'Vulnerability Analyst';
   var defaultGR = new GlideRecord('sys_user_group');
   defaultGR.get('name', defaultAssignmentGroup);
   var defaultAssignmentGroupID = defaultGR.sys_id;

   var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
   var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
   var customValues = {
      "maxDepth": maxDepthValue,
      "maxSize": maxSizeValue
   };
   var ciu = new global.CIUtils();
   var services = ciu.servicesAffectedByCI(ci, customValues);
   var svc = new GlideRecord("cmdb_ci_service");
   var hasSvc = false;
   if (services && services.length > 0) {
      svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
      svc.addNotNullQuery("busines_criticality"); // typo intended
      svc.orderBy("busines_criticality");
      svc.setLimit(1);
      svc.query();
      hasSvc = svc.next();
   }
   if (!hasSvc) {
      // If there are no services it should be assigned to a default assignent group
      return defaultAssignmentGroupID;
   } else {
      var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
      return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
   }
}
```

6. Wählen Sie **Absenden**.

Nächste Maßnahme

Überprüfen Sie Vulnerability Response Übersicht über Zuweisungsregeln, um allgemeinere Informationen über Zuweisungsregeln und die geplante Aufgabe *`Reapply all vulnerability assignment rules`* zu erhalten.

Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben

Nachdem Sie Ihre erste Bewertung der Regeln für Korrekturaufgaben mit dem Setup-Assistenten abgeschlossen haben, können Sie Regeln erstellen, um angreifbare Elemente automatisch basierend auf Filterbedingungen zu gruppieren. Diese Regeln gruppieren automatisch angreifbare Elemente, wenn sie importiert oder manuell erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie den Filter, um die von dieser Regel gruppierten angreifbaren Elemente einzuschränken, z. B. die Auswahl aller angreifbaren Elemente mit Exploits.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Das Basissystem enthält eine Regel für Korrekturaufgaben, **Vulnerability**, die angreifbare Elemente nach Schwachstelle und Zuweisungsgruppe (unter **Zuweisungsregeln**) gruppiert. Sie können die Regeln aus dem Formular oder der Listenansicht erneut anwenden. Für einige Beispieleinträge Vulnerability Response Beispiele für Regeln für Korrekturaufgaben.

Diese Regel kann wie folgt geändert werden:

Mithilfe von Filterbedingungen und Auswahlmöglichkeiten für „Gruppieren nach“.

Standardmäßig verwenden Korrekturaufgaben, sofern verfügbar, **Zuweisungsregeln**als Teil ihrer Filterkriterien.

Hinweis:
Wenn keine Zuweisungsregeln vorhanden sind, können Sie eine Gruppe mithilfe des Felds **Benutzergruppe** auswählen.

Ab Version 18.0 von Vulnerability Responseist die Regel für Nachbesserungsaufgaben für **Schwachstellen** in Vulnerability Response für Neuimplementierungen deaktiviert.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben**.
2. Öffnen Sie die Regel, oder klicken Sie auf **Neu**.
3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

Regel für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Aufgabenregel.
Aktiv	Gibt an, ob die Aufgabe aktiv ist.
Beschreibung	Eine Beschreibung der Regel.
Groß-/ Kleinschreibung beachten	Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht. **Hinweis:** Beim Standardwert wird zwischen Groß- und Kleinschreibung unterschieden.
Bedingung	Optionale Filterbedingungen für die Regel. **Hinweis:** Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Regeln für Korrekturaufgaben verfügbar zu machen, müssen Sie die Rapid7 InsightVM Asset-Listenintegration vor den anderen Rapid7 InsightVM -Integrationen ausführen. Standardmäßig (Kontrollkästchen**„Groß-/Kleinschreibung beachten** “ deaktiviert) berücksichtigt der Suchtext, den Sie im Bedingungsgenerator für Aufgabenregeldatensätze und Formulare

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	eingeben, Groß-/Kleinschreibung. Sie können die Suche nach Groß-/Kleinschreibung für Aufgabendatensätze und Formulare aktivieren.
Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)	
Angreifbare Elemente gruppieren aus	Die Tabelle, die von der Regel zum Gruppieren von AEs verwendet wird. Sie können bis zu sechs Filter verwenden. Die Auswahlmöglichkeiten lauten wie folgt: ○ Angreifbares Element [sn_vul_vulnerable_item] ○ Angreifbares Element → Konfigurationselement [cmdb_ci] ○ Angreifbares Element → Schwachstelle [sn_vul_ third_party_entry] **Hinweis:** Wenn Sie eine erweiterte Tabelle wählen, wird das **Feld Verwendet** nur für angreifbare Elemente angewendet, die diese erweiterte Tabelle verwenden.
Mit Feld	Feld in der Tabelle, das von der Regel zum Gruppieren von AEs verwendet wird.
Zuweisung	
Korrekturaufgaben zuweisen nach	Bei der automatischen Zuweisung von Korrekturaufgaben wird die Option Zuweisung zusätzlich zu den Auswahlmöglichkeiten **für Gruppieren nach** verwendet, um die angreifbaren Elemente zu gruppieren. Neue Aufgaben werden nach Bedarf erstellt, um sicherzustellen, dass jedes angreifbare Element in einer Aufgabe mit einer übereinstimmenden Zuweisungsgruppe platziert wird. Um die Zuweisung von auf der Grundlage dieser Regel erstellten Aufgaben zu automatisieren, wählen Sie eine der verfügbaren Optionen aus. ○ Feld Gruppieren nach: Wenn Sie ein Benutzergruppenfeld aus Feldwerte **werden verwendet** im Abschnitt **Gruppieren nach**ausgewählt haben, werden diese im Dropdown-Menü angezeigt. ○ Benutzergruppe: Verwenden Sie die Suchliste, um eine statische Benutzergruppe auszuwählen.

Hinweis:
Wenn Sie Ihre Meinung zu einer der Einstellungen **für Gruppieren nach** ändern, setzt der zugehörige Link **Gruppieren nach Feldern** löschen die Felder **für Gruppieren** im Formular zurück.

Wenn eine Gruppenregel gelöscht wird, können Sie im Formular oder in der Listenansicht alle **offenen** Gruppen löschen, die von dieser Regel erstellt wurden. Gruppen, die sich nicht im Status **„Offen“** befinden, werden ausgeschlossen.

Einige Beispieleinträge finden Sie unter Vulnerability Response Beispiele für Regeln für Korrekturaufgaben.

Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, um Risikopunktzahlen zu generieren, die die für Ihre Organisation eindeutigen Schwachstellen- und Asset-Daten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwenden. Durch Auswahl der Felder, die in der Risikoregel enthalten sind, können Sie ein effektives Framework für die Risikobewertung definieren.

Vorbereitungen

Darüber hinaus können Sie Attribute in „configuration_item“ [cmdb_ci] in der Configuration Management Database (CMDB) verwenden, um die Logik für Ihre Vulnerability Response-Risikorechner zu erstellen. Wenn Sie beispielsweise feststellen, dass in Ihrer Organisation nach außen gerichtete CIs angreifbarer sind und möglicherweise eine sofortige Korrektur erfordern, können Sie für diese CIs Attribute wie z. B. `Internet Facing` zuweisen. Dieses und andere Attribut sind in den Versionshinweisen zum Common Service Data Model für das Orlando-Familienrelease aufgeführt. Aktuelle Informationen und Anleitungen zu CMDBfinden Sie in den folgenden Themen:

- Konzeptionelles Modell des Common Service Data Model
- CMDB-Schemamodell

Erforderliche Rolle: sn_vul.manage_risk_score_configuration

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**.
2. Wählen Sie auf der Seite „Schwachstellen-Rechner **“ Standardrisiko-Rechner**.
3. Navigieren zu **Seite „Schwachstellen-Rechner“.** > **Registerkarte Regeln des Schwachstellen-Rechners** > **Standardrisikoregel**.
4. **Wahlweise:** Legen Sie im Abschnitt „Kriterien des Risikorechners“ der Seite „Regel für Schwachstellenrisiko“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung in der Berechnung der Gesamtrisikopunktzahl fest.
5. Um die Regel zu deaktivieren, müssen Sie das Kontrollkästchen **Aktiv** deaktivieren.
6. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, wählen Sie **Kriterien hinzufügen**.
7. Füllen Sie die Felder des Formulars aus.

Formular „Risikoregelfeld“.

Feld	Beschreibung
Referenztabelle auswählen	Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Sie können eine dieser Optionen auswählen: ○ **Angreifbares Element**: Fügen Sie Felder hinzu, die direkt vom angreifbaren Element (VI) aus punktweise durchlaufbar sind. ○ **Angreifbares Element – Konfigurationselement**: Fügen Sie Dot-Walking-Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. der Hardwaretabelle. Diese Felder sind nicht Teil der Basistabelle (cmdb_ci). ○ **Angreifbares Element – Schwachstelle**: Fügen Sie Dot-Walking-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. Drittpartei-Eintrag. Diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Felder sind nicht Teil der Basistabelle des Schwachstelleneintrags. ○ **Referenztabelle für angreifbare Elemente**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) oder Tabellen sind, die einen Verweis auf das angreifbare Element enthalten. Diese Felder sind nicht direkt vom VI aus punktweise durchlaufbar. ○ **Referenztabelle für Konfigurationselement**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci enthalten. Diese Felder sind nicht direkt vom VI aus punktweise durchlaufbar. ○ **Referenztabelle für Schwachstellen**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von „sn_vul_entry“ sind, oder Tabellen, die einen Verweis auf „sn_vul_entry“ enthalten. Diese Felder sind nicht direkt vom VI aus punktweise durchlaufbar. ○ **Anwenderdefinierte Bedingungen**: Verwenden Sie diese Option, um der Regel durch Auswertung der Bedingung Gewichtungen zuzuweisen. Beispielsweise bestimmt der Filter mit Internetverbindung, ob ein Configuration Item (CI) extern oder intern ist.
Tabelle	Feld, das nur angezeigt wird, wenn in der Referenzauswahltabelle eine der folgenden Optionen ausgewählt wird: ○ **Angreifbares Element -> Konfigurationselement** ○ **Angreifbares Element -> Schwachstelle** ○ **Referenztabelle für angreifbare Elemente** ○ **Referenztabelle für Konfigurationselemente** ○ **Referenztabelle für Schwachstellen**
Feld	Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet werden soll.
Aggregation	Feld, das nur angezeigt wird, wenn eine Referenztabelle aus der Referenztabelle auswählen ausgewählt wird. Wählen Sie den Mindest- oder Höchstwert aus, der für Berechnungen berücksichtigt werden soll, wenn das Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gewichtung	Gewichtung dieses Feldes innerhalb der Risikoregel. Der Wert muss eine ganze Zahl von 0 bis 100 sein.
Definieren Sie die Wertgewichtung	Komponente zum Zuweisen von Gewichtungen zu jedem Feldwert. Für numerische Felder können Feldwerte als Bereich definiert werden (z. B. 1–5). Die Gewichtungen müssen Ganzzahlen zwischen 0 und 100 sein. **Hinweis:** Dieses Feld wird nicht angezeigt, wenn in der Referenztabelle „Auswählen“ die Option „Anwenderdefinierte Bedingungen“ ausgewählt ist.
Bedingungstabelle	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenzauswahltabelle ausgewählt werden. Wählen Sie eine Bedingung aus der Liste aus.
Feldname	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenzauswahltabelle ausgewählt werden. Geben Sie einen Namen für die Risikokriterien ein.
Bedingung	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenzauswahltabelle ausgewählt werden. Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen.

8. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für die aktiven angreifbaren Elemente neu zu bewerten.

Hinweis:
Ab Version 23.0 von Vulnerability Responseim Fall von:

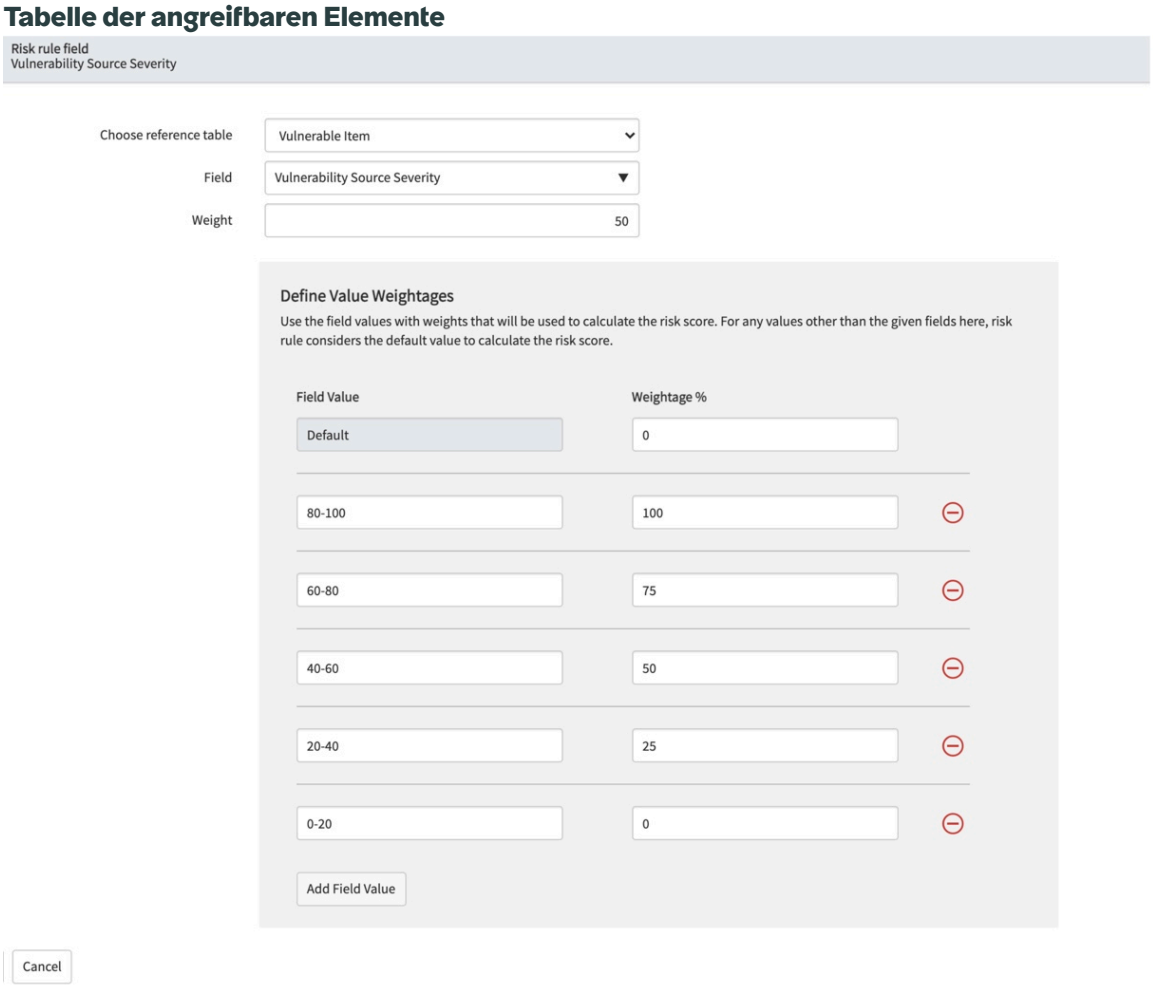
- Regel**des Standardrisiko-Rechners** : Wenn sich die Risikopunktzahl für ein angreifbares Element (VIT) ändert, werden die folgenden Details im Abschnitt „Hinweise“ des VIT dokumentiert:
  - Name der Rechnergruppe
  - Name des Rechners
  - Feldwerte, die eine Gewichtung von mehr als 1 haben, und ihr Beitrag zur Risikopunktzahl.
  - Endgültige Risikopunktzahl
- Risikoregel**für Schwachstellenschweregrad** : Bei jeder Aktualisierung der Risikopunktzahl für eine VIT wird der Abschnitt **„Hinweise“** mit den folgenden Details aktualisiert:
  - Name der Rechnergruppe
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, werden dem Namen die Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und aktivieren Sie das Kontrollkästchen **Erweiterte Ansicht**. Wählen Sie im Dropdown-Feld **Werttyp** die gewünschte Option aus. Wenn **Vorlage** ausgewählt ist, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** ausgewählt ist, können Sie entweder das vorhandene Skript hinzufügen oder aktualisieren.

Example:
Beispiel 1: Hinzufügen eines Quellschweregrads als Kriterium für eine Risikoregel.

Anwendungsfall: Drittanbieter wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden im Feld **Quellenschweregrad** in der Tabelle sn_vul_entry eingetragen. Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl. Um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

1. Navigieren Sie zur Seite Risikoregel.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, wählen Sie **Kriterien hinzufügen**.
4. Wählen Sie in der Liste Referenztabelle auswählen **die Option Angreifbares Element**aus.
5. Wählen Sie in der Liste Feld **die Option Schwachstelle.Quelle Schweregrad**aus.
6. Geben Sie im Feld **Gewicht** die relative Bedeutung des Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl von 0 bis 100 sein.
7. Fügen Sie im Abschnitt „Wertgewichtung definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Wählen Sie **Absenden**.

Beispiel 2: Fügen Sie eine Geschäftsrelevanz als Kriterium für eine Risikoregel hinzu.

Anwendungsfall: Angenommen, Ihre Organisation verfügt über viele Geschäftsservices. Das Configuration Item (CI) LINUX-SF-6381 wird von den folgenden Services verwendet:

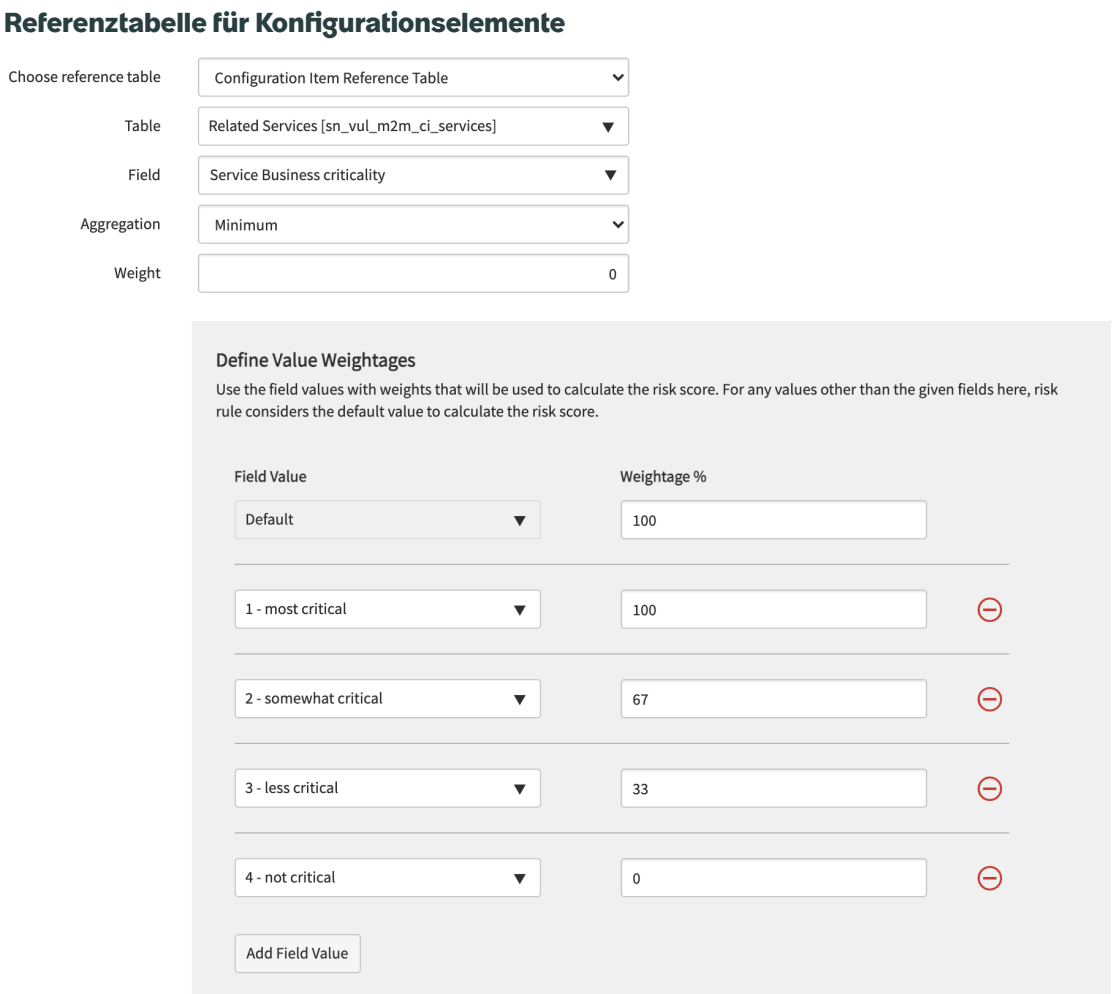
Relevanz der Business-Services

Business-Service	Relevanz
Cloud-Management	1 – Sehr kritisch
E-Commerce	2 – Kritisch
Client-Services	3 – Weniger kritisch
Reisekosten und Spesen	4 – Nicht kritisch

Die Zuordnung zwischen CI und Services wird in der Tabelle „Zugehörige Services“ [sn_vul_m2m_ci_services] gespeichert. Wenn im Asset LINUX-SF-6381 eine Schwachstelle gefunden wird, wird ein angreifbares Element (VI) erstellt. Sie können den Wert der Geschäftskritikalität aus den betroffenen Services verwenden, um die Risikopunktzahl für dieses AE zu berechnen. Um den Kritikalitätswert dieser Services zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren Sie zur Seite Risikoregel.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, wählen Sie **Kriterien hinzufügen**.
4. Wählen Sie in der Liste Referenztabelle auswählen **die Option Konfigurationselement-Referenztabelle**aus.
5. Wählen Sie in der Liste „Tabelle“ **Zugehörige Services [sn_vul_m2m_ci_services]**aus.
6. Wählen Sie in der Liste Feld **die Option Service.Business-Relevanz**aus.
7. Wählen Sie im Feld **Zusammenfassung** die **Option Minimum** aus, um den kritischsten Service für diesen Anwendungsfall abzurufen (**1 – Kritischster** Wert) oder Maximum, um den am wenigsten kritischen Service für diesen Anwendungsfall abzurufen (**4 – Kein kritischer** Wert) für diesen Anwendungsfall.
8. Geben Sie im Feld **Gewicht** die relative Bedeutung des Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl von 0 bis 100 sein.
9. Fügen Sie im Abschnitt „Wertgewichtungen definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung zu.



10. Wählen Sie **Absenden**.

Beispiel 3: Fügen Sie dem Risikorechner ein bedingtes Kriterium hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

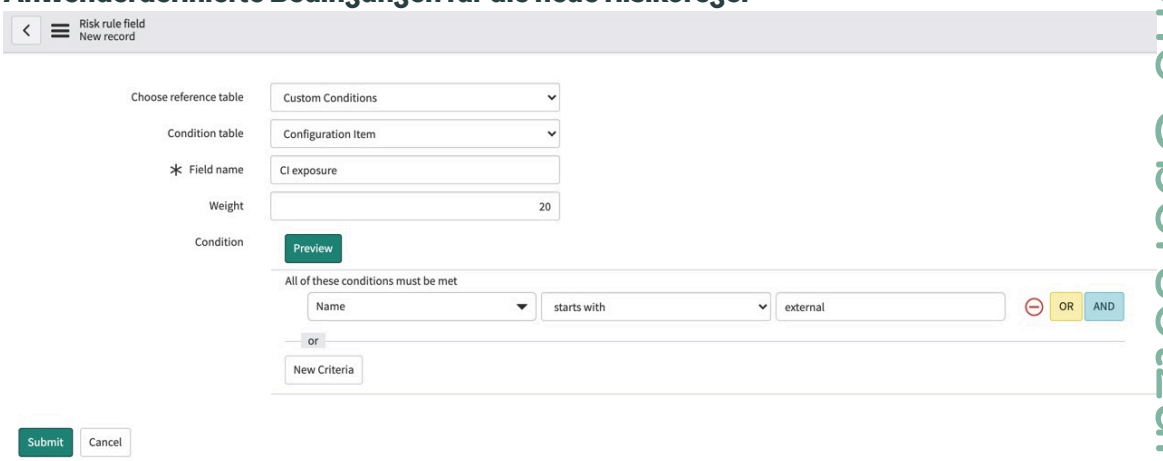
Angenommen, eine Organisation verfügt über mehrere Configuration Items (CIs), von denen ein externer Anwender nur auf einige wenige zugreifen kann. Benutzer können Gewichtungen der Risikopunktzahl für diese nach außen gerichteten CIs hinzufügen.

Hinweis:
Sie können diese CIs anhand ihres Namens identifizieren. Die Namen beginnen mit „external“.

Um der Risikoregel ein bedingtes Kriterium hinzuzufügen, gehen Sie wie folgt vor:

1. Navigieren Sie zur Seite Risikoregel.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, wählen Sie **Kriterien hinzufügen**.
4. Wählen Sie in der Liste Referenztabelle auswählen **die Option Anwenderdefinierte Bedingungen**aus.
5. Wählen Sie in der Liste Bedingungstabelle **Konfigurationselement**aus.
6. Geben Sie im **Feld** Feldname den Namen **CI Risiko**ein.
7. Geben Sie im Feld **Gewicht** die relative Bedeutung des Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl von 0 bis 100 sein.
8. Wählen Sie im Feld **Bedingung** die Option aus **Name** > **beginnt mit** und geben Sie den Wert **external**ein.

Anwenderdefinierte Bedingungen für die neue Risikoregel



9. Wählen Sie **Absenden**.

Hinweis:
Das Hinzufügen bedingter Kriterien zu Ihrer Risikoregel kann die Leistung beeinträchtigen.

Zugehörige Informationen

Vulnerability Response-Rechner und Regeln des Schwachstellen-Rechners

Erstellen Sie einen Vulnerability Response-Rechner

Filtern in Vulnerability Response

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Rollup-Rechner

Verwenden Sie nach der ersten Bewertung der Risikorechner im Setup-Assistenten die Rechner für Schwachstellen-Rollup, um zu konfigurieren, wie die kumulative Risikopunktzahl für Korrekturaufgaben und importierte Schwachstellen berechnet wird.

Verwenden Sie die Rechner für Schwachstellen-Rollup, um zu konfigurieren, wie die kumulative Risikopunktzahl für Korrekturaufgaben und importierte Schwachstellen berechnet wird. Die folgenden Rollup-Rechner sind im Lieferumfang des Basissystems enthalten:

- *`Remediation Task Rollup`*: Rollup der Risikopunktzahlen für alle angreifbaren Elemente in Korrekturaufgaben, um eine Gesamtrisikopunktzahl für die gesamte Gruppe angreifbarer Elemente bereitzustellen.
- *`Patch Update Rollup`*: Rollup der Risikopunktzahlen für alle angreifbaren Elemente mit demselben Patch-Update, um eine Gesamtrisikopunktzahl für das Patch-Update bereitzustellen.
- *`Organization Risk Score Rollup`*: Fasst die Risikopunktzahlen für alle angreifbaren Host-Elemente, angreifbaren Anwendungselemente, Container-angreifbaren Elemente und Konfigurationsprobleme in einer Organisation zusammen, um eine Gesamtrisikopunktzahl für die gesamte Organisation in einem einheitlichen Dashboard bereitzustellen.

  Hinweis:
  Ab v22.0 von Vulnerability Responsekönnen Sie Rollup-Gewichtungen für die Punktzahl der Organisation konfigurieren. Außerdem wurden einzelne Rollup-Rechner entfernt.

- *`Vulnerable Item Rollup`*: Fasst die Risikopunktzahlen für alle angreifbaren Host-Elemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl der gesamten Organisation für das einheitliche Dashboard beizutragen.
- *`Vulnerability Entry Rollup`*: Rollup der Risikopunktzahlen für alle angreifbaren Elemente mit demselben Schwachstelleneintrag, um eine Gesamtrisikopunktzahl für den Schwachstelleneintrag bereitzustellen.
- *`Rollup EPSS Scores from NVD to TPEs`*: Rollup der EPSS-Punktzahlen für alle angreifbaren Elemente/CVEs, die in der NVD-Tabelle aufgeführt sind, zu vorhandenen TPEs, um eine Gesamtwahrscheinlichkeit für die Ausnutzung der Schwachstelle bereitzustellen.
- *`Remediation Effort Rollup`*: Fasst die Risikopunktzahlen für alle Datensätze in einer Korrekturmaßnahme zusammen, um eine Gesamtrisikopunktzahl für die Korrekturmaßnahme bereitzustellen.

Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Rechner für Schwachstellen-Rollup**.

Konfigurieren Sie den Rollup-Rechner, um anzugeben, wie viel Gewichtung jeder dieser berechneten Werte beim Festlegen der kumulativen Risikopunktzahl erhalten soll. Je höher die Gewichtung, desto mehr wird dieser Wert zur Bestimmung der zusammengefassten Risikopunktzahl in den Schwachstellen- oder Korrekturaufgaben verwendet.

Hinweis:
Wenn **Include verzögerte Elemente** ausgewählt ist, werden alle zurückgestellten angreifbaren Elemente in die Rollup-Berechnung für die Korrekturaufgaben einbezogen. Stellen Sie sicher, dass Sie die Auswirkungen auf die Gesamtberechnung verstehen, bevor Sie diese Option auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollup-Rechner führen alle 15 Minuten die geplante Aufgabe *`Rollup vulnerable item values to vulnerability and groups`*aus, um Änderungen zu übernehmen und die Details und Risikopunktzahlen für Korrekturaufgaben und Schwachstellen zusammenzufassen. Diese geplanten Aufgaben berechnen auch kumulative Werte für die Anzahl der VIs, die maximale Risikopunktzahl, das Zieldatum der Korrektur und den Status für Korrekturaufgaben.

Hinweis:
Berechnete Werte für Schwachstelleneinträge enthalten keine Korrekturzieldaten.

Die Risikopunktzahl wird berechnet, wenn:

- Risikopunktzahl, Korrekturziel, Korrekturstatus oder Schwachstellen-Changes für die angreifbaren Elemente.
- Der Status des angreifbaren Elements ändert sich in Offen, Zurückgestellt, Geschlossen oder ändert sich von Geschlossen oder Zurückgestellt.
- Angreifbare Elemente werden gelöscht.
- Angreifbare Elemente werden der Korrekturaufgabe hinzugefügt oder daraus entfernt.

Beispiel für den Schwachstellen-Rollup-Rechner: Betrachten Sie die Korrekturaufgabe VUL324567 mit den folgenden angreifbaren Elementen:

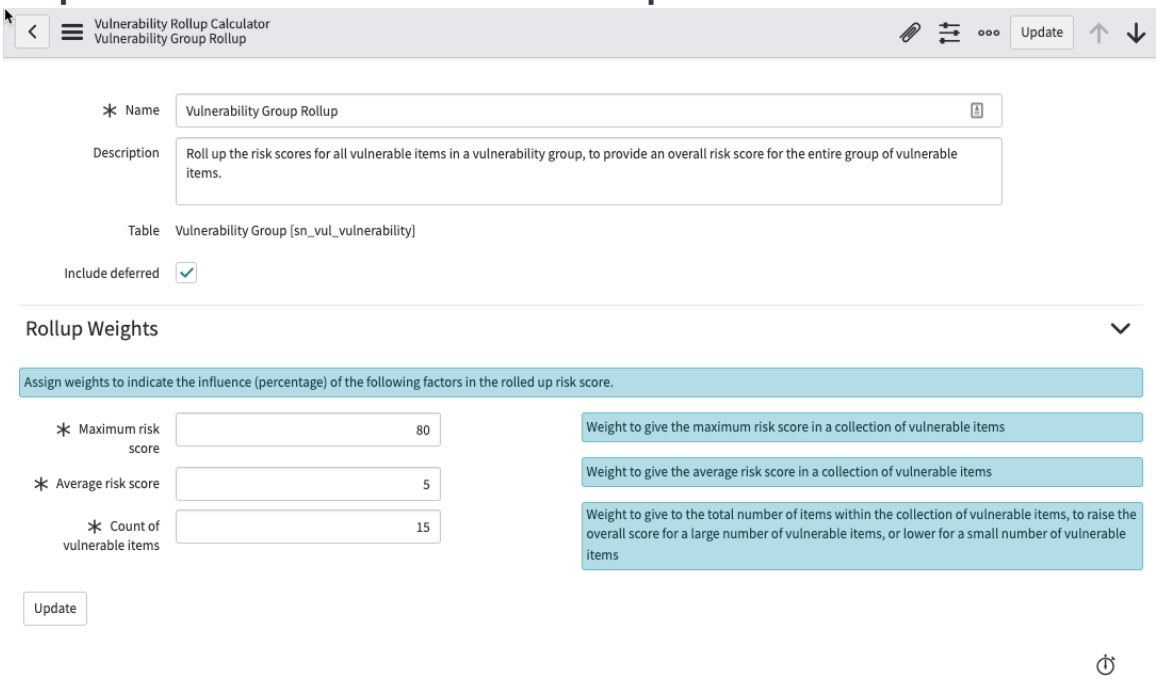
- VIT1001 mit Risikopunktzahl 30
- VIT1002 mit Risikopunktzahl 40
- VIT1003 mit Risikopunktzahl 50

Berücksichtigen Sie außerdem die folgenden Gewichtungen im Rechner für Schwachstellen-Rollup:

- Maximale Risikopunktzahl: 80
- Durchschnittliche Risikopunktzahl: 5
- Anzahl der angreifbaren Elemente: 15

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für den Rechner für Schwachstellen-Rollup



Im Beispiel des Schwachstellen-Rollup-Rechners lautet die Formel zur Bestimmung der **Risikopunktzahl** der Korrekturaufgabe:

(**Maximale Risikopunktzahl**/100) * 80 + (**Durchschnittliche Risikopunktzahl** /100) * 5 + (Faktor * 15)

Der Faktor wird wie folgt bestimmt:

VI-Anzahl	Faktor
<10	0,2
10–100	0,4
101-1000	0,6
1001-10000	0,8
> 10.000	1

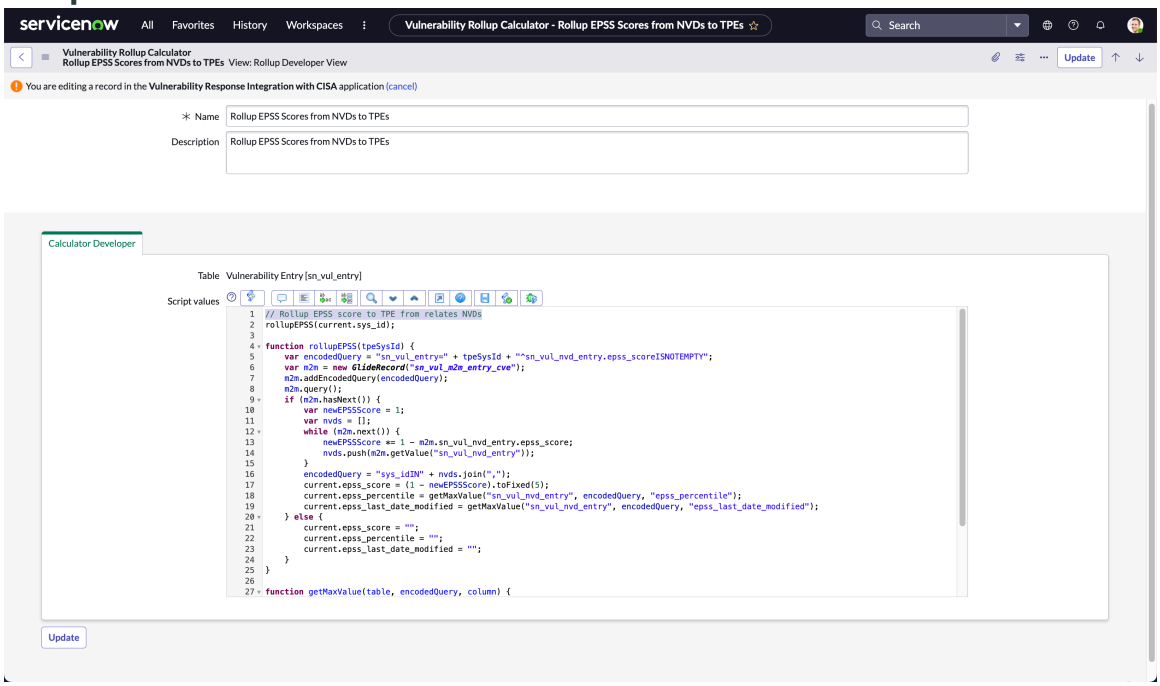
Für die Korrekturaufgabe VUL324567:

- Die durchschnittliche Risikopunktzahl beträgt 40
- Die maximale Risikopunktzahl beträgt 50
- 50 (Maximale Risikopunktzahl)
- Faktor ist 0,2

Die **Risikopunktzahl** wäre 45 [(50/100) * 80 + (40/100) * 5 + 0,2 * 15 = 40 + 2 + 3 = 45]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollup von EPSS-Punktzahlen von NVDs zu TPEs



EPSS-Rollup-Rechner – Beispiel

Betrachten Sie beispielsweise eine Organisation mit 100 Schwachstellen mit einer Wahrscheinlichkeit von jeweils 5 %, ausgenutzt zu werden. Die Frage, die für einen Netzwerkverteidiger von besonderem Interesse ist, könnte folgende sein: Wie hoch ist die Wahrscheinlichkeit, dass mindestens eine dieser Schwachstellen ausgenutzt wird, und wie hoch ist daher meine allgemeine Bedrohung? Die Wahrscheinlichkeit, dass mindestens ein Ereignis eintritt, ist einfach das Gegenteil von „keine Ereignisse“, d. h.:

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

Die Wahrscheinlichkeit, dass keine Schwachstellen vorhanden sind, ist das lineare Produkt jeder Schwachstelle, die nicht ausgenutzt wird. Da in diesem Beispiel die Wahrscheinlichkeit, dass Schwachstellen ausgenutzt werden, bei 5 % liegt, beträgt die Wahrscheinlichkeit, dass sie nicht ausgenutzt werden, jeweils 95 %. Und da es 100 davon gibt, können wir dies schreiben als:

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

Diese besagt, dass die Wahrscheinlichkeit, dass mindestens eine der Schwachstellen ausgenutzt wird, 99,4 % beträgt.

Wichtig:
Um *`Rollup EPSS Scores from NVD to TPEs`*zu ändern, müssen Sie die Kontextmenüansicht „Formular“ von der **Ansicht „Standard“** in **die Rollup-Entwickleransicht**ändern.

[store-future: BEGIN review]

Rollup-Berechnungen der Risikopunktzahl für Organisation

Die Funktion „Rollup für Risikopunktzahl der Organisation“ berechnet die Gesamtrisikopunktzahl für eine Organisation im einheitlichen Dashboard. Es fasst die Risikopunktzahlen für angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Konfigurationsprobleme zusammen. Zuvor wurde die maximale Risikopunktzahl durch Mittelung der Punktzahlen für VIT, AVIT, Testergebnisse

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und CVIT bestimmt. Ab Version 22 von Vulnerability Responsewird jedoch die maximale Risikopunktzahl durch die Auswahl der höchsten der vier Punktzahlen bestimmt.

Zur Berechnung der maximalen Risikopunktzahl wird die höchste Punktzahl unter VIT, AVIT, Testergebnissen und CVIT ausgewählt. Wenn beispielsweise VITs die höchste Punktzahl aufweisen, wird diese Punktzahl als maximale Risikopunktzahl betrachtet.

Sobald die Anzahlen von VIT, AVIT, CVIT und Testergebnissen ermittelt wurden, werden sie addiert und mithilfe einer Zählmethode normalisiert. Die resultierende Risikopunktzahl wird dann mit der in der Konfiguration angegebenen Anzahlgewichtung multipliziert.

Nach dem gleichen Verfahren wird die durchschnittliche Risikopunktzahl berechnet. Die Risikopunktzahlen für AVIT, Konfigurationsprobleme, Testergebnisse und andere Punktzahlen werden summiert und dann durch die Gesamtzahl geteilt, um die durchschnittliche Risikopunktzahl zu erhalten. Abschließend werden alle Risikopunktzahlen addiert, um die Risikopunktzahl der Organisation abzuleiten.

[End]

Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln

Nach der ersten Bewertung der Korrekturzielregeln im Setup-Assistenten können Schwachstellenmanager eine Korrekturzielregel auf Ebene des angreifbaren Elements einrichten, um die Behebung von Schwachstellen mit hohem Risiko zeitnah zu fördern. Wenn das Korrekturdatum für ein angreifbares Element näher rückt, wird eine Benachrichtigung an die in der Regel angegebenen Benutzer oder Gruppen gesendet.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Korrekturzielregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Name der Regel.
Ziel (Tage)	Geben Sie die Anzahl der Tage ab dem letzten Öffnen an, in denen die angreifbaren Elemente nachgebessert werden sollen.
V17.1: Ziel ab (Datum)	Datum, ab dem die Ziel-SLAs berechnet werden. Sie können nur das Datum oder die Felder für den Datums- und Uhrzeittyp angeben. Der Standardwert ist Datum der letzten Öffnung. Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1642413 .
Aktiv	Standardmäßig ist das Kontrollkästchen **Aktiv** aktiviert, was bedeutet, dass die Korrekturzielregel aktiv ist. Wenn dieses Kontrollkästchen deaktiviert ist, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Benachrichtigen (Tage vor dem Fälligkeitsdatum)	Anzahl der Tage vor der angestrebten Korrekturzeit, für die eine Benachrichtigung gesendet werden soll. Das mit diesem Wert berechnete Benachrichtigungsdatum wird verwendet, um den Korrekturstatus und die Farbcodierung anzuzeigen. Wenn das Datum vor dem Benachrichtigungsdatum liegt, lautet der Korrekturstatus „In Bearbeitung“. Wenn es nach dem Benachrichtigungsdatum und vor dem Korrekturzieldatum liegt, wird der Status als „Ziel erreicht“ angezeigt. **Hinweis:** Wenn dieses Feld auf 0 festgelegt ist, wird nur die Benachrichtigung **„Ziel verfehlt“** gesendet.
Beschreibung	Text, der die Korrekturzielregel beschreibt.
Bedingung	Wählen Sie mithilfe des Bedingungsfilters die Kriterien für die Anwendung der Regel auf die angreifbaren Elemente aus. Um eine Beeinträchtigung der Leistung zu vermeiden, testen Sie Ihre Bedingungen im vollen Produktionsmaßstab. Durch Tests können Sie bestimmen, wie lange die Ausführung des Auftrags **„Korrekturziele auswerten“** unter Berücksichtigung der Bedingungen und der Größe von Configuration Management Database (CMDB)dauert. Die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.
Benachrichtigungen **Hinweis:** Die in der Benachrichtigungs-E-Mail angezeigte Anzahl enthält keine angreifbaren Elemente im Status „ **Zurückgestellt“**, **„Gelöst“**oder **„Geschlossen“**.	
Anwender	Die zu benachrichtigenden Personen, wenn das ausgewählte angreifbare Element die Zielzeit für die Korrektur erreicht oder überschreitet.
Gruppe	Die Gruppe, die benachrichtigt werden soll, wenn das ausgewählte angreifbare Element die Zielzeit für die Korrektur erreicht oder überschreitet.
Update-Verlauf	
	Wird für die erstmalige Erstellung einer Regel nicht verwendet. Anschließend werden hier Systemarbeitsnotizen protokolliert.

4. Klicken Sie auf **Absenden**.
   Diese Regel tritt während der nächsten Ausführung der geplanten Aufgabe, *`Evaluate remediation targets`*, oder bei Verwendung der Schaltfläche **Changes anwenden** in der Listenansicht für Korrekturzielregeln in Kraft. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird. Weitere Informationen zur geplanten Aufgabe und **zum Anwenden von Changes**finden Sie unter Vulnerability Response Korrekturzielregeln.

Konfigurieren Sie installierte Drittanbieterintegrationen mit dem Setup-Assistenten

Konfigurieren Sie Vulnerability Response für die Verwendung mit allen Ihrer installierten Bereitstellungen von Drittanbieteranwendungen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration**.
2. Wählen Sie **Scannerintegrationen** aus, um die Bereitstellungen installierter Drittanbieteranwendungen zu konfigurieren.
3. Wenn Solution Management for Vulnerability Response installiert ist, können Sie **Lösungsintegrationen** auswählen, um die Anbieter Ihrer Schwachstellenlösungen zu konfigurieren.

Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten

Nachdem Sie die Anwendung Vulnerability Solution Management installiert haben, können Sie Ihre Anbieter von Schwachstellenlösungen mit dem Setup-Assistenten konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Eingabeaufforderungen im Setup-Assistenten für installierte Lösungsintegrationen für Solution Management for Vulnerability Responsezu ergänzen.

- Stellen Sie sicher, dass Vulnerability Solution Management und die gewünschten Lösungsintegrationen bereits installiert sind, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.
- Stellen Sie sicher, dass Anmeldeinformationen für Drittpartei-Accounts verfügbar sind. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten.
- Unter Anwendung Solution Management for Vulnerability Response installieren finden Sie weitere Informationen, bevor Sie installierte Lösungen konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen**.

   Integration der Microsoft Security Response Center-Lösung erfordert einen API-Schlüssel und eine URL von Microsoft Security Response Center, um es zu konfigurieren.

   Hinweis:
   Die Eingabe des API-Schlüssels ist für MSRCoptional. Um den Schlüssel MSRC zu erhalten, benötigen Sie eine Microsoft-ID von einem live.com-, outlook.com- oder Microsoft.com-E-Mail-Account, eine bei Microsoft registrierte Telefonnummer oder eine Kontoanmeldung bei Microsoft.

2. Geben Sie die URL ein.
   Die URL im Setup-Assistenten für MSRC lautet `https://api.msrc.microsoft.com`.
3. Klicken Sie auf **Fertigstellen**.
4. **Wahlweise:** Sie können Importe bei Bedarf ausführen, indem Sie auf der Konfigurationsseite auf **Jetzt ausführen** klicken, nachdem Sie Ihre Anmeldeinformationen eingegeben haben.
5. Red Hat Solution Integration ist ebenfalls verfügbar.
   Es ist kein API-Schlüssel erforderlich.
6. Klicken Sie im Setup-Assistenten rechts neben Red Hat Solution Integrationauf **Bearbeiten**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Vergewissern Sie sich, dass die URL im Setup-Assistenten für RHSIhttps://access.redhat.com/admin/restlautet
8. **Wahlweise:** Sie können Importe bei Bedarf ausführen, indem Sie auf der Konfigurationsseite auf **Jetzt ausführen** klicken.
9. Klicken Sie auf **Fertigstellen** und anschließend auf **Als abgeschlossen markieren,** um die Konfiguration abzuschließen.
   Wenn Sie die Konfiguration abgeschlossen haben, wird im Setup-Assistenten für Lösungsintegrationen ein Häkchen angezeigt.

Konfigurieren Sie die MS TVM-Schwachstellenintegration mit dem Setup-Assistenten

Konfigurieren Sie die Integration Vulnerability Response mit der Anwendung Microsoft Threat and Vulnerability Management (MS TVM), nachdem Sie sie mit dem Setup-Assistenten installiert haben.

Vorbereitungen

Führen Sie zusätzlich zu den Anweisungen und Eingabeaufforderungen im Setup-Assistenten für die Vulnerability Response -Integration mit Microsoft Threat and Vulnerability Management-Integration die folgenden Aktionen aus:

- Stellen Sie sicher, dass Sie die Anwendung bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.
- Unter Vorbereitung auf die Microsoft Threat and Vulnerability Management Vulnerability Integration finden Sie weitere Informationen, bevor Sie die Integration von Microsoft Threat and Vulnerability Management für Vulnerability Responsekonfigurieren.
- Stellen Sie sicher, dass die Anmeldeinformationen für das MS TVM-Konto verfügbar sind. Informationen zum Abrufen dieser Anmeldeinformationen finden Sie unter Richten Sie MicrosoftMicrosoft Azure Event Hubs Azure für die MS TVM-Integration ein.

Erforderliche Rolle: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.vulnerability_admin) oder sn_vul.admin (veraltet) und Integration konfigurieren (sn_vul_msft_tvm.configure_integration) für die -Konfiguration

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.

   Die Kachel Microsoft Threat & Vulnerability Management wird angezeigt.

   MS TVM ist eine Integration mit mehreren Quellen. Dies bedeutet, dass Sie mehrere Bereitstellungen derselben Drittanbieterintegration haben können. Die Einstellungen aus der ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

   Hinweis:
   Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

   Daten aus jeder Drittanbieterintegration sind eindeutig identifiziert und in einer einzigen Instanz von Vulnerability Responseverfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Klicken Sie zum Konfigurieren der Microsoft Threat and Vulnerability Management-Integration **auf Bearbeiten**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Account-Anmeldeinformationen“.

Feld	Beschreibung
Name	Name der Instanz.
TVM-Region	Region in der Nähe Ihres Serverstandorts. Verwenden Sie den Server in der Nähe Ihres Standorts, um eine optimale Leistung der API zu erzielen.
Authentifizierungstyp	Methode zum Überprüfen der Identität. Die Anwenderauthentifizierung steuert die Sichtbarkeit bestimmter Assets für bestimmte Anwender. MS TVM exportiert die Gerätegruppen, die für diesen Anwender berechtigt sind. Der Standardwert ist „Anwendung“.
Mandanten-ID	Mandantenidentität Ihrer Organisation.
Client-ID	Client-Identität, die nach der Registrierung von MS TVM in Microsoft Azure generiert wird.
Anwendername	Benutzer, der Zugriff auf die gesamte Gerätegruppe hat. Dieses Feld wird nur angezeigt, wenn Anwender als Authentifizierungstyp ausgewählt wird.
Passwort	Passwort für den Anwendernamen, der Zugriff auf die gesamte Gerätegruppe hat. Dieses Feld wird nur angezeigt, wenn Anwender als Authentifizierungstyp ausgewählt wird.
Geheimer Clientschlüssel	Geheimer Clientschlüssel, der nach der Registrierung der MS TVM-Anwendung generiert wird. Dieses Feld wird nur angezeigt, wenn Anwendung als Authentifizierungstyp ausgewählt wird.

4. Klicken Sie **auf Weiter**, um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren.
   Das Formular „Konfiguration des Imports von Schwachstellen“ wird angezeigt.
5. Aktivieren oder deaktivieren Sie den Import von Schwachstellen, legen Sie das anfängliche Startdatum für die zu importierenden Schwachstellen fest, und planen Sie, wann der Import von MS TVM-Schwachstellen ausgeführt werden soll.
   Wenn Sie alle Schwachstellen importieren möchten, lassen Sie das anfängliche Startdatum leer.
   a. Um Daten bei Bedarf zu importieren, klicken Sie auf **Schwachstellen jetzt importieren**.
   b. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen**.
6. Klicken Sie **auf Weiter**, um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren.
   Das Formular „Konfiguration des Empfehlungsimports“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Aktivieren oder deaktivieren Sie den Import von Empfehlungen, und legen Sie den Zeitplan fest, wann der Import von MS TVM-Schwachstellen ausgeführt werden soll.
   a. Um Daten bei Bedarf zu importieren, klicken Sie auf **Empfehlungen jetzt importieren**.
   b. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen**.
8. Klicken Sie **auf Weiter**, um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren.
   Das Formular „Konfigurationen des Rechnerimports“ wird angezeigt.
9. Aktivieren oder deaktivieren Sie den Import von Computern, legen Sie das anfängliche Startdatum für die zu importierenden Computer fest, und planen Sie, wann der Import von MS TVM-Computern ausgeführt werden soll.
   Wenn Sie alle Maschinen importieren möchten, lassen Sie das anfängliche Startdatum leer.

   Hinweis:
   Computer-Tags werden standardmäßig importiert und zum Organisieren und Nachverfolgen der in der MS TVM-Umgebung aufgeführten Computer verwendet.

   a. Klicken Sie zum Anzeigen der standardmäßigen CI-Suchregeln (Configuration Item, Konfigurationselement) auf **CI-Suchregeln**. CI-Suchregeln definieren, wie Maschinendaten aus Drittanbieterquellen zum Identifizieren von Configuration Items (CI) in Now Platform CMDBverwendet werden. Auf dieser Seite können Sie Suchregeln hinzufügen oder die standardmäßigen CI-Suchregeln ändern. Weitere Informationen finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.
   b. Um Daten bei Bedarf zu importieren, klicken Sie auf **Import Machines Now (Computer jetzt importieren)**.

   Hinweis:
   Computer, die in MS TVM den Status „Onboarding“ aufweisen, werden von der Anwendung ServiceNow abgerufen.

   c. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen**.
10. Klicken Sie **auf Weiter**, um Ihre Änderungen zu speichern und zum ersten Integrationsformular zu wechseln.
    Das Formular „Importkonfiguration für Computer-Schwachstellen“ wird angezeigt.
11. Aktivieren Sie die folgenden Integrationen, und bestimmen Sie das anfängliche Startdatum für die Schwachstellen, die Sie importieren möchten.

Formular „Konfigurationen des Imports von Computer-Schwachstellen“.

Integration	Beschreibung
Delta-Import von Microsoft TVM-Computer-Schwachstellen	Ruft Schwachstellen ab, die während des vollständigen Imports von Schwachstellen aktualisiert wurden, einschließlich neuer, behobener und aktualisierter Schwachstellen. Sie können Delta-Daten nur für die letzten 14 Tage importieren.
Vollständiger Import von Microsoft TVM-Computer-Schwachstellen	Ruft alle offenen Schwachstellen ab. Aufgrund des hohen Datenimportvolumens können Sie eine wöchentliche Ausführung planen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Führen Sie den Computerimport vor der Integration von Computer-Schwachstellen aus. Andernfalls werden für die fehlenden Computer keine VIs erstellt.

12. Klicken Sie auf **Fertigstellen**, um Ihre Änderungen zu speichern und die Konfiguration im Setup-Assistenten abzuschließen.

Nächste Maßnahme

Wenn Sie eine Gruppierung angreifbarer Elemente in der klassischen Umgebung aktivieren möchten, navigieren Sie zu > **Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben** > **Microsoft TVM-Empfehlung**.

Wählen Sie im angezeigten Formular die Option **Aktiv** aus, um sie zu aktivieren. Alternativ können Sie **Neu** wählen, um eine neue Regel zu erstellen.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

Qualys Vulnerability Integration mit dem Setup-Assistenten konfigurieren

Nachdem Sie die Anwendung Qualys installiert haben, konfigurieren Sie sie mit dem Setup-Assistenten.

Vorbereitungen

Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Eingabeaufforderungen im Setup-Assistenten für die Konfiguration von Qualys Vulnerability Integrationzu ergänzen.

- Vergewissern Sie sich, dass die Anwendung bereits installiert ist, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.
- Unter Vorbereitung auf das Qualys Vulnerability Integration finden Sie weitere Informationen, bevor Sie Qualys Vulnerability Integrationkonfigurieren.
- Stellen Sie sicher, dass Anmeldeinformationen für Drittpartei-Accounts verfügbar sind. Sie sind erforderlich, um einige Anwendungen von Drittparteien zu bearbeiten.

Erforderliche Rolle: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.vulnerability_admin) oder sn_vul.admin (veraltet) für die Konfiguration.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
   Die installierten Integrationen werden angezeigt.
2. Klicken Sie rechts neben Qualys Vulnerability Integration, das Sie konfigurieren möchten, **auf Bearbeiten**.
3. Geben Sie im Formular „Account-Anmeldeinformationen“ Ihre Qualys Cloud Platform -Anmeldeinformationen ein.
   Zur Konfiguration sind Ihre Anmeldeinformationen erforderlich.
4. Verwenden Sie die folgenden Hinweise als Leitfaden, während Sie mit der Konfiguration fortfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Über den Link **Erweiterte Einstellungen** gelangen Sie zum Integrationsdatensatz Qualys. Sie können Parameter hinzufügen, die vom Produkt Qualys für Ihre geplanten Abfragen unterstützt werden, um die importierten Schwachstellendaten zu filtern. Weitere Informationen finden Sie unter Legen Sie zusätzliche Filterparameter für Qualys -Importe fest.
- Wenn Sie das Upgrade von einer früheren Version von Vulnerability Response mit einer bereits konfigurierten Version von Qualys Vulnerability Integration durchgeführt haben, ist diese Version mit beibehaltenen Konfigurationseinstellungen weiterhin verfügbar.

  Unter „Importeinstellungen“ in der Host-Erkennungskonfiguration für Qualys Vulnerability Integrationfinden Sie eine Option zum Anzeigen der Datensätze der Erkennung behobener Qualys -Schwachstellen. Wenn diese Option aktiviert ist, können Sie angreifbare Elemente aus Erkennungsdatensätzen in einem festen Status (Status =**Behoben**) erstellen. Weitere Informationen zur Erkennung von angreifbaren Elementen finden Sie unter Vulnerability Response Erkennungen von angreifbaren Elementen durch Integrationen von Drittparteien.

  Auf der Seite „Konfiguration der Host-Erkennung“ können Sie das Kontrollkästchen **„Suche nach Netzwerkpartition“** aktivieren, um den Bezeichner der Netzwerkpartition in die IP-Adressensuche einzubeziehen. Weitere Informationen finden Sie unter Aktualisieren Sie Configuration Items mit dem Netzwerkpartitionsbezeichner für Qualys Vulnerability Integration.

  Alle Host-Tags werden als Teil der Qualys -Hostlisten-Integration importiert. Host-Tags werden hauptsächlich zum Filtern in Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben verwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

  Hinweis:
  Die Integration der Hostliste Qualys muss vor der Erstellung von Regeln für Zuweisungs- oder Korrekturaufgaben in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

  Qualys **Asset-Tags** werden im Modul „Host-Tags“ unter Qualys Vulnerability Integrationgespeichert.

- Qualys Vulnerability Integration unterstützt mehrere Quellen. Sie können mehrere Bereitstellungen derselben Drittparteiintegration haben. Um eine weitere Integration hinzuzufügen, klicken Sie auf der Seite Scanner-Integrationen **auf Integration hinzufügen**.

  Die Einstellungen aus der ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

  Hinweis:
  Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

  Daten aus jeder Drittanbieterintegration sind eindeutig identifiziert und in einer einzigen Instanz von Vulnerability Responseverfügbar.

- Sie können Importe bei Bedarf ausführen, indem Sie auf einer Konfigurationsseite **auf Jetzt ausführen** klicken.

5. Klicken Sie auf **Fertigstellen**, um die Konfiguration im Setup-Assistenten abzuschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten

Nachdem Sie die Anwendung Vulnerability Response Integration with Tenable installiert haben, konfigurieren Sie sie mit dem Setup-Assistenten.

Vorbereitungen

Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Eingabeaufforderungen im Setup-Assistenten für die Integration Vulnerability Response Integration with Tenable zu ergänzen.

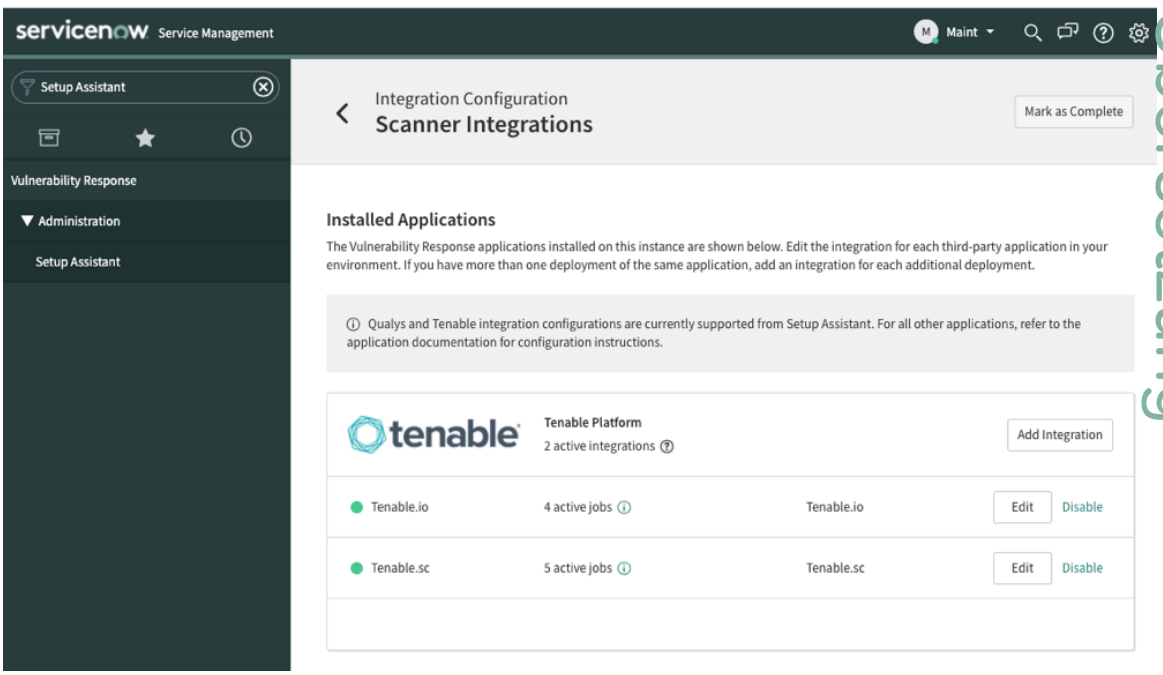
- Vergewissern Sie sich, dass die Anwendung bereits installiert ist, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.
- Unter Vorbereitung der Tenable Vulnerability-Integration finden Sie weitere Informationen, bevor Sie Tenable for Vulnerability Responsekonfigurieren.
- Stellen Sie sicher, dass Anmeldeinformationen für Drittpartei-Accounts verfügbar sind. Sie sind erforderlich, um einige Anwendungen von Drittparteien zu bearbeiten.

Erforderliche Rolle: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.vulnerability_admin) oder sn_vul.admin (veraltet) und Integration konfigurieren (sn_vul_tenable.configure_integrations) für die -Konfiguration.

Prozedur

1. Wenn er nicht angezeigt wird, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.

   Die Integrationen Tenable.io und Tenable.sc werden angezeigt.



   Tenable ist eine Integration mit mehreren Quellen, und Sie können mehrere Bereitstellungen derselben Drittanbieterintegration haben. Die Einstellungen aus der ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Daten aus jeder Drittanbieterintegration sind eindeutig identifiziert und in einer einzigen Instanz von Vulnerability Responseverfügbar.

2. Klicken Sie rechts neben der Tenable-Integration, die Sie konfigurieren möchten, auf **Bearbeiten**.
3. Füllen Sie die Felder im Formular „Account-Anmeldeinformationen“ aus.

   - Tenable.io erfordert Administratorzugriff mit einem Berechtigungsattribut, das größer oder gleich 64 ist.

     Hinweis:
     Ab v3.8 von Vulnerability Response Integration with Tenable sind für den Zugriff auf Tenable.io keine Administratorrechte mehr erforderlich. Ein Standardbenutzer mit einem Berechtigungsattribut gleich 16 kann ebenfalls auf das Produkt zugreifen.

   - Tenable.sc erfordert Sicherheitsanalysten- oder Managerzugriff.

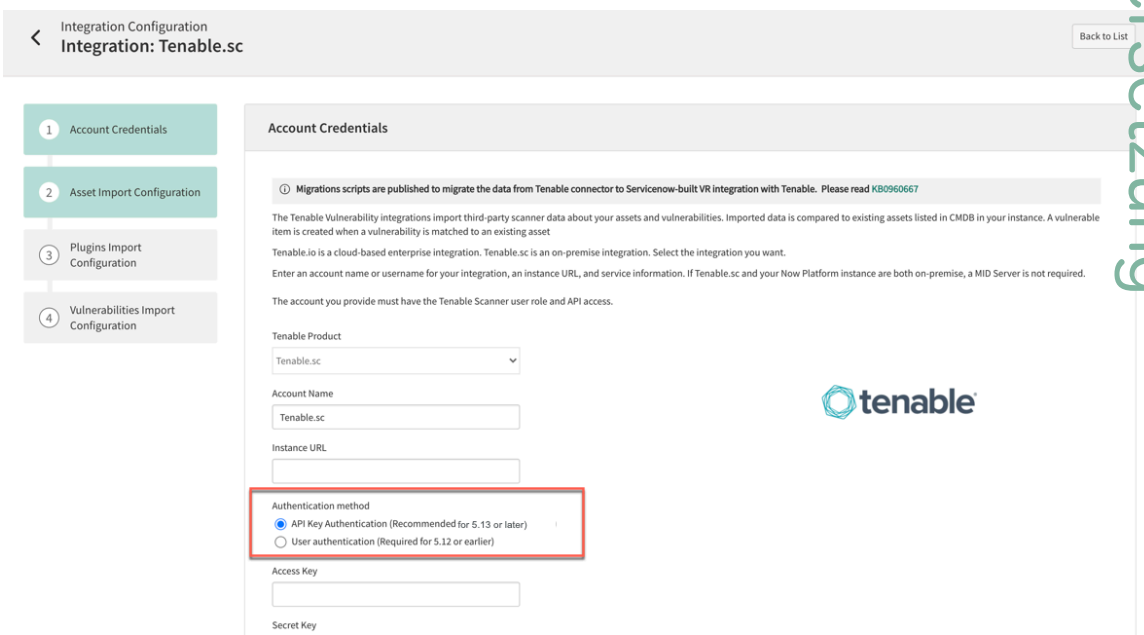
   a. Wählen Sie Ihr Tenable-Produkt aus.

   b. Geben Sie Ihren Tenable-Accountnamen ein.

   c. Geben Sie im Feld Instanz-URL die URL für Ihre Tenable-Plattform ein.

   d. Wählen Sie eine Authentifizierungsmethode aus.

      Je nach Version von Tenable.schaben Sie zwei Optionen für die Authentifizierung:



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Ab v5.13 von Tenable.scwählen Sie **die API-Schlüsselauthentifizierung**aus. Geben Sie Ihren Tenable-Zugriff und Ihre geheimen Schlüssel ein.

ii. Vor v5.13 wird die Anwenderauthentifizierung von Ihrer Instanz Now Platform® unterstützt und ist erforderlich. Geben Sie Ihren Now Platform -Anwendernamen und Ihr Passwort ein.

Für Tenable.scwird nur die API-Schlüsselauthentifizierung unterstützt. Geben Sie Ihren Tenable-Zugriff und Ihre geheimen Schlüssel ein.

e. **Wahlweise:** Wählen Sie einen MID Server aus.

(Optional) Wenn sich Ihre Instanz Now Platform und die Anwendung Tenable.sc nicht am selben Speicherort befinden, wählen Sie einen konfigurierten MID-Server aus der Auswahlliste aus. Weitere Informationen finden Sie unter MID-Server .

- Ab v15.0 von Vulnerability Response und v3.0 von Tenable Vulnerability Integrationkönnen Sie den Parameter `Async_request` wie in Datenabrufeinstellungen für die Tenable Vulnerability-Integrationbeschrieben aktivieren. Tenable muss entsprechend konfiguriert werden, wenn Sie synchrone Aufrufe tätigen möchten. Wenden Sie sich an das Tenable-Produkt, um Hilfe zu erhalten. Sobald dieser Parameter aktiviert ist, gilt er für alle Integrationen von Tenable.sc und es gibt eine Zeitüberschreitung von 30 Sekunden. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**.

- (Optional) Für bestehende Kunden ist ein Korrekturskript verfügbar, wenn Sie asynchrone Anrufe verwenden.

Wenn Ihre Now Platform -Instanz und Ihre Tenable.sc -Anwendung beide lokal sind, aber nicht erforderlich sind, können Sie in der Auswahlliste einen konfigurierten MID-Server auswählen.

Hinweis:
Unabhängig davon, ob Sie einen MID-Server verwenden oder nicht, laufen die Integrationen nach fünf Minuten ab, und wenn keine Antwort vom Server eingeht, wird eine Meldung angezeigt.

(Optional) Wenn ein Zeitüberschreitungsfehler auftritt, überprüfen Sie im Setup-Assistenten, ob Sie die richtigen Anmeldeinformationen und die richtige URL eingegeben haben.

4. Klicken Sie **auf Weiter**, um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren.
Das Formular „Asset-Importkonfiguration“ wird angezeigt.

5. In diesem Formular können Sie die Asset-Importintegration aktivieren oder deaktivieren, das anfängliche Startdatum für die zu importierenden Assets festlegen und planen, wann der Tenable-Asset-Import ausgeführt werden soll.

Für Tenable.io

- Assets Integration kann mit den Tenable.io Compliance-Ergebnissen und der Compliance-Ergebnisauffüllungs-Integration verwendet werden, um sichere Konfigurationsbewertungsdaten zu Ihren Assets in die Anwendung Konfigurations-Compliance zu importieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Version 12.2 der Anwendung Konfigurations-Compliance ist in Ihrer Instanz erforderlich, wenn Sie diese sicheren Konfigurationsbewertungsdaten importieren und anzeigen möchten.

  Unter Konfigurations-Compliance importierte Daten finden Sie weitere Informationen dazu, welche Daten mit diesen Integrationen importiert und wo sie veröffentlicht werden.

- Die Tenable.io Compliance-Ergebnisse und Compliance-Ergebnisauffüllungs-Integrationen sind standardmäßig nicht aktiviert. Wenn Sie sie aktivieren, möchten Sie möglicherweise die bereitgestellten Standardzeitplaneinstellungen verwenden. In den unten aufgeführten Schritten erfahren Sie, wie Sie Integrationen für Tenable Vulnerability Integrationsuchen und aktivieren.
- Sie können bei Bedarf von Ihrer -Instanz aus einen erneuten Scan auf angreifbare Elemente für das Produkt Tenable.io initiieren. Die Tenable.io Template Integration und die Tenable.io Scan Credential Integration müssen aktiviert werden, bevor erneute Scans initiiert werden können.

Standardmäßig sind diese Integrationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für Tenable.ioeingeben, werden alle Tenable.io Integrationen automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

a. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.

b. Suchen Sie in der angezeigten Liste nach den Tenable.io Integrationsdatensätzen, die Sie benötigen.

c. Öffnen Sie jeden Datensatz, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren.

d. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

e. Kehren Sie zum Setup-Assistenten zurück, um mit der Konfiguration für Tenable Vulnerability Integration mit Vulnerability Responsefortzufahren.

- Für die Tenable.io -Integration haben Sie auch die Möglichkeit, den Import von Asset-Tags zu aktivieren und zu deaktivieren. Asset-Tags werden standardmäßig importiert und zum Organisieren und Nachverfolgen der in Ihrer CMDB in der Umgebung Tenable.io aufgeführten Assets verwendet.
- Wenn Sie für die Produkte Tenable.io und Tenable.sc unter Suche **nach Netzwerkpartition die Option Suche nach Netzwerkpartition aktivieren** auswählen, können Sie mit der Engine Identification and Reconciliation (IRE) einzelne CIs erstellen, die über dieselbe IP-Adresse verfügen. Siehe Aktualisieren Sie Configuration Items mit dem Netzwerkpartitionsbezeichner für Tenable Vulnerability Integration und CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt, um weitere Informationen zu erhalten.
- Klicken Sie oben im Bildschirm neben dem Link Asset-Import auf den Link **CI-Suchregeln**, um die standardmäßigen Suchregeln für Configuration Item (CI) anzuzeigen. CI-Suchregeln definieren, wie Asset-Daten aus Drittanbieterquellen zum Identifizieren von Configuration Items (CI) in der Now Platform -CMDB verwendet werden. Auf dieser Seite können Sie Suchregeln hinzufügen oder die standardmäßigen CI-Suchregeln ändern. Weitere Informationen finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.
- Klicken Sie auf **Assets jetzt importieren**, um Daten bei Bedarf zu importieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Über den Link **Erweiterte Einstellungen** gelangen Sie zum Datensatz Asset-Integration. Ab v3.3 können Sie Parameter hinzufügen, die vom Produkt Tenable.io für Ihre geplanten Abfragen unterstützt werden, um die Schwachstellendaten zu filtern, die Sie mit den Assets Tenable.io sowie den Integrationen für feste und offene Schwachstellen importieren. Weitere Informationen finden Sie unter Legen Sie zusätzliche Filterparameter für Tenable.io -Importe fest.

6. Klicken Sie **auf Weiter**, um Ihre Änderungen zu speichern und mit dem nächsten Formular fortzufahren. Das Formular „Plugins-Importkonfiguration“ wird angezeigt.
7. Aktivieren oder deaktivieren Sie in diesem Formular den Import von Plugins (Schwachstelleneinträge von Drittparteien), bestimmen Sie das anfängliche Startdatum für die Plugins, die Sie importieren möchten, und planen Sie, wann der Import der Tenable-Plugins ausgeführt werden soll.

   Wenn Sie alle Plugins, Schwachstellen und Assets importieren möchten, lassen Sie das anfängliche Startdatum leer.

   - Klicken Sie auf **Plugins jetzt importieren,** um Daten bei Bedarf zu importieren.
   - Über den Link **„Erweiterte Einstellungen“** gelangen Sie zum Datensatz „Plugins Integration“.
   - Für den Import von Schwachstellen können Sie einen Zeitplan erstellen und Schweregrade für Tenable.io für die Schwachstellen festlegen, die erfasst werden sollen. Legen Sie ein Datum fest, damit nur die Schwachstellen importiert werden, die ab einem bestimmten Datum erstellt oder aktualisiert wurden.
   - Für die Integration Tenable.sc können Sie einen Abfragefilter und ein Datum festlegen, sodass nur die Schwachstellen importiert werden, die ab einem bestimmten Datum erstellt oder aktualisiert wurden.
8. Klicken Sie **auf Weiter**, um Ihre Änderungen zu speichern und mit dem nächsten Formular fortzufahren. Das Formular „Konfiguration des Imports von Schwachstellen“ wird angezeigt. Aktivieren oder deaktivieren Sie die Integration, und bestimmen Sie das anfängliche Startdatum für die Schwachstellen, die Sie importieren möchten.

   Für das Produkt Tenable.io :

   - Importieren Sie nur die Schwachstellen und die zugehörigen VIs, die den von Ihnen mit dem Schweregradfilter ausgewählten Bedingungen entsprechen.
   - Für die Asset-Integration Tenable.io wird `Last Scan Time` nur für Assets importiert und aktualisiert, die Schwachstellen aufweisen.
   - Aktivieren Sie die Option **Behobene Schwachstellen,** um VIs für Datensätze mit behobener Erkennung anzuzeigen. Wenn diese Kennzeichnung im Setup-Assistenten aktiviert ist, werden neue VIs für Erkennungen im Status **„Fest“** erstellt, die in Ihrer Instanz noch nicht vorhanden sind. Wenn diese Funktion aktiviert ist, kann sie sich negativ auf Ihre Erfassungsleistung auswirken.
   - Der Link **Erweiterte Einstellungen** neben Importfilter verweist Sie auf den Datensatz Integration der Schwachstellen.
   - Klicken Sie oben auf den Link **Zeitpläne importieren,** um zu konfigurieren, wie oft Schwachstellen erfasst werden, und aktivieren Sie die Integration.

   Für das Produkt Tenable.sc :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Importieren Sie nur die Schwachstellen und zugehörigen VIs, die den von einer Tenable-Abfrage in der Tenable-Plattform festgelegten Bedingungsfiltern entsprechen. Weitere Informationen zu Tenable-Abfragen finden Sie in der Tenable-Dokumentation.

  Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für die Tenable.sc Assets Integration. Nur die Assets mit den Schwachstellen, die den Bedingungen des Abfragefilters entsprechen, werden importiert.

- Aktivieren Sie die Option **Behobene Schwachstellen,** um VIs für Datensätze mit behobener Erkennung anzuzeigen. Wenn diese Kennzeichnung im Setup-Assistenten aktiv ist, werden neue VIs für Erkennungen im Status **„Fest"** erstellt, die in Ihrer Instanz noch nicht vorhanden sind. Wenn diese Funktion aktiv ist, kann sie sich negativ auf Ihre Erfassungsleistung auswirken.
- Um den Netzwerkpartitionsbezeichner in die IP-Adressensuche einzubeziehen, wählen Sie **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen aus **Suche nach Netzwerkpartition** Abschnitt. Weitere Informationen finden Sie unter Aktualisieren Sie Configuration Items mit dem Netzwerkpartitionsbezeichner für Tenable Vulnerability Integration.
- Klicken Sie oben auf **Zeitpläne importieren,** um zu konfigurieren, wie oft Schwachstellen erfasst werden, und aktivieren Sie die Integration.
- Der Link **Erweiterte Einstellungen** neben Importfilter verweist Sie auf den Datensatz Integration der Schwachstellen.
- Die ServiceNow® Tenable.sc Integration zum Scannen von Anmeldeinformationen wird automatisch über den Setup-Assistenten in Ihrer Instanz aktiviert (Aktiv), wenn Sie die Integrationen für Tenable.sc Schwachstellen (Tenable.sc Integrationen offener und fester Schwachstellen) konfigurieren.

  Diese Integration importiert und aktualisiert Scanner-Anmeldeinformationen aus dem -Produkt Tenable.sc in Ihrer -Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationen zu importieren und sicher zu speichern. Navigieren zu **Tenable-Schwachstellen-Integration** > **Integrationen** > **Integration von Tenable.sc-Scan-Anmeldeinformationen** um weitere Informationen zur Integration der Scan-Anmeldeinformationen anzuzeigen.

9. Klicken Sie auf **Fertigstellen**, um Ihre Änderungen zu speichern und die Konfiguration im Setup-Assistenten abzuschließen.

Nächste Maßnahme

(Optional) Navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Schwachstellen-Rechner** > **Standardrisikorechner** > **Tenable-Risikoregel** um die Tenable-Risikoregel zu aktivieren.

Aktivieren Sie im angezeigten Formular „Regel des Schwachstellen-Rechners" das Kontrollkästchen Aktiv.

Die Tenable-Risikoregel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisiko-Rechners in den Schwachstellen-Rechnern von Vulnerability Responseinstalliert. Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit dem neuen Standardrisikorechner verwendet wird. Diese Risikoregel ist standardmäßig deaktiviert. Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte verwendet, um die Risikopunktzahl für angreifbare Elemente zu berechnen. Standardgewichtsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Business-Relevanz = 15 %. Das Aktivieren dieser Regel des Tenable-Risikorechners kann sich auf die Leistung der Datenerfassung auswirken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners

Lösungsanbieter für Schwachstellen einrichten

Richten Sie Schwachstellenlösungsanbieter ein, indem Sie die Prüfliste befolgen und dann die Anbieter im Setup-Assistenten konfigurieren.

Bereiten Sie die Prüfliste für die Lösungsintegration vor

Verwenden Sie den Setup-Assistenten, um die Implementierung einer Solution Intelligence-Integration für alle Lieferanten vorzubereiten, die das Datenformat Common Vulnerability Reporting Framework (CVRF) oder Common Security Advisory Framework (CSAF) unterstützen.

Integration der CVRF-Lösung (Common Vulnerability Reporting Framework) wird vorbereitet

Verwenden Sie den Setup-Assistenten, um die Implementierung einer Solution Intelligence-Integration für alle Lieferanten vorzubereiten, die das Datenformat des Common Vulnerability Reporting Framework (CVRF) unterstützen.

Bevor Sie beginnen

Um die Integration mit den Lieferanten zu integrieren, die die Lösungen bereitstellen, müssen Sie die Aufgaben in der folgenden Prüfliste ausführen. Sie können die Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren.

Prüfliste für die Vorbereitung der Integration

Aufgabe	Beschreibung
Abhängige Anwendungen ☐	Stellen Sie sicher, dass die folgenden Anwendungen von ServiceNow Storeinstalliert sind: • Vulnerability Solution Management: Weitere Informationen zur Installation von Vulnerability Solution Managementfinden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten und Anwendung Solution Management for Vulnerability Response installieren. • Vulnerability Response: Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher.
Anmeldeinformationen für Drittparteikonto ☐	Stellen Sie sicher, dass Anmeldeinformationen für Drittpartei-Accounts verfügbar sind. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
Lieferantenauthentifizierung ☐	Stellen Sie sicher, dass Sie die Lieferanten für den Import von Lösungen mithilfe der APIs authentifiziert haben. Weitere Informationen zur Authentifizierung von Lieferanten finden Sie unter Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen. Wenn Sie keinen API-basierten Lieferanten konfigurieren möchten, können Sie diesen Schritt überspringen.
Anpassung von Flow und Flow-Aktion ☐	Wenn Sie einen anderen API-basierten Lieferanten als Cisco konfigurieren möchten, müssen Sie den Flow und die Flow-Aktion für das Extrahieren eines eindeutigen Schlüssels und einer CVRF-URL aus der Antwort auf eine Beratung anpassen. **Hinweis:** Das Veröffentlichen der CVRF-URL ist nicht bei allen Anbietern Standard. Informationen zum Anpassen des -Flows für andere Anbieter als Cisco finden Sie unter Einen anderen Common Vulnerability Reporting Framework-Anbieter als Cisco konfigurieren. Sie können diesen Schritt überspringen, wenn keine anderen Lieferanten als Cisco konfiguriert werden sollen. Standardmäßig wird der Flow für Cisco mit der Anwendung bereitgestellt.
Rollen ☐	Vergewissern Sie sich, dass Sie über eine Administratorgruppe oder einen Benutzer verfügen, der bzw. der die Integration verwalten kann. Wenn dies nicht zugewiesen ist, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu.

Integration der CSAF-Lösung (Common Security Advisory Framework) wird vorbereitet

Verwenden Sie den Setup-Assistenten, um die Implementierung einer Solution Intelligence-Integration für alle Lieferanten vorzubereiten, die das Datenformat des Common Security Advisory Framework (CSAF) unterstützen.

Bevor Sie beginnen

Um die Integration mit den Lieferanten zu integrieren, die die Lösungen bereitstellen, müssen Sie die Aufgaben in der folgenden Prüfliste ausführen. Sie können die Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration

Aufgabe	Beschreibung
Abhängige Anwendungen ☐	Stellen Sie sicher, dass die folgenden Anwendungen von ServiceNow Storeinstalliert sind: • Vulnerability Solution Management: Weitere Informationen zur Installation von Vulnerability Solution Managementfinden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten und Anwendung Solution Management for Vulnerability Response installieren. • Vulnerability Response: Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher.
Anmeldeinformationen für Drittparteikonto ☐	Stellen Sie sicher, dass Anmeldeinformationen für Drittpartei-Accounts verfügbar sind. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten.
Lieferantenauthentifizierung ☐	Stellen Sie sicher, dass Sie die Lieferanten für den Import von Lösungen mithilfe der APIs authentifiziert haben. Weitere Informationen zur Authentifizierung von Lieferanten finden Sie unter Aliasse für Verbindungen und Anmeldeinformationen für CSAF (Common Security Advisory Framework) konfigurieren. Wenn Sie keinen API-basierten Lieferanten konfigurieren möchten, können Sie diesen Schritt überspringen.
Anpassung von Flow und Flow-Aktion ☐	Wenn Sie einen anderen API-basierten Lieferanten als Red Hatkonfigurieren möchten, müssen Sie den Flow und die Flow-Aktion für das Extrahieren eines eindeutigen Schlüssels und einer CSAF-URL aus der Antwort auf eine Beratung anpassen. **Hinweis:** Die Veröffentlichung der CSAF-URL ist nicht bei allen Lieferanten Standard. Informationen zum Anpassen des -Flows für andere Lieferanten als Red Hatfinden Sie unter Konfigurieren Sie einen anderen Anbieter des Common Security Advisory Framework als Red Hat. Sie können diesen Schritt überspringen, wenn keine anderen Lieferanten als Red Hatkonfiguriert werden sollen. Standardmäßig wird der -Flow für Red Hat mit der Anwendung bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
Rollen ☐	Vergewissern Sie sich, dass Sie über eine Administratorgruppe oder einen Benutzer verfügen, der bzw. der die Integration verwalten kann. Wenn dies nicht zugewiesen ist, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu.

Konfigurieren Sie die Anbieter von Schwachstellenlösungen

Nachdem Sie die Anwendung Vulnerability Solution Management installiert haben, konfigurieren Sie die Anbieter der Schwachstellenlösungen mit dem Setup-Assistenten.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration**.
2. Klicken Sie auf **Lösungsintegrationen**.
3. Rufen Sie im Abschnitt Installierte Lösungen Daten mithilfe einer URL, einer API oder eines Imports ab.
   - Um Daten mithilfe einer URL oder API abzurufen, klicken Sie auf **Integration hinzufügen**.
   - Um Daten durch Hochladen einer CVRF-Datei (Common Vulnerability Response Framework) oder CSAF-Datei (Common Security Advisory Framework)abzurufen, klicken Sie auf **Datei importieren**.

Nächste Maßnahme

Je nachdem, in welchem Format Sie die -Daten inimportieren möchten, können Sie eine der folgenden Aufgaben ausführen:

- Für CVRF:
  - Wenn Sie eine CVRF-Datei importieren möchten, lesen Sie Importieren Sie Common Vulnerability Reporting Framework-Daten über einen Dateiimport.
  - Wenn Sie CVRF-Daten mithilfe der APIs importieren möchten, lesen Sie Importieren Sie CVRF-Daten (Common Vulnerability Reporting Framework) über die CVRF-URL.
  - Wenn Sie CVRF-Daten über Hinweise importieren möchten, lesen Sie unter Common Vulnerability Reporting Framework-Daten aus Hinweismeldungen importierennach.
- Für CSAF:
  - Wenn Sie eine CSAF-Datei importieren möchten, lesen Sie Importieren Sie Framework-Daten für Sicherheitswarnhinweise über einen Dateiimport.
  - Wenn Sie CSAF-Daten mithilfe der APIs importieren möchten, finden Sie weitere Informationen unter Importieren Sie CSAF-Daten (Common Security Advisory Framework) über die CSAF-URL.
  - Wenn Sie CSAF-Daten über Beratungshinweise importieren möchten, lesen Sie unter Importieren Sie Framework-Daten für Sicherheitswarnhinweise aus Hinweismeldungennach.
-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Common Vulnerability Reporting Framework (CVRF)

Das Common Vulnerability Reporting Framework (CVRF) bietet ein standardisiertes Framework für die Erstellung von Dokumentationen zu Schwachstellenberichten. Es handelt sich um eine XML-basierte Sprache, die die gemeinsame Nutzung wichtiger sicherheitsbezogener Informationen zwischen verschiedenen Stakeholdern in mehreren Organisationen vereinfacht. Durch die Verwendung des CVRF-Formats können Informationsaustausch und -verarbeitung beschleunigt werden.

Importieren Sie Common Vulnerability Reporting Framework-Daten über einen Dateiimport

Importieren Sie eine CVRF-Datei, um Daten im CVRF-Format anzuzeigen. Der Importvorgang ist eine einmalige Aktivität.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin.

Warum und wann dieser Vorgang ausgeführt wird

Nach dem Import wird ein Warteschlangeneintrag mit einem Anhang erstellt, der bei der Verarbeitung des Eintrags analysiert wird. Die Daten werden dann in die entsprechenden Tabellen gefüllt. Vor dem Analysieren der CVRF-Daten wird basierend auf der Konfiguration ein Scanner-Zuordnungsdatensatz erstellt. Anschließend werden die Scannerzuordnungsdaten in Lieferantenzuordnungsdaten umgewandelt.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Common Vulnerability Response Framework**.
2. Klicken Sie auf **Datei importieren**.

   Hinweis:
   Sie können jeweils nur eine XML-Datei mit einer maximalen Dateigröße von 1 GB hochladen.

3. Geben Sie im Feld **Name** einen eindeutigen Namen für die Integration ein.
   Der Zeitplaner wird mit diesem Namen erstellt.
4. Geben Sie im Feld **Lieferant** den Namen des Lieferanten ein.
   Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt.
5. Klicken Sie auf **Fertigstellen**.

Ergebnisse

Eine Importwarteschlange wird erstellt. Klicken Sie auf den Link in der Infoleiste, um die Warteschlangeneinträge für den Lieferanten zusammen mit der zugehörigen Liste anzuzeigen. Sie können auch den Status des Auftrags anzeigen.

Nachdem die Daten in das CVRF-Format importiert wurden, werden sie wie folgt verarbeitet:

1. Bei der Verarbeitung der Warteschlange wird die Datei mit einer dedizierten Datenquelle analysiert.
2. Sobald die Verarbeitung abgeschlossen ist, wird das Anwendungsprotokoll aktualisiert.
3. Sobald die CVRF-XML-Datei analysiert wurde, werden die folgenden Tabellen in der Anwendung ServiceNow® Vulnerability Response gefüllt.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_nvd_entry
- sn_vul_software
- sn_vul_product_category

Detaillierte Informationen zu Fehlern oder Ausnahmen finden Sie in den Anwendungsprotokollen.

Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen

Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen, um Lieferanten zu authentifizieren. Bei der Beratungsanalyse werden Drittanbieter authentifiziert.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

Prozedur

1. Erstellen Sie die OAuth-Authentifizierung.
   Weitere Informationen finden Sie unter Endpunkte für Clients zum Zugriff auf die Instanz erstellen .
2. Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen.
   Weitere Informationen finden Sie unter Alias für Verbindungen und Anmeldeinformationen erstellen .
3. Erstellen Sie eine Verbindung.
   a. Klicken Sie auf den Namen des neu erstellten Alias für Verbindungen und Anmeldeinformationen.
   b. Klicken Sie auf der Registerkarte **Verbindungen** auf **Neu**.
   c. Wenn der Authentifizierungstyp OAuth ist, wählen Sie das in Schritt 1 erstellte Anwendungsregistrierungsprofil als **OAuth-Entitätsprofil**aus.
   d. Erstellen Sie einen Datensatz in „Verbindungen“ anhand der zugehörigen Liste des Datensatzes.
   e. Wählen Sie im Feld **Anmeldeinformationen** den in Schritt 3d erstellten Anmeldeinformationsdatensatz aus.
   f. Geben Sie im Feld **Verbindungs-URL** die URL des Lieferanten ein.
   g. Klicken Sie auf **Absenden**.

Einen anderen Common Vulnerability Reporting Framework-Anbieter als Cisco konfigurieren

Konfigurieren Sie einen anderen Anbieter des Common Vulnerability Reporting Framework (CVRF) als Cisco mit API-Unterstützung.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Verbindung und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Erstellen Sie einen Datensatz mit dem vom Lieferanten unterstützten Authentifizierungstyp.
   Weitere Informationen zum Authentifizieren eines Lieferanten finden Sie unter Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen.
3. Navigieren zu **Alle** > **Vulnerability Response** > **Flow Designer**.
4. Duplizieren Sie den Flow mit dem Namen „Advisory Parsing“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn eine der Aktionen geändert werden muss, kopieren Sie die Aktion, und verwenden Sie sie im neuen Flow.
- Aktualisieren Sie die paginierungsbezogene Logik entsprechend dem Lieferanten

5. Wenn die Parameterlogik für den Datumsbereich nicht mit der von Cisco identisch ist, kopieren Sie die Aktion **Paginierungsparameter aktualisieren,** und nehmen Sie die erforderlichen Änderungen für den Lieferanten vor.
6. Navigieren zu **Alle** > **Vulnerability Response** > **Ergänzungsdatenzuordnungen**.
7. Erstellen Sie einen Datensatz gemäß Cisco, indem Sie den **Eigenschaftsschlüsselwert** entsprechend dem Lieferanten ändern.
   Diese Logik dient zum Zuordnen erforderlicher Felder aus einer Beratungsnutzlast zu einer Tabelle ServiceNow.
8. Ordnen Sie die folgenden API-Tags aus der API-Nutzlast zu.
   Diese Tags müssen Details zugeordnet werden, die in der Ergänzungsdatenzuordnungstabelle ausgefüllt werden sollen. Standardmäßig wird die Cisco-spezifische Zuordnung bereitgestellt.

Hinweis:
Sie müssen einen Datensatz erstellen, wenn Sie mehrere Lieferanten konfigurieren müssen, die Erfahrungsberichte veröffentlichen.

Tag der Beratungsnutzlast	Spalte aus der Tabelle „sn_vul_cvrf_solution_integratio	Beschreibung
CVRF-URL	cvrf_url	Tag-Name, der die CVRF-URL enthält.
Beratungs-ID (Eindeutiger Schlüssel für Antwort)	ID	Tag-Name, der einen eindeutigen Bezeichner enthält.
Datum der letzten Änderung	last_modified_date	Tag-Name, der das Datum enthält, an dem der Datensatz zuletzt aktualisiert wurde.
securityAdvisoryIntegrationSysId	Integration	Bezieht sich auf die sysId der geplanten Integrationsaufgabe, die die Datensätze der Schwachstellenlösungen erstellt.

9. Ändern Sie basierend auf dem Antwortformat die Analyselogik, indem Sie die Aktion **Liste abrufen** aus dem Beratungsanalyse-Flow kopieren.

Common Vulnerability Reporting Framework-Daten aus Hinweismeldungen importieren

Importieren Sie CVRF-Daten aus Hinweismeldungen, indem Sie die Lieferanten-URL mit dem Importtyp als API konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Integration ausgeführt wird, werden die Beratungshinweise abgerufen. Die CVRF-URL und die Empfehlungs-ID werden aus der Nutzlast extrahiert. Die REST API-Aufrufe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden für jede CVRF-URL durchgeführt, und die Daten werden analysiert und in der Tabelle sn_vul_solution gespeichert.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Common Vulnerability Response Framework**.
2. Klicken Sie auf **Integration hinzufügen**.
3. Füllen Sie die Felder des Formulars aus.

Formular für Lösungshinweise importieren

Feld	Beschreibung
Importtyp	Option zum Auswählen des Importtyps. Wählen Sie **API**aus.
Name	Eindeutiger Name für die Integration.
Lieferant	Name des Lieferanten. **Hinweis:** Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt.
Verbindungsalias	Option zum Auswählen authentifizierter Anmeldeinformationen. **Hinweis:** In der Tabelle „sys_alias“ werden Anmeldeinformationen und die Basis-URL für Hinweise gespeichert.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Wochenzeit, zu der die Daten aktualisiert werden sollen.
API-Konfiguration	
Flow	Option zum Auswählen des Flows. Der Flow wird ausgelöst, wenn der Planer ausgeführt wird. Der Flow berücksichtigt die Analyse der Hinweismeldungen, extrahiert die CVRF-URL und speichert diese Details in den Aktualisierungstabellen. Sie können den vorhandenen Flow kopieren und nach Bedarf bearbeiten. Sie können beispielsweise Änderungen in Bezug auf die Paginierung vornehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Flow-Aktion	Option zum Auswählen der Flow-Aktion. Flow-Aktionen sorgen für die Fähigkeit des gleitenden Fensters. Sie können die Flow-Aktionen aktualisieren und den Abfrageparameter durch Ziehen direkt zur Aktion hinzufügen.
Zuordnungstabelle	Option zum Auswählen der Zuordnungstabelle. Der Datensatz der Ergänzungsdaten-Zuordnungstabelle wird zum Extrahieren der CVRF-URL und der Advisory-ID aus der Nutzlast der Advisories verwendet.
Hinweise aus Antwort	Option zum Eingeben des Tag-Namens aus der Nutzlast der Hinweise, aus der die Liste der Hinweise extrahiert werden kann.
Filterkriterien	
Zeitbereichsparameter	Option zum Auswählen des Zeitbereichs für die Anforderung und des Datumsformats für API-Aufrufe. Der Parameter „Anforderung für Startdatum/Enddatum“ ist der Parametername, der für das Startdatum und das Enddatum während API-Aufrufen verwendet wird. Beispiel: StartDate, start_date, endDate, end_date.
Datumsformat	Option zur Eingabe des Datumsformats, z. B. MM/TT/JJJJ.. Das Datumsformat ist das Format, das die API zum Filtern benötigt. Formate, die von GlideDate nicht unterstützt werden, funktionieren nicht.
Anfänglicher Bereich in Tagen	EGeben Sie die Tage ein, für die die Daten abgerufen werden müssen, wenn der Scheduler zum ersten Mal ausgeführt wird. Für nachfolgende Ausführungen wird der Gleitfenstermechanismus verwendet. **Hinweis:** Wenn Sie keinen Zeitraum auswählen möchten, wählen Sie **Keine Parameter**aus.
Scanner-Zuordnungen	
Scannerquelle	Option zum Auswählen der Quelle des Drittparteieintrags (TPE).
Schwachstellenspalte	Option zum Auswählen des Stichworts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Stichwörter	Option zur Eingabe des Stichworts für die Suche in der ausgewählten Schwachstellenspalte.

4. Klicken Sie auf **Fertigstellen**.

Importieren Sie CVRF-Daten (Common Vulnerability Reporting Framework) über die CVRF-URL

Importieren Sie CVRF-Daten, indem Sie die Lieferanten-URL im Setup-Assistenten konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden Daten von der URL abgerufen und anschließend analysiert. Die Daten werden dann in der Tabelle sn_vul_solution mit dem Lieferantennamen als Quelle gespeichert.

Hinweis:
Oracle veröffentlicht die CVRF-URL zur Bereitstellung von Lösungen direkt. Wenn Sie also die Integration für den Import von Oracle-Daten konfigurieren möchten, stellen Sie sicher, dass Sie die CVRF-URL für Oracle haben, und führen Sie die folgenden Schritte aus.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Common Vulnerability Response Framework**.
2. Klicken Sie auf **Integration hinzufügen**.
3. Füllen Sie die Felder des Formulars aus.

CVRF-Formular importieren

Feld	Beschreibung
Importtyp	Typ des Imports Wählen Sie **URL**aus.
Name	Eindeutiger Name für die Integration.
Lieferant	Name des Lieferanten. **Hinweis:** Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt.
URL	URL, von der Sie die Lösungsdaten im CVRF-Format abrufen möchten.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn das Status-Tag von CVRF „FINAL“ anzeigt, wird das Feld automatisch auf **On Demand** festgelegt, um unnötige Ausführungen zu verhindern.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Wochenzeit, zu der die Daten aktualisiert werden sollen.

4. Klicken Sie auf **Fertigstellen**.

Problembehandlung beim Datenimport für das Common Vulnerability Reporting Framework

Aktionen zur Fehlerbehebung können zur Behebung allgemeiner Probleme beim Import von CVRF-Daten in die Anwendung Vulnerability Response beitragen.

Problem	Aktion
Dauer der Integrationsausführung ist lang	Wenn die Integration länger als erwartet ausgeführt wird, gehen Sie wie folgt vor: 1. Navigieren Sie zur Tabelle sn_vul_ds_import_q_entry. 2. Nach dem Feld **Status** gruppieren. Sie können die Einträge sehen, die sich im Status Abgeschlossen, In Bearbeitung oder In der Warteschlange befinden.
Integration im API-basierten Import fehlgeschlagen	Wenn die Integration beim API-basierten Import fehlschlägt, gehen Sie wie folgt vor: 1. Navigieren Sie zu **Flow Designer**. 2. Öffnen Sie den Flow, der in der Konfiguration ausgewählt wurde. **Hinweis:** Öffnen Sie im Fall von Cisco den Flow „Advisory Parsing“. 3. Klicken Sie auf **Ausführungen**. 4. Öffnen Sie die aktuelle Ausführung oder die Ausführung, die debuggt werden muss. 5. Überprüft den Flow in den einzelnen Phasen.
Die Integration ist im API-basierten Import mit einem Zeitüberschreitungsfehler fehlgeschlagen	Wenn die Integration in einem API-basierten Import aufgrund einer Zeitüberschreitung im Flow zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Aktion
	Beratungsanalyse fehlschlägt, gehen Sie wie folgt vor: 1. Erhöhen Sie die Zeitüberschreitung, indem Sie sys_properties.LISTöffnen. 2. Suchen Sie in der Spalte „Name“ nach sn_vul.CVRFFlowTimeout (inMiliSeconds). **Hinweis:** Die Zeit wird in Millisekunden angegeben. 3. Öffnen Sie den Datensatz, und aktualisieren Sie den Wert mit einer großen Zahl. 4. Speichern Sie den Datensatz, und führen Sie die Integration erneut aus.
Integration mit Fehler „Transformation von Scanner-Zuordnung zu Lieferantenzuordnungsdaten“ ist in Bearbeitung fehlgeschlagen.	Überprüfen Sie, ob die Integration während des URL- oder API-basierten Imports mit dem folgenden Fehler fehlschlägt:Die Transformation von Scanner-Zuordnung zu Lieferantenzuordnungsdaten wird ausgeführt. Daten werden erst ausgefüllt, nachdem die Transformation abgeschlossen ist. Versuchen Sie nach einiger Zeit auszuführen. Wenn dieser Fehler auftritt, warten Sie einige Zeit, und führen Sie die Integration erneut aus.
Importwarteschlange wird während des Dateiimports nicht erstellt	Während eines Dateiimports wird die Importwarteschlange manchmal nicht erstellt. Dieser Fehler bedeutet, dass die Transformation, die Scannerzuordnungsdaten zu Lieferantenzuordnungsdaten zuordnet, ausgeführt wird. Der Warteschlangeneintrag wird erstellt, sobald der Prozess abgeschlossen ist.

Common Security Advisory Framework (CSAF)

Bei Verwendung mit Vulnerability Solution Managementermöglicht das Common Security Advisory Framework (CSAF) die Automatisierung von Sicherheitsbenachrichtigungen über ein maschinenlesbares JSON-Format.

Mit CSAF können Sie jeden Lösungsintelligenz-Anbieter integrieren, indem Sie das Framework für Lösungsmanagement verwenden, um die Intelligenzdaten zu importieren. Die CSAF-Sicherheitsbenachrichtigungen können einen der folgenden Typen aufweisen.

- Sicherheitswarnhinweise
- Vulnerability Exploitability Exchange (VEX)
- Security Incident Response
- Informational Advisory

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CSAF unterstützt nur die Dateiimporte, URL-Importe und API-Importe von Sicherheitswarnhinweisen von Lieferanten.

Importieren Sie Framework-Daten für Sicherheitswarnhinweise über einen Dateiimport

Importieren Sie eine CSAF-Datei, um Daten im CSAF-Format anzuzeigen. Der Importvorgang ist eine einmalige Aktivität.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird
Nach dem Import wird ein Warteschlangeneintrag mit einem Anhang erstellt, der bei der Verarbeitung des Eintrags analysiert wird. Die Daten werden dann in die entsprechenden Tabellen gefüllt. Vor dem Analysieren der CSAF-Daten wird basierend auf der Konfiguration ein Scanner-Zuordnungsdatensatz erstellt. Anschließend werden die Scannerzuordnungsdaten in Lieferantenzuordnungsdaten umgewandelt.

Die Scannerzuordnung gilt nicht für Schwachstellen, die auf der National Vulnerability Database (NVD) basieren. Hierbei handelt es sich um Schwachstellen mit einem Common Vulnerability Eintrag (CVE) in der NVD-Datenbank.

Wenn Sie nur eine höchste Ersatzlösung haben, und ein Rolldown bis zu den angreifbaren Elementen durchführt, wird die bevorzugte Lösung ausgefüllt. Wenn in einem NVD-Eintrag mehrere Lieferantenlösungen enthalten sind, wird die bevorzugte Lösung nicht ausgefüllt, da es mehr als eine höchste Ersatzlösung gibt. In diesem Fall müssen Sie manuell eine Lösung auswählen. Bei Schwachstellen von Drittparteien wird die bevorzugte Lösung nur ausgefüllt, wenn Sie die entsprechende Scannerzuordnung hinzufügen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Framework für allgemeine Sicherheitswarnhinweise**.
2. Wählen Sie **Importdatei**.

   Hinweis:
   Sie können jeweils nur eine JSON-Datei mit einer maximalen Dateigröße von 15 MB hochladen.

3. Geben Sie im Feld **Name** einen eindeutigen Namen für die Integration ein.
   Der Zeitplaner wird mit diesem Namen erstellt.
4. Geben Sie im Feld **Lieferant** den Namen des Lieferanten ein.
   Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt.
5. Wählen Sie **Fertigstellen** aus.

Ergebnisse
Eine Importwarteschlange wird erstellt. Wählen Sie den Link in der Infoleiste, um die Warteschlangeneinträge für den Lieferanten zusammen mit der zugehörigen Liste anzuzeigen. Sie können auch den Status des Auftrags anzeigen.

Nachdem die Daten in das CSAF-Format importiert wurden, werden sie wie folgt verarbeitet:

1. Bei der Verarbeitung der Warteschlange wird die Datei mit einer dedizierten Datenquelle analysiert.
2. Sobald die Verarbeitung abgeschlossen ist, wird das Anwendungsprotokoll aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Sobald die CSAF-JSON-Datei analysiert wurde, füllt sie die folgenden Tabellen in der Anwendung ServiceNow® Vulnerability Response aus.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Detaillierte Informationen zu Fehlern oder Ausnahmen finden Sie in den Anwendungsprotokollen.

Aliasse für Verbindungen und Anmeldeinformationen für CSAF (Common Security Advisory Framework) konfigurieren

Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen, um Lieferanten zu authentifizieren. Bei der Beratungsanalyse werden Drittanbieter authentifiziert.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

Prozedur

1. Erstellen Sie die OAuth-Authentifizierung.
   Weitere Informationen finden Sie unter Endpunkte für Clients zum Zugriff auf die Instanz erstellen .
2. Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen.
   Weitere Informationen finden Sie unter Alias für Verbindungen und Anmeldeinformationen erstellen .
3. Erstellen Sie eine Verbindung.
   a. Wählen Sie den Namen des neu erstellten Alias für Verbindungen und Anmeldeinformationen aus.
   b. Wählen Sie auf der Registerkarte **Verbindungen** die **Option Neu**aus.
   c. Wenn der Authentifizierungstyp OAuth ist, wählen Sie das in Schritt 1 erstellte Anwendungsregistrierungsprofil als **OAuth-Entitätsprofil**aus.
   d. Erstellen Sie einen Datensatz in „Verbindungen“ anhand der zugehörigen Liste des Datensatzes.
   e. Wählen Sie im Feld **Anmeldeinformationen** den in Schritt 3d erstellten Anmeldeinformationsdatensatz aus.
   f. Geben Sie im Feld **Verbindungs-URL** die URL des Lieferanten ein.
   g. Wählen Sie **Absenden**.

Konfigurieren Sie einen anderen Anbieter des Common Security Advisory Framework als Red Hat

Konfigurieren Sie einen anderen CSAF-Lieferanten (Common Security Advisory Framework) als Red Hat mit API-Unterstützung.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Verbindung und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Erstellen Sie einen Datensatz mit dem vom Lieferanten unterstützten Authentifizierungstyp.
   Weitere Informationen zum Authentifizieren eines Lieferanten finden Sie unter Aliasse für Verbindungen und Anmeldeinformationen für CSAF (Common Security Advisory Framework) konfigurieren.
3. Navigieren zu **Alle** > **Vulnerability Response** > **Flow Designer**.
4. Duplizieren Sie den Flow mit dem Namen „Advisory Parsing“.

   Hinweis:
   - Wenn eine der Aktionen geändert werden muss, kopieren Sie die Aktion, und verwenden Sie sie im neuen Flow.
   - Überprüfen Sie die Parameter „page_index_key“ und „page_size_key“ gemäß der Lieferanten-API.
   - Aktualisieren Sie die paginierungsbezogene Logik entsprechend dem Lieferanten
5. Wenn die Parameterlogik für den Datumsbereich nicht mit Red Hatidentisch ist, kopieren Sie die Aktion **Paginierungsparameter aktualisieren,** und nehmen Sie die erforderlichen Änderungen für den Lieferanten vor.
6. Navigieren zu **Alle** > **Vulnerability Response** > **Ergänzungsdatenzuordnungen**.
7. Erstellen Sie einen Datensatz gemäß Red Hat, indem Sie den **Eigenschaftsschlüsselwert** entsprechend dem Lieferanten ändern.
   Diese Logik dient zum Zuordnen erforderlicher Felder aus einer Beratungsnutzlast zu einer Tabelle ServiceNow.
8. Ordnen Sie die folgenden API-Tags aus der API-Nutzlast zu.
   Diese Tags müssen Details zugeordnet werden, die in der Ergänzungsdatenzuordnungstabelle ausgefüllt werden sollen. Standardmäßig wird die spezifische Zuordnung Red Hat geliefert.

   Hinweis:
   Sie müssen einen Datensatz erstellen, wenn Sie mehrere Lieferanten konfigurieren müssen, die Erfahrungsberichte veröffentlichen.

Tag der Beratungsnutzlast	Spalte aus der Tabelle „sn_vul_cvrf_solution_integratio	Beschreibung
CSAF-URL (Ressourcen-URL, die auf die CSAF-Nutzlast verweist)	cvrf_url	Tag-Name, der die CSAF-URL enthält.
Beratungs-ID (Eindeutiger Schlüssel für Antwort)	ID	Tag-Name, der einen eindeutigen Bezeichner enthält.
Datum der letzten Änderung	last_modified_date	Tag-Name, der das Datum enthält, an dem der Datensatz zuletzt aktualisiert wurde.
csaf (statischer Wert)	Advisory_Format	Beratungsformatwert für CSAF-Nutzlasten. Beachten Sie, dass dies ein statischer Wert ist, der für alle CSAF-Integrationen gilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag der Beratungsnutzlast	Spalte aus der Tabelle „sn_vul_cvrf_solution_integratio	Beschreibung
securityAdvisoryIntegrationSysId	Integration	Bezieht sich auf die sysId der geplanten Integrationsaufgabe, die die Datensätze der Schwachstellenlösungen erstellt.

9. Ändern Sie basierend auf dem Antwortformat die Analyselogik, indem Sie die Aktion **Liste abrufen** aus dem Beratungsanalyse-Flow kopieren.

Importieren Sie Framework-Daten für Sicherheitswarnhinweise aus Hinweismeldungen

Importieren Sie CSAF-Daten aus Hinweismeldungen, indem Sie die Lieferanten-URL mit dem Importtyp als API konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Integration ausgeführt wird, werden die Beratungshinweise abgerufen. Die CSAF-URL und die Empfehlungs-ID werden aus der Nutzlast extrahiert. Die REST API-Aufrufe erfolgen für jede CSAF-URL, und die Daten werden analysiert und in der Tabelle sn_vul_solution gespeichert.

Die Scannerzuordnung gilt nicht für Schwachstellen, die auf der National Vulnerability Database (NVD) basieren. Hierbei handelt es sich um Schwachstellen mit einem Common Vulnerability Eintrag (CVE) in der NVD-Datenbank.

Wenn Sie nur eine höchste Ersatzlösung haben, und ein Rolldown bis zu den angreifbaren Elementen durchführt, wird die bevorzugte Lösung ausgefüllt. Wenn in einem NVD-Eintrag mehrere Lieferantenlösungen enthalten sind, wird die bevorzugte Lösung nicht ausgefüllt, da es mehr als eine höchste Ersatzlösung gibt. In diesem Fall müssen Sie manuell eine Lösung auswählen. Bei Schwachstellen von Drittparteien wird die bevorzugte Lösung nur ausgefüllt, wenn Sie die entsprechende Scannerzuordnung hinzufügen.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Framework für allgemeine Sicherheitswarnhinweise**.
2. Wählen Sie **Integration hinzufügen**.
3. Füllen Sie die Felder des Formulars aus.

Formular für Lösungshinweise importieren

Feld	Beschreibung
Importtyp	Option zum Auswählen des Importtyps. Wählen Sie **API**aus.
Name	Eindeutiger Name für die Integration.
Lieferant	Name des Lieferanten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt.
Verbindungsalias	Option zum Auswählen authentifizierter Anmeldeinformationen. **Hinweis:** In der Tabelle „sys_alias“ werden Anmeldeinformationen und die Basis-URL für Hinweise gespeichert.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Wochenzeit, zu der die Daten aktualisiert werden sollen.
API-Konfiguration	
Flow	Option zum Auswählen des Flows. Der Flow wird ausgelöst, wenn der Planer ausgeführt wird. Der Flow berücksichtigt die Analyse der Hinweismeldungen, extrahiert die CSAF-URL und speichert diese Details in den Aktualisierungstabellen. Sie können den vorhandenen Flow kopieren und nach Bedarf bearbeiten. Sie können beispielsweise Änderungen in Bezug auf die Paginierung vornehmen.
Flow-Aktion	Option zum Auswählen der Flow-Aktion. Flow-Aktionen sorgen für die Fähigkeit des gleitenden Fensters. Sie können die Flow-Aktionen aktualisieren und den Abfrageparameter durch Ziehen direkt zur Aktion hinzufügen.
Zuordnungstabelle	Option zum Auswählen der Zuordnungstabelle. Der Datensatz der Ergänzungsdaten-Zuordnungstabelle wird zum Extrahieren der CSAF-URL und der Advisory-ID aus der Nutzlast der Advisories verwendet.
Hinweise aus Antwort	Option zum Eingeben des Tag-Namens aus der Nutzlast der Hinweise, aus der die Liste der Hinweise extrahiert werden kann.
Filterkriterien	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeitbereichsparameter	Option zum Auswählen des Zeitbereichs für die Anforderung und des Datumsformats für API-Aufrufe. Der Parameter „Anforderung für Startdatum/Enddatum“ ist der Parametername, der für das Startdatum und das Enddatum während API-Aufrufen verwendet wird. Beispiel: StartDate, start_date, endDate, end_date.
Datumsformat	Option zur Eingabe des Datumsformats, z. B. MM/TT/JJJJ.. Das Datumsformat ist das Format, das die API zum Filtern benötigt. Formate, die von GlideDate nicht unterstützt werden, funktionieren nicht.
Anfänglicher Bereich in Tagen	EGeben Sie die Tage ein, für die die Daten abgerufen werden müssen, wenn der Scheduler zum ersten Mal ausgeführt wird. Für nachfolgende Ausführungen wird der Gleitfenstermechanismus verwendet. **Hinweis:** Wenn Sie keinen Zeitraum auswählen möchten, wählen Sie **Keine Parameter**aus.
Scanner-Zuordnungen	
Scannerquelle	Option zum Auswählen der Quelle des Drittparteieintrags (TPE).
Schwachstellenspalte	Option zum Auswählen des Stichworts.
Stichwörter	Option zur Eingabe des Stichworts für die Suche in der ausgewählten Schwachstellenspalte.

4. Wählen Sie **Fertigstellen** aus.

Importieren Sie CSAF-Daten (Common Security Advisory Framework) über die CSAF-URL

Importieren Sie CSAF-Daten, indem Sie die Lieferanten-URL im Setup-Assistenten konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden Daten von der URL abgerufen und anschließend analysiert. Die Daten werden dann in der Tabelle sn_vul_solution mit dem Lieferantennamen als Quelle gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die URL kann entweder eine direkte CSAF-Nutzlast sein, die die Beratungsdetails enthält, oder eine ROLIE-Feed-URL (Resource-Oriented Lightweight Information Exchange). In beiden Fällen wird die Nutzlast entsprechend analysiert, und die Lösungsdatensätze werden erstellt. Führen Sie die folgenden Schritte für den CSAF-URL-Import aus.

Sie können Schwachstellenlösungen auch über einen URL-Import importieren, der ROLIE-Feed unterstützt. Diese Schwachstellenlösungen werden basierend auf Common Vulnerabilities and Exposures (CVE) automatisch den richtigen Lieferanten und angreifbaren Elementen (VITs) zugeordnet.

Die Scannerzuordnung gilt nicht für Schwachstellen, die auf der National Vulnerability Database (NVD) basieren. Hierbei handelt es sich um Schwachstellen mit einem Common Vulnerability Eintrag (CVE) in der NVD-Datenbank.

Wenn Sie nur eine höchste Ersatzlösung haben, und ein Rolldown bis zu den angreifbaren Elementen durchführt, wird die bevorzugte Lösung ausgefüllt. Wenn in einem NVD-Eintrag mehrere Lieferantenlösungen enthalten sind, wird die bevorzugte Lösung nicht ausgefüllt, da es mehr als eine höchste Ersatzlösung gibt. In diesem Fall müssen Sie manuell eine Lösung auswählen. Bei Schwachstellen von Drittparteien wird die bevorzugte Lösung nur ausgefüllt, wenn Sie die entsprechende Scannerzuordnung hinzufügen.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Framework für allgemeine Sicherheitswarnhinweise**.
2. Wählen Sie **Integration hinzufügen**.
3. Füllen Sie die Felder des Formulars aus.

CSAF-Formular importieren

Feld	Beschreibung
Importtyp	Typ des Imports Wählen Sie **URL**aus.
Name	Eindeutiger Name für die Integration.
Einzelner Lieferant	Wählen Sie diese Option aus, wenn Sie CSAF von einem Lieferanten importieren.
Lieferant	Name des Lieferanten. Dieses Feld ist nur verfügbar, wenn Sie **Einzelner Lieferant**auswählen. **Hinweis:** Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt.
Mehrere Lieferanten	Wählen Sie diese Option aus, wenn Sie CSAF von mehreren Lieferanten importieren.
Aggregator	Ein vertrauenswürdiger Anbieter, dessen Lösung Sie importieren können.
URL	URL, von der Sie die Lösungsdaten im CSAF-Format abrufen möchten.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn das Status-Tag von CSAF „FINAL“ lautet, wird das Feld automatisch auf **„Bei Bedarf“** festgelegt, um unnötige Ausführungen zu verhindern.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Wochenzeit, zu der die Daten aktualisiert werden sollen.
Scanner-Zuordnungen **Hinweis:** Der Abschnitt „Scanner-Zuordnungen“ ist für CSAF optional.	
Scannerquelle	Option zum Auswählen der Quelle des Drittparteieintrags (TPE).
Schwachstellenspalte	Option zum Auswählen des Stichworts.
Stichwörter	Option zur Eingabe des Stichworts für die Suche in der ausgewählten Schwachstellenspalte.

4. Wählen Sie **Fertigstellen** aus.

Problembehandlung beim Datenimport im Framework für allgemeine Sicherheitswarnhinweise

Aktionen zur Fehlerbehebung können zur Behebung allgemeiner Probleme beim Import von CSAF-Daten in die Anwendung Vulnerability Response beitragen.

Problem	Aktion
Dauer der Integrationsausführung ist lang	Wenn die Integration länger als erwartet ausgeführt wird, gehen Sie wie folgt vor: 1. Navigieren Sie zur Tabelle sn_vul_ds_import_q_entry. 2. Nach dem Feld **Status** gruppieren. Sie können die Einträge sehen, die sich im Status Abgeschlossen, In Bearbeitung oder In der Warteschlange befinden.
Integration im API-basierten Import fehlgeschlagen	Wenn die Integration beim API-basierten Import fehlschlägt, gehen Sie wie folgt vor: 1. Navigieren Sie zu **Flow Designer**. 2. Öffnen Sie den Flow, der in der Konfiguration ausgewählt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Aktion
	Hinweis: Öffnen Sie im Fall von Red Hatden Beratungsanalyse-Flow. 3. Wählen Sie **Ausführungen**aus. 4. Öffnen Sie die aktuelle Ausführung oder die Ausführung, die debuggt werden muss. 5. Überprüft den Flow in den einzelnen Phasen.
Die Integration ist im API-basierten Import mit einem Zeitüberschreitungsfehler fehlgeschlagen	Wenn die Integration in einem API-basierten Import aufgrund einer Zeitüberschreitung im Flow zur Beratungsanalyse fehlschlägt, gehen Sie wie folgt vor: 1. Erhöhen Sie die Zeitüberschreitung, indem Sie sys_properties.LISTöffnen. 2. Suchen Sie in der Spalte „Name“ nach sn_vul.CVRFFlowTimeout (inMiliSeconds). **Hinweis:** Die Zeit wird in Millisekunden angegeben. 3. Öffnen Sie den Datensatz, und aktualisieren Sie den Wert mit einer großen Zahl. 4. Speichern Sie den Datensatz, und führen Sie die Integration erneut aus.
Integration mit Fehler „Transformation von Scanner-Zuordnung zu Lieferantenzuordnungsdaten“ ist in Bearbeitung fehlgeschlagen.	Überprüfen Sie, ob die Integration während des URL- oder API-basierten Imports mit dem folgenden Fehler fehlschlägt:Die Transformation von Scanner-Zuordnung zu Lieferantenzuordnungsdaten wird durchgeführt. Daten werden erst ausgefüllt, nachdem die Transformation abgeschlossen ist. Versuchen Sie nach einiger Zeit auszuführen. Wenn dieser Fehler auftritt, warten Sie einige Zeit, und führen Sie die Integration erneut aus.
Importwarteschlange wird während des Dateiimports nicht erstellt	Während eines Dateiimports wird die Importwarteschlange manchmal nicht erstellt. Dieser Fehler bedeutet, dass die Transformation, die Scannerzuordnungsdaten zu Lieferantenzuordnungsdaten zuordnet, ausgeführt wird. Der Warteschlangeneintrag wird erstellt, sobald der Prozess abgeschlossen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Setup- und Konfigurationsaufgaben für Vulnerability Response .

Um Sie bei der Korrektur zu unterstützen, können Sie diese zusätzlichen administrativen Setupaufgaben als Teil Ihrer Konfiguration außerhalb des Basis-Setups ausführen. Sie führen diese Aufgaben außerhalb des Setup-Assistenten durch.

Sie können die mit Vulnerability Response bereitgestellte Standardberichterstellung verwenden, um Ihre Sicherheitslage zu überwachen. Sie können diese Berichte bearbeiten, wenn sie nicht für Ihre Umgebung geeignet sind, oder sie als Vorlagen zum Erstellen eigener Berichte verwenden.

Wenn die Anwendung Performance Analytics for Vulnerability Response installiert ist, können Sie Berichte, reaktionsfähige Dashboards und vieles mehr erstellen. Weitere Informationen finden Sie unter Erste Schritte mit Berichten .

E-Mail-Benachrichtigungen erhöhen die Produktivität und sorgen für einen reibungslosen Workflow.

Mit der Bewertung des Gefahrenpotenzials von Software suchen Sie in Software Asset Management (SAM Foundation) nach dem Herausgeber, dem Produktnamen und der Versionsnummer, um Ihr Risiko für angreifbare Software zu bestimmen.

Transparenz in Schwachstellenbibliotheken bietet Flexibilität bei Gruppierungs- und Korrekturaufgaben.

Konfigurieren Sie die Ausnahmeverwaltung so, dass Sie eine Ausnahme anfordern können, wenn Ihre Organisation eine veröffentlichte Richtlinie für das Schwachstellenmanagement oder eine Sicherheitsrichtlinie, einen Standard oder eine Leitlinie nicht einhalten kann.

Weitere zusätzliche Setupaufgaben finden Sie in den Themen nach dieser Übersicht.

Schnellstarttests für Vulnerability Response

Überprüfen Sie, ob Vulnerability Response immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwickeln einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demo-Accounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird. Unter Führen Sie die Automated Test Framework-Test-Suite (ATF) für aus Vulnerability Response finden Sie weitere Informationen zum Einrichten und Ausführen der Test-Suite für Vulnerability Response.

Vulnerability Response-Schnellstarttests erfordern die Aktivierung der Anwendung Vulnerability Response (sn_vul) und das Laden der Demodaten.

Vulnerability Response-Tests

Test	Beschreibung	Release-Version
VR: Fehlerkorrektur-Zielregel erstellen	Erstellt eine Fehlerkorrektur-Zielregel.	Madrid
VR: Schwachstellengruppenregel erstellen	Erstellt eine Schwachstellengruppenregel.	Madrid

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
VR: Erstellen eines angreifbaren Elements über das Formular	Ermittelt, ob ein Benutzer ein angreifbares Element erfolgreich aus dem Formular „Angreifbares Element“ erstellen kann.	Madrid
VR: Schwachstellengruppen-Lebenszyklus	Ermittelt, ob ein Benutzer eine Schwachstellengruppe erfolgreich beheben kann.	Madrid
VR: Lebenszyklus von angreifbaren Elementen	Ermittelt, ob ein Benutzer ein angreifbares Element erfolgreich durch seinen Lebenszyklus bewegen kann, und ermittelt zudem, ob ein abgeschlossenes angreifbares Element erneut geöffnet werden kann.	Madrid
VR: Rollup-Rechner	Ermittelt, ob der Rollup-Risiko-Rechner eine Gesamtrisikopunktzahl für eine ganze Gruppe angreifbarer Elemente mit den Punktzahlen für alle angreifbaren Elemente in einer Schwachstellengruppe verfügbar machen kann.	New York
VR: Vulnerability Response-Zuweisungsregeln	Ermittelt, ob mit einem Mustersatz von Zuweisungsregeln angreifbare Elemente automatisch einer Zuweisungsgruppe zur Nachbesserung zugewiesen werden können.	New York
VR: Schwachstellen-Rechner	Testen Sie die Schwachstellen-Rechner.	New York
VR: CI-Suche – Qualys	Erstellt mithilfe der Methode „field_matching“ eine neue Suchregel mit der Bezeichnung „Suche nach Netzwerkadapter“ für Qualys. Ermittelt, ob Konfigurationselemente mit der neuen Suchregel erfolgreich nach Netzwerkadapter und IP-Adresse mit der Tabelle „Erkannte Elemente“ abgeglichen werden.	Orlando
VR: Normale Change-Anforderungen und Notfall-Change-Anforderungen erstellen	Ermittelt, ob der Benutzer erfolgreich normale Change-Anforderungen und Notfall-Change-Anforderungen aus einer Schwachstellengruppe erstellen kann.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
VR: Schwachstellengruppen aufteilen	Ermittelt, ob der Benutzer Schwachstellengruppen erfolgreich aufteilen kann.	Orlando
VR: SG-Status bei Abbruch von CHG aktualisieren	Ermittelt, ob in einer Schwachstellengruppe die Angabe im Feld „Status“ erfolgreich wechselt, wenn eine Change-Anforderung, die der Schwachstellengruppe zugeordnet ist, abgebrochen wird.	Orlando
VR: SG-Status aktualisieren, wenn CHG zur Überprüfung wechselt	Ermittelt, ob in einer Schwachstellengruppe die Angabe im Feld „Status“ erfolgreich wechselt, wenn eine Change-Anforderung, die der Schwachstellengruppe zugeordnet ist, in den Überprüfungsstatus wechselt.	Orlando
VR: CI-Suche – Rapid7	Testen Sie die CI-Suche mithilfe der vorhandenen Rapid7 Vulnerability-Integration-Suchregel **IP-Adresse**.	Orlando
VR: CI-Suche – Qualys	Testen Sie die CI-Suche, indem eine neue Suchregel für Qualys Vulnerability Integration erstellt wird.	Orlando
VR: Ausnahmegenehmigungs-Workflow für VI	Erstellen Sie eine Ausnahmeanforderung, und überprüfen Sie, ob der Genehmigungsprozess funktioniert.	Orlando
VR: Falsch positiver Genehmigungsworkflow für VI	Erstellen Sie eine falsch positive Ausnahmeanforderung, und überprüfen Sie, ob der Genehmigungsprozess funktioniert.	Orlando
VR: Application Vulnerability Response (AVR)	Bestimmen Sie, ob Ihre Regeln und Rechner ordnungsgemäß funktionieren. Stellen Sie sicher, dass Updates funktionieren.	Orlando
Korrekturzielregeln: VI-Importtest	Testet die VR-Korrekturzielregeln während des Imports.	Paris
VR: Klassifizierungsregel	Beispiel für eine Klassifizierungsregel, die eine Schwachstelle automatisch klassifiziert.	Tokyo

Zugehörige Informationen

Schnellstarttests

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie die Automated Test Framework-Test-Suite (ATF) für aus Vulnerability Response

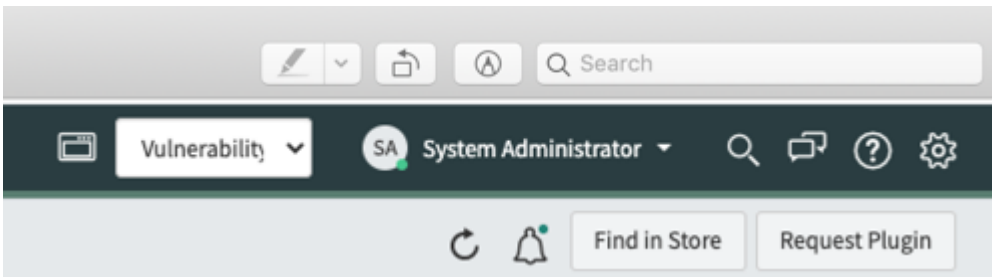
Führen Sie die Automated Test Framework-Test-Suite (ATF) aus, nachdem Sie die Anwendung Vulnerability Response installiert oder aktualisiert haben.

Vorbereitungen
Bestätigen Sie eine erfolgreiche Installation und dass Ihre Instanz ordnungsgemäß funktioniert.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demo-Accounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird.

- Vergewissern Sie sich, dass Sie bei der Installation Vulnerability Responsevon die Demodaten installiert haben. Zum Ausführen der Vulnerability Response -Test-Suite sind Demodaten erforderlich.
- Um den Test zu aktivieren, gehen Sie wie folgt vor:
  1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Administration** > **Eigenschaften**.
  2. Wenn die Option nicht ausgewählt ist, aktivieren Sie das Kontrollkästchen **Ausführung von Test-/Test-Suites aktivieren**.
  3. Klicken Sie auf **Speichern**.
  4. Wenn der Bereich im Header nicht auf **Vulnerability Response** festgelegt oder der Bereich nicht im Header angezeigt wird, klicken Sie auf das Einstellungssymbol oben auf der Seite im Browserfenster .
  5. Klicken Sie im Fenster „Systemeinstellungen“ auf **Entwickler**.
  6. Wenn die Option nicht ausgewählt ist, klicken Sie auf **Anwendungsauswahl in Header anzeigen**, und schließen Sie das Fenster.
  7. Klicken Sie in der Liste, die neben Systemadministratorangezeigt wird, auf **Vulnerability Response** für das Feld.

     Das Feld wird wie in der folgenden Abbildung dargestellt angezeigt.



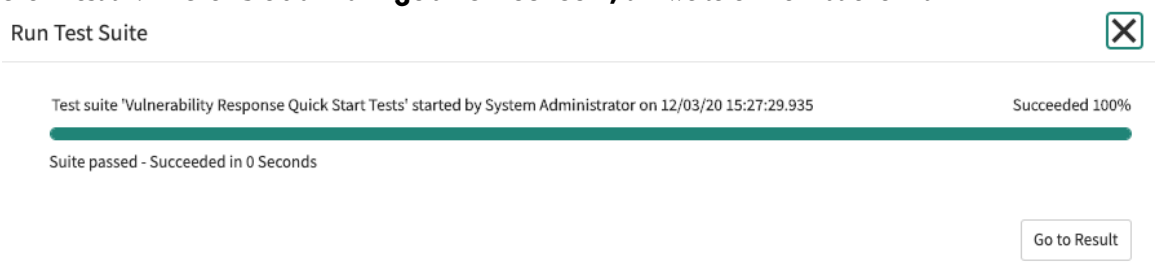
Erforderliche Rolle: admin oder atf_test_admin

Prozedur

1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Suites**.
2. Suchen Sie in der Liste Test-Suites nach **Vulnerability Response-Schnellstarttests**.
3. Wählen Sie es aus, um den Datensatz zu öffnen.
4. Aktivieren Sie im geöffneten Datensatz das Kontrollkästchen **Aktiv**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Aktualisieren**.
6. Wenn die Schaltfläche **Test-Suite ausführen** nicht angezeigt wird, aktualisieren Sie den Bildschirm, öffnen Sie den Datensatz erneut, und klicken Sie auf **Test-Suite ausführen**, um den Test zu starten. Nach einigen Minuten zeigt das Dialogfeld Run Test Suite (Test-Suite ausführen) einen erfolgreichen Test an. Klicken Sie **auf Zu Ergebnis wechseln,** um weitere Informationen zu



erhalten.

Nächste Maßnahme

Herzlichen Glückwunsch! Sie können mit der Konfiguration von Vulnerability Responsefortfahren.

Weitere Informationen zu automatisierten Tests für Vulnerability Response sowie zu automatisierten Tests, Test-Suites und zum Erstellen automatisierter Tests finden Sie unter Automated Test Framework (ATF) .

Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response installieren

Installieren Sie Empfehlungen für die Zuweisung von Schwachstellen, um die Zeit zu reduzieren, die Sie für die Identifizierung von Besitzern von nicht oder falsch zugewiesenen Schwachstellenergebnissen aufwenden müssen. Diese Anwendung ist als separates Abonnement im ServiceNow Storeverfügbar.

Vorbereitungen

Bevor Sie die Funktion Empfehlungen für die Zuweisung von Schwachstellen von Vulnerability Response in Ihrer Instanz Now Platform® ausführen, müssen Sie zuerst die Anwendung Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response herunterladen und installieren. Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Weitere Informationen finden Sie unter Eine ServiceNow Store-Anwendung aktivieren.

Erforderliche Rolle: admin

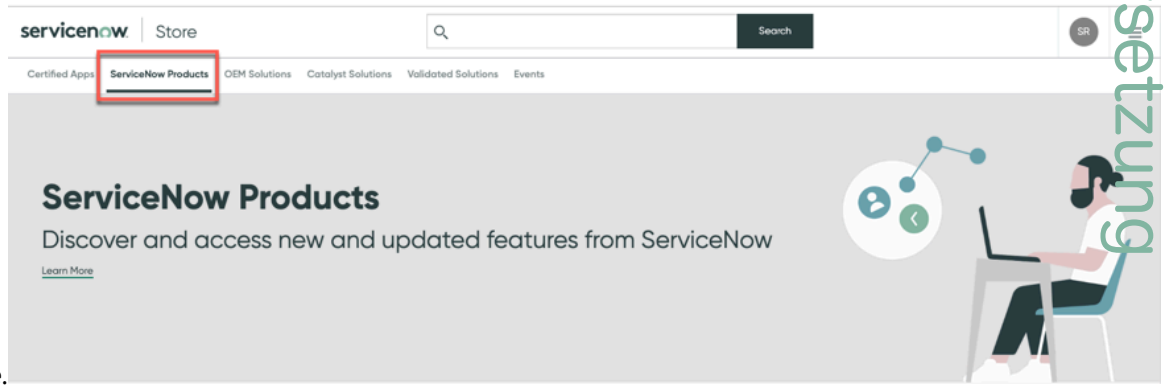
Setupaufgaben	Aktion
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **In Ihrer Instanz installiert**. Vulnerability Response wird in dieser Liste angezeigt, wenn installiert ist. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Aktion
Stellen Sie sicher, dass die Anwendung Predictive Intelligence installiert und aktiviert ist.	Navigieren zu **Systemanwendungen** > **Alle Anwendungen** > **In Ihrer Instanz installiert**. Predictive Intelligence wird in dieser Liste angezeigt, wenn installiert ist. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Install Predictive Intelligence .
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Stellen Sie sicher, dass Sie über die folgenden erforderlichen Rollen für die Installation und Verifizierung der erwarteten Ergebnisse verfügen: • „vulnerability_admin“: Erforderlich, um Empfehlungen für die Zuweisung von Schwachstellenzu aktivieren und zu konfigurieren. Sie können es auch verwenden, um Zuweisungsempfehlungen für angreifbare Elemente und Korrekturaufgaben anzuzeigen und auszuwählen. • ServiceNow admin: Erforderlich, um Anwendungen zu installieren.

Prozedur

1. Navigieren Sie zum ServiceNow Store.
2. Klicken Sie auf **Anmelden**, und geben Sie Ihre HI-Anmeldeinformationen ein.
3. Um die verfügbaren ServiceNow -Produkte anzuzeigen, klicken Sie auf die Registerkarte ServiceNow **Produkte**.



4. Um alle zugeordneten Anwendungen anzuzeigen, für die Sie Berechtigungen für Empfehlungen für die Zuweisung von Schwachstellenerwerben, klicken Sie auf das Produkt Vulnerability Response.

   Auf der Seite werden alle Anwendungen aufgelistet, zu denen Sie berechtigt sind, wenn Sie sich anmelden. Um Informationen zu einer Anwendung zu erhalten, klicken Sie auf den Link für die Anwendung.

5. Um zu überprüfen, ob Sie die Berechtigung für Empfehlungen für die Zuweisung von Schwachstellenhaben, klicken Sie **auf Aktivieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Eingabeaufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.
   Es wird eine Meldung angezeigt, dass Sie sich erfolgreich für die Anwendung entschieden haben.
7. Fahren Sie mit Schritt 10 fort, um die Anwendung in Ihrer Instanz Now Platform zu installieren.
8. **Wahlweise:** Wenn Sie Ihre Berechtigung für die Anwendung Empfehlungen für die Zuweisung von Schwachstellen in anderen Now Platform -Instanzen verwalten möchten, klicken Sie auf **Berechtigung verwalten**.

   Hinweis:

   (Optional) Wenn die Schaltfläche **Berechtigung verwalten** nicht angezeigt wird, klicken Sie auf die Anwendung Empfehlungen für die Zuweisung von Schwachstellen in der Produktliste, um sie anzuzeigen.

   a. Wählen Sie eine Option.

   b. Klicken Sie auf **OK** oder **Abbrechen,** um fortzufahren.
   Sie können jetzt Plugins aktivieren und die Anwendung in Ihren Now Platform -Instanzen installieren.
9. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Empfehlungen für die Zuweisung von Schwachstellen installieren möchten.
10. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
11. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Empfehlungen für die Zuweisung von Schwachstellen (sn_vul_recom), und klicken Sie auf **Installieren**.
    Das Dialogfeld „Anwendungsinstallation“ wird angezeigt, und alle installierten Abhängigkeiten werden angezeigt.
12. **Wahlweise:** Wenn Sie Demodaten wünschen, aktivieren Sie das Kontrollkästchen **Demodaten laden**, und klicken Sie auf **Installieren**.

    Hinweis:
    Wenn Sie das Kontrollkästchen **Demodaten laden** nicht aktivieren, können die Demodaten nicht später über den Anwendungsmanager installiert werden. Informationen zur Installation oder erneuten Installation von Demodaten nach der Erstinstallation finden Sie im Artikel Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] in der Knowledge Base Now Support.

    Diese Installation kann einige Zeit in Anspruch nehmen. Nachdem die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden, wird im Dialogfeld „Installieren“ eine Meldung angezeigt.
13. Klicken Sie auf **Schließen**.
14. Informationen zur Konfiguration von Empfehlungen für die Zuweisung von Schwachstellenfinden Sie unter Konfigurieren Sie Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response.

Konfigurieren Sie Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response

Aktivieren Sie Empfehlungen für die Zuweisung von Schwachstellen, um die Zeit zu reduzieren, die Sie für die Identifizierung der Verantwortlichen für nicht oder falsch zugewiesene Schwachstellenergebnisse verwenden.

Vorbereitungen

Erforderliche Rolle: sn_vul.manage_assignment_recom_config

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Diese Anwendung ist standardmäßig nicht aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsempfehlungen**.
2. Wählen Sie **Zuweisungsempfehlungen aktivieren**aus.
   Das **Feld Predictive Intelligence-Lösungsdefinition** wird angezeigt. Der Standardwert ist **„Zuweisung angreifbarer Elemente“**.
3. Klicken Sie auf **Speichern**.

Erstellen und trainieren Sie eine Lösungsdefinition für Vulnerability Response

Erstellen und trainieren Sie ein Lösungsdefinitionsmodell für Vulnerability Response mithilfe von Predictive Intelligence. Sie können dieses Modell verwenden, um die Zuweisungsgruppe für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT) basierend auf vorhandenen Daten vorherzusagen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Klassifizierung** > **Lösungsdefinitionen**.
2. Klicken Sie im Formular „Klassifizierungsdefinitionen“ **auf Zuweisung angreifbarer Elemente**.
   Dies ist die Standardlösungsdefinition.

   Hinweis:
   - Die standardmäßige Schulungshäufigkeit beträgt 30 Tage. Dies bedeutet, dass das Modell alle 30 Tage automatisch mit dem VI-Datensatz neu trainiert wird, der der konfigurierten Filterbedingung entspricht.
   - Felder aus der Tabelle der angreifbaren Elemente können für Schulungen verwendet werden. Die Standardlösungsdefinition trainiert auf zwei VI-Feldern: **Vulnerability.Summary** und **Configuration item.Name**. Je nachdem, welche Felder für Sie hilfreich sind, um die Verantwortung für Schwachstellen in Ihrer Organisation vorherzusagen, können Sie die für das Training verwendeten Felder anpassen.
3. Informationen zum Erstellen und Trainieren der Klassifizierungslösung finden Sie unter Klassifizierungslösung erstellen und trainieren .

   Hinweis:
   Sie können auch eine Ähnlichkeitslösung oder eine Clustering-Lösung erstellen und trainieren. Weitere Informationen finden Sie unter:
   - Ähnlichkeitslösung erstellen und trainieren .
   - Erstellen und trainieren Sie eine Clustering-Lösung .
4. Klicken Sie auf **Update & Retrain (Aktualisieren und neu trainieren)**.

   Hinweis:
   Informationen zur Konfiguration erweiterter Einstellungen für ML-Lösungen finden Sie unter Erweiterte Einstellungen für Ihre ML-Lösungen konfigurieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Vulnerability Response -Rechner

Ein Schwachstellen-Rechner ist eine vordefinierte Formel zur Berechnung eines Zielfelds, wenn bestimmte Kriterien erfüllt sind. Rechner, die die **Risikopunktzahl**des angreifbaren Elements berechnen, können **Risikoregeln**enthalten.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Hinweis:
Sie können eine Leistungsverschlechterung feststellen, wenn Sie Schwachstellen-Rechner ausführen, die Skripts enthalten.

Ordnen Sie Ihre Regeln so an, dass die einfachsten Regeln zuerst ausgeführt werden und Skripts nur für die Elemente ausgeführt werden, die nicht mit einer Bedingung und einem Vorlagenwert oder einer Risikoregel behandelt werden können.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellen-Rechner**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Formular „Schwachstellen-Rechner“.

Feld	Beschreibung
Name	Der Name des Schwachstellen-Rechners.
Tabelle	Automatisch mit dem Namen der Tabelle der angreifbaren Elemente gefüllt.
Anwendung	Automatisch ausgefüllt mit Vulnerability Response.
Zielfeld	Zu berechnendes Feld.
Beschreibung	Textbeschreibung des Rechners.
Aktiv	Rechner ein- oder ausschalten.

4. Klicken Sie mit der rechten Maustaste in den Header, um **Speichern**zu wählen.
   Der Abschnitt **Regeln des Schwachstellen-Rechners** wird angezeigt.
5. Erstellen Sie eine Regel für den Rechner, indem Sie auf **Neu**klicken.

Hinweis:
Das Formular **„Neue Risikoregeln“** (nur verfügbar, wenn das **Feld Zielauf Risikopunktzahl**festgelegt ist) finden Sie in Schritt 10.

6. Füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Regel des Schwachstellen-Rechners“.

Feld	Beschreibung
Name	Name der Rechnerregel.
Bestellung	Reihenfolge, in der der Schwachstellen-Rechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeneintrag von 100 wird vor einem Rechner mit einem Reihenfolgeneintrag von 200 ausgeführt.
Rechner	Automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist das Kontrollkästchen **Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden.
Erweiterte Ansicht	Wenn diese Option ausgewählt ist, können geskriptete Bedingungen und geskriptete Werte unter **Bedingungstyp** und **Werttyp**ausgewählt werden.

7. Füllen Sie die Felder auf der Registerkarte **Wenn diese Bedingung erfüllt ist** entsprechend aus.

Registerkarte, wenn diese Bedingung erfüllt ist

Feld	Beschreibung
Name	Name der Rechnerregel.
Bestellung	Reihenfolge, in der der Schwachstellen-Rechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeneintrag von 100 wird vor einem Rechner mit einem Reihenfolgeneintrag von 200 ausgeführt.
Rechner	Automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist das Kontrollkästchen **Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für angreifbare Elemente, die im System erstellt wurden.
Erweiterte Ansicht	Wenn diese Option ausgewählt ist, wählen Sie geskriptete Bedingungen und geskriptete Werte unter **Bedingungstyp** und **Werttyp**aus.
Bedingungstyp	Verfügbar, wenn Sie die **Ansicht „Erweitert“**auswählen. Zur Auswahl stehen: ○ Filter: Verwendet Filterbedingungen. ○ Filtergruppe: Siehe Eine neue Filtergruppe erstellen, um die Rechnerkriterien zu definieren. ○ Skript: Skriptbedingung, anhand derer bestimmt wird, wann dieser Rechner angewendet werden soll. **Hinweis:** Bevor Sie Skripts schreiben, um zu bestimmen, wann die Rechner angewendet werden sollen, kehren Sie zur Liste **der Schwachstellen-Rechner** zurück. Machen Sie sich mit den Datensätzen des Schwachstellen-Rechners vertraut, die im Lieferumfang des Basissystems enthalten sind.
Bedingung	Definiert grundlegende Filterbedingungen, um zu bestimmen, ob der Rechner verwendet werden soll oder nicht. Wenn Sie entweder den Bedingungstyp **„Filtergruppe“** oder **„Skript“** auswählen, wird dieses Feld ausgeblendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.

8. Klicken Sie auf die Registerkarte **Diese Werte festlegen**, und füllen Sie die Felder im Formular entsprechend aus.

Legen Sie die Registerkarte für diese Felder fest

Feld	Beschreibung
Werttyp	Verfügbar, wenn Sie die **Ansicht „Erweitert“**auswählen. Zur Auswahl stehen: ○ Vorlage: Definieren Sie die Werte, die für jedes Feld festgelegt werden sollen. ○ Skript: Wird verwendet, um die Werte für jedes Feld festzulegen.
Skriptwerte	Verfügbar, wenn Sie den Werttyp **„Skript“** ausgewählt haben. Definiert, auf welche Werte die Berechnungen angewendet werden sollen.
Vorlage	Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten. Wenn Sie den Werttyp **„Skript“** auswählen, wird dieses Feld ausgeblendet.

9. Wenn Sie alle Eingaben abgeschlossen haben, klicken Sie auf **Absenden**.

Hinweis:
Wenn Sie einen vorhandenen Rechner bearbeiten und alle vorhandenen Punktzahlen aktualisieren möchten, können Sie die Schaltfläche **Rechner erneut** anwenden verwenden. Es durchläuft alle aktiven angreifbaren Elemente (VIs), und wenn dieser Rechner zum Festlegen des Werts verwendet wird, wird der Wert für diese VIs neu berechnet. Da das erneute Anwenden eines Rechners sehr lange dauern kann, wird dies von einer regelmäßigen Aufgabe verarbeitet.

10. Füllen Sie im Formular **„Neue Risikoregeln“** die entsprechenden Felder aus.

Legen Sie jede Gewichtung entsprechend dem Prozentsatz des Ergebnisses fest, der von diesem Wert stammen soll. Legen Sie für alle Daten, die Ihr Scanner nicht bereitstellt, oder für Daten, die nicht Teil der Risikopunktzahl sein sollen, die Gewichtung auf Null fest.

Sie können die Felder hinzufügen, löschen oder aktualisieren. Sie können auch den Gewichtungsprozentsatz für die Feldwerte konfigurieren. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.

Wenn Sie die Gewichtungen aktualisieren, zeigen die Szenarien die verbleibenden Gewichtungen sowie die erwarteten **Risikopunktzahlergebnisse** an.

Feld	Beschreibung
Name	Name der Rechnerregel.

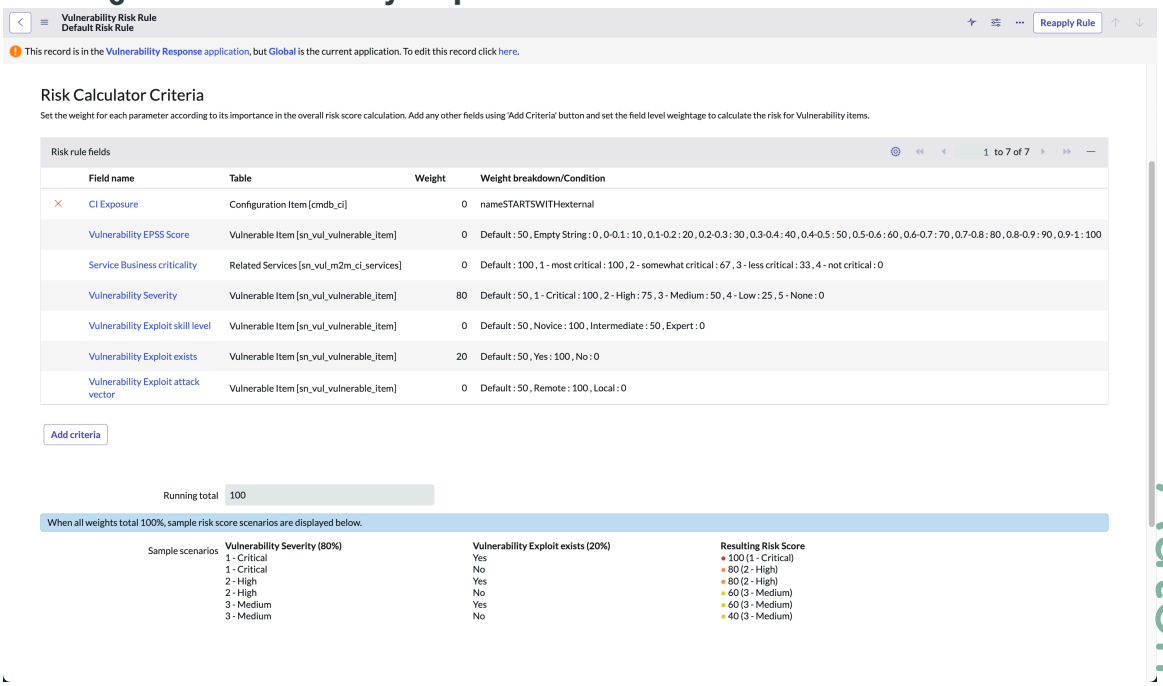
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bestellung	Reihenfolge, in der der Schwachstellen-Rechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeneintrag von 100 wird vor einem Rechner mit einem Reihenfolgeneintrag von 200 ausgeführt.
Rechner	Automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist das Kontrollkästchen **Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden.
Bedingung	Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll. Wenn Sie entweder den Bedingungstyp **„Filtergruppe“** oder **„Skript“** auswählen, wird dieses Feld ausgeblendet.
Gewichte	
Schwachstellenschweregrad	Prozentsatz des Ergebnisses, der sich aus dem Schweregrad ergibt.
EPSS-Punktzahl der Schwachstelle	Wahrscheinlichkeit, dass die Schwachstelle ausgenutzt wird. Standardmäßig ist die Gewichtung dieser Kriterien Null. Wenn Sie dies für die Berechnung der Risikopunktzahl verwenden möchten, legen Sie eine entsprechende Gewichtung für diese Kriterien fest.
Exploit vorhanden	Prozentsatz des Ergebnisses, der aus dem Vorhandensein eines Exploits stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0.
Exploit-Kompetenzniveau	Prozentsatz des Ergebnisses, der aus dem für den Exploit erforderlichen Kompetenzniveau stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0.
Exploit-Angriffsvektor	Prozentsatz des Ergebnisses, der von der Stelle stammt, an der der Angriff anvisiert wurde. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, legen Sie die Gewichtung auf 0 fest.
Service Business-Relevanz	Prozentsatz des Ergebnisses, der sich aus der Geschäftsrelevanz ergibt. Wenn Sie Ihre CIs nicht mit Business-Services verknüpft haben, setzen Sie die Gewichtung auf 0.
CI-Gefahrenpotenzial	Prozentsatz des Ergebnisses, der davon abhängt, ob das CI mit dem Internet verbunden ist. Wenn die Gewichtung nicht Null ist, wird ein Bedingungsfilter angezeigt, mit dem definiert wird, welche CIs mit dem Internet verbunden sind. Legen Sie den Filter fest, um Ihre Configuration Items mit Internetverbindung auszuwählen. Sie können eine Vorschau der Datensätze anzeigen, die der Bedingung entsprechen.
Laufende Summe	Automatisch berechnete Prozentsätze insgesamt. Wenn dieser Wert 100 erreicht, zeigt die Szenariovorschau Beispiel-Risikopunktzahlen in verschiedenen Szenarien an.
Risikopunktzahl-Szenarien	Wenn alle Gewichtungen insgesamt 100 % ergeben, werden Risikopunktzahl-Szenarien angezeigt, die eine Vorschau der Risikopunktzahl in einigen der möglichen Szenarien bieten.

Sie können Kriterien hinzufügen oder entfernen und die Gewichtung jedes Kriteriums mithilfe der eingebetteten Liste anpassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikoregel-CI für Vulnerability Response v20.x



11. Klicken Sie auf **Absenden**.

Deaktivieren Sie den standardmäßigen Schwachstellen-Rechner, wenn er nicht verwendet wird

Wenn Sie keine Schwachstellen-Rechner verwenden, deaktivieren Sie den Standard-Rechner zusätzlich zu allen anderen, die Sie definiert haben. Sicherheitsrisiko-Rechner werden jedes Mal ausgeführt, wenn der Datensatz eines angreifbaren Elements erstellt oder aktualisiert wird, und können sich auf die Leistung des anfänglichen Imports auswirken.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**.
2. Öffnen Sie den entsprechenden Rechner.
3. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um den Rechner zu deaktivieren.
4. Klicken Sie auf **Aktualisieren**.

Erstellen, aktivieren oder ändern Sie Vulnerability Response Regeln für die automatische Löschung

Sie können die Löschregeln für das Löschen von angreifbaren Elementen (VIs) und Korrekturaufgaben (RT) erstellen, aktivieren oder ändern. Verwenden Sie die automatische Löschung, um ältere Datensätze aus den Tabellen „VI“ und „RT“ zu entfernen.

Vorbereitungen

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rollen:

- Administrator: die Regeln für die automatische Löschung ändern
- sn_vul.vulnerability_admin oder sn_vul.admin (veraltet): Modul für automatische Löschung anzeigen

Warum und wann dieser Vorgang ausgeführt wird

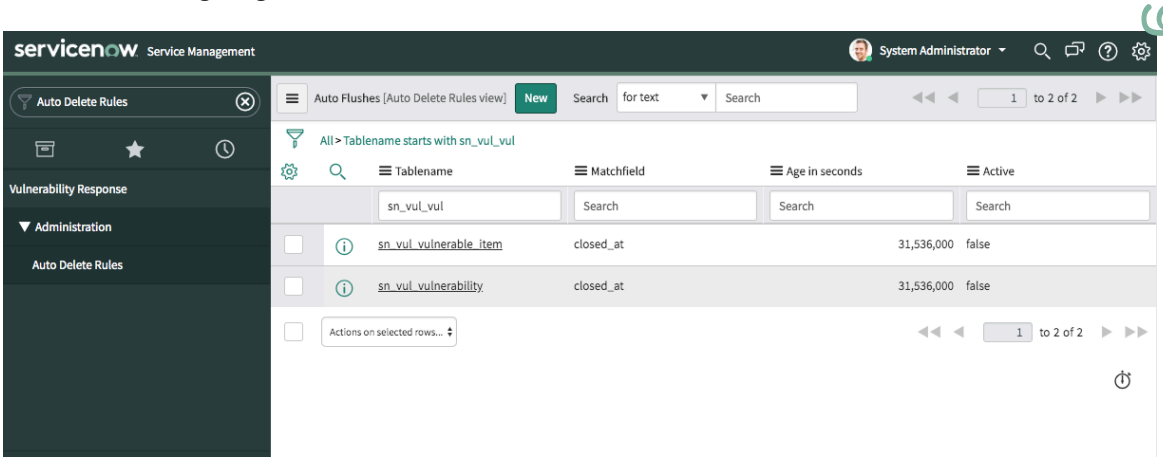
Mit der Zeit sammelt sich in den Tabellen „VI“ und „VUL“ in Ihrer Instanz wahrscheinlich eine große Menge geschlossener Datensätze an. Viele dieser Datensätze waren möglicherweise länger als 365 Tage geschlossen, wurden jedoch nicht entfernt. Verwenden Sie Regeln zum automatischen Löschen, um viele dieser älteren, geschlossenen Datensätze zu entfernen. Durch das Entfernen dieser Datensätze verringert sich nicht nur die Anzahl der Datensätze in den Tabellen „VI“ und „VUL“, durch das Löschen wird auch die Leistung hoch gehalten.

Obwohl die automatische Löschung standardmäßig auf Datensätze abzielt, die 365 Tage lang geschlossen wurden, kann es bei der allerersten Ausführung versuchen, zu viele Datensätze in einer einzigen Transaktion zu löschen. Abhängig von der Größe Ihrer Umgebung können Sie den Löschvorgang zeitlich versetzt durchführen, um den Umfang der Abfrage zu begrenzen. Beispielsweise können Sie Ihre erste Ausführung für geschlossene Datensätze starten, die älter als 450 Tage sind. Nach Abschluss dieses Durchlaufs können Sie sich in kleineren Schritten (425, 400, 375) nach unten arbeiten, bis Sie die Anzahl der Datensätze reduziert haben, die älter als 365 Tage sind.

Mit Now Platform® werden zwei Regeln bereitgestellt, die geschlossene Datensätze, die bestimmte Bedingungen erfüllen, sowie alle darauf verweisenden Datensätze automatisch löschen. Eine Regel löscht angreifbare Elemente, die andere Korrekturaufgaben. Standardmäßig sind diese Regeln für die automatische Löschung deaktiviert, sodass Sie sie vor dem Löschen von Datensätzen manuell aktivieren müssen. Sie können die beiden vorkonfigurierten Regeln auswählen, die mit Ihrer Instanz bereitgestellt werden, oder Sie können eine eigene Regel erstellen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für das automatische Löschen**.
   Die Listenansicht wird angezeigt.



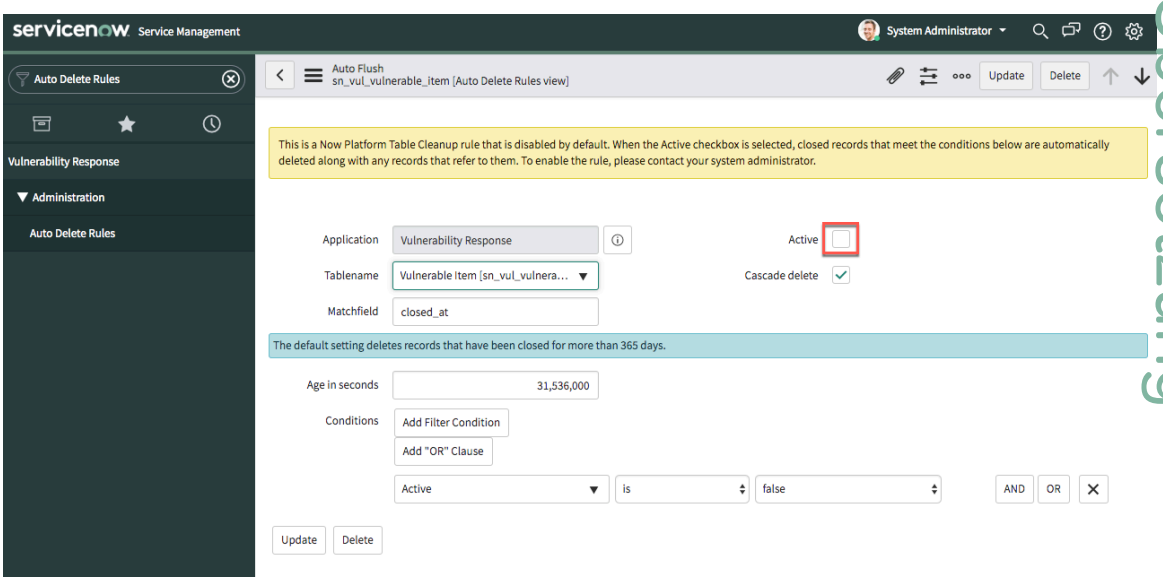
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie zum Bearbeiten die Regel zum Löschen von angreifbaren Elementen (sn_vul_vulnerable_item) oder die Regel für Korrekturaufgaben (sn_vul_vulnerability).
3. Klicken Sie zum Erstellen einer neuen Regel auf **Neu**.
4. Füllen Sie die Felder im Formular entsprechend aus, oder bearbeiten Sie sie.

Feld	Beschreibung
Anwendung	Name der Anwendung, in der Datensätze gelöscht werden. Der Standardwert ist Vulnerability Response.
Tabellenname	Name der Tabelle, für die die Regel angewendet wird.
Feld abgleichen	Feld, für das das System die Dauer überwacht.
Aktiv	Option zum Aktivieren der Regel. Nach der Aktivierung kann der Datensatz gelöscht werden.
Kaskadierendes Löschen	Option zum Löschen aller übereinstimmenden Datensätze sowie aller darauf verweisenden Datensätze. Wenn diese Option nicht ausgewählt ist, werden nur übereinstimmende Datensätze gelöscht, nicht jedoch die darauf verweisen.
Alter in Sekunden	Alter des zu löschenden Schwachstellen-Datensatzes. Sowohl für VI- als auch für RT-Regeln beträgt das Alter 365 Tage. Dieses Alter wird in Sekunden angezeigt.
Bedingungen	Filterbedingungen, die die Datensätze in den Tabellen „VI“ und „RT“ (VUL) definieren, für die die Regeln gelten.

5. Aktivieren Sie das Kontrollkästchen **Aktiv**, um eine Regel zu aktivieren.



Sobald die Regel aktiviert ist, löscht die stündliche Plattformfunktion **Automatische Leerung**die Datensätze aus der Tabelle, für die die Regel aktiviert ist.

Wenn Ihre Umgebung Millionen oder mehrere zehn Millionen Datensätze enthält, die Ihren Löschkriterien entsprechen, sollten Sie sich an ServiceNow den -Kundensupport wenden, bevor Sie die Regeln für die automatische Löschung aktivieren, damit Sie Datensätze in einem stufenweisen Prozess löschen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie der Vulnerability Response-Homepage Diagramme zur Bedeutung von Schwachstellen hinzu

Sie können der Übersicht Diagramme zur Definition der Bedeutung der Schwachstelle und andere Visualisierungen hinzufügen.

Vorbereitungen

- Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.
- Das Plugin „Vulnerability Analytics“ muss aktiviert sein.

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Übersicht**.
   Einige Berichte werden dem Dashboard standardmäßig hinzugefügt. Weitere Informationen zu diesen Berichten finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..
2. Klicken Sie neben dem Header des Dashboards auf das Kartenansichtssymbol + **Inhalt hinzufügen**, um das Dialogfeld zum Hinzufügen weiterer Widgets zu öffnen.
3. Wählen Sie in den Listen im Dialogfeld **„Widgets hinzufügen“Berichte** aus, um weitere Vulnerability Response -Berichte anzuzeigen.
4. Klicken Sie auf die Position auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
5. Schließen Sie das Feld **Inhalt hinzufügen**.

Definieren Sie E-Mail-Benachrichtigungen Vulnerability Response .

Richten Sie E-Mail-Benachrichtigungen ein, um nützliche Informationen über wichtige Updates und Aktivitäten wie die Genehmigung und Ablehnung von falsch positiven Anforderungen zu teilen. Beim Erstellen einer E-Mail-Benachrichtigung müssen Sie angeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **E-Mail-Vorlagen**.
2. Wählen Sie **Neu**.

   Ausführliche Anweisungen zum Erstellen von E-Mail-Benachrichtigungen finden Sie unter Create an email notification .

Ergebnisse

Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Links je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Im Vulnerability Manager Workspace werden Links für Benutzer mit den Rollen sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin geöffnet.
- Im IT Remediation Workspace werden Links für Benutzer mit der Rolle sn_vul.remediation_owner geöffnet.

Wenn der Empfänger über keine der genannten Rollen verfügt, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Definieren Sie Vulnerability Response E-Mail-Vorlagen

Beim Erstellen einer E-Mail-Benachrichtigung müssen Sie angeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **E-Mail-Vorlagen**.
2. Wählen Sie **Neu**.

   Ausführliche Anweisungen zum Erstellen von E-Mail-Vorlagen finden Sie unter Construct an email message with a template .

Erstellen oder bearbeiten Sie Benachrichtigungen für Korrekturziele

Schwachstellenadministratoren können die Korrekturzielbenachrichtigung bearbeiten oder neue hinzufügen und angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**.
2. Wählen Sie den Benachrichtigungsdatensatz des Korrekturziels oder **Neu**aus.
3. Füllen Sie die Felder des Formulars entsprechend aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie **Benachrichtigungsvorschau** aus, um die Nachricht anzuzeigen.

Ergebnisse
Ab v21.0 von Vulnerability Responsewerden Empfänger, die auf die Links in einer E-Mail-Benachrichtigung klicken, je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

- Im Vulnerability Manager Workspace werden Links für Benutzer mit den Rollen sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin geöffnet.
- Im IT Remediation Workspace werden Links für Benutzer mit der Rolle sn_vul.remediation_owner geöffnet.

Wenn der Empfänger über keine der genannten Rollen verfügt, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Bewertung des Gefahrenpotenzials für Schwachstelle .

Bewerten Sie die Zero-Day-Gefährdung (aktueller Tag) Ihrer Assets durch angreifbare Software mit der Anwendung Schwachstellenbewertung Bewertung des Gefahrenpotenzials.

Wichtig:
Sie können die Bewertung des Gefahrenpotenzials nach Common Vulnerabilities and Exposures (CVE) und Software durchführen, um die zusätzlichen Funktionen im Arbeitsbereich für die Schwachstellenbewertung zu nutzen. Weitere Informationen finden Sie unter Erkunden Sie den Arbeitsbereich der Schwachstellenbewertung.

Erforderliche Rolle: Administrator

Kompatibilität und Systemanforderungen

Die Anwendung Vulnerability Response ist unter ServiceNow Storeverfügbar. Die Anwendung Software Asset Management (SAM) Foundation [com.snc.asset_management] wird als Teil der Anwendung Vulnerability Response installiert. Um sicherzustellen, dass die Anwendung SAM Foundation auf Ihrer Instanz installiert ist, navigieren Sie zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie nach com.snc.asset_management. Wenn die Anwendung nicht installiert ist, wählen Sie **Installieren**aus. Weitere Informationen zu SAM Foundation finden Sie unter Software Asset Management Foundation plugin .

Da die Anwendung Schwachstellenbewertung Bewertung des Gefahrenpotenzials Zugriff auf die Asset-Daten in Ihrer Instanz Now Platform® erfordert, müssen die Asset-Verwaltungsanwendungen über Referenzdaten verfügen. Die Tabelle „Software-Discovery-Modelle“ [cmdb_sam_sw_discovery_model] und die Softwareinstallationen [cmdb_sam_sw_install] erfordern Daten.

Die Anwendung Schwachstellenbewertung Bewertung des Gefahrenpotenzials und funktioniert entweder mit den Anwendungen SAM Foundation oder SAM Pro Now Platform®. Die Anwendung „SAM Pro“ ist nicht Teil des Kernprodukts Vulnerability Response von ServiceNow Store und erfordert ein separates Abonnement.

Hinweis:
Die Anwendung „SAM Pro“ ist nur für die Inhaltsbibliothek erforderlich, mit der Sie bessere Ergebnisse erzielen können.

Ab v23.0 von Vulnerability Responsewerden Sie mit dem Abonnement Pro oder Enterprise basierend auf Ihrer Rolle zur Seite **„Risikobewertung“** in den Arbeitsbereichen weitergeleitet, wenn Sie im Menü **„Alle“** auf den Link **„Risikobewertung“** klicken:

Zugriff auf die Seite „Risikobewertung“ in den Arbeitsbereichen

Rolle	Arbeitsbereich
Schwachstellenmanager	Arbeitsbereich des Schwachstellenmanagers
Ereignismanager [sn_vul_analyst.vul_event_manager] oder Notfallmaßnahmen [sn_vul_analyst.emergency_response]	Arbeitsbereich der Schwachstellenbewertung

Um zu vermeiden, dass Sie zu den Arbeitsbereichen umgeleitet werden und auf der Seite „Classic Exposure Assessment“ bleiben, setzen Sie den **Linktyp** auf der Registerkarte Linktyp auf der Seite „Module – Bewertung des Gefahrenpotenzials“ auf *Liste der Datensätze*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können auf die Seite „Modul – Bewertung des Gefahrenpotenzials“ zugreifen, indem Sie im Menü **„Alle“** neben dem Link **„Bewertung des Gefahrenpotenzials“** das Symbol **„Modul bearbeiten“** wählen.

Mit der Rolle „Schwachstelle – Schreiben“ [sn_vulnerability_write] können Sie das Modul „Bewertung des Gefahrenpotenzials“ anzeigen und bei Bedarf mit der Anwendung Vulnerability Response Datensätze zur Bewertung des Gefahrenpotenzials für angreifbare Software in Ihrer Instanz erstellen und bearbeiten.

Zugehörige Informationen

Bewerten Sie Ihre Gefährdung durch angreifbare Software

Konfigurieren Sie die Ausnahmeverwaltung für Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Richtlinie, einen Standard oder eine Leitlinie für das Schwachstellenmanagement oder die Sicherheit nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT), die nicht gemäß der Richtlinie behoben werden können.

Vorbereitungen

Begrenzen Sie die Dauer einer angeforderten Ausnahme, und fügen Sie der Ausnahme oder der falsch positiven Anforderung mithilfe des Moduls Vulnerability Responseeinen Fragebogen hinzu . Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Vulnerability Response angefordert. Sie können auch mit der -Integration GRC: Richtlinien- und Compliance-Management eine Ausnahme anfordern.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.manage_exception_configuration

Warum und wann dieser Vorgang ausgeführt wird

Wenn Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Richtlinien- und Compliance-Management installiert ist, GRC: Richtlinien- und Compliance-Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder falsch positive Anforderung ausgelöst hat. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für das Anfordern der Ausnahme zu verstehen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular „Ausnahmeverwaltungskonfiguration“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option in der Liste **Ausnahmen verwalten mit** auswählen.
   Sie können entweder Vulnerability Response oder GRC: Richtlinien- und Compliance-Managementauswählen. Sie müssen das Plugin GRC aktivieren, um mit GRC: Richtlinien- und Compliance-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Management eine Ausnahme anzufordern. Das Ändern der Konfiguration hat keine Auswirkungen auf die vorhandenen Daten.

3. Wenn Sie die Option Vulnerability Response ausgewählt haben, geben Sie die folgenden Informationen ein:

Einstellungen für das Formular „VR-Ausnahmeverwaltung“.

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Zeigt den von Ihnen ausgewählten Fragebogen zum Anfordern einer Ausnahme an. Der **Ausnahmefragebogen** wird standardmäßig angezeigt. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Fragebogen zum Anfordern einer Ausnahme aktivieren** aktivieren.
Fragebogen für Ausgleichssteuerung	Zeigt den Fragebogen an, den ein Korrekturbesitzer für Risikominderungsanforderungen beantworten muss. Ab v20.0 von Vulnerability Responsekönnen Sie Fragebogen für Risikominderungsanforderungen festlegen. Der **Fragebogen zur Ausgleichssteuerung** ist standardmäßig ausgewählt. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Fragebogen zum Anfordern einer Ausnahme aktivieren** aktivieren.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung.
Fragebogen, um falsch positive Meldung zu markieren	Zeigt den von Ihnen ausgewählten Fragebogen als falsch positiv an. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt. **Hinweis:** Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **„Fragebogen zum Markieren von falsch positiv aktivieren“** aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie den vorhandenen Fragebogen angepasst haben und auf v20.0 upgraden, wird dieser angepasste Fragebogen für die Anforderung zur Risikominderung anstelle des standardmäßigen **Fragebogens zur Ausgleichssteuerung**angezeigt.

4. Wenn Sie die Option GRC: Richtlinien- und Compliance-Management ausgewählt haben, geben Sie die folgenden Informationen ein:

Einstellungen für das Formular „VR-Ausnahmeverwaltung“.

Feld	Beschreibung
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung.
Fragebogen, um falsch positive Meldung zu markieren	Zeigt den von Ihnen ausgewählten Fragebogen als falsch positiv an. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt.

5. So konfigurieren Sie Fragebogen basierend auf Bedingungen für Ausnahme- und falsch positive Anforderungen:

   a. Wählen Sie im Abschnitt „Konfiguration des VR-Fragebogens“ **Neu**.

   b. Füllen Sie im Formular „Fragebogenkonfiguration – Neuer Datensatz“ die Felder aus, und wählen Sie **Absenden**aus.
   Weitere Informationen zu den Formularfeldern „Fragebogenkonfiguration“ finden Sie unter Formularfelder „Fragebogenkonfiguration“..
   Der erstellte Fragebogen wird im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ angezeigt.

   Wenn Sie beispielsweise einen Fragebogen für falsch positive Anforderungen für kritische angreifbare Elemente konfigurieren möchten, wählen Sie die Genehmigungsregel **„Falsch positiv für angreifbare Elemente“**, geben Sie die Bedingung „ Risikobewertung ist 1 – Kritisch“ an, und wählen Sie den gewünschten Fragebogen im Formular „Fragebogenkonfiguration “ aus .

6. Wählen Sie **Speichern**.

Fügen Sie einen Ausnahmegenehmiger hinzu

Fügen Sie den Genehmigergruppen Benutzer hinzu, um eine Ausnahme anzufordern.

Vorbereitungen

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.exception_approver

Warum und wann dieser Vorgang ausgeführt wird

Bis Vulnerability Response v14.0 wird eine Ausnahmeanforderungfür ein angreifbares Element oder eine Korrekturaufgabe mit dem standardmäßigen zweistufigen Genehmigungsworkflow genehmigt. Die Anforderung muss von zwei Genehmigungsebenen genehmigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Bis Vulnerability Response v14.0 kann keine Ausnahme angefordert werden, wenn es keinen Genehmiger der ersten Ebene gibt. Ab Vulnerability Response v15.0 wird jedoch, wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**.
2. Suchen Sie in der Spalte Name nach **Ausnahme**, und klicken Sie auf **Ausnahmegenehmiger - Ebene 1**.

   Hinweis:
   Ab Vulnerability Response v12.8.1 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme- oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie *sn_vul.exception_approver_L1*, *sn_vul.exception_approver_L2*oder *sn_vul.false_positive_approver_group*, um den Eigenschaftswert zu ändern.

3. Klicken Sie im Formular „Gruppenausnahmegenehmiger – Ebene 1“ auf die zugehörige Liste Gruppenmitglieder.
4. Klicken Sie zum Erstellen einer Liste **auf Neu**.
5. Füllen Sie die Felder des Formulars aus.

Anwenderformular

Feld	Beschreibung
Anwender-ID	Eindeutiger Bezeichner für den Benutzer
Vorname	Vorname des Anwenders.
Nachname	Nachname des Anwenders.
Titel	Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus.
Abteilung	Abteilung des Anwenders.
Passwort	Dem Anwender zugewiesenes Passwort. Dieses Passwort kann dauerhaft oder vorübergehend sein.
Passwort muss zurückgesetzt werden	Option, mit der der Anwender das Passwort zurücksetzen kann, um die Sicherheit zu gewährleisten.
Gesperrt	Option, den Anwender für die Instanz zu sperren und alle aktiven Sitzungen des Anwenders zu beenden. Das System verhindert, dass Benutzer mit der Rolle admin sich selbst sperren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option zum Aktivieren dieses Anwenders. Nur Sie können inaktive Anwender in den folgenden Bereichen sehen: ○ Listen von Benutzern ○ Auswahlliste für Referenzfelder (Lupensymbol) ○ AutoVervollständigen Sie die Liste, die angezeigt wird, wenn Sie etwas in ein Referenzfeld eingeben
Nur Webservice-Zugang	Option, um diesen Anwender als nicht interaktiven Anwender festzulegen.
Interner Integrationsanwender	Option, um diesen Anwender als internen Integrationsanwender festzulegen.
E-Mail	E-Mail-Adresse des Anwenders.
Sprache	Bevorzugte Sprache des Anwenders.
Kalenderintegration	Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook.
Zeitzone	Zeitzone für den Standort dieses Anwenders.
Datumsformat	Bevorzugtes Format des Anwenders für Datumsangaben.
Telefon (geschäftlich)	Geschäftstelefon des Benutzers.
Mobiltelefon	Mobiltelefon des Benutzers.
Foto	Foto, das Sie hochladen können, indem Sie auf **„Zum Hinzufügen klicken...“ klicken**.

6. Klicken Sie auf **Absenden**.
7. Wiederholen Sie die Schritte 1 bis 5, um einen Ausnahmegenehmiger der Ebene 2 zu erstellen. Der Genehmiger muss zu **Vulnerability Response** > **Meine Genehmigungen** navigieren und Anforderungen genehmigen.

Hinweis:
Informationen zum Genehmigen einer Ausnahme für GRC: Richtlinien- und Compliance-Managementfinden Sie unter Richtlinien- und Compliance-Management – Optionales Setup .

Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung

Verwenden Sie ab Vulnerability Response v15.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung, Ausnahmeregeln und die Verwaltung falsch positiver Ergebnisse zu genehmigen. Wenn Sie Vulnerability Response (VR) zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie bereits VR-Benutzer sind, lautet die Standardoption Workflow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Vulnerability Response v15.0 oder höher bereitgestellt haben, ist der Wert der Systemeigenschaft *sn_vul.flow_designer_activation* auf „true“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie Vulnerability Response bereits vor v15.0 verwenden, ist der Wert dieser Systemeigenschaft auf „false“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in true ändern.

Hinweis:
Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Elemente
- Ausnahmeregel
- Falsch positiv für Korrekturaufgaben
- Falsch positiv für angreifbare Elemente

Hinweis:
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für die Ausnahmeverwaltung.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.
Anwendung	Der Standardwert ist Vulnerability Response.
Regeltyp	Gibt den Regeltyp an. Beispiele: Ausnahmeverwaltung, falsch positive Meldung oder Ausnahmeregel.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurze Beschreibung der Genehmigungsregeln.
Genehmigungsablaufy (Tage)	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ab v21.0 von Vulnerability Response	
Genehmiger benachrichtigen (Tage) Ab v21.0 von Vulnerability Response	Datum, nach dem der Genehmiger benachrichtigt wird, um Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel.

Hinweis:
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für die Ausnahmeverwaltung.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die für verschiedene Konfigurationselemente gefunden wurden.

Erstellen Sie Konfigurationen für eine Genehmigungsregel

Definieren Sie die Bedingungen, um übereinstimmende angreifbare Elemente, Korrekturaufgaben oder Ausnahmeregeln für eine Genehmigungsebene herauszufiltern.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Im Modul Genehmigungskonfigurationen können Sie mehrere Genehmigungsebenen für verschiedene Konfigurationen konfigurieren. Definieren Sie bedingungsbasierte Regeln, wobei jede Regel mehrere Genehmigungsebenen enthält.

Hinweis:
Verwenden Sie das Modul Genehmigungsregeln, um Genehmigungsregeln für die Ausnahmeverwaltungs-Workflows zu konfigurieren. Informationen zum Konfigurieren von Genehmigungsregeln finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungskonfiguration“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Bestellung	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungskonfiguration verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungskonfigurationsebenen.

5. Legen Sie auf eine der folgenden Arten eine Bedingung für die angreifbaren Elemente oder Korrekturaufgaben fest:

Feld	Beschreibung
Bedingung	Identifiziert die übereinstimmenden angreifbaren Elemente oder Korrekturaufgaben.
Erweiterte Bedingung	Skript, das die Bedingung für die angreifbaren Elemente oder Korrekturaufgaben definiert. **Hinweis:** Dieses Feld erscheint, wenn Sie das Kontrollkästchen **Erweitert** aktivieren.

6. Wählen Sie **Aktualisieren**.
Sie können Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für die Ausnahmeverwaltung.

Example:
Sie können verschiedene Genehmigungspfade definieren für:

- Beispiel 1: Verschiedene Arten von Schwachstellen oder Konfigurationselementen (mit Internetzugriff oder intern).
- Beispiel 2: Zurückstellungs- und Risikominderungsanforderungen, wenn ein Korrekturbesitzer diese Anforderungen gleichzeitig für angreifbare Host-Elemente (VITs) oder Korrekturaufgaben (VUL) stellt.

  Die Spalte „Change-Genehmigung“ enthält die Change-Genehmigungsdatensätze mit Zurückstellungsstatus. Wenn Sie mit dem Bedingungsgenerator eine Bedingung für die Spalte „Change-Genehmigung“ festlegen, wird der Genehmigungsdatensatz für die Zurückstellung berücksichtigt, nicht jedoch der Genehmigungsdatensatz für die Risikominderung. Um die Bedingung für den Change-Genehmigungsdatensatz für den Risikominderungsstatus festzulegen, verwenden Sie das Feld **Erweiterte Bedingung**.

  Für die Genehmigungsregel **„Ausnahmeanforderung für angreifbare Elemente“** ist die **Anforderung einer Risikobewertung von Mittel bis Niedrig** im Lieferumfang

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

des Basissystems enthalten. Diese Konfiguration ist standardmäßig auf „false“ festgelegt. Sie können diese Konfiguration verwenden, um einen Genehmigungspfad für Risikominderungsanforderungen von „Mittel“ auf „Niedrig“ festzulegen. Sie können das Skript in dieser Konfiguration auch aktualisieren, sodass es für verschiedene Änderungen der Risikoeinstufung in den Risikominderungsanforderungen gilt.

Anforderung einer Risikoeinstufung von Konfiguration „Mittel“ bis „Niedrig“:

```
function evaluate() {
   var gr = new GlideRecord("sn_vul_change_approval");
   gr.addQuery("sys_id", approval);
   gr.addQuery("current_value", "3 - Medium");
   gr.addQuery("desired_value", "4 - Low");
   gr.query();
   if (gr.next()) {
      return true;
   }
   return false;
}
evaluate();
```

Legen Sie die vorhergehende Konfiguration auf „wahr“ mit der niedrigsten Reihenfolge fest, und legen Sie die **Standardkonfiguration – Ausnahmeanforderung für VI-**Konfiguration auf „wahr“ fest.

Ergebnis: Wenn ein Remediationsbesitzer im IT-Korrektur-Arbeitsbereich gleichzeitig eine Zurückstellung und Risikominderungsanforderungen auslöst, werden die Genehmigungsanforderungen für die Zurückstellung an die Genehmiger weitergeleitet, die in der **Standardkonfiguration - Ausnahmeanforderung für AE** definiert sind, und die Genehmigungsanforderungen für die Risikominderung werden an die Genehmiger weitergeleitet ist in der Konfiguration der **Anforderung einer Risikoeinstufung von mittel bis niedrig** definiert.

Erstellen Sie Genehmigungsebenen für die Ausnahmeverwaltung

Definieren Sie die Ebenen von Anwendern und Anwendergruppen, die die Ausnahmeanforderungen genehmigen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. Wählen Sie im Abschnitt Genehmigerebenen eine Genehmigerebene aus.
5. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Genehmigerebene“

Feld	Beschreibung
Name	Name der Genehmigungsebene.
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ○ Ein Genehmiger erforderlich ○ Alle Anwender müssen genehmigen
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.
Bestellung	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen.
Zuweisen mit	Wählen Sie eine Option aus: ○ Anwender und Anwendergruppe ○ Genehmigungstabellenfeld ○ Skript
Gruppen	Gruppe auf Genehmigerebene, die aus mehreren Anwendern besteht. Der Benutzer muss eine der folgenden Rollen aufweisen: ○ sn_vul.exception_approver: Für Ausnahmeverwaltung und Ausnahmeregeln ○ sn_vul.false_positive_approver: Für falsch positiv
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

6. Um die Änderungen zu speichern, wählen Sie **Aktualisieren**.

Hinweis:
Vor v15.0 funktionierte der Workflow-Prozess, wenn Benutzer nur auf Ausnahmeebene 1 vorhanden sind. Ab v15.0 muss jedoch mindestens ein Benutzer auf jeder Ebene vorhanden sein.

Vor v15.0 wurde im Workflow das angreifbare Element oder die angreifbare Gruppe zurückgestellt, wenn kein Benutzer auf der zweiten Ebene vorhanden war. Wenn jedoch ab v15.0 kein Benutzer in der zweiten Ebene vorhanden ist, wird die Genehmigungsanforderung automatisch abgelehnt.

Example:
Es kann unterschiedliche Genehmigungsebenen für Schwachstellen für Linux- und Windows-Server geben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer

Ab Vulnerability Response v15.0 wird, wenn Sie Vulnerability Response (VR) zum ersten Mal bereitstellen, der Flow Designer für die Genehmigung von Ausnahmeanforderungen in der Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie bereits VR-Benutzer sind, lautet die Standardoption Workflow.

Hinweis:
Ab Vulnerability Response v19.0 wird für Neukunden nur Flow Designer unterstützt. Wenn Sie ein vorhandener -Benutzer sind und ein Upgrade auf Vulnerability Response v19.0 durchführen, werden sowohl der Flow Designer als auch der Ausnahmeverwaltungs-Workflow unterstützt.

Workflow im Vergleich zu Flow Designer

Überlegungen	Workflow	Flow Designer
Version	Vor v15.0 von Vulnerability Response.	Ab v15.0 von Vulnerability Response.
Standardoption	Standardoption, wenn Sie ein vorhandener VR-Benutzer sind.	Standardoption für neue VR-Benutzer ab v15.0.
Genehmigungsprozess festlegen	Die Ausnahmeverwaltung umfasst Anforderungen für Ausnahmen und falsch positive Ergebnisse sowie Ausnahmeregeln.	Umfasst die Definition verschiedener Ebenen und das Hinzufügen verschiedener Genehmiger für verschiedene Anwendungsfälle. Einfacher zu implementieren als der Workflow. Die Ausnahmeverwaltung umfasst Anforderungen für Ausnahmen und falsch positive Ergebnisse sowie Ausnahmeregeln.
Upgrade auf Flow Designer	Sie können vom Workflow ein Upgrade auf den Flow Designer durchführen. Bestehende Anforderungen können jedoch nur mit dem Workflow genehmigt werden.	Flow Designer ist standardmäßig aktiviert.
Systemeigenschaft `sn_vul.flow_designer_activation`	Wenn Sie den Workflow für die Ausnahmeverwaltung vor v15.0 verwendet haben, ist die Systemeigenschaft auf „false“ festgelegt. Um den Flow Designer zu aktivieren, legen Sie diese Eigenschaft auf „true“ fest. **Hinweis:** Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben.	Wenn Sie VR zum ersten Mal für v15.0 oder höher verwenden, wird der Wert der Systemeigenschaft standardmäßig auf „true“ festgelegt.
Modul „Genehmigungsregeln“.	Nachdem die Systemeigenschaft auf true festgelegt wurde, wird die geplante Aufgabe **zum Aktivieren von Modulgenehmigungsregeln**	Wenn Sie VR ab VR v15.0 zum ersten Mal bereitstellen, ist dieses Modul standardmäßig verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow im Vergleich zu Flow Designer (Fortsetzung)

Überlegungen	Workflow	Flow Designer
	innerhalb von 24 Stunden ausgeführt. Diese geplante Aufgabe aktiviert das Modul **„Genehmigungsregeln“**. Um dieses Modul sofort zu aktivieren, führen Sie diese Aufgabe manuell aus.	
Genehmigungsstufen	Bietet die Option, nur zwei Ebenen von Genehmigern festzulegen.	Bietet mehrere Optionen, z. B. das Festlegen einer beliebigen Anzahl von Konfigurationen, Genehmigerebenen und das dynamische Hinzufügen von Genehmigern für jede Regel.

Fügen Sie einen falsch positiven Genehmiger hinzu

Nur Anwender, die der Falsch-positiv-Genehmigergruppe hinzugefügt werden, können Falschmeldungen für angreifbare Elemente (VIs) und Korrekturaufgaben (VULs) genehmigen. Die Gewährung eines falsch positiven Werts ist ein einstufiger Genehmigungsprozess.

Vorbereitungen

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Hinweis:

Ab Vulnerability Response v15.0 wird der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert, wenn Sie die VR-Anwendung zum ersten Mal bereitstellen. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > > **Anwenderadministration** > **Gruppen**.
2. Suchen Sie in der Spalte **Name** nach **False Positive (Falsch positiv)**, und klicken Sie auf die Option.
3. Navigieren Sie im Gruppenformular zu **Gruppenmitglieder** > **Neu** (oder **Bearbeiten**).
4. Erstellen Sie im Formular „Benutzer“ einen Datensatz, indem Sie die Benutzerdetails eingeben, und klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Rollen werden dem Benutzer gewährt. Die ausgewählten Benutzer werden der Liste Gruppenmitglieder hinzugefügt. Diese Mitglieder können Anforderungen genehmigen, um VIs oder Korrekturaufgaben als falsch positiv zu kennzeichnen. Nach der Genehmigung wird der Status des Datensatzes auf „Geschlossen“ aktualisiert und erst am angegebenen Datum erneut geöffnet.

Konfigurieren Sie den Fragebogen zur Risikominderung

Ab Vulnerability Response v20.0 können Sie den Fragebogen der Risikominderungsanfrage für eine Reihe von gefilterten angreifbaren Elementen oder Korrekturaufgaben anpassen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der **Fragebogen für Ausgleichssteuerungen für angreifbare Elemente** und **der Fragebogen für Ausgleichssteuerungen für Genehmigungsregeln für angreifbare Gruppen** sind im Lieferumfang des Basissystems enthalten.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Aktivieren Sie im Formular „Einstellungen für VR-Ausnahmeverwaltung“ das Kontrollkästchen Fragebogen zum Anfordern einer Ausnahme aktivieren.
3. So konfigurieren Sie Fragebogen basierend auf Bedingungen für Risikominderungsanforderungen:
   a. Wählen Sie im Abschnitt „Konfiguration des VR-Fragebogens“ **Neu**.
   b. Wählen Sie im Formular „Fragebogenkonfiguration – Neuer Datensatz“ die Genehmigungsregel „**Fragebogen für Ausgleichssteuerungen für angreifbare Gruppen“** oder **„Fragebogen für Ausgleichssteuerungen für angreifbare Elemente“** aus, und geben Sie die Bedingung an.
   c. Wählen Sie den gewünschten Fragebogen und dann **Absenden**aus.
   Weitere Informationen zu den Formularfeldern „Fragebogenkonfiguration“ finden Sie unter Formularfelder „Fragebogenkonfiguration“..
   Der erstellte Fragebogen wird im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ angezeigt.
4. Wählen Sie im Formular Einstellungen für VR-Ausnahmeverwaltung **die Option Speichern aus**.

Zeigen Sie Vulnerability Response-SLAs für Korrekturaufgaben an

Um sicherzustellen, dass angreifbare Elemente korrekt verarbeitet werden, können Sie eine Servicelevel-Vereinbarung (Service Level Agreement, SLA) für Korrekturaufgaben für Vulnerability Response definieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die SLA-Definitionen in dieser Liste sind eine Teilmenge der Plattform-SLA-Liste, spezifisch für Vulnerability Response.

Detaillierte Anweisungen hierzu finden Sie unter Create an SLA definition .

Wenn Sie die Zeit nachverfolgen, die zur Korrektur von AEs benötigt wird, sollten Sie Vulnerability Response Korrekturzielregelnverwenden. Korrekturzielregeln definieren die erwarteten Zeitrahmen für die Korrektur angreifbarer Elemente (VI), insbesondere im Kontext von Vulnerability Response, während SLAs einen Zeitrahmen für die Korrektur der Schwachstelle selbst bieten können.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **SLA-Definitionen**.
2. Klicken Sie auf eine Definition.
   Aufgaben-SLAs werden in den zugehörigen Listen der **Korrekturaufgaben**angezeigt.

Konfigurieren Sie den Watchdog

Verwenden Sie die Watchdog-Konfigurationsseite, um neue Watchdogs mit Bedingungen zu erstellen oder zu aktualisieren, die Sie angeben möchten. Sie können die Benachrichtigung für jeden Watchdog aktivieren und sich benachrichtigen lassen, wenn die Bedingungen erfüllt sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **WatchDog** > **Konfiguration**.
2. Wählen Sie den Watchdog aus, den Sie implementieren möchten.
3. Füllen Sie die Felder des Formulars aus.

Formular „Watchdog-Integration“.

Feld	Beschreibung
Name	Name des Watchdogs.
Aktiv	Setzen Sie das Kontrollkästchen auf `true`, um den Watchdog zu aktivieren.
Bedingungstyp	Wählen Sie aus Filter oder Skript aus.
Erweiterte Bedingung	Dieses Feld wird nur angezeigt, wenn Skript als Bedingungstyp ausgewählt wird.
Tabelle	Wählen Sie die Tabelle aus, um die Watchdog-Bedingung auszuführen.
Bedingung	Bedingung zum Auswerten des Watchdogs.
Benachrichtigen	Checkbox, um die Gruppen oder Anwender zu benachrichtigen, wenn die Watchdog-Bedingung erfüllt ist.
Anwender	Liste der Anwender, die benachrichtigt werden sollen, wenn die Watchdog-Bedingung erfüllt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gruppen	Gruppe, die informiert werden soll, wenn die Watchdog-Bedingung erfüllt ist.
Überwachungsprotokoll	
WatchDog	Verweis auf die Watchdog-Tabelle.
Anzahl	Anzahl der Datensätze, die die Watchdog-Kriterien erfüllen.
Notizen	Zusätzliche Hinweise zu den Watchdog-Protokollen.

4. Wählen Sie **Aktualisieren**.

Erweiterte Konfigurationsaufgaben Vulnerability Response.

Die folgenden Setupaufgaben erfordern Programmierkenntnisse oder fortgeschrittene ServiceNow Kenntnisse und werden nicht als Teil der Basiskonfiguration betrachtet.

Möglicherweise möchten Sie diese Aufgaben nur ausführen, wenn Sie über fortgeschrittene Codierungserfahrung verfügen oder über Expertenwissen mit Now Platformverfügen.

Erstellen Sie domänengetrennte Importe für eine Integration

Wenn sich importierte Daten in einer bestimmten Domäne befinden müssen, muss der Benutzer, der für die Ausführung der Integrationen zugewiesen ist, zu dieser Domäne gehören.

Vorbereitungen

Erforderliche Rolle:
import_admin und die Rolle zum Konfigurieren der Integration für Ihre spezifische Integration, z. B. sn_vul.configure_r7_integration oder sn_vul_tenable.configure_integration.

Warum und wann dieser Vorgang ausgeführt wird

Diese Gruppe von Aufgaben erfordert Programmierkenntnisse oder fortgeschrittene ServiceNow -Kenntnisse.

Die Importwarteschlangen enthalten Datenanhänge, die von geplanten Aufgaben (Integrationen) verarbeitet werden. In einer domänengetrennten Umgebung müssen Sie die geplante Aufgabe mit der richtigen Importwarteschlange abgleichen.

Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede von Ihnen erstellte Domäne einen Anwender, und weisen Sie ihn dieser Domäne zu.

   Stellen Sie sich diesen Benutzer als **run_as-** Platzhalter für die Domäne in Ihrer Schwachstellenintegration vor. Er entspricht dem **VR.System** -Benutzer in der globalen Domäne. Dieser Anwender benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   Hinweis:
   Verwenden Sie diesen Anwender nicht für andere Zwecke.

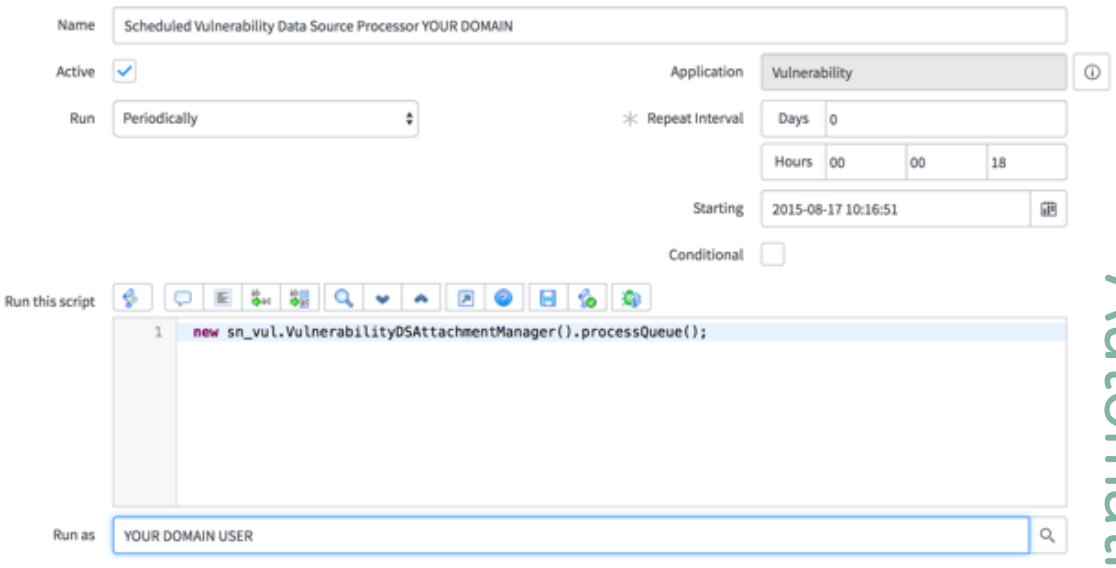
3. Erstellen Sie eine geplante Aufgabe in jeder Domäne.
   Weitere Informationen zu zusätzlichen Vorsichtsmaßnahmen und Einstellungen finden Sie unter Zusätzliche Einstellungen für Domain Separation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.

b. Kopieren Sie **den geplanten Schwachstellen-Datenquellenprozessor** in die Domäne.

c. Um die geplante Aufgabe zu identifizieren, hängen Sie die Domäne an den Namen an.



d. Ändern Sie im Feld **Ausführen als** den Benutzer **run_as** in den Benutzer, den Sie in Schritt 2 erstellt haben.

Ab v20.1 von Vulnerability Responsewerden die folgenden Skriptänderungen mit dem Basissystem geliefert.

4. **Hinweis:**
   Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Benutzerdomäne **run_as** ausgeführt wird.

   Bearbeiten Sie die UI-Aktion „ **Jetzt ausführen“** im Integrationsauftrag **„Integration der Qualys-Host-Erkennung“** , um diesen Codeblock am Anfang der Datei hinzuzufügen.

   Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

5. **Hinweis:**
   Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in der Benutzerdomäne **„run_as“** ausgeführt wird.

   Bearbeiten Sie die Skripteinbindungsmethode **addIntegrationRun** für **VulnerabilityIntegrationUtils**, um den hervorgehobenen Code hinzuzufügen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Bearbeiten Sie die Skripteinbindungsmethode **VulnerabilityIntegrationUtils**, **addProcessRun**, um den hervorgehobenen Code in der folgenden Abbildunghinzuzufügen.
addProcessRun-Code

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

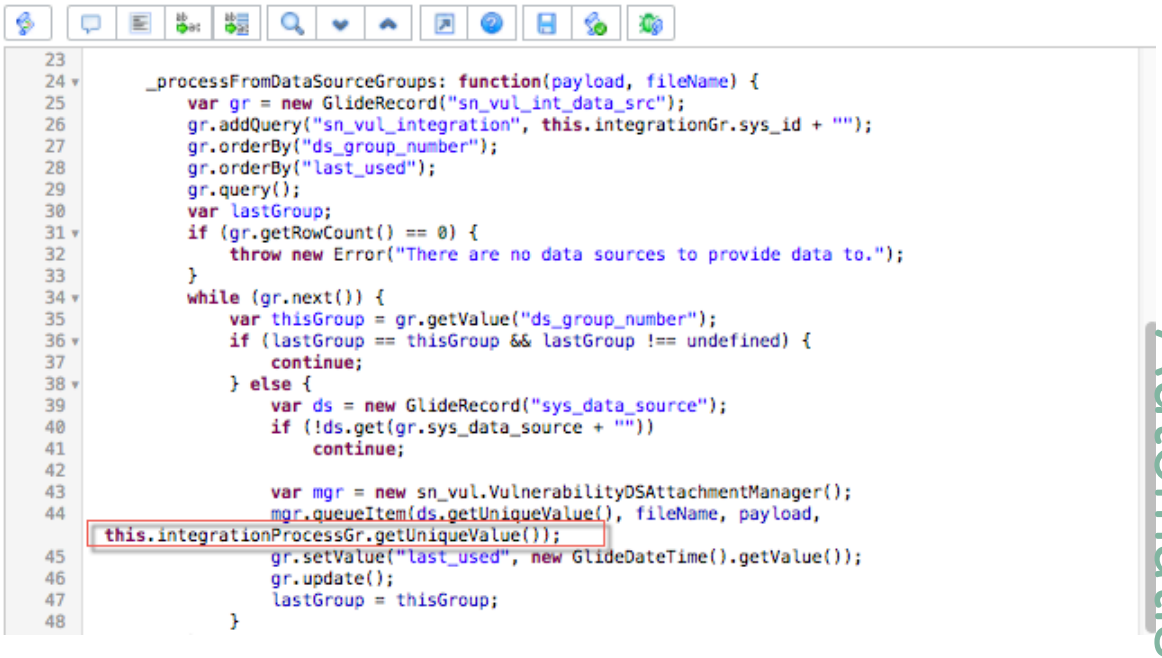
7. Bearbeiten Sie die Skripteinbindungsmethode **VulnerabilityIntegrationUtils(copyProcess)**, um den hervorgehobenen Code in der folgenden Abbildung hinzuzufügen.
kopierenProzesscode

Script

```
_copyProcess: function(intProcGr, isProcessErrored) {
    var copy = new GlideRecord('sn_vul_integration_process');
    copy.initialize();
    copy.setValue('integration_run', intProcGr.getValue('integration_run'));
    copy.setValue('parameters', intProcGr.getValue('parameters'));
    copy.setValue('state', 'new');
    copy.setValue('notes', '');
    copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
    if (isProcessErrored) {
        copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
        var nextRetryDueOn;
        if (intProcGr.getValue('next_retry_due_on') != '')
            nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
        else
            nextRetryDueOn = new GlideDateTime();

        var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
        var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
        nextRetryDueOn.addSeconds(nextRetryDelay * 60);
        if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
            copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
    } else
        copy.setValue('retries', intProcGr.retries + 1);

    copy.insert();
    return copy;
},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

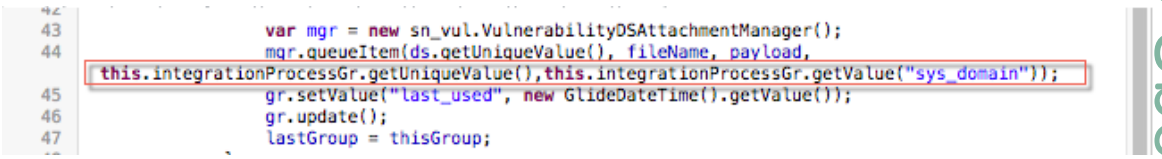
8. Bearbeiten Sie die Skripteinbindungsmethode **„DataSourceVulnReportRefreshProcessor“_processFromDataSourceGroups**, um diesen ursprünglichen Code zu ändern:
Ursprünglicher _processFromDataSourcesGroups-Code



```
23
24      _processFromDataSourceGroups: function(payload, fileName) {
25          var gr = new GlideRecord("sn_vul_int_data_src");
26          gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27          gr.orderBy("ds_group_number");
28          gr.orderBy("last_used");
29          gr.query();
30          var lastGroup;
31          if (gr.getRowCount() == 0) {
32              throw new Error("There are no data sources to provide data to.");
33          }
34          while (gr.next()) {
35              var thisGroup = gr.getValue("ds_group_number");
36              if (lastGroup == thisGroup && lastGroup !== undefined) {
37                  continue;
38              } else {
39                  var ds = new GlideRecord("sys_data_source");
40                  if (!ds.get(gr.sys_data_source + ""))
41                      continue;
42
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
48              }
```

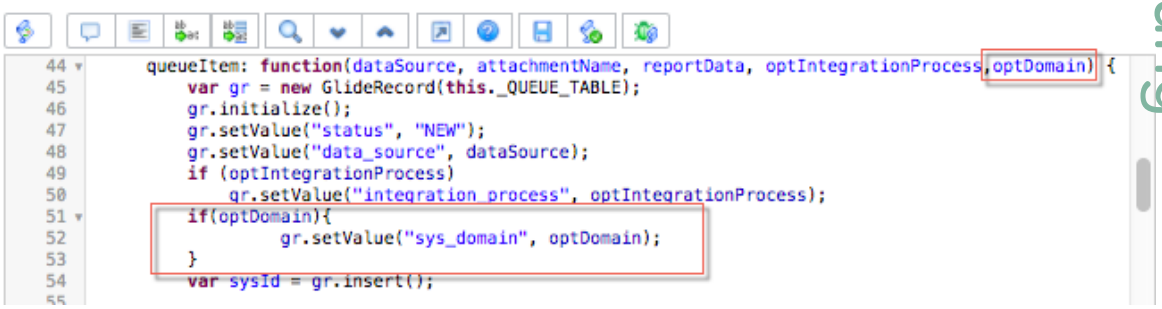
An:

_processFromDataSourcesGroups-Code wurde bearbeitet



```
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
```

9. Bearbeiten Sie die Skripteinbindungsmethode **VulnerabilityDSAttachmentManager**, **queueItem**, um die folgenden hervorgehobenen Codeblöcke hinzuzufügen
queueItem



```
44      queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
45          var gr = new GlideRecord(this._QUEUE_TABLE);
46          gr.initialize();
47          gr.setValue("status", "NEW");
48          gr.setValue("data_source", dataSource);
49          if (optIntegrationProcess)
50              gr.setValue("integration_process", optIntegrationProcess);
51          if(optDomain){
52                  gr.setValue("sys_domain", optDomain);
53          }
54          var sysId = gr.insert();
```

_getNext

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
156     _getNext: function() {
157         // First go through the retries, if any
158         var gUser = new GlideRecord("sys_user");
159         gUser.get(gs.getUserID());
160         var sysDomainUser = gUser.getValue("sys_domain");
161         var gr = new GlideRecord(this._QUEUE_TABLE);
162         gr.addQuery("status", "RETRY");
163         gr.addQuery("sys_domain", sysDomainUser);
164         gr.orderBy("queued_on");
165         gr.query();
166         if (gr.next()) {
167             return gr;
168         }
169
170         // Then handle the regular queued items
171         gr = new GlideRecord(this._QUEUE_TABLE);
172         gr.addQuery("status", "QUEUED");
173         gr.orderBy("queued_on");
174         gr.addQuery("sys_domain", sysDomainUser);
175         gr.query();
176         if (gr.next()) {
177             return gr;
178         }
179
```

Funktion „_processQueueEntry“.

```
182     _processQueueEntry: function(entry) {
183         var schedGrId = this._getScheduledImportSet(entry.data_source);
184         if (gs.nil(schedGrId)) {
185             return;
186         }
187
188         var dataSourceGr = new GlideRecord("sys_data_source");
189         if (!dataSourceGr.get(entry.data_source)) {
190             gs.warn("Non existent data source - marking as complete");
191             entry.setValue("status", "COMPLETE");
192             entry.setValue("processing_notes", "Data source does not exist, could not process.");
193             entry.update();
194             return;
195         }
196
197         try {
198             this._deleteDataSourceAttachments(entry.data_source);
199             if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
200                 gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
201                 throw "Attachments not deleted";
202             }
203             var attachmentApi = new GlideSysAttachment();
204             attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
205             var schedGr = new GlideRecord("scheduled_import_set");
206             schedGr.get(schedGrId);
207             schedGr.setValue("data_source", entry.data_source);
208             schedGr.setValue("run_as", gs.getUserID());
209             schedGr.update();
```

Jetzt sind Sie bereit für domänengetrennte Importe.

Hinweis:
Wenn Sie mehrere Bereitstellungen einer Vulnerability Response - oder Application Vulnerability Response -Integration haben, wiederholen Sie diesen Vorgang für jede Bereitstellung.

Erstellen und unterstützen Sie mehrere Domänen im Framework für Hintergrundaufträge

Hintergrundaufträge in Vulnerability Response-Produkten sind so konzipiert, dass sie über einen längeren Zeitraum ausgeführt werden, um mehrere Prozesse für Ihre Datensätze auszuführen. Im Lieferumfang des Basissystems sind Hintergrundauftragsprozessoren enthalten, die über den Systembenutzer ausgeführt werden und Datensätze in der globalen Domäne erstellen.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**.
2. Erstellen Sie eine Domäne.

   Weitere Informationen zum Erstellen einer Domäne finden Sie unter Create a domain .

   Erstellen Sie für jede erstellte Domäne einen Anwender, und weisen Sie ihn der Domäne zu. Angenommen, dieser Benutzer ist ein run_as-Platzhalter für die Domäne. Dies entspricht dem VR.System-Benutzer in der globalen Domäne. Dieser Anwender benötigt Zugriff auf Schwachstellendaten.

3. Ändern Sie die run_as der geplanten Aufgaben `Scheduled Background Job Manager`, und `Close the parent background job`.

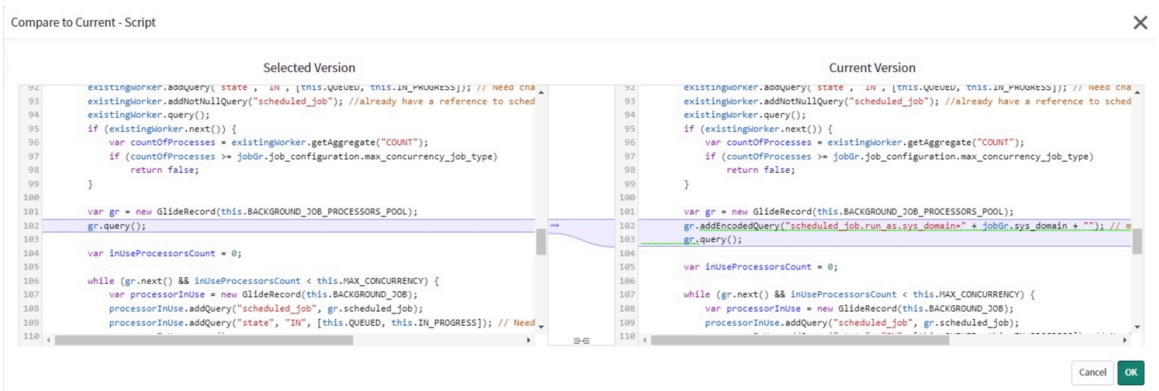
   Wenn Sie mehrere Domänen erstellt haben, duplizieren Sie diesen Auftrag, und ändern Sie den Benutzer „run_as“ entsprechend. Möglicherweise möchten Sie auch eine Kopie der vorherigen Aufträge mit dem Benutzer „run_as“ der globalen Domäne in einem inaktiven Modus beibehalten.

   Im Basissystem sind zehn Prozessoraufträge (z. B. `Background job processor 10`) enthalten. Ändern Sie die Ausführung dieser Aufträge in den domänengetrennten Benutzer. Wenn mehrere Domänen vorhanden sind, genügen zwei Aufträge pro Domäne, diese Aufträge können bei Bedarf jedoch auch dupliziert werden. Behalten Sie zwei Prozessoraufträge mit dem Benutzer „run_as“ in der globalen Domäne bei.

   Ab v20.0 von Vulnerability Responsewerden die folgenden Skriptänderungen mit dem Basissystem geliefert.

4. Ändern Sie die Skripteinbindung `BackgroundJobManager`, und fügen Sie die folgende Zeile hinzu (siehe folgende Abbildung).

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```



Hinweis:
Lösen Sie bei Bedarf die erneute Anwendung von Regeln aus der richtigen Domäne aus.

Erstellt eine Vulnerability Response-CI-Suchregel

Das Modul **CI-Suchregeln** enthält Regeln, mit denen der übereinstimmende Datensatz für Hostinformationen gefunden wird, die während des Imports von Drittpartei-Schwachstellenintegrationen empfangen wurden. Die Hostinformationen werden mit den erkannten Elementen, den nicht abgeglichenen Klassen von Konfigurationselementen und dem Configuration Management Database (CMDB)abgeglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Das Erstellen von CI-Suchregeln erfordert fortgeschrittene Kenntnisse ServiceNow von und Vulnerability Response. Anstatt eine der vorhandenen Suchregeln zu ändern, sollten Sie sie kopieren und die Kopie ändern. Wenn Sie zufrieden sind, dass die neue Regel das bewirkt, was Sie möchten, deaktivieren Sie die ursprüngliche.

Hinweis:
Einmal entfernte Regeln können nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **CI-Suchregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „CI-Suchregel“.

Feld	Beschreibung
Name	Name der Regel.
Suchmethode	Für die Übereinstimmung verwendete Methode. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Skript**: Vorgefertigt (IP-Adresse, DNS-Name usw.) oder anwenderdefiniertes Skript. ○ **Feldabstimmung**: Suchen Sie in der Tabelle oder dem Feld in der CMDB.
Typ	Typ, der mit der **Skriptsuchmethode**verwendet wird.
Bestellung	Rangfolge für die Regel. Die Regeln mit der niedrigsten Ordnungszahl werden zuerst ausgewertet.
Aktiv	Checkbox, um festzulegen, ob die Regel aktiv oder deaktiviert ist.
Quelle	Quelle, die als Eingabe für diese Regel verwendet wird.
Quellenfeld	Quellfeld, das als Eingabe für diese Regel verwendet wird. Wählen Sie ein beliebiges Feld aus, es wird jedoch als -Zeichenfolgenwert behandelt.
Bedingung	Bedingung, auf deren Grundlage die CI-Suchregel angewendet wird. Diese Bedingung hängt vom Attribut des Drittanbieterscanners ab. **Hinweis:** Das Asset-Attribut ist Teil der Nutzlast. Sie wird vom Scanner der Drittpartei empfangen. Nutzlastbeispiele finden Sie in der Tabelle „Erkannte Elemente“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

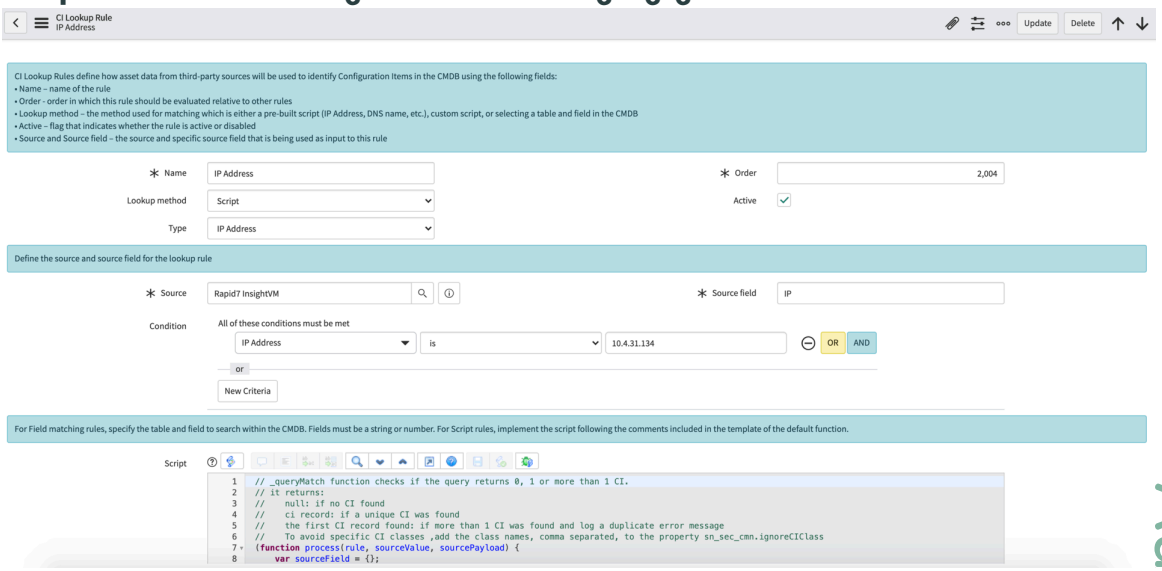
Feld	Beschreibung
Skript	Bearbeitbares Beispielskript, basierend auf dem **Typ**, wird angezeigt. Implementieren Sie das anwenderdefinierte Skript nach den Kommentaren, die in der Vorlage der Standardfunktion enthalten sind. **Hinweis:** Die Funktion process besitzt drei Parameter: `rule`, `sourceValue`und `sourcePayload`
Tabelle durchsuchen	Tabelle für die Suche in der CMDB. Wird mit **der Suchmethode**für die Feldübereinstimmung verwendet.
Feld durchsuchen	Feld, das Informationen enthält, die zum Suchen eines CI verwendet werden können. Wird mit der **Suchmethode**für übereinstimmende Felder verwendet. Dieses Feld kann sich im CI-Datensatz oder in einem zugehörigen Datensatz wie einem Netzwerkadapter befinden.

4. Klicken Sie auf **Absenden**.

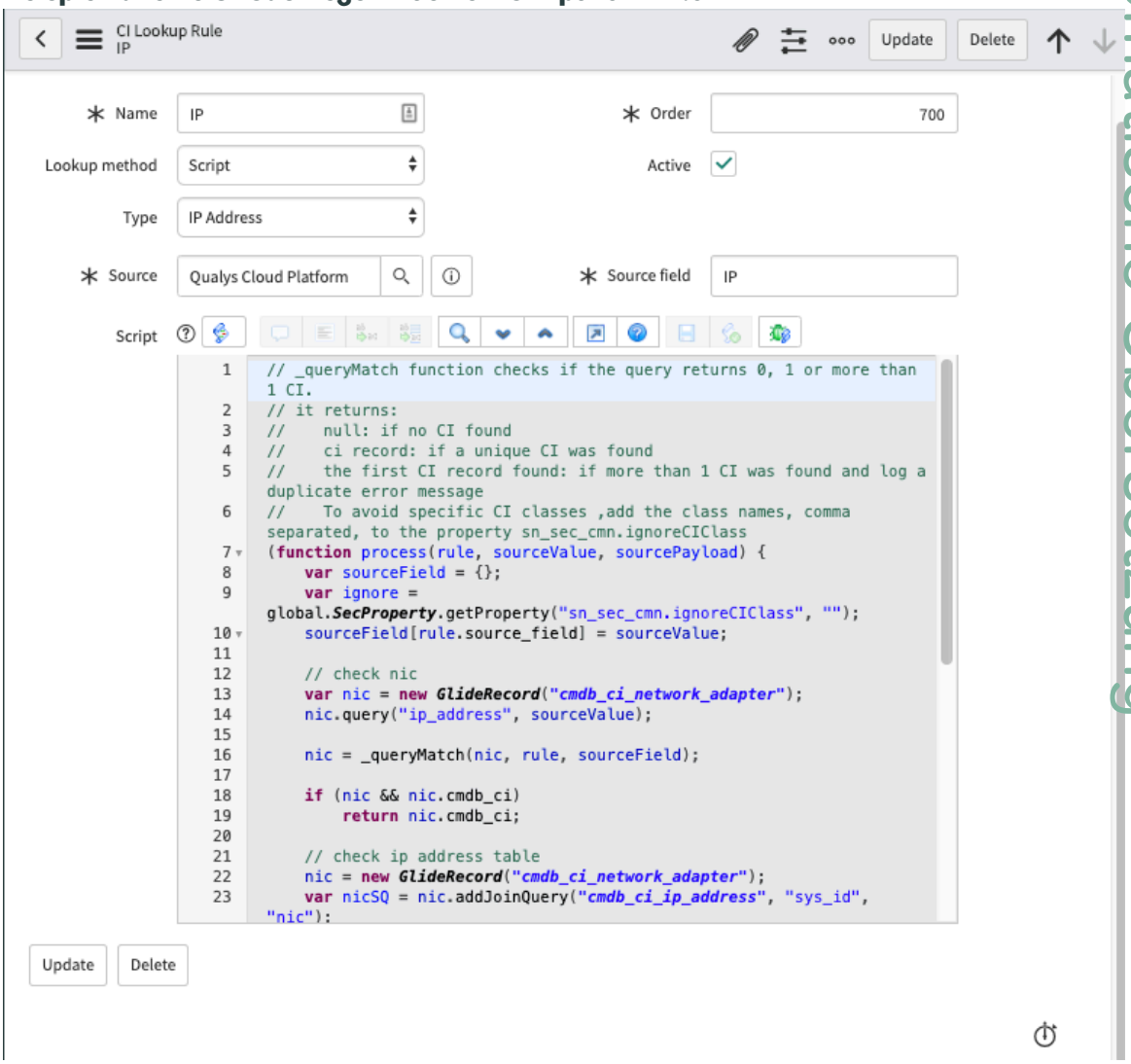
Weitere Informationen zur Implementierung von CI-Suchregeln finden Sie unter Schritte zum Verhindern von doppelten oder verwaisten Datensätzen nach dem Ausführen von Vulnerability Response CI-Suchregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine CI-Suchregel mit einem Bedingungsgenerator für V12.0



Beispiel für eine CI-Suchregel mit einem Skript vor V12.0



Automatische Übersetzung

Zugehörige Informationen

Vulnerability Response Formularfelder für angreifbare Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Klassen ignorieren

Um beim Ausführen von CI-Suchregeln einige Klassen von Konfigurationselementen (CI) zu ignorieren, z. B. das Lastenausgleichsmodul [cmdb_ci_lb], legen Sie die Systemeigenschaft **„ignoreCIClass** “ [*sn_sec_cmn.ignoreCIClass*] fest.

Vorbereitungen

Erforderliche Rolle: Administrator

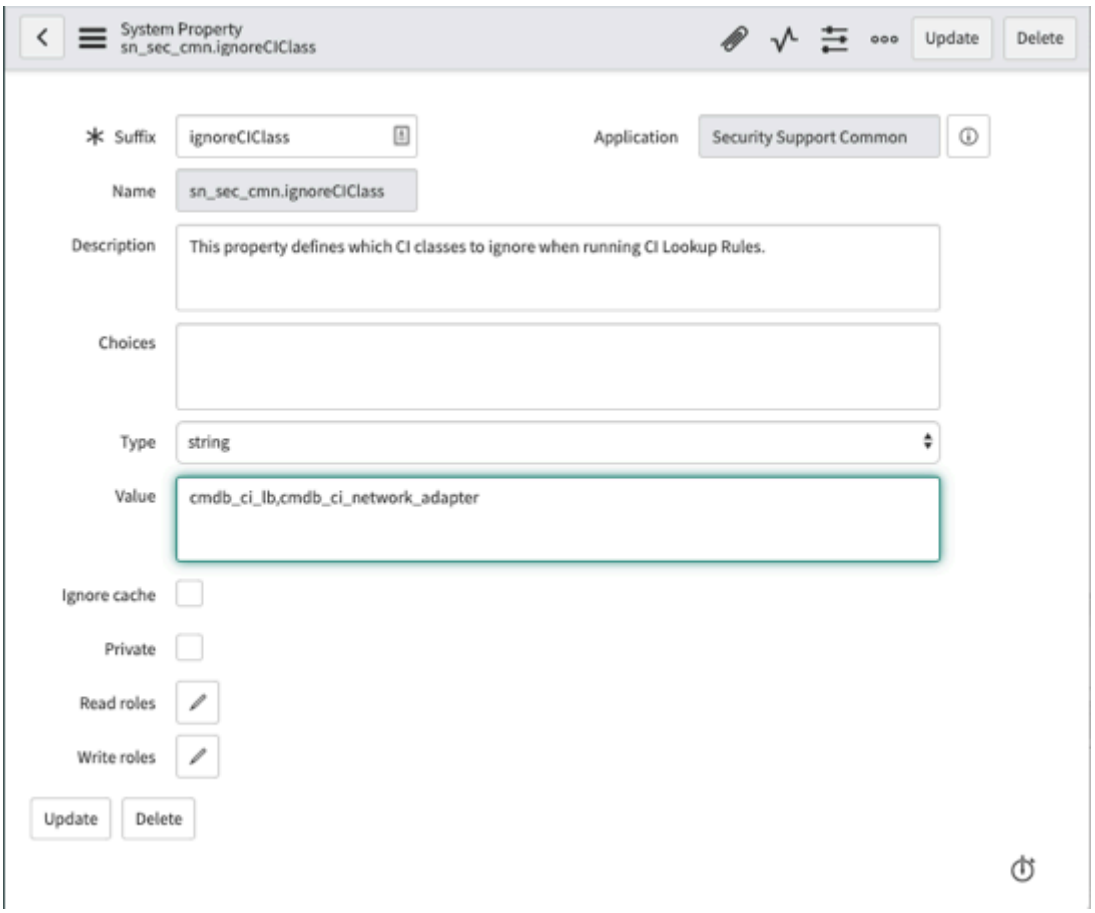
Hinweis:

Die Systemeigenschaft **„ignoreCIClass** “ ist ab Vulnerability Response v9.0 verfügbar. Die Eigenschaftsfunktionalität ist jedoch beim Upgrade von einer früheren Version nicht verfügbar.

Wenn Sie ein Upgrade von einer Anwendung Security Operations vor Version 9.0 durchgeführt haben, finden Sie unter KB0788209 Anweisungen zum Aktivieren dieser Funktionalität.

Prozedur

1. Geben Sie in der linken Navigationsleiste sys_properties.list ein.
2. Klicken Sie auf **Eingeben**.
3. Geben Sie im Menü **Suchen** unter **Name**sn_sec_cmn.ignoreCIClassein.
4. Geben Sie im Textfeld **Wert** die auszuschließenden CI-Klassen in einer durch Kommas getrennten Liste ein.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Aktualisieren**.
   Diese Liste wird während des nächsten Imports von CI-Suchregeln verwendet. Während des Imports erstellte angreifbare Elemente sind keinem CI eines Typs zugeordnet, der im Feld **Wert** der Systemeigenschaft sn_sec_cmn.ignoreCIClass aufgeführt ist.

Filtern Sie stillgelegte CIs

Filtert außer Betrieb genommene Configuration Items (CIs) während der Ausführung der CI-Suchregeln. Um außer Betrieb genommene CIs bei der Ausführung der CMDB-CI-Suchregeln für Security Operations zu filtern, legen Sie die Systemeigenschaft **filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] auf „true“ fest.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der Standardwert der Systemeigenschaft ist true. Diese Eigenschaft gilt nur für CI-Suchregeln in Vulnerability Response und hat keine Auswirkungen auf die IRE-Suchlogik.

Prozedur

1. Geben Sie in der linken Navigationsleiste sys_properties.list ein.
2. Drücken Sie **die Eingabetaste**.
3. Geben Sie im Menü **Suchen** unter **Name**sn_sec_cmn.filterOutDecommissionedCI ein, um die außer Betrieb genommenen CIs zu filtern.
4. Geben Sie im Textfeld **Wert** den Wert true oder false ein.
   Der Standardwert ist „true“.
5. Wählen Sie **Aktualisieren**.
   Dieser Wert wird während des nächsten Imports von CI-Suchregeln verwendet. Die Systemeigenschaft sn_sec_cmn.filterOutDecommissionedCI filtert CIs heraus, die die folgenden Bedingungen erfüllen, während die Suchregeln ausgeführt werden.

```
_isCIDecommissioned: function(gr, filterDecommissionCi) {
      var install_status = false;
      var life_cycle_stage_status = false;
      // check for property
      if (filterDecommissionCi == "true") {
         if (gr.isValidField("install_status"))
            install_status = gr.install_status == 7;
         if (gr.isValidField("life_cycle_stage_status"))
            life_cycle_stage_status = gr.life_cycle_stage_status == "Retired";
      }
      return install_status || life_cycle_stage_status;
```

CIs automatisch heraufstufen

Bearbeiten Sie die JSON-Zeichenfolge in der Systemeigenschaft **autoHeraufstufenFields** [**sn_sec_cmn.autoHeraufstufen**], damit Ihre Suchregeln für Konfigurationselemente (Configuration Item, CI) alle CMDB-CIs von Security Operations automatisch zu übereinstimmenden Einträgen in der Tabelle [cmdb_ci] heraufstufen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der Systemeigenschaftstyp ist „Zeichenfolge“ und erfordert die Eingabe einer JSON-Zeichenfolge. Diese Eigenschaft ist standardmäßig aktiviert und stuft übereinstimmende CIs hoch, während die CI-Suchregeln ausgeführt werden.

Anwenderdefinierte Suchskripts geben möglicherweise untergeordnete Tabellendatensätze aus dem Skript zurück. Für diese Eigenschaft verwendet die Funktion *`_autoPromoteCI`* in *`CIIdentify Script Include`* das vom Suchskript zurückgegebene CI, durchläuft automatisch die Beziehungen, um zum Eintrag *`cmdb_ci`* zu gelangen und ihn zurückzugeben.

Um die Logik für die automatische Heraufstufung zu überschreiben, d. h. um neue CI-Klassen hinzuzufügen oder zu aktualisieren, fügen Sie das JSON-Objekt im Feld Wert in der Systemeigenschaft [**sn_sec_cmn.autoHeraufstufenFields**] hinzu.

Prozedur

1. Geben Sie in der linken Navigationsleiste sys_properties.list ein.
2. Drücken Sie **die Eingabetaste**.
3. Suchen Sie die Systemeigenschaft [**sn_sec_cmn.autoHeraufstufenFields**], und wählen Sie den Datensatz aus, um ihn zu öffnen.

   Standardzeichenfolge:

   ```
   {
    "dscy_switchport":"cmdb_ci",
    "cmdb_ci_network_adapter":"cmdb_ci",
    "cmdb_ci_nic":"cmdb_ci",
    "cmdb_ci_ip_address":"nic"
   }
   ```

4. Bearbeiten Sie im Textfeld **Wert** die Zeichenfolge im Standard-Paarungsformat.
5. Wählen Sie **Aktualisieren**.
   Dieser Wert wird während des nächsten Imports von CI-Suchregeln verwendet.

Konfigurieren Sie den Schlüssel des angreifbaren Elements

Konfigurieren Sie die Granularität des Schlüssels für angreifbare Elemente in der Anwendung Vulnerability Response, um zu definieren, was ein angreifbares Element in Ihrer Organisation angreifbar macht.

Vorbereitungen

Erforderliche Rolle: Administrator

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Schlüsselbegriffe:

Konfigurationselement bzw. Configuration Item (CI)

Ein vorhandenes Asset, das in Ihrer CMDB aufgeführt ist.

Schwachstelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Datensatz einer bekannten Schwachstelle, der aus dem National Institute of Standards and Technology (NIST), der National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CWE) oder Drittanbieterintegrationen mit Vulnerability Responseimportiert wird.

Angreifbares Element

Ein angreifbares Element wird erstellt, wenn eine importierte Schwachstelle mit einem Konfigurationselement in Ihrer CMDB übereinstimmt.

Erkennung

Ein einzelnes, eindeutiges Auftreten einer Schwachstelle, das von den Scannern Ihrer Drittanbieterintegrationen gemeldet wird. Erkennungen werden importiert und sowohl im Erkennungsdatensatz als auch im Datensatz für angreifbare Elemente in Ihrer -Instanz angezeigt. Wird auch als Erkennung eines angreifbaren Elements bezeichnet.

Standardmäßig ist ein angreifbares Element eine eindeutige Kombination aus einem Configuration Item (CI), einer Schwachstelle und einer Integrationsinstanz. Um angreifbare Elemente mit größerer Granularität zu erstellen, fügen Sie eindeutige Ports aus Erkennungen von angreifbaren Elementen hinzu, damit Sie die Nachbesserung von Schwachstellen auf der Ebene verwalten können, die für Ihre Organisation am effektivsten ist.

Wenn Sie angreifbare Elemente mit höherer Granularität erstellen möchten, konfigurieren Sie den Schlüssel des angreifbaren Elements so, dass er den Port enthält. Wenn „Port einbeziehen“ aktiviert ist, werden angreifbare Elemente von eindeutigen Ports aus Erkennungen angreifbarer Elemente erstellt.

Ab Vulnerability Response V17.1 können Sie Rapid7-Schwachstellen identifizieren und beheben, indem Sie Nachweise als VI-Schlüssel hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Nachweises zu Rapid7-Schlüsseln für angreifbare Elemente.

Wählen Sie eine Option aus der folgenden Tabelle aus, um die Option Port einbeziehen zu aktivieren.

Drei Szenarien zum erstmaligen Aktivieren der Option „Port einbeziehen“ mit der VI-Taste

Wenn...	Beschreibung
Mindestens eine der folgenden Bedingungen ist zutreffend: • Sie führen ein Upgrade von einer Version Vulnerability Response vor v10.0 durch, die keine Erkennung von angreifbaren Elementen unterstützt hat. • Sie sind ein neuer Kunde und haben keine Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen angreifbarer Elemente) in Ihrer Instanz Now Platform®. • Sie haben bereits alle Datensätze für angreifbare Elemente und zugehörige Daten in Ihrer Instanz gelöscht, und Sie sind bereit, alle Ihre Vulnerability Response-Daten zu erstellen. Beginnen Sie mit einem	Aktivieren Sie Port einbeziehen. Nachdem „Port einschließen“ aktiviert ist, erstellen importierte Erkennungen ab dem nächsten Import angreifbare Elemente, die VIs enthalten, die sich durch den eindeutigen Port unterscheiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Drei Szenarien zum erstmaligen Aktivieren der Option „Port einbeziehen“ mit der VI-Taste (Fortsetzung)

Wenn...	Beschreibung
neuen Import, um VIs einzubeziehen, die sich durch einen eindeutigen Port unterscheiden.	
Beide Bedingungen sind wahr: • Sie haben v10.0 oder höher von Vulnerability Response und verfügen über vorhandene Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen angreifbarer Elemente) in Ihrer Instanz, die Sie beibehalten möchten. • Sie möchten mit der Erstellung neuer angreifbarer Elemente beginnen, um VIs einzuschließen, die sich durch einen eindeutigen Port unterscheiden.	Aktivieren Sie Port einbeziehen. Ihre vorhandenen Erkennungen und die zugehörigen angreifbaren Elemente bleiben erhalten. Wenn „Port einschließen“ aktiviert ist, erstellen neue Erkennungen ab dem nächsten Import neue angreifbare Elemente, die VIs enthalten, die sich durch einen eindeutigen Port unterscheiden.
Beide Bedingungen sind wahr: • Sie haben v10.0 oder höher von Vulnerability Response. • Sie verfügen über vorhandene Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen von angreifbaren Elementen), möchten Ihre vorhandenen Daten jedoch nicht beibehalten, da Sie es vorziehen, Ihre Schwachstellendaten ausgehend von einem neuen Import zu erstellen, und VIs einschließen möchten, die sich durch einen eindeutigen Port unterscheiden.	1. Löschen Sie alle Datensätze zu angreifbaren Elementen und zugehörigen Daten aus Ihrer Instanz. 2. Aktivieren Sie Port einbeziehen. Wenn „Port einschließen“ aktiviert ist, erstellen neue Erkennungen ab dem nächsten Import neue angreifbare Elemente, die VIs enthalten, die sich durch einen eindeutigen Port unterscheiden.

Hinweis:

Wenn die Option „Port einbeziehen“ aktiviert ist, können für ein Konfigurationselement mehr als ein angreifbares Element erstellt werden. Wenn beispielsweise eine Schwachstelle für zwei Ports eines Konfigurationselements, die Ports 80 und 443, besteht, werden zwei eindeutige VIs erstellt, eines für jeden Port ab dem nächsten Import.

Hinweis:

Stellen Sie sicher, dass Sie VIs erstellen, um VIs nach eindeutigen Ports einzubeziehen, bevor Sie diese Funktion aktivieren. Sobald Sie den VI-Schlüssel zum Einbeziehen des Ports aktiviert haben, müssen Sie zuerst Ihre Vulnerability Response-Daten löschen, bevor Sie „Port einbeziehen“ deaktivieren und zum Importieren von Schwachstellendaten mit der standardmäßigen VI-Schlüsselgranularität zurückkehren können, d. h. wobei VIs für den Port erstellt, aber nicht nach unterschieden werden Eindeutiger Port Weitere Informationen zum Löschen von Schwachstellendaten finden Sie unter Löschen Sie alle Datensätze zu angreifbaren Elementen und zugehörigen Daten in Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.

   Das Feld Zuletzt aktualisiert zeigt das Datum an, an dem die VI-Taste zuletzt konfiguriert wurde.

2. Klicken Sie auf das Kontrollkästchen Port einbeziehen, um ihn zu aktivieren.

3. Klicken Sie auf **Speichern**.
   Das Dialogfeld Bestätigung wird angezeigt.

   Wenn Sie in Ihrer Instanz keine Datensätze zur Erkennung angreifbarer Elemente haben, werden ab dem nächsten Import sowohl Erkennungen von angreifbaren Elementen als auch angreifbare Elemente von einem eindeutigen Port erstellt.

   Wenn Sie über vorhandene Erkennungen angreifbarer Elemente und angreifbare Elemente in Ihrer Instanz verfügen, werden vorhandene Erkennungen und zugehörige angreifbare Elemente beibehalten. Neue Erkennungen erstellen ab dem nächsten Import neue angreifbare Elemente, die VIs enthalten, die sich durch einen eindeutigen Port unterscheiden.

Nächste Maßnahme

Verifiziert, dass angreifbare Elemente nach Port in den Datensätzen „Erkennung angreifbarer Elemente“ und „Angreifbare Elemente“ angezeigt werden. Weitere Informationen finden Sie unter Zeigen Sie Vulnerability Response Erkennungsdaten für angreifbare Elemente an.

Hinzufügen eines Nachweises zu Rapid7-Schlüsseln für angreifbare Elemente

Fügen Sie den Nachweis als angreifbaren Element(VI)-Schlüssel für die Rapid7 VIs hinzu. Das Einschließen des Nachweises für bestimmte Schwachstellen ermöglicht es der Scannerintegration Rapid7, VIs für jeden von Rapid7empfangenen Nachweis zu erstellen.

Ein VI-Schlüssel ist die Kombination aus Schwachstelle, Configuration Item (CI) und Integrationsinstanz. Durch die Aufteilung von Erkennungen in verschiedene VIs basierend auf Nachweisen entstehen mehrere VIs. Sie können die Schwachstellen den entsprechenden Korrekturbesitzern zuweisen.

Beispielsweise kann es zwei Erkennungen mit derselben Schwachstelle und demselben CI, aber unterschiedlichen Nachweisen geben, die zur Erstellung desselben VI führen. Ab Vulnerability Response V17.1 können Sie Schwachstellen durch Hinzufügen von Nachweisen als VI-Schlüssel identifizieren und beheben.

Sie können den Nachweis wie folgt als VI-Schlüssel hinzufügen:

Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren** und wählen Sie die Option zum Einschließen eines Nachweises.

Anwendungsfall: Aufnahme von Nachweisen in VI-Schlüssel für vorhandene AEs oder Aufteilung vorhandener AEs basierend auf dem Erkennungsnachweis

Um VIs basierend auf Nachweisen zu erstellen, können Sie die R7 Log4J-Schwachstellen verwenden. Sie können beispielsweise eine der mehreren R7-log4j-Schwachstellen verwenden, z. B. R7-apache-log4j-core-cve-2021-44228, R7-amazon_linux-cve-2021-44228oder R7-amazon-linux-ami-2- cve-2021-44228.

Wenn alle Erkennungen in einem VI denselben Nachweis haben, wird das vorhandene VI aktualisiert und enthält „Nachweis im VI-Schlüssel (external_id)“. Wenn mehrere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennungen mit unterschiedlichen Nachweisen vorhanden sind, wird das vorhandene AE geschlossen. Die Erkennungen werden mit „Nachweis im VI-Schlüssel (external_id)“ auf die neuen VIs aufgeteilt.

Hinweis:

Wenn Sie die Schwachstellen-ID angeben, werden die vorhandenen VIs basierend auf dem Nachweis aufgeteilt. Die neuen Schwachstellen für diese Schwachstellen-ID haben auch einen Nachweis als einen der VI-Schlüssel.

Löschen Sie alle Datensätze zu angreifbaren Elementen und zugehörigen Daten in Vulnerability Response

Entfernen Sie alle Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen angreifbarer Elemente) und zugehörige Daten und Datensätze dauerhaft aus der Anwendung Vulnerability Response in Ihrer Instanz Now Platform®.

Vorbereitungen

Löschen Sie Datensätze zur Erkennung angreifbarer Elemente, angreifbare Elemente, Schwachstellen-Gruppen und alle zugehörigen Datensätze in der Anwendung Vulnerability Response aus Ihrer -Instanz. Verwenden Sie diesen Prozess, um Ihre Instanz zu bereinigen, um Daten aus Ihren Drittanbieterintegrationen neu zu importieren oder als Voraussetzung dafür, die Schlüsselkonfiguration des angreifbaren Elements (VI) auf die Standardeinstellung zurückzusetzen. Weitere Informationen zum Konfigurieren der VI-Taste finden Sie unter Konfigurieren Sie den Schlüssel des angreifbaren Elements.

Hinweis:

Mit dieser Aktion werden alle Datensätze zu angreifbaren Elementen und alle zugehörigen Daten aus Ihrer Instanz gelöscht. Diese gelöschten Daten können nicht abgerufen werden. Außerdem müssen Sie den Datenimport anhalten und Ihre aktiven Drittanbieterintegrationen mit Vulnerability Responsedeaktivieren.

Das Löschen der Daten Ihrer angreifbaren Elemente mit diesem Prozess ist erforderlich, bevor die VI-Schlüsselkonfiguration geändert wird. Durch das Entfernen aller Daten wird sichergestellt, dass alle Ihre angreifbaren Elemente und Erkennungen von angreifbaren Elementen zugeordnet und mit den neuesten Daten aktualisiert werden, beginnend mit dem nächsten Import.

Stellen Sie sicher, dass die folgenden Bedingungen zutreffen, bevor Sie Ihre Daten löschen:

- Sie haben v10.0 oder höher von Vulnerability Response installiert. Weitere Informationen finden Sie unter Vulnerability Response Erkennungen von angreifbaren Elementen durch Integrationen von Drittparteien.
- Sie möchten „Port einbeziehen“ deaktivieren und die VI-Schlüsselkonfiguration auf ihre Standardeinstellung zurücksetzen.
- Sie haben vorhandene angreifbare Elemente und Erkennungen angreifbarer Elemente, möchten oder müssen sie jedoch nicht aktualisieren und beibehalten.
- Sie haben entschieden, dass Sie alle vorhandenen Vulnerability Response-Daten und zugehörigen Datensätze entfernen möchten, um Ihre Instanz zu bereinigen.

Erforderliche Rolle: sn_vul.vulnerability_admin

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellen-Integrationen**.
2. Zeichnen Sie alle angezeigten aktiven Integrationen auf.

   Alle aktiven Integrationen, die mit geplanten Aufgaben aufgeführt sind, werden vor dem Löschen aller Ihrer angreifbaren Elemente und zugehörigen Daten deaktiviert, sodass während der Datenentfernung keine neuen Daten importiert werden. Wenn Sie diese Liste aufzeichnen, können Sie Ihre Integrationen nach Abschluss des Löschvorgangs aktivieren.
3. Lesen Sie den Artikel How to delete Existing Vulnerability Response Data for Reimport (Wie sich vorhandene Vulnerability Response-Daten für den erneuten Import löschen) in der HI Knowledge Base.
4. Wenn eine Warnmeldung angezeigt wird, die Sie daran hindert, in die Spalte „Aktiv“ zu schreiben, führen Sie die folgenden Schritte aus, um aktive Integrationen zu deaktivieren.

   a. Klicken Sie in der Spalte Name auf ein Element, um den Datensatz zu öffnen.

   b. Wenn Sie das Kontrollkästchen Aktiv nicht bearbeiten können, klicken Sie auf den Link **hier,** um den Datensatz zu bearbeiten.

   c. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu deaktivieren und die nächste geplante Aufgabe abzubrechen.

   d. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Liste zurückzukehren.

   e. Vergewissern Sie sich, dass Sie alle aktiven Integrationen in der Liste „Integrationen“ deaktiviert haben. Nachdem Sie eine Integration deaktiviert haben, wird sie nicht mehr in der Liste der aktiven Integrationen angezeigt. Um eine Liste inaktiver Integrationen anzuzeigen und alle Integrationen zu suchen, die Sie deaktiviert haben, nachdem Sie alle Ihre Schwachstellendaten gelöscht haben, geben Sie in der Spalte Aktiv oben =falseein.
5. Fahren Sie mit den Schritten im KB-Artikel zum Löschen Ihrer vorhandenen Schwachstellendaten fort.
6. Nachdem Sie bestätigt haben, dass alle Daten erfolgreich gelöscht wurden, navigieren Sie zu **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.
7. Im Formular:
   - Wenn Sie Daten gelöscht haben, weil Sie es vorziehen, Ihre Schwachstellendaten so zu erstellen, dass ein Port aus einem neuen Import aufgenommen wird, aktivieren Sie Port einbeziehen, und klicken Sie auf **Speichern**.
   - Wenn Sie Daten gelöscht haben, weil Sie den VI-Schlüssel auf seine Standardeinstellung zurücksetzen möchten, deaktivieren Sie Port einbeziehen, und klicken Sie auf **Speichern**.

   Weitere Informationen finden Sie unter Konfigurieren Sie den Schlüssel des angreifbaren Elements.

Filtern in Vulnerability Response

Regeln für Korrekturaufgaben, Rechner und Zuweisungsregeln verwenden während des Imports Bedingungen, die mit dem **Bedingungsgenerator**erstellt wurden. Änderungen an

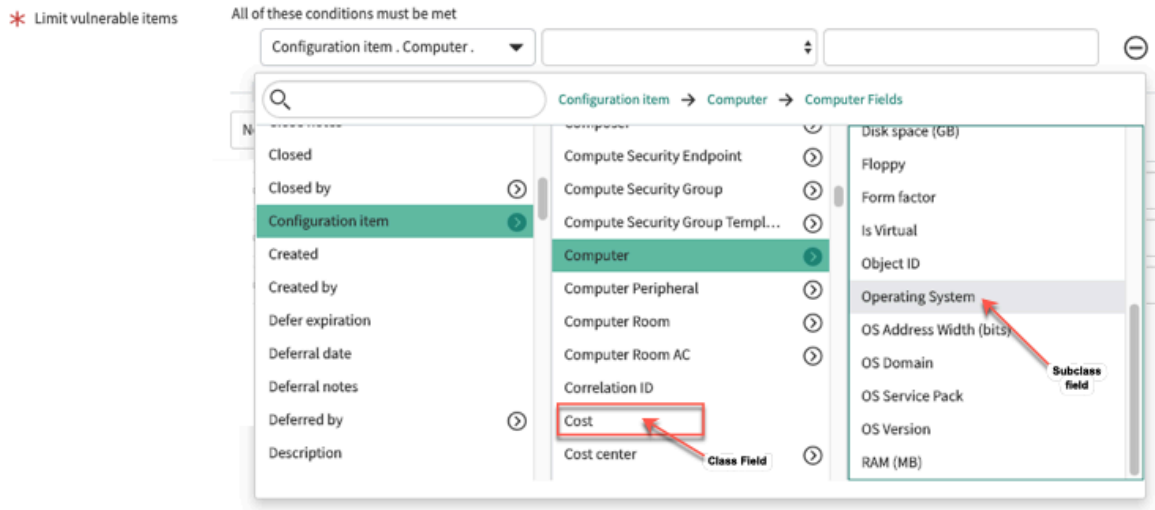
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Kriterien können sich auf die Leistung auswirken, da jeder Datensatz mit diesen Filtern ausgewertet wird.

Die im Lieferumfang des Basissystems enthaltenen Regeln und Rechner sind auf Leistung optimiert. Das Bearbeiten oder Erstellen von Regeln oder Rechnern erfordert Sorgfalt und erfordert möglicherweise sowohl ServiceNow - als auch Vulnerability Response -Kenntnisse.

Vermeiden Sie die Filterung auf Grundlage von Unterklassenfeldern

Einige Tabellen unterstützen Erweiterungen. Ein Beispiel hierfür ist die CMDB-CI-Tabelle [cmdb_ci]. Tabellen wie „cmdb_ci_hardware“ und „cmdb_ci_computer“ erweitern diese Tabelle. Wenn Sie basierend auf einem Feld filtern, das sich nicht in der übergeordneten Tabelle befindet, kann die Erstellung und Auswertung dieses Filters teuer sein.



Filtern Sie beispielsweise nach **Konfigurationselement** > **Kosten** würde die Leistung nicht beeinträchtigen, da **Kosten** ein Klassenfeld und kein Unterklassenfeld von **Configuration Item**ist.

Konfigurationselement > **Computer**ist jedoch eine Unterklasse, die einen Dot-Walk zu einem anderen Feld erfordert, in diesem Fall **Betriebssystem**. Dieser Prozess kann viele Millisekunden dauern, was sich schnell summiert, wenn Millionen von angreifbaren Elementen importiert werden, und die Leistung beeinträchtigen.

Hinweis:
Die Verwendung der Bedingung [enthält] ist wie eine Platzhaltersuche und kann Auswirkungen auf die Leistung haben. Wo immer möglich, ist die Verwendung von [is] effizienter.

Schweregradzuordnung für Vulnerability Response

Im Lieferumfang von Vulnerability Response enthalten ist die National Vulnerability Database (NVD) zur normalisierten ServiceNow-Schweregradzuordnung. ServiceNow-Drittparteiintegrationen bieten bei der Installation Schweregradzuordnungen. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 – Schweregradzuordnung für Schwachstellenintegration

Normalized_Severity

Berechnen Sie „normalized_severity“ für den Drittparteieintrag anhand des Schweregrads aus der Tabelle **„sn_vul_nvd_entry“**. Dies wird mithilfe von „Business-Regeln für Suche nach normalisiertem Schweregrad“ in der Tabelle **„sn_vul_entry“** festgelegt.

Source_severity

Daten aus der Tabelle **„severity_score“** werden der Tabelle **„source_severity“** zugeordnet, während die **Rapid7 Vulnerability Integration – API** ausgeführt wird.

Priorität

Dieses Feld ist leer.

Qualys Schweregradzuordnung für Schwachstellenintegration

Normalized_Severity

Berechnen Sie „normalized_severity“ für den Drittparteieintrag anhand des Schweregrads aus der Tabelle **„sn_vul_nvd_entry“**. Dies wird mithilfe von „Business-Regeln für Suche nach normalisiertem Schweregrad“ in der Tabelle **„sn_vul_entry“** festgelegt.

Source_severity

Daten aus **SEVERITY_LEVEL** werden der Tabelle **„source_severity“** zugeordnet, während die **Qualys Knowledge Base-Integration** ausgeführt wird.

Priorität

Daten für das Feld Priorität werden aus **der SEVERITY-Tabelle** abgerufen und der **Prioritätstabelle** zugeordnet, während **die Qualys-Host-Erkennungsintegration** unter Verwendung der Geschäftsregel ausgeführt wird, die Qualys-Daten zugeordnet ist.

Hinweis:
Geschäftsregeln werden im Hintergrund ausgeführt, überprüfen die Priorität für Qualys und ordnen die Priorität entsprechend zu. Für die Zuordnung von Qualys-Daten ist also BR verantwortlich.

Tenable.io-Schwachstellenschweregradzuordnung für Schwachstellenintegration

Normalized_Severity

Berechnen Sie „normalized_severity“ für den Drittparteieintrag anhand des Schweregrads aus der Tabelle **„sn_vul_nvd_entry“**. Dies wird mithilfe von „Business-Regeln für Suche nach normalisiertem Schweregrad“ in der Tabelle **„sn_vul_entry“** festgelegt.

Source_severity

Daten aus der Tabelle **„risk_factor“** werden der Tabelle **„source_severity“** zugeordnet, während die **Tenable.io-Plugin-Integration** ausgeführt wird.

Priorität

Daten aus **„severity_id“** werden **„source_severity“** zugeordnet, während **Tenable.io Open Vulnerabilities Integration** ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VPR

Daten aus **der Punktzahl** werden **Source_risk_score** zugeordnet, während **die Tenable.io-Plugin-Integration** ausgeführt wird.

Daten aus **„Berechnet aus Punktzahl“** werden **Source_risk_rating** zugeordnet, während **die Tenable.io-Plugin-Integration** ausgeführt wird.

Tenable.sc-Schwachstellenintegrations-Schweregradzuordnung

Normalized_Severity

Berechnen Sie **„normalized_severity“** für den Drittparteieintrag anhand des Schweregrads aus der Tabelle „sn_vul_nvd_entry“. Dies wird mithilfe von „Business-Regeln für Suche nach normalisiertem Schweregrad“ in der Tabelle **„sn_vul_entry“** festgelegt.

Source_severity

Daten für die Tabelle **„riskFactor“** werden „ **source_severity“** zugeordnet, während die **Tenable.io-Plugin-Integration** ausgeführt wird.

Priorität

Daten aus **dem Schweregrad**, die als **„severity“: { "id": "0", "name": "Info", "description": "Informative" }** empfangen wurden, werden **source_severity** zugeordnet, während die **Tenable.io Open Vulnerabilities-Integration** ausgeführt wird.

VPR

Daten aus **vprScore** werden **Source_risk_score** zugeordnet, während **die Tenable.io-Plugin-Integration** ausgeführt wird.

Daten aus **„Von vprScore berechnet“** werden **Source_risk_rating** zugeordnet, während **die Tenable.io-Plugin-Integration** ausgeführt wird.

TVM-Schweregradzuordnung

Normalized_Severity

Berechnen Sie „normalized_severity“ für den Drittparteieintrag anhand des Schweregrads aus der Tabelle **„sn_vul_nvd_entry“**. Dies wird mithilfe von „Business-Regeln für Suche nach normalisiertem Schweregrad“ in der Tabelle **„sn_vul_entry“** festgelegt.

Source_severity

Daten aus **der Schweregradtabelle** werden **„source_severity“** zugeordnet, während **die Microsoft TVM-Schwachstellenintegration (CVE)** ausgeführt wird.

Priorität

Dieses Feld ist leer.

Erstellen Sie eine Vulnerability Response -Schweregradzuordnung

Die SchweregradzuordnungVulnerability Response wandelt Quellschweregradfelder von Drittparteien in erkennbare Felder in Vulnerability Responseum.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response wird mit der Schweregradzuordnung National Vulnerability Database (NVD) zur normalisierten ServiceNow geliefert. ServiceNow Drittanbieterintegrationen wie Qualys Vulnerability Integration bieten Schweregradzuordnungen bei der Installation. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.

Das Erstellen oder Bearbeiten einer Schweregradzuordnung ist nur für anwenderdefinierte oder nicht standardmäßige Drittpartei-Zuordnungen in Ihrer Umgebung vorgesehen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Normalisierte Schweregradzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldzuordnung

Feld	Beschreibung
Quelle	Der Name der Quelle für die Schweregradzuordnung.
Quellwert	Der Wert des Quellschweregrads.
Zielwert	Der Zielschweregradwert. Die Auswahlmöglichkeiten lauten wie folgt: ○ 1 – Kritisch ○ 2 – Hoch ○ 3 – Mittel ○ 4 – Niedrig ○ 5 – Keine

4. Wiederholen Sie Schritt 3 für jeden Quellschweregrad.
5. Klicken Sie auf **Absenden**.

Definieren Sie Serviceklassifizierungen für die Berichterstellung Vulnerability Response und zugehörige Listen

Durch die Definition von Serviceklassifizierungen können Sie Berichterstellung und zugehörige Listen in Vulnerability Response stärker in den Fokus rücken. Darüber hinaus kann die Anzahl der angeforderten Serviceklassifizierungen reduziert werden, um die Leistung der Vulnerability Response -Datenerfassung zu verbessern.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Das Bearbeiten von Systemeigenschaften erfordert das Fachwissen ServiceNow und Vulnerability Response.

Prozedur

1. Geben Sie in der linken Navigationsleiste sys_properties_list.do ein.
2. Klicken Sie auf **Eingeben**.
3. Geben Sie im Menü **Suchen** unter **Name**sn_vul.service_classificationsein.
4. Öffnen Sie die Systemeigenschaft *sn_vul.service_classifications*.
5. Geben Sie im Textfeld **Wert** die durch Kommas getrennte Liste der gewünschten Serviceklassifizierungen ein.

   Hinweis:
   Wenn diese Einstellung leer ist, werden alle Services aufgelistet.

   Beispiele:

   Um Business-Services, technische Services und Anwendungsservices anzuzeigen und Serviceangebote, gemeinsam genutzte Services und nicht klassifizierte Services auszuschließen, legen Sie den Wert fest: **Business-Service,Technischer Service,Anwendungsservice**.

   Um Anwendungsservices anzuzeigen, legen Sie den Wert auf **Anwendungsservice**fest.

6. Klicken Sie auf **Aktualisieren**.
   Die Daten in jedem Bericht und in der zugehörigen Liste für angreifbare Elemente werden bei der nächsten Ausführung des nächtlichen Performance Analytics-Auftrags nach Serviceklassifizierung gefiltert.

Prüfen Sie ausgewählte Felder in der Tabelle der angreifbaren Elemente

Aktivieren Sie Auditing für Felder, die Sie in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item] angeben. Diese Audit-Methode ist nützlich, wenn Sie Felder prüfen möchten, die Sie standardmäßig nicht überwachen können.

Vorbereitungen

Erforderliche Rolle: Administrator

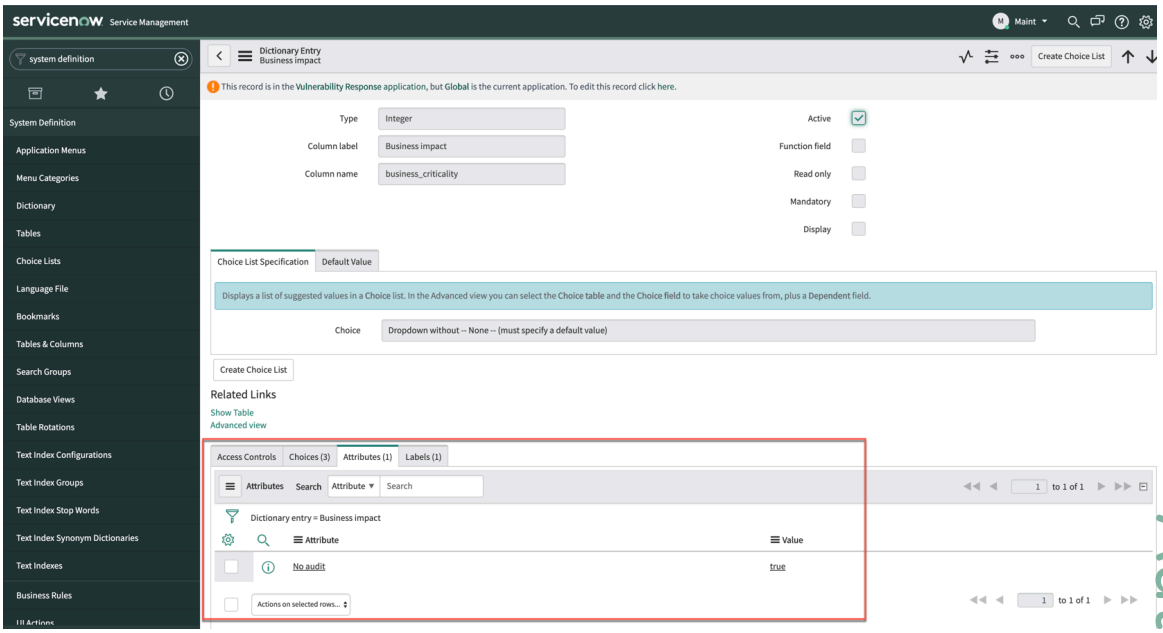
Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle sn_vul_vulnerable_item kann standardmäßig geprüft werden. Felder, für die das Attribut „no_audit“ auf „wahr“ festgelegt ist, können nicht geprüft werden. Weitere Informationen zum Auditing von Tabellen finden Sie unter Auditing für Tabelle aktivieren .

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Systemdefinition** > **Tabellen** und suchen Sie nach der Tabelle sn_vul_vulnerable_item.
   Die Liste der Wörterbucheinträge für die Tabelle wird angezeigt.
2. Um das Auditing für ein Feld zu aktivieren, klicken Sie auf den Namen des Eintrags.
   Die Seite „Wörterbucheintrag“ für diesen Eintrag wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Navigieren zu **Attribute** > **Kein Audit**.
   Die Seite „Wörterbuchattribut“ wird angezeigt.
4. Klicken Sie auf **Löschen**, um das Attribut „no audit=true“ zu entfernen.
   Auditing für dieses Feld ist aktiviert.

Vulnerability Response Konfiguration des Hintergrundauftrags-Frameworks

Definieren Sie das Framework für Hintergrundaufträge in Ihrer Instanz Now Platform®. Diese Konfigurationsänderungen können Ihnen helfen, die Leistung zu verbessern, indem Sie die Menge der für die Ausführung Ihrer Hintergrundaufträge verwendeten Systemressourcen reduzieren.

Was können Sie im Hintergrundauftrags-Framework bearbeiten?

Mit dem Modul zur Konfiguration des Hintergrundauftrags stehen Ihnen im -Framework folgende Einstellungsoptionen zur Verfügung:

- Sie können die Anzahl der Hintergrundaufträge definieren, die gleichzeitig für Vulnerability Response Prozesse ausgeführt werden.
- Für lange Aufgaben, die im Hintergrund ausgeführt werden und große Datenmengen verarbeiten, können Sie Partitionen erstellen, um Daten in kleineren Blöcken zu verarbeiten.
- Sie können einen Auftrag abbrechen.

Warum das Hintergrundauftrags-Framework konfiguriert werden soll

Hintergrundaufträge in Now Platform® sind so konzipiert, dass sie über einen längeren Zeitraum ausgeführt werden, um mehrere Prozesse für Ihre Datensätze in Vulnerability Responseauszuführen. Diese Aufgaben basierten zuvor auf asynchron ausgeführten Geschäftsregeln. Es gibt keine Begrenzung für die Anzahl dieser Aufgaben, die in Ihrer Instanz im Hintergrund ausgeführt werden können, sodass die großen Mengen von Datensätzen, die von diesen Aufgaben betroffen sind, verarbeitet werden können. Wenn mehrere Aufgaben, deren Abschluss viel Zeit in Anspruch nimmt, gleichzeitig im Hintergrund ausgeführt werden, sind die Systemressourcen für die Ausführung der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

geplanten Aufgaben betroffen, was sich wiederum negativ auf Ihre Leistung auswirken kann.

Durch die Konfiguration des Frameworks für Hintergrundaufträge können Sie Ihre Leistung verbessern, indem Sie die Menge der für die Ausführung Ihrer Hintergrundaufträge verwendeten Systemressourcen reduzieren.

Wichtige Begriffe

Auftragsfähigkeit

Beschreibt die jeweiligen Aufgaben. Beispielsweise kann ein bestimmter Auftrag die folgenden Fähigkeiten enthalten:

- Der Auftrag kann parallel zu einem anderen Auftrag des gleichen Typs ausgeführt werden.
- Der Auftrag kann partitioniert werden.
- Der Auftrag kann während der Ausführung abgebrochen werden.

Gleichzeitigkeit

Bezieht sich auf Aufträge oder Teile von Aufträgen, die parallel ausgeführt werden.

Partition

Partitionen sind Teile von Aufgaben, die aufgeteilt werden können, um parallel verarbeitet zu werden und eine bessere Leistung zu erzielen. Bezieht sich normalerweise auf Aufträge mit langen Laufzeiten.

Auftragskonfiguration

Bezieht sich auf die Einstellungen für eine bestimmte geplante Aufgabe.

Geplante Aufgabe

Regelmäßige Aufgaben sind automatisierte Aufgaben, die zu einem bestimmten Zeitpunkt oder nach einem wiederkehrenden Zeitplan ausgeführt werden können.

Systemressourcen

Bezieht sich auf die Menge der Systemressourcen, die Sie für die Unterstützung einer bestimmten Anzahl von Hintergrundaufgaben und geplanten Aufgaben in Ihrer Umgebung benötigen.

Systemeigenschaft

Systemeigenschaften speichern Konfigurationsinformationen, die sich selten oder nie ändern. Jedes Mal, wenn Sie eine Systemeigenschaft ändern oder hinzufügen, leert das System den Cache, damit alle Knoten im Cluster synchron bleiben. Diese Cacheleerung wirkt sich auf die Leistung aus.

Business-Regel

Eine Business Rule ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder eine Tabelle abgefragt wird. Business-Regeln erfüllen Aufgaben wie das automatische Ändern von Werten in Formularfeldern, wenn bestimmte Bedingungen erfüllt sind, oder das Erstellen von Ereignissen für E-Mail-Benachrichtigungen und Skriptaktionen.

Anwendungsfall zum Definieren des Hintergrundauftrags-Frameworks

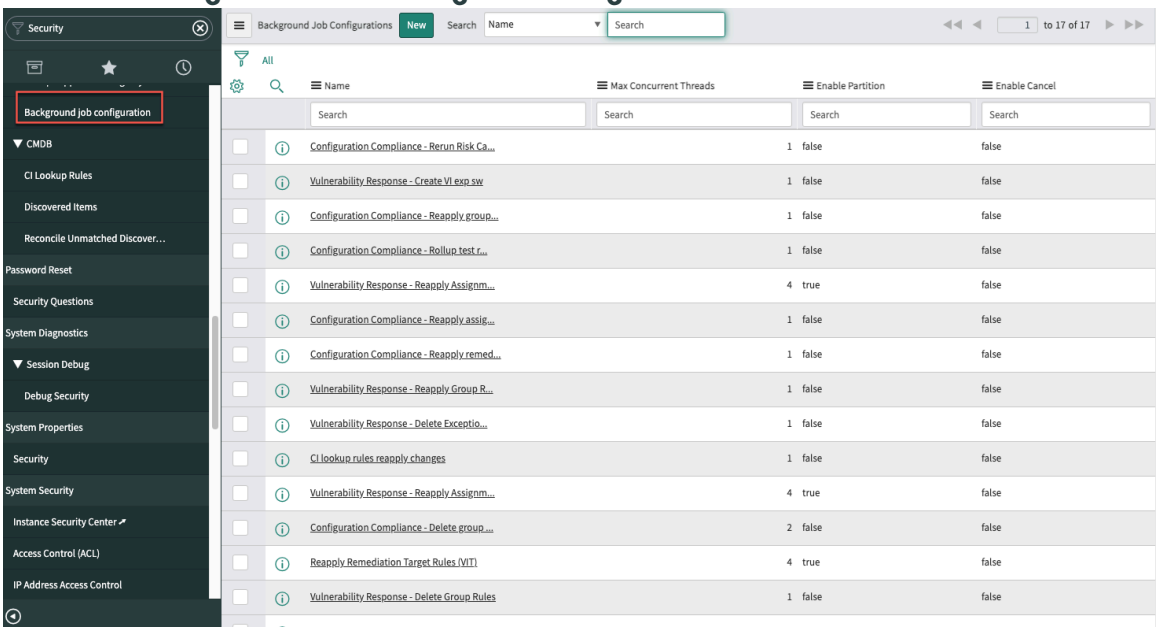
Beispielsweise verarbeitet der Hintergrundauftrag, der Nachbesserungszielregeln für Datensätze zu angreifbaren Elementen (VITs) und Datensätze für angreifbare Elemente in Application Vulnerability Response anwendet, gleichzeitig große Mengen von Datensätzen mit mehreren Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängig von der Größe des Imports und der Anzahl der Datensätze in Ihrer Umgebung kann dieser Auftrag einen großen Teil Ihrer verfügbaren Systemressourcen verbrauchen und es lange dauern, bis er erfolgreich abgeschlossen wird. Systemwartungsaufgaben oder andere geplante Aufgaben werden möglicherweise langsamer ausgeführt.

Im Modul zur Konfiguration des Hintergrundauftrags werden Aufträge nach Name und einer eindeutigen Konfigurations-ID aufgelistet. Für diese Datensätze können Sie definieren, wie viele Aufgaben gleichzeitig für einen bestimmten Hintergrundauftrag ausgeführt werden sollen. Sie können die Aufgabe auch so einstellen, dass Datenpartitionen verarbeitet werden, damit die Aufgaben schneller und einfacher abgeschlossen werden und weniger Systemressourcen verbrauchen. Sie können einen Auftrag auch abbrechen, wenn Sie feststellen, dass er zu lange dauert.

Modul zur Konfiguration des Hintergrundauftrags



Weitere Informationen zu den erforderlichen Schritten zum Definieren der Hintergrundauftragskonfigurationen finden Sie unter Definieren Sie Konfigurationen für Hintergrundaufträge in Vulnerability Response.

Definieren Sie Konfigurationen für Hintergrundaufträge in Vulnerability Response

Definieren Sie, wie viele Aufgaben gleichzeitig für einen bestimmten Hintergrundauftrag ausgeführt werden sollen. Sie können den Auftrag auch so einstellen, dass Datenpartitionen importiert werden, damit die Aufgaben schneller und einfacher abgeschlossen werden und weniger Systemressourcen verbrauchen. Sie können einen Auftrag auch abbrechen, wenn Sie feststellen, dass er zu lange dauert.

Vorbereitungen

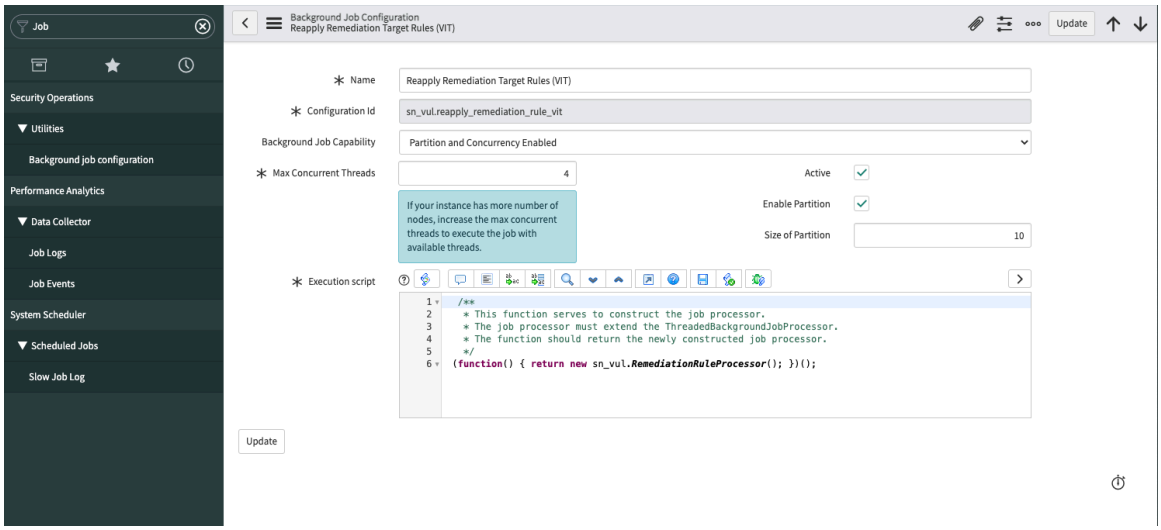
Erforderliche Rolle: sn_vul.vulnerability_admin oder Schwachstellenmanager mit der granularen Rolle sn_sec_cmn.manage_background_job

Ein Beispiel finden Sie im Abschnitt unter den Schritten.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Hintergrundauftrags-Konfigurationen**.
2. Klicken Sie in der Spalte Name auf einen Datensatz, um ihn zu öffnen.
3. Bearbeiten Sie die Felder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



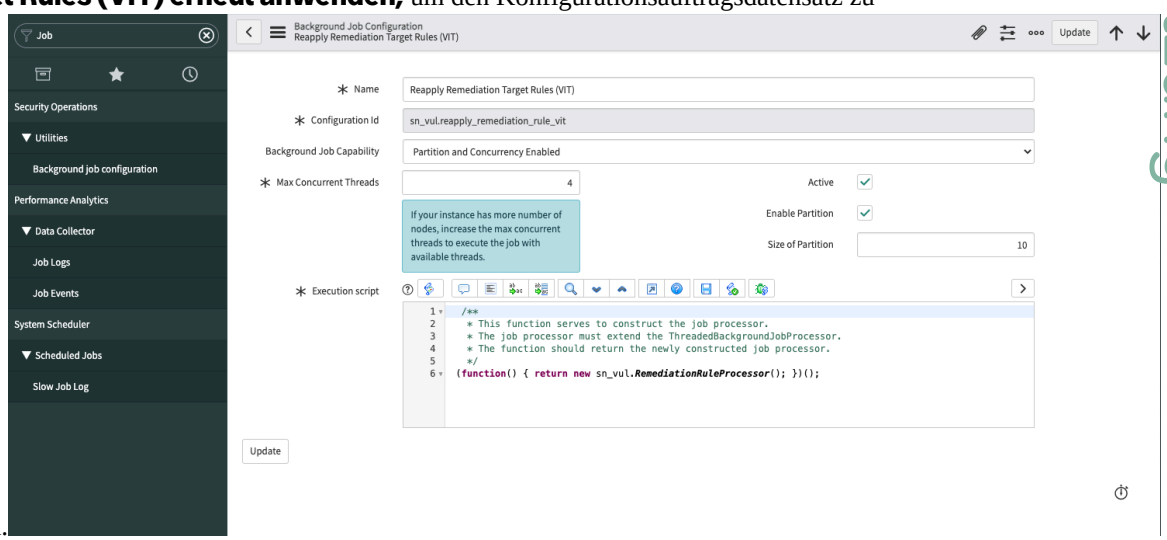
4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
   Im folgenden Beispiel erfahren Sie, wie Sie die Ergebnisse für Ihre Konfigurationsänderungen überprüfen können.

   Es gibt zwei Konfigurationen für Korrekturzielregeln-Aufträge, die in der Anwendung enthalten sind, eine für angreifbare Elemente und eine für angreifbare Anwendungselemente:

   - Korrekturzielregeln erneut anwenden (VIT)
   - Korrekturzielregeln erneut anwenden (AVIT)

   Angenommen, Sie ändern Ihre Korrekturzielregeln und möchten sie erneut anwenden, ohne die meisten verfügbaren Systemverarbeitungsressourcen zu verwenden. Um die Verarbeitungsressourcen zu begrenzen, können Sie im Modul „Hintergrundauftragskonfigurationen“ die Anzahl der von Ihnen ausgeführten Hintergrundaufträge und die Anzahl der pro Auftrag verarbeiteten Elemente steuern.

5. Um diese Einstellungen zu definieren, navigieren Sie zu **Security Operations** > **Hintergrundauftrags-Konfigurationen** und klicken Sie auf **Remediation Target Rules (VIT) erneut anwenden,** um den Konfigurationsauftragsdatensatz zu öffnen.



   Nehmen wir für das Beispiel an, Sie wissen, dass Sie etwas mehr als 300 AEs haben.

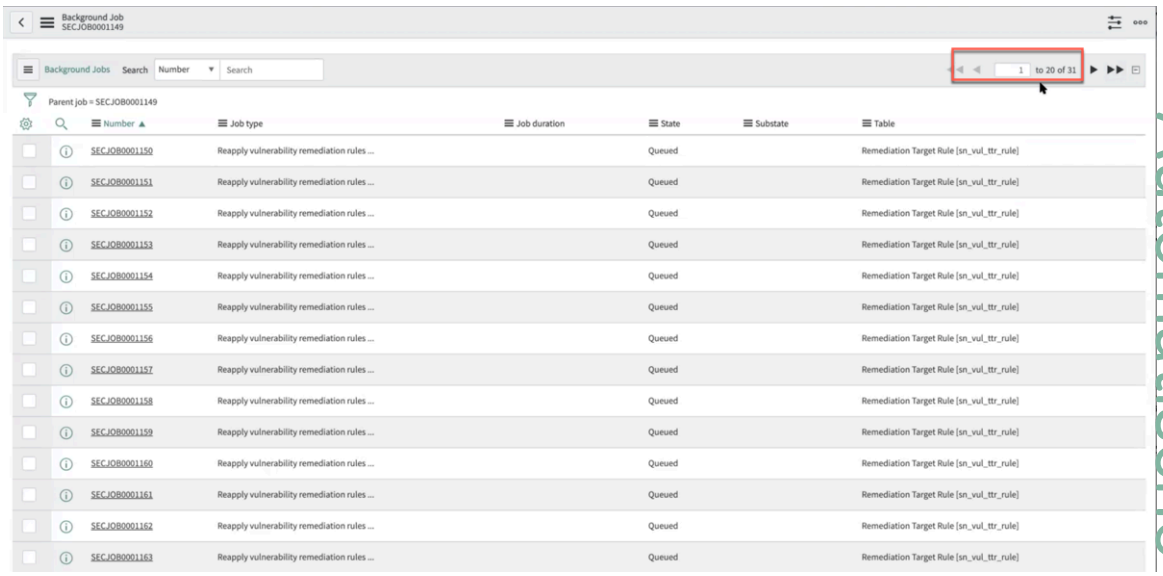
6. Ändern Sie im Datensatz des geöffneten Konfigurationsauftrags den Wert der Partitionsgröße von **4** in **10**.

Automatische Übersetzung

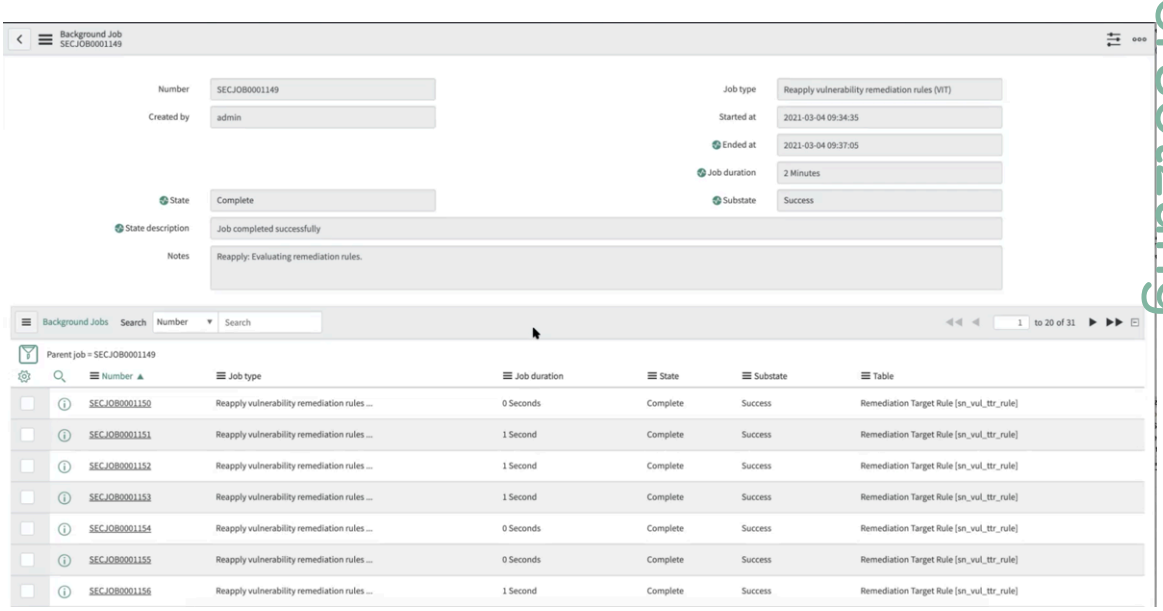
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Navigieren zu **Vulnerability Response** > **Korrekturzielregeln**, suchen Sie die von Ihnen geänderte Schwachstellen-Korrekturregel erneut anwenden, wählen Sie den Datensatz aus der Liste aus, und klicken Sie auf **Änderungen übernehmen**, um Ihre Zielregeln für Ihre vorhandenen AEs neu auszuwerten.
Der Auftrag „Schwachstellenkorrekturregeln (Vulnerability Remediation Rules, VIT)“ erneut anwenden befindet sich in der Warteschlange.

8. Klicken Sie auf den Link **Status anzeigen**, um den Datensatz des Hintergrundauftrags anzuzeigen und sicherzustellen, dass sich die Aufträge in der Warteschlange befinden (siehe folgende Abbildung).
In diesem Beispiel werden 31 Aufträge erstellt, um Zielregeln für 307 VIs zu verarbeiten (maximal 10 Elemente pro Auftrag). Diese Aufträge sind untergeordnete Aufträge des primären Hintergrundauftrags. Die untergeordneten Aufgaben verarbeiten die Datensätze nacheinander.



Wenn alle Aufträge erfolgreich abgeschlossen wurden, werden die Felder im Datensatz „Hintergrundauftrag“ aktualisiert.



9. Navigieren Sie zu Ihren angreifbaren Elementen, und überprüfen Sie, ob sie die neue Regeländerung widerspiegeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte parallele Verarbeitung für Hintergrundaufträge in Vulnerability Response

Mit dieser erweiterten Einstellung können Sie die Gesamtzahl der Hintergrundaufträge steuern, die unabhängig vom Auftragstyp parallel verarbeitet werden.

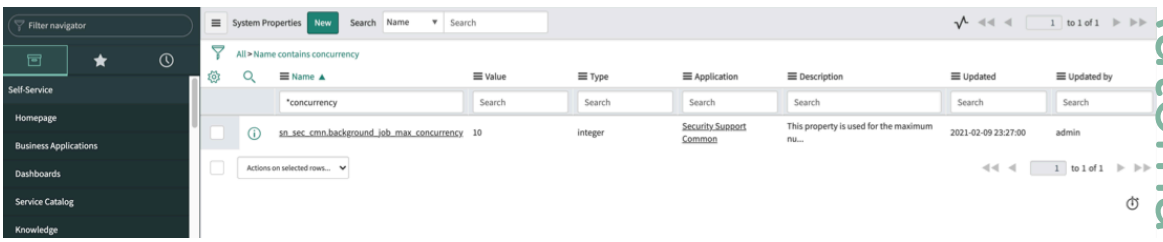
Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder Schwachstellenmanager mit der granularen Rolle sn_sec_cmn.manage_background_job

Hinweis:
Dieses Verfahren erfordert fortgeschrittene Programmierkenntnisse.

Prozedur

1. Geben Sie im Filternavigator **sys_properties.list** ein, und suchen Sie die Systemeigenschaft *sn_sec_cmn.background_job_max_concurrency*.



2. Klicken Sie darauf, um den Datensatz zu öffnen.

   Standardmäßig führt die Systemeigenschaft *sn_sec_cmn.background_job_max_concurrency* maximal 10 Hintergrundaufträge parallel aus.

   Wenn Ihre Instanz eine geringe Anzahl von Knoten hat, können Sie diesen Wert in der Systemeigenschaft reduzieren. Angenommen, Sie haben sieben Zuweisungsregeln in der Liste Gruppenregeln. Im Konfigurationsdatensatz des Auftrags „Zuweisungsregeln erneut anwenden“ werden drei Aufträge für die Max. gleichzeitige Threads festgelegt. Ihr Gleichzeitigkeitswert für Ihr -Framework ist 10, aber Ihr System ist eine Einzelknoteninstanz, sodass Sie zwei partitionierte Aufträge aus Ihrem Auftrag „Zuweisungsregeln erneut anwenden“ gleichzeitig verarbeiten können. Wenn Sie die maximale Anzahl gleichzeitiger Threads auf einen Datensatz für den Auftrag „Zuweisungsregeln“ festlegen, werden alle Auftragstypen „Zuweisungsregeln erneut anwenden“ nacheinander verarbeitet.

   Wenn Ihre Instanz hingegen mehr Knoten hat, können Sie diesen Wert erhöhen, müssen aber auch weitere geplante Aufgaben hinzufügen, um diese Änderung vorzunehmen.

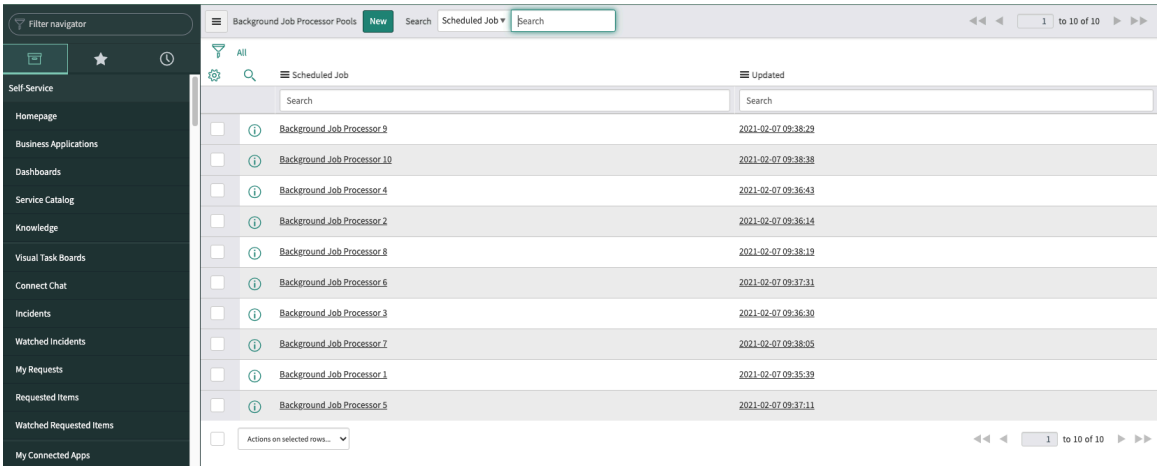
   Um die Anzahl der geplanten Aufgaben zu erhöhen, duplizieren Sie eine geplante Aufgabe so oft, bis sie dem Wert entspricht, um den Sie Ihre Systemeigenschaft erhöht haben. Standardmäßig gibt es beispielsweise 10 geplante Aufgaben. Wenn Sie also 20 Aufträge wünschen, müssen Sie einen Auftrag 10 Mal duplizieren.

   Die zehn geplanten Aufgaben, die in Now Platform® zur Verarbeitung enthalten sind, werden in der Tabelle sn_sec_cmn_background_job_processor_pool angezeigt.

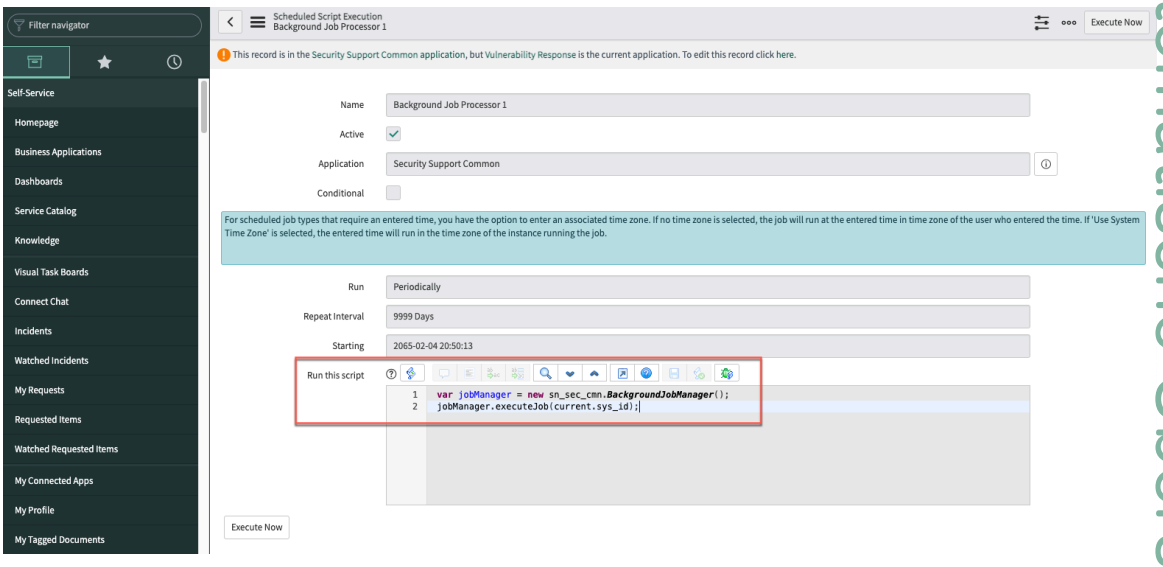
3. Geben Sie im Filternavigator **sn_sec_cmn_background_job_processor_pool.list**ein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf einen Auftrag, um ihn so oft wie nötig zu kopieren und zu duplizieren, bis die Anzahl der Aufträge dem Wert entspricht, um den Sie Ihre Systemeigenschaft erhöht haben.



5. Nachdem die geplante Aufgabe definiert wurde, fügen Sie eine Referenz hinzu, indem Sie in der Liste sn_sec_cmn_background_job_processor_pool für die von Ihnen kopierte Aufgabe auf **Neu** klicken.

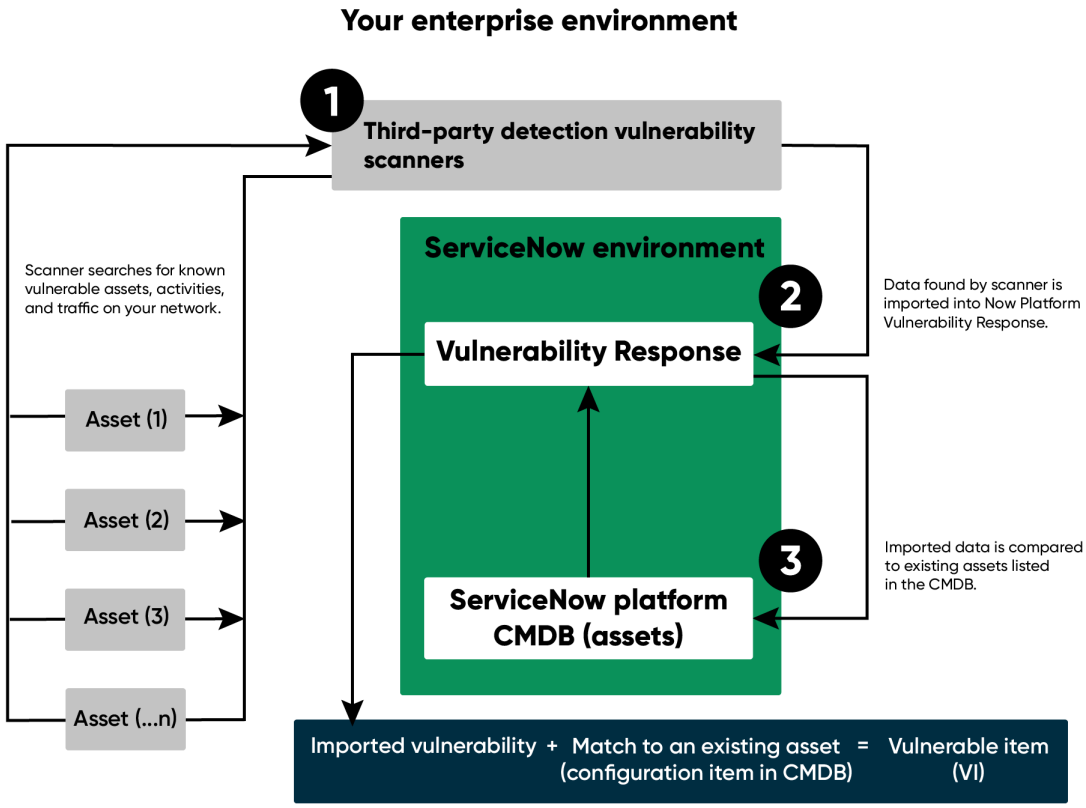
Vulnerability Response-Integrationen

Vulnerability Response beinhaltet Unterstützung für Drittanbieterintegrationen. Dieser Abschnitt enthält einige grundlegende Richtlinien für die Entwicklung eigener Integrationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen von Drittparteien



Importierte Schwachstellen aus der National Vulnerability Database (NVD) und Erkennungsdaten von Drittanbieter-Scannern werden mit den Assets in Ihrer CMDB abgeglichen. Wenn eine importierte Schwachstelle mit einem vorhandenen Asset übereinstimmt, wird ein angreifbares Element erstellt. Angreifbare Elemente werden automatisch in zu korrigierenden Aufgaben gruppiert, mit Risikobewertung für den Geschäftskontext bewertet, priorisiert und den entsprechenden Teams zur Korrektur zugewiesen.

Hinweis:

Drittanbieterintegrationen werden separat behandelt. Wenn in Ihrer Umgebung mehr als eine Integrationsanwendung von Drittparteien verwendet wird, gibt es keine integrationsübergreifende Deduplizierung angreifbarer Elemente (VIs, Vulnerable Items). Beispielsweise ist die VI-Deduplizierung zwischen Rapid7 und Qualys nicht verfügbar.

Nichtübereinstimmungen in der Erkennungsanzahl zwischen einem Drittanbieterscanner (z. B. Qualys) und VIs in Ihrer Instanz ServiceNow sind jedoch zu erwarten, da die Deduplizierung über IPs, Ports usw. erfolgt.

Informationen zu von Application Vulnerability Response unterstützten Drittanbieterintegrationen finden Sie unter Integration von Application Vulnerability Response mit anderen Anwendungen

- Integration von CISA Known Exploit Vulnerability (KEV)
- Informationen zur Schwachstellenintegration von Microsoft Threat and Vulnerability Management
- Informationen zur Integration der HCL BigFix Patch Orchestration in mit Vulnerability Response

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Informationen zur Integration der Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM
- Grundlagen zu NVD-Integrationen
- Qualys Vulnerability Integration
- Rapid7 Vulnerability-Integration verstehen
- Shodan Exploit Integration
- Die Tenable-Schwachstellenintegration verstehen
- Integration der Microsoft Security Response Center-Lösung

  Integration der Microsoft Security Response Center-Lösung ist mit Vulnerability Solution Managementverfügbar. Informationen zur Installation und Konfiguration von Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integrationfinden Sie unter Anwendung Solution Management for Vulnerability Response installieren. Sie können Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration im Setup-Assistenten konfigurieren, bearbeiten, planen und bei Bedarf starten.

Zusätzliche Hinweise zu Integrationen

Wenn für eine Integration mehrere Bereitstellungen unterstützt werden, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

- Sie können viele der Integrationsanwendungen vom Setup-Assistenten aus installieren, konfigurieren, planen und bei Bedarf starten.
- Sie können die Anwendung Rapid7 Vulnerability-Integration über den Setup-Assistenten installieren, die Konfiguration dieser Integration wird jedoch nicht vom Setup-Assistenten unterstützt. Weitere Informationen finden Sie unter Rapid7 Vulnerability-Integration installieren.
- Die Anwendung Tenable for Vulnerability Response von Tenable wird von Tenable erstellt und verwaltet. Weitere Informationen finden Sie unter Tenable for Vulnerability Response.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Ab VR v17.1 wurden die folgenden Statusnamen des Integrationsprozesses aktualisiert:

Statusname vor V17.1	Statusname V17.1 und höher
In Verarbeitung	Wird abgerufen
WartenAbgeschlossen	Warten/Bearbeitung läuft

Hinweis:
Sie können die Anhänge anzeigen, die heruntergeladen und verarbeitet werden. Wenn der Status der Integrationsausführung `warten – abgeschlossen`ist, wird der Prozentsatz der abgeschlossenen Integration angezeigt.

[store-future: BEGIN review]Ab v22.1.2 von Vulnerability Responsekönnen Sie Schwachstellen mithilfe von Ausschlussregeln von der Erfassung ausschließen. Wenn Sie Integrationen vom Typ Rapid7, Qualys, Tenable for Vulnerability Response, Microsoft Defender Threat and Vulnerability Management ausführen oder Schwachstellen manuell erfassen, können Sie außerdem die Anzahl der Erkennungen anzeigen, die ausgeschlossen wurden. Auf diese Informationen kann auf der Registerkarte **Erkennungen** im Bildschirm der Integrationsausführung zugegriffen werden. Weitere Informationen finden Sie unter Übersicht über Ausschlussregeln und Erstellen Sie eine Ausschlussregel.[End]

Manuell erstellte Integrationen

Sie können bei Bedarf weitere Integrationen hinzufügen, die nicht als ServiceNow Store -Anwendungen verfügbar sind. Weitere Informationen finden Sie unter Erstellen Sie manuell eine Schwachstellen-Integration.

Grundlagen zu NVD-Integrationen

Die NVD-Integrationen verwenden Daten, die aus der National Vulnerability Database (NVD) des National Institute of Standards and Technology (NIST) importiert werden, um Ihnen zu helfen, die Auswirkungen und Priorität von Fehlern in Ihrem Code zu bestimmen. Führen Sie diese Integration im Rahmen der Ersteinrichtung von Vulnerability Response und bevor Sie Schwachstellendaten mit dem Scannerprodukt einer Drittpartei in Ihre Instanz importieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Der NIST NVD sammelt Daten zu Common Vulnerabilities and Exposures (CVE) und Common Platform Enumeration (CPE) und stellt diese Daten dem Now Platform®zur Verfügung. Es lässt sich problemlos in Vulnerability Response integrieren, um CVE- und CPE-Schwachstellen abzubilden und die Daten in Ihrer Instanz zu ergänzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Anwender. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Nach der Installation wird die Integration mit der NIST National Vulnerability Database Integration-API (nur CVE) automatisch als geplante Aufgabe aufgerufen und täglich ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Tipp:
Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response Integration mit NVD v1.2	

Anfänglicher Import von Schwachstellendaten mit den NVD- und CWE-Integrationen

1. Führen Sie einen ersten Import von CWE-Daten mit der CWE Comprehensive 2000 Integration durch.

   Weitere Informationen finden Sie unter Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus. Sie führen CWE-Aktualisierungen **bei Bedarf** standardmäßig über den Integrationsdatensatz durch und müssen diesen konfigurieren.

   Hinweis:
   Planen Sie die Ausführung des CWE-Updates vor dem Update der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**.

2. Stellen Sie sicher, dass die Anwendung Vulnerability Response Integration with NVD installiert ist und ein erster Datenimport aus der Integration der US-Schwachstellendatenbank NIST National Vulnerability Database – API (nur CVE) oder der US-Schwachstellendatenbank Integration NIST National Vulnerability Database Integration API (CVE und CPE) erfolgreich ist.

   Verifiziert für CPEs, ob ein erster Datenimport aus der API-Integration der US-Schwachstellendatenbank (National Vulnerability Database Integration) des NIST (Nur CPE) erfolgreich ist.

   Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Nach der Installation des Plugins wird standardmäßig die API-Integration der US-Schwachstellendatenbank (National Vulnerability Database Integration) des NIST (Nur CVE) aktiviert. Sie wird täglich ausgeführt. Weitere Informationen finden Sie unter Installieren Sie die -Integration Vulnerability Response mit der US-Schwachstellendatenbank (National Vulnerability Database) des NIST.

3. Drittpartei-Bibliotheken werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importierte Schwachstellendaten und angreifbare Elemente verstehen

In Ihrer Instanz Now Platform wird jede importierte Schwachstelle durch einen Schwachstelleneintrag in den Quellbibliotheken von Scanner-Produkten von Drittanbietern dargestellt, z. B. Qualys. Die angreifbaren Elemente (VI), die in Ihrer Instanz importiert und aktualisiert werden, sind Verweise auf Drittanbieterbibliotheken, z. B. die Bibliothek Qualys. Eine Drittanbieterbibliothek kann wiederum auf den NVD zurückverweisen.

Wenn Sie beispielsweise Schwachstellendaten von Drittparteien aus einem Produkt wie Qualyserfassen, erfassen Sie VIs, die auf eine QID (BezeichnerQualys) verweisen. Im Fall von Qualysverweist diese QID wiederum auf ein CVE aus der NVD-Bibliothek. Wenn Sie in einer Korrekturaufgabe oder einem Datensatz für ein angreifbares Element in der Anwendung Vulnerability Response auf diese QID klicken und die NVD- und CWE-Integrationen zur Erfassung von Daten ausgeführt haben, werden aktuelle, angereicherte Schwachstellendaten angezeigt, mit denen Sie die Beziehungen sehen können, die zwischen bestehen Ihre VIs und CVEs, CWEs und CPEs.

Bevor Sie ein Scannerprodukt einer Drittpartei wie Qualys ausführen, das über eine eigene Bibliothek verfügt, müssen Sie mindestens die Integration NIST National Vulnerability Database Integration- API (nur CVE) installieren und ausführen (enthält auch CISA-bezogene Details). , CWE-Integration zur Erfassung von Schwachstellendaten. Diese NVD- und CWE-Datenimporte ergänzen Ihre Vulnerability Response - oder Application Vulnerability Response -Daten, bevor Sie Daten mit einem Drittanbieterprodukt importieren.

Weitere Informationen zum Verwalten und Anzeigen der NVD-, CWE- und Drittanbieterbibliotheken finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien und Zeigen Sie Schwachstellenbibliotheken Vulnerability Response an.

Nachdem Sie den erfolgreichen NVD-Import verifiziert haben, bereichern Sie Ihre Schwachstellendaten weiter: Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus.

Führen Sie die NVD- und CWE-Importe durch, bevor Sie Schwachstellendaten mit einem Drittanbieterprodukt importieren. Drittpartei-Bibliotheken werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

Auffinden der NVD-Integrationen

Um die NVD-Integrationen anzuzeigen, navigieren Sie zu **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

Hinweis:
Standardmäßig ist nur die Integration der NIST National Vulnerability Database Integration – API (nur CVE) aktiv.

NVD-Integrationen

Integration	Beschreibung
NIST National Vulnerability Database	Ruft nur NIST NVD-Schwachstellendaten (CVE) ab. Standardmäßig ist diese Integration auf „Täglich ausgeführt“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

NVD-Integrationen (Fortsetzung)

Integration	Beschreibung
Integration – API (nur CVE)	
NIST National Vulnerability Database Integration-API (nur CPE)	Ruft CPE-Daten von NIST NVD ab. Diese Integration ist standardmäßig inaktiv. Aktivieren Sie diese Integration, wenn Sie CPE-Daten erfassen möchten, die ein formales Namensformat, eine Methode zum Überprüfen von Namen anhand eines Systems und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen enthalten. Diese Informationen werden in angreifbarer Software gespeichert. Diese Integration wird täglich ausgeführt und ist standardmäßig inaktiv. Informationen zum Aktivieren dieser Integration finden Sie unter NIST National Vulnerability Database–API aktivieren (nur CPE).
NIST National Vulnerability Database Integration-API (Nicht zugeordnete CPE)	Ruft CPE-Daten ab, die dem abgerufenen CVE aus NIST NVD zugeordnet sind. Diese Integration ist standardmäßig inaktiv. Aktivieren Sie diese Integration, wenn Sie CPE-Daten erfassen möchten, die ein formales Namensformat, eine Methode zum Überprüfen von Namen anhand eines Systems und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen enthalten. Diese Informationen werden in einer zugehörigen Liste für einen NVD-Schwachstelleneintragsdatensatz gespeichert. Diese Integration ist auf die Ausführung bei Bedarf festgelegt und standardmäßig inaktiv. Informationen zum Aktivieren dieser Integration finden Sie unter National Vulnerability Database–API des NIST (National Vulnerability Database) des NIST (Nicht zugeordnete CPE) aktivieren.

Wichtig:
Die Integration „NIST National Vulnerability Database Integration – API (CVE und CPE)“ ist veraltet.

Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus des NVD-Integrationsimports (National Vulnerability Database) an.

Vorbereitung der NVD-Integrationen

Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Die NVD-Integrationen setzen voraus, dass Sie mit der NIST National Vulnerability Database (NVD) vertraut sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der NVD-Integrationen alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus

Data-Importe aus der CWE ergänzen die Schwachstellendaten in Ihrer Instanz zusätzlich. Verwenden Sie die aus der CWE-Datenbank heruntergeladenen CWE-Datensätze (Common Weakness Enumeration) als Referenz, wenn Sie entscheiden, ob eine Schwachstelle eskaliert werden muss. Führen Sie diese Integration im Rahmen der Ersteinrichtung von Vulnerability Response und bevor Sie Schwachstellendaten mit dem Scannerprodukt eines Drittanbieters in Ihre Instanz importieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Hinweis:
Planen Sie die Ausführung des CWE-Updates vor dem Update der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**.

Aktualisieren Sie allgemeine Schwachstellendatensätze regelmäßig aus der Common Weakness Enumeration-Datenbank. Sie können bei Bedarf auch das Standardskript aktualisieren oder eigene Skripts schreiben.

Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über die Seite mit den allgemeinen Schwachstellenaufzählungen eskalieren.

- Wenn Sie über die Administratorrolle verfügen, können Sie der geplanten Aufgabe Repositorys hinzufügen.
- Mit sn_vul.vulnerability_read können Sie die geplante Aufgabe ausführen.
- Wenn Sie über sn_vul.vulnerability_write verfügen, können Sie die Details der geplanten Aufgabe bearbeiten.

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie die geplante Aufgabe **„CWE Comprehensive 2000 Integration“** aus.
3. Ändern Sie die Felder nach Bedarf.

Formular „Schwachstellenintegration“.

Feld	Beschreibung
Name	Name des geplanten Auftrags.
Aktiv	Gibt an, ob die geplante Aufgabe aktiv ist. Wenn der Auftrag für einen bestimmten Zeitraum nicht ausgeführt werden soll, können Sie die zu verwendenden Parameter einrichten und den Auftrag deaktivieren.
Ausführen	Häufigkeit, mit der der Auftrag ausgeführt werden soll. Nachfolgende Felder werden basierend auf Ihrer Einstellung in diesem Feld ein- oder ausgeblendet. **Hinweis:** Das CWE-Update ist standardmäßig Bei **Bedarf**. Legen Sie dies auf einen geplanten Zeitraum fest, der vor Ihren NVD-Updates liegt. Zur Auswahl stehen: ○ Täglich: Wählen Sie eine **Uhrzeit**aus ○ Wöchentlich: (häufigste Option) Wählen Sie einen **Tag** und**eine Uhrzeit**aus ○ Monatlich: Wählen Sie **Tag** und **Uhrzeit**aus ○ Regelmäßig: Wählen Sie ein **Wiederholungsintervall**, **Startdatum** und -uhrzeit aus ○ Einmal: Wählen Sie ein **Startdatum** und eine Startuhrzeit aus
Tag	Der Tag, an dem die geplante Aufgabe ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Sie **Wöchentlich** im Feld **Ausführen** ausgewählt haben, zeigt dieses Feld die Wochentage an. Wenn Sie **Monatlich** im Feld **Ausführen** ausgewählt haben, zeigt dieses Feld die Tage des Monats an. **Hinweis:** Planen Sie die Ausführung des CWE-Updates vor dem Update der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**.
Zeit	Die Zeit, zu der die geplante Aufgabe starten soll. **Hinweis:** Planen Sie die Ausführung des CWE-Updates vor dem Update der NVD-Datenbank. Die Standardzeit für das NVD-Update ist 01:00:00
Integrationsskript	Das Skript zum Abrufen von Daten aus den in der zugehörigen Liste **„Datenquellen“** angegebenen Datenquellen.
Quellenintegration	[Schreibgeschützt]
Quellinstanz	[Schreibgeschützt]
Anwendung	[Schreibgeschützt] Der Name der Anwendung, für die Sie die geplante Aufgabe ausführen.
Wiederholungsintervall	Anzahl der Tage und Stunden, bis die geplante Aufgabe erneut ausgeführt wird. Dieses Feld wird angezeigt, wenn in der Liste **Ausführen** die Option **Regelmäßig** ausgewählt ist.
Wird gestartet	Datum und Uhrzeit für den Start der regelmäßigen Aktualisierungen. Dieses Feld wird angezeigt, wenn in der Liste **Ausführen** die Option **Regelmäßig** ausgewählt ist.
Bedingt	Checkbox zum Hinzufügen bedingter Parameter.
Bedingung	Die Bedingungen zum Ausführen der geplanten Aufgabe. Dieses Feld wird angezeigt, wenn **das Kontrollkästchen** Bedingung aktiviert ist.
Berichtsprozessorstrategie	Die Strategie für das Abrufen von Daten und die Verarbeitung der geplanten Aufgabe. ○ Um Daten aus den Datenquellen in der zugehörigen Liste **„Datenquellen“** mithilfe des Skripts im Skriptfeld **Integration** abzurufen, wählen Sie **Datenquellenanhang**aus. ○ Um einen anwenderdefinierten Prozessor im Skriptfeld

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Berichtsprozessor auszuwählen, wählen Sie den **Anwenderdefinierten Berichtsprozessor**aus.
Berichtsprozessor-Skript	Das bei Ausführung der geplanten Aufgabe auszuführende Skript Dieses Feld wird angezeigt, wenn in der Liste der **Berichtsprozessorstrategiender anwenderdefinierte Berichtsprozessor** ausgewählt ist.
Prozessorwerksskript	Das Skript zum Erstellen des Berichtsprozessors. Dieses Feld wird angezeigt, wenn in der Liste der **Berichtsprozessorstrategiender anwenderdefinierte Berichtsprozessor** ausgewählt ist.

4. Klicken Sie mit der rechten Maustaste in den Header, um Ihre Änderungen zu **speichern**.
5. Um den Scheduled Job sofort auszuführen, klicken Sie auf **Jetzt ausführen**.
   Sie kehren zur Ansicht „Schwachstellenintegrationen“ zurück.
6. Um den Fortschritt des Imports zu überwachen, wählen Sie die geplante Aufgabe **„CWE Comprehensive 2000 Integration“** erneut aus, und wählen Sie dann die Registerkarte **Integrationsausführungen für Schwachstellen** aus.

   Informationen zu den importierten Einträgen finden Sie unter Zeigen Sie Schwachstellenbibliotheken Vulnerability Response an.

Installieren Sie die -Integration Vulnerability Response mit der US-Schwachstellendatenbank (National Vulnerability Database) des NIST

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt NIST National Vulnerability Database (NVD) ordnungsgemäß in Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn die Anwendung noch nicht zugewiesen wurde, installiert der Systemadministrator [admin] die Anwendung und weist Benutzer dem Schwachstellenmanager in Vulnerability Response oder der App-Sec-Manager-Gruppe in Application Vulnerability Responsezu. Informationen zu Gruppenrollen in Vulnerability Response finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response. Informationen zu Gruppenrollen in Application Vulnerability Response finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen. • Der Schwachstellenmanager oder App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: admin

Hinweis:
Nehmen Sie vor dem Ausführen der NVD-Integrationen alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Anwender. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie die NVD-Integrationen installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Vulnerability Response Integration with NVD.
4. Wählen Sie die Anwendungskachel aus.
   Es werden detaillierte Informationen zu der Anwendung angezeigt, die Sie installieren.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Wählen Sie **App anfordern** aus, und geben Sie Ihre Now Support -Anmeldeinformationen ein.
6. Wählen Sie **Abrufen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance (Instanz validieren)**.
8. Wählen Sie **Anforderung**aus.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Alle** > **Systemanwendungen** > **Anwendungen** > **Alle**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie **Installieren**aus.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Nächste Maßnahme

Änderungen nach der Erstinstallation finden Sie unter Optionale Änderung und Aktivitäten für die NVD-Integration.

National Vulnerability Database–API des NIST (National Vulnerability Database) des NIST (Nicht zugeordnete CPE) aktivieren

Um CPE-Daten (Common Platform Enumeration) für abgerufene CVE-Daten (Common Vulnerabilities and Exposures) zu erfassen, können Sie einen vollständigen Datenimport mit einer geplanten Aufgabe bei Bedarf durchführen.

Vorbereitungen

Die National Vulnerability Database Integration (NVD)–API-Integration (Unmapped CPE) des National Institute of Standards and Technology (NIST) erfasst Daten (CPE-Daten), die ein formales Namensformat, eine Methode zum Überprüfen von Namen anhand eines Systems und ein Beschreibungsformat für umfassen Binden von Text und Tests an einen Namen. Diese Informationen werden in einer zugehörigen Liste für einen NVD-Schwachstelleneintragsdatensatz gespeichert.

Erforderliche Rolle: sn_vul.vulnerability_admin oder App-Sec Manager

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **NVD** > **Integrationen**.
2. Wählen Sie die Integration NIST National Vulnerability Database Integration– API (Nicht zugeordnete CPE) aus.
3. Aktivieren Sie die Checkbox **Aktiv**.

> **Hinweis:**
> Die Integration ist so vorkonfiguriert, dass sie bei Bedarf ausgeführt wird. Wenn Sie die Integration aktivieren, wird sie automatisch nach der Integration der NIST NVD Integration-API (nur CVE) ausgeführt. Das Ändern anderer Integrationsparameter erfordert sowohl ServiceNow als auch Vulnerability Response sowie Fachwissen und kann zu unvollständigen Daten führen.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
   b. Wählen Sie NIST National Vulnerability Database Integration– API-Integration (nicht zugeordnetes CPE).
   c. Wählen Sie die Registerkarte **Integrationsdetails**.
   Unabhängig vom Wert des Felds „ **Importieren seit“** werden CPEs für alle abgerufenen CVEs abgerufen.
4. Wählen Sie **Jetzt ausführen aus**, um eine erste Integrationsausführung mit vollständiger Unterstützung durchzuführen.
   Nach Abschluss des ersten Imports werden die geplanten Importe von Delta-Daten fortgesetzt. Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus des NVD-Integrationsimports (National Vulnerability Database) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

NIST National Vulnerability Database–API aktivieren (nur CPE)

Um CPE-Daten (Common Platform Enumeration) zu erfassen, können Sie einen vollständigen Datenimport mit einer täglichen geplanten Aufgabe durchführen.

Vorbereitungen

Die National Vulnerability Database Integration (NVD)–API-Integration (nur CPE) des National Institute of Standards and Technology (NIST) erfasst Daten (CPE-Daten), die ein formales Namensformat, eine Methode zum Überprüfen von Namen anhand eines Systems und ein Beschreibungsformat für umfassen Binden von Text und Tests an einen Namen. Diese Informationen werden in einer Tabelle für angreifbare Software gespeichert.

Erforderliche Rolle: sn_vul.vulnerability_admin oder App-Sec Manager

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **NVD** > **Integrationen**.
2. Wählen Sie die Integration NIST National Vulnerability Database Integration–API (nur CPE) aus.
3. Aktivieren Sie die Checkbox **Aktiv**.
   - Die Integration ist für die tägliche Ausführung vorkonfiguriert. Das Ändern anderer Integrationsparameter erfordert Fachwissen von ServiceNow und kann zu unvollständigen Daten führen.
   - Durch die Aktivierung dieser Integration werden die Integrationen NIST National Vulnerability Database Integration-API (nur CVE) und NIST National Vulnerability Database Integration-API (Nicht zugeordnetes CPE) automatisch aktiviert und das zugehörige Ausführungsfeld auf „Bei Bedarf“ festgelegt.
   - Darüber hinaus löst eine erfolgreiche Integrationsausführung der NIST National Vulnerability Database Integration- API (nur CPE) automatisch die NIST National Vulnerability Database Integration API (nur CVE) aus. Durch den erfolgreichen Abschluss der Integration der NIST National Vulnerability Database-API (nur CVE) wird automatisch die Integration der NIST National Vulnerability Database-API (nicht zugeordnetes CPE) ausgelöst.

Hinweis:
Das Feld „Import seit Datum“ in der Integration der NIST National Vulnerability Database Integration – API (nur CPE) ist standardmäßig leer. Lassen Sie das Feld leer, um Daten der letzten 357 Tage abzurufen.

Um Verlaufsdaten während des ersten Imports aus dem NVD-Scan abzurufen, legen Sie ein Startdatum im Integrationsdatensatz der NIST National Vulnerability Database Integration – API (nur CPE) fest.

a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
b. Wählen Sie NIST National Vulnerability Database Integration– API Integration (nur CPE) aus.
c. Wählen Sie die Registerkarte **Integrationsdetails**.
d. Legen Sie den Wert des Felds **„Importieren seit“** auf das früheste Datum fest, das Sie abrufen möchten. Bei jedem erfolgreichen Import wird dieses Datum auf das Datum und die Uhrzeit des ausgewählten Tages zurückgesetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Jetzt ausführen aus**, um eine erste Integrationsausführung mit vollständiger Unterstützung durchzuführen.
   Nach Abschluss des ersten Imports werden die geplanten Importe von Delta-Daten fortgesetzt. Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus des NVD-Integrationsimports (National Vulnerability Database) an.

Optionale Änderung und Aktivitäten für die NVD-Integration

Konfigurieren Sie optionale Änderungen speziell für die NVD-Integrationen.

Hinweis:
Das Ändern anderer als der hier aufgeführten NVD-Integrationseinstellungen erfordert fortgeschrittene Kenntnisse ServiceNow von und Vulnerability Response und liegt außerhalb des Umfangs dieser Produktdokumentation.

Führen Sie einen manuellen NVD-Integrationsimport durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie einen vollständigen Datenimport unabhängig von der täglichen oder wöchentlichen geplanten Aufgabe durchführen.

Vorbereitungen

Hinweis:
Die Integrationen NIST National Vulnerability Database Integration-API (nur CPE) und NIST National Vulnerability Database Integration-API (Unmapped CPE) sind standardmäßig inaktiv. Siehe NIST National Vulnerability Database–API aktivieren (nur CPE) und National Vulnerability Database–API des NIST (National Vulnerability Database) des NIST (Nicht zugeordnete CPE) aktivieren, um weitere Informationen zu erhalten.

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie und Integration, z. B. Integration der NIST National Vulnerability Database Integration – API (nur CVE).
3. Wählen Sie **Jetzt ausführen**.

   Hinweis:
   Wenn die Integration der NIST National Vulnerability Database Integration-API (Unmapped CPE) aktiviert ist, werden zugehörige CPE-Daten in der zugehörigen Liste Schwachstellensoftware des NVD-Schwachstelleneintrags gespeichert. Weitere Informationen finden Sie unter Vulnerability Response Schwachstellenformularfelder.

4. Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus des NVD-Integrationsimports (National Vulnerability Database) an.

Zeigen Sie den Ausführungsstatus des NVD-Integrationsimports (National Vulnerability Database) an

Verwenden Sie die zugehörige Liste **„Integrationsausführungen für Schwachstellen“,** um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Nachbesserungsentscheidungen zu treffen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

So zeigen Sie den Ausführungsstatus des NVD-Integrationsimports an:

- Vulnerability Response und die Anwendung Vulnerability Response integration with NVD integration muss installiert und konfiguriert sein.
- Die NVD-Integrationsimporte müssen ausgeführt werden. Die Integration mit der NIST National Vulnerability Database Integration-API (nur CVE) wird standardmäßig ausgeführt.

Hinweis:
Die Integrationen NIST National Vulnerability Database Integration-API (nur CPE) und NIST National Vulnerability Database Integration-API (Nicht zugeordnetes CPE) sind standardmäßig inaktiv. Siehe NIST National Vulnerability Database–API aktivieren (nur CPE) und National Vulnerability Database–API des NIST (National Vulnerability Database) des NIST (Nicht zugeordnete CPE) aktivieren, um weitere Informationen zu erhalten.

Erforderliche Rolle: sn_vul.vulnerability_admin oder App-Sec Manager

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist.

Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er ebenfalls älter als eine Stunde ist. Wenn der zuletzt verarbeitete Datensatz älter als eine Stunde ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Wenn Sie nicht das Statusdiagramm für die NVD-Integrationsausführung verwenden, Navigieren Sie zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie einen **Link** für eine Integration aus.
3. Wählen Sie die zugehörige Liste **Integrationsausführungen für Schwachstellen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Stellen Sie sicher, dass alle Importe erfolgreich waren.

   Trouble?

   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

   - Netzwerkunterbrechung.
   - Ein Problem bei der Datenübertragung, das während der Transformation zu beschädigten Daten führt.

   Wenn eine dieser Bedingungen bei Ihnen auftritt, wählen Sie **Jetzt ausführen aus**, und führen Sie die Integration erneut aus.

Zugehörige Informationen

Vulnerability Response Schwachstellenformularfelder

CVEs zu Drittparteieinträgen hinzufügen

Common Vulnerability and Exposure (CVE) können sich auf eine einzelne Drittpartei-Schwachstelle beziehen. Es wird normalerweise während des Imports einer Drittanbieterintegration hinzugefügt. Sie können jedoch mehrere CVEs (Schwachstellen) manuell hinzufügen.

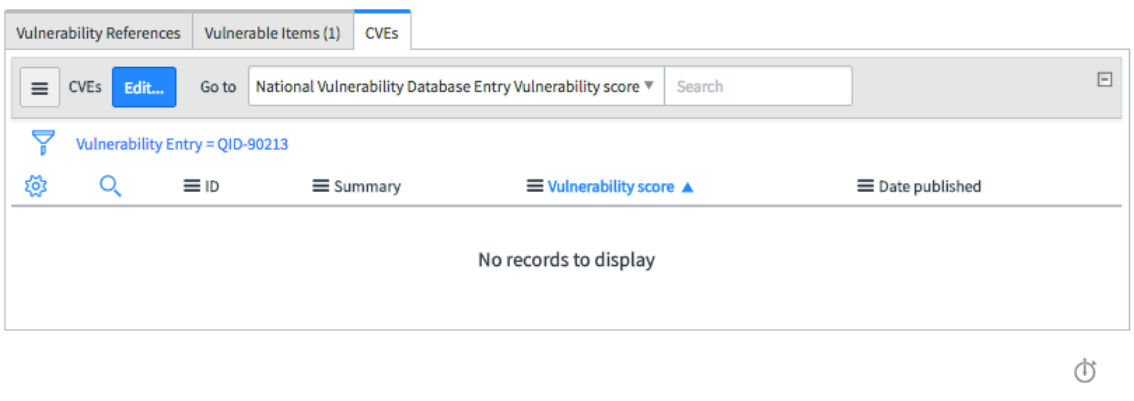
Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **Drittpartei**.
2. Öffnen Sie einen Datensatz.
3. Klicken Sie auf die Registerkarte Zugehörige Liste **CVEs**.



4. Klicken Sie auf **Bearbeiten**.
5. Wählen Sie aus, welche CVEs hinzugefügt werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können Bedingungsfilter verwenden, um die CVE-Sammlung zu verfeinern.

6. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Vulnerability Response Schwachstellenformularfelder

Zeigen Sie Schwachstellenbibliotheken Vulnerability Response an

Sie können Schwachstellendaten anzeigen, die aus der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder von Drittanbietern importiert wurden, um zu entscheiden, ob eine Korrekturaufgabe eskaliert werden soll.

Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken**.

   Informationen zu bestimmten Feldern finden Sie unter Vulnerability Response Schwachstellenformularfelder.

   Die folgenden Bibliotheken sind verfügbar:

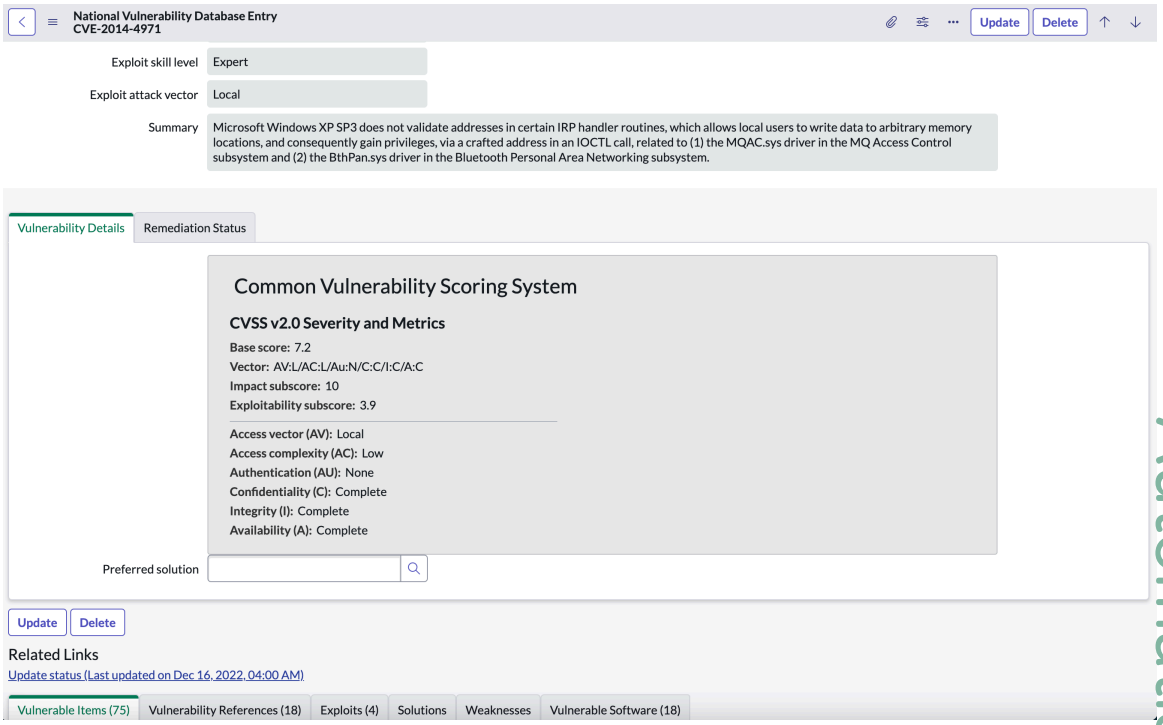
Bibliotheken	Beschreibung
NVD	Liste der von NVD gefundenen Schwachstellen, einschließlich Sicherheitsprüflisten, sicherheitsbezogener Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits.
CWE	Liste der von der Community entwickelten Software-Schwachstellentypen. Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Common Weakness Enumerations“ eskalieren, er dient nur zur Referenz.
Drittpartei	Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs.

2. Wählen Sie eine Bibliothek, um Schwachstellen anzuzeigen.
3. Klicken Sie auf einen Link in der Liste, um einen Datensatz zu öffnen.

   Ein CVE-Datensatz in der Bibliothek der Einträge in der US-Schwachstellendatenbank (National Vulnerabilities Database). Weitere Informationen finden Sie unter **Zugehörige Links**. Nach einem Datenimport können Sie eine Schwachstelle auswählen und deren Beziehungen zu angreifbaren Elementen, Exploits, möglichen Lösungen, potenziellen Patches und Verweisen auf KB-Artikel in der HI Knowledge Base untersuchen. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Solution Management installiert ist, können Sie eine bevorzugte Lösung in NVD-Datensätzen anzeigen, sofern eine verfügbar ist.



Integration von CISA Known Exploit Vulnerability (KEV)

Die Integration Vulnerability Response von mit dem CISA-Katalog für bekannte Schwachstellen (Known Exploited Vulnerabilities, KEVs) erfasst Daten, um Sie bei der effektiven Priorisierung und Behebung dieser Schwachstellen zu unterstützen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

CISA ermöglicht Behörden und Unternehmen die dringende und priorisierte Behebung von aktiv ausgenutzten Schwachstellen.

Über CISA

Die Cybersecurity and Infrastructure Security Agent (CISA) ist eine US-Behörde für Cybersicherheit und Infrastruktursicherheit, die einen Bericht zu den am häufigsten ausgenutzten Schwachstellen veröffentlicht. Die Integration mit Vulnerability Response ermöglicht die Zuordnung von Common Vulnerabilities and Exposures (CVE)-Schwachstellen zur Ergänzung der Daten in Ihrer -Instanz. Diese Informationen werden dann in der Tabelle „Drittpartei-Schwachstelleneinträge“ zusammengefasst. Für den Rollup zu den angreifbaren Elementen wird das früheste Fälligkeitsdatum berücksichtigt.

Hinweis:
Das Kontrollkästchen **„CISA vorhanden“** für CVEs, die von CISA abgerufen wurden.

Werte, die aus der CISA-Integration abgerufen wurden:

- CVE-ID
- Fälligkeitsdatum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Hinzugefügt am
- Lieferant/Projekt
- Produkt
- Known Ransomware (ab v21.0 von Vulnerability Responsewird ein neues Feld, **das bekanntermaßen in Ransomware-Kampagnen verwendet wird,** aus dem CISA-Katalog für bekannt ausgenutzte Schwachstellen (KEVs) erfasst. Dies wird durch die Kennzeichnung des Felds **„Bekannte Ransomware"** in der Datenbanktabelle „National Vulnerability Eintrag" angezeigt. Die Kennzeichnung wird auf der Ebene „Allgemeine Schwachstellen und Risiken" (Common Vulnerabilities and Exposures, CVE) festgelegt und ein Rollup bis zum Drittparteieintrag durchgeführt.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Geplante Aufgaben

Die CISA-Integration wird automatisch als tägliche geplante Aufgabe aufgerufen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response v16.5, v18.0 Vulnerability Response Integration mit CISA v1.0, v1.2	

CISA-Integration anzeigen

Um die CISA-Integration anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Administration** > **Integrationen** > **CISA-Integration für Known Exploit Vulnerability**.

Die folgenden Integrationen sind im Basissystem enthalten.

Hinweis:
Standardmäßig ist nur die CISA-Integration aktiv.

CISA-Integration

Integration	Beschreibung
Integration der Cybersicherheits- und Infrastruktursicherheitsbehörde (CISA).	Ruft CISA-Schwachstellendaten (CVE) ab und ergänzt die vorhandenen Schwachstellendaten. Diese Integration wird automatisch auf „Täglich" ausgeführt.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Zeigen Sie Schwachstellenbibliotheken Vulnerability Response an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitung der CISA-Integration

Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Die Integration von CISA Known Exploited Vulnerability setzt voraus, dass Sie mit der Cybersecurity & Infrastructure Security Agent (CISA) vertraut sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:

Nehmen Sie vor der Ausführung der CISA-Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:

Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Installieren Sie die Anwendung ServiceNow® Vulnerability Response Integration with CISA

Bevor Sie die Integration auf Ihrer -Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit der Known Exploited Vulnerability Advisor der Cybersecurity & Infrastructure Security Agent (CISA) in Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Stellen Sie sicher, dass die Anwendung Vulnerability Response Integration with NVD installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Installieren Sie die -Integration Vulnerability Response mit der US-Schwachstellendatenbank (National Vulnerability Database) des NIST.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen wurden, installiert der Systemadministrator [admin] die Anwendung und weist dem Schwachstellenmanager in Vulnerability ResponseBenutzer zu. Informationen zu Gruppenrollen in Vulnerability Response finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response. • Der Schwachstellenmanager überwacht die -Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie Vulnerability Response integration with CISA installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Vulnerability Response integration with CISA.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Wählen Sie **App anfordern** aus, und geben Sie Ihre Now Support -Anmeldeinformationen ein.
6. Wählen Sie **Abrufen aus**.
7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance (Instanz validieren)**.
8. Wählen Sie **Anforderung**aus.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie dann **Installieren**aus.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Nächste Maßnahme

Hinweis:
Für die Integration CISA ist keine Konfiguration erforderlich.

Informationen zur Integration des Exploit Prediction Bewertungssystems (EPSS).

Übersicht über die EPSS-Integration mit Vulnerability Response.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht

Die Integration des Exploit Prediction Scorering System (EPSS) importiert EPSS-Daten im Zusammenhang mit allgemeinen Schwachstellen und Gefährdungen (CVE) von First.org, um Schwachstellen zu priorisieren und zu beheben. Weitere Informationen finden Sie unter https://www.first.org . Das Exploit Prediction Scoreing System (EPSS) ist eine datengesteuerte Maßnahme zum Schätzen der Wahrscheinlichkeit, dass eine Software-Schwachstelle in der freien Produktion ausgenutzt wird. Das EPSS-Modell erzeugt eine Wahrscheinlichkeitspunktzahl zwischen 0 und 1 (0 und 100 %). Je höher die Punktzahl, desto größer ist die Wahrscheinlichkeit, dass eine Schwachstelle ausgenutzt wird.

Durch Datenimporte aus der EPSS-Integration werden die NVD-Daten in Ihrer Instanz zusätzlich angereichert. Wenn keine NVD-Datensätze vorhanden sind, wird ein Platzhalter in der CVE-Tabelle erstellt und EPSS-Details in derselben Tabelle hinzugefügt. Führen Sie diese Integration im Rahmen der Ersteinrichtung von Vulnerability Response und bevor

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie Schwachstellendaten mit dem Scannerprodukt eines Drittanbieters in Ihre Instanz importieren.

Wichtig:
Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist VR.System. Ändern Sie diesen Wert nicht.

Anfänglicher Import von Daten mit der EPSS-Integration

1. Führen Sie einen ersten Import von EPSS-Daten mit der First.org EPSS-Integration durch. Weitere Informationen finden Sie unter Konfigurieren Sie eine geplante Aufgabe, und führen Sie sie aus, um CVE-Datensätze mit EPSS-Daten zu aktualisieren.

   Wichtig:
   EPSS-Aktualisierungen werden standardmäßig **täglich** über den Integrationsdatensatz durchgeführt. Sie müssen sie konfigurieren, wenn sie als geplante Aufgabe ausgeführt werden sollen.

2. Drittpartei-Bibliotheken werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

   Wichtig:
   Es wird empfohlen, die Integrationen der NIST National Vulnerability Database Integration – API (nur CVE) vor EPSS durchzuführen.

Führen Sie die EPSS-Importe durch, bevor Sie Schwachstellendaten mit einem Drittanbieterprodukt importieren. Drittpartei-Bibliotheken werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

Wichtig:
Die folgende Integration ist im Basissystem enthalten. Die Integration ist standardmäßig aktiv.

Nach der ersten Ausführung werden die Integrationen von geplanten Aufgaben des Basissystems automatisch der Reihe nach ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Bei der Aktivierung der EPSS-Integration werden die Felder „EPSS-Punktzahl“, „EPSS-Perzentil“ und „EPSS – Zuletzt geändert“ der Tabelle „Schwachstelleneinträge“ hinzugefügt. Für vorhandene CVEs werden diese Felder nach erfolgreichem Abschluss des ersten Importauftrags automatisch aktualisiert. Wenn der Tabelle „Schwachstelleneinträge“ nach Abschluss der geplanten EPSS-Aufgabe neue CVEs hinzugefügt werden, geben die neu hinzugefügten CVEs ihre Quelle als EPSS an. Für die Punktzahlen wird ein Rollup für vorhandene TPEs von CVEs aus der NVD-Tabelle unter Verwendung des Basissystems `Rollup EPSS score from NVD to TPEs calculator`durchgeführt. Sie können auch den Rechner modifizieren. Weitere Informationen finden Sie unter Vulnerability Response Rollup-Rechner.

Zugehörige Informationen

Erstellen Sie einen Vulnerability Response -Rechner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie eine geplante Aufgabe, und führen Sie sie aus, um CVE-Datensätze mit EPSS-Daten zu aktualisieren

Passen Sie die geplante Aufgabe des Basissystems an, um CVE-Datensätze mit EPSS-Daten zu aktualisieren.

Vorbereitungen

Wichtig:
Sie müssen das Plugin Vulnerability Response integration with CISA (com.snc.vulnerability.cisa) herunterladen und aktivieren, um die EPSS-Integration zu aktivieren.

Im Folgenden finden Sie die Liste der neuen Felder, die der NVD-Tabelle zum Speichern von EPSS-Daten hinzugefügt wurden.

- EPSS-Punktzahl
- EPSS-Perzentil
- EPSS – Zuletzt geändert

Hinweis:
Konfigurieren Sie die Listenansicht oder Formularansicht je nach Anforderung, um neu hinzugefügte Felder anzuzeigen.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Durch Datenimporte aus der EPSS-Integration werden die NVD-Daten in Ihrer Instanz zusätzlich angereichert. Wenn keine NVD-Datensätze vorhanden sind, wird ein Platzhalter in der CVE-Tabelle erstellt und EPSS-Details in derselben Tabelle hinzugefügt. Führen Sie diese Integration als Teil der Ersteinrichtung von Vulnerability Response und nach dem Importieren von Schwachstellendaten in Ihre Instanz aus.

Hinweis:
Standardmäßig befindet sich die First.org-EPSS-Integration im Status **„Aktiv“**. Die geplante Aufgabe des Basissystems ist standardmäßig auf die tägliche Ausführung konfiguriert.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
2. Suchen und wählen Sie First.org EPSS-Integration.
3. Ändern Sie die Felder nach Bedarf.
4. Klicken Sie mit der rechten Maustaste auf den Header, um Ihre Änderungen zu **speichern**.
5. Wählen Sie **Jetzt ausführen aus**, um die geplante Aufgabe sofort auszuführen.
   Sie kehren zur Ansicht „Schwachstellenintegrationen“ zurück.
6. Auswahlvorgang **First.org-EPSS** > **Registerkarte „Integrationsausführungen für Schwachstellen“.** um den Fortschritt des Imports anzuzeigen.
   Bei erfolgreichem Abschluss der geplanten Aufgabe werden die EPSS-Punktzahlen, das Perzentil und die Zeitstempel der letzten geänderten EPSS-Punktzahl in den CVEs aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Weitere Informationen finden Sie unter Fügen Sie die Bedingung „EPSS-Punktzahl“ in der Geschäftsregel „Risikorechner“ hinzu.
- Informationen zu den importierten Einträgen finden Sie unter Zeigen Sie Schwachstellenbibliotheken Vulnerability Response an.

Fügen Sie die Bedingung „EPSS-Punktzahl“ in der Geschäftsregel „Risikorechner“ hinzu

Ändern Sie die Business-Regel, um dem Risikorechner die Bedingung der EPSS-Punktzahl hinzuzufügen.

Vorbereitungen

Hinweis:
Das folgende Verfahren ist erforderlich, damit die EPSS-Updates für Schwachstellen ein Rolldown zu den angreifbaren Elementen durchführen.

Erforderliche Rolle: sn_vul.manage_risk_score_configuration

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regel**.
2. Suchen Sie nach **„Neuberechnungskennzeichnung festlegen“**.

   Hinweis:
   Es gibt zwei `Set recalculate flag` -Geschäftsregeln. Sie können eine der beiden Optionen verwenden.

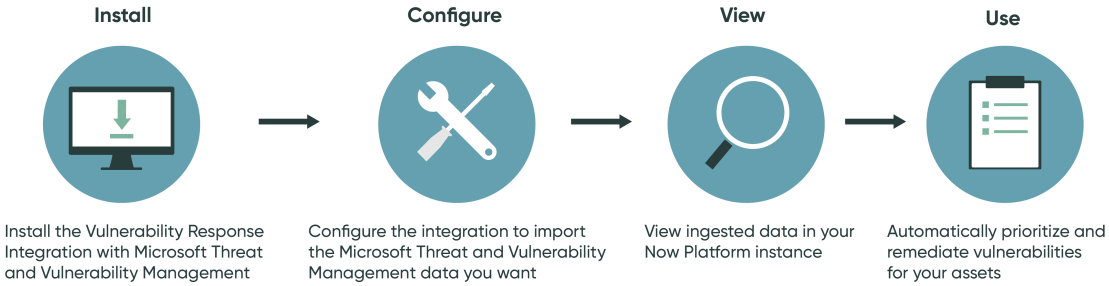
3. Navigieren Sie zur Registerkarte **Zeitpunkt für Ausführung**.
4. Wählen Sie **„ODER“-Klausel hinzufügen**, und wählen Sie EPSS-Punktzahl im **Auswahlfeld** sowie Änderungen im Feld **Operator auswählen aus**.
5. Wählen Sie **Aktualisieren**.

Informationen zur Schwachstellenintegration von Microsoft Threat and Vulnerability Management

Die Vulnerability Response -Integration mit Microsoft Threat and Vulnerability Management (MS TVM) verwendet aus MS TVM importierte Daten, um Sie bei der Priorisierung und Behebung von Schwachstellen für Ihre Assets zu unterstützen. Die Anwendung ist mit einem separaten Abonnement aus dem ServiceNow Storeverfügbar.

Sie können die MS TVM-Schwachstellenintegration verwenden, um Scannerdaten von Drittanbietern zu Ihren Assets und Schwachstellen zu importieren. Anschließend können Sie in den Dashboards Vulnerability Response Berichte zu Schwachstellen und angreifbaren Elementen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response Integration mit MS TVM v2.2	Weitere Informationen zu veröffentlichten Versionen der Anwendung Vulnerability Response, zur Kompatibilität und zu Schemaänderungen finden Sie im Artikel Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen [KB0856498] in der HI Knowledge Base.

Domain Separation und MS TVM

Importieren Sie Daten einer Schwachstellenintegration in eine angegebene Domäne, indem Sie in dieser Domäne einen Benutzer zuweisen, der die Integrationen ausführen soll. Informationen zum Erstellen von domänengetrennten Importen für die MS TVM-Schwachstellenintegration finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration.

Begriffe und wichtige Funktionen der Integrationen

Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in Ihrer Instanz Now Platform erstellt, wenn:

- Eine importierte Schwachstelle aus einem Drittanbieterscanner wird mit einem vorhandenen Asset (Konfigurationselement) in Ihrem CMDBabgeglichen. Das MS TVM-Produkt bezeichnet diese Übereinstimmungen als Schwachstellen.
- Eine importierte Schwachstelle aus einem Drittanbieterscanner wird keinem vorhandenen Asset in Ihrem CMDBzugeordnet. In diesem Fall wird auch ein nicht abgeglichenes Configuration Item (CI) mit einem angreifbaren Element erstellt.

  Verwenden Sie die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE), um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI keinem Host zugeordnet werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt.

Einträge für Drittpartei-Schwachstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einträge für Schwachstellen von Drittparteien werden aus Scannern von Drittparteien wie MS TVM importiert und in der Tabelle „Schwachstelleneinträge von Drittparteien“ in Ihrer Instanz Now Platform aufgeführt. Außerdem werden Einträge in die National Vulnerability Database (CVE) aus MS TVM importiert. Die Exploit-Informationen, die diesen beiden Arten von Einträgen zugeordnet sind, stammen aus MS TVM. Diese Exploit-Informationen können für die Risikoberechnung verwendet werden.

Hinweis:
Eine Drittpartei-Schwachstelle wird nur für Schwachstellen abgerufen, denen kein CVE zugewiesen ist. MS TVM kann einen temporären Namen für die Schwachstelle hinzufügen, z. B. TVM-XXXX-XXXX. Dieser Name wird aktualisiert, nachdem eine CVE-ID zugewiesen wurde.

Konfigurationselement bzw. Configuration Item (CI)

CIs sind die vorhandenen Assets, die in Ihren CMDBaufgeführt sind.

Erkanntes Element

Erkannte Elemente sind die Assets, die aus dem Import des MS TVM-Computers erfasst werden und vorhandenen CIs in Ihrem CMDBentsprechen.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der CI-Klasse ohne Übereinstimmung von CMDBerstellt. Aktivieren Sie das Plugin „CMDB CI Class Models“. Die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) erstellt CIs mithilfe neuer Klassen. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt. Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden die Datensätze des erkannten Elements entsprechend aktualisiert. Erkannte Elemente geben Ihnen Einblick in die Art und Weise, wie Assets identifiziert und CIs in CMDBzugeordnet werden.

CI-Suchregeln

Wenn Daten aus MS TVM importiert werden, verwendet Vulnerability Response automatisch Maschinendaten (Asset-Daten), um nach Übereinstimmungen in CMDBzu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und zu VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden.

Instanz

Eine Instanz bezieht sich auf mehrere Konten von MS TVM. Jeder Account kann eine Instanz in der MS TVM-Anwendung sein.

Integration

Eine Integration ist eine geplante Aufgabe, die Informationen von einer Drittanbieterquelle abruft, z. B. die Integration der MS TVM-Computer.

Bereitstellung

Wenn eine Integration mehrere Quellen unterstützt, wird das Vorhandensein einer einzelnen Integration als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie in Ihrer Umgebung über mehrere Bereitstellungen von MS TVM verfügen.

Die MS TVM-Integration enthält außerdem die folgenden wichtigen Funktionen:

- Sie können die Assets in Ihrer Umgebung identifizieren und die CIs für Ihre vorhandenen erkannten Elemente, angreifbaren Elemente und Erkennungsdatensätze aktualisieren, um weitere Details zu Ihren Schwachstellen zu erhalten.
- Sie können planen, wann die Aufgaben für alle MS TVM-Integrationen ausgeführt werden sollen. Sie können geplante Aufgaben auch bei Bedarf ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können angreifbare Elemente gruppieren.
- Sie können CI-Suchregeln konfigurieren, um zu definieren, wie die Asset-Daten aus Drittanbieterquellen zum Identifizieren von CIs in Ihrem CMDBverwendet werden.

Erforderliche Now Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrer Instanz Now Platform.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Administrator

Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung MS TVM zu installieren. Wenn dies nicht zugewiesen ist, weist der Administrator im Setup-Assistenten den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu.

sn_vul.vulnerability_admin

Nach der Zuweisung schließt der Schwachstellen-Administrator die Konfiguration der MS TVM-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle Vulnerability Response -Anwendungen und -Regeln für installierte Drittanbieterintegrationen.

sn_vul_msft_tvm.configure_integration

Diese Rolle enthält die granulare Rolle sn_vul_msft_tvm.read_integration. Benutzer mit dieser Rolle können Vulnerability Response Integration mit der Anwendung Microsoft Threat and Vulnerability Management konfigurieren.

sn_vul_msft_tvm.read_integration

Benutzer mit dieser Rolle können die Datensätze der Anwendung „Vulnerability Response Integration with the Microsoft Threat and Vulnerability Management“ nur anzeigen.

Vulnerability Response-Gruppe

Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen „sn_vul.read_all“ und „sn_vul.remediation_owner“ automatisch.

MS TVM-Integrationen

Mehrere Quellen werden für alle MS TVM-Integrationen unterstützt. Sie können über den Setup-Assistenten in Vulnerability Responsemehrere Instanzen der folgenden Integrationen in Ihrer Umgebung hinzufügen und bereitstellen. Außerdem installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration mit der Anwendung MS TVM über den Setup-Assistenten.

Um die MS TVM-Integrationen anzuzeigen, navigieren Sie zu **Microsoft TVM-Schwachstellenintegration** > **Administration** > **Integrationen**. Vulnerability Response bietet Integrationen mit MS TVM-Endpunkten, um die Daten gemäß den geplanten Zeitintervallen zu importieren. Die folgenden Integrationen sind im Basissystem enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MS TVM-Integrationen

Ausführungssequenz	Zeitplan	Integration	Beschreibung
1	Täglich	Microsoft TVM-Empfehlungsintegration	Ruft eine Liste aller umsetzbaren Sicherheitsempfehlungen zum Beheben der Schwachstellen ab.
2	Täglich	Integration von Microsoft TVM Vulnerability (CVE).	Ruft eine Liste der Einträge in der US-Schwachstellendatenbank (National Schwachstellendatenbank) und Schwachstelleneinträge von Drittparteien sowie deren Exploit-Informationen ab.
3	Täglich	Integration von Microsoft TVM-Computern	Ruft alle Asset-(Computer-)Daten, einschließlich Computer-Tags, von Microsoft TVM ab und verarbeitet sie in Ihrer Instanz.
4	Wöchentlich **Hinweis:** Nach der Installation wird diese Integration automatisch nach dem Import der Computer ausgeführt.	Microsoft TVM-Computer – Schwachstellen-Integration (vollständiger Import)	Ruft alle offenen Schwachstellen für alle Assets ab.
5	Täglich	Microsoft TVM Machines Vulnerabilities Integration (Delta-Import)	Ruft alle Informationen ab, die sich im vollständigen Import von Schwachstellen der Organisation geändert haben, einschließlich der neuen, behobenen und aktualisierten Schwachstellen.

Angreifbare Elemente werden gemäß den von Ihnen festgelegten Gruppenregeln in Korrekturaufgaben gruppiert und werden basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Vulnerability Response Übersicht über Zuweisungsregeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Suchregeln

Wenn Daten aus MS TVM importiert werden, verwendet Vulnerability Response automatisch Maschinendaten (Asset-Daten), um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und zu VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

Hinweis:
Sobald Sie eine Regel entfernt haben, können Sie sie nicht wiederherstellen. Anstatt eine vorhandene Regel zu entfernen, sollten Sie sie deaktivieren.

Die folgenden MS TVM-Suchregeln sind im Lieferumfang des Basissystems enthalten:

- MAC_ADDRESS
- FQDN
- IP

Hinweis:
Sie können mehrere Werte für die IP_ADDRESS und MAC_ADDRESS eines Assets verwenden. Eine CI-Suchregel berücksichtigt alle Werte für den Abgleich.

Erkannte Elemente

Sie können die CIs anzeigen, die während eines Imports aus der Integration von MS TVM-Computern erkannt wurden.

Hinweis:
Der Standardfilter für diese Liste ist auf Nicht abgeglichenfestgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen finden Sie unter Erkannte Elemente.

Maschinen-Tags

Computer-Tags, auch Host-Tags genannt, werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie weisen Ihren Computern Tags zu.

Alle Computer-Tags werden als Teil der MS TVM Machines-Integration importiert. Computer-Tags werden im Allgemeinen zum Filtern in Zuweisungsregeln für Vulnerability Response und Regeln für Korrekturaufgaben verwendet. Die Tags werden im Formular „Erkanntes Element“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Führen Sie die MS TVM-Computerintegration aus, bevor Sie in der Anwendung Vulnerability ResponseVulnerability Response Regeln für Zuweisungs- oder Korrekturaufgaben vom Typ „“ erstellen, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein Paris-Tag erstellt wird, kann kein PARIS-Tag in der Maschinen-Tag-Tabelle gespeichert werden. Paris und PARIS werden vom System als dasselbe Maschinen-Tag betrachtet. Welches Tag zuerst importiert wird, ist das Tag, das gespeichert und erkannt wird.
- Die Verwendung von Computer-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Gruppenschlüssel sind Spalten in der Tabelle der Korrekturaufgaben, während Maschinen-Tags nur im Bedingungsgenerator verwendet werden sollen.
- Computer-Tags werden von der globalen Systemeigenschaft sn_vul.import_host_tags gesteuert. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Durch das Deaktivieren von Tags werden sie für alle Now Platform® -Instanzen deaktiviert.

Nächste Schritte

Nachdem Sie die Vulnerability Response -Integration mit Microsoft Threat and Vulnerability Management von ServiceNow® Storeheruntergeladen haben, werden Installation und Konfiguration durch den Setup-Assistenten in Vulnerability Responseunterstützt. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration mit der Anwendung MS TVM mithilfe des Setup-Assistenten.

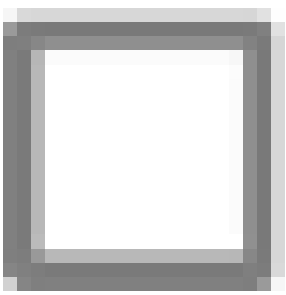
Vorbereitung auf die Microsoft Threat and Vulnerability Management Vulnerability Integration

Sie können sich auf die Schwachstellenintegration ServiceNow® von Microsoft Threat and Vulnerability Management (MS TVM) vorbereiten, indem Sie Setupaufgaben ausführen.

Bevor Sie eine Prüfliste verwenden

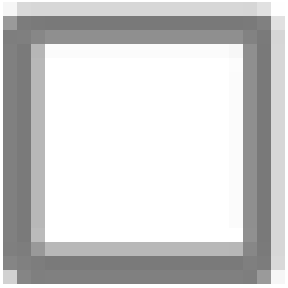
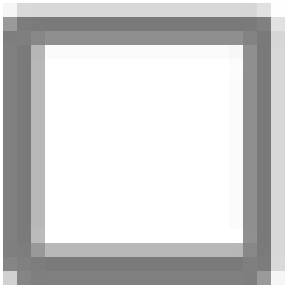
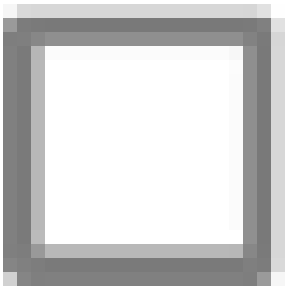
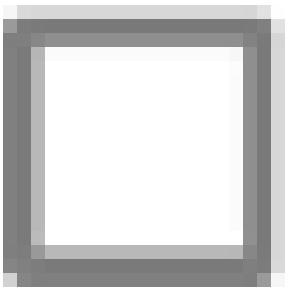
Um die Integration Vulnerability Response von mit der MS TVM-Anwendung zu installieren und zu konfigurieren, können Sie die folgende Prüfliste ausdrucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in Ihre Instanz Now Platform® importieren.

Prüfliste für die Vorbereitung der Integration

Aufgabe	Beschreibung
	Vergewissern Sie sich, dass Sie über einen der folgenden Informationssätze verfügen: • ClientSecret, ClientId und TenantId für Ihr MS TVM-Konto • Username, Password, ClientId und TenantId für Ihr MS TVM-Konto. Diese Informationen finden Sie unter Richten Sie MicrosoftMicrosoft Azure Event Hubs Azure für die MS TVM-Integration ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

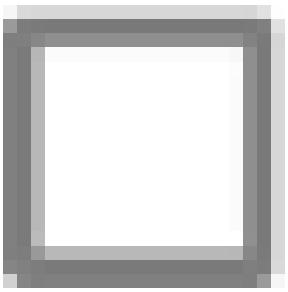
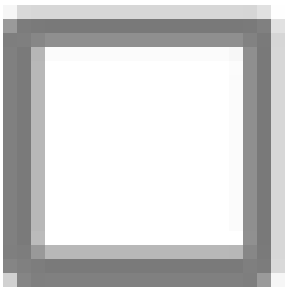
Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
	Wenn die Anwendung Vulnerability Response [] noch nicht installiert und aktiviert ist, installieren Sie die Anwendung , bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 14.0 von Vulnerability Response oder höher.
	Wenn Sie die Anwendung noch nicht in Ihrer -Instanz haben, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response integration with MS TVM (Integration von []) mit MS TVM auf Ihre Instanz Now Platform® herunter. Weitere Informationen finden Sie unter .
	Schätzen Sie die Anzahl der zu importierenden angreifbaren Elemente. Vergewissern Sie sich, dass Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie voraussichtlich importieren werden. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support ServiceNow® von .
	Vergewissern Sie sich, dass Sie über die folgenden Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren: **Administrator** Verwendet den Setup-Assistenten, um die Vulnerability Response-Integration mit der Anwendung MS TVM zu installieren. Wenn dies nicht zugewiesen ist, weist der Administrator im Setup-Assistenten den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu. **sn_vul.vulnerability_admin** Schließt die Konfiguration der MS TVM-Integration ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Dieser Administrator konfiguriert alle VR-Anwendungen und -Regeln sowie Integrationen von Drittanbietern. **sn_vul_msft_tvm.configure_integration** Konfiguriert die MS TVM-Schwachstellen-Integration. Diese Rolle enthält die granulare Rolle sn_vul_msft_tvm.read_integration. **sn_vul_msft_tvm.read_integration**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
	Zeigt Datensätze der MS TVM-Schwachstellenintegration an (und liest sie). **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen „sn_vul.read_all“ und „sn_vul.remediation_owner“ automatisch. Wenn dies noch nicht geschehen ist, können Sie zusätzliche Gruppen erstellen und Benutzer mit dem Benutzerverwaltungsmodul in Ihrer Instanz hinzufügen, bevor Sie den Setup-Assistenten verwenden. Weitere Informationen finden Sie unter Benutzergruppen erstellen. Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.
	Installieren Sie die Integration Vulnerability Response mit NVD, und führen Sie die Integration der US-Schwachstellendatenbank (National Vulnerability Database Integration) des NIST API – API (nur CVE) aus.
	Um die Leistung beim ersten Import zu verbessern, können Sie bestimmte Funktionen, Regeln oder Aufgaben in Ihrer Instanz deaktivieren. • Deaktivieren Sie die Schwachstellen-Rechner, wenn Sie sie nicht verwenden. Diese Rechner und die von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für ein angreifbares Element erstellt oder aktualisiert wird. Weitere Informationen finden Sie unter Standard-Schwachstellen-Rechner deaktivieren, wenn er nicht verwendet wird. • Während des ersten Imports von Datensätzen können bestimmte Benachrichtigungs-Business-Regeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung der Erfassung auswirken kann.

Sie sind bereit für Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration mit der Anwendung MS TVM mithilfe des Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie MicrosoftMicrosoft Azure Event Hubs Azure für die MS TVM-Integration ein

Richten Sie Ihr Konto im Azure-Portal MicrosoftMicrosoft Azure Event Hubs ein, um Remotezugriff auf die Microsoft Threat and Vulnerability Management-API (MS TVM) zu erhalten. Sie benötigen diesen Account, um auf den MS TVM-Mandanten zuzugreifen und Informationen zu Computern, Schwachstellen und Sicherheitsempfehlungen zu sammeln.

Vorbereitungen

Erforderliche Rolle: MicrosoftMicrosoft Azure Event Hubs Azure-Portaladministrator.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Setupaufgaben in Ihrem MicrosoftMicrosoft Azure Event Hubs Azure-Portal aus, bevor Sie die Anwendung ServiceNow® für diese Integration installieren.

Um sicherzustellen, dass Sie Zugriff auf die neuesten Inhalte haben, konsultieren Sie die Microsoft-Dokument -Website. Wenn Sie im Azure-Portal MicrosoftMicrosoft Azure Event Hubs keine Anwendungs-ID für die OAuth 2.0-Authentifizierung erstellt haben, führen Sie die Schritte in diesem Verfahren aus.

Prozedur

1. Melden Sie sich beim Azure-Portal MicrosoftMicrosoft Azure Event Hubs mit den Anmeldeinformationen Ihres Azure-Portal-Administrators an.
2. Klicken Sie im linken Navigationsbereich der Startseite auf **Azure Active Directory**.
3. Klicken Sie im Übersichtsbereich auf **App-Registrierungen (Vorschau)**.
4. Klicken Sie im Bereich App-Registrierungen (Vorschau) auf **Neue Registrierung**.
   Das Formular „Anwendung registrieren“ wird angezeigt.
5. Füllen Sie die Felder des Formulars aus.

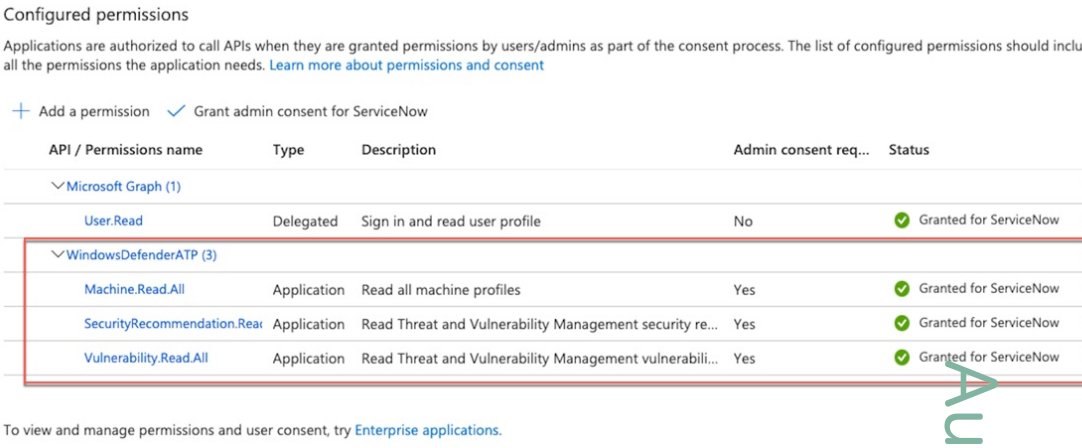
Registrieren Sie ein Anwendungsformular

Feld	Beschreibung
Name	Name für die Anwendung. In diesem Beispiel ist ServiceNow MS TVM Integration eingegeben.
Unterstützte Account-Typen	Klicken Sie für diesen Account unter Unterstützte Accounttypen **auf Accounts in diesem Organisationsverzeichnis (nur ServiceNow – Einzelner Mandant)**.
Umleitungs-URL (optional)	Wenn Sie einen Wert für dieses Feld eingeben, wird es von der Integration nicht verwendet.

6. Klicken Sie auf **registrieren**.
   Die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) werden erstellt. Geben Sie diese Werte auf der Konfigurationsseite in die Felder **Client-ID** und **Mandanten-ID** während des Konfigurationsschritts im Setup-Assistenten der VR-TVM-Integration ServiceNow ein. Dieser Schritt wurde in Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration mit der Anwendung MS TVM mithilfe des Setup-Assistentenbeschrieben.
7. Wenn im Bereich ServiceNow MS TVM-Integration die Anwendungs-ID (Client) angezeigt wird, klicken Sie auf **API-Berechtigungen anzeigen**.
8. Navigieren zu **Fordern Sie API-Berechtigungen an** > **APIs, die meine Organisation verwendet**und klicken Sie dann auf **Windows Defender ATP**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie im Bereich ServiceNow MS TVM Integration – API-Berechtigungen auf **Add a Permission (Berechtigung hinzufügen)**.
10. Gewähren Sie Lesezugriff für Computer, Schwachstellen und



Sicherheitsempfehlungen.

11. Klicken Sie auf **Administratorzustimmung erteilen für**<your organization name> .

Hinweis:
Um sich als Anwendung von einer Instanz ServiceNow aus zu authentifizieren, gehen Sie wie folgt vor:

a. Navigieren zu **ServiceNow MS TVM Integration** > **Zertifikate und Geheimnisse**und klicken Sie dann auf **Neuer Clientschlüssel**.

b. Füllen Sie die Felder des Formulars aus.

Formular „Geheime Clientschlüssel“.

Feld	Beschreibung
Beschreibung	Name der Anwendung.
Läuft ab	Ablaufdatum.

c. Klicken Sie auf **Hinzufügen**.

Das Feld **Wert** wird mit dem neuen geheimen Clientschlüssel ausgefüllt, der Ihr neues Passwort ist.

Hinweis:
Sie benötigen dieses Passwort, wenn Sie die Integration in Ihrer Instanz Now Platform konfigurieren. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration mit der Anwendung MS TVM mithilfe des Setup-Assistenten.

d. Speichern Sie dieses Passwort an einem sicheren Ort. Nachdem Sie diese Seite verlassen haben, ist dieses Passwort nicht mehr verfügbar.

Sie haben erfolgreich eine Anwendungs-ID für die Authentifizierung im Azure-Portal MicrosoftMicrosoft Azure Event Hubs erstellt.

Nächste Maßnahme

Sie sind bereit, Ihre Instanz Now Platform® für die Integration einzurichten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration mit der Anwendung MS TVM mithilfe des Setup-Assistenten

Installieren und konfigurieren Sie die Vulnerability Response -Integration mit der Anwendung Microsoft Threat and Vulnerability Management (MS TVM), damit Sie die aus MS TVM importierten Daten verwenden können, um Schwachstellen für Ihre Assets zu priorisieren und zu beheben.

Vorbereitungen

Bevor Sie die ServiceNow® Microsoft Threat and Vulnerability Management Vulnerability-Integration ausführen, müssen Sie die Anwendung Vulnerability Response Integration with Microsoft Threat and Vulnerability Management aus dem ServiceNow Store herunterladen und mit dem Setup-Assistenten in der Anwendung Vulnerability Response installieren und konfigurieren.

Bevor Sie die Anwendung MS TVM installieren, vergewissern Sie sich, dass Sie alle Elemente der Prüfliste Vorbereitung auf die Microsoft Threat and Vulnerability Management Vulnerability Integration abgeschlossen haben. Informationen zum Einrichten Ihres MicrosoftMicrosoft Azure Event Hubs Azure-Kontos finden Sie unter Richten Sie MicrosoftMicrosoft Azure Event Hubs Azure für die MS TVM-Integration ein.

Erforderliche Rolle: admin für die erstmalige Zuweisung der Rolle sn_vul.vulnerability_admin und die Installation der Anwendung Microsoft Threat and Vulnerability Management im Setup-Assistenten. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)), um die Anwendung nach der Installation im Setup-Assistenten zu konfigurieren.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie das folgende Verfahren durch, bevor Sie die MS TVM-Integration installieren und konfigurieren.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz von verfügbar sind.

2. Suchen Sie die Kachel **Microsoft Threat and Vulnerability Management,** und klicken Sie auf **Installieren**.

   Die Anwendung Vulnerability Response Integration with Microsoft Threat and Vulnerability Management, die Sie von ServiceNow Store heruntergeladen haben, wird installiert.

3. Folgen Sie den Eingabeaufforderungen im Setup-Assistenten, um mit der Installation fortzufahren. Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.

Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie zu **Integrationskonfiguration** > **Scannerintegrationen** im Setup-Assistenten, um mit der Konfiguration fortzufahren. Weitere Informationen zur Ergänzung der Eingabeaufforderungen im Setup-Assistenten finden Sie unter Konfigurieren Sie die MS TVM-Schwachstellenintegration mit dem Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufeinstellungen für die Microsoft Threat and Vulnerability Management-Integration

Sie können Datenabrufeinstellungen verwenden, um den Typ und Umfang der Daten zu bestimmen, die Sie aus der Schwachstellenintegration von ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) in Ihre Instanz Now Platform® importieren möchten.

Mit den Einstellungen zum Datenabruf können Sie steuern, welche Daten Sie importieren möchten. Sie können die Werte dieser Filter in Integrationsinstanzen festlegen. Um die Integrationsinstanzen anzuzeigen, navigieren Sie zu **Microsoft Threat and Vulnerability Management – Schwachstellen-Integration** > **Integrationsinstanzen** und klicken Sie auf Ihre MS TVM-Integration.

Klicken Sie auf der Seite „Integrationsinstanz“ auf die **Option Integrationsinstanzparameter**, um eine Liste der Parameter anzuzeigen, oder klicken Sie auf die Registerkarte **Schwachstellenintegrationen,** um einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung zu erhalten.

Einstellungen und Filter für den Datenabruf für die MS TVM-Integrationen in Ihrer Instanz Now Platform .

Die folgenden Einstellungen sind für die MS TVM-Integrationen in Ihrer Instanz Now Platform verfügbar. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ Ihrer Instanz Now Platform angezeigt. Unter Umständen möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardeinstellungen beibehalten.

MS TVM

VI_size_limit

Definiert die Anzahl der Datensätze für angreifbare Elemente, die in den Ergebnissatz der MS TVM-Integration für Computer-Schwachstellen aufgenommen werden sollen. Diese Einstellung muss im Format „int32“ vorliegen. Der Standardwert ist 2.000.

„vulnerabilities_size_limit“

Definiert die Anzahl der Schwachstellen-Datensätze, die in den Ergebnissatz der MS TVM Vulnerability-Integration (CVE) aufgenommen werden sollen. Diese Einstellung muss im Format „int32“ vorliegen. Der Standardwert ist 2.000.

Recommendations_size_limit

Definiert die Anzahl der Schwachstellen-Datensätze, die in den Ergebnissatz aus der MS TVM-Empfehlungsintegration aufgenommen werden sollen. Diese Einstellung muss im Format „int32“ vorliegen. Der Standardwert ist 2.000.

asset_size_limit

Definiert die Anzahl der Schwachstellen-Datensätze, die in den Ergebnissatz aus der MS TVM-Computer-Integration aufgenommen werden sollen. Diese Einstellung muss im Format „int32“ vorliegen. Der Standardwert ist 2.000.

maschine_filter

Filtert die Computer, die von MS TVM stammen. Dieser Filter wird auf die Integration von MS TVM-Computern angewendet. Der Standardwert dient zum Einbeziehen von Computern, bei denen „onBoardingStatus“ auf „onBoarded“ festgelegt ist.

REST-Nachrichten für die Microsoft Threat and Vulnerability Management-Schwachstellenintegration

Sie können die REST-Nachrichten für die Schwachstellenintegration ServiceNow® von Microsoft Threat and Vulnerability Management (MS TVM) verwenden, um Aufrufe an die MS TVM-API zu tätigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MS TVM-Zugriffstoken

Sie können auch die REST-Nachrichten für das MS TVM-Zugriffstoken verwenden, um das Zugriffstoken von der MS TVM-API abzurufen und REST API-Anforderungen zu authentifizieren. Änderungen an der Aufzeichnungsmethode der REST-Nachricht wirken sich auf die Authentifizierungsanforderungen aus, die an MS TVM gesendet werden.

MS TVM-Integration

Sie können die REST-Nachricht für die MS TVM-Integration verwenden, um Informationen von MS TVM abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen aus, die an MS TVM zum Abrufen von Informationen gerichtet werden. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methoden

REST-Methode	Beschreibung der Methode
GET-Schwachstellen	Ruft Schwachstellen- und Exploit-Informationen aus MS TVM ab.
GET Software-Schwachstellen nach Computer	Ruft alle offenen Schwachstellen ab.
GET-Empfehlungen	Ruft die Liste aller umsetzbaren Sicherheitsempfehlungen ab, die sich auf die Organisation auswirken.
GET-Computer	Ruft die Sammlung von Assets ab.
GET Software-Schwachstellen-Changes nach Computer	Ruft alle Informationen ab, die sich im vollständigen Import von Schwachstellen der Organisation geändert haben, einschließlich neuer, behobener und aktualisierter Schwachstellen.

Datentransformation für die Schwachstellen-Integration von Microsoft Threat and Vulnerability Management

Nachdem Sie die zu importierenden Daten identifiziert haben, werden die Daten aus der Anwendung ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer -Instanz transformiert.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „Normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen wandeln importierte MicrosoftMicrosoft Azure Event Hubs Schweregrade von Drittpartei-Schwachstellen in Standardschweregrade um, um sie in Ihrer -Instanz zu verarbeiten. Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung.

MS TVM-Computer – Import

Die Daten von den importierten Computern werden zuerst in die Tabelle „MS TVM-Computerimport“ [sn_vul_msft_tvm_maschines_import] geladen.

Die MS TVM-Maschinentransformation wird verwendet, um die importierten Maschineninformationen umzuwandeln.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Verarbeitung von Daten aus dem MS TVM-Computerimport.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach **Microsoft TVM Machines Transformieren**.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

MS TVM-Maschinen transformieren Zuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID für Assets. Diese ID ist der source_id des Datensatzes des erkannten Elements zugeordnet.
u_ipaddresses.macAddress	mac_address	MAC-Adresse, die von der API dem Host-MAC-Adressfeld des cmdb_ci-Datensatzes zugeordnet wird.
u_ipaddresses.ipAddress	ip_address	IP-Adressfeld, das dem IP-Adressfeld des cmdb_ci-Datensatzes zugeordnet ist.
u_lastseen	last_scan_date	Feld, das dem Feld „last_scan_date“ im Datensatz des erkannten Elements zugeordnet ist.
u_maschinetags		Tags, die in „sn_sec_cmn_host_tag“ gespeichert sind Die Zuordnung von Tags zu Assets wird in „sn_sec_cmn_m2m_src_ci_tag“ gespeichert.
u_osplatform	os	Feld, das dem Feld „os“ im Datensatz „cmdb_ci“ zugeordnet ist.
u_computerdnsname	fqdn	Feld, das das Feld „dnsname“ aus der API dem Feld „fqdn“ im Datensatz „cmdb_ci“ zuordnet.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Timing und Zweck des MS TVM Machines-Transformationszuordnungsskripts

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Aktualisieren von Werten auf dem Host und Überprüfen, ob der Host

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	vorhanden ist, verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Umfangsvariablen (sn_vul_msft_tvm). Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, mit dem die Anzahl der erstellten, aktualisierten und ignorierten CIs festgelegt wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Die MicrosoftTVMMachineProcessor-Skripteinbindung wird vom onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe aus der Integration der Microsoft TVM-Computer und wandelt sie in ein CI um. Alle Änderungen an dieser Skripteinbindung können die Transformation der Daten der Microsoft TVM-Computer in der CI-Tabelle und der Tabelle „Erkannte Elemente“ ändern.

MS TVM – Schwachstellen-Integration

Die importierten Schwachstellendaten werden zuerst in die Microsoft TVM-Tabelle „CVE-Import (Schwachstellen)“ [sn_vul_msft_tvm_vulnerabilities_import] geladen.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Verarbeitung von Daten aus dem MS TVM-Schwachstellenimport.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach der **Microsoft TVM-Transformation für Schwachstellen**.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Transformationszuordnungsfelder für Microsoft TVM-Schwachstellen

Quellenfeld	Zielfeld	Beschreibung
u_id	id	Entspricht der ID-Spalte des sn_vul_entry-Datensatzes.
u_severity	source_severity	Ordnet das Feld Schweregrad dem Schweregrad zu. Der Standardwert ist 5.
u_publishedon	date_published	Ordnet das Feld „u_publishedon“ dem Veröffentlichungsdatum zu.
u_publicexploit	public_exploit	Ordnet den vom Scanner bereitgestellten u_publicexploit der Spalte „Öffentlicher Exploit“ in der Schwachstelleneintragstabelle zu.
u_cvssv3	v3_base_score	Ordnet die cvssv3-Punktzahl der v3-Basispunktzahl im Datensatz des Schwachstelleneintrags zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für Microsoft TVM-Schwachstellen (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_description	Zusammenfassung	Ordnet die Beschreibung dem Zusammenfassungsfeld im Datensatz des Schwachstelleneintrags zu.
u_exploitinkit	malware_kit	Ordnet das Feld „u_exploitinkit“ dem Malware-Kit in der Exploit-Tabelle zu.
u_exploittypes	Typ	Ordnet den Exploit-Typ dem Typ in der Exploit-Tabelle zu.
u_exploitverified	is_exploit_verified	Ordnet das Feld „u_exploitverified“ dem verifizierten Exploit in der Exploit-Tabelle zu.
u_exploituris	Exploit_links	Ordnet das Feld „u_exploituris“ den Exploit-Links in der Exploit-Tabelle zu.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Erstellen oder Aktualisieren der Werte in der NVD- oder Drittpartei-Eintragstabelle verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Werte der neu erstellten Elemente und der Elemente, die aktualisiert und ignoriert wurden, verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

MS TVM-Empfehlungsimport

Die importierten Empfehlungsdaten werden zuerst in die Tabelle „MS TVM-Empfehlungsimport“ [sn_vul_msft_tvm_recom_import] geladen.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie die Daten aus dem MS TVM-Empfehlungsimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach **MS TVM-Empfehlungstransformation**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

MS TVM-Empfehlung – Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_recommendedvendor	Recommended_vendor	Ordnet das Feld u_recommendedvendor der Spalte Lieferant zu.
u_weaknesses	Schwachstellen	Ordnet das Feld u_weaknesses der Spalte „Schwächen“ zu.
u_expositioned Machinescount	src_exposition_computer_cnt	Ordnet das Feld u_expositioned Machinescount der Spalte Anzahl risikogefährdeter Computer zu.
u_status	status	Ordnet den Status dem Feld Status im Empfehlungsdatensatz zu.
u_productname	product_name	Ordnet das Feld u_productname dem Produktnamen im Empfehlungsdatensatz zu.
u_nonproductiv_impactedassets	Non_prod_impacted_assets	Ordnet das Feld u_nonproductiv_impactedassets der Spalte „Betroffene Assets“ im Empfehlungsdatensatz zu.
u_activealert	active_alert	Ordnet das Feld u_activealert der Spalte Aktive Warnung im Empfehlungsdatensatz zu.
u_recommendedversion	Recommended_version	Ordnet das Feld u_recommendedversion der Spalte Empfohlene Version im Empfehlungsdatensatz zu.
u_totalmaschinecount	total_maschine_count	Ordnet das Feld u_totalmaschinecount der Spalte Gesamtanzahl der Computer im Empfehlungsdatensatz zu.
u_exposureimpact	„exposure_impact“	Ordnet das Feld „u_exposureimpact“ der Spalte „Risikoauswirkung“ im Empfehlungsdatensatz zu.
u_recommendationname	„recommendation_name“	Ordnet das Feld u_recommendationname der Spalte „Empfehlungsname“ im Empfehlungsdatensatz zu.
u_subcategory	Unterkategorie	Ordnet das Feld u_subcategory der Spalte „Unterkategorie“ im Empfehlungsdatensatz zu.
u_id	source_id	Ordnet die Empfehlungs-ID aus MS TVM der Spalte Quell-ID zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MS TVM-Empfehlung – Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_remediationtype	remediation_type	Ordnet das Feld u_remediationtype der Spalte „Korrekturtyp“ im Empfehlungsdatensatz zu.
u_relatedcomponent	related_component	Ordnet das Feld u_relatedcomponent der Spalte „Zugehörige Komponente“ im Empfehlungsdatensatz zu.
u_recommendedprogram	Recommended_program	Ordnet das Feld u_recommendedprogram der Spalte Empfohlenes Programm im Empfehlungsdatensatz zu.
u_recommendationcategory	Recommendation_category	Ordnet das Feld u_recommendationcategory der Spalte „Empfehlungskategorie“ im Empfehlungsdatensatz zu.
u_publicexploit	public_exploit	Ordnet das Feld „u_publicexploit“ der Spalte „Öffentlicher Exploit“ im Empfehlungsdatensatz zu.
u_vendor	Lieferant	Ordnet das Feld „u_vendor“ der Spalte „Lieferant“ im Empfehlungsdatensatz zu.
[Skript]	integration_instance	Name der Instanz, aus der die Empfehlung importiert wird.
[Skript]	sys_domain	Domäne, in die dieser Datensatz importiert wird.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

MS TVM-Empfehlung – Transformationszuordnungsskript

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript, mit dem Werte in den Empfehlungen aktualisiert und überprüft werden, ob die Empfehlungen vorhanden sind. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Werte von erstellten, aktualisierten und ignorierten Elementen verwendet wird. Dieses Skript ist zur internen Verwendung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MS TVM-Empfehlung – Transformationszuordnungsskript (Fortsetzung)

Wenn das Skript ausgeführt wird	Zweck
	vorgesehen und darf nicht geändert oder gelöscht werden.

Import von MS TVM-Computer-Schwachstellen

Die Transformationszuordnung für MS TVM-Computer-Schwachstellen wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus MS TVM importiert werden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Verarbeitung von Daten aus dem MS TVM-Computer-Schwachstellenimport.

Um auf die Transformationszuordnungen für offene und feste Schwachstellen von MS TVM zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach der **Transformation für MS TVM-Computer-Schwachstellen**.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Transformationszuordnungsfelder für MS TVM-Computer-Schwachstellen

Quellenfeld	Zielfeld	Beschreibung
u_id	discovery_key	Ordnet das Feld u_id der Erkennungsschlüssel-Spalte in der Erkennungstabelle zu.
u_diskpaths	Nachweis	Ordnet das Feld u_diskpaths der Nachweisspalte in der Erkennungstabelle zu.
u_registrypaths	Nachweis	Ordnet das Feld u_registrypaths der Nachweisspalte in der Erkennungstabelle zu.
u_recommendedsecurityupdateid	Preferred_solution	Ordnet das Feld u_recommendedsecurityupdateid der Spalte Bevorzugte Lösung in der Tabelle der angreifbaren Elemente zu, wenn die Lösung mit derselben ID in der Tabelle sn_vul_solution vorhanden ist.
u_recommendationreference	Empfehlung	Ordnet das Feld u_recommendationreference der Spalte „Empfehlung“ in der Tabelle der angreifbaren Elemente zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für MS TVM-Computer-Schwachstellen (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_cveid	Schwachstelle	Ordnet das Feld u_cveid der Spalte „Schwachstelle“ in der Tabelle der angreifbaren Elemente zu.
u_status	source_status	Ordnet das Feld u_status der Spalte Quellstatus in der Erkennungstabelle zu.
u_eventtimestamp	temporal_score	Ordnet das Feld u_eventtimestamp der Spalte Zuletzt gefunden in der Tabelle der angreifbaren Elemente zu.
u_lastseentimestamp	last_seen	Ordnet das Feld u_lastseentimestamp der Spalte Zuletzt gesehen in der Tabelle der angreifbaren Elemente zu.
u_firstseentimestamp	first_seen	Ordnet das Feld u_firstseentimestamp der Spalte „Zuerst gesehen“ in der Tabelle der angreifbaren Elemente zu.
u_recommendedsecurityupdate	solution_summary	Ordnet das Feld u_recommendedsecurityupdate der Spalte „Lösungszusammenfassung“ in der Tabelle der angreifbaren Elemente zu.
u_recommendedsecurityupdatel	solution_summary	Ordnet das Feld u_recommendedsecurityupdatel der Spalte „Lösungszusammenfassung“ in der Tabelle der angreifbaren Elemente zu.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript, mit dem überprüft wird, ob der Schwachstelleneintrag und die Erkennungen vorhanden sind. Andernfalls werden diese Datensätze

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	in ihren jeweiligen Tabellen erstellt. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Aktualisieren der Anzahl der VIs und Erkennungen verwendet wird, wie sie aus MS TVM importiert wurden. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Statusdiagramm der Integrationsausführung für die Microsoft Threat and Vulnerability Management-Schwachstellenintegration

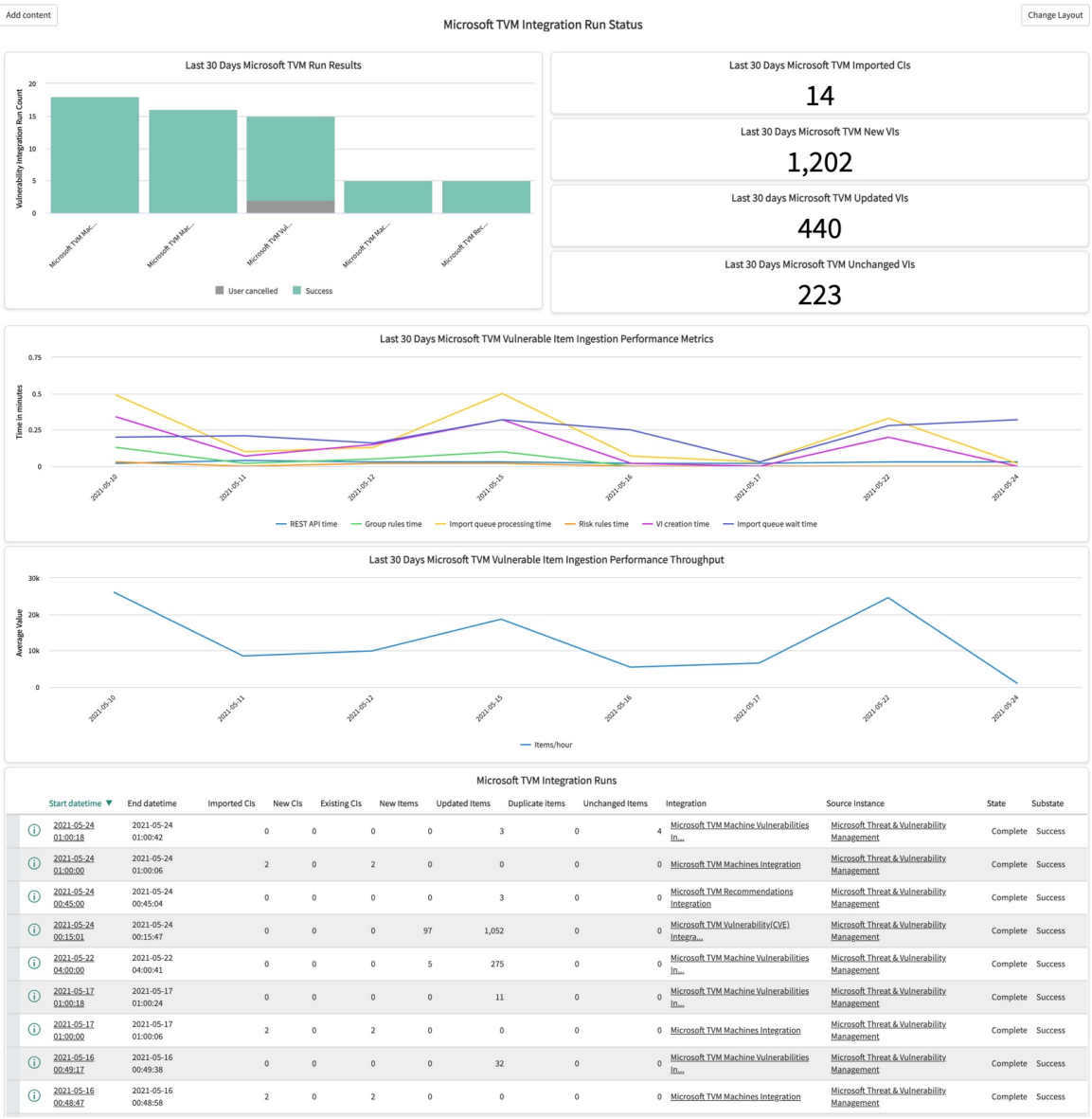
Sie können das Modul „Microsoft Threat and Vulnerability Management (MS TVM) Integrationsausführungsstatus“ verwenden, um sich eine grafische Ansicht des Status der MS TVM-Integrationsausführungen anzuzeigen.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Im Diagramm können Sie auf einen beliebigen Teil des Diagramms zeigen, um eine Zusammenfassung der spezifischen Daten für diesen Teil anzuzeigen. Wenn Sie auf ein Teil des Balkendiagramms klicken, wird eine Liste mit detaillierteren Informationen geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Diagrammberichte zum Status der MS TVM-Integrationsausführung

Name	Beschreibung
Microsoft TVM-Ergebnisse der letzten 30 Tage	Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. In diesem Bericht werden sowohl die erfolgreichen als auch die fehlgeschlagenen Ausführungen angezeigt. Jede Ausführung wird als Balken im Diagramm angezeigt.
Microsoft TVM – Neue AEs der letzten 30 Tage	Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden.
Von Microsoft TVM aktualisierte AEs der letzten 30 Tage	Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden.
Unveränderte Microsoft TVM-VIs der letzten 30 Tage	Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden.
MS TVM-Integrationsausführungen	Datensätze der Integrationsausführung in einer Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: **V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle *sn_vul_detection*. Während die Integration ausgeführt wird, ändert sich möglicherweise die Anzahl der Erkennungen oder Ergebnisse. In diesem Bericht wird die Anzahl der Erkennungen in der Spalte „Anzahl bis Datum“ in der Instanz nach Abschluss der Integrationsausführung angezeigt.
Angreifbares Microsoft TVM-Element – Erfassungsleistungsmetriken der letzten 30 Tage	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage.
Angreifbares Microsoft TVM-Element – Erfassungsleistungsdurchsatz der letzten 30 Tage	Täglicher Durchsatz bei der Erfassung von angreifbaren Elementen, der für die Microsoft TVM-Hosterkennungsintegration in den letzten 30 Tagen gemessen wurde.
Von Microsoft TVM importierte CIs der letzten 30 Tage	Anzahl der neuen Configuration Items, die in den letzten 30 Tagen importiert wurden.

Verifiziert den Status der Importausführung der Microsoft Threat and Vulnerability Management-Integration

Verwenden Sie den Importausführungsstatus von Microsoft Threat and Vulnerability Management (MS TVM), um den Erfolg Ihrer Integrationsausführungen zu überprüfen und etwaige Probleme zu lokalisieren.

Vorbereitungen

Dieses Verfahren geht von den folgenden Annahmen aus:

- Sie haben Vulnerability Response und die MS TVM-Schwachstellenintegration installiert und konfiguriert.
- Die Importe von MS TVM-Schwachstellenintegrationen sind geplant und werden ausgeführt.

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Threat and Vulnerability Management** > **Integrationen**.
   a. Wählen Sie eine Integration aus.
   b. Klicken Sie auf die zugehörige Liste Integrationsausführungen für Schwachstellen.
2. Vergewissern Sie sich, dass der Status der Importe „Abgeschlossen“ und der Substatus „Erfolg“ lautet. Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:
   - Netzwerkunterbrechung.
   - Bitverfall bei der Datenübertragung, der zu beschädigten Daten während der Transformation führt.
3. **Wahlweise:** Wenn eine dieser Bedingungen zu einer fehlgeschlagenen Ausführung führt, klicken Sie auf **Execute now (Jetzt ausführen)**, und führen Sie die Integration erneut aus.

Teilen Sie Microsoft TVM-Erkennungen basierend auf der Schwachstelleninstanz auf, um angreifbare Elemente aufzuteilen

ServiceNow® Vulnerability Response ermöglicht die Aufteilung von Erkennungen von Microsoft Threat and Vulnerability Management-Scannern (MS TVM) und ermöglicht die Erstellung eines eindeutigen angreifbaren Elements (VIT) für jede erkannte Schwachstelleninstanz. Diese Aufteilung ermöglicht die Zuweisung von VITs zu verschiedenen Nachbesserungsteams, wodurch die Verwaltung und Nachverfolgung von Schwachstellen verbessert wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Nutzlast des Microsoft Threat and Vulnerability Management-Scanners (MS TVM) enthält Erkennungsdaten, wobei jeder Pfad innerhalb des Nachweises zur Aufteilung der Erkennungen verwendet wird. Das Tag „diskpath“ in der Nutzlast gibt den Ort der Schwachstelle an und erleichtert so die genaue Identifizierung und Verwaltung von Schwachstellen entsprechend ihren spezifischen Pfaden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Legen Sie in der Tabelle „Drittparteiintegrationen“ [sn_sec_int_integration] den Wert **Nachweis in VI-Schlüsselspalte einschließen** für Tenable.io und Tenable.scauf true fest.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.
3. Aktivieren Sie im Formular „Port einbeziehen“ das Kontrollkästchen Port einbeziehen, und wählen Sie den Link **Hier klicken**.
4. Wählen Sie in der Liste Nachweis zu VI-Schlüssel hinzufügen die **Option Neu**aus.
5. Fügen Sie im Formular „Nachweis zum VI-Schlüssel hinzufügen – Neuer Datensatz“ im Feld **Schwachstelle** das CVE von Microsoft Threat and Vulnerability Management (MS TVM) hinzu, für das Sie den Nachweis hinzufügen möchten, und wählen Sie **Absenden aus**.
   Die ausgewählte Schwachstelle wird in der Liste Nachweis zu VI-Schlüssel hinzufügen angezeigt.

Example: Erkennungen vom Microsoft Threat and Vulnerability Management-Scanner (MS TVM) aufteilen

Die folgende Erkennung des Scanners Microsoft Threat and Vulnerability Management (MS TVM) zeigt einen Nachweis im Tag „diskpath“.

```
          "id": "329f3283
fae116€796ff1b59c8dd56fef4067elf_mozilla_firefox_126.0.1.0_CVE-2024-7528",
          "deviceId":"329f3283fae116e796ff1b59c8dd56fef4067e1f",

         "rbacGroupId":
    "rbacGroupName": "Unassigned",
     "deviceName": "ip-0a1409fd.secops.com",
      "osPlatform": "WindowsServer2019",
        "oVersion": "10.0.17763.5936",
      "osArchitecture": "x64",
       "softwareVendor": "mozilla",
      "softwareName": "firefox",
      "softwareVersion": "126.0.1.0",

          "cveId"; "CVE-2024-7528",
         #vulnerabilitySeverityLevel": "High",
       #recommendedSecurityUpdate":; "mfsa2024-33",

       "recommendedSecurityUpdateId": null,

         "recommendedSecurityUpdateUrl": null,
          "diskPaths": ['c: llprogram files\lamazonllcfn-bootstraplilibcrypto-3.dll", "C: \lprogram
files\lamazon\lcfn-bootstrap\\libsst-3.dll,

        "registryPaths":
          1 "HKEY LOCAL, MACHINE\\SOFTWAREW\WOW6432Nodel
lMicrosoft|\Windows|1CurrentVersion\|Uninstalll\Mozilla Firefox 126.0.1 (x86 en-US)"


       #lastSeenTimestamp": "2024-08-28 19:36:07",

        "firstSeenTimestamp": "2024-08-06 20:32:34",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    "end0fSupportStatus": null,
      "end0fSupportDate": null,
   "exploitabilityLevel": "NoExploit",
      "recommendationReference": "va-_-mozilla-_-firefox",

      "cvssScore": 8.8,
   "securityUpdateAvailable": true,
     "cveMitigationStatus": null
```


Informationen zur Integration der HCL BigFix Patch Orchestration in mit Vulnerability Response

Sie können Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen von Assets mit der Integration von Patch Orchestration Vulnerability Response in das HCL BigFix-Produkt verwalten.

Patch-Orchestrierung mit Vulnerability Response

Bei der Patch-Orchestrierung mit Vulnerability Response werden geplante Importe von Lösungsintegrationen von Drittanbietern, Patch-Anbietern und Schwachstellen-Scannern verwendet. Die Scanner-Erkennungsdaten gleichen die Assets in Ihrer Umgebung mit Schwachstellen und den Patch-Updates ab, die sie beheben können. Übermitteln Sie Patch-Anforderungen zur Genehmigung, planen Sie Patch-Updates zur Behebung angreifbarer Elemente, und überwachen Sie den Korrekturfortschritt – alles über Datensätze in der Anwendung Vulnerability Response in Ihrem Now Platform®.

Vulnerability Response Patch Orchestration with HCL BigFix

Wenn die Anwendung „Vulnerability Response Patch Orchestration with HCL BigFix integration“ mit den Anwendungen ServiceNow® Vulnerability Solution Management, Patch Orchestration und Vulnerability Response verwendet wird, können Schwachstellenmanager und Analysten die folgenden Aufgaben ausführen:

- Sehen Sie sich weiteren Kontext und Informationen zu den Arten von Patches und den Lösungen der Lieferanten (Patches) an.
- In den -Arbeitsbereichen Vulnerability Response können Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Nachbesserung von Schwachstellen aus Datensätzen anzeigen und überwachen.

IT-Spezialisten und Korrekturbesitzer können die folgenden Aufgaben ausführen:

- Stellen Sie Patches, die vom BigFix-Produkt für Windows, CentOS, MAC, Oracle und andere Assets unterstützt werden, in regelmäßigen, geplanten Intervallen außerhalb der Geschäftszeiten bereit, um Arbeitskonflikte zu vermeiden.
- Identifizieren Sie Assets ohne Patch mit Schwachstellen oder Assets, die durch geplante Patches nicht erfolgreich aktualisiert wurden, aus importierten Erkennungsdaten von Drittanbieterscannern.
- Planen Sie verfügbare Patches aus dem IT-Korrekturarbeitsbereich oder aus der klassischen Umgebung für angreifbare, nicht gepatchte Assets aus Patch-Updates, Korrekturaufgaben und Datensätzen erkannter Elemente.

Schlüsselbegriffe in den Anwendungen Vulnerability Response und BigFix

Konfigurationselement bzw. Configuration Item (CI)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs sind die vorhandenen Assets, die in Ihren Configuration Management Database (CMDB)aufgeführt sind. BigFix bezeichnet CIs als Computer.

Computergruppen

Im BigFix-Produkt verwendete Terminologie, die sich auf eine Gruppe von Assets bezieht.

Angreifbares Element

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht.

Instanz

Ein eindeutiger Account für die BigFix-Anwendung. Jedes Benutzerkonto kann eine Instanz in der BigFix-Anwendung sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für eine Instanz Now Platform.

Integration

Eine Integration ist eine geplante Aufgabe in Now Platform, die Informationen von einer Drittanbieterquelle abruft, z. B. die Integration mit den BigFix-Computern.

Lösung

Im Kontext dieser Integration gibt es zwei Arten von Lösungen: potenzielle und bevorzugte. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben kann. Schwachstellen haben oft viele potenzielle Lösungen. Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte, erkannte Schwachstelle.

Patch

Software-Updates, die Schwachstellen beheben. In der BigFix-Anwendung werden Patches als Fixlets bezeichnet. BigFix hat beispielsweise Fixlets für Windows, CentOS, MAC, Oracle und andere Produkte.

Bevorzugter Patch

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Sobald Patches bereitgestellt wurden, werden sie den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und beheben sie.

Nachbesserungsaufgabe

Listen angreifbarer Elemente in der Anwendung Vulnerability Response von Aktionen, die zum Beheben von Schwachstellen erforderlich sind.

Bereitstellung

Für die Zwecke dieser Integration bedeutet Bereitstellung, wenn Sie einen Patch auf einen Computer anwenden, initiieren oder planen. BigFix bezeichnet diese Bereitstellungen als Aktionen. Sie können für die von BigFix heruntergeladenen Patches (Aktionen erstellen) in Ihrem Now Platformbereitstellen (Erstellungsaktionen). Navigieren Sie zu erkannten Elementen, Patches oder Korrekturaufgaben aus einzelnen Datensätzen in Vulnerability Response. Sie können Patches mit geplanten Aufgaben auf einzelnen Computern oder Computergruppen bereitstellen.

Die Bereitstellung in Now Platform kann sich auch auf eine Integration beziehen, die mehrere Quellen unterstützt. Das Vorhandensein einer einzelnen Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie in Ihrer Umgebung über mehrere Bereitstellungen der BigFix Vulnerability-Integration verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Solution Management und Vulnerability Response Patch Orchestration with HCL BigFix Integration

Das Lösungsmanagement erfolgt über die Anwendung Vulnerability Solution Management, eine Anwendung Now Platform, die Ihre Schwachstellenergebnisse mit der Aufgliederung der Lösungen (Patches) korreliert, die sie beheben. Identifizieren Sie die Softwarepatches von Drittanbietern für Produkte und Services, Konfigurationsupdates und andere Steuerungen, die die größten Auswirkungen für Ihre Organisation haben. Die Anwendungen Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration with HCL BigFix arbeiten mit den Informationen zu Drittparteiscannern zusammen, um ein Rollup der bevorzugten Patches von der Lösung über die Schwachstelle bis zum angreifbaren Element durchzuführen, damit Sie sie beheben und schließen können Schwachstellen in Ihrer Umgebung.

Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration with HCL BigFix Integration sind alle in ServiceNow® Storeverfügbar.

Erforderliche Now Platform-Rollen

Für die Installation, Konfiguration und Korrekturaufgaben der Integration sind die folgenden Rollen in Ihrer Instanz Now Platform erforderlich.

Administrator

Benutzer mit dieser Rolle erhalten Berechtigungen für Anwendungen in den Instanzen ServiceNow Store und laden sie in die Instanzen Now Platform herunter.

sn_vul.vulnerability_admin

Benutzer mit dieser Rolle aktivieren Anwendungen in der Instanz Now Platform und schließen die Konfiguration der Anwendung Vulnerability Response ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Dieser Administratorbenutzer konfiguriert alle VR-Anwendungen, Regeln und Drittanbieterintegrationen.

sn_vul_bigfix.configure_integration

Benutzer mit dieser Rolle konfigurieren die Anwendung „BigFix Patch Orchestration Integration“. Diese Rolle enthält die granulare Rolle sn_vul_bigfix.read_integration.

sn_vul_bigfix.read_integration

Benutzer mit dieser Rolle können die Datensätze der Anwendung Vulnerability Response und der Anwendung BigFix Patch Orchestration Integration sowie die Daten der Patch-Orchestration anzeigen (schreibgeschützt).

sn_vul_patch_orch.configure_patch

Benutzer mit dieser Rolle können -Patches konfigurieren und anwenden.

sn_vul_patch_orch.read_patch

Benutzer mit dieser Rolle können Patch-Informationen anzeigen (schreibgeschützt).

Verantwortliche Vertragsgenehmigung

Mit können Sie den Genehmigergruppen Genehmigerebene 1 und Genehmigerebene 2 verwenden, wenn Sie möchten, dass übermittelte Patch-Anforderungen vor der Bereitstellung genehmigt werden.

Weitere Informationen zum Zuweisen dieser Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zu den -Rollen Vulnerability Response in Ihrem Now Platformfinden Sie unter Vulnerability Response Personae und granulare Rollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Suchregeln

Wenn Daten aus der BigFix-Anwendung importiert werden, sucht die Anwendung Vulnerability Response anhand von Maschinendaten (Asset-Daten) automatisch nach Übereinstimmungen in Configuration Management Database (CMDB). CI-Suchregeln werden verwendet, um CIs (Assets) zu identifizieren und sie automatisch zu Datensätzen angreifbarer Elemente (VI) hinzuzufügen, wenn VIs erstellt werden.

Die folgenden CI-Suchregeln sind im Lieferumfang des -Basissystems enthalten und werden verwendet, um CIs (Assets) zu identifizieren und der Anwendung Vulnerability Response hinzuzufügen:

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

Sie können mehrere Werte für die IP_ADDRESS eines Assets verwenden. Eine CI-Suchregel berücksichtigt alle Werte für den Abgleich. Weitere Informationen zur Funktionsweise und Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

MID-Server

Die Vulnerability Response Patch Orchestration with HCL BigFix integration ist eine lokale Integration. Erfordert einen eigenständigen MID Server, der nicht Teil eines MID Server-Clusters ist. Der MID-Server wird benötigt, um auf entfernten Computern von Ihrer Instanz Skripts auszuführen und Daten vom BigFix-Server zu importieren. APIs für diese Integration werden mithilfe von MID-Servern aufgerufen, die Sie in Ihrer Instanz Now Platform einrichten. Weitere Informationen finden Sie unter Vorbereitung auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix.

Integrationen und Abhängigkeiten der Integration von Vulnerability Response Patch Orchestration mit HCL BigFix

Die folgenden Produkt- und Abhängigkeitsanwendungen sind für Vulnerability Response Patch Orchestration with HCL BigFix Integration erforderlich. Diese Anwendungen sind im ServiceNow® Storeverfügbar.

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

Zum Anzeigen von Patch-Orchestrationsdaten und verfügbaren Updates (Patches) in den Arbeitsbereichen in Vulnerability Responsesind die folgenden Anwendungen erforderlich. Alle aufgeführten Anwendungen sind unter ServiceNow® Storeverfügbar. Einige Anwendungen erfordern separate Abonnements.

Weitere Informationen zur Versionskompatibilität mit den erforderlichen Anwendungen und Familienreleases finden Sie im Artikel KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen in der HI Knowledge Base.

Anwendungs- und Releaseversion
Vulnerability Response
Vulnerability Solution Management

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungs- und Releaseversion
Anwendung Vulnerability Response Patch Orchestration
Vulnerability Response Patchen Sie Orchestration mit der Anwendung HCL BigFix
Security Support Common
Security Support Orchestration
Eine unterstützte Schwachstellen-Scanner-Anwendung von Drittanbietern

Vulnerability Response Patchen Sie Orchestration-Anwendungstabellen

Die Anwendung Vulnerability Response Patch Orchestration enthält die folgenden Tabellen:

Tabelle	Beschreibung
Patch-Update [sn_vul_patch_orch_update]	Speichert Informationen zu den Patches, die auf verschiedenen Instanzen verfügbar sind.
Geräte-Update [sn_vul_patch_orch_m2m_src_ci_update]	Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in Datensätzen für erkannte Elemente angezeigt werden.
Sammlung [sn_vul_patch_orch_collection]	Speichert Sammlungsdaten aus verschiedenen Instanzen.
Gerätesammlung [sn_vul_patch_orch_m2m_src_ci_collection]	Speichert Sammlungsdaten zu erkannten Elementen.
Patch-Bereitstellung [sn_vul_patch_orch_deployment]	Speichert Informationen über bereitgestellte Patches für Sammlungen und CIs.
Potenzieller Patch [sn_vul_patch_orch_m2m_vuln_patch]	Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zum Beheben einer Schwachstelle verwendet werden können.

Integrationen von Vulnerability Response Patch Orchestration mit HCL BigFix

Die von ServiceNow® Engineering entwickelten Integrationen bilden die orchestrierte Lösungsbereitstellung mit dem BigFix-Produkt. Die folgenden Integrationen sind in der Anwendung Vulnerability Response Patch Orchestration Integration with HCL BigFix enthalten, die Sie aus dem ServiceNow® Storeherunterladen.

Nachdem Sie die Integrationsanwendung in Ihrer Instanz Now Platform installiert haben, navigieren Sie zum Anzeigen dieser Integrationen zu **Integrationen** > **Integration der BigFix Patch Orchestration** > **Integrationen**. Die Anwendung Vulnerability Response verarbeitet Daten in geplanten Zeitintervallen, die von diesen Integrationen mit BigFix-Endpunkten importiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
Integration der BigFix-Sammlung	• Diese Integration ist für die tägliche Ausführung geplant und wird zuerst in der verketteten Integrationsausführung ausgeführt. • Ruft die Computer und Computergruppen, aus denen die Computergruppen bestehen (Konfigurationselemente), aus der BigFix-Anwendung ab.
BigFix Fixlet Integration	• Wenn sie geplant ist, wird diese Integration durch den Abschluss der Integration der BigFix-Sammlung ausgelöst. Sie können ihn auch bei Bedarf ausführen. • Ruft Informationen zu allen verfügbaren Fixlets (Patches) vom BigFix-Server ab.
BigFix Device Fixlet Integration	• Wenn sie geplant ist, wird diese Integration durch den Abschluss der BigFix-Fixlet-Integration ausgelöst. Sie können ihn auch bei Bedarf ausführen. • Ruft Informationen zu den Fixlets ab, die sich derzeit auf Computern (Assets) befinden, vom BigFix-Server.
BigFix Actions Integration	• Wenn sie geplant ist, wird diese Integration durch den Abschluss der Integration des BigFix Device Fixlet ausgelöst. Sie können ihn auch bei Bedarf ausführen. • Ruft Informationen zu den Patches ab, die vom IT-Team auf dem BigFix-Server geplant wurden.

Vorbereitung auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix

Bereiten Sie die Integration vor, indem Sie die folgenden Setupaufgaben ausführen.

Vorbereitungen

Erforderliche Rolle: admin für die Installation der Anwendungen und das Zuweisen von Rollen. Andere Rollen sind in der folgenden Tabelle aufgeführt.

Warum und wann dieser Vorgang ausgeführt wird

Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration.

Sie sind bereit für Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix.

Prozedur

1. Befolgen Sie die bereitgestellte Prüfliste für eine reibungslose Installation und Konfiguration der Anwendung Vulnerability Response Patch Orchestration with HCL BigFix.
2. Unter Umständen möchten Sie vor der Installation der Anwendung die folgende Prüfliste ausdrucken und überprüfen, ob die aufgelisteten Elemente abgeschlossen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

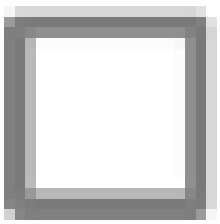
Importieren Sie nach der Installation und Konfiguration Informationen zu Schwachstellen und Patches in Ihre Instanz Now Platform®.

Aufgabe	Beschreibung
☐	(Optional) Wenn die Anwendung noch nicht installiert und aktiviert ist, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.0 von Vulnerability Response oder höher.
☐	Wenn noch nicht installiert ist, beschaffen Sie sich Berechtigungen und installieren Sie die Scanner-Anwendung einer Drittpartei, um Schwachstellendaten zu importieren. Unter Vulnerability Response-Integrationen finden Sie weitere Informationen zu Scannern von Drittparteien, die von Vulnerability Responseunterstützt werden. Weitere Informationen finden Sie unter .
☐	Wenn die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix noch nicht installiert ist, rufen Sie Berechtigungen ab, und laden Sie sie in Ihre Instanz Now Platform® herunter. Weitere Informationen finden Sie unter .
	Rufen Sie die BigFix-Anmeldeinformationen ab. Stellen Sie sicher, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre BigFix-Produkte erforderlich sind, damit Sie darauf zugreifen können.
☐	Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator ruft Berechtigungen ab, lädt die Anwendung BigFix Patch Orchestration und die anderen für die Integration erforderlichen Anwendungen herunter und installiert sie. Wenn dies nicht zugewiesen ist, weist der Administrator den Schwachstellen-Administrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten in Vulnerability Response oder über das Modul Benutzeradministration zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	sn_vul.vulnerability_admin Nach der Zuweisung schließt der Schwachstellen-Administrator die Konfiguration der BigFix-Integrationen und der anderen Drittanbieteranwendungen ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Diese Rolle konfiguriert alle VR-Anwendungen, Regeln, Drittanbieterintegrationen, Vulnerability Response Patch Orchestration- und Vulnerability Solution Management-Anwendungen. **sn_vul_bigfix.configure_integration** Benutzer mit dieser Rolle konfigurieren die Anwendung „BigFix Patch Orchestration Integration“. Diese Rolle enthält die granularen Rollen sn_vul_bigfix.read_integration und connection_admin, die es dem Benutzer ermöglichen, eine Verbindung zur BigFix-Konsole herzustellen und die Integrationsinstanzen in Ihrem Now Platformzu konfigurieren. **sn_vul_bigfix.read_integration** Benutzer mit dieser Rolle können die Datensätze der Anwendung Vulnerability Response und der Anwendung BigFix Patch Orchestration Integration sowie die Daten der Patch-Orchestration anzeigen (schreibgeschützt). **sn_vul_patch_orch.configure_patch** Benutzer mit dieser Rolle können -Patches konfigurieren und anwenden. Von diesem Anwender angeforderte Patches aus Datensätzen für angreifbare Elemente und Patch-Updates werden zur Genehmigung gesendet, wenn Change-Management aktiv ist und Genehmiger zugewiesen sind. **sn_vul_patch_orch.read_patch** Benutzer mit dieser Rolle können Patch-Informationen für Datensätze anzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind. **Verantwortliche Vertragsgenehmigung** Benutzer, die der Genehmigerebene 1 und optional der Genehmigerebene 2 zugewiesen sind, genehmigen die Genehmigergruppen, die eingereichte Patch-Anforderungen genehmigen. Standardmäßig werden Patches vor der Bereitstellung zur Genehmigung an die Gruppe der Genehmiger der Ebene 1 übermittelt. Weitere Informationen zum Genehmigungsprozess finden Sie unter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Patch-Orchestrierung mit Vulnerability Response. Weitere Informationen zum Einrichten von Genehmigern und Gruppen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Die erstmalige Zuweisung von Rollen zu Benutzern und Gruppen für die Integration erfolgt durch den Systemadministrator. Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Wenn dies noch nicht erstellt wurde, können Sie zusätzliche Gruppen für die Rollen „Remediationsspezialist“ und „Schwachstellenanalyst“ erstellen und Benutzer mit dem Modul „Benutzeradministration“ in Ihrer Instanz hinzufügen. Weitere Informationen finden Sie unter Benutzergruppen erstellen .
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz von aktiviert haben, die für die Integration erforderlich sind. ○ Vulnerability Response Patch Orchestration with HCL BigFix ist eine lokale Integration, für die Sie einen eigenständigen MID Server verwenden müssen. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . ○ Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es.

Nächste Maßnahme

Sie sind jetzt bereit für Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix.

Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix

Laden Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix aus dem ServiceNow® Storeherunter.

Vorbereitungen

Erforderliche Rolle: admin für die erstmalige Zuweisung der Rolle sn_vul.vulnerability_admin und die Installation der Anwendung. Der Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)) konfiguriert die Vulnerability Response Patch Orchestration mit HCL BigFix und anderen Anwendungen nach der Installation.

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie vor der Installation der Anwendung sicher, dass Sie alle Elemente in der Prüfliste in Vorbereitung auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFixabgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie die Anwendung **Vulnerability Response Patch Orchestration with HCL BigFix**, und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung installiert, die Sie aus ServiceNow Storeheruntergeladen haben.

3. Alternativ können Sie Anwendungen über den Setup-Assistenten installieren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.

Nächste Maßnahme
Navigieren Sie nach Abschluss der Installation zu **Alle** > **Integration der BigFix Patch Orchestration** > **Konfiguration** um mit der Konfiguration fortzufahren.

Konfigurieren Sie die Integration der Patch-Orchestration-Integration Vulnerability Response mit HCL BigFix

Nachdem Sie die Anwendung installiert haben, konfigurieren Sie sie mit Ihren BigFix-Kontoinformationen, und validieren Sie Ihre Anmeldeinformationen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin und sn_vul_bigfix.configure_integration

Prozedur

1. Navigieren zu **Integration der BigFix Patch Orchestration** > **Konfiguration**.
2. Füllen Sie die Felder mit Ihren BigFix-Informationen und -Anmeldeinformationen aus.

Feld	Beschreibung
Integrationsinstanz	Der Name des BigFix-Instanzkontos, das Sie verwenden möchten, z. B. BigFix Patch Management Integration.
Hostname	Geben Sie die URL für den BigFix-Host ein.
Anwendername	Geben Sie Ihren BigFix-Account-Anwendernamen ein.
Passwort	Geben Sie Ihr Passwort für den BigFix-Account ein.
MID-Server	Geben Sie den Namen des eigenständigen MID-Servers aus der Liste ein, den Sie verwenden möchten. Weitere Informationen zu MID-Servern und zum Einrichten von Aufgaben in Ihrem Now Platform®finden Sie unter Vorbereitung auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf Anmeldeinformationen speichern und testen.
   Der Status Ihrer Verbindung zwischen BigFix und Ihrer Instanz Now Platform® wird im Feld Validierungsstatus angezeigt. Wenn Sie keinen erfolgreichen Test sehen, befolgen Sie die Eingabeaufforderungen.
4. **Wahlweise:** Domänentrennung wird für diese Integration unterstützt.
   Sie können Ihrer -Instanz mehrere Konfigurationen hinzufügen. So fügen Sie zusätzliche Konfigurationen hinzu:

   a. Navigieren zu **Integration der BigFix Patch Orchestration Integrationsinstanzen**.

   b. Stellen Sie sicher, dass im Feld Anwendungsbereich der Anwendungsbereich Vulnerability Response Patch Orchestration with HCL BigFixangezeigt wird.

   c. Klicken Sie auf **Neu**.

   d. Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Name für die Integrationsinstanz.
Anwendung	Vulnerability Response Patch Orchestration with HCL BigFix
Integration	[Schreibgeschützt] Die Verwaltung von BigFix Patch ist Standard.
Aktiv	Standardmäßig ist aktiviert (ausgewählt). Wenn diese Option gelöscht wird, ist die Instanz nicht aktiv.

   e. Klicken Sie auf **Absenden**.
   Ihre neue Integrationsinstanz wird in der Liste Integrationsinstanzen angezeigt.

   f. Wiederholen Sie die Schritte 1 bis 3, um Ihre Integrationsinstanz zu konfigurieren und Ihre Anmeldeinformationen zu testen.

5. Richten Sie Genehmigungen für Patch-Anforderungen ein.
   Standardmäßig ist eine Systemeigenschaft [**sn_vul_patch_orch.patch_approval_required**] aktiviert, sodass Patch-Bereitstellungen, die geplant werden, zur Überprüfung und Genehmigung an Benutzer übermittelt werden, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind.

   Wenn Sie möchten, dass Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Genehmigung planen, können Sie die Eigenschaft [**sn_vul_patch_orch.patch_approval_required**] deaktivieren. Möglicherweise möchten Sie Genehmigungen aktiviert lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen.

   Hinweis:
   Wenn Sie die Systemeigenschaft „Genehmigung“ deaktivieren, kann jeder Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So deaktivieren Sie als Benutzer mit der Rolle sn_vul.vulnerability_admin die Systemeigenschaft:

a. Navigieren zu **sys.properties.list**.

b. Suchen Sie nach **sn_vul_patch_orch.patch_approval_required,** und klicken Sie darauf, um den Datensatz zu öffnen.

c. Im Feld Wert geben Sie `false`ein.

d. Klicken Sie auf **Aktualisieren**.

6. Wenn Sie diese Eigenschaft nicht deaktivieren, müssen Sie für Patch-Anforderungen Genehmiger zuweisen. Führen Sie als Benutzer mit der Rolle sn_vul.vulnerability_admin die folgenden Schritte aus.

a. Navigieren zu **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.

b. Wenn die Genehmigungsregel **für Patch-Update-Genehmigung bereitstellen** nicht in der Liste angezeigt wird, klicken Sie oben links im Bildschirm rechts neben dem grünen Filtersymbol auf **Alle**, um die gesamte Liste anzuzeigen.

c. Klicken Sie in der Liste auf **Deploy Patch Update Approval (Patch-Update-Genehmigung bereitstellen**) .

d. Klicken Sie im Datensatz bei ausgewählter Registerkarte Genehmigungskonfiguration **auf Standardkonfiguration Patch-Update approval**.

e. Klicken Sie im -Datensatz auf **Level 1 - Patch update approval (Ebene 1 - Patch-Update-Genehmigung)**.

f. Fügen Sie Anwender in dieser Gruppe hinzu.

Die dieser Gruppe zugewiesenen Benutzer genehmigen Patch-Anforderungen, die von Benutzern mit der Rolle „sn_vul_patch_orch.configure_patch“ übermittelt wurden. Navigieren Sie zu **Meine Genehmigungen**, um die Anforderungen anzuzeigen und zu verarbeiten.

7. Klicken Sie auf**Aktualisieren**, um Ihre Änderungen zu speichern.

8. **Wahlweise:** Sie können Genehmigungen auf mehreren Ebenen einrichten, sodass vor der Bereitstellung geplanter Patch-Anforderungen mehr als eine Genehmigung erforderlich ist.

a. Klicken Sie bei angezeigtem Genehmigungsdatensatz für Patch-Updates für Standardkonfiguration auf **Neu**.

b. Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Genehmigungsebene, z. **B. Ebene 2 - Patch-Update-Genehmigung**.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ▪ Ein Genehmiger erforderlich ▪ Alle Anwender müssen genehmigen
Bestellung	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt.
Rolle	Wählen Sie in der Liste eine Rolle für die Gruppe aus.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen.
Zuweisen mit	Wählen Sie eine Option aus: ▪ Anwender und Anwendergruppe ▪ Genehmigungstabellenfeld ▪ Skript
Gruppen	Gruppe auf Genehmigerebene, die aus mehreren Anwendern besteht. Der Benutzer muss eine der folgenden von Ihnen angegebenen Rollen aufweisen.
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

c. Klicken Sie auf **Absenden**, um Ihre Änderungen zu speichern.

Patch-Daten für die Integration der Patch Orchestration Vulnerability Response mit HCL BigFix anzeigen

Patch-Daten und Patch-Rollup-Daten sowie Informationen zu Schwachstellen und Korrekturstatus Ihrer Schwachstellen werden in den Datensätzen in Ihrer Instanz angezeigt.

Patch-Daten werden in den Vulnerability Response -Arbeitsbereichen angezeigt

Erforderliche Rollen:

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch zum Anzeigen (schreibgeschützt) von Patch-Informationen zu Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

Im Arbeitsbereich für IT-Korrekturen können Sie Patches anzeigen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In der Ansicht „Homepage“, in der Sie auf Bewertungslisten klicken können, um Datensätze für Bevorzugte Lösungen für VIs, angreifbare CIs und Bevorzugte Patches für VIs anzuzeigen.
- In der Listenansicht können Sie alle Patch-Update-Datensätze (VPUs) aus den Patches-Links und die Ihnen zugewiesenen angreifbaren Elemente (VITs) mit Patches anzeigen.

Sie können Patches von den folgenden Datensätzen aus planen:

- Von Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Discovered Item (SDI)-Datensätze

Im Arbeitsbereich des Schwachstellenmanagers können Sie Patches anzeigen:

- Über die Ansicht Startseite zu Überwachungsthemen, in der Sie bevorzugte und potenzielle Patches, geplante Patch-Daten und, falls der Patch heruntergeladen wurde, alle auf der Registerkarte **Angreifbare Elemente** anzeigen können.
- Listenansicht zu Korrekturmaßnahmen, in der Sie Patchdaten für VI-Datensätze auf der Registerkarte**Angreifbare Elemente** anzeigen können.

Navigieren Sie in der klassischen Umgebungsansicht zu **Alle** > **Vulnerability Response** > **Patches**.

Patch-Update-Datensätze in den VR-Arbeitsbereichen und in der klassischen Umgebungsansicht

Patch-Daten und Patch-Rollup-Daten sowie deren Status werden für die Datensätze in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit Vulnerability Responseenthalten. Zeigen Sie VPU-Datensätze (Patch) in Arbeitsbereichen Vulnerability Response aus der Listenansicht im Arbeitsbereich für IT-Fehlerkorrekturen an. Patch-Update-Datensätze in der klassischen Ansicht und in den Arbeitsbereichen Vulnerability Response enthalten die folgenden Daten:

- Daten und Informationen zur Schwachstellenlösung von Patch-Lieferanten, die von der Anwendung Vulnerability Solution Management importiert werden.
- Quellkorrekturstatus, der die Gesamtzahl der Geräte mit einer bestimmten Schwachstelle enthält, die durch einen Patch behoben werden kann, sowie alle Geräte, für die Updates fehlen.
- Korrekturstatus, der den Prozentsatz der korrigierten VIs und die Gesamtzahl der VIs enthält, die einen Patch als bevorzugten Patch haben.
- Zugehörige Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen für zugehörige Links zu Datensätzen in der Klassenansicht. Diese Daten werden auf Registerkarten in Datensätzen in den Vulnerability Response -Arbeitsbereichen angezeigt.
- Patch-Anforderungen, die von Korrekturbesitzern zur Genehmigung übermittelt wurden.

Status-Rollup für Datensätze von angreifbaren Elementen

Weitere Informationen zum Status-Rollup zu Datensätzen finden Sie unter Patchen Sie Daten und Status-Rollup für die Patch-Orchestrierung in Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze, die aktive AEs-Anzahlen zusammenfassen

Um zu vermeiden, dass für alle Patches für alle Schwachstellen ein Rollup durchgeführt wird, werden für die geplante Aufgabe nur Änderungen an der Anzahl aktiver AEs berücksichtigt. Für diese Anzahländerungen und zugehörigen Daten wird ein Rollup für die folgenden Datensätze in Vulnerability Responsedurchgeführt:

- VIT
- RT
- Schwachstellenlösung
- Patch-Update

Daten für Patches ohne Lösungen anzeigen

Weitere Informationen zum Anzeigen von Patches ohne Lösungen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Patchen Sie Daten auf Vulnerability Response

Die Dashboards „Schwachstellenmanagement“ (PA) und „CISO“ sind in einem Abonnement mit Performance Analytics für die Anwendung Vulnerability Response enthalten. Wenn Sie ein -Abonnement für Performance Analyticshaben, aber keine Patch-Orchestration-Integration installieren, wird die Registerkarte „Nachbesserung“ im CISO-Dashboard angezeigt, ist jedoch nicht mit Daten gefüllt.

Navigieren Sie für das Dashboard für Schwachstellenmanagement (PA) zu **Alle** > **Vulnerability Response** > **Übersicht**. Klicken Sie auf die Registerkarte **Nachbesserung**, und scrollen Sie zum Ende der Seite, um die Daten der Patch-Updates anzuzeigen: geplante und nicht geplante Patches, Patches mit fehlendem Zieldatum und wöchentliche Anzahl.

Navigieren Sie für das CISO-Dashboard zu **Alle** > **Vulnerability Response** > **CISO-Dashboard**. Wählen Sie die Registerkarte Übersicht aus, scrollen Sie zum Ende der Seite, um Daten zur Patch-Abdeckung anzuzeigen: Relevanz, geplante und nicht geplante Patches und Patches mit fehlendem Zieldatum.

Weitere Informationen zu den Vulnerability Response -Dashboards finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ., Patchen Sie die Orchestrierung mit den -Arbeitsbereichen Vulnerability Response .und Patch-Orchestrationsdaten werden in den Dashboards Vulnerability Response angezeigt.

Planen Sie -Patches mit der Vulnerability Response Patch Orchestration Integration HCL BigFix

Planen Sie Patches aus den Datensätzen für Patch-Updates und Korrekturaufgaben in der Anwendung Vulnerability Response in Ihrer Instanz Now Platform von .

Vorbereitungen
Ab Version 16.1 können Sie Patches aus den -Arbeitsbereichen Vulnerability Response oder der klassischen Umgebung planen.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch zum Anzeigen (schreibgeschützt) von Patch-Informationen zu Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

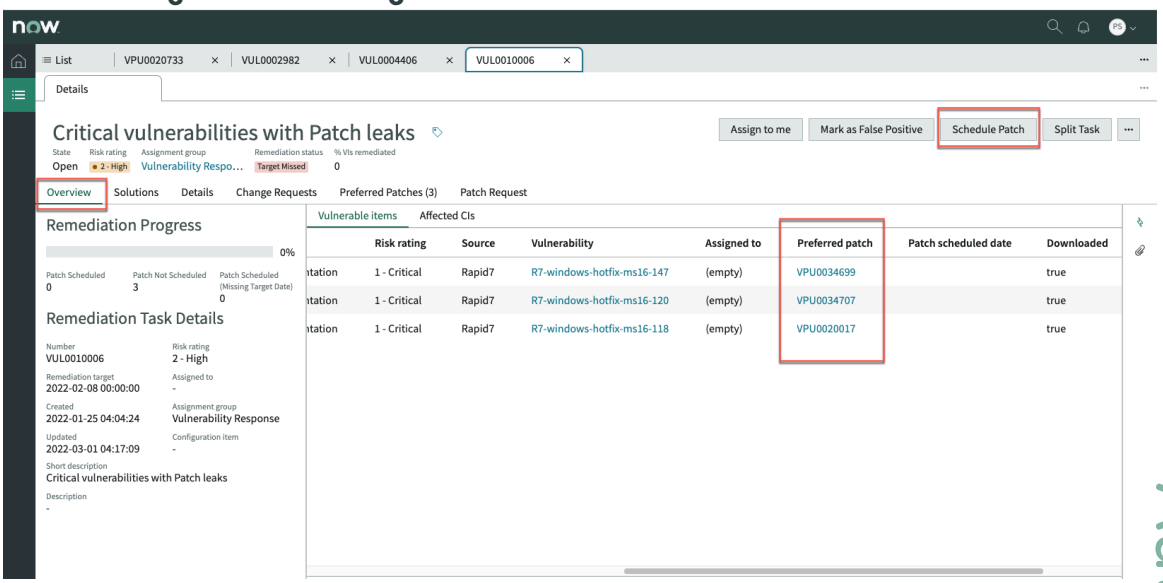
Prozedur

1. Navigieren Sie in den Schwachstellen-Arbeitsbereichen Vulnerability Response als Benutzer mit der Rolle sn_vul.remediation_owner zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Klicken Sie auf der Homepage auf **Preferred patch on VIs (Bevorzugter Patch) zu VIs**.
   Die Liste der Patch-Update-Datensätze für die VIs mit bevorzugten Patches, die Ihnen zugewiesen sind, wird angezeigt.
3. Suchen Sie einen Datensatz, den Sie öffnen möchten, und klicken Sie darauf, um ihn zu öffnen.
4. Alternativ können Sie in der Listenansicht im Arbeitsbereich auf klicken **Patches** > **Alle** und suchen Sie einen Patch-Update-Datensatz.
   Der Patch-Update-Datensatz wird angezeigt. Möglicherweise möchten Sie die Daten überprüfen, bevor Sie einen Patch planen, da möglicherweise bereits andere Patches geplant sind.
5. In der folgenden Tabelle erfahren Sie, welche Daten angezeigt werden und welche Aktionen Sie ausführen können.
6. Klicken Sie auf **Patch planen**.
7. Füllen Sie die Felder im Dialogfeld aus.
8. Klicken Sie auf **Bereitstellen**.
   Die Patch-Anforderung wird zur Überprüfung an gesendet. Sie können den Status aller Ihrer übermittelten Anforderungen im anzeigen **Ausnahmeanforderungen** > **Meine Anforderungen** in der Listenansicht.
9. Alternativ können Sie Patches von Korrekturaufgaben aus planen, die Ihnen oder Ihrer Gruppe zugewiesen sind.

Hinweis:
Die Option zum Planen eines Patches aus einem Korrekturaufgabendatensatz ist nur verfügbar, wenn den AEs in der Aufgabe Patches zugeordnet (mit ihnen) vorhanden sind. Diese Patches werden in der Spalte „Bevorzugter Patch“ angezeigt, wenn Sie bei ausgewählter Registerkarte Übersicht rechts neben dem Datensatz einer Korrekturaufgabe einen Bildlauf durchführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgabe mit bevorzugten Patches



10. Klicken Sie im RT-Datensatz **auf Patch planen** und befolgen Sie die oben aufgeführten Schritte, um die Anwendung im Dialogfeld zu planen.
11. Sie können Patches für die zuvor in der klassischen Umgebung aufgeführten Schritte planen.
    Um diese Datensätze zu finden, führen Sie die folgenden Schritte aus.

    a. Navigieren Sie in der klassischen Umgebung zu **Vulnerability Response** > **Patches** > **Alle**.

    b. Suchen Sie in der angezeigten Liste nach einem Patch-Update-Datensatz.

    c. Navigieren Sie für Korrekturaufgaben zu **Vulnerability Response** > **Korrekturaufgaben** und suchen Sie einen Datensatz.
    Sie können den Korrekturstatus auf der Registerkarte Korrekturstatus nachverfolgen. Am unteren Rand des Datensatzes werden Patch-Daten unter Zugehörige Links angezeigt.

    d. Klicken Sie auf Patch planen, und füllen Sie die Felder aus.

Feld	Beschreibung
Bereitstellungsname	Geben Sie einen Namen für diese Patch-Bereitstellung ein. Dieser Name hilft Ihnen, Ihre Updates nachzuverfolgen.
Patch-Update	Wählen Sie einen aus den verfügbaren Patches in der Liste aus.
Assets	Wählen Sie eines aus: ▪ Computergruppe: Wählen Sie diese Option aus, wenn Sie eine Sammlung (eine Gruppe von Assets) für diesen Patch auswählen möchten. Die Gruppen bestehen aus den Configuration Items, die aus der BigFix-Anwendung importiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Computerliste: Wählen Sie diese Option aus, wenn Sie einzelne Computer (Assets) für diesen Patch auswählen möchten. Im angezeigten Dialogfeld werden Daten zu Hersteller, Standort, Klasse, Zeitpunkt der letzten Aktualisierung und Wartungsplan angezeigt.
Startzeit und Endzeit	Geben Sie die Start- und Endzeiten für das Zeitfenster ein. Geben Sie ein, wann die Bereitstellung des Patches beginnen soll, und geben Sie an, an welchem Tag der Patch installiert werden kann.

REST-Nachrichten für die Integration der Vulnerability Response-Patchorchestrierung mit HCL BigFix

Die Integration der Patch-Orchestration-Integration Vulnerability Response mit HCL BigFix-REST-Nachrichten wird verwendet, um Aufrufe an die BigFix-API zu erstellen.

BigFix-Anmeldung

Sie können auch die REST-Nachrichten für die BigFix-Anmeldung verwenden, um REST-API-Anforderungen zu authentifizieren. Änderungen an der Aufzeichnungsmethode der REST-Nachricht wirken sich auf die an BigFix gesendeten Authentifizierungsanforderungen aus.

Parametername	Wert	Beschreibung
sourceType	kumulativ	Gibt an, dass die Quellintegration Daten aus abruft. Von Code verwendet. Änderungen werden nicht empfohlen.
sortDIR	desc	Gibt die Sortierrichtung für die aus der Integration abgerufenen Daten an. Änderungen werden nicht empfohlen.
sortField	Schweregrad	Gibt das Feld an, auf dem die Datensortierung basiert. Änderungen werden nicht empfohlen.
Typ	Schwachstelle	Gibt den Typ der Daten an, die aus der Integration für die Assets-Integration abgerufen werden sollen. Änderungen werden nicht empfohlen.

BigFix-Integration

Sie können die REST-Nachricht für die BigFix-Integration verwenden, um Informationen von BigFix abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf die Anforderungen an BigFix zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methoden

REST-Methode	Beschreibung
GET – Daten abrufen	Ruft basierend auf der angegebenen Abfrage Informationen von BigFix zu einem der folgenden Elemente ab: • Computer/Computergruppen • Fixlets • Relevante Fixlets auf Computern • Aktionen

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der BigFix-Konsole an

BigFix Patch bereitstellen

Sie können die REST-Nachricht für die BigFix-Integration verwenden, um Patches von Ihrem Now Platform® für BigFix zu planen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an BigFix zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methode	Beschreibung
POST-Bereitstellungs-Patch	Plant den Patch für die BigFix-Konsole auf einem einzelnen/mehreren Computer.

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der BigFix-Konsole an.
Titel	Dynamische Werte basierend auf Anwender	Titel der Bereitstellung.
„settings_tag“	XML-Tag-basierte Einstellungen mit Werten	Gibt Einstellungen an, die andere Parameter aufweisen und während der Planung des Patches an BigFix gesendet werden.
computer_tag	Computer mit XML-Tag und Werten	Gibt die Liste der Computer an, auf denen der Patch geplant wird.
site_name	Wert aus Patch-Update	Name des Standorts, auf dem das Fixlet vorhanden ist.
fixlet_id	Wert aus Patch-Update	ID des Fixlet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datentransformation für die Patch-Orchestration-Integration mit HCL BigFix

Daten werden aus der Patch-Orchestration Vulnerability Response mit HCL BigFix-Integration abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz Now Platform® transformiert.

Import der BigFix-Sammlung

Die Daten aus den importierten Assets (Computer und Computergruppen) werden in die Tabelle „BigFix-Sammlungsimport“ [sn_vul_bigfix_collection_import] geladen. Das Import-TM für BigFix-Computer und Computergruppen (Transformationszuordnung?) wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import der BigFix-Sammlung verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach BigFix Computer und Computer Groups Import TM. In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Skript-Timing für BigFix-Computer und Computergruppen transformieren

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und Sammlungen sowie der Beziehung zwischen ihnen. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Umfangsvariablen [sn_vul_bigfix]. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, mit dem die Anzahl der erstellten, aktualisierten und ignorierten CIs festgelegt wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

BigFix-Fixlet Import

Die Daten aus den importierten Fixlets werden in die Tabelle „BigFix-Fixlet-Import“ [sn_vul_bigfix_patch_update_import] geladen.

Das BigFix Fixlet Import TM wird zum Transformieren der importierten Informationen verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem BigFix-Fixlet-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie das BigFix-Fixlet Import-TM.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Transformationszuordnungsfelder für BigFix-Fixlet importieren

Quellenfeld	Zielfeld	Beschreibung
u_id	Artikel-ID	Eindeutige ID eines Fixlets in einer Site.
u_id	source_id	Eindeutige ID eines Fixlets in einer Site.
U_site_name	sn_vul_bigfix_site_name	Name der Site in BigFix, auf die sich das Fixlet verlässt.
U_display_name	Titel	Titel des Fixlet.
[Skript]	Bulletin_id	Quell-ID der Lösung.
[Skript]	sn_vul_solution	Lösung basierend auf der Quell-ID.
U_source	bulletin_source	Quellanbieter der Lösung.
[Skript]	Date_release	Release-Datum des Fixlets.
U_category	Update_category	Kategorie des Fixlets.
[Skript]	Ist_höchste_Supersedence	Boolescher Wert, der angibt, ob das Fixlet die höchste Ersatzlösung ist oder nicht.
[Skript]	Ist_downloadet	Boolescher Wert, der festlegt, ob das Fixlet heruntergeladen wurde oder nicht.
[Skript]	Integrationsinstanz	Name der Instanz, aus der das Fixlet importiert wird.
U_source_severity	Source_severity	Schweregrad des Fixlets.
U_applicable_count	Num_total	Gesamtanzahl der Geräte mit fehlenden Fixlets.
[Skript]	Last_modified	Datum der letzten Änderung des Fixlet.

Skript-Timing für BigFix-Fixlet-Importtransformationszuordnung

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skript-Timing für BigFix-Fixlet-Importtransformationszuordnung (Fortsetzung)

Skript	Beschreibung
	zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Das Skript, das zum Aktualisieren der Werte in der Umfangsvariablen [sn_vul_bigfix] verwendet wird Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Fixlets verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

BigFix Device Fixlet Import

Die Daten aus den importierten relevanten Fixlets auf Computern werden in die Tabelle „BigFix Device Fixlet Import“ [sn_vul_bigfix_device_patch_import] geladen.

Das BigFix Device Fixlet TM wird zum Transformieren der importierten Informationen verwendet.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem BigFix Device Fixlet-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie das BigFix Device Fixlet TM.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Skript-Timing für BigFix-Geräte-Fixlet-Transformationszuordnung

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und Sammlungen sowie der Beziehung zwischen ihnen. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Umfangsvariablen [sn_vul_bigfix]. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skript-Timing für BigFix-Geräte-Fixlet-Transformationszuordnung (Fortsetzung)

Skript	Beschreibung
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, mit dem die Anzahl der erstellten, aktualisierten und ignorierten CIs festgelegt wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von BigFix-Aktionen

Die Daten aus den importierten Aktionen werden in die Tabelle „BigFix-Aktionsimport“ [sn_vul_bigfix_deployment_import] geladen.

Das BigFix Actions Import-TM wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem BigFix-Aktionsimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie das BigFix-Fixlet Import-TM.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

BigFix-Aktionen importieren Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID einer Aktion.
U_name	name	Name der Aktion
[Skript]	sn_vul_bigfix_discovered_item	Referenz des erkannten Elements, für das der Patch bereitgestellt wird
U_status	status	Status der Aktion
[Skript]	sn_vul_patch_orch_update	Referenz des Patches
U_apply_count	Anzahl_Erfolg	Erfolgsanzahl der Aktion.
U_retry_count	Erneut versuchen	Wiederholungsanzahl der Aktion.
[Skript]	Bereitstellungszeit	Startzeit der Aktion.
[Skript]	Frist	Endzeit der Aktion.
[Skript]	Quelle_erstellt	Erstellungszeit der Aktion.
[Skript]	Integrationsinstanz	Name der Instanz, aus der die Aktion importiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

BigFix-Aktionen importieren das Timing des Transformationszuordnungsskripts

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Das Skript, das zum Aktualisieren der Werte in der Umfangsvariablen [sn_vul_bigfix] verwendet wird Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, mit dem die Anzahl der erstellten, aktualisierten und ignorierten Aktionen festgelegt wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Beispiel-Workflow für die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix

Ein Beispiel für die Funktionsweise der Patch-Orchestrierung mit dem HCL BigFix-Produkt.

Vorbereitungen

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gepatcht. Das letzte Patchfenster wurde vor einer Woche abgeschlossen, Sie möchten jedoch einen Patch anwenden, um eine kritische Schwachstelle zu beheben, die kürzlich bekannt wurde. Aufgrund der Relevanz dieser Schwachstelle können Sie nicht zwei weitere Wochen auf den nächsten geplanten Patch warten.

Erforderliche Rollen:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für den Arbeitsbereich des Schwachstellenmanagers.
- sn_vul.remediation_owner, um den Arbeitsbereich des IT-Korrekturbesitzers anzuzeigen.
- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches.
- sn_vul_patch_orch.read_patch zum Anzeigen (schreibgeschützt) von Patch-Informationen zu Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind.

Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenmanager oder Analyst, der im Arbeitsbereich des Schwachstellenmanagers arbeitet, können Sie Überwachungsthemen erstellen oder vorhandene Überwachungsthemen bearbeiten, um importierte VIs mit kritischen Schwachstellen zu erfassen. Mit der Patch-Orchestration-Integration können Sie auch die Patches anzeigen, die Sie zum Beheben und Nachverfolgen dieser Schwachstellen verwenden möchten. In der folgenden Tabelle sind einige Beispiele mit den Bedingungen aufgeführt, die Sie für Überwachungsthemen für die Patch-Orchestrierung festlegen können. Verwenden Sie diese Beispiele, um die Einstellungen zu bestimmen, die für Ihre Umgebung am besten geeignet sind. Weitere Informationen zum Einrichten des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachungsthemas finden Sie unter Erstellen Sie ein Überwachungsthema in Vulnerability Manager Workspace.

Beispiel-Überwachungsthemen für Patch-Orchestrierung im Arbeitsbereich des Schwachstellen-Managers

Name des Überwachungsthemas	Beschreibung
Kritische Schwachstellen mit Patchverlusten	Risikobewertung ist 1 – kritisch UND Grund: Patch nicht geplant
Kritische Schwachstellen mit geplanten Patches (fehlendes SLA)	Grund: Patch geplant (fehlendes Zieldatum)
Kritische Schwachstellen mit geplanten Patches	Risikobewertung ist 1 – kritisch UND Geplantes Patch-Datum ist nicht leer UND Grund: Patch geplant

- Als Schwachstellenmanager oder Analyst generieren Sie nach dem Erstellen der Überwachungsthemen und Korrekturmaßnahmen Korrekturaufgaben. Von VI-Datensätzen und Korrekturaufgaben aus können Sie einen Drilldown zur Registerkarte Erkennungen durchführen und die Datensätze erkannter Elemente finden, die die von Ihnen verfolgte Schwachstelle aufweisen, zusammen mit den vom BigFix-Produkt importierten Assets.
- Als Schwachstellenanalyst oder Administrator können Sie die mit der Schwachstelle verknüpften Patchdaten überwachen. Sie können auch einen oder mehrere Patches für ein bestimmtes Asset (Konfigurationselement) aus einem Datensatz für ein erkanntes Element bereitstellen.

Als IT-Nachbesserungsspezialist haben Sie verschiedene Möglichkeiten, um die Schwachstelle mit einer Patch-Bereitstellung zu beheben.

- Sie können den Patch von einem Patch Update-Datensatz (VPU#) aus planen.
- Wenn angreifbaren Elementen (VI) bevorzugte Lösungen zugeordnet sind und Sie oder Ihre Gruppen zugewiesen sind, können Sie die Patches über eine Korrekturaufgabe mit diesen angreifbaren Elementen planen.

Prozedur

1. Klicken Sie als IT-Korrekturspezialist im IT-Korrektur-Arbeitsbereich auf die Ansicht Startseite.
2. Klicken Sie in der Ansicht „Start“ auf die Bewertungsliste **Zugewiesene Korrekturaufgaben,** um die Datensätze anzuzeigen.

   Für dieses Beispiel können Sie das Feld Kurzbeschreibung der Korrekturaufgabe (VUL#) auf beliebigen Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht. Angenommen, Sie wissen vielleicht, dass Ihr Schwachstellenmanager ein Überwachungsthema mit der Bezeichnung Kritische Schwachstellen mit Patch-Lecks zum Erfassen von VIs (VIT#) mit dieser kritischen Schwachstelle erstellt hat.

   Bei geöffnetem Datensatz können Sie auch die VIs und die bevorzugten Patches überprüfen und sehen, ob Sie oder andere Mitglieder Ihrer Gruppe bereits Patch-Anforderungen zur Genehmigung übermittelt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenn Sie über genügend Informationen verfügen, können Sie jetzt von dieser Korrekturaufgabe aus eine Patch-Anforderung senden.

   Hinweis:
   Wenn den AEs, die dem Datensatz zugeordnet sind, keine Patches zugeordnet sind, ist die Schaltfläche **Patch planen** für den Datensatz nicht verfügbar.

4. Klicken Sie auf **Patch planen** und füllen Sie die Felder im Dialogfeld aus.
   Weitere Informationen zum Planen von Patches finden Sie unter Planen Sie -Patches mit der Vulnerability Response Patch Orchestration Integration HCL BigFix.

5. Alternativ können Sie in der Listenansicht im IT-Korrekturarbeitsbereich auf die Links Korrekturaufgaben, Angreifbare Elemente, Lösungenund Patches klicken, um diese Datensätze anzuzeigen.

   In diesem Beispiel kennen Sie anstelle des Namens eines Überwachungsthemas möglicherweise die Artikel-ID oder die Bulletin-ID und den Titel des Patches. Wenn dies der Fall ist, sollten Sie überprüfen, ob Ihnen oder Ihren Gruppen eines der VIs mit dieser Schwachstelle zugewiesen ist. Von Patch-Update-Datensätzen aus können Sie Patch-Anforderungen übermitteln. In VI-Datensätzen können Sie nach potenziellen Patches suchen und die zugehörige Korrekturaufgabe öffnen, wenn Sie eine Patch-Anforderung senden möchten.

6. Wenn Sie keinen Zugriff auf die Arbeitsbereiche von haben oder Daten anzeigen und Patches in der klassischen Umgebung planen möchten, führen Sie die folgenden Schritte aus.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**.

   b. Suchen Sie den gewünschten Patch Update-Datensatz.
      Unter Umständen möchten Sie die Datensätze nach kritischen Risikopunktzahlen filtern.

   c. Überprüfen Sie die zugeordneten Felder „VIs“ und „% der korrigierten AEs“ auf der Registerkarte Korrekturstatus.
      Wenn für die VIs Patches verfügbar sind, wird oben rechts im Datensatz die Schaltfläche **Patch planen** angezeigt.

   d. Wenn Sie eine Anforderung senden möchten, klicken Sie auf **Patch planen**.
      Weitere Informationen zum Planen von Patches finden Sie unter Planen Sie -Patches mit der Vulnerability Response Patch Orchestration Integration HCL BigFix.

   e. Angenommen, Sie haben keine Patch-ID-Informationen, können jedoch im Feld Kurzbeschreibung der Korrekturaufgaben, die Ihrer Gruppe zugewiesen sind, nach Text suchen, der sich auf Ihre kritische Schwachstelle bezieht.

   f. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.

   g. Suchen Sie den gewünschten Datensatz, und klicken Sie darauf, um ihn zu öffnen.
      Überprüfen Sie im geöffneten Datensatz die Registerkarte Korrekturstatus auf AEs und Behobene AEs in Prozent. Klicken Sie auf die zugehörigen Links für VI-Datensätze, Bevorzugte Lösungen, Bevorzugte Patchesund Patch-Anforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn den AEs, die dem Datensatz zugeordnet sind, keine Patches zugeordnet sind, ist die Schaltfläche **Patch planen** für den Datensatz nicht verfügbar.

h. Klicken Sie im Datensatz **auf Patch planen,** wenn Sie eine Patch-Anforderung senden möchten.

Informationen zur Integration der Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM

Verwalten Sie Patches und Patch-Bereitstellungen für die kritischen Schwachstellen in Ihren Assets mit der Integration von Vulnerability Response in das Produkt MicrosoftMicrosoft Azure Event Hubs System Center Configuration Manager (SCCM).

Patch-Orchestrierung mit Vulnerability Response

Bei der Patch-Orchestrierung mit Vulnerability Response werden geplante Importe von Lösungsintegrationen von Drittanbietern, Patch-Anbietern und Schwachstellen-Scannern verwendet. Die Scanner-Erkennungsdaten gleichen die Assets in Ihrer Umgebung mit Schwachstellen und den Patch-Updates ab, die sie beheben können. Sie übermitteln Patch-Anforderungen zur Genehmigung, planen Patch-Updates, um angreifbare Elemente zu beheben, und überwachen den Fortschritt der Remediation – alles von Ihrer Instanz Now Platform® aus.

Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM

Wenn die Anwendung Vulnerability Response Patch Orchestration mit der Anwendung MicrosoftMicrosoft Azure Event Hubs SCCM mit den Anwendungen ServiceNow® Vulnerability Solution Management, Patch Orchestration und Vulnerability Response verwendet wird, können Schwachstellenmanager und -analysten die folgenden Aufgaben ausführen:

- Sehen Sie sich weiteren Kontext und Informationen zu den Arten von Patches und den Lösungen der Lieferanten (Patches) an.
- In den -Arbeitsbereichen Vulnerability Response können Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Nachbesserung von Schwachstellen aus Datensätzen anzeigen und überwachen.

IT-Spezialisten und Korrekturbesitzer können die folgenden Aufgaben ausführen:

- Stellen Sie Patches, die vom Produkt MicrosoftMicrosoft Azure Event Hubs SCCM unterstützt werden, für Windows, CentOS, macOS, Oracleund andere Assets in regelmäßigen, geplanten Intervallen außerhalb der Geschäftszeiten bereit, um Konflikte mit der Arbeit zu vermeiden.
- Identifizieren Sie Assets ohne Patch mit Schwachstellen oder Assets, die durch geplante Patches nicht erfolgreich aktualisiert wurden, aus importierten Erkennungsdaten von Drittanbieterscannern.
- Planen Sie verfügbare Patches aus dem IT-Korrekturarbeitsbereich oder der klassischen Anwenderoberfläche für angreifbare, nicht gepatchte Assets aus Patch-Updates, Korrekturaufgaben und Datensätzen erkannter Elemente.

Schlüsselbegriffe in den SCCM-Anwendungen Vulnerability Response und MicrosoftMicrosoft Azure Event Hubs .

Konfigurationselement bzw. Configuration Item (CI)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs sind die vorhandenen Assets, die in Ihren Configuration Management Database (CMDB)aufgeführt sind. MicrosoftMicrosoft Azure Event Hubs SCCM bezeichnet CIs als Geräte.

Sammlungen und Gerätesammlungen

Im Produkt MicrosoftMicrosoft Azure Event Hubs SCCM verwendete Terminologie, die sich auf eine Gruppe von Assets bezieht.

Angreifbares Element

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht.

Instanz

Ein eindeutiger Account der SCCM-Anwendung MicrosoftMicrosoft Azure Event Hubs. Jeder Benutzeraccount kann eine Instanz in der SCCM-Anwendung MicrosoftMicrosoft Azure Event Hubs sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für eine Instanz Now Platform.

Integration

Eine -Integration ist eine geplante Aufgabe in Now Platform, die Informationen von einer Drittanbieterquelle abruft, z. B. die Integration mit den MicrosoftMicrosoft Azure Event Hubs -SCCM-Computern.

Lösung

Im Kontext dieser Integration gibt es zwei Arten von Lösungen: potenzielle und bevorzugte. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben kann. Schwachstellen haben oft viele potenzielle Lösungen. Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte, erkannte Schwachstelle.

Patches

Software-Updates, die Schwachstellen beheben. In der Anwendung MicrosoftMicrosoft Azure Event Hubs SCCM werden Patches als Patches bezeichnet. MicrosoftMicrosoft Azure Event Hubs SCCM enthält beispielsweise Patches für Windows, CentOS, MAC, Oracle und andere Produkte.

Bevorzugter Patch

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Sobald Patches bereitgestellt wurden, werden sie den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und beheben sie.

Korrekturaufgabe oder, vor v15.0 von Vulnerability Response, Schwachstellen-Gruppen

Listen angreifbarer Elemente in der Anwendung Vulnerability Response von Aktionen, die zum Beheben von Schwachstellen erforderlich sind.

Bereitstellung

Für die Zwecke dieser Integration bedeutet Bereitstellung, wenn Sie einen Patch auf einen Computer anwenden, initiieren oder planen. Sie können die von MicrosoftMicrosoft Azure Event Hubs SCCM heruntergeladenen Patches in Now Platform bereitstellen, indem Sie zu erkannten Elementen, Patches oder Korrekturaufgaben aus einzelnen Datensätzen in Vulnerability Responsenavigieren. Sie können Patches mit geplanten Aufgaben auf einzelnen Computern oder Computergruppen bereitstellen.

Die Bereitstellung in Now Platform kann sich auch auf eine Integration beziehen, die mehrere Quellen unterstützt. Das Vorhandensein einer einzelnen Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie mehrere Bereitstellungen der MicrosoftMicrosoft Azure Event Hubs SCCM Vulnerability-Integration in Ihrer Umgebung haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Solution Management und die Vulnerability Response Patch-Orchestration-Integration mit MicrosoftMicrosoft Azure Event Hubs SCCM

Die Anwendung Vulnerability Solution ManagementNow Platform korreliert Ihre Schwachstellenergebnisse mit der Aufgliederung der Lösungen (Patches), die sie beheben. Identifizieren Sie die Softwarepatches von Drittanbietern für Produkte und Services, Konfigurationsupdates und andere Steuerungen, die die größten Auswirkungen für Ihre Organisation haben. Zusammen mit den Informationen zu Drittparteiscannern arbeiten die Anwendungen Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM zusammen, um ein Rollup bevorzugter Patches von der Lösung über die Schwachstelle bis zum angreifbaren Element durchzuführen, um Sie bei der Behebung von und zu unterstützen Schwachstellen in Ihrer Umgebung zu schließen. Die SCCM-Integrationsanwendungen Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration MicrosoftMicrosoft Azure Event Hubs sind alle in ServiceNow® Storeverfügbar.

Erforderliche Now Platform-Rollen

Für die Installation, Konfiguration und Korrekturaufgaben der Integration sind die folgenden Rollen in Ihrer Instanz Now Platform erforderlich.

Administrator

Benutzer mit dieser Rolle erhalten Berechtigungen für Anwendungen in den Instanzen ServiceNow Store und laden sie in die Instanzen Now Platform herunter.

sn_vul.vulnerability_admin

Benutzer mit dieser Rolle aktivieren Anwendungen in der Instanz Now Platform und schließen die Konfiguration der Anwendung Vulnerability Response ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Dieser Administratorbenutzer konfiguriert alle VR-Anwendungen, Regeln und Drittanbieterintegrationen.

sn_vul_sccm.configure_integration

Benutzer mit dieser Rolle konfigurieren die Anwendung MicrosoftMicrosoft Azure Event Hubs SCCM Patch Orchestration Integration. Diese Rolle enthält die granulare Rolle sn_vul_sccm.read_integration.

sn_vul_sccm.read_integration

Benutzer mit dieser Rolle können die Datensätze der Anwendungen Vulnerability Response und MicrosoftMicrosoft Azure Event Hubs SCCM Patch Orchestration Integration und die Patch Orchestration-Daten anzeigen (schreibgeschützt).

sn_vul_patch_orch.configure_patch

Benutzer mit dieser Rolle können -Patches konfigurieren und anwenden.

sn_vul_patch_orch.read_patch

Benutzer mit dieser Rolle können Patch-Informationen anzeigen (schreibgeschützt).

Verantwortliche Vertragsgenehmigung

Mit können Sie den Genehmigergruppen Genehmigerebene 1 und Genehmigerebene 2 verwenden, wenn Sie möchten, dass übermittelte Patch-Anforderungen vor der Bereitstellung genehmigt werden.

Weitere Informationen zum Zuweisen dieser Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Suchregeln

Wenn Daten aus der SCCM-Anwendung MicrosoftMicrosoft Azure Event Hubs importiert werden, sucht die Anwendung Vulnerability Response anhand von Ressourcen-ID-Daten automatisch nach Übereinstimmungen in Configuration Management Database (CMDB). CI-Suchregeln werden verwendet, um CIs (Assets) zu identifizieren und sie automatisch zu Datensätzen angreifbarer Elemente (VI) hinzuzufügen, wenn VIs erstellt werden. Die folgenden CI-Suchregeln sind im Lieferumfang des Basissystems enthalten und werden verwendet, um CIs (Assets) zu identifizieren und den erkannten Elementen hinzuzufügen.

Diese Suchregel basiert auf den Daten, die vom Service Graph Connector mit SCCM importiert werden. Sie müssen die CMDB-Integration installieren und ausführen, bevor Sie die SCCM-Integrationen ausführen. Wenn Sie mehrere Installationen des SCCM-Servers haben, können Sie den Service Graph Connector-Verbindungsalias auf der Konfigurationsseite der SCCM-Patch-Orchestration konfigurieren.

MID-Server

Die Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM ist eine lokale Integration. Erfordert einen eigenständigen Windows MID Server, der nicht Teil eines MID Server-Clusters ist. Der MID-Server ist erforderlich, um auf Remotecomputern von Ihrer Instanz Skripts auszuführen und Daten vom SCCM-Server zu importieren. APIs für diese Integration werden mithilfe von MID-Servern aufgerufen, die Sie in Ihrer Instanz Now Platform einrichten. Bereiten Sie die Integration der Patch Orchestration Vulnerability Response mit MicrosoftMicrosoft Azure Event Hubs SCCM vor.

Integrationen und Abhängigkeiten von Vulnerability Response Patch Orchestration mit der Anwendung MicrosoftMicrosoft Azure Event Hubs SCCM

Die folgenden Produkt- und Abhängigkeitsanwendungen sind für die Integration von Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs System Center Configuration Manager (SCCM) erforderlich. Diese Anwendungen sind im verfügbar ServiceNow® Store

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

Zum Anzeigen von Daten der Patch-Orchestrierung und verfügbarer Updates (Patches) in den Arbeitsbereichen und auf der klassischen Anwenderoberfläche in Vulnerability Responsesind die folgenden Anwendungen erforderlich. Alle aufgeführten Anwendungen sind unter ServiceNow® Storeverfügbar. Einige Anwendungen erfordern separate Abonnements.

Weitere Informationen zur Versionskompatibilität mit den erforderlichen Anwendungen und Familienreleases finden Sie im Artikel KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen in der HI Knowledge Base.

Anwendungs- und Releaseversion
Vulnerability Response
Vulnerability Solution Management
Anwendung Vulnerability Response Patch Orchestration
Anwendung Vulnerability Response Patch Orchestration with Microsoft SCCM
Security Support Common

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungs- und Releaseversion
Security Support Orchestration
Service Graph Connector mit SCCM

Vulnerability Response Patch Orchestration-Anwendungstabellen

Die Anwendung Vulnerability Response Patch Orchestration enthält die folgenden Tabellen:

Tabelle	Beschreibung
Patch-Update [sn_vul_patch_orch_update]	Speichert Informationen zu den Patches, die auf verschiedenen Instanzen verfügbar sind.
Geräte-Update [sn_vul_patch_orch_m2m_src_ci_update]	Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in Datensätzen für erkannte Elemente angezeigt werden.
Sammlung [sn_vul_patch_orch_collection]	Speichert Sammlungsdaten aus verschiedenen Instanzen.
Gerätesammlung [sn_vul_patch_orch_m2m_src_ci_collection]	Speichert Sammlungsdaten zu erkannten Elementen.
Patch-Bereitstellung [sn_vul_patch_orch_deployment]	Speichert Informationen über bereitgestellte Patches für Sammlungen und CIs.
Potenzieller Patch [sn_vul_patch_orch_m2m_vuln_patch]	Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zum Beheben einer Schwachstelle verwendet werden können.

Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM integrations

Die von ServiceNow® Engineering entwickelten Integrationen bilden die orchestrierte Lösungsbereitstellung mit dem Produkt MicrosoftMicrosoft Azure Event Hubs SCCM. Die folgenden Integrationen sind in der Anwendung Microsoft SCCM Patch Orchestration Integration enthalten, die Sie von ServiceNow® Storeherunterladen können.

Nachdem Sie die Integrationsanwendung in Ihrer Instanz Now Platform installiert haben, navigieren Sie zum Anzeigen dieser Integrationen zu **Integrationen** > **SCCM Patch Orchestration Integration** > **Integrationen**. Die Anwendung Vulnerability Response verarbeitet Daten in geplanten Zeitintervallen, die von diesen Integrationen importiert wurden, mit MicrosoftMicrosoft Azure Event Hubs -SCCM-Endpunkten.

Integration	Beschreibung
MicrosoftMicrosoft Azure Event Hubs Integration der SCCM-Sammlung	• Diese Integration ist für die tägliche Ausführung geplant und wird zuerst in der verketteten Integrationsausführung ausgeführt. • Ruft die Gerätesammlungen aus den SCCM-Sammlungen ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
MicrosoftMicrosoft Azure Event Hubs Integration der SCCM-Gerätesammlung	• Wenn sie geplant ist, wird diese Integration durch den Abschluss der Integration der SCCM-Sammlung ausgelöst. Sie können ihn auch bei Bedarf ausführen. • Diese Integration ruft die Geräte unter jeder Sammlung ab. Diese Integration erstellt Datensätze in der Tabelle „Erkannte Elemente“ und in der Tabelle „Gerätesammlung“.
MicrosoftMicrosoft Azure Event Hubs Integration mit SCCM-Patch-Updates	• Wenn sie geplant ist, wird diese Integration durch den Abschluss der Integration für die SCCM-Gerätesammlung ausgelöst. Sie können ihn auch bei Bedarf ausführen. • Ruft vom SCCM-Server Informationen zu den Patches ab, die auf Geräten (Assets) installiert sind oder fehlen.
MicrosoftMicrosoft Azure Event Hubs Integration von SCCM-Bereitstellungen	• Wenn diese Integration geplant ist, wird sie durch den Abschluss der Patch-Update-Integration ausgelöst. Sie können ihn auch bei Bedarf ausführen. • Ruft Informationen zu den Patches ab, die vom IT-Team auf dem SCCM-Server geplant wurden.

Bereiten Sie die Integration der Patch Orchestration Vulnerability Response mit MicrosoftMicrosoft Azure Event Hubs SCCM vor

Bereiten Sie die Integration vor, indem Sie die folgenden Setupaufgaben ausführen.

Vorbereitungen

Erforderliche Rolle: admin für die Installation der Anwendungen und das Zuweisen von Rollen. Andere Rollen sind in der folgenden Tabelle aufgeführt.

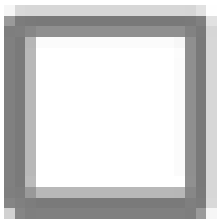
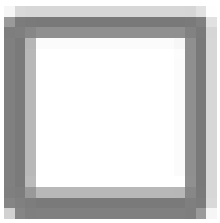
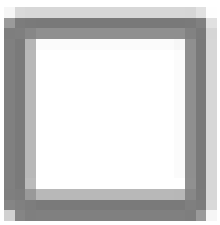
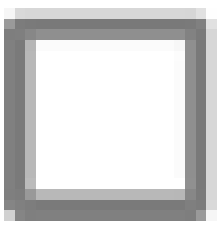
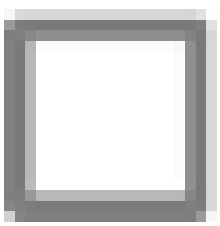
Warum und wann dieser Vorgang ausgeführt wird

Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration.

Prozedur

1. Befolgen Sie die folgende Prüfliste für eine reibungslose Installation und Konfiguration der Anwendung Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM.
2. Sie können die folgende Prüfliste ausdrucken und überprüfen, ob die aufgelisteten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Informationen zu Schwachstellen und Patches in Ihre Instanz Now Platform® importieren.

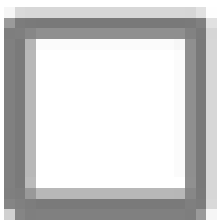
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	(Optional) Wenn die Anwendung noch nicht installiert und aktiviert ist, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher.
	Wenn noch nicht installiert ist, beschaffen Sie sich Berechtigungen und installieren Sie die Scanner-Anwendung einer Drittpartei, um Schwachstellendaten zu importieren. Unter Vulnerability Response-Integrationen finden Sie weitere Informationen zu Scannern von Drittparteien, die von Vulnerability Responseunterstützt werden. Weitere Informationen finden Sie unter .
	Wenn die Anwendung Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM noch nicht installiert ist, rufen Sie Berechtigungen ab und laden Sie sie in Ihre Instanz Now Platform® herunter. Weitere Informationen finden Sie unter .
	Rufen Sie die SCCM-Anmeldeinformationen MicrosoftMicrosoft Azure Event Hubs ab. Stellen Sie sicher, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre MicrosoftMicrosoft Azure Event Hubs -Produkte erforderlich sind, damit Sie darauf zugreifen können.
	Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator ruft Berechtigungen ab, lädt die Anwendung MicrosoftMicrosoft Azure Event Hubs SCCM Patch Orchestration und die anderen für die Integration erforderlichen Anwendungen herunter und installiert sie. Wenn dies nicht zugewiesen ist, weist der Administrator den Schwachstellen-Administrator (sn_vul.vulnerability_admin) und andere Rollen im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Setup-Assistenten in Vulnerability Response oder über das Modul Benutzeradministration zu. **sn_vul.vulnerability_admin** Nach der Zuweisung schließt der Schwachstellen-Administrator die Konfiguration der MicrosoftMicrosoft Azure Event Hubs SCCM-Integrationen und der anderen Anwendungen von Drittparteien ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Diese Rolle konfiguriert alle VR-Anwendungen, Regeln, Drittanbieterintegrationen, Vulnerability Response Patch Orchestration- und Vulnerability Solution Management-Anwendungen. **sn_vul_sccm.configure_integration** Benutzer mit dieser Rolle konfigurieren die Anwendung MicrosoftMicrosoft Azure Event Hubs SCCM Patch Orchestration Integration. Diese Rolle enthält die granularen Rollen sn_vul_sccm.read_integration und connection_admin, die es dem Benutzer ermöglichen, eine Verbindung zur SCCM-Konsole herzustellen und die Integrationsinstanzen in Ihrem Now Platformzu konfigurieren. **sn_vul_sccm.read_integration** Benutzer mit dieser Rolle können die Datensätze der Anwendungen Vulnerability Response und MicrosoftMicrosoft Azure Event Hubs SCCM Patch Orchestration Integration und die Patch Orchestration-Daten anzeigen (schreibgeschützt). **sn_vul_patch_orch.configure_patch** Benutzer mit dieser Rolle können -Patches konfigurieren und anwenden. Von diesem Anwender angeforderte Patches aus Datensätzen für angreifbare Elemente und Patch-Updates werden zur Genehmigung gesendet, wenn Change-Management aktiv ist und Genehmiger zugewiesen sind. **sn_vul_patch_orch.read_patch** Benutzer mit dieser Rolle können Patch-Informationen für Datensätze anzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind. **Verantwortliche Vertragsgenehmigung** Benutzer, die der Genehmigerebene 1 und optional der Genehmigerebene 2 zugewiesen sind, genehmigen die Genehmigergruppen, die eingereichte Patch-Anforderungen genehmigen. Standardmäßig werden Patches vor der Bereitstellung zur Genehmigung an die Genehmigerebene-1-Gruppe übermittelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Weitere Informationen zum Genehmigungsprozess finden Sie unter Konfigurieren Sie die Integration von Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM. Weitere Informationen zum Einrichten von Genehmigern und Gruppen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Die erstmalige Zuweisung von Rollen zu Benutzern und Gruppen für die Integration erfolgt durch den Systemadministrator. Standardmäßig ist die Gruppe Vulnerability Response verfügbar. Wenn dies noch nicht erstellt wurde, können Sie zusätzliche Gruppen für die Rollen „Remediationsspezialist“ und „Schwachstellenanalyst“ erstellen und Benutzer mit dem Modul „Benutzeradministration“ in Ihrer Instanz hinzufügen. Weitere Informationen finden Sie unter Benutzergruppen erstellen .
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz von aktiviert haben, die für die Integration erforderlich sind. ○ Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM ist eine lokale Integration, für die Sie einen eigenständigen Windows MID Server verwenden müssen. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . ○ Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es.

Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM

Laden Sie die Anwendung von ServiceNow Storeherunter.

Vorbereitungen

Stellen Sie vor der Installation der Anwendung sicher, dass Sie alle Elemente in der Prüfliste in Bereiten Sie die Integration der Patch Orchestration Vulnerability Response mit MicrosoftMicrosoft Azure Event Hubs SCCM vorabgeschlossen haben.

Erforderliche Rolle: admin für die erstmalige Zuweisung der Rolle sn_vul.vulnerability_admin und die Installation der Anwendung. (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)), um Vulnerability Response Patch Orchestration MicrosoftMicrosoft Azure Event Hubs SCCM und andere Anwendungen nach der Installation zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, ist es nicht erforderlich, die Berechtigung „Weiter mit Aktivieren Sie eine ServiceNow Store -Anwendung“ zu erhalten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie die Anwendung **Vulnerability Response Patch Orchestration with Microsoft SCCM,** und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung installiert, die Sie aus ServiceNow Storeheruntergeladen haben.

3. Alternativ können Sie Anwendungen über den Setup-Assistenten installieren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.

Nächste Maßnahme
Navigieren Sie nach Abschluss der Installation zu **Alle** > **Microsoft SCCM Patch Orchestration Integration** > **Konfiguration** um mit der Konfiguration fortzufahren.

Konfigurieren Sie die Integration von Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM

Nachdem Sie die Anwendung installiert haben, konfigurieren Sie sie mit Ihren Kontoinformationen, und validieren Sie Ihre Anmeldeinformationen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin und sn_vul_sccm.configure_integration

Prozedur

1. Navigieren zu **Alle** > **Microsoft SCCM Patch Orchestration Integration** > **Konfiguration**.
2. Füllen Sie die Felder mit Ihren MicrosoftMicrosoft Azure Event Hubs SCCM-Informationen und -Anmeldeinformationen aus.

Feld	Beschreibung
Integrationsinstanz	Der Name des MicrosoftMicrosoft Azure Event Hubs -SCCM-Instanzkontos, das Sie verwenden möchten, z. B. Microsoft SCCM Patch Management Integration.
Hostname	Geben Sie die URL für den SCCM-Host MicrosoftMicrosoft Azure Event Hubs ein.
Anwendername	Geben Sie Ihren MicrosoftMicrosoft Azure Event Hubs SCCM-Account-Anwendernamen ein.
Passwort	Geben Sie Ihr MicrosoftMicrosoft Azure Event Hubs Passwort für den SCCM-Account ein.
MID-Server	Geben Sie den Namen des eigenständigen MID-Servers aus der Liste ein, den Sie verwenden möchten. Weitere Informationen zu MID-Servern und zum Einrichten von Aufgaben in Ihrem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Now Platform® finden Sie unter Bereiten Sie die Integration der Patch Orchestration Vulnerability Response mit MicrosoftMicrosoft Azure Event Hubs SCCM vor.

3. Klicken Sie auf Anmeldeinformationen speichern und testen.
   Der Status Ihrer Verbindung zwischen MicrosoftMicrosoft Azure Event Hubs SCCM und Ihrer Instanz Now Platform® wird im Feld Validierungsstatus angezeigt. Wenn Sie keinen erfolgreichen Test sehen, befolgen Sie die Eingabeaufforderungen.

4. **Wahlweise:** Domänentrennung wird für diese Integration unterstützt.
   Sie können Ihrer -Instanz mehrere Konfigurationen hinzufügen. So fügen Sie zusätzliche Konfigurationen hinzu:

   a. Navigieren zu **Alle** > **Microsoft SCCM Patch Orchestration Integration Integrationsinstanzen**.

   b. Stellen Sie sicher, dass im Feld Anwendungsbereich der Anwendungsbereich Vulnerability Response Patch Orchestration with Microsoft SCCMangezeigt wird.

   c. Klicken Sie auf **Neu**.

   d. Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Name für die Integrationsinstanz.
Anwendung	Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM
Integration	[Schreibgeschützt] MicrosoftMicrosoft Azure Event Hubs SCCM Patch Management (SCCM-Patchverwaltung) ist Standard.
Aktiv	Standardmäßig ist aktiviert. Wenn diese Option gelöscht wird, ist die Instanz nicht aktiv.

   e. Klicken Sie auf **Absenden**.
   Ihre neue Integrationsinstanz wird in der Liste Integrationsinstanzen angezeigt.

   f. Wiederholen Sie die Schritte 1 bis 3, um Ihre Integrationsinstanz zu konfigurieren und Ihre Anmeldeinformationen zu testen.

5. Richten Sie Genehmigungen für Patch-Anforderungen ein.
   Standardmäßig ist eine Systemeigenschaft [**sn_vul_patch_orch.patch_approval_required**] aktiviert, sodass Patch-Bereitstellungen, die geplant werden, zur Überprüfung und Genehmigung an Benutzer übermittelt werden, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind.

   Wenn Sie möchten, dass Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Genehmigung planen, können Sie die Eigenschaft [**sn_vul_patch_orch.patch_approval_required**] deaktivieren. Möglicherweise möchten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie Genehmigungen aktiviert lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen.

Hinweis:
Wenn Sie die Systemeigenschaft „Genehmigung“ deaktivieren, kann jeder Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

So deaktivieren Sie als Benutzer mit der Rolle sn_vul.vulnerability_admin die Systemeigenschaft:

a. Navigieren zu **Alle** > **sys.properties.list**.
b. Suchen Sie nach **sn_vul_patch_orch.patch_approval_required,** und klicken Sie darauf, um den Datensatz zu öffnen.
c. Im Feld Wert geben Sie `false`ein.
d. Klicken Sie auf **Aktualisieren**.

6. Wenn Sie diese Eigenschaft nicht deaktivieren, müssen Sie Genehmiger für Patch-Anforderungen zuweisen. Führen Sie als Benutzer mit der Rolle sn_vul.vulnerability_admin die folgenden Schritte aus.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
   b. Wenn die Genehmigungsregel **für Patch-Update-Genehmigung bereitstellen** nicht in der Liste angezeigt wird, klicken Sie oben links im Bildschirm rechts neben dem grünen Filtersymbol auf **Alle**, um die gesamte Liste anzuzeigen.
   c. Klicken Sie in der Liste auf **Deploy Patch Update Approval (Patch-Update-Genehmigung bereitstellen**) .
   d. Klicken Sie im Datensatz bei ausgewählter Registerkarte Genehmigungskonfiguration **auf Standardkonfiguration Patch-Update approval**.
   e. Klicken Sie im -Datensatz auf **Level 1 - Patch update approval (Ebene 1 - Patch-Update-Genehmigung)**.
   f. Fügen Sie Anwender in dieser Gruppe hinzu.

      Die dieser Gruppe zugewiesenen Benutzer genehmigen Patch-Anforderungen, die von Benutzern mit der Rolle „sn_vul_patch_orch.configure_patch“ übermittelt wurden. Navigieren Sie zu **Meine Genehmigungen**, um die Anforderungen anzuzeigen und zu verarbeiten.

7. Klicken Sie auf**Aktualisieren**, um Ihre Änderungen zu speichern.
8. **Wahlweise:** Sie können Genehmigungen auf mehreren Ebenen einrichten, sodass vor der Bereitstellung geplanter Patch-Anforderungen mehr als eine Genehmigung erforderlich ist.

   a. Klicken Sie bei angezeigtem Genehmigungsdatensatz für Patch-Updates für Standardkonfiguration auf **Neu**.
   b. Füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name der Genehmigungsebene, z. **B. Ebene 2 - Patch-Update-Genehmigung**.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ▪ Ein Genehmiger erforderlich ▪ Alle Anwender müssen genehmigen
Bestellung	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt.
Rolle	Wählen Sie in der Liste eine Rolle für die Gruppe aus.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen.
Zuweisen mit	Wählen Sie eine Option aus: ▪ Anwender und Anwendergruppe ▪ Genehmigungstabellenfeld ▪ Skript
Gruppen	Gruppe auf Genehmigerebene, die aus mehreren Anwendern besteht. Der Benutzer muss eine der folgenden von Ihnen angegebenen Rollen aufweisen.
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

c. Klicken Sie auf **Absenden**, um Ihre Änderungen zu speichern.

Patch-Daten und Patch-Daten-Rollup für die Integration Vulnerability Response von Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM anzeigen

Patch-Daten und Patch-Rollup-Daten sowie Schwachstelleninformationen und der Korrekturstatus Ihrer Schwachstellen werden in den Datensätzen in Ihrer Instanz angezeigt.

Patch-Daten werden in den Vulnerability Response -Arbeitsbereichen angezeigt

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch zum Anzeigen (schreibgeschützt) von Patch-Informationen zu Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

Im Arbeitsbereich für IT-Korrekturen können Sie die Patches anzeigen:

- In der Ansicht „Homepage“, in der Sie auf Bewertungslisten klicken können, um Datensätze für Bevorzugte Lösungen für VIs, angreifbare CIs und Bevorzugte Patches für VIs anzuzeigen.
- In der Listenansicht können Sie alle Patch-Update-Datensätze (VPUs) aus den Patches-Links und die Ihnen zugewiesenen angreifbaren Elemente (VITs) mit Patches anzeigen.

Sie können Patches von den folgenden Datensätzen aus planen:

- Von Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Discovered Item (SDI)-Datensätze

Im Arbeitsbereich des Schwachstellenmanagers können Sie Patches anzeigen:

- Über die Ansicht Startseite zu Überwachungsthemen, in der Sie bevorzugte und potenzielle Patches, geplante Patch-Daten und, falls der Patch heruntergeladen wurde, alle auf der Registerkarte **Angreifbare Elemente** anzeigen können.
- Listenansicht zu Korrekturmaßnahmen, in der Sie Patchdaten für VI-Datensätze auf der Registerkarte**Angreifbare Elemente** anzeigen können.

Navigieren Sie in der klassischen Umgebungsansicht zu **Alle** > **Vulnerability Response** > **Patches**.

Patch-Update-Datensätze in den VR-Arbeitsbereichen und in der klassischen Umgebungsansicht

Patch-Daten und Patch-Rollup-Daten sowie deren Status werden für die Datensätze in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit Vulnerability Responseenthalten. Zeigen Sie VPU-Datensätze (Patch) in Arbeitsbereichen Vulnerability Response aus der Listenansicht im Arbeitsbereich für IT-Fehlerkorrekturen an. Patch-Update-Datensätze in der klassischen Umgebung und in Vulnerability Response Arbeitsbereichen enthalten die folgenden Daten:

- Daten und Informationen zur Schwachstellenlösung von Patch-Lieferanten, die von der Anwendung Vulnerability Solution Management importiert werden.
- Korrekturstatus der Quelle, der die Gesamtzahl der Geräte enthält, die eine bestimmte Schwachstelle aufweisen, die durch einen Patch behoben werden kann. Darüber hinaus enthält sie auch und alle Geräte, für die Updates fehlen.
- Korrekturstatus, der den Prozentsatz der korrigierten VIs und die Gesamtzahl der VIs enthält, die einen Patch als bevorzugten Patch haben.
- Zugehörige Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen für zugehörige Links zu Datensätzen in der Klassenansicht. Diese Daten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden auf Registerkarten in Datensätzen in den Vulnerability Response -Arbeitsbereichen angezeigt.

- Patch-Anforderungen, die von Korrekturbesitzern zur Genehmigung übermittelt wurden.

Status-Rollup für Datensätze von angreifbaren Elementen

Weitere Informationen zum Status-Rollup zu Datensätzen finden Sie unter Patchen Sie Daten und Status-Rollup für die Patch-Orchestrierung in Vulnerability Response.

Datensätze, die aktive AEs-Anzahlen zusammenfassen

Um zu vermeiden, dass für alle Patches für alle Schwachstellen ein Rollup durchgeführt wird, werden für die geplante Aufgabe nur Änderungen an der Anzahl aktiver AEs berücksichtigt. Für diese Anzahländerungen und zugehörigen Daten wird ein Rollup für die folgenden Datensätze in Vulnerability Responsedurchgeführt:

- VIT
- RT
- Schwachstellenlösung
- Patch-Update

Daten für Patches ohne Lösungen anzeigen

Weitere Informationen zum Anzeigen von Patches ohne Lösungen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Patchen Sie Daten auf Vulnerability Response

Die Dashboards „Schwachstellenmanagement“ (PA) und „CISO“ sind in einem Abonnement mit Performance Analytics für die Anwendung Vulnerability Response enthalten. Wenn Sie ein -Abonnement für Performance Analyticshaben, aber keine Patch-Orchestration-Integration installieren, wird die Registerkarte „Nachbesserung“ im CISO-Dashboard angezeigt, ist jedoch nicht mit Daten gefüllt.

Navigieren Sie für das Dashboard für Schwachstellenmanagement (PA) zu **Alle** > **Vulnerability Response** > **Übersicht**. Klicken Sie auf die Registerkarte **Nachbesserung**, und scrollen Sie zum Ende der Seite, um die Daten der Patch-Updates anzuzeigen: geplante und nicht geplante Patches, Patches mit fehlendem Zieldatum und wöchentliche Anzahl.

Navigieren Sie für das CISO-Dashboard zu **Alle** > **Vulnerability Response** > **CISO-Dashboard**. Wählen Sie die Registerkarte Übersicht aus, scrollen Sie zum Ende der Seite, um Daten zur Patch-Abdeckung anzuzeigen: Relevanz, geplante und nicht geplante Patches und Patches mit fehlendem Zieldatum.

Weitere Informationen zu den Vulnerability Response -Dashboards finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ., Patchen Sie die Orchestrierung mit den -Arbeitsbereichen Vulnerability Response .und Patch-Orchestrationsdaten werden in den Dashboards Vulnerability Response angezeigt.

Planen Sie Patches mit der MicrosoftMicrosoft Azure Event Hubs SCCM-Integration mit Vulnerability Response

Planen Sie Patches aus den Datensätzen für Patch-Updates und Korrekturaufgaben in der Anwendung Vulnerability Response in Ihrer Instanz Now Platform von .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Ab Version 16.1 können Sie Patches aus den -Arbeitsbereichen Vulnerability Response oder der klassischen Umgebung planen.

Erforderliche Rollen:

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch zum Anzeigen (schreibgeschützt) von Patch-Informationen zu Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

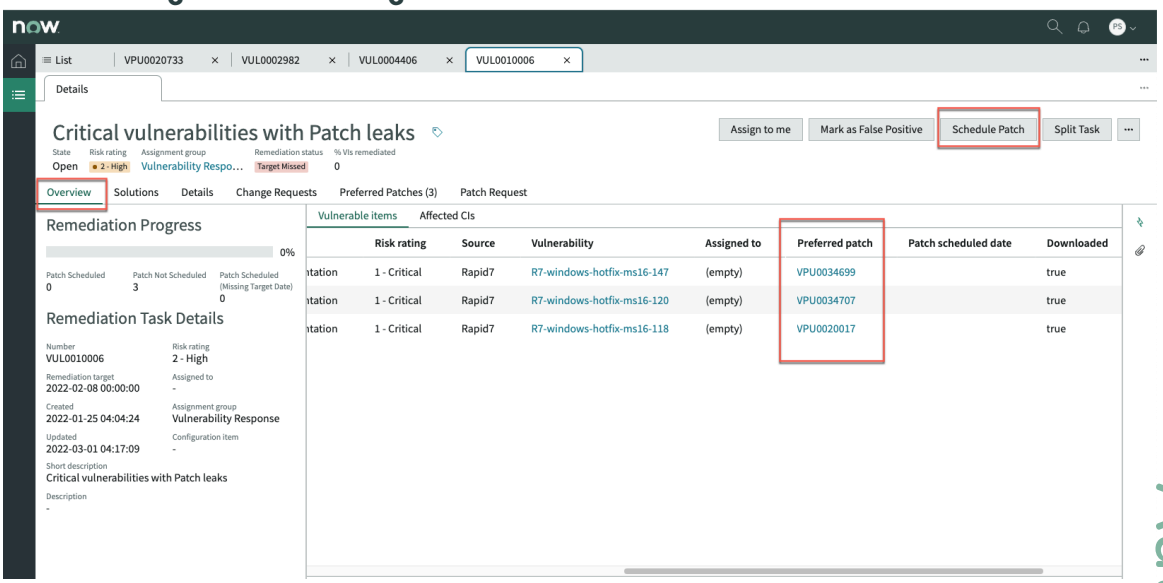
Prozedur

1. Navigieren Sie in den Schwachstellen-Arbeitsbereichen Vulnerability Response als Benutzer mit der Rolle sn_vul.remediation_owner zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Klicken Sie auf der Homepage auf **Preferred patch on VIs (Bevorzugter Patch) zu VIs**.
   Die Liste der Patch-Update-Datensätze für die VIs mit bevorzugten Patches, die Ihnen zugewiesen sind, wird angezeigt.
3. Suchen Sie einen Datensatz, den Sie öffnen möchten, und klicken Sie darauf, um ihn zu öffnen.
4. Alternativ können Sie in der Listenansicht im Arbeitsbereich auf klicken **Patches** > **Alle** und suchen Sie einen Patch-Update-Datensatz.
   Der Patch-Update-Datensatz wird angezeigt. Möglicherweise möchten Sie die Daten überprüfen, bevor Sie einen Patch planen, da möglicherweise bereits andere Patches geplant sind.
5. In der folgenden Tabelle erfahren Sie, welche Daten im Arbeitsbereich für IT-Fehlerkorrekturen angezeigt werden und was Sie tun können.
6. Klicken Sie auf **Patch planen**.
7. Füllen Sie die Felder im Dialogfeld aus.
8. Klicken Sie auf **Bereitstellen**.
   Die Patch-Anforderung wird zur Überprüfung an gesendet. Sie können den Status aller Ihrer übermittelten Anforderungen im anzeigen **Ausnahmeanforderungen** > **Meine Anforderungen** in der Listenansicht.
9. Alternativ können Sie Patches von Korrekturaufgaben aus planen, die Ihnen oder Ihrer Gruppe zugewiesen sind.

Hinweis:
Die Option zum Planen eines Patches aus einem Korrekturaufgabendatensatz ist nur verfügbar, wenn den AEs in der Aufgabe Patches zugeordnet (mit ihnen) vorhanden sind. Diese Patches werden in der Spalte „Bevorzugter Patch“ angezeigt, wenn Sie bei ausgewählter Registerkarte Übersicht rechts neben dem Datensatz einer Korrekturaufgabe einen Bildlauf durchführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgabe mit bevorzugten Patches



10. Klicken Sie im RT-Datensatz **auf Patch planen** und befolgen Sie die oben aufgeführten Schritte, um die Anwendung im Dialogfeld zu planen.

11. **Wahlweise:** Sie können Patches für die Schritte zuvor in der klassischen Umgebung planen. Um diese Datensätze zu finden, führen Sie die folgenden Schritte aus.

    a. Navigieren Sie in der klassischen Umgebung zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**.

    b. Suchen Sie in der angezeigten Liste nach einem Patch-Update-Datensatz.

    c. Navigieren Sie für Korrekturaufgaben zu **Vulnerability Response** > **Korrekturaufgaben** und suchen Sie einen Datensatz.
    Sie können den Korrekturstatus auf der Registerkarte Korrekturstatus nachverfolgen. Am unteren Rand des Datensatzes werden Patch-Daten unter Zugehörige Links angezeigt.

    d. Klicken Sie auf **Patch planen**, und füllen Sie die Felder aus.

Feld	Beschreibung
Bereitstellungsname	Geben Sie einen Namen für diese Patch-Bereitstellung ein. Dieser Name hilft Ihnen, Ihre Updates nachzuverfolgen.
Beschreibung	Fügen Sie mehr Text für über den Patch hinzu. Diese Informationen werden im Beschreibungsfeld des Patch-Update-Datensatzes angezeigt.
Bereitstellungstyp	Wählen Sie eine Option aus der Liste aus. ▪ Erforderlich: Dieser Patch ist ein erforderliches Update. ▪ Verfügbar: Dieser Patch ist nicht erforderlich, aber für die Bereitstellung verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sammlung	Wählen Sie eine Sammlung (Gruppe von Assets) aus der Liste aus, um fortzufahren. Diese Gruppen sind die aus SCCM importierten Asset-Sammlungen.
Bereitstellungszeit basierend auf	Wählen Sie eine Zeitzone aus der Liste aus, auf der Ihr Bereitstellungszeitfenster basiert.
Verfügbare Zeit	Legen Sie den Wert für den Zeitpunkt fest, zu dem der Patch zuerst für die Bereitstellung verfügbar wird.
Frist	Legen Sie die Frist fest. Dieser Wert gibt den letzten Tag an, an dem der Patch installiert werden kann.

e. Klicken Sie auf **Bereitstellen**.

REST-Nachrichten für die Vulnerability Response Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM

Die Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM verwendet die Klassen von SCCM Windows Management Instrumentation (WMI), um Aufrufe an die SCCM-Server-API zu erstellen.

Übersicht

Der SMS-Anbieter stellt der API einen Interoperabilitätszugriff über HTTPS bereit, den so genannten Verwaltungsservice. Der Verwaltungsservice ist eine REST-API (Representational State Transfer), die auf dem Protokoll Open Data (OData) v4 basiert.

Weitere Informationen zur Verwendung des Verwaltungsservice mit dieser Integration finden Sie unter Was ist der Verwaltungsservice in Configuration Manager ?

Da für die erforderliche Authentifizierung das NTLM-Protokoll von Windows New Technology LAN Manager verwendet wird, werden die APIs über den MID-Server mithilfe von PowerShell-Skripts aufgerufen.

MicrosoftMicrosoft Azure Event Hubs SCCM-Integration

Sie können die REST-Nachricht für die MicrosoftMicrosoft Azure Event Hubs SCCM-Integration verwenden, um Informationen von MicrosoftMicrosoft Azure Event Hubs SCCM abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an MicrosoftMicrosoft Azure Event Hubs SCCM zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

WMI-Klassennamen:

- SMS_Sammlung
- SMS_DeploymentSummary

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der SCCM-Konsole an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs SCCM-Bereitstellungs-Patch

Sie können die REST-Nachricht für die Microsoft SCCM-Integration verwenden, um Patches von Ihrem Now Platform® zum MicrosoftMicrosoft Azure Event Hubs SCCM zu planen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an SCCM zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methode	Beschreibung
POST-Bereitstellungs-Patch	Plant den Patch für die SCCM-Konsole auf einem einzelnen/mehreren Computer.

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der SCCM-Konsole an.
Titel	Dynamische Werte basierend auf Anwender	Titel der Bereitstellung.
„settings_tag“	XML-Tag-basierte Einstellungen mit Werten	Gibt Einstellungen an, die andere Parameter haben und während der Planung des Patches an SCCM gesendet werden.
computer_tag	Computer mit XML-Tag und Werten	Gibt die Liste der Computer an, auf denen der Patch geplant wird.
site_name	Wert aus Patch-Update	Name des Standorts, an dem der Patch vorhanden ist
patch_id	Wert aus Patch-Update	ID des Patches.

Datentransformation für die Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM-Integration

Daten werden aus der Patch Orchestration with MicrosoftMicrosoft Azure Event Hubs SCCM Integration abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz von Now Platform® transformiert.

Import der SCCM-Sammlung

Die Daten aus den importierten Sammlungen werden in die Tabelle „SCCM-Sammlungsimport“ [sn_vul_sccm_collection_import] geladen. Die SCCM-Sammlungen (Transformationszuordnung) werden verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import der SCCM-Sammlung verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach SCCM-Sammlungstransformation. In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_collectionid	source_id	Eindeutige ID der Sammlung.
u_name	name	Name der Sammlung
u_membercount	device_count	Anzahl der Geräte in dieser Sammlung.
[Skript]	integration_instance	Name der Instanz, aus der der Patch importiert wird.

Skript-Timing für Transformationszuordnung für SCCM-Sammlungsimport

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Das Skript, das zum Aktualisieren der Werte in der Umfangsvariablen [sn_vul_sccm] verwendet wird Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von SCCM-Patch-Updates

Die Daten aus den importierten Patches werden in die Tabelle „SCCM-Patch-Update-Import“ [sn_vul_sccm_patch_update_import] geladen.

Die SCCM-Patch-Update-Transformation wird verwendet, um die importierten Informationen umzuwandeln.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import des SCCM-Patch-Updates verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie die SCCM-Patch-Update-Transformation.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für Import von SCCM-Patch-Updates

Quellenfeld	Zielfeld	Beschreibung
[Skript]	URLs	URLs für den Patch.
u_nummissing	num_missing	Anzahl der Geräte, für die dieser Patch fehlt.
[Skript]	date_release	Patch-Veröffentlichungsdatum.
u_bulletinid	message_id	Bulletin-ID für den Patch.
u_numtotal	num_total	Gesamtanzahl der Geräte.
u_localizeddescription	description	Beschreibung für den Patch.
[Skript]	is_highest_supersedence	Ist der Patch mit der höchsten Ersatzlösung.
u_numnotapplicable	num_not_applicable	Anzahl der Geräte, die für diesen Patch nicht geeignet sind.
u_iscontentprovisioned	is_downloaded	Wenn Patch auf den SCCM-Server heruntergeladen wird.
u_numunknown	num_unknown	Gesamtzahl der unbekannten Geräte.
u_articleid	Artikel-ID	Artikel-ID des Patch.
u_localizeddisplayname	Titel	Titel des Patches.
u_ci_id	source_id	Eindeutige ID für den Patch in SCCM.
u_numpresent	num_present	Anzahl der Geräte, auf denen der Patch installiert ist.
[Skript]	integration_instance	Name der Instanz, aus der der Patch importiert wird.
[Skript]	sn_vul_solution	Lösung basierend auf der Quell-ID.
[Skript]	last_modified	Datum der letzten Patch-Änderung.
u_severity	source_severity	Schweregrad des Patches.

Skript-Timing für SCCM-Patch-Update-Import-Transformationszuordnung

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Das Skript, das zum Aktualisieren der Werte in der Umfangsvariablen [sn_vul_sccm] verwendet wird Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skript-Timing für SCCM-Patch-Update-Import-Transformationszuordnung (Fortsetzung)

Skript	Beschreibung
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von SCCM-Geräte-Patch-Updates

Die Daten aus den importierten relevanten Patches auf Geräten werden in die Tabelle „SCCM Device Patch Update Import“ [sn_vul_sccm_device_patch_import] geladen.

„SCCM Device Patch Update Transformieren“ wird verwendet, um die importierten Informationen umzuwandeln.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import von SCCM-Geräte-Patch-Updates verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie die SCCM-Geräte-Patch-Update-Transformation.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Skript-Timing für SCCM-Geräte-Patch-Update-Transformationszuordnung

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und Patches sowie der Beziehung zwischen ihnen. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Umfangsvariablen [sn_vul_sccm]. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Import der SCCM-Gerätesammlung

Die Daten aus den importierten Gerätesammlungen werden in die Tabelle „Import der SCCM-Gerätesammlung“ [sn_vul_sccm_device_collection_import] geladen.

Die Importtransformation der SCCM-Gerätesammlung wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem SCCM-Gerätesammlungsimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie die SCCM-Gerätesammlungstransformation.

In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Timing für Transformationszuordnungsskript für Gerätesammlungsimport

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Das Skript, das zum Erstellen und Aktualisieren von CIs basierend auf den CI-Suchregeln und -sammlungen sowie auf der Beziehung zwischen ihnen verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript Werte in der Umfangsvariablen [sn_vul_sccm]. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Transformationszuordnungsfelder für SCCM-Gerätesammlungsimport

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID einer Aktion.
U_name	name	Name der Aktion
[Skript]	sn_vul_sccm_discovered_item	Referenz des erkannten Elements, für das der Patch bereitgestellt wird
U_status	status	Status der Aktion

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für SCCM-Gerätesammlungsimport (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
[Skript]	sn_vul_patch_orch_update	Referenz des Patches
U_apply_count	Anzahl_Erfolg	Erfolgsanzahl der Aktion.
U_retry_count	Erneut versuchen	Wiederholungsanzahl der Aktion.
[Skript]	Bereitstellungszeit	Startzeit der Aktion.
[Skript]	Frist	Endzeit der Aktion.
[Skript]	Quelle_erstellt	Erstellungszeit der Aktion.
[Skript]	Integrationsinstanz	Name der Instanz, aus der die Aktion importiert wird.

SCCM-Bereitstellungsimport

Die Daten aus importierten Bereitstellungen werden in die Tabelle „SCCM-Bereitstellungsimport“ [sn_vul_sccm_deployment_import] geladen.

Die Importtransformation für die SCCM-Bereitstellung wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Verarbeitung von Daten aus dem SCCM-Bereitstellungsimport.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie den SCCM-Bereitstellungstransformation.

SCCM-Bereitstellung Transformieren – Felder zuordnen

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID einer Bereitstellung.
u_name	name	Name der Bereitstellung.
[Skript]	Frist	Frist für die Bereitstellung.
u_numberinprogress	count_progress	Anzahl der Geräte, die für die Bereitstellung ausgeführt werden.
[Skript]	deployment_time	Startzeit der Bereitstellung.
[Skript]	integration_instance	Name der Instanz, aus der die Bereitstellung importiert wird.
[Skript]	source_created	Erstellungszeit der Bereitstellung.
[Skript]	sn_vul_patch_orch_update	Referenz des Patches
[Skript]	sn_vul_patch_orch_collection	Referenz des erkannten Elements, für das der Patch bereitgestellt wird.
u_softwarename	name	Name der Bereitstellung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCCM-Bereitstellung Transformieren – Felder zuordnen (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_numberother	count_other	Andere Anzahl von Geräten für die Bereitstellung.
u_numberunknown	count_unknown	Unbekannte Statusanzahl von Geräten für die Bereitstellung.
u_deploymentid	source_id	Eindeutiger Bezeichner der Bereitstellung.
u_numbersuccess	count_success	Anzahl erfolgreicher Geräte für die Bereitstellung.
u_numbererrors	count_error	Fehleranzahl von Geräten für die Bereitstellung.
u_numbertargeted	count_total	Gesamtanzahl der Geräte für die Bereitstellung.

Skript-Timing für SCCM-Bereitstellungsimport-Transformationszuordnung

Skript	Beschreibung
Beim Start (wenn ein Importsatz eine Transformation erstellt hat)	Skript, das zum Initialisieren der Werte in der Umfangsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Das Skript, das zum Aktualisieren der Werte in der Umfangsvariablen [sn_vul_sccm] verwendet wird Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Beispiel-Workflow für die Integration von Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM

Ein Beispiel für die Funktionsweise der Patch-Orchestrierung mit MicrosoftMicrosoft Azure Event Hubs SCCM.

Vorbereitungen

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gepatcht. Das letzte Patchfenster wurde vor einer Woche abgeschlossen, Sie möchten jedoch einen Patch anwenden, um eine kritische Schwachstelle zu beheben, die kürzlich bekannt wurde. Aufgrund der Relevanz dieser Schwachstelle können Sie nicht zwei weitere Wochen auf den nächsten geplanten Patch warten.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für den Arbeitsbereich des Schwachstellenmanagers.
- sn_vul.remediation_owner, um den Arbeitsbereich des IT-Korrekturbesitzers anzuzeigen.
- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches.
- sn_vul_patch_orch.read_patch zum Anzeigen (schreibgeschützt) von Patch-Informationen zu Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.remediation_owner“ und „sn_vuln.vulnerability_analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind.

Warum und wann dieser Vorgang ausgeführt wird
Als Schwachstellenmanager oder Analyst, der im Arbeitsbereich des Schwachstellenmanagers arbeitet, können Sie Überwachungsthemen erstellen oder vorhandene Überwachungsthemen bearbeiten, um importierte VIs mit kritischen Schwachstellen zu erfassen. Mit der Patch-Orchestration-Integration können Sie auch die Patches anzeigen, die Sie zum Beheben und Nachverfolgen dieser Schwachstellen verwenden möchten. In der folgenden Tabelle sind einige Beispiele mit den Bedingungen aufgeführt, die Sie für Überwachungsthemen für die Patch-Orchestrierung festlegen können. Verwenden Sie diese Beispiele, um die Einstellungen zu bestimmen, die für Ihre Umgebung am besten geeignet sind. Weitere Informationen zum Einrichten des Überwachungsthemas finden Sie unter Erstellen Sie ein Überwachungsthema in Vulnerability Manager Workspace.

Beispiel-Überwachungsthemen für Patch-Orchestrierung im Arbeitsbereich des Schwachstellen-Managers

Name des Überwachungsthemas	Beschreibung
Kritische Schwachstellen mit Patchverlusten	Risikobewertung ist 1 – kritisch UND Grund: Patch nicht geplant
Kritische Schwachstellen mit geplanten Patches (fehlendes SLA)	Grund: Patch geplant (fehlendes Zieldatum)
Kritische Schwachstellen mit geplanten Patches	Risikobewertung ist 1 – kritisch UND Geplantes Patch-Datum ist nicht leer UND Grund: Patch geplant

- Als Schwachstellenmanager oder Analyst generieren Sie nach dem Erstellen der Überwachungsthemen und Korrekturmaßnahmen Korrekturaufgaben. Von VI-Datensätzen und Korrekturaufgaben aus können Sie einen Drilldown zur Registerkarte Erkennungen durchführen und die Datensätze erkannter Elemente finden, die die von Ihnen verfolgte Schwachstelle aufweisen, zusammen mit den vom SCCM-Produkt importierten Assets.
- Als Schwachstellenanalyst oder Administrator können Sie die mit der Schwachstelle verknüpften Patchdaten überwachen. Sie können auch einen oder mehrere Patches für ein bestimmtes Asset (Konfigurationselement) aus einem Datensatz für ein erkanntes Element bereitstellen.

Als IT-Nachbesserungsspezialist haben Sie verschiedene Möglichkeiten, um die Schwachstelle mit einer Patch-Bereitstellung zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können den Patch von einem Patch Update-Datensatz (VPU#) aus planen.
- Wenn angreifbaren Elementen (VI) bevorzugte Lösungen zugeordnet sind und Sie oder Ihre Gruppen zugewiesen sind, können Sie die Patches über eine Korrekturaufgabe mit diesen angreifbaren Elementen planen.

Prozedur

1. Klicken Sie als IT-Korrekturspezialist im IT-Korrektur-Arbeitsbereich auf die Ansicht Startseite.
2. Klicken Sie in der Ansicht „Start“ auf die Bewertungsliste **Zugewiesene Korrekturaufgaben,** um die Datensätze anzuzeigen.

   Für dieses Beispiel können Sie das Feld Kurzbeschreibung der Korrekturaufgabe (VUL#) auf beliebigen Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht. Angenommen, Sie wissen vielleicht, dass Ihr Schwachstellenmanager ein Überwachungsthema mit der Bezeichnung Kritische Schwachstellen mit Patch-Lecks zum Erfassen von VIs (VIT#) mit dieser kritischen Schwachstelle erstellt hat.

   Bei geöffnetem Datensatz können Sie auch die VIs und die bevorzugten Patches überprüfen und sehen, ob Sie oder andere Mitglieder Ihrer Gruppe bereits Patch-Anforderungen zur Genehmigung übermittelt haben.

3. Wenn Sie über genügend Informationen verfügen, können Sie jetzt von dieser Korrekturaufgabe aus eine Patch-Anforderung senden.

   Hinweis:
   Wenn den AEs, die dem Datensatz zugeordnet sind, keine Patches zugeordnet sind, ist die Schaltfläche **Patch planen** für den Datensatz nicht verfügbar.

4. Klicken Sie auf **Patch planen** und füllen Sie die Felder im Dialogfeld aus.
   Weitere Informationen zum Planen von Patches finden Sie unter Planen Sie Patches mit der MicrosoftMicrosoft Azure Event Hubs SCCM-Integration mit Vulnerability Response.
5. Alternativ können Sie in der Listenansicht im IT-Korrekturarbeitsbereich auf die Links Korrekturaufgaben, Angreifbare Elemente, Lösungenund Patches klicken, um diese Datensätze anzuzeigen.
   In diesem Beispiel kennen Sie anstelle des Namens eines Überwachungsthemas möglicherweise die Artikel-ID oder die Bulletin-ID und den Titel des Patches. Wenn dies der Fall ist, sollten Sie überprüfen, ob Ihnen oder Ihren Gruppen eines der VIs mit dieser Schwachstelle zugewiesen ist. Von Patch-Update-Datensätzen aus können Sie Patch-Anforderungen übermitteln. In VI-Datensätzen können Sie nach potenziellen Patches suchen und die zugehörige Korrekturaufgabe öffnen, wenn Sie eine Patch-Anforderung senden möchten.
6. Wenn Sie keinen Zugriff auf die Arbeitsbereiche von haben oder Daten anzeigen und Patches in der klassischen Umgebung planen möchten, führen Sie die folgenden Schritte aus.

   a. Navigieren zu **Vulnerability Response** > **Patches** > **Alle**.

   b. Suchen Sie den gewünschten Patch Update-Datensatz.
   Unter Umständen möchten Sie die Datensätze nach kritischen Risikopunktzahlen filtern.

   c. Überprüfen Sie die zugeordneten Felder „VIs“ und „% der korrigierten AEs“ auf der Registerkarte Korrekturstatus.
   Wenn für die VIs Patches verfügbar sind, wird oben rechts im Datensatz die Schaltfläche **Patch planen** angezeigt.

   d. Wenn Sie eine Anforderung senden möchten, klicken Sie auf **Patch planen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Planen von Patches finden Sie unter Planen Sie Patches mit der MicrosoftMicrosoft Azure Event Hubs SCCM-Integration mit Vulnerability Response.

e. Angenommen, Sie haben keine Patch-ID-Informationen, können jedoch im Feld Kurzbeschreibung der Korrekturaufgaben, die Ihrer Gruppe zugewiesen sind, nach Text suchen, der sich auf Ihre kritische Schwachstelle bezieht.

f. Navigieren zu **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.

g. Suchen Sie den gewünschten Datensatz, und klicken Sie darauf, um ihn zu öffnen.
Überprüfen Sie im geöffneten Datensatz die Registerkarte Korrekturstatus auf AEs und Behobene AEs in Prozent. Klicken Sie auf die zugehörigen Links für VI-Datensätze, Bevorzugte Lösungen, Bevorzugte Patchesund Patch-Anforderungen.

Hinweis:
Wenn den AEs, die dem Datensatz zugeordnet sind, keine Patches zugeordnet sind, ist die Schaltfläche **Patch planen** für den Datensatz nicht verfügbar.

h. Klicken Sie im Datensatz **auf Patch planen,** wenn Sie eine Patch-Anforderung senden möchten.

Qualys Vulnerability Integration verstehen

Die Qualys Produktsensoren erfassen die Daten und senden sie automatisch an die Anwendung Qualys, die die Informationen kontinuierlich analysiert und korreliert. Die Integration mit Vulnerability Response als Qualys Vulnerability Integration ermöglicht die einfache Zuordnung von Schwachstellen zu CIs und Business-Services zur Bestimmung der Auswirkung und Priorität potenziell schädlicher Bedrohungen.

Konfigurieren Sie Qualys Vulnerability Integration mit **Schwachstelle** > **Administration** > **Setup-Assistent** um den Datenabruf flexibler und skalierbarer zu gestalten.

Wenn Sie über mehrere Bereitstellungen der Anwendung Qualys Cloud Platform verfügen, können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die von mehreren Drittanbieterbereitstellungen und ihren Schwachstellen identifiziert wurden, werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scan-Prozesse zwischen den mehreren Bereitstellungen überschneiden. Daten, die aus den einzelnen Bereitstellungen stammen, werden identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar. Qualys Vulnerability Integration Knowledge Base-Datensätze werden über alle Bereitstellungen hinweg normalisiert, um sicherzustellen, dass Instanzen derselben Schwachstelle in allen Bereitstellungen als dieselbe Schwachstelle behandelt werden.

Hinweis:
Sie können die ursprüngliche Schwachstellenintegration nicht löschen, aber deaktivieren. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Hinweis:
Qualys Vulnerability Integration erstellt zwar Integrationen für die Appliance-Liste, die Asset-Gruppe, die dynamische Suchliste und die statische Suchliste, sie sind jedoch für den normalen Betrieb nicht erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen

Release-Version für Yokohama	Release-Hinweise
Qualys Vulnerability Integration v12.7, v12.8	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Installierte Komponenten

Eine aktuelle Liste der Rollen, Integrationsaufgaben und Tabellen, die mit der Integration installiert werden, sowie einen Link zu Anweisungen zum Anzeigen der derzeit in Ihrer Instanz installierten Elemente finden Sie unter Mit installierte Komponenten Qualys Vulnerability Integration.

Primäre und unterstützende Integrationen

Qualys Primäre und unterstützende Integrationen ergänzen die Schwachstellendaten in Ihrer Instanz, indem sie Daten aus der Qualys-Schwachstellenintegration abrufen. Die Integrationen werden automatisch durch eine Reihe von geplanten Aufgaben aufgerufen. Sie können sie auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren. Primäre und unterstützende Integrationen können geändert werden.

Die Qualys Integrationen werden als geplante Aufgaben ausgeführt. Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Dieser Wert darf nicht geändert werden.

Hinweis:
Wenn keine gültige Ausführung als Anwender festgelegt werden kann, kommt es bei jeder Ausführung der Integration zu mehreren, häufig doppelten Datenabrufanhängen in den Datenquellen-Datensätzen. Mehrere Anhänge in der Datenquelle erhöhen die Verarbeitungsdauer, was zu inkonsistenten Transformationsergebnissen führt.

Während des Imports werden CVE-Datensätze, die noch nicht vorhanden sind, als NVD-Datensätze erstellt und standardmäßig in Einträgen von Drittparteien für Qualys referenziert.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Primäre Integrationen

Eine primäre Integration ist ein Einstiegspunkt für Qualys Cloud Platform, der mit der Qualys -API interagiert, die gemäß einem Zeitplan aufgerufen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die primären Integrationen an, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.

Unterstützende Integrationen

Eine unterstützende Integration ist ein Prozess, der nicht zur Ausführung nach einem Zeitplan oder ohne Aufruf durch eine primäre Integration vorgesehen ist.

Zeigen Sie die unterstützenden Integrationen an, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Administration** > **Unterstützende Integrationen**.

Service Graph Connector für Qualys

Ab Version 2.2 ist der Service Graph Connector für Qualys im ServiceNow® Storeverfügbar. Weitere Informationen finden Sie unter Service Graph Connector for Qualys .

Daten aus den Feldern der Datenquelle Qualys werden mit der Global Asset API und der Asset Management and Tagging API importiert.

Globale Asset-API:

- Eine CSAM-Lizenz ist erforderlich.
- Asset-Informationen enthalten Details wie Hardwarekategorie und Betriebssystemkategorie.

API für Asset-Verwaltung und Tagging:

- Eine CSAM-Lizenz ist nicht erforderlich
- Asset-Informationen enthalten keine Details zur Hardwarekategorie und zur Betriebssystemkategorie.

Weitere Informationen finden Sie unter Service Graph Connector for Qualys APIs

.

CIs mit der Engine Identification and Reconciliation (IRE) erstellen

Sie können die Engine „Identification and Reconciliation“ (Identifizierung und Abgleich) verwenden, um neue CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der aus einem Drittanbieterscanner importiert wurde. Aktivieren Sie das Plugin „CMDB CI Class Models“ (CMDB-CI-Klassenmodelle), um CIs mit den neuen Klassen zu erstellen. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt. Weitere Informationen zum Konfigurieren der Kategorisierung von nicht abgeglichenen Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets aktualisieren.

Suchlisten

Suchlisten werden in Qualys verwendet, um anwenderdefinierte Gruppen von Schwachstellen zu erstellen. Sie können sie speichern und für die Ticketerstellung verwenden sowie Schwachstellen-Scans und Berichte anpassen. Mit dem Modul „Suchlisten“ können Sie Suchlistendaten von Qualys regelmäßig auf Ihre Instanz herunterladen.

Suchlisten werden mithilfe der Datentransformationszuordnungen „Dynamischer Suchlistenimport“ und/oder „Statischer Suchlistenimport“ aus Qualys abgerufen. In jeder dieser Transformationen können Sie Zeitpläne für den Import definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionsprofile

Optionsprofile sind mit den Scan-Einstellungen Qualys verfügbar. Ein Optionsprofil ist erforderlich, wenn Sie einen Scan von Ihrem Now Platformaus initiieren.

Optionsprofile werden durch die Option Profile List Integration (Optionsprofillistenintegration) aus dem Produkt Qualys importiert. Möglicherweise möchten Sie die Integration der Optionsprofilliste nach einem Import aus den Integrationen der Suchlisten, der Qualys Integrationen der dynamischen Suchliste und der Integrationen Qualys der statischen Suchliste ausführen, damit Sie sehen können, welche Suchlisten mit Optionsprofilen verknüpft sind.

Asset-Gruppen

Asset-Gruppen werden auf der Plattform Qualys eingerichtet. Asset-Gruppen geben an, welche Scanner-Geräte zum Scannen übereinstimmender IP-Adressen verwendet werden, wenn ein Scan von Now Platformaus initiiert wird.

Asset-Gruppen, denen Geräte zugeordnet sind, werden von der Asset-Gruppenlisten-Integration aus Qualys abgerufen.

Initiieren Sie die Integration der Appliance-Listenintegration, nachdem Sie Asset-Gruppen importiert haben, um die Felder Appliance-Name und Appliance-Status in den Datensätzen Qualys Standardanwendungen in Ihrer Now Platform auszufüllen.

Host-Tags

Alle Host-Tags werden als Teil der Qualys -Hostlisten-Integration importiert. Host-Tags werden hauptsächlich zum Filtern in Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben verwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

Hinweis:
Die Integration der Hostliste Qualys muss vor der Erstellung von Regeln für Zuweisungs- oder Korrekturaufgaben in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein **San Diego** -Tag erstellt wird, kann kein **SAN DIEGO** -Tag in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das zuerst importierte Tag gewinnen.
- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft **sn_vul.import_host_tags**gesteuert. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Durch das Deaktivieren von Tags werden sie für alle Instanzen deaktiviert.

Host-Tags (auch als Asset-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Host-Assets Tags zuweisen. Dann können Sie beim Starten von Scans Tags auswählen, die den Hosts zugeordnet sind, die Sie scannen möchten. Mit dem Modul „Host-Tags“ können Sie Host-Tag-Daten von Qualys zeitplanbasiert in Ihre Instanz herunterladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffnen Sie gelöste angreifbare Elemente, die nicht durch Scans geschlossen wurden

Angreifbare Elemente, die in Ihrer Instanz Now Platform auf „Gelöst“ festgelegt, aber von den Integrationsausführungen der Drittpartei nicht in den Status „Geschlossen/Behoben“ versetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Wenn der Scanner für Qualys -Erkennungen weiterhin VIs findet, die auf „Gelöst“ gesetzt wurden, dann aber nicht durch nachfolgende Scans in den Status „Geschlossen/Behoben“ überführt wurden, kehren diese VIs zu „Offen“ zurück, wenn das zuletzt gefundene Datum nach dem liegt Datum der Lösung.

Einschränkungen beim Datenabruf

Standardmäßig gibt es keine Einschränkungen für den Abruf von Daten aus Qualys. Viele Datensätze können sich auf Schwachstellen mit niedrigem Schweregrad beziehen, die ein Kunde nicht bereit ist, mit seinem Vulnerability Response-Prozess zu beheben. Durch Aktualisieren der entsprechenden REST-Nachrichten-/Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/-Methode ist **Qualys Host Detection – Standard/post**. Um die Werte zu aktualisieren, fügen Sie der Post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3–5 (oder die gewünschten Schweregrade)

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Zugehörige Informationen

Qualys-REST-Nachrichten

Vorbereitung auf das Qualys Vulnerability Integration

Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Es ist wichtig, dass Sie sich auf die Integration vorbereiten, indem Sie die folgenden Schritte ausführen. Qualys Vulnerability Integration setzt voraus, dass Sie mit Qualys Cloud Platform-Scans in Ihrer Umgebung vertraut sind und diese ausführen.

Hinweis:
Nehmen Sie alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor, bevor Sie die Integrationen ausführen.

Wichtige Voraussetzungen

Validiert die Größe Ihrer Instanz basierend auf der Anzahl der angreifbaren Elemente, die importiert werden sollen. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Verwenden Sie Filter, um die Anzahl der Elemente für den ersten Import zu begrenzen und Ihre Bereitstellung zu stufen, indem Sie Filter in nachfolgenden Importen anpassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Qualys -Scanner sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die Schaltfläche **Erneut scannen** nicht verfügbar.

Auszuführende Aktionen

- Bestimmen Sie ein anfängliches Startdatum für Integrationen **des Imports von Host-Erkennungslisten**.

  Erwägen Sie, das Feld **Startzeit** auf einige Stunden oder Tage in der Vergangenheit zu setzen. Wählen Sie idealerweise das Datum des letzten Qualys-Scans. Das Startdatum kann Schwachstellen enthalten, die vor der Verwendung der Schwachstellenmanagementlösung erkannt wurden. Legen Sie die früheste Startzeit auf den Beginn Ihres Scan-Zyklus fest. Wenn es also eine Woche dauert, bis alle Hosts gescannt werden, legen Sie diesen Wert auf eine Woche vor diesem Zeitpunkt fest.

- Fügen Sie den Rollen „admin“, „sn_vuln.admin“ und „sn_vul_qualys.admin“ Benutzer hinzu. Weitere Informationen finden Sie unter Einem Benutzer eine Rolle zuweisen .

- Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

- Wenn Sie keine Schwachstellen-Rechner verwenden, Deaktivieren Sie den standardmäßigen Schwachstellen-Rechner, wenn er nicht verwendet wird, zusätzlich zu anderen, die Sie definiert haben. Sicherheitsrisiko-Rechner werden jedes Mal ausgeführt, wenn der Datensatz eines angreifbaren Elements erstellt oder aktualisiert wird, und können sich auf die Leistung des anfänglichen Imports auswirken.
- Während des ersten Imports von Datensätzen können bestimmte Benachrichtigungs-Business-Regeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Deaktivieren Sie vor dem ersten Import die Business-Regeln.
- Wenn Sie einen anderen als den Qualys-Standardscanner verwenden möchten, finden Sie weitere Informationen unter Scanner-Appliances einrichten.
- Halten Sie die Qualys-Server-URL und die Anmeldeinformationen für die Authentifizierung bereit. Die Anmeldeinformationen müssen ausreichende Berechtigungen zum Abrufen von Wissens-, Scan- und Erkennungsinformationen für ein Qualys-Abonnement bieten.
- Wenn Sie Host-Tags in den Zuweisungsregeln für Vulnerability Response oder in den Regeln für Korrekturaufgaben verwenden möchten, stellen Sie sicher, dass die Integration mit der Qualys -Hostliste vor dem Erstellen von Regeln ausgeführt wurde.

Qualys Vulnerability Integration installieren

Bevor Sie Qualys Vulnerability Integration in Ihrer Instanz von ausführen, müssen Sie die Anwendung Qualys Vulnerability Integration installieren und konfigurieren. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:

Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Herunterladen und Installieren der Anwendung erforderliche Rolle: admin

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Rufen Sie Berechtigungen für die Anwendung Qualys Vulnerability Integration ab, und laden Sie sie in Ihre Instanz Now Platform® herunter.	Wenn die Anwendung noch nicht auf Ihre Instanz heruntergeladen wurde, finden Sie weitere Informationen unter .
Bereiten Sie die Integration vor.	Weitere Informationen finden Sie unter Vorbereitung auf das Qualys Vulnerability Integration.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz von verfügbar sind.

2. Suchen Sie die Kachel Qualys Vulnerability Integration, und klicken Sie auf **Installieren**.
3. Folgen Sie den Eingabeaufforderungen im Setup-Assistenten.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.
4. Navigieren Sie im Setup-Assistenten zu **Integrationskonfiguration > Scanner-Integrationen,** um mit der Konfiguration fortzufahren.
   Weitere Informationen zur Ergänzung der Eingabeaufforderungen im Setup-Assistenten finden Sie unter Qualys Vulnerability Integration mit dem Setup-Assistenten konfigurieren.

Nächste Maßnahme

Aktivieren Sie die Scanner, da die Scanner in der Anwendung Vulnerability Response standardmäßig inaktiv sind. Weitere Informationen zum Aktivieren der Qualys -Scanner finden Sie unter Aktivieren Sie die Qualys -Scanner.

Aktivieren Sie die Qualys -Scanner

Sie müssen die Scanner nach der Installation von Qualys Vulnerability Integration aktivieren, da die Scanner in der Anwendung Vulnerability Response standardmäßig deaktiviert sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die Schaltfläche **Erneut scannen** nicht verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und wählen Sie den Datensatz aus, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox **Aktiv**.
4. Wählen Sie **Aktualisieren**.
5. Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld **Quelle** für Datensätze für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

Mit installierte Komponenten Qualys Vulnerability Integration

Die folgenden Rollen, Integrationsaufgaben und Tabellen werden mit Qualys Vulnerability Integrationinstalliert.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Zeigen Sie gefilterte Listen für mit einer Anwendung installierte Komponenten an

Filtern Sie die Tabelle „Anwendungsdateien“, damit nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert wurden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert werden, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie diese Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator **sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **AND**und dann aus. **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_qualys.read	Hat Lesezugriff auf die Datensätze Qualys Vulnerability Integration.	
sn_vul_qualys.user	Anwender für Qualys Vulnerability Integration. Kann Datensätze lesen und schreiben	sn_vul_qualys.read

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_qualys.admin	Administrator fürQualys Vulnerability Integration. Sie können beispielsweise Startdaten der Integration ändern und einige erweiterte Konfigurationseinstellungen vornehmen.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Kann konfigurieren Qualys Vulnerability Integration	sn_vul_qualys.admin

Integrationsaufträge installiert

Integrationsauftrag	Beschreibung
Qualys Integration statischer Suchlisten	Synchronisiert Qualys Suchlisten für die Suche nach angreifbaren Einträgen. Ruft nur Datensätze vom Typ „Statische Liste“ ab.
Qualys Comprehensive Host Detection Integration	Ruft Host- und Schwachstellendaten von Qualys ab und verarbeitet sie in Ihrer -Instanz. Sie koordiniert die REST-Nachrichtenaufrufe an die Host-Erkennungs-API. Die Ausgabe dieser Integration sind angreifbare Elemente. Diese Integration importiert alle Status der Schwachstelle: Neu, Behoben, Aktiv und Erneut geöffnet. Standardmäßig ist diese Integration inaktiv und wird wöchentlich ausgeführt. **Hinweis:** Nachdem diese Integration aktiviert wurde, importiert die tägliche umfassende Aufgabe nur die Status „Neu“, „Repariert“ und „Erneut geöffnet“.
Qualys Hostlistenintegration	Ruft einmal pro Woche authentifizierte und nicht authentifizierte Host-Scandaten und Host-Tags von Qualys ab und speichert sie im Modul „Erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden.
Qualys Integration der Host-Erkennung	Ruft Host- und Schwachstellendaten von Qualys ab und verarbeitet sie in Ihrer -Instanz. Sie koordiniert die REST-Nachrichtenaufrufe an die Hostlisten-Erkennungs-API. Die Ausgaben dieser Integration sind angreifbare Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsauftrag	Beschreibung
	Qualys Host-Tags werden in dieser Integration importiert.
Qualys Ticketintegration	Ruft Tickets vom Qualys Typ ab und fügt sie Ihrer Instanz hinzu. Sie koordiniert die REST-Nachrichtenaufrufe an die Ticketlisten-API. Häufig sind weniger Tickets als Hosterkennungen vorhanden, da die Einstellungen für Qualys die Erkennungen einschränken können, die zu einem Ticket führen.
Qualys Integration der Optionsprofilliste	Ruft Optionsprofile vom Produkt Qualys ab. Optionsprofile enthalten Scaneinstellungen, die erforderlich sind, wenn Sie Scans von Ihrer Instanz Now Platform aus initiieren.
Qualys Integration der Appliance-Liste	Ruft Informationen zur Scanner-Anwendung von Qualysab.
Qualys Asset-Gruppenintegration	Ruft Asset-Gruppeninformationen von Qualysab. Asset-Gruppen werden verwendet, um zu identifizieren, welche Scanner-Geräte zum Scannen übereinstimmender Configuration Items verwendet werden sollen.
Qualys Knowledge Base (Auffüllen)	Ruft Qualys Knowledge Base-Einträge ab. Geplant zur Ausführung nach der Qualys Host-Erkennungsintegration. Aktualisiert Ihre Instanz mit allen QIDs, auf die in der Integration der Hosterkennung verwiesen wurde, die jedoch nicht im System vorhanden waren.
Qualys Knowledge Base	Ruft Qualys Knowledge Base-Einträge ab. Die abgerufenen Daten basieren auf dem Datum der Aktualisierung der Schwachstellen durch Qualys und seit der letzten Ausführung der Integration. Diese Daten sind nützlich, um Verlaufsdaten in Ihre -Instanz zu füllen und sicherzustellen, dass die Qualys Bezeichner (QIDs) aktuell sind.
Qualys Integration dynamische Suchliste	Synchronisiert Qualys Suchlisten für die Suche nach angreifbaren Einträgen und ruft Datensätze vom Typ „Dynamische Liste“ ab.
Korrektur der Erkennungen für aktualisierten Schlüssel für Qualys	Eine Hash-Kombination von Feldern, die eine Möglichkeit bietet, eine Erkennung zu identifizieren und an ein angreifbares Qualys -Element zu binden.
Qualys Aktualisiert vorhandene erkannte Elemente mit dem Netzwerkpartitionsbezeichner	Aktualisiert Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Qualys Vulnerability Integration-Daten werden erstellt oder aktualisiert, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsauftrag	Beschreibung
	die Granularität des Netzwerkpartitionsbezeichners einzubeziehen.

Installierte Tabellen

Tabelle	Beschreibung
Schwachstelle der Suchliste sn_vul_qualys_m2m_search_list_vul	Speichert die Zuordnung zwischen der Suchliste Qualys und einer Schwachstelle.
Qualys Schwachstellenscanner sn_vul_qualys_scanner	Tabelle, die Schwachstellenscanner um die Speicherung von Scannerinformationen für die Funktion zum erneuten Scannen Qualys von erweitert.
Qualys Suchlisten sn_vul_qualys_search_list	Speichert Suchlisten, die von der Suchlistenintegration Qualys abgerufen wurden.
Qualys Appliance-Import sn_vul_qualys_appliance_imp	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.
Qualys CI sn_vul_qualys_ci	Tabelle wird nicht mehr verwendet.
Host-Erkennungspaginierung sn_vul_qualys_host_detection_pagination	Tabelle wird nicht mehr verwendet.
Qualys Integrationsausführung sn_vul_qualys_integration_run	Tabelle wird nicht mehr verwendet.
Qualys Integration sn_vul_qualys_integration	Tabelle, die die Schwachstellen-Integration erweitert und speichert alle Integrationen, die Qualysentsprechen.
Qualys Import von Listen für statische Suche sn_vul_qualys_static_search_list_imp	Tabelle, die die Importsatzzeile erweitert. Feldzuordnungen werden verwendet, um Daten in die Zieltabelle Qualys Suchlisten zu transformieren.
Qualys Knowledge Base sn_vul_qualys_knowledge_base	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.
Qualys Ticketliste sn_vul_qualys_ticket_list_imp	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.
Qualys Optionsprofil	Tabelle, in der die von Qualysabgerufenen Optionsprofile gespeichert werden. Diese Tabelle wurde mit dem erneuten Scannen verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vul_qualys_option_profile	
Qualys Import dynamische Suchliste sn_vul_qualys_dynamic_search_list_imp	Tabelle, die die Importsatzzeile erweitert. Feldzuordnungen werden verwendet, um Daten in die Zieltabelle Qualys Suchlisten zu transformieren.
Qualys Erneute Ausführung des Importsatzes sn_vul_qualys_import_rerun	Tabelle wird nicht mehr verwendet.
Qualys Import von Optionsprofilen sn_vul_qualys_option_profile_import	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.

Aktualisieren Sie Configuration Items mit dem Netzwerkpartitionsbezeichner für Qualys Vulnerability Integration

Erstellen Sie eindeutige Configuration Items (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um weitere Details zu Ihren Schwachstellen zu erhalten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig können Sie Ihre Assets in der Anwendung Vulnerability Response anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch in Ihrer CMDB als ein CI gespeichert.

Wie in den folgenden Tabellen gezeigt, können beispielsweise mehrere Assets (CI) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, verfügen jedoch über eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche in der Regel als einzelnes CI (CI 1) identifiziert und gespeichert.

Standardmäßige IP-Suche und CI-Erstellung

Quelle	IP-Adresse	NETWORK_ID	Konfigurationselement
Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	REPOSITORY_ID	Konfigurationselement
Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse aufweisen, um sie als unterschiedliche Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die geplante Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integration im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzu. Von der IRE erstellte vorhandene CIs werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Ab v14.0 von Vulnerability Response und v12.1 der Qualys Vulnerability Integration Vulnerability Integration werden die CMDB-CI-Klassenmodelle (1.0.21.) unterstützt. Die -Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

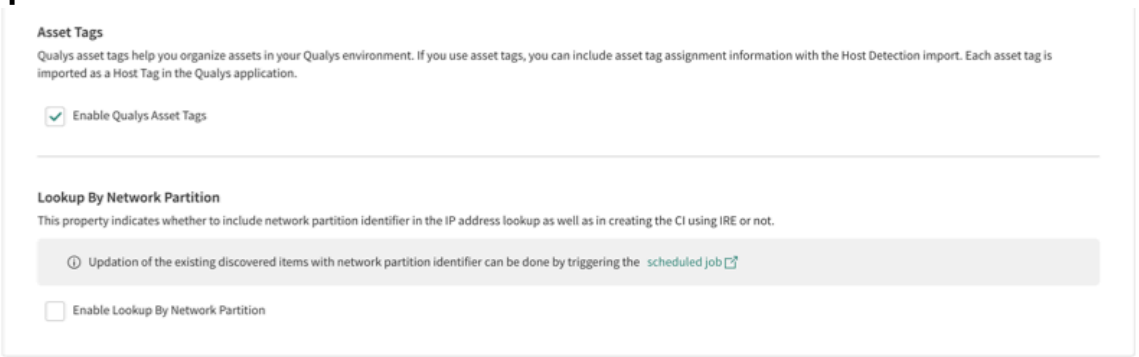
Option	Beschreibung
Geplante Aufgaben bei Bedarf ausführen.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Daten Qualys Vulnerability Integration werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartitionsbezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.
Warten Sie mit den nächsten geplanten Aufgaben auf Importe neuer Daten aus den Integrationen.	Erstellen Sie CIs für jedes neue Asset unter Verwendung des Netzwerkpartitionsbezeichners, beginnend mit der nächsten geplanten Aufgabe. CI, angreifbares Element und Erkennungsdatensätze werden mit der neuen Granularität aktualisiert. Neue CIs werden erstellt, wenn keine exakte Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Qualys Vulnerability Integrationaus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Wählen **Hosterkennungskonfiguration**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen aus **Suche nach Netzwerkpartition**



Abschnitt.

6. Klicken Sie auf **Fertigstellen**.

Die Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY_ID sind in der IP-Suche und der CI-Erstellung enthalten

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI2

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Qualys: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI2

Die Suchregeln für die IP-Adresse und die unvollständige IP-Adressen-CI-Identifizierung enthalten das Attribut des Netzwerkpartitionsbezeichners für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integrationautomatisch.

Nachdem Sie die geplante Aufgabe aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie bei Bedarf geplante Aufgaben starten. Die CIs in vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen werden automatisch aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionale Qualys-Änderungen

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Qualys-Integration.

Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen oder Business-Regeln so ändern, dass sie während eines ersten Imports deaktiviert werden.

Deaktivieren Sie benachrichtigungsbezogene Business-Regeln vor dem ersten Datensatzimport

Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln viele Benachrichtigungen generieren, was sich auf die Leistung auswirkt. Diese Business-Regeln müssen geändert werden, um sie während des Imports zu deaktivieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu**Alle** > **Systemdefinition** > **Business-Regeln**.
2. Suchen Sie nach **Benachrichtigungen von betroffenen CIs**.
3. Öffnen Sie die Geschäftsregel, und fügen Sie diese Bedingung ein: `current.sys_class_name != “sn_vul_vulnerable_item“`.
4. Klicken Sie auf **Aktualisieren**.
5. Wiederholen Sie dieses Verfahren für die folgenden Geschäftsregeln:
   - Benachrichtigungen für betroffene Kostenstellen
   - Betroffene Gruppenbenachrichtigungen
   - Benachrichtigungen zum betroffenen Standort

Hinweis:
Nach Abschluss des ersten Datensatzimports können Sie diese Business-Regeln erneut aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und sich auf die Leistung Ihrer Instanz auswirken.

Ändern Sie ein anfängliches Startdatum

Während der Installation mit dem Setup-Assistenten legen Sie ein anfängliches Startdatum für die Qualys-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen (siehe unten).

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
2. Klicken Sie auf **Qualys Integration für Host-Erkennung**.
3. Klicken Sie auf **Integrationsdetails**.
4. Legen Sie das Feld **Startzeit** auf einen Wert in der Vergangenheit fest, damit alle seit dieser Zeit gescannten und erkannten Schwachstellen erkannt werden.

   Wenn Sie Qualys mit dem Setup-Assistenten konfiguriert haben, ist das Feld **Startzeit** vorab ausgefüllt, zunächst bis drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum.

   Hinweis:
   Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass große Datenmengen die Qualys-API-Quotenbeschränkungen überschreiten und Ausführungszeitüberschreitungen ausgelöst werden.

5. Klicken Sie auf **Absenden** oder **Aktualisieren**.
6. **Wahlweise:** Klicken Sie auf **Jetzt ausführen**, um die Ausführung sofort zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationen und Änderungen Qualys .

Konfigurieren Sie erweiterte optionale Änderungen, und optimieren Sie einige der Daten speziell für die Qualys -Integration. Die meisten dieser Änderungen erfordern Codierung oder fortgeschrittene ServiceNow - oder Qualys Cloud Platform -Kenntnisse.

Weitere Tipps für Qualys -Importe finden Sie im Wissensartikel mit Tipps zur Leistungsoptimierung für Qualys-Importaufträge in der HI Knowledge Base.

Ändern Sie die Werte für die Zuordnung von Qualys zu ServiceNow für Priorität und Status

Ändern Sie die Zuordnungswerte für Priorität und Status für Ihre Anforderungen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Dies ist eine erweiterte Anpassungsoption.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
2. Suchen Sie nach **Qualys-Werten zuordnen**, und öffnen Sie sie.
3. Klicken Sie auf die Registerkarte **Erweitert**.
4. Ändern Sie gemäß Ihren Anforderungen.
   Die häufigsten Änderungen umfassen das Hinzufügen neuer Statuswerte oder das Überarbeiten der Kritikalität oder Priorität.
5. Klicken Sie auf **Aktualisieren**.

Schränkt die Möglichkeit zum Schreiben in einen Datensatz basierend auf einer Zuweisungsgruppe ein

Sie können Schreib-/Leserechte für Datensätze basierend auf der Mitgliedschaft in einer zugewiesenen Gruppe einschränken. Ändern Sie Bedingungen und Skripts basierend auf bestimmten Anforderungen.

Vorbereitungen
Erforderliche Rolle: security_admin (erweiterte Rolle von Administrator)

Hinweis:
Diese Aktion wird im Schwachstellenbereich von ausgeführt.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerung (ACL)**.
2. Suchen Sie nach ACLs, die mit `sn_vul` beginnen.
3. Wählen Sie einen Zugriffssteuerungsdatensatz, z. B. sn_vul_vulnerable_item, **Operation write**.
4. Aktivieren Sie im Datensatz ggf. das Kontrollkästchen **Erweitert**, um die **Rolleneinträge** anzuzeigen.
5. Ändern Sie das **Rollenskript** entsprechend Ihren Anforderungen.
   Skriptbeispiel zum Ändern des Zugriffs nach Gruppe.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Klicken Sie auf **Aktualisieren**.

Richten Sie Scanner-Appliances ein

Wenn Sie Scans von Ihrem Now Platform® anstatt direkt von Qualys aus initiieren, können Sie Scans für IP-Adressbereiche einrichten.

Vorbereitungen

Die Daten stammen aus der Qualys -Integration basierend auf den Asset-Gruppen Qualys und den zugehörigen Standardgeräten (Scannern).

Wenn für die Ziel-IP-Adressbereiche keine Geräte konfiguriert sind, wird das Gerät, das als Standard für die Integrationsinstanz festgelegt ist, für den Scan verwendet.

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Scannergeräte**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Gerätename	Sie werden aufgefordert, dieses Feld auszufüllen, wenn Sie einen Datensatz manuell erstellen. Geben Sie den Namen für die Scanner-Appliance Qualys ein, die zum Aufrufen von Scans für übereinstimmende Configuration Items verwendet werden soll. Verwenden Sie den Wert Extern, wenn der Scan mit einem externen Scanner gestartet werden soll.
Geräte-ID	Geben Sie den Gerätebezeichner für das Scannergerät Qualys ein, das zum Aufrufen von Scans für übereinstimmende Configuration Items verwendet werden soll. Sie werden aufgefordert, dieses Feld auszufüllen, wenn Sie einen Datensatz manuell erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Verwenden Sie den Wert 0, wenn der Scan mit einem externen Scanner gestartet werden soll.
Gerätestatus	Zeigt den letzten Status der Scanner-Appliance für die von der Qualys -Integration zurückgegebenen Daten an. Bei manuell erstellten Datensätzen wird der Status nur aktualisiert, wenn eine gültige **Appliance-ID** angegeben ist.
Asset-Gruppen-ID	Zeigt den Bezeichner der Asset-Gruppe Qualys an, die diesen Datensatz erstellt hat. Dieses Feld zeigt einen Wert nur für Datensätze an, die durch die Qualys -Integration erstellt wurden.
Asset-Gruppenname	Zeigt den Namen der Asset-Gruppe Qualys an, die diesen Datensatz erstellt hat. Dieses Feld zeigt einen Wert nur für Datensätze an, die durch die Qualys -Integration erstellt wurden.
Bestellung	Geben Sie einen Wert ein, der zur Bestimmung der Scan-Priorität verwendet werden soll. Bei Geräten, die widersprüchliche Kriterien aufweisen, erhält ein Gerät mit einem niedrigeren Reihenfolgewert eine höhere Priorität.
Manuell erstellt	Gibt an, ob dieser Datensatz manuell vom Anwender erstellt wurde.
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine Filtergruppe für die Suche nach übereinstimmenden Konfigurationselementen für das Scannen anzugeben.
Filtergruppe	Wählen Sie die Filtergruppe aus, die Sie verwenden möchten, um übereinstimmende Configuration Items zum Scannen zu finden. Dieses Feld wird nur angezeigt, wenn Sie **Filtergruppe verwenden**ausgewählt haben.
IPs	Kommagetrennte Liste von IP-Adressen oder IP-Adressbereichen, die von diesem Gerät beim Aufrufen von Scans verwendet werden sollen.
Integrationsinstanz	Die Qualys -Integrationsinstanz, die dieser Appliance zugeordnet ist.
Optionsprofil	Wählen Sie das Optionsprofil aus, das Sie für Scans nach übereinstimmenden Configuration Items verwenden möchten.

3. Klicken Sie auf **Aktualisieren**.

Konfigurieren und verwalten Sie Qualys Schwachstellenscanner und Scans

Qualys Es können Schwachstellen-Scans durchgeführt werden, um Softwareschwachstellen zu finden, die sich auf Ihre CIs auswirken. Sie können Scans von einem Datensatz eines angreifbaren Elements aus initiieren oder indem Sie einen Scan-Datensatz direkt für Configuration Items (CIs) und IP-Adressen erstellen.

Wenn Sie Qualys angreifbare Elemente direkt vom Bildschirm „Angreifbare Elemente“ aus scannen, können Sie auch mehrere angreifbare Elemente gleichzeitig scannen.

Wenn Security Incident Response aktiviert ist, können Sie einen Scan auch aus dem Security Incident-Katalog, einem Security Incident-Datensatz oder einer Sicherheitsscan-Anforderung initiieren.

Scans, die von Qualys angreifbaren Elementen, Security Incident Catalog, Security Incidents oder Sicherheitsscananforderungen übermittelt werden, werden vom Standardscanner Qualys ausgeführt.

Sie können das Optionsprofil auswählen, das Sie für Scans für übereinstimmende Configuration Items verwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Optionsprofile enthalten Qualys Scan-Einstellungen.
- Ein Optionsprofil ist erforderlich, wenn Sie einen Qualys -Scan von Ihrem Now Platform®aus initiieren.

Konfigurieren Sie den von ServiceNow initiierten Qualys IP-Scan

Der im Basissystem enthaltene Scanner Qualys bietet eine Baselineintegration zum Initiieren von Scans basierend auf IP-Adressen.

Vorbereitungen
Sie können das Optionsprofil auswählen, das Sie für Scans für übereinstimmende Configuration Items verwenden möchten.

- Optionsprofile enthalten Qualys Scan-Einstellungen.
- Ein Optionsprofil ist erforderlich, wenn Sie einen Qualys-Scan von Ihrem Now Platform®aus initiieren.

Erforderliche Rolle: sn_vul_qualys.admin

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Öffnen Sie den Datensatz Qualys.
3. Aktivieren Sie die Kontrollkästchen**Aktiv** und **Standard**.

   Die Auswahl von **„Aktiv“** ist erforderlich, um den Scanner Qualys zum automatischen Scannen von VIs Qualys zu verwenden. Sie müssen auch nicht **Standard** auswählen, damit er automatisch ausgeführt wird.

   Vor v12.0 ist **Active** erforderlich, um den Scanner zu verwenden. Wenn auch **Standard** ausgewählt ist, wird der Scanner automatisch verwendet, ohne dass er während des Scanvorgangs ausgewählt werden muss.
4. Klicken Sie im Feld Quellenintegration auf das Suchsymbol, und wählen Sie die Option für **Qualys**aus, z. B. **Qualys-Cloud-Plattform**.
5. Klicken Sie auf **Aktualisieren**.
6. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
7. Öffnen Sie die **Qualys-Asset-Gruppenlistenintegration**.
   a. Aktivieren Sie die Checkbox **Aktiv**.
   b. Klicken Sie auf **Jetzt ausführen**.
8. Befolgen Sie diese Schritte, um Ihre Scanner-Geräte zu füllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Möglicherweise möchten Sie die Integration der Optionsprofilliste nach einem Import aus den Suchlistenintegrationen, der dynamischen Qualys-Suchliste und der statischen Qualys-Suchlistenintegration ausführen, um zu sehen, welche Suchlisten mit Optionsprofilen verknüpft sind.

a. Öffnen Sie die **Qualys-Optionsprofil-Listenintegration**.

b. Aktivieren Sie die Checkbox **Aktiv**.

c. Klicken Sie auf **Jetzt ausführen**.

d. Führen Sie die unter Richten Sie Scanner-Appliances ein aufgeführten Schritte aus, um Ihre Scanner-Geräte zu konfigurieren.
Kehren Sie hierher zurück, nachdem Sie diese Schritte abgeschlossen haben, um mit der Konfiguration fortzufahren.

e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.

f. Öffnen Sie die **Qualys-Appliance Listenintegration**.

g. Aktivieren Sie die Checkbox **Aktiv**.

h. Klicken Sie auf **Jetzt ausführen**.
Ihre Scanner-Geräte Qualys sind jetzt korrekt gefüllt.

Zugehörige Informationen

Qualys Vulnerability Integration verstehen

Scannen Sie mehrere Qualys Schwachstellen oder angreifbare Elemente

Sie können gleichzeitig mehrere Qualys Schwachstellen oder angreifbare Elemente scannen, die mindestens ein betroffenes Configuration Item (CI) oder eine im Formular ausgefüllte IP-Adresse enthalten.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Führen Sie einen der folgenden Schritte aus:

- Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
- Navigieren zu **Alle** > **Vulnerability Response** > **Alle angreifbaren Elemente**.

2. Aktivieren Sie die Kontrollkästchen für die Datensätze, die Sie scannen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie **auf die Liste Aktionen für ausgewählte Zeilen** und dann auf **Erneut nach angreifbaren Elementen suchen**.
   Es wird eine Nachricht mit einem Link zum Scan angezeigt, und die Arbeitsnotizen werden aktualisiert.
4. Klicken Sie auf den Link, um den Fortschritt oder die Ergebnisse des Scans anzuzeigen.

Konfigurieren Sie die automatische Prüfung Qualys auf gelöste Korrekturaufgaben

Sie können den Scan planen, der automatisch ausgeführt wird, um Ihre angreifbaren Qualys Elemente zu aktualisieren.

Vorbereitungen

Nachdem eine Korrekturaufgabe in **den Status Gelöst**überführt wurde, wird automatisch ein Scan initiiert, um den Status der zugehörigen angreifbaren Elemente zu aktualisieren.

- Die Prüfung ist standardmäßig deaktiviert.
- Aktivieren Sie die Prüfung mit dem Integrationsinstanzparameter **scan_on_resolved** im **Qualys** -Datensatz unter **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen** > **Qualys-IDs**. Weitere Informationen finden Sie in den folgenden Schritten.
- Diese Prüfung ist instanzspezifisch. Wenn Sie mehrere Instanzen haben und diesen Scan aktivieren oder deaktivieren möchten, müssen Sie den Parameter **scan_on_resolved** in den Parametern der Integrationsinstanz für jede Instanz deaktivieren, die Sie ändern möchten.
- Wenn die Prüfung aktiviert ist, können Sie sie bei Bedarf initiieren oder die Prüfung so planen, dass sie nur in einem bestimmten Zeitfenster ausgeführt wird. Informationen zum Festlegen der Start- und Endzeiten für das Zeitfenster finden Sie unter Konfigurieren Sie erneute Scans Qualys so, dass sie nur innerhalb geplanter Intervalle ausgeführt werden.

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**.
2. Wählen Sie **Qualys** aus, um den Datensatz zu öffnen.
   Die Parameter der Integrationsinstanz für Qualys werden auf einer Registerkarte angezeigt.
3. Um die automatische Suche zu aktivieren, suchen Sie den Parameter `scan_on_resolved`.
4. Geben Sie in der Spalte „Wert“ für die Eigenschaft `true`ein.
5. Klicken Sie auf **Aktualisieren**.

Konfigurieren Sie erneute Scans Qualys so, dass sie nur innerhalb geplanter Intervalle ausgeführt werden

Legen Sie für Qualys Vulnerability Integration die Parameter für die Start- und Endzeit des Scans so fest, dass erneute Scans nur während der gewünschten Stunden ausgeführt werden oder verfügbar sind.

Vorbereitungen

Diese Konfiguration gilt für geplante erneute Scans und manuell im Produkt Qualys von Ihrer Instanz von Now Platform® aus.

Durch das Festlegen der Start- und Endzeitparameter für Scans für Integrationsinstanzen können Sie Zeitfenster angeben, in denen erneut Scans im Produkt Qualys verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise können Sie angeben, dass erneute Scans nur außerhalb der Geschäftszeiten verfügbar sind, z. B. von Mitternacht bis 10:00 Uhr.

Diese Einstellung ist instanzspezifisch. Wenn Sie mehrere Instanzen haben, müssen Sie die Werte scan_start_time und scan_end_time in den Parametern der Integrationsinstanz in jeder Instanz konfigurieren, die Sie ändern möchten.

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen** > **Qualys-IDs**.
2. Klicken Sie auf **Qualys**, um den Datensatz zu öffnen.
   Die Parameter der Integrationsinstanz für Qualys werden angezeigt.
3. Geben Sie für den Parameter scan_start_time in der Spalte Wert die Zeit in der UTC-Zeitzone im 24-Stunden-Format (00:00 bis 24:00) für die Startzeit des Fensters ein, für das erneute Scans verfügbar sein sollen.
4. Geben Sie für scan_end_time in der Spalte „Wert“ Zeiten im gleichen Format (00:00 bis 24:00) für die Endzeit des verfügbaren Fensters ein.
   Wenn Sie beispielsweise eine Startzeit von 00:00 Uhr für den Parameter scan_start_time und eine scan_end_time von 10:00 Uhr am selben Morgen eingeben, werden Scans, die außerhalb des Zeitfensters von Mitternacht bis 10:00 Uhr geplant sind oder manuell gestartet werden, in die Warteschlange gestellt und im gestartet Startzeit des Zeitfensters des folgenden Tages, 00:00.

   Im gleichen Beispiel: Wenn ein Korrekturbesitzer manuell einen erneuten Scan um 11:00 Uhr initiiert, wird der erneute Scan nicht sofort gestartet, da er außerhalb der verfügbaren konfigurierten Scan-Zeiten liegt. Die Scan-Anforderung bleibt bis zum Beginn des Zeitfensters des folgenden Tages in der Warteschlange, in diesem Beispiel (00:00).
5. Klicken Sie auf **Aktualisieren**, um Ihre Einstellungen zu speichern.

Qualys Quotenbegrenzungen für Schwachstellen-Scans

Sie können die Rate definieren, mit der verschiedene Arten von Scans durchgeführt werden, um die Anzahl der Anforderungen zu begrenzen, die an einen externen Scanner gesendet werden. Nachdem Sie Quotengrenzen definiert haben, können Sie sie auf die Qualys -Scanner anwenden.

Definieren Sie Qualys Scanratengrenzen

Sie können die Rate definieren, mit der verschiedene Arten von Scans durchgeführt werden, um die Last in Ihrer Scan-Warteschlange auszugleichen. In der Quotengrenze definierte Bedingungen bestimmen, ob die Quotenbegrenzungen auf Einträge in der Warteschlange angewendet werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.admin

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Quotengrenzdefinitionen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Definition der Quotengrenze

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an, der die Bedingungen identifiziert, die der Warteschlangeneintrag erfüllen muss. Beispiel: Scans pro Minute
Bedingungen der Warteschlange	Geben Sie Bedingungen ein, anhand derer bestimmt wird, ob ein Scan-Eintrag in der Warteschlange dieser Quotenbegrenzung unterliegt. Die Bedingungen dürfen nicht für einen bestimmten Scanner spezifisch sein.
Auswertungsskript	Schreiben Sie ein Skript mit der Logik zum Auswerten des Eintrags in der Warteschlange. Es ist wichtig, dass das Skript „wahr“/„falsch“ zurückgibt, um zu definieren, ob der Eintrag verarbeitet wird. Basieren Sie das Bewertungsskript außerdem auf dem Eintrag in der Warteschlange, der ausgewertet wird.

4. Klicken Sie auf **Absenden**.

Wenden Sie Scanratenbegrenzungen auf Qualys Scanner an

Nachdem Sie mit **„Quotenbegrenzungsdefinitionen“**Scan-Quotengrenzen definiert haben, können Sie „Quotengrenzen“ auf bestimmte Qualys -Scanner anwenden.

Vorbereitungen

Erforderliche Rolle: sn.vul_admin

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scannerquotengrenzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Scannerquotengrenze

Feld	Beschreibung
Scanner	Wählen Sie den Scanner aus, für den Sie eine Quotengrenze anwenden möchten.
Quotengrenze	Wählen Sie die Quotengrenze aus, die Sie auf diesen Scanner anwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schwellenwert	Geben Sie den Schwellenwert für den ausgewählten Scanner für die ausgewählte Quotengrenze ein. Wenn der Scanner beispielsweise 4 Scans pro Minute zulässt und die Quotengrenze auf Anforderungen pro Minute festgelegt ist, liegt der Schwellenwert bei 4.

4. Klicken Sie auf **Absenden**.

Zeigen Sie die Schwachstellen-Scan-Warteschlange Qualys an

Anforderungen für Schwachstellenprüfungen, die an die Schwachstellenscanintegration Qualys übermittelt werden, werden in die Warteschlange gestellt, um die Systemressourcen nicht zu überlasten. Sie können den Status von Anforderungen in der Warteschlange bei Bedarf anzeigen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
In der Liste der Scans in der Warteschlange enthält jeder Scan einen automatisch generierten Scan-Namen, der das gescannte CI identifiziert.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scan-Warteschlange**.
   Alle Qualys Scan-Anforderungen, die übermittelt wurden, werden in einer Liste angezeigt. Die Spalte **„Status“** zeigt den aktuellen Status jedes Eintrags in der Warteschlange an. Der Status **Abgeschlossen** gibt an, dass der Scan die Warteschlange verlassen hat. Dies bedeutet nicht unbedingt, dass die Verarbeitung des Scans abgeschlossen ist. Wenn die Prüfungen abgeschlossen wurden oder fehlgeschlagen sind, wird in der Spalte **„In Verarbeitung“** der entsprechende Text in den Arbeitsnotizen angezeigt.

   Hinweis:
   Wenn ein Hash-Wert zum Scannen übermittelt wurde und der Scanner kein Ergebnis findet, wird unter **StatusAbgeschlossen** angezeigt, und in der Arbeitsnotiz in der Spalte **Verarbeitung** wird **Unbekannt**angezeigt.

2. Klicken Sie nach Abschluss der Verarbeitung eines Scans auf einen Datensatz in der Warteschlange, um Details für die Scan-Anforderung anzuzeigen.

Basissystemfilter für bestätigte Erkennungsimporte aktivieren

Aktivieren Sie einen Standardfilter mit Integrationsparametern, um nur bestätigte Erkennungen aus Qualys Cloud Platformzu importieren.

Vorbereitungen
Erforderliche Rolle: sn_vul_qualys.admin, sn_vul.vr_import_admin

Warum und wann dieser Vorgang ausgeführt wird
Für den Import einer gefilterten Liste von Erkennungen aus Qualys Cloud Platformist ein Instanzparameter für die Basissystemintegration „include_only_confirmed“ verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig ist dieser Parameter auf *FALSE*festgelegt, und alle Erkennungen (Potenzielle Erkennungen, Bestätigte Erkennungen oder Informationserkennungen) werden importiert.

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**.
2. Öffnen Sie die Qualys-Cloud-Plattformintegration aus der Liste der Integrationsinstanzen.
3. Öffnen Sie in der Liste „Integrationsinstanzparameter“ den Parameter „*include_only_confirmed*“.
4. Aktualisieren Sie den Standardwert auf *True*.
5. Klicken Sie auf **Aktualisieren**.
   Sie haben den Filter aktiviert, um bestätigte Erkennungen aus der Qualys Cloud Platform Integration zu importieren.

Ergebnisse

Standardmäßig werden nur bestätigte Erkennungen aus der Integration Qualys Cloud Platform importiert, wenn der nächste Qualys-Schwachstellenimport ausgeführt wird. Alle anderen Erkennungen wie informative und potenzielle Erkennungen werden ignoriert und nicht importiert. Weitere Informationen finden Sie unter Erkennungsdaten für angreifbare Elemente in Vulnerability Response anzeigen.

Initiieren Sie den erneuten Scan für Qualys Vulnerability Integration

Stellen Sie sicher, dass die angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie bei Bedarf im Produkt Qualys von Ihrem Now Platform aus erneut Scans initiieren.

Vorbereitungen

Sie können erneute Scans über die Vulnerability Response-Arbeitsbereiche initiieren. Weitere Informationen finden Sie unter Scannen Sie Datensätze und Korrekturaufgaben im erneut Vulnerability Manager Workspace und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.

Informationen zum erneuten Scannen in der klassischen Umgebung finden Sie in den folgenden Abschnitten.

Erforderliches Setup für erneute Scans im Produkt Qualys, das über Ihren Now Platforminitiiert wurde:

Sie können bei Bedarf von Ihrer Instanz Now Platform® aus einen erneuten Scan auf angreifbare Elemente für das Produkt Qualys initiieren.

Um den Aufwand und das Volumen zu reduzieren, die mit geplanten, vollständigen Scans verbunden sind, können Nachbesserungsbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen für Assets (Konfigurationselemente) in ihren Umgebungen initiieren. Sie können erneute Scans im Produkt Qualys aus Datensätzen von angreifbaren Elementen (VI), Korrekturaufgaben (RT), Drittparteieinträgen (TPE) oder erkannten Elementen in Ihrer Instanz von Now Platform initiieren.

Durch erneute Scans können Sie überprüfen, ob durch Ihre Nachbesserungsaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben wurden.

Anwendungsfall:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Now Platform für angreifbare Elemente vom Typ Qualys initiieren.

Sie können erneute Scans für VIs mit Qualys als Quelle in anderen Status als „Geschlossen“ initiieren. Siehe Scannen Sie Datensätze und Korrekturaufgaben im erneut Vulnerability Manager Workspace und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.

Stellen Sie sicher, dass Sie das folgende Setup abgeschlossen haben, das für erneute Scans erforderlich ist. Weitere Informationen finden Sie in den Schritten beginnend mit Konfigurieren und Verwalten von Qualys -Schwachstellenscannern und den in den vorherigen Abschnitten aufgeführten Scans.

Erforderliche Rolle: sn_vul_manually_initiate_rescan

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, von dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Sie können erneute Scans nur für VIs mit Qualys als Quelle initiieren. Überprüfen Sie, ob Qualys in der Spalte **„Quelle“** in den VI-Listenansichten oder in den Feldern **„Quelle“** in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol**Liste personalisieren** (Zahnradsymbol), und verwenden Sie den Slushbucket, um **die Quelle** von **Verfügbar** in **Ausgewählt**zu verschieben.

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**, **Vulnerability Response** > **Bibliotheken** > **Drittpartei**, oder zu **Erkannte Elemente** für die Korrekturaufgabe, den Drittparteieintrag oder die Datensätze zu erkannten Elementen, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die Schaltfläche **Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem Produkt Qualys stammen und sich in einem anderen Status als **Geschlossen befinden**. Bei mehreren VI-Datensätzen müssen alle VIs Qualys als Quelle haben und sich in einem anderen Status als **Geschlossen befinden**.
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem beliebigen anderen Status als **Geschlossen**befinden, und alle zugeordneten VIs müssen Qualys als Quelle haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In einem TPE-Datensatz (Drittparteieintrag) muss der Datensatz über mindestens einen zugeordneten VI-Datensatz in einem anderen Status als „ **Geschlossen“** mit Qualys als Quelle verfügen.
- In einem Datensatz eines erkannten Elements ist dem Konfigurationselement mindestens ein VI mit Qualys als Quelle in einem anderen Status als **Geschlossen**zugeordnet.

4. Klicken Sie oben rechts im ausgewählten Datensatz auf **Erneut scannen**.
Wählen Sie im angezeigten Dialogfeld eine aus, um fortzufahren.

Option	Beschreibung
Aktivieren Sie das Kontrollkästchen **Optionsprofile** angeben.	Wählen Sie in der Liste das Optionsprofil für den Scanner Qualys aus, den Sie für den erneuten Scan verwenden möchten. Dies sind die Geräte (Scanner), die Sie konfiguriert und unter aufgelistet haben **Qualys Schwachstellenintegration** > **Scannergeräte**.
Deaktivieren Sie das Kontrollkästchen **Optionsprofile angeben** (nicht ausgewählt).	Für den Scan wird das Optionsprofil Qualys für den Scanner verwendet, den Sie als Standardscanner in der Liste Scanner-Appliances festgelegt haben. Weitere Informationen zum Festlegen der Standardscanner, die Sie über Now Platforminitiieren, finden Sie unter Setup-Scanner-Appliances, die im vorherigen Abschnitt aufgeführt sind.

5. Klicken Sie auf **Scan anfordern**.

Es wird eine Nachricht angezeigt, die anzeigt, dass Ihre Prüfung verarbeitet wird. Der Status für alle erneut gescannten Elemente kann jederzeit unter den zugehörigen Scan-Listen in den Datensätzen für VI, RT, TPE und erkannte Elemente gefunden werden, mit denen Sie die erneuten Scans gestartet haben. Klicken Sie in der Nachricht **auf Details anzeigen**, um den Status des erneuten Scans und alle anderen von einem bestimmten Datensatz gestarteten erneuten Scans anzuzeigen.

Ihre Instanz von verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist (je nachdem, was zuerst eintritt). Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde.

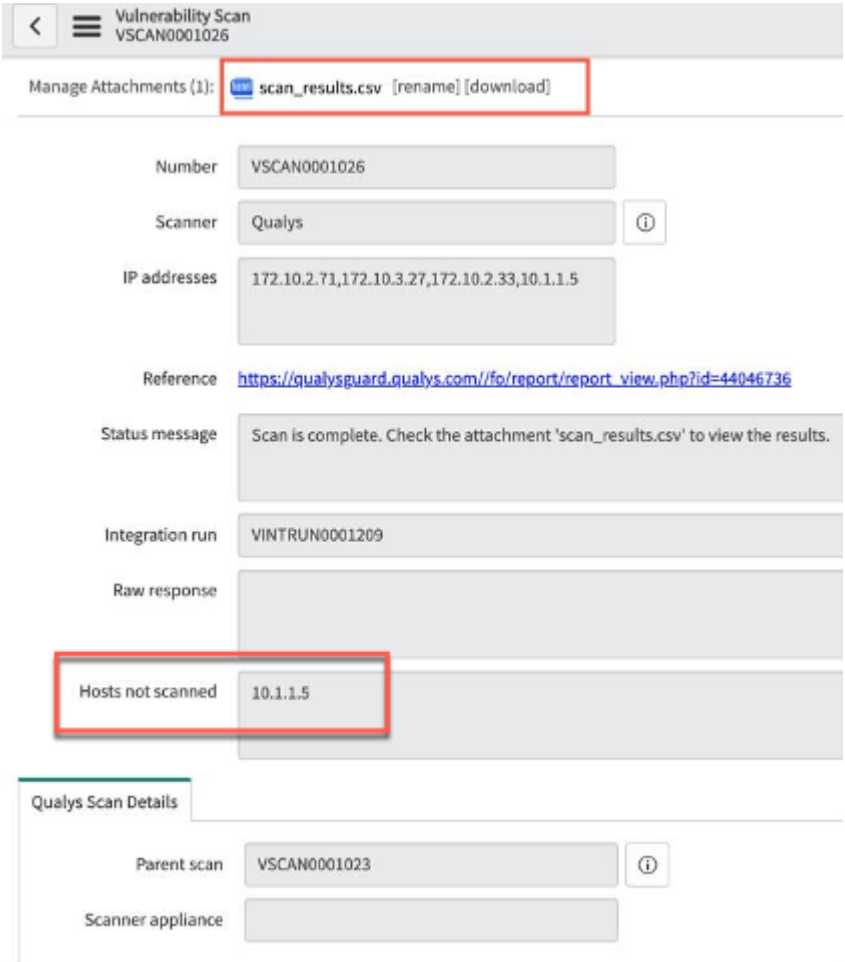
Nach dem erneuten Scannen wird automatisch die Qualys Host Detection Integration initiiert, um Ihre angreifbaren Elemente zu aktualisieren. Je nachdem, wie viele VIs Sie haben, werden Ihre Erkennungen, VIs und RTs nach Abschluss des Scans Qualys Integration für Host-Erkennung aktualisiert. Navigieren Sie zu diesen Datensätzen, um die Aktualisierungen anzuzeigen, nachdem die Hosterkennungsintegration abgeschlossen wurde.

Dieser Scan ist instanzspezifisch und kann deaktiviert werden. Weitere Informationen zu den Qualys -Integrationen und zur Anzeige der Integrationen finden Sie unter Qualys Vulnerability Integration verstehen.

Nächste Maßnahme

Sie können einen CSV-Anhang im Scan-Datensatz anzeigen, um Details zu den erneuten Scans anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wie in der vorherigen Abbildung gezeigt, werden bei einem erneuten Scan die Erkennungen und VIs, die diesen Assets zugeordnet sind, nicht aktualisiert, wenn Hosts (Konfigurationselemente) in Ihrer Umgebung nicht zugänglich sind, wenn der erneute Scan abgeschlossen ist. Damit Sie verstehen, warum sie nicht enthalten sind, werden die Asset-IP-Adressen für diese CIs nach Abschluss des erneuten Scans in den Schwachstellen-Datensätzen im Feld Nicht gescannte Hosts aufgeführt.

Qualys Metadaten für Schwachstellen

Die Qualys Hosterkennungsintegration wird um weitere Felder von Qualyserweitert. Diese Felder helfen beim Filtern der nicht ausnutzbaren Linux -Schwachstellen. Diese Erweiterung verbessert die Integration auf Erkennungsebene und auf Ebene der angreifbaren Elemente (VI, Vulnerable Item).

Importieren Sie zusätzliche Metadaten aus Qualys

Importieren Sie zusätzliche Metadaten für Vulnerability Items (VI), um Schwachstellen basierend auf den Auswirkungen auf einen Kernel oder Service zu filtern.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.
2. Klicken Sie unter Integrationskonfiguration auf **Scanner-Integrationen**.
3. Klicken Sie unter „Installierte Anwendung“ für die Anwendung Qualys**auf Bearbeiten**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Hosterkennungskonfiguration**.
5. Navigieren zu **Weitere Metadaten für Erkennungen importieren**.
6. Um zusätzliche Metadaten aus Qualyszu importieren, aktivieren Sie manuell eines der folgenden Kontrollkästchen.
   - **Kernel-Metadaten**: Identifiziert Schwachstellen, die in laufenden oder nicht ausgeführten Linux-Kerneln gefunden wurden.

     Wenn der Wert der zurückgegebenen Metadaten **„No"**ist, bedeutet dies, dass die Schwachstelle aufgrund eines nicht ausgeführten Kernels nicht ausgenutzt werden kann. Informationen zu den abgerufenen Werten finden Sie unter Qualys Metadatenwerte für Schwachstellen.
   - **Service-Metadaten**: Identifiziert Schwachstellen, die für laufende oder nicht laufende Ports oder Services gefunden wurden.
   - **Nutzbare Konfigurationsmetadaten**: Identifiziert Schwachstellen, die aufgrund der aktuellen Hostkonfiguration ausgenutzt werden können oder nicht.

   Hinweis:
   Standardmäßig sind diese Kontrollkästchen nicht aktiviert.
7. Integration der Hosterkennung Qualys mit einem Backdate ausführen.
   Weitere Informationen zum Festlegen des Startdatums finden Sie unter Optionale Qualys-Änderungen.

Ergebnisse
Die Metadaten wurden importiert.

Nächste Maßnahme
Um die importierten Metadaten anzuzeigen, geben Sie in der Filternavigation `sn_vul_detection.list` ein. Die Liste der Erkennungen von angreifbaren Elementen wird angezeigt. Weitere Informationen zu den in den neu hinzugefügten Spalten angezeigten Werten finden Sie unter Qualys Metadatenwerte für Schwachstellen.

Qualys Metadatenwerte für Schwachstellen

Wenn die Kernel-Metadaten, Service-Metadaten und Konfigurationsmetadaten importiert werden, werden auch einige Werte abgerufen. Die Werte **0**, **1** und **Nicht verfügbar** werden im Back-End verarbeitet und in **Nein**, **Ja** bzw. **Leer** konvertiert.

Diese Werte werden in den folgenden Spalten in der Liste „Erkennungen von Schwachstellenelementen" und „Schwachstellenelemente" ausgefüllt:

- Betrifft die Spalte für den laufenden Service
- Betrifft die ausnutzbare Konfigurationsspalte
- Wirkt sich auf die Ausführung von Kernelspalten aus

Hinweis:

- Diese Spalten sind standardmäßig nicht sichtbar. Weitere Informationen zum Konfigurieren des Formularlayouts finden Sie unter Formularlayout konfigurieren
- Bei älteren Erkennungen können die Werte für diese Spalten leer sein. Um die Daten zu aktualisieren, führen Sie eine rückwirkende Qualys-Host-Erkennungsintegration aus. Weitere Informationen zum Festlegen des Startdatums finden Sie unter Optionale Qualys-Änderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Tabelle zeigt die abgerufenen Werte und ihre Bedeutung.

Abgerufene Feldwerte und ihre Bedeutung

Feld	Wert	Bedeutung
AFFECT_RUNNING_KERN	0	Schwachstelle in einem nicht ausgeführten Kernel gefunden. Die Schwachstelle kann nicht ausgenutzt werden.
AFFECT_RUNNING_KERN	1	Schwachstelle in einem laufenden Kernel gefunden. Die Schwachstelle ist ausnutzbar.
AFFECT_RUNNING_KERN	Nicht verfügbar	Die Schwachstelle ist keine Kernel-bezogene Schwachstelle.
AFFECT_RUNNING_SERVICE	1	Die Schwachstelle liegt an nicht ausgeführten Ports oder Services. Die Schwachstelle kann nicht ausgenutzt werden.
AFFECT_RUNNING_SERVICE	0	Schwachstelle in laufenden Ports oder Services gefunden. Die Schwachstelle ist ausnutzbar.
AFFECT_RUNNING_SERVICE	Nicht verfügbar	Schwachstelle ist keine zugehörige Schwachstelle.
AFFECT_EXPLOITABLE_CONFIG	1	Schwachstelle kann aufgrund der Hostkonfiguration nicht ausgenutzt werden.
AFFECT_EXPLOITABLE_CONFIG	0	Schwachstelle ist aufgrund der Hostkonfiguration ausnutzbar.
AFFECT_EXPLOITABLE_CONFIG	Nicht verfügbar	Schwachstelle ist keine zugehörige Schwachstelle.

Legen Sie zusätzliche Filterparameter für Qualys -Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Qualys Vulnerability Integration an, um die Schwachstellendaten, die Sie mit den unterstützten Integrationen Qualys importieren, weiter zu verfeinern.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, um nur bestimmte Schwachstellendetails überprüfen zu können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach bestimmten IPs oder IP-Bereichen gefiltert werden. Oder Sie möchten nur Computer importieren, die sich in Ihrem Anwendungsbereich befinden, z. B. nur Computer innerhalb Ihres Unternehmensnetzwerks, die keine externen Geräte sind.

Um diese Daten zu sammeln, können Sie Qualys Parameter hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit den Parametern Qualys in Ihrem Now Platformanpassen. Sie können diese Werte in Ihrem HTTP-Methodendatensatz unter der REST-Methode für die unterstützten Qualys -Integrationen von Qualys Vulnerability Integrationändern oder hinzufügen.

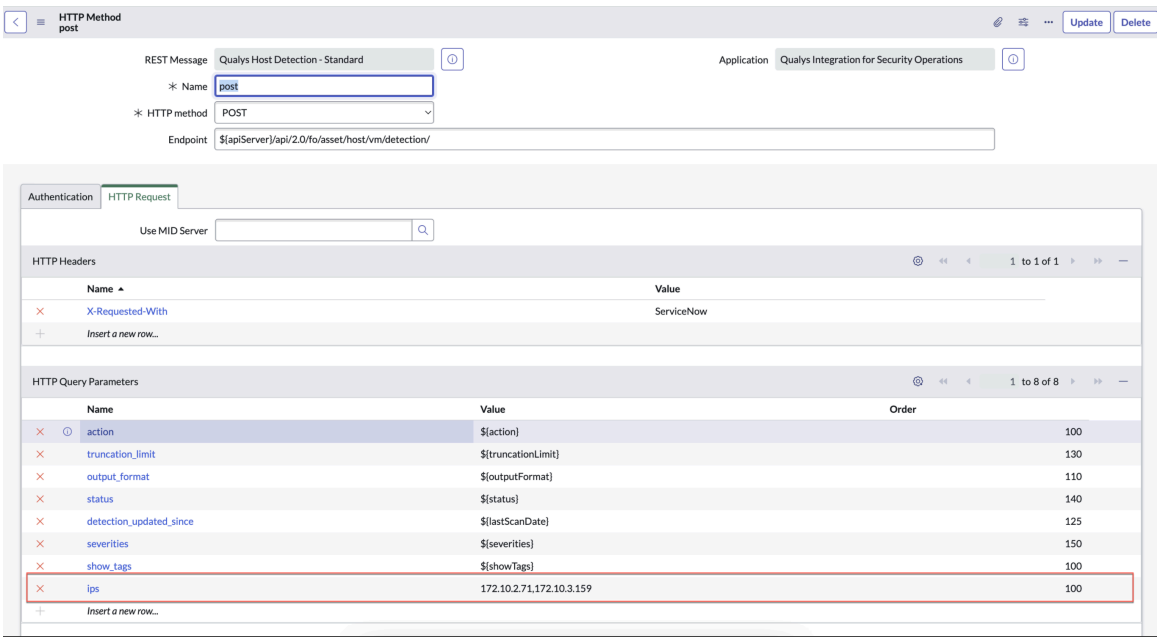
Erforderliche Rolle: sn_vul.vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Suchen Sie die vom Produkt Qualys unterstützten Parameter auf der Entwickler-Site, die Sie für die Filterung verwenden möchten.
   Parameter und Werte, die Sie aus dem Produkt Qualys eingeben, werden nur auf der Ebene der Integrationsinstanz in Ihrem Now Platformunterstützt. Alle Qualys Integrationen unterstützen die Filterung anhand von Abfrageparametern.
2. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
3. Klicken Sie auf der Listenseite Qualys Integrationen auf den Datensatz für die Integration, für die Sie den Datensatz öffnen möchten.
4. Wählen Sie die Registerkarte Qualys REST-Details aus, suchen Sie das Informationssymbol (I) für die REST-Methode und anschließend auf **Datensatz öffnen,** und klicken Sie darauf, um den Datensatz für die HTTP-Methode zu öffnen.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Fügen Sie in den HTTP-Abfrageparametern für den Anforderungstext die Werte hinzu, die Sie von der Developer Site Qualys erhalten haben.

   In der folgenden Abbildung wurde als Beispiel der Parameter *ips={value}* hinzugefügt, der nur bestimmte IP-Adressen/Bereiche erfasst. In diesem Fall entspricht **der Wert** einer oder mehreren von Ihnen angegebenen IPs/Bereiche. Mehrere Einträge werden durch Kommas getrennt, 172.10.2.71, 172.10.3.159, und ein Bereich wird mit einem Bindestrich angegeben, 10.10.10.1-10.10.10.100. Weitere Informationen finden Sie auf der Entwickler-Website Qualys.



   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Qualys weitere Informationen zum Trennen der einzelnen Werte.

   Hinweis:
   Sie sollten sich Ihrer API-Anforderungen bewusst sein. Möglicherweise müssen Sie diese API-Eigenschaften den Abfrageparametern oder dem Textinhalt hinzufügen.

   Einige andere Parameter, die auf der Entwicklerseite Qualys nützlich sein könnten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `ag_ids` Abzurufende Asset-Gruppenlisten-IDs. Dieser Parameter stellt sicher, dass nur Computer in Ihrem Bereich einbezogen werden.
- `qids` Dieser Parameter beschränkt die Ergebnisse auf bestimmte Schwachstellen (QID in der Tabelle „Drittpartei-Einträge“). Diese Einstellung verhindert, dass Ihr System mit Informationsdatensätzen überschwemmt wird.

7. Klicken Sie auf **Aktualisieren**.

Behebung von Problemen bei der Qualys-Schwachstellenintegration

Einige häufig auftretende Probleme und Problemumgehungen werden besprochen.

Anhänge werden nach dem Import nicht angezeigt

Wenn Anhänge nach dem Import von Drittparteiintegrationen für Datenquellen oder bei einem Security Incident nicht wie erwartet angezeigt werden, überprüfen Sie Ihre IP-Beschränkungen.

IP-Zugriffsbeschränkungen können verhindern, dass Anhänge sichtbar sind, es sei denn, Sie sind von einer sicheren IP angemeldet. Da bei jedem Import ein neuer Anhang hinzugefügt wird, kann dies zu Duplikaten führen, die Sie entfernen müssen.

Wenn Sie beispielsweise die Importintegration eines Drittanbieterhosts ausführen und keine Anhänge in Ihren Datenquellen angezeigt werden, überprüfen Sie die IP-Einschränkungen, und fügen Sie vor dem Import der sicheren Liste Anwender hinzu.

Ändern Sie Transformationszuordnungen

Transformationszuordnungen werden mit Basiskonfigurationen bereitgestellt und reichen normalerweise aus. Sie können die Transformationszuordnungen entsprechend den Anforderungen Ihrer Organisation ändern.

Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin + import_admin

Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Administration** > **Transformationszuordnungen** um die REST-Nachrichten anzuzeigen.
2. Filtern Sie die resultierende Liste nach Anwendung, und beschränken Sie die Liste auf die Anwendung **Qualys Vulnerability Integration**.
3. Ändern Sie die Transformationszuordnungen gemäß den Kundenanforderungen.

   Einzelheiten zu den von der Qualys-API bereitgestellten Daten finden Sie in der Dokumentation zur Qualys-API .

Überprüft die Größe der XML-Anhangeigenschaft

Überprüft, ob die XML-Anhangseigenschaft für große Dateien ausreichend ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Import Export**.
2. Scrollen Sie nach unten zu **Importeigenschaften** > **XML-Format** unten auf der Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ändern Sie den Wert bei Bedarf in 250, und klicken Sie auf **Speichern**.

Zugehörige Informationen

Verfügbare Systemeigenschaften

Einschränkungen beim Datenabruf

Standardmäßig gibt es keine Einschränkungen für den Abruf von Daten aus Qualys. Viele Datensätze können sich auf Schwachstellen mit niedrigem Schweregrad beziehen, die ein Kunde nicht bereit ist, mit seinem Vulnerability Response-Prozess zu beheben. Durch Aktualisieren der entsprechenden REST-Nachrichten-/Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/-Methode ist **Qualys Host Detection – Standard/post**. Um die Werte zu aktualisieren, fügen Sie der Post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3–5 (oder die gewünschten Schweregrade)

Fehler bei der Qualys-Knowledge Base-Integration wird behoben

Beheben Sie den Fehler bei Qualys der Knowledge Base-Integration, indem Sie die von Qualys empfangene Nutzlast-Anhanggröße auf den angegebenen Grenzwert reduzieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Stellen Sie sicher, dass die Anhangsgröße der Nutzlast innerhalb des angegebenen Grenzwerts liegt.
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.
   b. Wählen Sie die Registerkarte **Integrationsinstanzparameter**.
   c. Wählen Sie **max_delta_days** aus, und ändern Sie den Standardwert in 3.
2. Wenn die Integration weiterhin fehlschlägt, führen Sie die folgenden Schritte aus:
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen**.
   b. Wählen Sie **Qualys Knowledge Base**aus.
   c. Wählen Sie die Registerkarte **Integrationsdetails**.
   d. Wählen Sie im Feld **Startzeit** das aktuelle Datum aus, um die Ausführung der Ausführung für diesen Tag zu überspringen.
   e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie die Registerkarte **Integrationsinstanzparameter**.

g. Wählen Sie **kb_backfill_full_import** aus, und ändern Sie den Standardwert in „wahr“.

Ergebnisse

Durch die Ausführung der Qualys-Knowledge Base-Auffüllungsintegration werden alle Drittparteieinträge (TPEs) im System aktualisiert. Die Qualys-Host-Erkennungsintegration erstellt einen Platzhaltereintrag, die Qualys-Knowledge-Base-Auffüllungsintegration aktualisiert ihn.

Qualys Vulnerability Integration Berichterstellung

Die Übersicht Qualys Cloud Platform bietet eine Ausführungsansicht der Schwachstellenaktivität. Durch die Bereitstellung von Trends, Berichten und Drilldowns zu bestimmten Daten können Administratoren oder Analysten schnell Problempunkte erkennen. Die Diagramme werden mit Daten gefüllt, nachdem angreifbare Elemente und die Knowledge Base-Daten Qualys abgerufen wurden.

Datenvisualisierungen in den -Arbeitsbereichen Vulnerability Response .

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad aktiver Schwachstellen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen anzeigen, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Vulnerability Manager Workspace und IT Remediation Workspace erkunden.

Frühere Versionen von Vulnerability Response

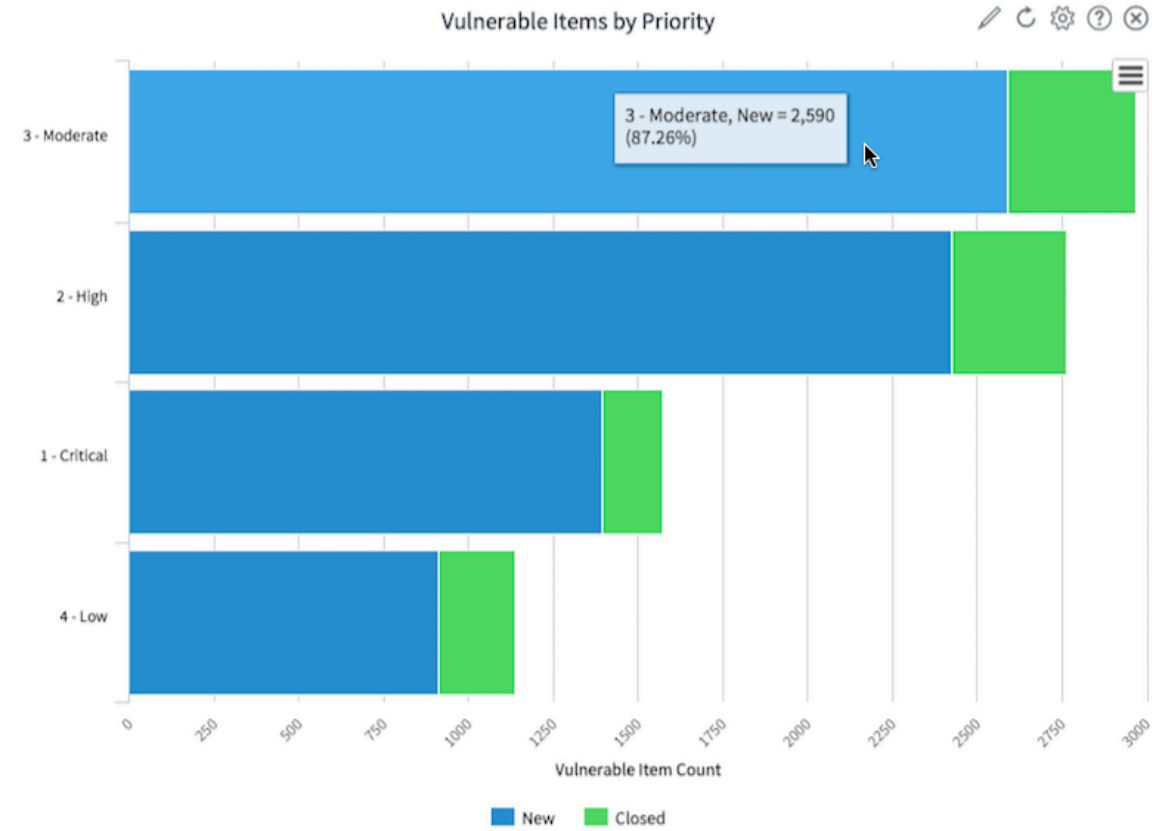
Schwachstellenanalysten können auch die Standarddashboards in der klassischen Umgebung zur Überwachung von Schwachstellendaten verwenden. Weitere Informationen finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..

Hinweis:
Die Verwendung der Qualys Cloud Platform Vulnerability-Integration setzt voraus, dass in Ihrer Instanz Optimierungs-, Test- und Bereitstellungsvorgänge durchgeführt wurden. Diese Funktionen sind Bereiche, die über den Umfang der Produktdokumentation hinausgehen. Wenden Sie sich zur Unterstützung an Kundenservice und Support.

In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms (Balken, Kreis, Datenpunkt usw.) zeigen, um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispieldiagramm Qualys Vulnerability Integration



Die folgenden Berichte sind auf der Homepage Qualys Cloud Platform verfügbar.

Qualys Vulnerability Integration Übersichtsberichte

Name	Visuell	Beschreibung
Mit Qualys synchronisierte CIs	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente an, die für jedes CI aufgezeichnet wurden, von der höchsten bis zur niedrigsten.
Offene angreifbare Qualys-Elemente	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente an, die Schwachstellen zugeordnet sind (CVE-Datensätze), von den meisten bis zu den wenigsten.
Angreifbare Qualys-Elemente insgesamt	Balkendiagramm	Zeigt die Anzahl der ignorierten angreifbaren Elemente an, die innerhalb von 7 Tagen ablaufen sollen.
Angreifbare Elemente nach Priorität	Trenddiagramm	Zeigt die Anzahl der pro Woche aufgezeichneten Schwachstelleneinträge an.
QID-Verbreitung	Balkendiagramm	Zeigt die Anzahl der für jedes Modell aufgezeichneten angreifbaren Elemente an, von der höchsten zur niedrigsten.
Offene angreifbare Qualys-Elemente	Liste	Zeigt die Anzahl der für jeden Herausgeber aufgezeichneten angreifbaren Elemente an, von der höchsten zur niedrigsten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys Statusdiagramm der Integrationsausführung

Das Modul „Status Qualys der Integrationsausführung bietet eine grafische Ansicht des Status von Qualys Integrationsausführungen.

Um den Status von Integrationsausführungen anzuzeigen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

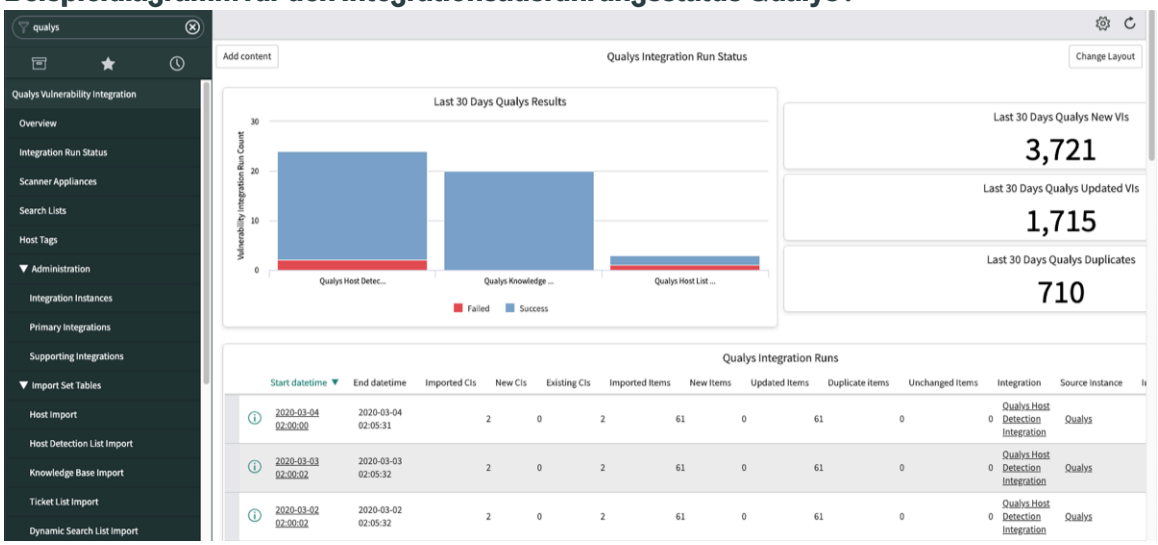
Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Zeigen Sie im Diagramm auf einen beliebigen Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Integrationsausführungsstatus Qualys zeigt den Ausführungsstatus der Schwachstellenintegration für die letzten 30 Tage an. Die von Qualys[qualys] aktualisierte VIs-Anzahl gibt die Anzahl der eindeutigen Erkennungen im selben Asset an. Das VI wird dann mit der neuen Erkennung aktualisiert.

Hinweis:
Die Anzahl der Ausführungen der Schwachstellen-Integrationen wird nur für die Integrationen angezeigt, die auf den Status „Aktiv“ festgelegt sind. Navigieren zu **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen** und legen Sie den Status auf aktiv fest.

Beispieldiagramm für den Integrationsausführungsstatus Qualys .



- Die Werte in der Spalte „Importierte Elemente“ stellen die Gesamtzahl der Datensätze dar, die aus einer Integrationsausführung erstellt werden.
- In der Spalte Neue Elemente wird die Anzahl der Datensätze angezeigt, die aus einer Integrationsausführung erstellt wurden.
- Die Spalte „Doppelte Elemente“ ist nicht mehr ausgefüllt. Unter Umständen möchten Sie diese Spalte aus der Anzeige entfernen.
- In der Spalte Aktualisierte Elemente wird angezeigt, wie oft Datensätze während einer Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eindeutigen Datensätze, die aktualisiert werden. Wenn beispielsweise ein Datensatz während der Integrationsausführung zweimal aktualisiert wird, wird er zweimal gezählt und als 2 aktualisierte Elemente angezeigt.

- Die Spalte „Unveränderte Elemente“ zeigt die während der Integrationsausführung gefundenen Datensätze an, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

Hinweis:
Die Integration wird für alle vier der folgenden Werte ohne Ergebnisse ausgeführt: **Neue CIs**, **Vorhandene CIs**, **Neue Elemente**und **Aktualisierte Elemente** werden aus der Liste **der Qualys-Integrationsausführungen** herausgefiltert.

Qualys Diagrammberichte zum Status der Integrationsausführung

Name	Beschreibung
Ergebnisse der letzten 30 Tage Qualys .	Die Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. In einer Balkenvisualisierung ausführen.
Letzte 30 Tage Qualys Neue AEs	Anzahl der neuen Datensätze, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Aktualisierte VIs der letzten 30 Tage Qualys	Die Anzahl der aktualisierten Datensätze, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Letzte 30 Tage Qualys Duplikate	Die Anzahl der doppelten Datensätze, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Qualys Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`. Während die Integration ausgeführt wird, ändert sich möglicherweise die Anzahl der Erkennungen oder Ergebnisse. In diesem Bericht wird die Anzahl der Erkennungen in der Spalte „Anzahl bis Datum“ in der Instanz nach Abschluss der Integrationsausführung angezeigt.
Letzte 30 Tage Qualys Angreifbares Element – Erfassungsleistungsmetriken	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage.
Angreifbares Element – Erfassungsleistungsdurchsatz der letzten 30 Tage Qualys .	Täglicher Durchsatz bei der Erfassung von angreifbaren Elementen, gemessen für die Integration der Qualys Hosterkennung in den letzten 30 Tagen.

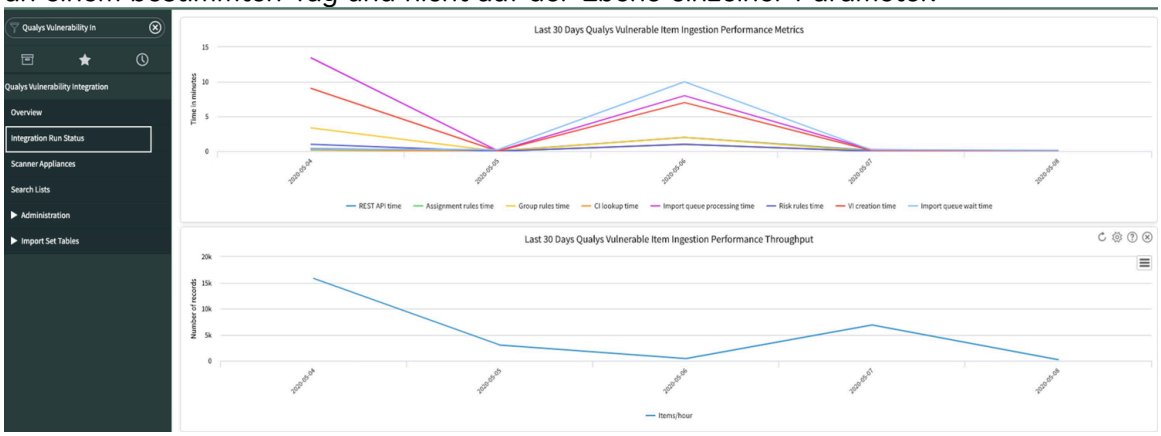
Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei Diagramme vergleichen die Leistungsmetriken:

- Qualys Erfassungsleistungsmetriken für angreifbare Elemente: Vergleichen Sie tägliche Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit und andere Statistiken für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbare Elemente für die letzten 30 Tage, um die Ursache für Leistungsabweichungen zu ermitteln. Die Leistung wird basierend auf der für jede Aktivität benötigten Zeit berechnet. Diese Parameter werden auf Integrationsausführungsebene berechnet und zugeordnet. Jeder Parameter ist zur einfachen Identifizierung farbcodiert.

- Qualys Leistungsdurchsatz bei der Erfassung von angreifbaren Elementen: Vergleichen Sie den täglichen Durchsatz bei der Erfassung von angreifbaren Elementen für die Qualys Host-Erkennungsintegration. Der Durchsatz wird in Elementen pro Stunde gemessen. Dieser Bericht zeigt die Gesamtleistung an einem bestimmten Tag und nicht auf der Ebene einzelner Parameter.



Qualys-Datentransformation

Die aus Qualys abgerufenen Daten werden über eine Reihe von Datenquellen und Transformationen verarbeitet.

Die meisten Transformationen für Qualys Vulnerability Integration werden mithilfe von Transformationsskripts durchgeführt. Diese Skripts sind für interne Verwendung vorgesehen. Das Löschen wird nicht empfohlen. Änderungen erfordern Kenntnisse in den Bereichen Codierung oder fortgeschrittene ServiceNow oder Qualys Vulnerability Integration. Die verbleibenden Zuordnungen sind in diesem Abschnitt aufgeführt und verwenden Feldzuordnungen.

Hinweis:
Während der Installation werden im Modul „Normalisierte Schweregradzuordnung“ Vulnerability Response normalisierte Schweregradzuordnungen installiert, die importierte Qualys Cloud Platform -Schweregrade in Standard-Schweregrade ServiceNow umwandeln. Weitere Informationen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung.

Import dynamische Suchliste

Die Transformationszuordnung für dynamische Qualys-Suchlisten wird zum Transformieren und Importieren dynamischer Qualys-Suchlisten verwendet. Änderungen an dieser Transformation ändern, wie dynamische Suchlisten verarbeitet und in das System eingefügt werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Listenimport für dynamische Suche**.

Die Tabelle zeigt die Felder, die gerade transformiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys – dynamische Suchliste – Felder der Transformationszuordnung

Quellfeld	Zielfeld	Beschreibung
u_id	id	Wird als Bezeichner für die dynamische Qualys-Suchliste verwendet
[Skript]	list_type	Der Typ der Suchliste. „Dynamisch“ ist der Standardwert für die Transformation „Dynamische Suchliste“.
u_title	Titel	Der Name in Qualys für diese Suchliste.

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

Timing und Zweck des Skripts für die dynamische Suchliste der Qualys-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck des Skripts
onAfter (nachdem ein Importsatz die Transformation abgeschlossen hat).	Erstellt die Beziehungen zwischen Suchlisten und den zugehörigen Schwachstellen. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Import statische Suchliste

Die Transformationszuordnung für Qualys-Listen für statische Suche wird zum Transformieren und Importieren von Qualys-Listen für die statische Suche verwendet. Änderungen an dieser Transformation ändern, wie statische Suchlisten verarbeitet und in das System eingefügt werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Import statische Suchliste**.

Die Tabelle zeigt die Felder, die gerade transformiert werden.

Qualys-Transformationszuordnungsfelder für statische Suchliste

Quellfeld	Zielfeld	Beschreibung
u_id	id	Wird als Bezeichner für die statische Qualys-Suchliste verwendet.
u_title	Titel	Der Name in Qualys für diese Suchliste.
[Skript]	list_type	Der Typ der Suchliste. „Statisch“ ist der Standard für die Transformation der statischen Suchliste.

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Timing und Zweck des Skripts für die Qualys-Transformationszuordnung für statische Suchlisten

Wenn das Skript ausgeführt wird	Zweck des Skripts
onAfter (nachdem ein Importsatz die Transformation abgeschlossen hat).	Erstellt die Beziehungen zwischen Suchlisten und den zugehörigen Schwachstellen. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Assetgruppenimport

Die Qualys-Asset-Gruppen-Appliance-Transformationszuordnung wird verwendet, um Qualys-Asset-Gruppendaten zu transformieren, um Scanner-Appliance-Datensätze zu erstellen. Änderungen an dieser Transformation ändern die Art und Weise, wie Scanner-Geräte erstellt und geändert werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Assetgruppenimport**.

Die Tabelle zeigt die Felder, die gerade transformiert werden.

Transformationszuordnungsfelder für Qualys-Asset-Gruppen

Quellfeld	Zielfeld	Beschreibung
u_id	id	Wird als Bezeichner für die Qualys-Asset-Gruppe verwendet.
[Skript]	Manuell	Geskripteter Wert, um zu bestimmen, wie der Zieldatensatz erstellt wurde. Wenn es durch Transformationen erstellt wird, ist dieses Feld immer „falsch“.
[Skript]	ips	Die IP-Adressen, die der zu transformierenden Assetgruppe zugeordnet sind.
u_default_appliance_id	Appliance_id	Der Qualys-Gerätebezeichner für das Standardgerät in dieser Asset-Gruppe.
u_title	asset_group_name	Der Name der Qualys-Asset-Gruppe.

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

Timing und Zweck des Skripts für die Transformationszuordnung für Qualys-Asset-Gruppen

Wenn das Skript ausgeführt wird	Zweck des Skripts
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Das Skript, das die Importe von Asset-Gruppen auf Asset-Gruppen mit einer Standard-Appliance und einem Satz zugeordneter IP-Adressen beschränkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Timing und Zweck des Skripts für die Transformationszuordnung für Qualys-Asset-Gruppen (Fortsetzung)

Wenn das Skript ausgeführt wird	Zweck des Skripts
	Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Appliance-Import

Die Qualys-Appliance-Transformationszuordnung wird verwendet, um Qualys-Appliance-Daten in Appliance-Datensätze zu transformieren. Dies wird verwendet, um die Gerätedatensätze zu aktualisieren, die ursprünglich aus dem Asset-Gruppenimport erstellt wurden. Änderungen an dieser Transformation ändern, wie Appliance-Datensätze mit Appliance-Details aktualisiert werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Appliance-Import**.

Die Tabelle zeigt die Felder, die gerade transformiert werden.

Qualys-Appliance-Transformationszuordnungsfelder

Quellfeld	Zielfeld	Beschreibung
u_name	device_name	Der Name der Qualys-Scanner-Appliance.
u_status	Appliance_status	Der zuletzt gemeldete Status der Qualys-Scanner-Appliance.
u_id	Appliance_id	Der Qualys-Gerätebezeichner.

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

Timing und Zweck des Skripts für die Qualys-Appliance-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck des Skripts
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Wird verwendet, um Namen und Status von Geräten für die angegebene ID zu aktualisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Qualys-REST-Nachrichten

Qualys-REST-Nachrichten werden verwendet, um Aufrufe an die Qualys-API zu tätigen.

Ab Version 12.9.2 von Qualyskönnen Sie zwischen Standardauthentifizierung und OAuth wählen. Die Qualys-Cloud-Authentifizierungsmethode des Instanzparameters ist für Standardauthentifizierung vorkonfiguriert. Wenn Sie OAuth verwenden möchten, müssen Sie den Parameter der Integrationsinstanz ändern und dann die REST-Nachricht direkt für OAuth einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachricht zur Qualys-Host-Erkennung

Die REST-Nachricht zur Qualys-Host-Erkennung führt den ersten Aufruf an die Hostlisten-Erkennungs-API für die Qualys-Host-Erkennungsintegration durch.

REST-Nachrichtenparameter für die Qualys-Host-Erkennung

Parametername	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Änderungen sind nicht erforderlich.
output_format	XML	Legt das Format des von Qualys zurückgegebenen Berichts fest. Die verschiedenen Skripts und Transformationen verwenden XML, daher werden Änderungen des Werts nicht empfohlen.
discovery_processed_after	${lastScanDate}	Zeigt nur Erkennungen an, deren Erkennungsstatus sich nach einem bestimmten Datum und einer bestimmten Uhrzeit geändert hat. Bei Erkennungen, die sich nie geändert haben, wird das Datum auf das Datum der letzten Erkennung angewendet.
„truncation_limit“	500	Die Anzahl der Hosts, von denen Daten gemäß der Anforderung abgerufen werden sollen. Dieser Parameter wird für Paginierungszwecke verwendet. Der Standardwert ist 500, es können jedoch größere oder kleinere Werte verwendet werden. Legen Sie keinen Wert unter 100 fest, da dies die Systemlast erheblich erhöht. Kleinere Werte erfordern mehr Aufrufe an die Qualys-API, und größere Werte führen zu größeren Ergebnissätzen für die Verarbeitung und potenziellen Zeitüberschreitungen beim Datenabruf/der Verarbeitung.
status	Neu, Repariert, Aktiv, Erneut geöffnet	Erkennungsstatus, die aus Qualys abgerufen werden sollen. Standardmäßig werden alle Status abgerufen. Bei großen Datenabrufen (häufig dem ersten Abruf von Daten) kann es nützlich sein, Feste Status aus dieser Liste auszuschließen. Es ist wichtig, den Status „Behoben“ anzugeben, wenn Sie bereits im System vorhandene Schwachstellen aktualisieren.

REST-Nachricht zur Paginierung der Qualys-Host-Erkennung

Die REST-Nachricht „Host-Erkennungspaginierung“ verarbeitet Paginierungsanforderungen an die Host-Erkennungs-API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Erkennung des primären Hosts ausgeführt wird und die Qualys-API eine URL zum Abrufen der nächsten Seite mit Daten bereitstellt, ruft diese REST-Nachricht diese zusätzlichen Daten ab. Diese Daten werden vom Paginierungshandler der Hosterkennung verwendet.

Host-Erkennungspaginierung – REST ist eine spezialisierte REST-Nachricht und darf nicht geändert werden.

REST-Nachricht für Qualys-Knowledge Base (Auffüllung).

Die REST-Nachricht Qualys Knowledge Base (Auffüllen) ruft Knowledge Base-Daten von Qualys basierend auf dem Zeitstempel der letzten Änderung der Schwachstellendaten für die Qualys Knowledge Base-Integration ab.

Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys zum Abrufen von Knowledge Base-Informationen aus.

Die folgende Tabelle zeigt die Anforderungsparameter, die gesendet werden.

REST-Nachrichtenparameter für die Qualys-Knowledge-Base-Auffüllung (Auffüllung).

Parameter	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Changes werden nicht empfohlen.
details	Alle	Gibt die Detailebene an, die für abgerufene Schwachstellen angezeigt wird. Sicher, nach Bedarf zu ändern.
ids	${QIDs}	Gibt an, welche QIDs von Qualys abgerufen werden sollen. Im Code referenziert. Änderungen werden nicht empfohlen.

REST-Nachricht zur Qualys-Knowledge Base (datumsbasiert).

Die REST-Nachricht „Qualys Knowledge Base (datumsbasiert)“ wird verwendet, um Qualys-Knowledge Base-Daten basierend auf dem Zeitstempel der letzten Änderung der Schwachstellendaten abzurufen. Diese Nachricht wird von der Qualys Knowledge Base-Integration verwendet.

Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys zum Abrufen von Knowledge Base-Informationen aus.

Die folgende Tabelle zeigt die Anforderungsparameter, die gesendet werden.

REST-Nachrichtenparameter der Qualys-Knowledge Base (datumsbasiert).

Quellfeld	Zielfeld	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Changes werden nicht empfohlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachrichtenparameter der Qualys-Knowledge Base (datumsbasiert). (Fortsetzung)

Quellfeld	Zielfeld	Beschreibung
details	Alle	Gibt die Detailebene an, die für abgerufene Schwachstellen angezeigt wird. Sicher, nach Bedarf zu ändern.
last_modified_after	${dateStart}	Gibt an, wann mit dem Abrufen von Verlaufsdaten begonnen werden soll. Wird vom Code verwendet, um sowohl die Startzeit zu bestimmen als auch die Paginierung zu unterstützen Änderungen oder Entfernungen werden nicht empfohlen.
last_modifiedbefore	${dateEnd}	Gibt an, wann das Abrufen von Verlaufsdaten beendet werden soll. Wird vom Code verwendet, um sowohl die Endzeit zu bestimmen als auch die Paginierung zu unterstützen Änderungen oder Entfernungen werden nicht empfohlen.

REST-Nachricht für Qualys-Tickets

Die REST-Nachricht für Qualys-Tickets ruft Qualys-Ticketinformationen für die Qualys-Ticket-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen zum Abrufen von Ticketinformationen an Qualys aus.

Die Tabelle zeigt die Anforderungsparameter, die gesendet werden.

REST-Nachrichtenparameter für Qualys-Tickets

Parametername	Wert	Beschreibung
modifiziert_seit_Datum/Uhrzeit	${lastRunDatetime}	Gibt das Datum der letzten Ausführung der Integration und das Datum an, nach dem Daten abgerufen werden sollen. Von Code verwendet. Changes werden nicht empfohlen.
since_ticket_number	${lastTicketNumber}	Gibt an, welches Ticket zuletzt von Qualys abgerufen wurde. Wird für die Paginierung verwendet. Changes werden nicht empfohlen.
show_vuln_details	1	Gibt an, ob die Schwachstellendetails abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 Vulnerability-Integration verstehen

ServiceNow® Rapid7 Vulnerability-Integration verwendet Daten, die aus dem Data Warehouse Rapid7 oder den Rapid7 InsightVM -Produkten importiert werden, um Ihnen zu helfen, die Auswirkung und Priorität potenziell schädlicher Bedrohungen zu bestimmen.

Rapid7 Nexpose -Sensoren erfassen Daten und senden sie automatisch an das Rapid7 Data Warehouse (lokal) oder Rapid7 InsightVM (cloudbasiert), welche die Informationen kontinuierlich analysieren und korrelieren. Die Integration mit ServiceNow® Vulnerability Response ermöglicht die Zuordnung von Schwachstellen zu CIs und Services. Rapid7 Vulnerability-Integration ergänzt die Schwachstellendaten in Ihrer Instanz.

Rapid7 -Integrationen sind Einstiegspunkte, die mit dem Rapid7 Data Warehouse oder den Produkten Rapid7 InsightVM von interagieren und als geplante Aufgaben aufgerufen werden. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren. Die geplanten Aufgaben werden automatisch und in der angegebenen Reihenfolge ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen.

Hinweis:

Wenn Sie das Data Warehouse Rapid7 und Rapid7 InsightVM als Quellen für Ihre Daten verwenden, laufen Sie Gefahr, dass doppelte Schwachstellen-Datensätze entstehen.

Hinweis:
Bei der Migration vom Integrationstyp **„Data Warehouse“** zum Typ **„Insight“** können Sie Ihre vorhandenen Data Warehouse-Datensätze deduplizieren. Weitere Informationen finden Sie unter Deduplizieren Sie Data Warehouse-Datensätze Rapid7 Vulnerability-Integration ..

Wenn Sie über mehrere Bereitstellungen der Schwachstellen-Integration Rapid7 InsightVM verfügen, können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die von mehreren Drittanbieterbereitstellungen und ihren Schwachstellen identifiziert wurden, werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scan-Prozesse zwischen den mehreren Bereitstellungen überschneiden. Daten, die aus den einzelnen Bereitstellungen stammen, werden identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

Hinweis:
Sie können die ursprüngliche Schwachstellenintegration nicht löschen, aber deaktivieren. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Release-Version für Yokohama	Release-Hinweise
Rapid7 Vulnerability-Integration v13.6, 13.7	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen

Rapid7 Aufgaben zur Schwachstellenintegration in betreffen die folgenden Rollen.

- sn_vul_r7.admin: Kann Datensätze lesen, schreiben und löschen.
- sn_vul_r7.user: Kann Datensätze lesen und schreiben.
- sn_vul_r7.read: Kann Datensätze lesen.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Rapid7 Vulnerability-Integration-Integrationen

Um Rapid7 Vulnerability-Integrationanzuzeigen, navigieren Sie zu **Rapid7** > **Administration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

Rapid7 Data Warehouse-Integrationen

Integration	Beschreibung
Rapid7 Vulnerability-Integration	Ruft Schwachstellendaten von Rapid7 Nexpose ab und verarbeitet sie in Ihrer Instanz.
Rapid7 Integration mit Asset-Listen	Ruft einmal pro Woche Scan-Daten aus dem Data Warehouse Rapid7 Nexpose ab und speichert sie im Modul „Erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden, anhand des Datums **des letzten Scans**. Zeigen Sie die Zeit **des letzten Scans** in der Liste „Erkannte Elemente“ in Vulnerability Responsean.
Rapid7 Kategorieintegration	Ruft Kategorieinformationen von Rapid7 Nexposeab. Kategorien bieten allgemeine Klassifizierungen für Schwachstellen.
Rapid7 Exploit-Integration	Ruft Informationen zum Exploit von Rapid7 Nexposeab.
Rapid7 Integration des Malware-Kits	Ruft Informationen zum Malware-Kit von Rapid7 Nexposeab.
Rapid7 Referenzintegration	Ruft Verweise auf externe regulatorische Dokumente wie CVEs oder lieferantenspezifische Schwachstellenreferenzen ab.
Rapid7 Lösungsintegration	Ruft Lösungsdaten von Rapid7 Nexposeab und stellt empfohlene Lösungen für bestimmte Schwachstellen bereit.
Rapid7 Ersatzlösungsintegration	Ruft Informationen darüber ab, welche Lösungen durch andere Lösungen ersetzt werden.
Rapid7 Erforderliche Lösungsintegration	Ruft Informationen zu den Lösungen ab, die Voraussetzungen für andere Lösungen sind. Wenn diese Integration ausgeführt wird, ruft sie die Zuordnung von Lösungen und erforderlichen Lösungen aus dem Data Warehouse Rapid7 ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 Data Warehouse-Integrationen (Fortsetzung)

Integration	Beschreibung
	Hinweis: Diese Integration funktioniert nur, wenn das Plugin Vulnerability Solution Management aktiviert ist.
Rapid7 Integration der Schwachstellenlösungszuordnung	Ruft die Zuordnung ab, um Lösungen mit Schwachstellen zu verknüpfen.
Rapid7 Integration angreifbarer Elemente	Ruft Daten zu angreifbaren Elementen von Rapid7 Nexpose ab und verarbeitet sie in Ihrer Instanz. Die Ausgaben dieser Integration sind angreifbare Elemente.
Rapid7 Integration zur Lösung von angreifbaren Elementen	Ruft Informationen darüber ab, welche angreifbaren Elemente in Rapid7 Nexpose als geschlossen markiert sind, und schließt die entsprechenden angreifbaren Elemente in Vulnerability Response.
Rapid7 Site Integration	Ruft Site-Daten von Rapid7 Nexposeab. Eine Site ist eine Sammlung von Assets, die geprüft werden sollen.
Rapid7 Integration mit Asset-Listen	Ruft Host-Tags und Scan-Daten einmal pro Woche aus dem Data Warehouse Rapid7 ab und speichert sie im Modul „Erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden, anhand des Datums **des letzten Scans**. Zeit des **letzten Scans** in der Liste „Erkannte Elemente“ in Vulnerability Responseanzeigen
Rapid7 Comprehensive Vulnerable Item Integration	Importiert alle Rapid7-Erkennungen für alle Configuration Items, die seit der letzten erfolgreichen Integrationsausführung gescannt wurden. Basierend auf den aktuellen importierten Daten werden angreifbare Elemente, die bei Scans nicht kürzlich gefunden wurden, automatisch in den Status „Geschlossen“ versetzt, wenn das Modul „Veraltete angreifbare Elemente automatisch schließen“ aktiviert ist.

Rapid7 InsightVM-Integrationen

Integration	Beschreibung
Rapid7 Integration angreifbarer Elemente – API	Ruft Daten zu angreifbaren Elementen von Rapid7 InsightVM ab und verarbeitet sie in Ihrer -Instanz.
Rapid7 Vulnerability-Integration — API	Ruft Referenz-, Kategorie-, Exploit-, Malware-Kit- und Schwachstellendaten von Rapid7 InsightVM ab und verarbeitet sie in Ihrer -Instanz.
Rapid7 Asset-Listenintegration – API	Ruft Host-Tags und Scan-Daten einmal pro Woche von Rapid7 InsightVM ab und speichert sie im Modul Erkannte Elemente in Ihrer -Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden, anhand des Datums **des letzten Scans**. Zeigen Sie die Zeit **des letzten Scans** in der Liste „Erkannte Elemente“ in Vulnerability Responsean.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 InsightVM-Integrationen (Fortsetzung)

Integration	Beschreibung
Rapid7 Comprehensive Vulnerable Item Integration – API	Importiert alle Rapid7-Erkennungen für alle Configuration Items, die seit der letzten erfolgreichen Integrationsausführung gescannt wurden. Basierend auf den aktuellen importierten Daten werden angreifbare Elemente, die bei Scans nicht kürzlich gefunden wurden, automatisch in den Status „Geschlossen“ versetzt, wenn das Modul „Veraltete angreifbare Elemente automatisch schließen“ aktiviert ist.
Rapid7 Site Integration	Ruft Site-Daten aus dem Produkt Rapid7 InsightVM ab. Diese Integration wird wöchentlich um 00:00:00 Uhr ausgeführt.

Während des Imports werden noch nicht vorhandene CVE-Datensätze als NVD-Datensätze erstellt und standardmäßig in Einträgen von Drittparteien für Rapid7 referenziert. Die Vorlagenintegration für Rapid7 kann nicht gelöscht werden. Deaktivieren Sie sie stattdessen.

Der Service Graph Connector für Rapid7

Ab Version 2.0 ist der Service Graph Connector für Rapid7 über den ServiceNow® Storeverfügbar. Weitere Informationen finden Sie unter Service Graph Connector for Rapid7 .

CI-Suchregeln

CI-Suchregeln bestimmen, wie das Feld **Konfigurationselement** in einem Datensatz für ein angreifbares Element ausgefüllt wird.

Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

Informationen zum Erstellen oder Bearbeiten von Suchregeln finden Sie unter Erstellt eine Vulnerability Response-CI-Suchregel.

Hinweis:
Einmal entfernte Regeln können nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus Rapid7 Integrationen für angreifbare Elemente (Data Warehouse oder InsightVM-API) und Asset-Listenintegrationen Rapid7 – API erkannt wurden. Die Rapid7 Asset-Listenintegration – API importiert alle Rapid7-Assets, die seit der letzten Integrationsausführung auf Schwachstellen gescannt wurden. Die Rapid7 Data Warehouse-Asset-Listenintegration ist enthalten.

Hinweis:
Der Standardfilter für diese Liste ist auf **Nicht abgeglichen**festgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „Erkannte Elemente“ finden Sie unter Erkannte Elemente in Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Host-Tags

Host-Tags werden als Teil der Rapid7 Asset-Listenintegration – API-Integration für Rapid7 InsightVMimportiert. Sie werden hauptsächlich zum Filtern in Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben in Rapid7 InsightVMverwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

Host-Tags

Hinweis:
Die Rapid7 Asset-Listenintegration – API-Integration muss vor der Erstellung von Regeln für Zuweisungs- oder Korrekturaufgaben in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein **San Diego** -Tag erstellt wird, kann kein **SAN DIEGO** -Tag in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das zuerst importierte Tag gewinnen.
- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft **sn_vul.import_host_tags**gesteuert. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Durch das Deaktivieren von Tags werden sie für alle Instanzen deaktiviert.

Sites

Eine Site ist eine Sammlung von Assets, die gescannt werden sollen. Eine Site besteht aus Ziel-Assets, einer Scan-Vorlage, einer oder mehreren Scan Engines und anderen scanbezogenen Einstellungen wie Zeitplänen oder Warnungen. Sites werden von den Anwendungen Rapid7 verwaltet.

Rapid7 Vulnerability-Integration Mithilfe der Site-Filterung während der Konfiguration können Sie Assets während des Imports nach Site kategorisieren und anfordern. Weitere Informationen zum Filtern von Importen finden Sie unter Filtern nach Rapid7 Sites.

Das Data Warehouse Rapid7 und die Sites-Integrationen Rapid7 InsightVM importieren Sites als wöchentliche geplante Aufgabe.

Um die importierten Websites in einer Liste anzuzeigen, navigieren Sie zu **Rapid7** > **Sites**.

Öffnen Sie gelöste angreifbare Elemente, die nicht durch Scans geschlossen wurden

Angreifbare Elemente, die in Ihrer Instanz Now Platform auf „Gelöst“ festgelegt, aber von den nachfolgenden Integrationsausführungen nicht in den Status „Geschlossen/Behoben“ versetzt werden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Für Rapid7 -Erkennungen ist auf der Rapid7-Konfigurationsseite in Ihrer -Instanz jetzt eine Option verfügbar, um gelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden AEs, die auf „Gelöst“ gesetzt werden, aber dann nicht durch nachfolgende Scans in „Geschlossen/Behoben“ geändert werden, nach der von Ihnen eingegebenen Anzahl von Tagen wieder in den Status „Offen“ geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs mit der Engine Identification and Reconciliation (IRE) erstellen

Sie können die Engine „Identification and Reconciliation“ (Identifizierung und Abgleich) verwenden, um neue CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der aus einem Drittanbieterscanner importiert wurde. Aktivieren Sie das Plugin „CMDB CI Class Models“ (CMDB-CI-Klassenmodelle), um CIs mit den neuen Klassen zu erstellen. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt. Weitere Informationen zum Konfigurieren der Kategorisierung von nicht abgeglichenen Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets aktualisieren.

Scannen Sie angreifbare Elemente erneut

Initiieren Sie erneute Scans auf der Plattform Rapid7, um sicherzustellen, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Weitere Informationen finden Sie unter Initiieren Sie den erneuten Scan für die Rapid7 Vulnerability Integration.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Rapid7 Lösungsmanagement

Wenn Sie das Plugin Vulnerability Solution Management aktiviert haben, werden die Lösungen Rapid7 für das Data Warehouse Rapid7 und Rapid7 InsightVM in die Tabelle „Schwachstellenlösungen“ [sn_vul_solution] eingetragen. Wenn Sie jedoch das Plugin Vulnerability Solution Management nicht aktiviert haben, funktioniert Rapid7 Vulnerability-Integration unverändert und importiert die Lösungen in die anwenderdefinierte Tabelle [sn_vul_r7_solution]. Weitere Informationen finden Sie unter Rapid7 Lösungsmanagement.

Vorbereitung auf das Rapid7 Vulnerability-Integration

Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Rapid7 Vulnerability-Integration setzt voraus, dass Sie mit Rapid7 Data Warehouse- oder Rapid7 InsightVM -Produktscans in Ihrer Umgebung vertraut sind und diese ausführen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Rapid7 -Scanner sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die Schaltfläche **Erneut scannen** nicht verfügbar.

Bevor Sie die Anwendung Rapid7 Vulnerability-Integration von ServiceNow® Store herunterladen und in Ihrer -Instanz installieren, lesen Sie die folgenden Informationen zu Integrationstypen und Setup-Informationen:

Rapid7 Vulnerability-Integration enthält zwei Arten von Integrationen, die in ServiceNow® Storeverfügbar sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rapid7 InsightVM
- Rapid7 Data Warehouse

Der Data Warehouse-Typ Rapid7 :

- Erfordert die URL des Data Warehouse-Servers Rapid7 und Ihre Anmeldeinformationen zur Authentifizierung
- Erfordert einen MID-Server
- Verwendet einen PostgresSQL-Treiber, um Abfragen im Data Warehouse auszuführen
- Unterstützt nicht mehrere Instanzen

Der Integrationstyp Rapid7 InsightVM :

- Ist cloudbasiert und verwendet eine REST API. Diese Integration erfordert einen API-Schlüssel aus Ihrem Rapid7 Insight-Konto.
- Unterstützt mehrere Instanzen.

Weitere Informationen zu den Setup-Anforderungen für diese Integrationstypen finden Sie unter Richten Sie die Data Warehouse-Integration für Rapid7 ein (Data Warehouse) und Richten Sie für die Rapid7 InsightVM -Integration ein.

Richten Sie die Data Warehouse-Integration für Rapid7 ein

Die Rapid7 Data Warehouse-Integration ist einer der Integrationstypen, die in Rapid7 Vulnerability-Integration Rapid7 Vulnerability-Integrationenthalten sind.

Vorbereitungen
Führen Sie vor dem Ausführen der Data Warehouse-Integration Rapid7 die folgenden Setupaufgaben aus:

- Rufen Sie das Data Warehouse-Add-on Rapid7 ab. Auf der Rapid7 Website und in der Dokumentation finden Sie Informationen zum Erwerben und Installieren dieses Add-ons.
- Ruft den aktuellen PostgresSQL-Treiber ab. Wechseln Sie zu https://jdbc.postgresql.org/ , und laden Sie den neuesten Treiber herunter.
- Ein MID-Server zum Ausführen von Abfragen an das Data Warehouse. Weitere Informationen zum Einrichten eines MID -Servers finden Sie unter MID-Server .

  Notieren Sie sich den Data Warehouse-Namen. Der Data Warehouse-Integrationstyp Rapid7 unterstützt nur eigenständige MID-Server. MID-Server in Clustern werden nicht unterstützt.

- Rufen Sie die URL des Data Warehouse-Servers Rapid7 und die Authentifizierungsanmeldeinformationen ab, und machen Sie Zugriff darauf.

Erforderliche Rolle: Der Systemadministrator [admin] lädt die App herunter und installiert sie. sn_vul.vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Rapid7 Vulnerability-Integration installieren möchten.
2. Installieren Sie die PostgreSQL-JAR-Datei, die Sie in den zuvor aufgeführten Setupaufgaben heruntergeladen haben.
   a. Navigieren Sie in Ihrer Instanz von Now Platform zu **Alle** > **MID-Server** > **JAR-Dateien**.
   b. Klicken Sie auf **Neu**.
   c. Geben Sie den Namen des PostgresSQL-Treibers ein, den Sie zuvor heruntergeladen haben.

      Geben Sie optional die Informationen zu **Version**, **Quelle**und **Beschreibung** ein. Lassen Sie das Kontrollkästchen **Aktiv** aktiviert.

   d. Hängen Sie die heruntergeladene JAR-Datei mithilfe des Büroklammer-Symbols im Header an.
   e. Klicken Sie auf **Absenden**.

Sie haben das Setup für die Data Warehouse-Integration Rapid7 abgeschlossen. Wenn Sie die Anforderungen für die Rapid7 InsightVM -Integration vor der Installation von Rapid7 Vulnerability-Integrationnicht überprüft haben, lesen Sie Richten Sie für die Rapid7 InsightVM -Integration ein und Vorbereitung auf das Rapid7 Vulnerability-Integration.

Schritte zum Abrufen von Berechtigungen, Herunterladen und Installieren von Rapid7 Vulnerability-Integrationfinden Sie unter Rapid7 Vulnerability-Integration installieren.

Richten Sie für die Rapid7 InsightVM -Integration ein

Die Rapid7 InsightVM Integration ist einer der Integrationstypen, die in Rapid7 Vulnerability-Integration Rapid7 Vulnerability-Integrationenthalten sind.

Vorbereitungen

Bevor Sie die -Integration Rapid7 InsightVM ausführen, führen Sie die folgenden Setupaufgaben aus.

Erforderliche Rolle: Der Systemadministrator [admin] lädt die App herunter und installiert sie. sn_vul.vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Prozedur

1. Halten Sie für den Integrationstyp Rapid7 InsightVM Ihre Region und Ihren API-Schlüssel bereit.
   Wenden Sie sich an Rapid7, um die entsprechende Region und den API-Schlüssel zu erhalten.
   Sie haben das Setup für die Rapid7 InsightVM -Integration abgeschlossen. Wenn Sie die Anforderungen für die Data Warehouse-Integration Rapid7 nicht überprüft haben, lesen Sie vor der Installation von Rapid7 Vulnerability-Integrationdie Informationen unter Richten Sie die Data Warehouse-Integration für Rapid7 ein und Vorbereitung auf das Rapid7 Vulnerability-Integration.
2. Schritte zum Abrufen von Berechtigungen, Herunterladen und Installieren von Rapid7 Vulnerability-Integrationfinden Sie unter Rapid7 Vulnerability-Integration installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 Vulnerability-Integration installieren

Nachdem Sie die Einrichtungsschritte für die Integration abgeschlossen haben, damit sie ordnungsgemäß in Vulnerability Responseintegriert wird, rufen Sie Berechtigungen ab, laden Sie die Anwendung herunter und installieren Sie sie in Ihrer Instanz Now Platform®.

Vorbereitungen
Erforderliche Rolle: „admin“ für Download und Installation, „sn_vuln.admin“ überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

1. Weitere Informationen zu den Integrationstypen und Setup-Anforderungen für Rapid7 Vulnerability-Integrationfinden Sie unter Vorbereitung auf das Rapid7 Vulnerability-Integration, Richten Sie die Data Warehouse-Integration für Rapid7 ein und Richten Sie für die Rapid7 InsightVM -Integration ein.
2. Führen Sie vor dem Herunterladen und der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.
3. Nachdem die Anwendung aktiviert wurde, führen Sie die unten aufgeführten Schritte aus, um Rapid7 Vulnerability-Integrationzu konfigurieren.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen Now Platform für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich. Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response. • Der Systemadministrator [admin] installiert die App. Wenn dies noch nicht geschehen ist, weist der Administrator die Rolle „Schwachstellen-Administrator“ [sn_vul.vulnerability_admin oder sn_vul.admin] zu. • Der Schwachstellenadministrator überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Die Administratorrolle Rapid7 wird geerbt, wenn Ihnen eine Administratorrolle in der Anwendung Vulnerability Response (VR) zugewiesen wird.
Validiert die Größe Ihrer Instanz basierend auf der Anzahl der angreifbaren Elemente, die importiert werden sollen.	Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.
Richten Sie die Filterung ein	Verwenden Sie Filter, um die Anzahl der Elemente für den ersten Import zu begrenzen und Ihre Bereitstellung zu stufen, indem Sie Filter in nachfolgenden Importen anpassen.
Schwachstellen-Rechner deaktivieren	Wenn Sie keine Schwachstellen-Rechner verwenden, Deaktivieren Sie den standardmäßigen Schwachstellen-Rechner, wenn er nicht verwendet wird, zusätzlich zu anderen, die Sie definiert haben. Sicherheitsrisiko-Rechner werden jedes Mal ausgeführt, wenn der Datensatz eines angreifbaren Elements erstellt oder aktualisiert wird, und können sich auf die Leistung des anfänglichen Imports auswirken.
Standardwert für „run-as“-Anwender beibehalten	Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.
Es werden Host-Tags verwendet	Wenn Sie Host-Tags in den Regeln für Zuweisungs- oder Korrekturaufgaben Vulnerability Response verwenden möchten, führen Sie die Integration der Rapid7-Asset-Liste aus, bevor Sie Regeln erstellen.
Deduplizieren Sie vorhandene Datensätze	Bei der Migration vom Integrationstyp **„Data Warehouse“** zum Typ **„Insight“** können Sie Ihre vorhandenen Data Warehouse-Datensätze deduplizieren. Weitere Informationen finden Sie unter Deduplizieren Sie Data Warehouse-Datensätze Rapid7 Vulnerability-Integration ..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie die Anwendung Rapid7 Vulnerability-Integration installieren möchten.
2. Navigieren Sie zu ServiceNow Store, und melden Sie sich an.
3. Suchen Sie in ServiceNow Storenach der Anwendung Rapid7 Vulnerability-Integration.

   Hinweis:
   In ServiceNow Storeheißt die Anwendung Rapid7 Integration for Security Operations. Diese Anwendung erfordert ein -Abonnement.

4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren Sie in Ihrer Instanz von Now Platform zu **Systemanwendungen** > **Alle Anwendungen** > **Alle**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Im Dialogfeld „Installieren“ wird Ihr Abhängigkeitsstatus angezeigt. Wenn Sie eine abhängige Anwendung benötigen, wird die benötigte Anwendung angezeigt. Befolgen Sie die Eingabeaufforderungen im Dialogfeld, um die Anwendung Rapid7 Vulnerability-Integration auf Ihrer Instanz von zu installieren.

    Hinweis:
    Der Schwachstellenadministrator kann jetzt die Konfiguration der Anwendung abschließen. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Rapid7 Vulnerability-Integration.

Konfigurieren Sie die Eigenschaften Rapid7 Vulnerability-Integration

Konfigurieren Sie Rapid7 Vulnerability-Integration, nachdem die Anwendung auf Ihrem Now Platform®installiert und aktiviert wurde.

Vorbereitungen

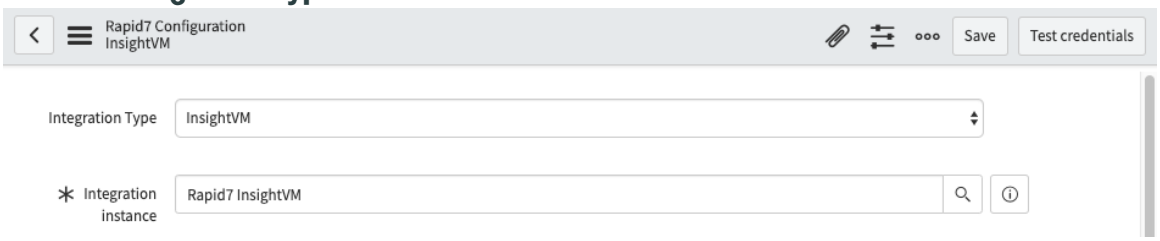
Erforderliche Rolle: Der -Administrator [admin] lädt die App herunter und installiert sie. sn_vul.vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Prozedur

1. Nachdem die Anwendung aktiviert (installiert) wurde, navigieren Sie zu **Rapid7 Vulnerability-Integration** > **Administration** > **Konfiguration**.
2. Wählen Sie einen Integrationstyp aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der Integrationstypen



3. Wählen Sie eine Integrationsinstanz aus.
   Die Standardintegrationsinstanz Rapid7 InsightVM ist standardmäßig ausgewählt. Wenn dies der gewünschte Integrationstyp ist, führen Sie die folgenden Schritte aus. Wenn Sie den Data Warehouse-Integrationstyp Rapid7 konfigurieren möchten, fahren Sie mit Schritt 4 fort.

   a. Füllen Sie bei ausgewählter Registerkarte **Integration Setup (Integrationssetup)** im angezeigten Formular die folgenden Felder aus:

Registerkarte „Integrationssetup“ für den Integrationstyp „InsightVM“.

Feld	Beschreibung
InsightVM-Region	Die Server-URL, die Sie von der Website Rapid7 erhalten haben.
API-Schlüssel	Der API-Schlüssel, den Sie von Ihrem Rapid7 Insight-Konto erworben haben.
Validierungsstatus	Schreibgeschützt: Status des Validierungsprozesses für Anmeldeinformationen.

   b. Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken. Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein.

   c. Klicken Sie nach einem erfolgreichen Test auf **Speichern**.

   d. Klicken Sie auf die Registerkarte **Importkonfiguration**.

   Füllen Sie die Felder im angezeigten Formular aus.

Registerkarte „Importkonfiguration“ für InsightVM

Feld	Beschreibung
CVSS-Mindestpunktzahl	Minimale CVSS-Punktzahl für angreifbare Elemente, die während des Imports zum Filtern angreifbarer Elemente verwendet wird.
Max. CVSS-Punktzahl	Maximale CVSS-Punktzahl für angreifbare Elemente, die während des Imports zum Filtern angreifbarer Elemente verwendet wird.
Standortfilter	Beschränkt die Daten auf die Sites Rapid7 InsightVM, die aus der Sites-Liste ausgewählt werden. Weitere Informationen finden Sie unter Filtern nach Rapid7 Sites. Sie können mehr als einen Standort auswählen. Der Standardwert (leer) ruft alle Sites ab. Um die Sites-Liste vorab auszufüllen, führen Sie vor dem Festlegen dieses Felds Rapid7 Site Integration – API aus. Informationen zur Verwendung von Standortfiltern finden Sie unter Filtern nach Rapid7 Sites.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
CVE-Eintrag automatisch erstellen	Die Systemeigenschaft zum Erstellen eines CVE-Eintrags ist standardmäßig aktiv (wahr). CVE-Platzhalter werden automatisch mit der Rapid7-Wissenserfassung erstellt, wenn die CVE-ID nicht vorhanden ist. Wenn diese Funktion deaktiviert werden soll, deaktivieren Sie die Eigenschaft [sn_vul_r7.create_cve_for_vulnerabilities] in der Liste „Systemeigenschaften“.
Gelöste nach Alter erneut öffnen	Wenn diese Option ausgewählt ist, werden angreifbare Elemente automatisch erneut geöffnet, wenn die Anzahl der Tage, die gelöst, aber nicht geschlossen wurden, mit dem im Feld **Gelöste erneut öffnen nach** übereinstimmen.

e. Klicken Sie auf **Speichern**.

Für mehrere Bereitstellungen des Integrationstyps Rapid7 InsightVM :

f. Öffnen Sie im Feld **Integrationsinstanz** das der Nachschlageliste, und wählen Sie eine vorhandene Integrationsinstanz aus, oder klicken Sie im Popup-Menü auf **Neu**.

g. Geben Sie unter **Neu**einen **Namen** für die Integrationsinstanz ein, und klicken Sie auf **Absenden**. Der Integrationstyp wird im Konfigurationsformular Rapid7 angezeigt.

Hinweis:
Sie können jede Integrationsinstanz außer der Standardinstanz löschen. Durch das Löschen einer Instanz wird Folgendes gelöscht (außer VIs):

- Integrationen
- Instanzparameter
- Integrationsausführungen
- Integrationsprozesse
- Instanzspalte im AE ist leer markiert

h. Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken.

i. Klicken Sie nach einem erfolgreichen Test auf **Speichern**.

4. Erweitern Sie im Feld Integrationstyp die Liste, und klicken Sie auf **Data Warehouse**.

a. Wählen Sie die Registerkarte **Integrationseinrichtung**.

Füllen Sie die Felder im angezeigten Formular aus.

Registerkarte „Integrationseinrichtung“ für den Integrationstyp „Data Warehouse“.

Feld	Beschreibung
JDBC-Anmeldeinformationsname	Name Ihrer Data Warehouse-Anmeldeinformationen.
Anwendername	Rapid7 Data Warehouse-Anwendername.
Passwort	Rapid7 Data Warehouse-Passwort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Validierungsstatus	Schreibgeschützt: Status des Validierungsprozesses für Anmeldeinformationen.
Validierungsdetail	Schreibgeschützt: Nur Data Warehouse. Zeigt zusätzliche Informationen zur Validierungsprüfung an, nachdem Sie mindestens einmal auf Anmeldeinformationen testen geklickt haben. Dies kann beim Debuggen Ihres Setups nützlich sein (z. B. um zu validieren, ob Ihr MID-Server falsch konfiguriert ist oder ob Sie einfach die falschen Anmeldeinformationen haben).
DNS/IP des Datenbankservers	DNS- oder IP-Adresse für Ihr Data Warehouse.
Datenbankanschluss	Für Ihre Data Warehouse-Integration zu verwendender Port.
Datenbankname	Name Ihres Data Warehouse.
Offset der Datenverzögerung (in Tagen)	Der Offsetfaktor für die Datenverzögerung berücksichtigt die Verzögerung zwischen den Echtzeitdaten im Scanner Rapid7 Nexpose und den Daten im Data Warehouse.
MID-Server	Zu verwendender MID-Server. Nur eigenständige MID-Server werden unterstützt. MID-Server in Clustern werden nicht unterstützt.
Timeout für MID-Server (Min.)	Anzahl der Minuten, die gewartet werden soll, bis der MID-Server antwortet, bevor eine Zeitüberschreitung bei der Integrationsausführung auftritt.

b. Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken.

c. Klicken Sie nach einem erfolgreichen Test auf **Speichern**.

d. Klicken Sie auf die Registerkarte **Importkonfiguration**.

Füllen Sie die Felder im angezeigten Formular aus.

Registerkarte „Importkonfiguration“ für Data Warehouse

Feld	Beschreibung
Vor v12.0: Kontrollkästchen CVE-Eintrag erstellen	Wenn diese Option aktiviert ist, werden Platzhalter für CVEs, die noch nicht vorhanden sind, als NVD-Datensätze erstellt und im Drittanbietereintrag für Rapid7 referenziert. Wenn diese Option deaktiviert ist, werden diese CVEs ignoriert.
CVSS-Mindestpunktzahl	Minimale CVSS-Punktzahl für angreifbare Elemente, die während des Imports zum Filtern angreifbarer Elemente verwendet wird.
Max. CVSS-Punktzahl	Maximale CVSS-Punktzahl für angreifbare Elemente, die während des Imports zum Filtern angreifbarer Elemente verwendet wird.
Standortfilter	Begrenzt die importierten Sites Integration-Daten auf die ausgewählten Sites. Sie können mehrere auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Da die Standardeinstellung darin besteht, Daten von allen Sites zu importieren, müssen Sie den Filter nicht verwenden, wenn Sie alle Sites möchten. Dadurch wird die Anforderung verlangsamt.
Gelöste nach Alter erneut öffnen	Wenn diese Option ausgewählt ist, werden angreifbare Elemente automatisch erneut geöffnet, wenn die Anzahl der Tage, die gelöst, aber nicht geschlossen wurden, mit dem im Feld **Gelöste erneut öffnen nach** übereinstimmen.

5. Klicken Sie auf **Speichern**.
6. **Wahlweise:** Wenn Sie in den Datensätzen Rapid7 Vulnerability Integration – API und Rapid7 Vulnerable Item Integration – API-Integrationsdatensätze ein Startdatum festlegen möchten, um während des ersten Imports aus dem Scan Rapid7 Verlaufsdaten abzurufen, führen Sie die folgenden Schritte aus.
   Sie können diese Daten für Veraltete Erkennungen in werden geschlossen Vulnerability Responseverwenden.

   a. Navigieren zu **Rapid7 Vulnerability-Integration** > **Administration** > **Integrationen**.
   Die Liste Rapid7 Integrationen wird angezeigt.

   b. Klicken Sie auf einen der Integrationsdatensätze, um ihn zu öffnen.

   (Optional) Klicken Sie oben im Formular auf den Link **hier**, um den Datensatz zu bearbeiten.

   Das Feld **„Import seit** Datum“ in den Rapid7 Integrationen ist standardmäßig leer, mit Ausnahme der Rapid7 Integration für Schwachstellen – API und der Integration von Rapid7 Vulnerable Item – API. Für diese Integrationen werden diese Felder auf 1998-12-31 oder 1999-01-01 festgelegt.

   Um während des ersten Imports Verlaufsdaten aus dem Scan Rapid7 abzurufen, legen Sie ein Startdatum in den entsprechenden Integrationsdatensätzen fest. Dieser Prozess funktioniert für jede Rapid7 -Integration mit den folgenden Ausnahmen:

   - Die Rapid7 Exploit- und Malware-Kit-Integrationen zeigen das Feld **„Importieren seit“** nicht an, da sie keine Delta-Updates durchführen und dieses Feld daher nicht verwenden.
   - Die Asset-Listenintegration Rapid7 ignoriert das Feld, da es alle Daten abrufen soll.
   - Für die erste Ausführung der Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API, wenn das Modul Veraltete angreifbare Elemente automatisch schließen aktiviert ist und das Feld **Importieren seit** leer gelassen wird.

     Wenn Sie die Funktion zum automatischen Schließen aktivieren, ist eine erfolgreiche Ausführung von Rapid7 Comprehensive Vulnerable Item Integration oder Rapid7 Comprehensive Vulnerable Item Integration – API erforderlich. Diese Integrationen sind standardmäßig deaktiviert.

     Wenn Sie die Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API aktivieren und das Feld **Import seit** auf der Konfigurationsseite der Integration leer lassen, wird der Wert im Feld **Tage her** des Formulars Veraltete angreifbare Elemente automatisch schließen auch für **Import seit** verwendet Datum der ersten Integrationsausführung. Der Standardwert für Veraltete angreifbare Elemente automatisch schließen lautet (90 Tage).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn beispielsweise das Feld **vor Tagen** im Formular „Veraltete angreifbare Elemente automatisch schließen“ 90 lautet und das Feld **Importieren seit** auf der Rapid7 Comprehensive Vulnerable Item Integration – API-Konfigurationsseite leer ist, importiert die erste Integrationsausführung die Daten für die letzten 90 Tage.

Diese Beziehung zwischen den Feldern **Importieren seit** und **Tage her** gilt nur für die erste Integrationsausführung. Danach hat das Ändern des Felds **„Vor** “ im Formular „Veraltete angreifbare Elemente automatisch schließen“ keine Auswirkung auf das Feld **„Importieren seit** “ auf der Konfigurationsseite „Rapid7 Comprehensive Vulnerable Item Integration – API“. Das Feld wird in die Startzeit der ersten Ausführung geändert, sodass die nachfolgenden Integrationsausführungen nur die Delta-Informationen importieren

Das Feld **Importieren seit** kann bearbeitet werden, und Sie können für jede der Integrationen beliebige Werte eingeben.

7. Navigieren zu **Alle** > **sn_sec_int_impl.list** > **Rapid7 InsightVM**.

   a. Der Parameter der Integrationsinstanz **import_starttime_buffer_comprehensive** legt eine Pufferzeit von 24 Stunden vor der im Feld **Importieren seit** fest, sodass die Assets, die aus dieser Pufferzeit gescannt werden, während der Ausführung **von Rapid7 Comprehensive Vulnerable Item Integration – API-** Integration abgerufen werden.
   Sie können diese Pufferzeit entsprechend Ihren Anforderungen ändern.

   b. **Wahlweise:** Legen Sie den Parameter **„close_stale_detections“** auf *„wahr“* fest, um die veralteten Erkennungen zu schließen, die nicht mehr über die Rapid7-API für die Assets kommen, die über die Rapid7-API über **die Rapid7 Comprehensive Vulnerable Item Integration – API**gescannt und abgerufen werden.

Sie haben die Einrichtungs-, Installations- und Konfigurationsschritte für Rapid7 Vulnerability-Integrationerfolgreich abgeschlossen. Sie können die importierten Daten jetzt überprüfen und verifizieren.

Nächste Maßnahme

Die Scanner Rapid7 und Qualys sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die Schaltfläche **Erneut scannen** nicht verfügbar.

Um diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin zu aktivieren:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in den Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

Wenn Ihre Umgebung domänengetrennte Importe erfordert, lesen Sie unter Erstellen Sie domänengetrennte Importe für eine Integrationnach.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Erstellen oder Verfeinern Ihrer Suchregeln vor dem Import finden Sie unter Erstellt eine Vulnerability Response-CI-Suchregel.

Filtern nach Rapid7 Sites

Filtern Sie nach Standort für Rapid7 InsightVM Integrationstypen und Rapid7 Nexpose Data Warehouse-Integrationstypen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Hinweis:
Die Verwendung von Site-Filtern kann die Leistung beeinträchtigen. Informationen zur Leistung und zu anderen Aspekten vor der Verwendung der Standortfilterung finden Sie unter KB0789221 .

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

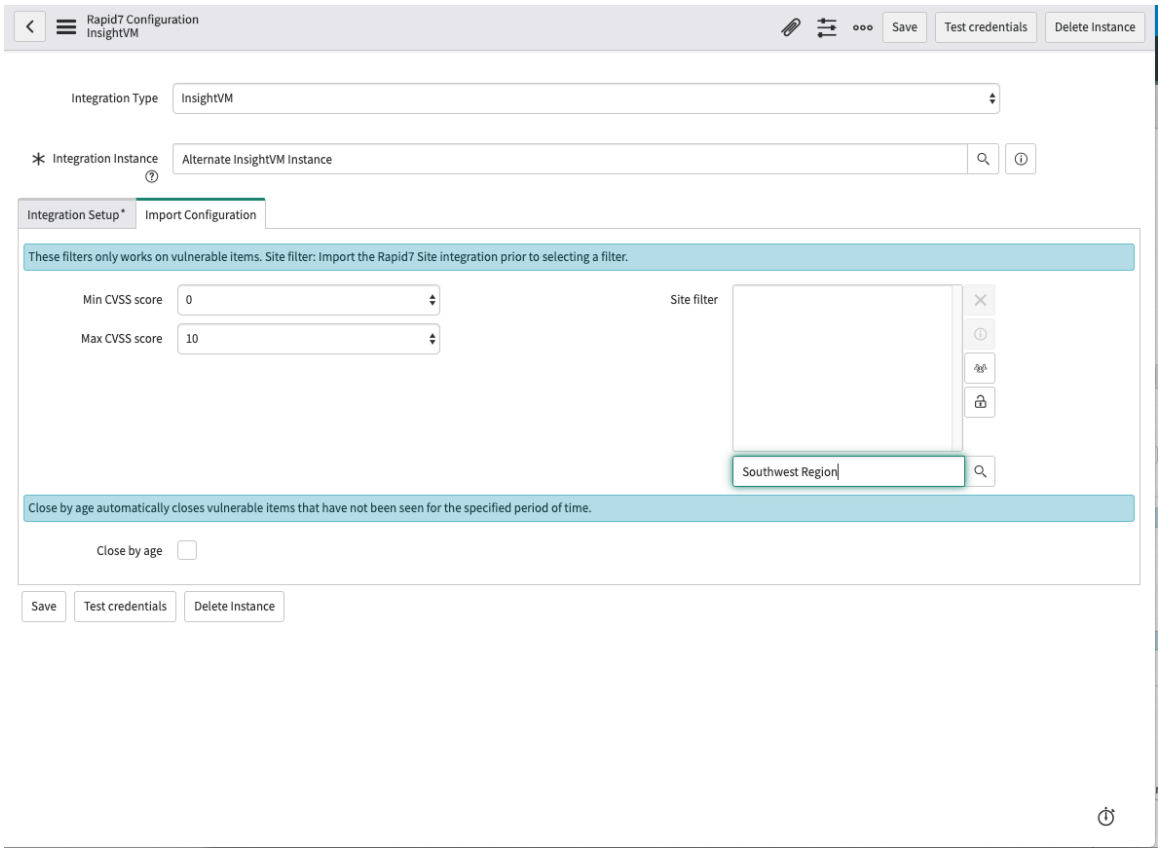
1. Navigieren zu **Alle** > **Rapid7 Vulnerability-Integration** > **Konfiguration**.
2. Wählen Sie eine Integrationsinstanz aus.
3. Klicken Sie auf die Registerkarte **Importkonfiguration**.

Hinweis:
Wenn Sie alle Sites möchten, lassen Sie das Site-Filterfeld leer. Kein Site-Filter entspricht dem Hinzufügen aller Sites.

Sites sind spezifisch für die Integrationsinstanz. In der Suchliste für Site-Filter werden die Sites Rapid7 InsightVM und Rapid7 Nexpose der Instanz der Data Warehouse-Integration angezeigt. Stellen Sie sicher, dass der ausgewählte Standort mit der ausgewählten Integrationsinstanz übereinstimmt. Wenn Sie beispielsweise versehentlich eine Data Warehouse-Site auswählen, funktioniert diese Site nicht für die Site-Filterung nach Rapid7 InsightVM.

4. Klicken Sie auf die Nachschlageliste, um die Site-Datensätze für die aktuelle Integrationsinstanz anzuzeigen.
5. Fügen Sie eine Site aus der Liste hinzu, um sie dem Site-Filter hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wiederholen Sie die Auswahl, um weitere Sites hinzuzufügen.
7. Klicken Sie auf **Speichern**.
   Diese Sites werden verwendet, um beim nächsten Import nach Site zu filtern. Informationen zum Hinzufügen des Präfix SITE zu Ihren Site-Daten finden Sie unter Stellen Sie Ihren Rapid7 InsightVM-Website-Tags SITE voran.

Stellen Sie Ihren Rapid7 InsightVM-Website-Tags SITE voran

Fügen Sie Ihren Rapid7 InsightVM -Website-Tags das Präfix SITE hinzu, um sie in der Tag-Liste hervorzuheben.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Hinweis:
Wechseln Sie bei Bedarf Ihren Bereich zu Rapid7 Integration for Security Operations.

Prozedur

1. Geben Sie im linken Navigationsfeld Folgendes ein: *`sys_properties.list`*.
2. Suchen Sie unter **Name**nach: *`sn_vul_r7.prefix_site_to_rapid7_tags`*.
3. Öffnen Sie *`sn_vul_r7.prefix_site_to_rapid7_tags`*.
4. Ändern Sie **den Wert** in **true**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Aktualisieren**.
   Neue und vorhandene Website-Tags werden beim nächsten Import von Rapid7 InsightVMvorangestellt.

Deduplizieren Sie Data Warehouse-Datensätze Rapid7 Vulnerability-Integration .

Bei der Migration vom Integrationstyp **„Data Warehouse** “ zum Integrationstyp **„Insight“** können Sie vorhandene angreifbare Data Warehouse-Elemente deduplizieren, sofern sie zu denselben Quelldaten wie Ihre Rapid7 InsightVM -Daten gehören.

Vorbereitungen

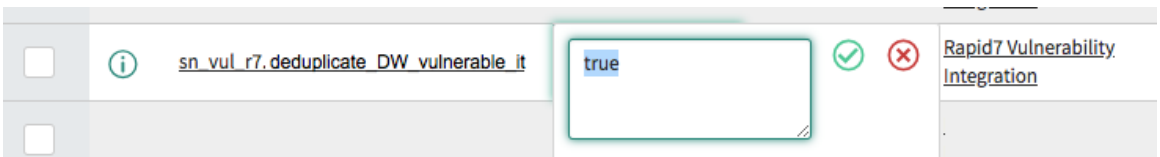
Erforderliche Rolle: sn_vul_r7.admin oder, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Diese Deduplizierung funktioniert nur, wenn Sie vom Data Warehouse Rapid7 Nexpose zur Rapid7 InsightVM Integration für angreifbare Elemente migrieren.

Prozedur

1. Navigieren zu **Alle** > **Rapid 7** > **Integrationen**.
2. Legen Sie alle Einstellungen für die Spalte **„Aktiv“** von Data Warehouse-Integrationen Rapid7 Nexpose in auf **False**fest, wodurch die Integrationen deaktiviert werden.
3. Geben Sie im linken Navigationsbereich sys_properties.list ein.
4. Suchen Sie nach dem **Namen**: sn_vul_r7.deduplicate_DW_vulnerable_item.
5. Ändern Sie das Feld **Wert** in **Wahr**.



6. Klicken Sie auf das grüne Häkchen-Symbol .
   Während des nächsten Rapid7 InsightVM Imports der Integration von angreifbaren Elementen verhindert jede Übereinstimmung mit vorhandenen Data Warehouse-Datensätzen, dass ein doppeltes angreifbares Element erstellt wird.

Rapid7 Vulnerability-Integration Statusdiagramm für die Ausführung

Rapid7 Nexpose -Sensoren erfassen die Daten und senden sie automatisch an die Produkte Rapid7 Nexpose oder Rapid7 InsightVM, welche die Informationen kontinuierlich analysieren und korrelieren.

Datenvisualisierungen in den -Arbeitsbereichen Vulnerability Response .

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad aktiver Schwachstellen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen anzeigen, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie unter Vulnerability Response Arbeitsbereiche, Vulnerability Manager Workspace und IT Remediation Workspace erkunden.

Rapid7 Vulnerability-Integration arbeitet problemlos mit Vulnerability Response zusammen, um Schwachstellen CIs und Business-Services zuzuordnen und so die Auswirkung und Priorität potenziell schädlicher Bedrohungen zu bestimmen. Das Modul Rapid7 Vulnerability-Integration „ Ausführungsstatus“ bietet eine grafische Ansicht des Status der Ausführungen von Rapid7 Vulnerability-Integration.

Um diese Daten in der Legacy-Ansicht anzuzeigen, navigieren Sie zu **Alle** > **Alle Rapid7 Vulnerability Integration** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Vorherige Versionen von Vulnerability Response

Zeigen Sie im Diagramm auf einen beliebigen Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zum Vergleich der Leistungsmetriken wurden zwei neue Diagramme hinzugefügt:

- Rapid7 Erfassungsleistungsmetriken für angreifbare Elemente: Vergleichen Sie tägliche Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit und andere Statistiken für angreifbare Elemente für die letzten 30 Tage, um die Ursache für Leistungsabweichungen zu ermitteln.
- Rapid7 Leistungsdurchsatz bei der Erfassung angreifbarer Elemente: Vergleichen Sie den täglichen Durchsatz bei der Erfassung von angreifbaren Elementen für die Rapid7 Integration angreifbarer Elemente – API. Der Durchsatz wird in Elementen pro Stunde gemessen.

Hinweis:
In Rapid7werden diese Diagramme nur für die Einblick-VM-Integration unterstützt.

Status der Rapid7-Integrationsausführung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Beispiel für ein Diagramm für den Ausführungsstatus Rapid7 Vulnerability-Integration .

- Der Wert in der Spalte Importierte Elemente stellt die Gesamtzahl der angreifbaren Elemente dar, die aus einer Integrationsausführung erstellt werden.
- In der Spalte Neue Elemente wird die Anzahl der angreifbaren Elemente angezeigt, die bei einer Integrationsausführung erstellt wurden.
- Die Spalte „Doppelte Elemente“ ist nicht mehr ausgefüllt. Unter Umständen möchten Sie diese Spalte aus der Anzeige entfernen.
- In der Spalte „Aktualisierte Elemente“ wird angezeigt, wie oft angreifbare Elemente während einer Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als 2 aktualisierte Elemente angezeigt.
- In der Spalte Unveränderte Elemente werden während der Integrationsausführung gefundene angreifbare Elemente angezeigt, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

Hinweis:
Die Integration wird für alle vier der folgenden Werte ohne Ergebnisse ausgeführt: **Neue CIs**, **Vorhandene CIs**, **Neue Elemente**und **Aktualisierte Elemente** werden aus der Liste **der Rapid7-Integrationsausführungen** herausgefiltert.

Rapid7 Vulnerability-Integration Diagrammberichte zum Ausführungsstatus

Name	Beschreibung
Ergebnisse der letzten 30 Tage Rapid7 .	Die Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. In einer Balkenvisualisierung ausführen.
Letzte 30 Tage Rapid7 Neue AEs	Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Aktualisierte VIs der letzten 30 Tage Rapid7	Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Letzte 30 Tage Rapid7 Duplikate	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Rapid7 Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 Vulnerability-Integration Diagrammberichte zum Ausführungsstatus (Fortsetzung)

Name	Beschreibung
	Hinweis: **V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`. Während die Integration ausgeführt wird, ändert sich möglicherweise die Anzahl der Erkennungen oder Ergebnisse. In diesem Bericht wird die Anzahl der Erkennungen in der Spalte „Anzahl bis Datum“ in der Instanz nach Abschluss der Integrationsausführung angezeigt.
Letzte 30 Tage Rapid7 Angreifbares Element – Erfassungsleistungsmetriken	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage.
Angreifbares Element – Erfassungsleistungsdurchsatz der letzten 30 Tage Rapid7 .	Täglicher Durchsatz bei der Erfassung von angreifbaren Elementen für die Rapid7 Integration von angreifbaren Elementen – API, gemessen für die letzten 30 Tage.

Zeigen Sie das Status-Dashboard für Importausführungen in Rapid7 Vulnerability-Integration an

Verwenden Sie das Dashboard zum Ausführungsstatus des Schwachstellenimports Rapid7, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Nachbesserungsentscheidungen zu treffen.

Vorbereitungen
Erforderliche Rolle: sn_vuln.admin

Warum und wann dieser Vorgang ausgeführt wird
Dieses Verfahren geht von den folgenden Annahmen aus.

- Sie haben Vulnerability Response und Rapid7 Vulnerability-Integration installiert und konfiguriert.
- Rapid7 Vulnerability-Integration Importe sind geplant und werden ausgeführt.
- Rapid7 Statusdiagramme der Integrationsausführung werden verwendet.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 19.0 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Rapid7** > **Status der Integrationsausführung**.

   Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

   Hinweis:
   Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

2. Wenn Sie das Statusdiagramm der Integrationsausführung Rapid7 nicht verwenden, navigieren Sie zu **Rapid7** > **Integrationen**.
   a. Wählen Sie eine Integration aus.
   b. Klicken Sie auf die zugehörige Liste **Integrationsausführungen für Schwachstellen**.
3. Stellen Sie sicher, dass alle Importe erfolgreich waren.

   Trouble?

   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung:

   - Netzwerkunterbrechung
   - Bitverfall bei der Datenübertragung, der zu beschädigten Daten während der Transformation führt

   Klicken Sie für alle diese Bedingungen auf **Execute now (Jetzt ausführen)**, und führen Sie die Integration erneut aus.

Initiieren Sie den erneuten Scan für die Rapid7 Vulnerability Integration

Initiieren Sie erneute Scans auf der Plattform Rapid7, um sicherzustellen, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden.

Vorbereitungen

Hinweis:
Erneute Scans für angreifbare Data Warehouse-Elemente Rapid7 werden nicht unterstützt.

Sie können erneute Scans über die Vulnerability Response-Arbeitsbereiche initiieren. Weitere Informationen finden Sie unter Scannen Sie Datensätze und Korrekturaufgaben im erneut Vulnerability Manager Workspace und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.

Erforderliche Rolle: Erforderliche Rolle: sn_vul.write_all oder sn_vul.write_assigned

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum erneuten Scannen in der klassischen Umgebung finden Sie in den folgenden Abschnitten.

Erneutes Scannen wird unterstützt. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente, die aus Rapid7 InsightVM -Integrationen importiert wurden, von Ihrer Instanz Now Platform® aus initiieren.

Hinweis:
Der Scanner Rapid7 ist in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die die Anwendung Rapid7 als Quelle haben, ist die Schaltfläche Erneut scannen nicht verfügbar.

Um den Aufwand und das Volumen zu reduzieren, die mit geplanten, vollständigen Scans verbunden sind, können Nachbesserungsbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen für Assets (Konfigurationselemente) in ihren Umgebungen initiieren.
Sie können erneute Scans von angreifbaren Elementen (VIs), Korrekturaufgaben (RTs), Drittparteieinträgen (TPE) oder von Datensätzen erkannter Elemente in Ihrer Instanz Now Platform® initiieren.

Durch erneute Scans können Sie überprüfen, ob durch Ihre Nachbesserungsaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben wurden.

Beispielsweise wird Ihre gesamte Umgebung alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Now Platform für angreifbare Elemente vom Typ Rapid7 initiieren. Sie können aktualisierte Ergebnisse für Ihre angreifbaren Elemente mit dem nächsten geplanten Import von Rapid7 InsightVM Integrationen für Schwachstelle und angreifbare Elemente anzeigen.

Prozedur

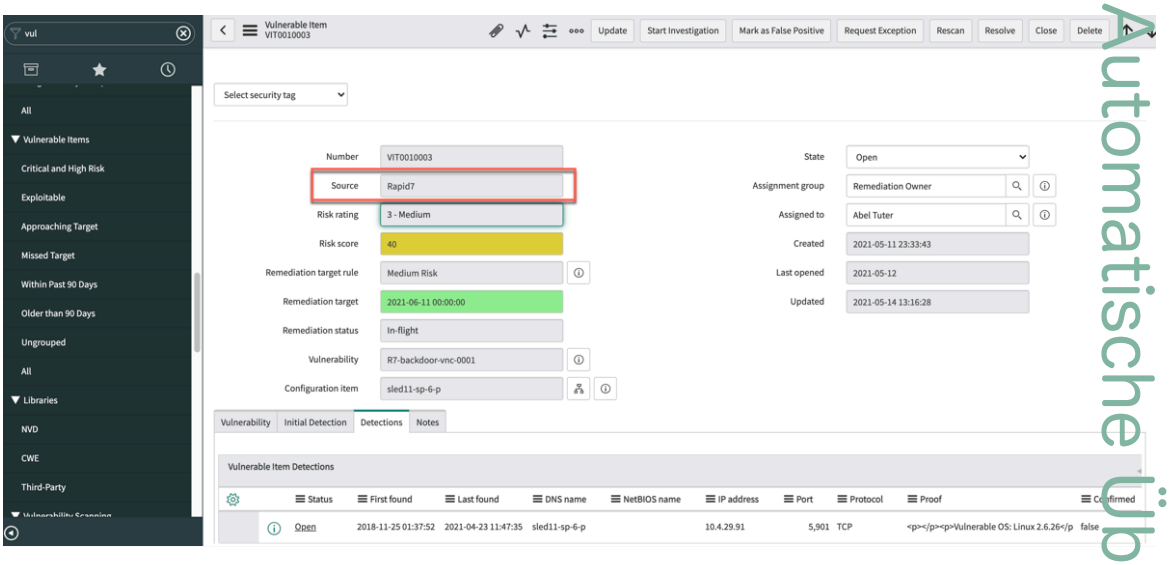
1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, von dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Initiieren Sie erneute Scans für VIs mit Rapid7 als Quelle. Überprüfen Sie, ob Rapid7 in der Spalte **„Quelle“** in den VI-Listenansichten oder in den Feldern **„Quelle“** in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte **Quelle** in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf das Zahnradsymbol, und verschieben Sie **Quelle** von **Verfügbar** in **Ausgewählt**.

Wenn Sie erneute Scans initiieren, vermeiden Sie, dass gleichzeitig Scans für eine Quell-ID aus mehreren Quellen ausgelöst werden. Bei der letzten Scan-Anforderung tritt ein Fehler auf.

Wenn Sie beispielsweise einen erneuten Scan für ein VI aus einem VI-Datensatz initiieren und außerdem einen weiteren erneuten Scan aus einem Korrekturaufgaben-Datensatz anfordern, der dasselbe VI enthält, schlägt die zweite Anforderung wahrscheinlich fehl.



3. Alternativ navigieren Sie zu **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Korrekturaufgabe bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die Schaltfläche **Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem Produkt Rapid7 stammen und sich in einem anderen Status als „Geschlossen“ befinden. Bei mehreren VI-Datensätzen müssen alle VIs, die Sie in der Listenansicht auswählen, aus dem Produkt Rapid7 stammen und sich in einem anderen Status als Geschlossen befinden.
   - In einem Korrekturaufgabendatensatz kann die Korrekturaufgabe einen anderen Status als „Geschlossen“ aufweisen, und alle zugehörigen VIs müssen aus dem Produkt Rapid7 stammen.
   - In einem TPE-Datensatz (Drittparteieintrag) muss der Datensatz über mindestens einen zugeordneten VI-Datensatz aus dem Produkt Rapid7 in einem anderen Status als „Geschlossen“ verfügen.
   - In einem Datensatz eines erkannten Elements muss das VI aus dem Produkt Rapid7 stammen und sich in einem anderen Status als **Geschlossen befinden**.

4. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie für Listenansichten die VIs aus der Liste aus, die Sie erneut scannen möchten, und wählen Sie in der Liste **Aktion für ausgewählte Zeilen die** Option **Erneut scannen aus**.

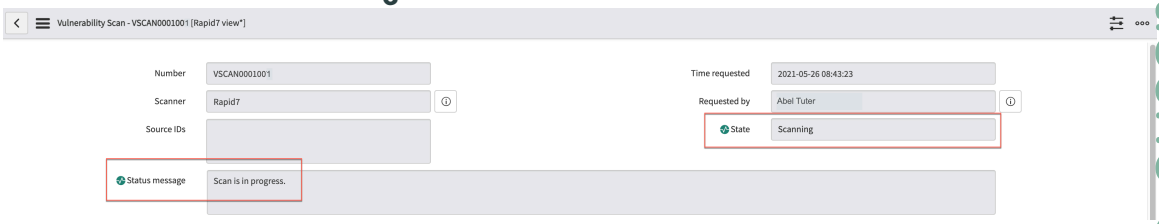
5. Bestätigen Sie im angezeigten Popup das erneute Scannen.
   Es wird eine Nachricht angezeigt, die anzeigt, dass Ihr Scan verarbeitet wird (**In Warteschlange**). Klicken Sie in der Nachricht auf den Link **Details anzeigen**, um den Status des erneuten Scans (untergeordneter Scan) zu überprüfen und alle anderen vom Datensatz gestarteten erneuten Scans anzuzeigen. Der Status für alle erneut gescannten Elemente kann jederzeit unter der zugehörigen Liste „Scans“ unten in den Datensätzen für VI, Korrekturaufgabe, TPE und erkannte Elemente gefunden werden, die Sie zum Starten der erneuten Scans verwenden.

Wenn der Scanvorgang läuft, ändert sich das Feld Status in Scanning (Wird **gescannt)**und im Feld Statusmeldung wird angezeigt **, dass Scan is in Bearbeitung (Scan wird ausgeführt)**angezeigt wird.

Hinweis:
Bei jedem erneuten Scannen werden 500 Assets pro Scan unterstützt. Wenn Ihre Anforderung mehr als 500 Assets umfasst, werden weitere untergeordnete Scans angefordert.

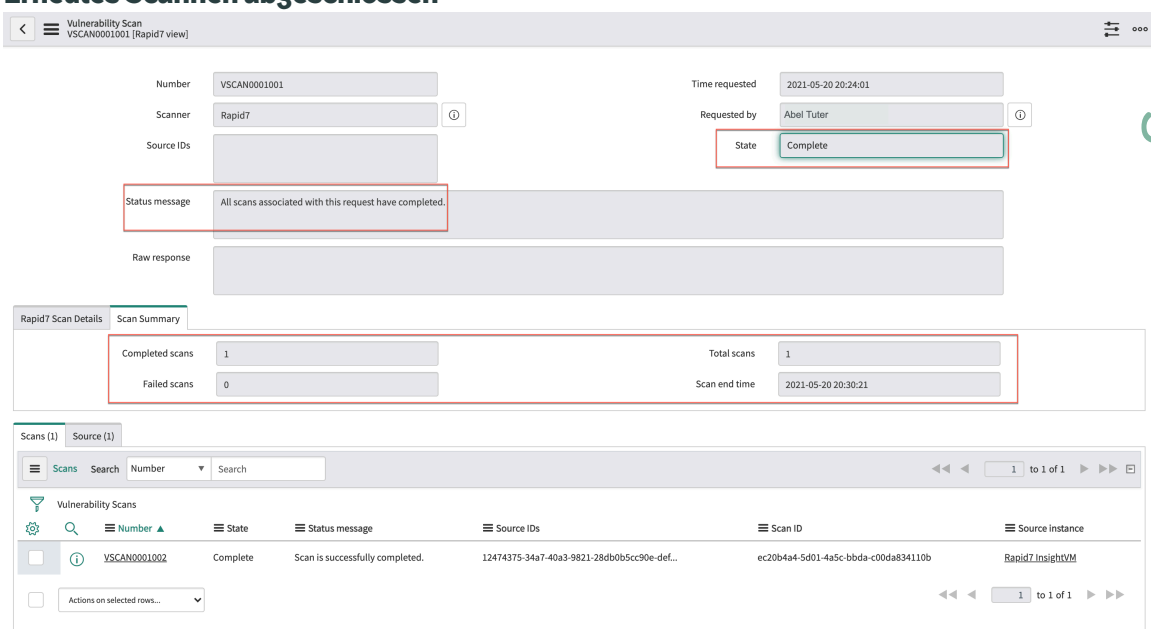
Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt).

Erneutes Scannen wird durchgeführt



Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde. Alle AEs, die in den Status „Geschlossen“/„Behoben“ übergingen oder übergehen werden, werden mit dem nächsten geplanten Import der Rapid7 Integrationen importiert.

Erneutes Scannen abgeschlossen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

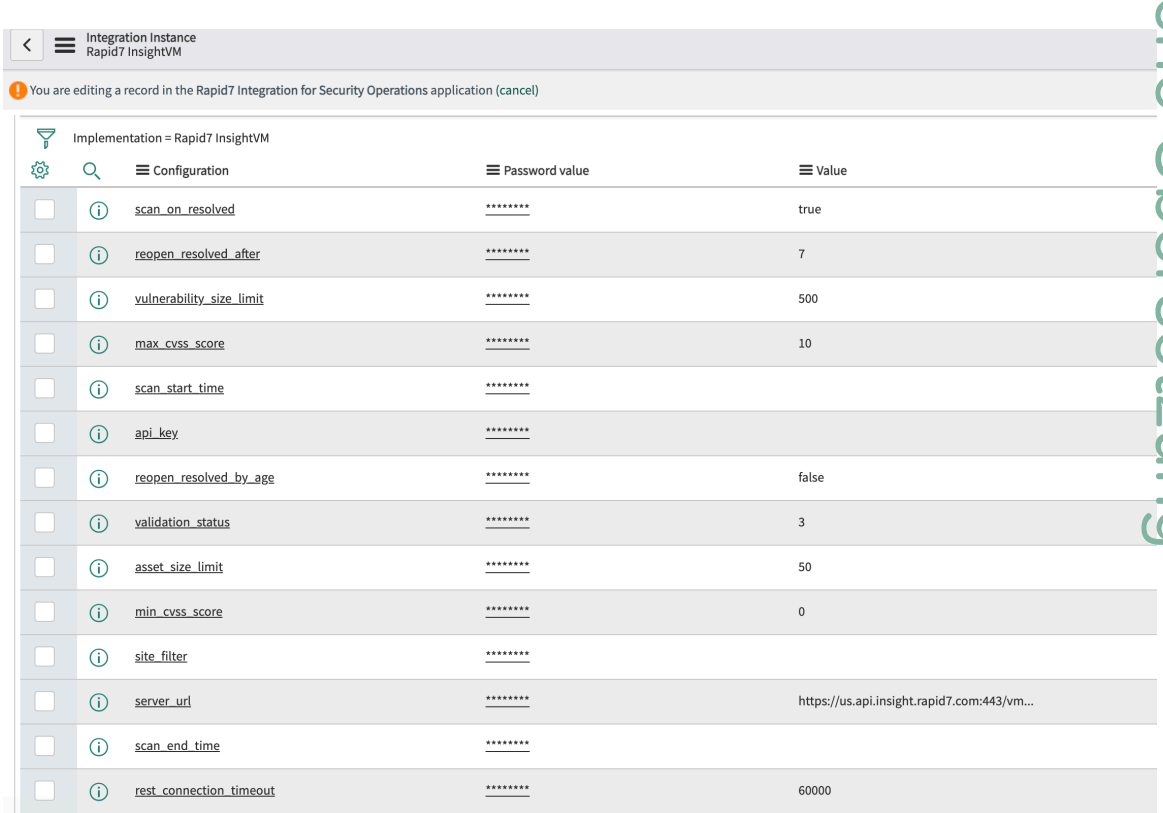
Alternativ können Sie bei Bedarf einen erneuten Scan für eine bestimmte Schwachstelle für ein bestimmtes Asset initiieren. Sie können die Ergebnisse dieser Scans anzeigen, sobald der Scan für die aktualisierten VI-, Korrekturaufgaben-, TPE- und erkannten Artikeldatensätze abgeschlossen ist, aus denen Sie den Scan gestartet haben.

Der Wert des Felds „Status“ in Datensätzen von Schwachstellen-Scans wird aus Rapid7importiert. Wenn der Scanvorgang erfolgreich abgeschlossen wurde, wird der Status auf Abgeschlossen festgelegt. Wenn der Scanvorgang nicht erfolgreich abgeschlossen wird, wird ein Fehlerwert angezeigt.

Automatische Scans und Geplante Scans

Als Schwachstellenmanager oder -analyst können Sie angeben und planen, wann erneute Scans für VIs und RTs initiiert werden. Sie können auch automatische Scans für VIs und Korrekturaufgaben aktivieren, die auf Lösung festgelegt sind.

6. Um die Integrationsparameter in der Integrationsinstanz zu ändern, navigieren Sie zu **Rapid7 Vulnerability-Integration** > **Administration** > **Konfiguration**.
7. Wenn diese Option im Datensatz „Rapid7 Configuration“ nicht ausgewählt ist, wählen Sie **Rapid7 InsightVM** aus der Liste **Integration Type (Integrationstyp)**aus.
8. Klicken Sie rechts neben dem Feld **Integrationsinstanz** auf das Informationssymbol und anschließend auf **Datensatz öffnen**.
9. Suchen Sie im Datensatz Integration Instance Rapid7 InsightVM (Integrationsinstanz – Rapid7 InsightVM) nach den Parametern für die Planung von Scans, und bearbeiten Sie sie nach Bedarf.



scan_on_resolved gibt an, ob die Prüfung initiiert wird, wenn eine Schwachstelle gelöst wird. Der Standardwert ist **„false“** (deaktiviert).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn dieser Parameter auf truefestgelegt ist und ein VI oder eine RT auf Gelöst gesetzt wird, wird automatisch der Workflow zum erneuten Scannen des entsprechenden VI und der Korrekturaufgabe ausgelöst.

scan_start_time

Legen Sie die Scan-Startzeit in **HH: mm** (24-Stunden-Format) in der UTC-Zeitzone für die Startzeit des Fensters fest, in dem erneut Scans verfügbar sein sollen.

Der Standardwert ist 00:00.

scan_end_time

Legen Sie die Scan-Endzeit in **HH:mm** (24-Stunden-Format) in der UTC-Zeitzone für die Endzeit des verfügbaren Scan-Fensters fest.

Der Standardwert ist 23:59.

Wenn ein Scan innerhalb des geplanten Zeitfensters initiiert wird, wird er sofort gestartet. Wenn der Scan außerhalb des Fensters initiiert wird, wird er für das nächste geplante Fenster in die Warteschlange gestellt.

Wenn Sie beispielsweise eine Startzeit von 00:00 Uhr für den Parameter *scan_start_time* und einen *scan_end_time* -Wert von 10:00 Uhr am selben Morgen eingeben, werden geplante oder manuell gestartete Scans außerhalb des Zeitfensters von Mitternacht bis 10:00 Uhr in die Warteschlange gestellt und gestartet zur Startzeit des Zeitfensters des folgenden Tages um 00:00 Uhr.

Wenn Sie im selben Beispiel einen erneuten Scan manuell um 11:00 Uhr initiieren, wird er nicht sofort gestartet, da er außerhalb der verfügbaren konfigurierten Scan-Zeiten liegt. Die Scan-Anforderung bleibt bis zum Beginn des Zeitfensters des folgenden Tages in der Warteschlange, in diesem Beispiel 00:00.

Legen Sie zusätzliche Filterparameter für Rapid7 InsightVM -Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Rapid7 Integration for Security Operations an, um die mit dem Produkt Rapid7 InsightVM importierten Schwachstellendaten weiter zu verfeinern.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen filtern, um nur bestimmte Schwachstellendetails überprüfen zu können. Beispielsweise können Sie nur importierte Schwachstellen anzeigen, die den Status „Kritisch“ und „Schwerwiegend“sind.

Um Sie beim Sammeln dieser Daten zu unterstützen, fügen Sie Rapid7 Parameter hinzu, mit denen Sie die spezifischen Schwachstellendetails importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie ab v13.4 mit der Funktion Ihre HTTP-Anforderungsinformationen mit den Parametern Rapid7 InsightVM in Ihrem Now Platformanpassen. Die folgenden Rapid7 InsightVM Integrationen unterstützen die Filterung durch Hinzufügen von JSON-Inhalten im Anforderungstext:

- Rapid7 InsightVM API zur Integration angreifbarer Elemente
- Rapid7 InsightVM API zur Integration von Schwachstellen
- Rapid7 InsightVM

Sie sollten wissen, wie JSON -Zeichenfolgen für diese Funktion verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_vul.vulnerability_admin

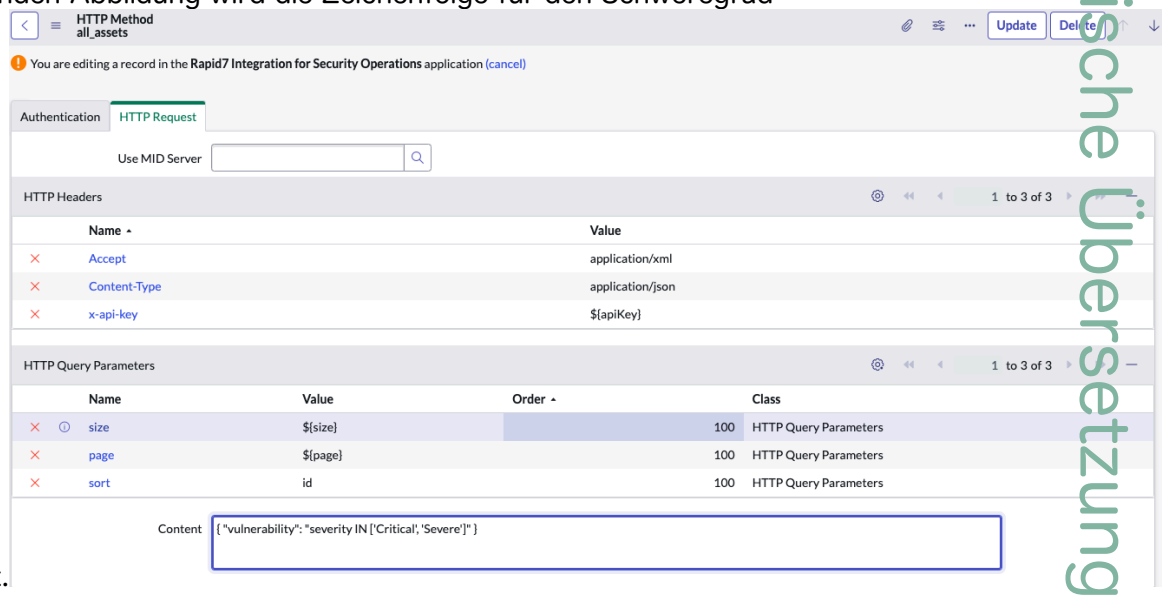
Prozedur

1. Suchen Sie die vom Produkt Rapid7 InsightVM unterstützten Parameter auf der Entwickler-Site Rapid7, nach der Sie filtern möchten.

   In der Rapid7 -Dokumentation können Sie die Parameter für den Anforderungstext erstellen. Parameter und Werte, die Sie aus dem Produkt Rapid7 InsightVM eingeben, werden nur auf Ebene der Integrationsinstanz unterstützt.

2. Navigieren zu **Alle** > **Rapid7 Vulnerability-Integration** > **Administration** > **Integrationen**.
3. Klicken Sie auf der Listenseite Rapid7 Integrations (Rapid7-Integrationen) auf den Datensatz für die Integration Rapid7 InsightVM, die Sie öffnen möchten.
4. Klicken Sie rechts auf der Seite auf das Informationssymbol (I) für die REST-Nachricht und anschließend auf **Datensatz öffnen**.
5. Klicken Sie bei ausgewählter Registerkarte HTTP-Anforderung unter HTTP-Methoden in der Spalte Name auf ein Element, um die zugehörigen HTTP-Abfrageparameter zu öffnen.
6. Geben Sie unter „HTTP-Methodendatensatz“ unter „HTTP-Abfrageparameter“ im Feld Inhalt die Parameterwerte ein, die Sie auf der Developer Site Rapid7 gefunden haben.

   In der folgenden Abbildung wird die Zeichenfolge für den Schweregrad hinzugefügt.



   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Rapid7 weitere Informationen zum Trennen der einzelnen Werte.

7. Klicken Sie auf **Aktualisieren**.

Informationen zur Shodan Exploit-Integration

Die Anwendung ServiceNow® Shodan Exploit Integration verwendet Daten, die aus der Suchmaschine Shodan importiert wurden, um Ihnen zu helfen, die Auswirkung und Priorität potenziell schädlicher Exploits zu ermitteln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Shodan Exploit Integration

Die Suchmaschine Shodan sammelt Exploit-Daten, und die Shodan-API stellt diese Datenbank für Now Platform®zur Verfügung. Die Anwendung ServiceNow® Vulnerability Response lässt sich problemlos integrieren, um Schwachstellen von Drittparteien Exploits zuzuordnen, welche die Exploit-Daten in Ihrer -Instanz ergänzen.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Jeden Tag rufen geplante Aufgaben die Integrationen automatisch in der Reihenfolge auf, in der sie aufgelistet sind. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Verfügbare Versionen

Release-Version für Yokohama	Release-Hinweise
Shodan Exploit-Integration v10.6, 10.7	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Rollen

Shodan Exploit-Integrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_shodan.admin: Benutzer mit dieser Rolle können Datensätze lesen, schreiben und löschen.
- sn_vul_shodan.user: Benutzer mit dieser Rolle können Datensätze lesen und schreiben.
- sn_vul_shodan.read: Benutzer mit dieser Rolle können Datensätze lesen.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Shodan-Exploit-Integrationen

Um die Exploit-Integrationen für Shodan anzuzeigen, navigieren Sie zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig aktiv.

Shodan-Exploit-Integrationen

Integration	Beschreibung
Shodan ExploitDB Integration	Ruft ExploitDB-Daten von Shodan ab und erweitert Ihre Drittpartei-Schwachstellendaten. Diese Integration wird täglich um 3:15:00 Uhr ausgeführt.
Shodan Metasploit Integration	Ruft Metasploit-Informationen von Shodan ab und erweitert Ihre Drittpartei-Schwachstellendaten. Diese Integration wird täglich um 01:15:00 ausgeführt.

Informationen zum Ändern der Standardstartzeit für geplante Integrationsimporte finden Sie unter Legen Sie die Importzeit Shodan für die Exploit-Integration fest.

Informationen zum Anzeigen von Exploit-Daten in Schwachstellen von Drittparteien finden Sie unter Zeigen Sie Schwachstellenbibliotheken Vulnerability Response an.

Das Ändern anderer Einstellungen für die Shodan Exploit-Integration erfordert fortgeschrittene Kenntnisse ServiceNow von und Vulnerability Response und geht über den Umfang der Produktdokumentation hinaus.

Vorbereitung auf die Shodan Exploit-Integration

Eine erfolgreiche Shodan Exploit-Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Die Shodan Exploit-Integration setzt voraus, dass Sie mit der Suchmaschine und API Shodan vertraut sind.

Vorbereitungen

Die Exploit-Integration Shodan erfordert einen API-Schlüssel. Registrieren Sie sich auf der Shodan Website, um ein kostenlose Abonnement zu erhalten und diesen Schlüssel zu erhalten.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen vor, die auf Ihren Anforderungen basieren.

- Wenn Sie keine Daten der NIST Vulnerability Database (NVD) in Vulnerability Responseimportiert haben, sollten Sie dies tun, bevor Sie die Exploit-Integration für Shodan installieren. Durch das Importieren der NVD-Daten wird sichergestellt, dass Ihre Common Vulnerability and Exposure-Daten (CVE) die Exploit-Datensätze automatisch ausfüllen.

  Ohne NVD-Daten wird im Exploit-Datensatz ein Platzhalter erstellt und erst beim nächsten NVD-Update eingegeben. Weitere Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

- Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Shodan Exploit-Integration für Security Operationsinstallieren und konfigurieren

Bevor Sie Shodan Exploit-Integration in Ihrer -Instanz ausführen können, laden Sie es aus dem ServiceNow Storeherunter, und installieren Sie es. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

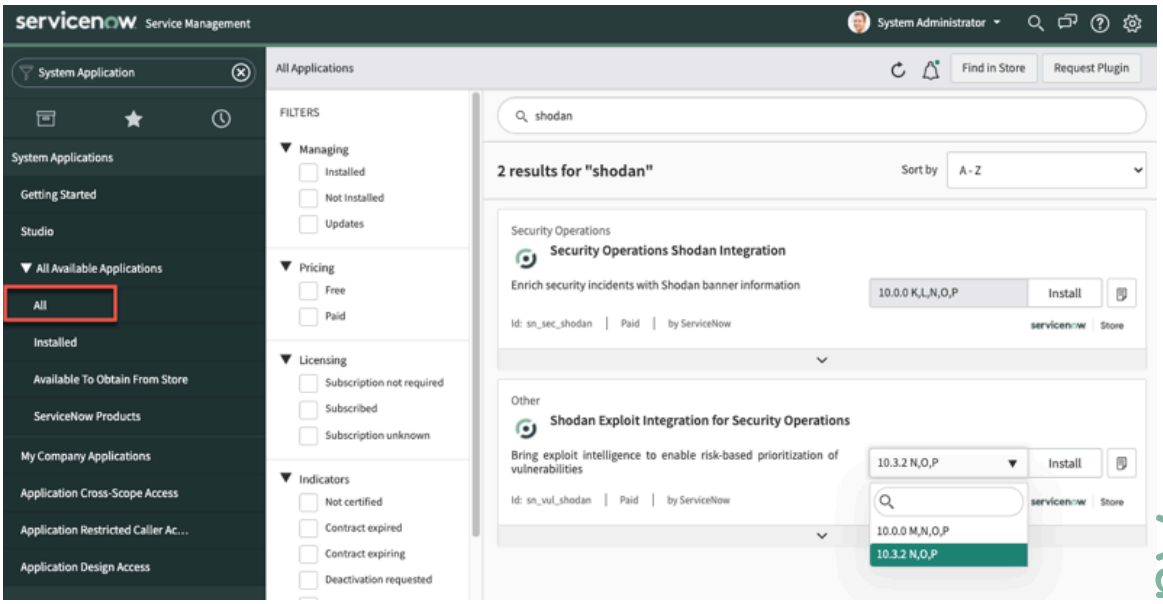
Setupaufgaben	Beschreibung
Vergewissern Sie sich, dass Sie gültige Berechtigungen ServiceNow für die Anwendung Vulnerability Response und die Anwendung Shodan Exploit-Integration für Security Operations haben.	Um Berechtigungen zu überprüfen, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Weitere Informationen zum Abrufen von Berechtigungen für eine Anwendung Security Operations aus ServiceNow Storefinden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab.
(Optional) Wenn die Anwendung noch nicht installiert und aktiviert ist, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren.	Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren.
Halten Sie den API-Schlüssel Shodan Exploit Integration bereit.	Weitere Informationen finden Sie unter Vorbereitung auf die Shodan Exploit-Integration.

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Shodan Exploit-Integration installieren möchten.
2. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
3. Suchen Sie die Anwendung Shodan Exploit-Integration für Security Operations, wählen Sie die gewünschte Version aus, und klicken Sie auf **Installieren**.

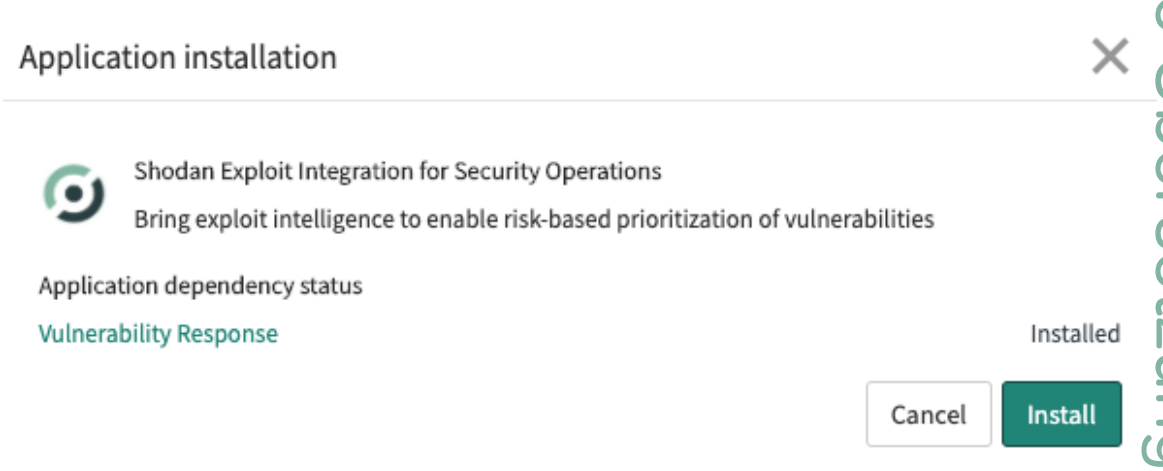
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wenn Sie berechtigt sind, ein Update für diese Anwendung zu erhalten, wird die Schaltfläche **Aktualisieren** angezeigt.

Im Dialogfeld „Anwendungsinstallation“ wird der Status der Anwendungsabhängigkeit angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.

4. Klicken Sie im Dialogfeld auf **Installieren**.

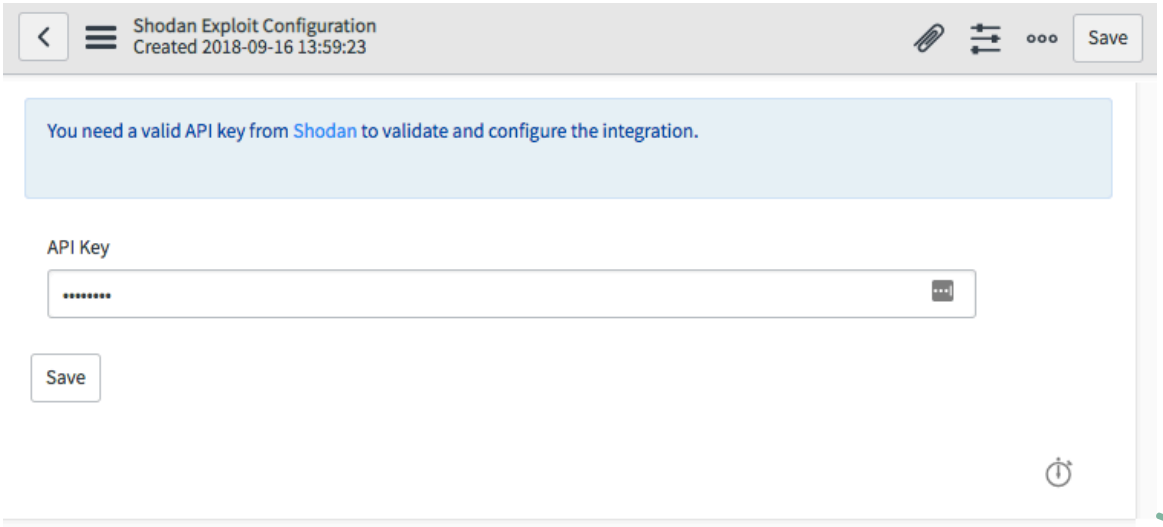


Im Dialogfeld „Installieren“ wird angezeigt, wenn die Installation erfolgreich abgeschlossen wurde.

5. Schließen Sie das Dialogfeld „Installation“.
6. Navigieren zu **Shodan Exploit Integration** > **Konfiguration**.
7. Geben Sie Ihren Shodan -API-Schlüssel ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Klicken Sie auf **Speichern**.
   Die Konfiguration von Shodan Exploit-Integration ist abgeschlossen.

Legen Sie die Importzeit Shodan für die Exploit-Integration fest

Zur Vereinfachung können Sie die Startzeit für die Exploit-Integrationen Shodan zurücksetzen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import führen Exploit-Integrationen Shodan von Delta-Daten ein, sofern kein vollständiger Import angefordert wird. Weitere Informationen zu vollständigen Importen finden Sie unter Führen Sie einen manuellen Shodan -Exploit-Import durch.

Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf den Link, um den Datensatz zu bearbeiten.
4. Legen Sie die neuen Optionen **für Ausführung** und **Zeit** fest.
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für Importe des Exploits Shodan ist 03:15:00.
5. Klicken Sie auf **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

Führen Sie einen manuellen Shodan -Exploit-Import durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie unabhängig von der täglichen geplanten Aufgabe einen vollständigen Datenimport durchführen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Aktivieren Sie das Kontrollkästchen **Vollständiger Datenimport**.
4. Klicken Sie auf **Jetzt ausführen**.
   Sobald der Import abgeschlossen ist, wird das Kontrollkästchen deaktiviert, und die Delta-Importe werden fortgesetzt.

Zeigen Sie den Ausführungsstatus des Exploit-Integrationsimports Shodan an

Verwenden Sie die zugehörige Liste „Integrationsausführungen für Schwachstellen“, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu finden, und treffen Sie fundierte Entscheidungen zur Problembehebung.

Vorbereitungen

So zeigen Sie den Ausführungsstatus des Shodan-Imports an:

- Die Anwendung Vulnerability Response und die Exploit-Integration Shodan müssen installiert und konfiguriert sein.
- Die Importe der Shodan Exploit-Integration müssen geplant sein und ausgeführt werden.

Erforderliche Rolle: sn_vuln.admin

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf die zugehörige Liste **Integrationsausführungen für Schwachstellen**.
4. Stellen Sie sicher, dass alle Importe erfolgreich waren.

Trouble?

Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

- Netzwerkunterbrechung
- Bitverfall bei der Datenübertragung, der zu beschädigten Daten während der Transformation führt

Wenn eine dieser Bedingungen auftritt, aktivieren Sie das Kontrollkästchen **Vollständiger Datenimport**, klicken Sie auf **Jetzt ausführen**, und führen Sie die Integration erneut aus.

Die Tenable-Schwachstellenintegration verstehen

Die Anwendung Vulnerability Response Integration with Tenable, die von den Entwicklern von ServiceNow für die Tenable Vulnerability Integration entwickelt wurde, verwendet Daten, die aus den Produkten Tenable.io und Tenable.sc importiert wurden, um Sie bei der Priorisierung und Behebung von Schwachstellen für Ihre Assets zu unterstützen. Die Anwendung ist mit einem separaten Abonnement aus dem ServiceNow® Storeverfügbar.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die Tenable-Schwachstellenintegration verwendet die beiden Tenable-Integrationen Tenable.io und Tenable.sc, um Scannerdaten von Drittparteien zu Ihren Assets und Schwachstellen zu importieren. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13.

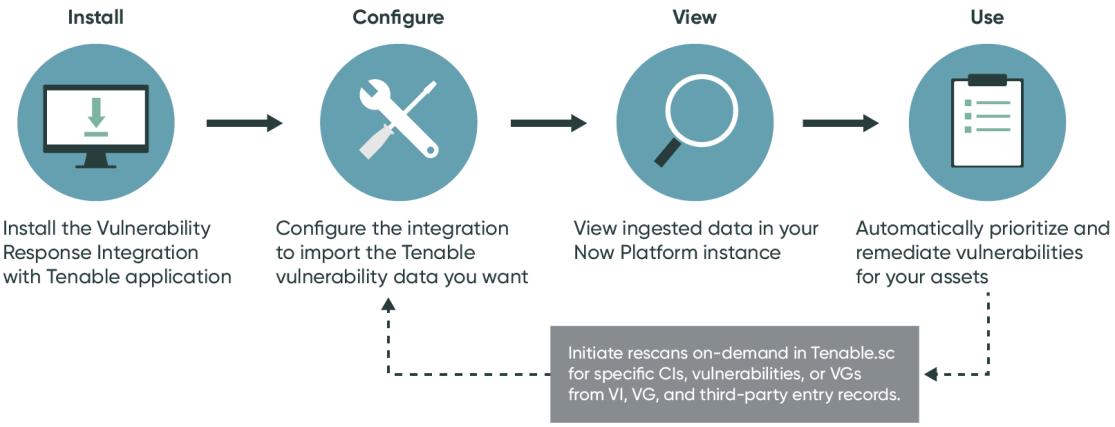
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Tenable.io ist eine cloudbasierte Unternehmensintegration.
- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID-Server verwenden.

Die Anwendung Vulnerability Response Integration with Tenable ist unter ServiceNow Store mit einem separaten Abonnement verfügbar.

Listen und Beschreibungen der Integrationen in Tenable Vulnerability Integrationfinden Sie unter Tenable.io -Integrationen mit den Anwendungen Vulnerability Response und Konfigurations-Compliance und Tenable.sc Integrationen mit der Anwendung Vulnerability Response.

Tenable-Schwachstellen-Integration



Verfügbare Versionen für Yokohama

Freigabeversion	Release-Hinweise
Vulnerability Response Integration with Tenable v3.5, v3.6	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Begriffe und Schlüsselfunktionen der Integrationen

Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in Ihrer Instanz Now Platform erstellt, wenn:

- Eine importierte Schwachstelle aus einem Drittanbieterscanner wird mit einem vorhandenen Asset (einem Konfigurationselement in Ihrem CMDB) abgeglichen. Das Tenable-Produkt bezeichnet diese Übereinstimmungen als **Schwachstellen**.
- Eine importierte Schwachstelle aus einem Drittanbieterscanner wird keinem vorhandenen Asset in Ihrem CMDBzugeordnet. In diesem Fall wird zusammen mit einem angreifbaren Element auch ein nicht abgeglichenes CI erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für nicht abgeglichene CIs können Sie auch die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) verwenden, um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt.

Schwachstelleneinträge und Plugins von Drittparteien

Einträge für Schwachstellen von Drittparteien werden aus Scannern von Drittparteien importiert und in der Tabelle „Schwachstellen von Drittparteien“ in Ihrer Instanz Now Platform aufgeführt. Ab v24.0 von Vulnerability Responsefüllt die Spalte „Software“ in der Tabelle „Einträge von Drittanbieter-Schwachstellen“ die Common Platform Enumerations (CPEs) aus, die einem Eintrag einer Drittpartei zugeordnet sind. Schwachstelleneinträge von Drittparteien von Tenable werden in Vulnerability Response erfasst und mit vorhandenen Assets abgeglichen, die in Ihrem CMDBaufgeführt sind. Schwachstelleneinträge von Drittparteien werden von Tenable als **Plugins**bezeichnet.

Konfigurationselement bzw. Configuration Item (CI)

Konfigurationselemente sind die vorhandenen Assets, die in Ihrem CMDBaufgeführt sind.

Erkanntes Element

Aus dem Tenable-Asset-Import erfasste Assets werden mit vorhandenen Configuration Items in Ihrem CMDBabgeglichen. Importierte Assets werden aktualisiert.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der CI-Klasse ohne Übereinstimmung von CMDBerstellt. Wenn das Plugin „CMDB CI Class Models“ aktiviert ist, erstellt die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) neue CIs mithilfe neuer Klassen. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt. Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden die Datensätze erkannter Elemente entsprechend dem Status aktualisiert. Erkannte Elemente geben Ihnen Einblick in die Art und Weise, wie Assets identifiziert und CIs in CMDBzugeordnet werden.

CI-Suchregeln

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Vulnerability Response automatisch Hostdaten (Asset-Daten), um in der Configuration Management Database (CMDB) nach Übereinstimmungen zu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und zu VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden, um Sie bei der Remediation zu unterstützen.

Erneut scannen und Korrekturscan durchführen

Sie können einen gezielten erneuten Scan-Befehl für ein bestimmtes Konfigurationselement, eine Korrekturaufgabe oder einen Drittanbietereintrag direkt aus den Datensätzen für angreifbare Elemente, Korrekturaufgaben und Schwachstelleneinträge von Drittparteien in Ihrer Instanz Now Platform initiieren. Tenable bezeichnet diesen erneuten Scan als **Korrekturscan**.

Ältere VIs automatisch schließen

Mit dem Modul Veraltete angreifbare Elemente automatisch schließen in Now Platformkönnen Sie ältere, veraltete angreifbare Elemente (VIs) bereinigen, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden. Wenn Sie diese AEs in **den Status „Geschlossen“** verschieben, können Sie die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben reduzieren und Assets in Ihrem CMDBabgleichen. Sie können alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen mit Vulnerability Response Integration with Tenable verwenden, um veraltete AEs automatisch zu schließen.

Instanz

Dieser Begriff bezieht sich auf ein bestimmtes Vorkommen Ihrer Anwendung Now Platform®.

Integration

Eine Integration ist ein produktspezifischer Verweis auf eine Integration, z. B. Tenable.io Assets Integration oder Tenable.sc Plugin Integration. Dies sind die separaten Integrationen, die zu bestimmten Tenable-Produkten in der Tenable-Schwachstellen-Integration in Ihrer Instanz gehören.

Integrationsinstanz

Dieser Begriff bezieht sich auf die separaten Tenable-Integrationen, die nach den Produkten Tenable.io und Tenable.sc aufgelistet sind.

Bereitstellung

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne, eindeutige Integration als Bereitstellung Ihrer Integration bezeichnet. Der Begriff bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie in Ihrer Umgebung über mehrere Bereitstellungen verschiedener Integrationen der Produkte Tenable.io und Tenable.sc verfügen.

Die Integrationen Tenable.io und Tenable.sc enthalten außerdem die folgenden Schlüsselfunktionen:

- Konfigurationsbewertungsergebnisse, d. h. Testergebnisse sowie Richtlinien, Konfigurationstests (Steuerungen) und Zitate mit maßgeblichen Quellen, können mit dem Produkt Konfigurations-Compliance in die Anwendung Tenable.io importiert werden. Unter Tenable.io -Integrationen mit den Anwendungen Vulnerability Response und Konfigurations-Compliance und Konfigurations-Compliance erkunden finden Sie weitere Informationen darüber, wie diese Integration mit der Anwendung Konfigurations-Compliance funktioniert.
- Ab v2.1 von Tenable Vulnerability Integrationerstellen Sie eindeutige Configuration Items (CIs), die unterschiedliche Netzwerkpartitionsbezeichner für Assets in Ihrer Umgebung enthalten, die dieselbe IP-Adresse verwenden. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um weitere Details zu Ihren Schwachstellen zu erhalten.
- Sie können planen, wann die Aufgaben für alle Tenable.io - und Tenable.sc -Integrationen ausgeführt werden sollen. Sie können geplante Aufgaben bei Bedarf auch manuell ausführen.
- Für Asset-Importe mit Tenable.iokönnen Sie Asset-Tags aktivieren, um die in Ihrem CMDB aufgeführten Assets in der Umgebung Tenable.io zu organisieren und nachzuverfolgen.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie CI-Suchregeln konfigurieren, um zu definieren, wie Asset-Daten aus Drittanbieterquellen zum Identifizieren von Configuration Items (CIs) in Ihrem Now Platform CMDBverwendet werden.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie Importfilter für den Import von Schwachstellen festlegen, um nur die gewünschten Schwachstellen aus Tenable zu importieren. Für Tenable.iohaben Sie die Möglichkeit, mit dem Import von Schwachstellen **behobene** Schwachstellen aus Tenable zu importieren.
- Für Tenable.schaben Sie die Möglichkeit, bei Bedarf erneute Scans direkt aus angreifbaren Elementen, Korrekturaufgaben und Drittpartei-Eintragsdatensätzen in Ihrer Instanz Now Platform zu initiieren. Wenn VIs in den Status **„Geschlossen"/„Behoben"** versetzt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wurden, in Ihrer Instanz jedoch noch nicht aktualisiert werden, können Sie überprüfen, ob Schwachstellen an bestimmten Konfigurationselementen behoben wurden. Weitere Informationen finden Sie unter Initiieren Sie den erneuten Scan für die Tenable.sc -Integration.

In den folgenden Abschnitten finden Sie weitere Details zu den Tenable-Integrationen.

Erforderliche Now Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrer Instanz Now Platform.

Administrator

Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn dies nicht zugewiesen ist, weist der Administrator im Setup-Assistenten den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu.

sn_vul.vulnerability_admin

Nach der Zuweisung schließt der Schwachstellen-Administrator die Konfiguration der Tenable-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle VR-Anwendungen und Regeln für installierte Drittanbieterintegrationen.

sn_vul_tenable.configure_integration

Diese Rolle enthält die granulare Rolle sn_vul_tenable.read_integration, und Benutzer mit dieser Rolle können die Anwendung Vulnerability Response Integration with Tenable konfigurieren.

sn_vul_tenable.read_integration

Anwender mit diesen Rollen können Datensätze der Anwendung Vulnerability Response Integration with Tenable anzeigen (lesen), aber nicht bearbeiten.

Vulnerability Response-Gruppe

Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen „sn_vul.read_all“ und „sn_vul.remediation_owner“ automatisch.

Angreifbare Elemente

Angreifbare Elemente werden gemäß den Regeln für Korrekturaufgaben in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Vulnerability Response Übersicht über Zuweisungsregeln.

Suchregeln für Configuration Item (CI)

CI-Suchregeln identifizieren CIs und bestimmen, wann sie einem angreifbaren Element hinzugefügt werden sollen. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

Hinweis:
Einmal entfernte Regeln können nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, sollten Sie sie beim Erstellen neuer Regeln deaktivieren.

Die folgenden Tenable.io Suchregeln sind im Lieferumfang des -Basissystems enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

Hinweis:
Die Tenable.io CI-Suchregeln priorisieren und füllen die nicht leeren Netzwerkschnittstellenwerte (FDQN, IPV4 und MacAddress) gegenüber den regulären FDQN-, IPV4- und MacAddress-Werten für ein erkanntes Element aus. Wenn diese Werte für die Netzwerkschnittstelle leer sind, werden die regulären Werte für FDQN, IPV4 und MacAddress für ein erkanntes Element ausgefüllt.

Die folgenden Tenable.sc Suchregeln sind im Lieferumfang des -Basissystems enthalten.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Hinweis:
Für ein Asset werden mehrere Werte für ip_address, mac_address, fqdns und network_interfaces verwendet. Alle Werte werden in den CI-Suchregeln für die Übereinstimmung berücksichtigt. Alle Werte werden verwendet, um mehrere Netzwerkadapter mit IRE zu erstellen.

Weitere Informationen zum Konfigurieren der Kategorisierung von nicht abgeglichenen Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets aktualisieren.

Neue Eigenschaften zum Ignorieren von IP-Adressen

In Tenable.iostehen Ihnen zwei Eigenschaften zur Verfügung, wenn Sie mehrere IP-Adressen oder Mac-Adressen als Teil Ihrer CI-Suchregeln ignorieren möchten:

ignorierenIPAddress

Eine Liste der IP-Adressen, die bei der CI-Suche und CI-Erstellung ignoriert werden sollen.

ignorierenMacAddress

Eine Liste der MAC-Adressen, die für die CI-Suche oder CI-Erstellung ignoriert werden sollen.

Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus den Tenable Vulnerable Item-Integrationen und den Tenable Asset-Integrationen erkannt wurden.

Hinweis:
Der Standardfilter für diese Liste ist auf Nicht abgeglichenfestgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „Erkannte Elemente“ finden Sie unter Erkannte Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Asset-Tags

Asset-Tags (auch als Host-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Assets Tags zuweisen. Dann können Sie beim Starten von Scans Tags auswählen, die den zu scannenden Assets zugeordnet sind. Mit dem Modul „Asset Tags“ können Sie Asset-Tag-Daten von Tenable.io zeitplanbasiert in Ihre Instanz herunterladen. Asset-Daten, die Asset-Tags enthalten, werden aus Tenable.io abgerufen und mithilfe der Transformationszuordnungen der Tenable.io Asset Transform- Integration transformiert.

Alle Asset-Tags werden als Teil der Asset-Integration Tenable.io importiert. Asset-Tags werden im Allgemeinen zum Filtern in Vulnerability Response -Zuweisungsregeln und Regeln für Korrekturaufgaben verwendet. Die Tags werden im Formular „Erkanntes Element“ angezeigt.

Hinweis:
Führen Sie die Asset-Integration Tenable.io aus, bevor Sie in der Anwendung Vulnerability Response Zuweisungsregeln für Vulnerability Response oder Regeln für Korrekturaufgaben erstellen, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie beispielsweise ein Tag zur Beschreibung von Assets an Ihrem Standort San Diego erstellen und das San Diego -Tag erstellen, können Sie nicht auch ein SAN DIEGO -Tag erstellen und in der Asset-Tag-Tabelle speichern. San Diego und SAN DIEGO werden vom System als dasselbe Asset-Tag betrachtet. Das zuerst importierte Tag ist das Tag, das in Zukunft gespeichert und erkannt wird.
- Die Verwendung von Asset-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Asset-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Asset-Tags werden von der globalen Systemeigenschaft sn_vul.import_asset_tags gesteuert. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Durch das Deaktivieren von Tags werden sie für alle Now Platform® -Instanzen deaktiviert.

Datenabruffilter

Mithilfe der Einstellungen zum Datenabruf können Sie insbesondere den Typ und Umfang der Daten bestimmen, die Sie aus der Tenable-Anwendung in Ihre Instanz Now Platform® importieren möchten. Eine Liste der am häufigsten verwendeten Einstellungen finden Sie unter Datenabrufeinstellungen für die Tenable Vulnerability-Integration.

Schwachstellenprioritätsbewertung (VPR)

Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in Vulnerability Responseverwendet wird. Die Tenable-Risikoregel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisiko-Rechners in den Schwachstellen-Rechnern von Vulnerability Responseinstalliert.

Diese Risikoregel ist standardmäßig deaktiviert.

Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte verwendet, um die Risikopunktzahl für angreifbare Elemente zu berechnen. Standardgewichtsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Business-Relevanz = 15 %. Das Aktivieren dieser Regel des Tenable-Risikorechners kann sich auf die Leistung der Datenerfassung auswirken. Weitere Informationen zu den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rechnern Vulnerability Response und zur Regel des Tenable-Risikorechners finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.

Installation und Konfiguration

Nachdem Sie Vulnerability Response Integration with Tenable von ServiceNow® Storeheruntergeladen haben, werden die Installation und Konfiguration durch den Setup-Assistenten in Vulnerability Responseunterstützt. Weitere Informationen finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

Tenable.io -Integrationen mit den Anwendungen Vulnerability Response und Konfigurations-Compliance

Die Tenable.io -Integrationen in der Anwendung Vulnerability Response Integration with Tenable sind in den Anwendungen Vulnerability Response und Konfigurations-Compliance verfügbar.

Liste von Tenable.io Integrationen

Multi-Quelle wird für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können über den Setup-Assistenten in Vulnerability Responsemehrere Instanzen der folgenden Integrationen in Ihrer Umgebung hinzufügen und bereitstellen. Außerdem installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Tenable über den Setup-Assistenten.

Tenable.io ist eine cloudbasierte Unternehmensintegration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für das Produkt Tenable.io.

Die Tenable.io Integration für Compliance-Ergebnisse und die Tenable.io Integration für die Auffüllung von Compliance-Ergebnissen sind standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
2. Klicken Sie in der Liste „Tenable Integrations“ (Tenable-Integrationen) auf einen Integrationsnamen, um den Datensatz zu öffnen, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen auf ihren Standardwerten belassen, damit diese Integrationen gestartet werden können.

Tenable.io-Integrationen

Integration	Beschreibung
Tenable.io Assets Integration	• Ruft alle Asset-Daten, einschließlich Asset-Tags, vom Produkt Tenable.io ab und verarbeitet sie in Ihrer -Instanz. • Ab v3.0 können Sie, wenn die Tenable.io Compliance-Ergebnisintegration aktiviert ist, auch sichere Konfigurationsbewertungsdaten zusammen mit importierten Asset-Daten importieren. Diese Daten können Ihnen helfen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Asset-API • Die Ausgabe dieser Integration sind erkannte Elemente. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. • Ab v2.2 wird `Last Scan Time` nur für Assets importiert und aktualisiert, die Schwachstellen aufweisen.
Tenable.io Integration von Compliance-Ergebnissen	• Ab v3.0 können Sie importierte Bewertungsdaten für die sichere Konfiguration aus der Compliance-Ergebnisintegration zusammen mit importierten Daten aus der Assets-Integration dabei unterstützen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und zu beheben. • Wenn diese Option aktiviert ist, werden allgemeine Bewertungsdaten der sicheren Konfiguration abgerufen und in der Instanz Now Platform verarbeitet. Importierte Daten umfassen Testergebnisse sowie Richtlinien, Konfigurationstests (Steuerungen) und Zitate mit autorisierenden Quellen. • Bewertungsdaten für fehlende Assets oder Assets ohne Asset-IDs werden nicht importiert. • Wenn ein Testergebnis importiert wird und das entsprechende Asset in Ihrer Instanz nicht abgeglichen werden kann, wird das Testergebnis ignoriert und die ID für das fehlende Asset in einem temporären Datensatz in der Tabelle [sn_vul_tenable_missing_asset] gespeichert. • Der Gesamtwert der ignorierten (fehlenden) Assets wird im Feld **Ignorierte CIs** auf der Registerkarte **Konfiguration** im Integrationsausführungsdatensatz für diese Integration aufgeführt.
Tenable.io Integration der Auffüllung von Compliance-Ergebnissen	• Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Assets-Integration im Rahmen einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. Diese Integration gleicht Konfigurationsbewertungsdaten mit fehlenden Assets ab, die in der Tabelle [sn_vul_tenable_missing_asset] aufgeführt sind. • Importiert bis zu 200 Asset-IDs für fehlende Assets, die erkannt wurden oder in der Instanz vorhanden sind,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	nachdem der Asset-Integrationsimport erfolgreich abgeschlossen wurde. • Entfernt die temporären Datensätze aus der Tabelle [sn_vul_tenable_missing_asset], wenn Assets mit entsprechenden Konfigurationsbewertungsdaten abgeglichen werden können.
Tenable.io Integration von Scan-Anmeldeinformationen	• Diese Integration ruft die in Tenable.iokonfigurierten Scan-Anmeldeinformationen ab. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. • Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_tenable_scan_credential], ausgefüllt sind. • Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von Now Platforminitiiert werden. • Diese Integration soll wöchentlich ausgeführt werden.
Tenable.io Vorlagenintegration	Während des erneuten Scannens wird ein Vorlagendatensatz an Tenable.io gesendet. Diese Integration ruft verfügbare Tenable.io -Anmeldeinformationen ab, um sie für erneute Scans zu verwenden. Anmeldeinformationen sind instanzspezifisch, und ein einzelner Vorlagendatensatz wird importiert und vorübergehend in der Tabelle [sn_vul_tenable_io_template] gespeichert.
Tenable.io Plugin-Integration	• Ruft die Plugin-Daten aus dem Produkt Tenable.io ab. Abgerufene Daten basieren auf dem Datum der letzten Aktualisierung der Plugins durch eine Tenable.io Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.io Bezeichner (10 IDs) aktuell sind. • Koordiniert die REST-Nachrichtenaufrufe an die Plugin-API. • Die Ausgabe dieser Integration sind Schwachstellen von Drittparteien.
Tenable.io Integration behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status **„Offen“** und **„Erneut geöffnet“** befinden, da für diese Datensätze eine Korrektur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	erforderlich ist. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn die Erkennungen **behoben**sind. Angreifbare Elemente werden jedoch standardmäßig nicht für **reparierte** Erkennungen erstellt, da Tenable **behobene** Schwachstellen **als gemindert**betrachtet. • Wenn im Setup-Assistenten die **Kennzeichnung Schwachstellenzeiten für Erkennungen fester Schwachstellen erstellen** aktiviert ist, werden neue AEs im Status **„Fest“** erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. Da VIs für **feste** Erkennungen erstellt werden, die in Ihrer Instanz noch nicht vorhanden sind, kann sich dies negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, sodass **feste** Erkennungen nur die Status vorhandener angreifbarer Elemente aktualisieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration sind **geschlossene/ reparierte** angreifbare Elemente (VIs). Außerdem werden Assets und Einträge von Drittparteien erstellt, falls diese nicht vorhanden sind. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Diese Integrationsausführung ist geplant. Es handelt sich um eine verkettete Integration. Das heißt, nach erfolgreichem Abschluss einer Ausführung wird die unten beschriebene Integration für offene Schwachstellen ausgelöst. Ab Tenable v3.3 können Sie die folgenden Informationen für die ausgeführten Schwachstellenintegrationen anzeigen: • **Blöcke gesamt:** Gesamtanzahl der von Tenable generierten Blöcke • **Verfügbare Blöcke:** Anzahl der zum Download verfügbaren Blöcke für ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
Tenable.io Integration offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss der Tenable.io Integration für behobene Schwachstellen ausgelöst. • Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration sind **Neue/Erneut geöffnete** angreifbare Elemente (VIs). Außerdem werden Konfigurationselemente und Einträge von Drittparteien erstellt, falls sie nicht vorhanden sind. Tenable betrachtet aktive Schwachstellen **als kumulativ** (aktuell). • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Ab Tenable v3.3 können Sie die folgenden Informationen für die ausgeführten Schwachstellenintegrationen anzeigen: • **Blöcke gesamt:** Gesamtanzahl der von Tenable generierten Blöcke • **Verfügbare Blöcke:** Anzahl der zum Download verfügbaren Blöcke für ServiceNow

Tenable.sc Integrationen mit der Anwendung Vulnerability Response

Die Tenable.sc -Integrationen in der Anwendung Vulnerability Response Integration with Tenable

Ab Vulnerability Response v20.0 wird, wenn ein Asset von einem Agent gescannt wird, in der Spalte „Agent vorhanden“ in der Liste Erkannte Elemente der Wert true angezeigt. Dies gibt an, dass es sich um einen echten Scan handelt.

Liste von Tenable.sc Integrationen

Multi-Quelle wird für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können über den Setup-Assistenten in Vulnerability Responsemehrere Instanzen der folgenden Integrationen in Ihrer Umgebung hinzufügen und bereitstellen. Außerdem installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Tenable über den Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID-Server verwenden.

Tenable.sc-Integrationen

Integration	Beschreibung
Tenable.sc Assets Integration	Um zu vermeiden, dass doppelte erkannte Elemente mit importierten Asset-Daten erstellt werden, besteht die Asset-Integration des Produkts Tenable.sc aus zwei Integrationen. **Die Tenable.sc Open Assets-Integration** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable **als kumulativ** (aktuell) oder **offen**betrachtet. Die angreifbaren Elemente (VIs), die in Ihrer -Instanz mit diesen importierten Asset-Daten erstellt werden, gelten als offen, also mit dem Status **Offen**. Diese angreifbaren Elemente müssen untersucht und möglicherweise korrigiert werden. **Tenable.sc Integration von festen Assets** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable als **verringert** (nicht mehr angreifbar) oder **behoben**ansieht. Die angreifbaren Elemente für diese Assets wechseln in Ihrer Instanz vom Status „ **Offen** “ in den Status **„Geschlossen“/ „Repariert“**, da die Ergebnisse der Scans zeigen, dass sie nicht mehr angreifbar sind. • Ruft alle Asset-Daten aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer -Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Assets-API • Die Ausgabe dieser Integration sind erkannte Elemente. • Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für die Tenable.sc Assets Integration. Nur die Assets mit den Schwachstellen, die den Bedingungen des Abfragefilters entsprechen, werden importiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
Tenable.sc Plugin-Integration	• Ruft die Plugin-Daten aus dem Produkt Tenable.sc ab. Abgerufene Daten basieren auf dem Datum der letzten Aktualisierung der Plugins durch eine Tenable.sc Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.sc Bezeichner (10 IDs) aktuell sind und nur aktive Schwachstellen importiert werden. • Koordiniert die REST-Nachrichtenaufrufe an die Plugins-API • Die Ausgabe dieser Integration sind Schwachstellen von Drittparteien.
Tenable.sc Integration behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status **„Offen“** und **„Erneut geöffnet“** befinden, da für diese Datensätze eine Korrektur erforderlich ist. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn die Erkennungen **behoben**sind. Angreifbare Elemente werden jedoch standardmäßig nicht für **reparierte** Erkennungen erstellt, da Tenable **behobene** Schwachstellen **als gemindert**betrachtet. • Wenn im Setup-Assistenten die **Kennzeichnung Schwachstellenzeiten für Erkennungen fester Schwachstellen erstellen** aktiviert ist, werden im Status **„Fest“** neue VIs erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. Da VIs für **feste** Erkennungen erstellt werden, die in Ihrer Instanz noch nicht vorhanden sind, kann sich dies negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, sodass **feste** Erkennungen nur die Status vorhandener angreifbarer Elemente aktualisieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration sind **geschlossene/ reparierte** angreifbare Elemente (VIs). Außerdem werden Assets und Einträge von Drittparteien erstellt, falls diese nicht vorhanden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	Diese Integrationsausführung ist eine geplante Ausführung. Es handelt sich um eine verkettete Integration. Das heißt, nachdem eine Ausführung erfolgreich abgeschlossen wurde, wird die unten beschriebene Tenable.sc Integration offener Schwachstellen ausgelöst. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.
Tenable.sc Integration offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss der Tenable.sc Integration für behobene Schwachstellen ausgelöst. • Ruft Schwachstellendaten basierend auf den im Produkt Tenable.sc ausgewählten Abfragefiltern ab und verarbeitet sie in Ihrer Instanz. • Erstellt entsprechende angreifbare Elemente für aktive Schwachstellen. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Aktualisieren/ Neu erstellen** angreifbare Elemente (VIs), wenn sie noch nicht vorhanden sind. Außerdem werden Konfigurationselemente und Einträge von Drittparteien erstellt, falls sie nicht vorhanden sind. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.
Tenable.sc Integration von Scan-Anmeldeinformationen	• Diese Integration ruft die in Tenable.scKonfigurierten Scan-Anmeldeinformationen ab. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. • Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_tenable_scan_credential] ausgefüllt sind. • Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von Now Platforminitiiert werden. • Diese Integration soll wöchentlich ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung

Tenable.sc Integration von Schwachstellen auffüllen	• Diese Auffüllungsintegration importiert alle offenen und behobenen Schwachstellen, die bei einem Import möglicherweise übersehen wurden.
	• Diese Integration importiert sowohl offene als auch behobene Schwachstellen aus den letzten sieben Tagen, um Ihre Erkennungen und angreifbaren Elemente zu aktualisieren.
	• Diese Integration kann sich auf Ihre Leistung auswirken.
	• Diese Integration ist standardmäßig deaktiviert.
	• Um Ihre Schwachstellendaten zu aktualisieren und potenzielle Leistungsprobleme zu vermeiden, können Sie die Ausführung der Tenable.sc-Integrationen für feste Schwachstellen und offene Schwachstellen zu einem Zeitpunkt planen, zu dem keine anderen Scans ausgeführt werden.
	• Die Ausgabe dieser Integration ist:
	  ○ **Geschlossene/behobene** angreifbare Elemente (VIs). Außerdem werden Assets und Einträge von Drittparteien erstellt, falls diese nicht vorhanden sind.
	  ○ zum **Aktualisieren/Erstellen neuer** angreifbarer Elemente (VIs), wenn sie noch nicht vorhanden sind. Außerdem werden Konfigurationselemente und Einträge von Drittparteien erstellt, falls sie nicht vorhanden sind.

Anwenderauthentifizierung und Tenable.sc

Die Anwenderauthentifizierung wird von Ihrer Instanz Now Platform® und Version 5.13 des Produkts Tenable.sc unterstützt. Wenn Sie Version 5.12 des Produkts Tenable.sc verwenden, ist die Anwenderauthentifizierung erforderlich.

Wenn Sie die Anwenderauthentifizierung für die Tenable.sc -Integrationen auswählen, können Token ablaufen und während der Integrationsausführungen ersetzt werden. In der Spalte „Hinweise“ im Datensatz der Schwachstellenintegrationsausführung (VIN) wird für einen Prozess die folgende Meldung angezeigt, wenn ein Token abläuft: Fehler: Tokenvalidierung ist fehlgeschlagen. Es ist keine Aktion erforderlich, wenn diese Nachricht angezeigt wird. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Nachricht zeigt keine Unterbrechung oder einen Fehler beim Integrationsprozess an.

Vorbereitung der Tenable Vulnerability-Integration

Bereiten Sie sich auf die Integration von ServiceNow® Tenable Vulnerability vor, indem Sie die folgenden Setupaufgaben ausführen.

Bevor Sie beginnen

Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Damit die Installation und Konfiguration der Anwendung Vulnerability

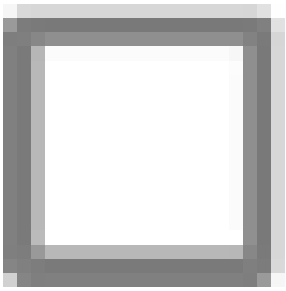
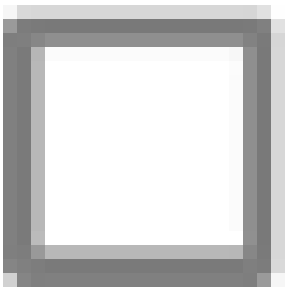
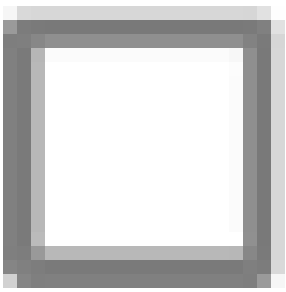
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Response Integration with Tenable reibungslos verläuft, können Sie die folgende Prüfliste ausdrucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in Ihre Instanz Now Platform® importieren.

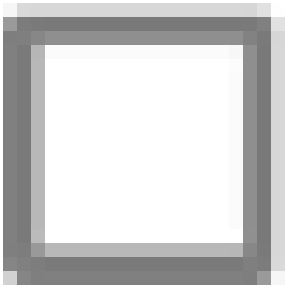
Hinweis:
Wenn Sie Daten mit der in Tenable erstellten -Integration importiert haben und die ServiceNow® Vulnerability Response-Integration mit Tenable verwenden möchten, lesen Sie

Aktuelle Informationen zur Datenbereinigung und Migration von der in Tenable erstellten Integration zur von ServiceNowerstellten Integration finden Sie im Artikel Richtlinien für die Migration von der Tenable-Vulnerability-Response-Integration zur ServiceNow-Vulnerability-Response-Integration mit Tenable [KB0960667] .

Zum Herunterladen und Installieren der Anwendung erforderliche Rolle: admin.

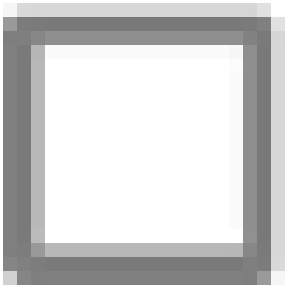
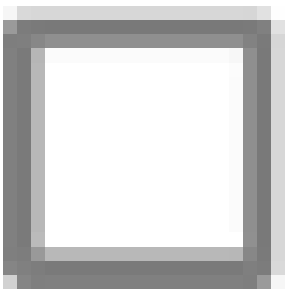
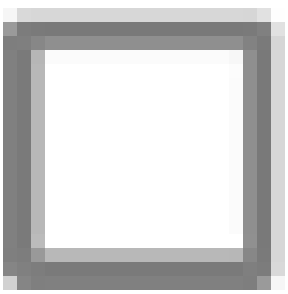
Aufgabe	Beschreibung
	(Optional) Wenn die Anwendung noch nicht installiert und aktiviert ist, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 12.1 von Vulnerability Response oder höher.
	Wenn Sie sie noch nicht in Ihrer -Instanz haben, beschaffen Sie sich Berechtigungen, und laden Sie die Anwendung Vulnerability Response Integration with Tenable auf Ihre Instanz Now Platform® herunter. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13. Weitere Informationen finden Sie unter .
	Schätzen Sie die Anzahl der angreifbaren Elemente, die importiert werden sollen. Stellen Sie sicher, dass Ihre Instanz die Anzahl der angreifbaren Elemente akzeptiert, die Sie importieren werden. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support ServiceNow® von .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn dies nicht zugewiesen ist, weist der Administrator im Setup-Assistenten den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu. **sn_vul.vulnerability_admin** Nach der Zuweisung schließt der Schwachstellen-Administrator die Konfiguration der Tenable-Integrationen ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Konfiguriert alle VR-Anwendungen und Regeln sowie Integrationen von Drittparteien. **sn_vul_tenable.configure_integration** Kann Tenable Vulnerability Integration konfigurieren. Diese Rolle enthält die granulare Rolle sn_vul_tenable.read_integration. **sn_vul_tenable.read_integration** Kann Datensätze der Tenable Vulnerability-Integration anzeigen (lesen). **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen „sn_vul.read_all“ und „sn_vul.remediation_owner“ automatisch. Die erstmalige Zuweisung von Rollen zu Benutzern und Gruppen im Setup-Assistenten für die Integration wird vom Systemadministrator vorgenommen. Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Wenn dies noch nicht geschehen ist, können Sie zusätzliche Gruppen erstellen und Benutzer mit dem Benutzeradministrationsmodul in Ihrer Instanz hinzufügen, bevor Sie den Setup-Assistenten verwenden. Weitere Informationen finden Sie unter Benutzergruppen erstellen . Persona-Rollen und granulare Rollen sind verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Um eine verbesserte Leistung beim ersten Import zu fördern, können Sie bestimmte Funktionen, Regeln oder Aufgaben in Ihrer Instanz deaktivieren. • Deaktivieren Sie die Schwachstellen-Rechner, wenn Sie sie nicht verwenden. Diese Rechner sowie die von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für ein angreifbares Element erstellt oder aktualisiert wird. Weitere Informationen finden Sie unter Schwachstellen-Rechner deaktivieren. • Während des ersten Imports von Datensätzen können bestimmte Benachrichtigungs-Business-Regeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Vor dem ersten Import möchten Sie möglicherweise Benachrichtigungs-Business-Regeln deaktivieren, wie in Importieren Sie Änderungen für die Tenable Vulnerability-Integrationbeschrieben.
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz von aktiviert haben, die für die Integration erforderlich sind. • Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn sich das Produkt Vulnerability Response Integration with Tenable und Ihre Instanz Now Platform in derselben Umgebung befinden. Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID-Server verwenden. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . • Vergewissern Sie sich, dass das IntegrationHub-Plugin installiert und aktiviert ist. Dieses Plugin ermöglicht Basissystemkomponenten das Aufrufen externer Systeme mithilfe von Integrations-APIs und aktiviert Protokollschritte wie REST. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es.
	Rufen Sie die Tenable-Anmeldeinformationen ab. Stellen Sie sicher, dass Sie über alle Accountnamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre Tenable-Produkte erforderlich sind, damit Sie darauf zugreifen können. Tenable.io erfordert Administratorzugriff mit einem Berechtigungsattribut, das größer oder gleich 64 ist. Tenable.sc erfordert Sicherheitsanalysten- oder Managerzugriff.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Hinweis: Ab v3.8 von Vulnerability Response Integration with Tenablesind für den Zugriff auf Tenable.io keine Administratorrechte mehr erforderlich. Ein Standardbenutzer mit einem Berechtigungsattribut gleich 16 kann ebenfalls auf das Produkt zugreifen.

Sie sind bereit für Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten.

Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten

Bevor Sie die ServiceNow® Tenable Vulnerability-Integration ausführen, müssen Sie die Anwendung Vulnerability Response Integration with Tenable von der Anwendung ServiceNow Store herunterladen und mit dem Setup-Assistenten in der Anwendung Vulnerability Response installieren und konfigurieren.

Vorbereitungen

Stellen Sie vor der Installation der Anwendung Tenable sicher, dass Sie alle Elemente in der Prüfliste in Vorbereitung der Tenable Vulnerability-Integrationabgeschlossen haben.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Erforderliche Rolle: admin für die erstmalige Zuweisung der Rolle „sn_vul.vulnerability_admin“ und die Installation der Tenable-Anwendung im Setup-Assistenten. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)), um die Anwendung nach der Installation im Setup-Assistenten zu konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz von verfügbar sind.

2. Suchen Sie die Kachel **Tenable (Tenable-Plattform)**, und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung Vulnerability Response Integration with Tenable installiert, die Sie aus ServiceNow Storeheruntergeladen haben.

3. Befolgen Sie die Eingabeaufforderungen im Setup-Assistenten, um mit der Installation fortzufahren.

4. Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.

Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie im Setup-Assistenten zu **Integrationskonfiguration > Scanner-Integrationen,** um mit der Konfiguration fortzufahren. Weitere Informationen zu den Eingabeaufforderungen im Setup-Assistenten finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufeinstellungen für die Tenable Vulnerability-Integration

Mit den folgenden Einstellungen für den Datenabruf können Sie insbesondere den Typ und Umfang der Daten festlegen, die Sie aus der Tenable-Schwachstellen-Integration ServiceNow® in Ihre Instanz Now Platform® importieren möchten.

Mit den in den folgenden Abschnitten beschriebenen Einstellungen können Sie steuern, welche Daten Sie importieren möchten. Darüber hinaus können Sie die Werte dieser Filter unter Integrationsinstanzen festlegen. Um Integrationsinstanzen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationsinstanzen** und klicken Sie auf Ihre Integration, Tenable.io oder Tenable.sc.

Klicken Sie auf der Seite „Integrationsinstanz“, die angezeigt wird, auf die Option Integrationsinstanzparameter, um eine Liste der Parameter anzuzeigen, oder auf die Registerkarten Schwachstellenintegrationen für einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung.

Allgemeine Einstellungen und Filter für Schweregrad und Abruf für Tenable.io und Tenable.sc in Ihrer Instanz Now Platform .

Die folgenden Einstellungen sind für die Integrationen Tenable.io und Tenable.sc in Ihrer Instanz Now Platform verfügbar. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ Ihrer Instanz Now Platform angezeigt. Unter Umständen möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardwerten belassen.

Tenable.io

insert_fixed

Wenn Sie im Setup-Assistenten die Kennzeichnung **„insert_fixed** “ für die Integration des Imports von Schwachstellen aktivieren, werden neue VIs für Erkennungen im Status **„Fest“** erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

„severe_critical“

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit kritischem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Festgelegte Schwachstellen zu erhalten.

severity_high

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit hohem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

„severe_mittel“

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Festgelegte Schwachstellen zu erhalten.

„severity_info“

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Fest Schwachstellen zu erhalten.

severity_low

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Fest Schwachstellen zu erhalten.

size

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Einstellung definiert die Anzahl der Plugin-Datensätze, die in den Ergebnissatz aus der Tenable.io Plugins-Integration aufgenommen werden sollen. Muss im Format int32 sein. Der Standardwert ist 1.000. Die maximale Größe beträgt 10.000.

num_assets

Die maximale Anzahl von Schwachstellen pro exportiertem Block aus den Integrationen Tenable.io Feste Schwachstellen und Tenable.io Offene Schwachstellen. Der Standardwert ist 50.

chunk_size

Gibt die Anzahl der Assets pro exportiertem Block durch die Tenable.io Assets Integration an. Der Standardwert ist 1.000.

Tenable.sc

async_request

Dieser Parameter ist standardmäßig inaktiv (falsch). Aktivieren oder deaktivieren Sie diesen Parameter, um asynchrone oder synchrone API-Aufrufe mit Tenable.sc durchzuführen. Wenn bei synchronen Aufrufen eine Zeitüberschreitung von 30 Sekunden auftritt, wenden Sie sich an den Support für das Tenable-Produkt, um die Box optimieren zu lassen. Sobald dieser Parameter aktiviert ist, gilt er für alle Integrationen von Tenable.sc. Für Bestandskunden, die asynchrone Anrufe verwenden, ist ein Korrekturskript verfügbar, das den vorhandenen Integrationsinstanzen Tenable.sc einen neuen Parameter „async_request“ hinzufügt. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**.

insert_fixed

Wenn Sie im Setup-Assistenten die Kennzeichnung **„insert_fixed** “ für die Integration des Imports von Schwachstellen aktivieren, werden neue VIs für Erkennungen im Status **„Fest“** erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

Offset

Gibt die Anzahl der Assets, Plugins und Schwachstellen an, die in einer Integrationsausführung importiert werden.

Abfragefilter

Abfragefilter werden in der Tenable-Konsole konfiguriert. Die IDs dieser Abfragefilter können im Setup-Assistenten oder auf der Seite „Integrationsinstanzen“ in Ihrer Instanz Now Platform ausgewählt werden. Diese Filter werden beim Abrufen der Daten aus den Tenable.sc Integrationen angewendet.

REST-Nachrichten für die Tenable-Schwachstellen-Integration

Die ServiceNow® REST-Nachrichten der Tenable-Schwachstellenintegration werden verwendet, um Aufrufe an die Tenable-API zu erstellen.

Tenable.io Assets-REST-Nachricht

Mit der REST-Nachricht „ Tenable.io Assets werden Asset-Informationen für die Tenable.io Asset-Integration abgerufen. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Assets-Informationen aus. Der Exportauftrag für Assets wird mit den folgenden Filtern übermittelt:

- „is_deleted“: falsch
- „is_licensed“: wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io REST-Nachricht für Plugins

Die REST-Nachricht Tenable.io „ Plugins ruft Plugin-Informationen für die Tenable.io Plugin-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Plugin-Informationen aus.

Tenable.io REST-Nachricht zu Schwachstellen

Mit der REST-Nachricht „ Tenable.io Schwachstellen ruft sie Schwachstelleninformationen für offene und geschlossene Schwachstellen aus der Schwachstellenintegration Tenable.io ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Informationen zu Schwachstellen aus.

Tenable.sc fragt die REST-Nachricht ab

Die REST-Nachricht Tenable.sc-Abfragen ruft die Abfragefilterinformationen für die Tenable.sc-Asset-Integration und die Tenable.sc-Schwachstellenintegration ab, für die der Abfragefilter konfiguriert ist.

Tenable.sc REST-Nachricht für Plugins

Die Tenable.sc Plugin-REST-Nachricht ruft Plugin-Informationen für die Tenable.sc Plugins-Integration ab. Änderungen am Datensatz der REST-Nachricht „Plugins abrufen“-Methode wirken sich auf die Anforderungen an Tenable.sc zum Abrufen von Plugins-Informationen aus.

Parametername	Wert	Beschreibung
Typ	aktiv	Gibt an, aus welcher Quelle Tenable Daten abruft. Von Code verwendet. Änderungen werden nicht empfohlen.
Felder	ID, Beschreibung, cvssVector,cvssV3Vector, cvssV3TemporalVector, Übersicht, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, Name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs,family, riskFactor, cpe, sieheAlso, Lösung, ExploitFrameworks, ExploitFrameworks Typ, Copyright, Version, SourceFile, Abhängigkeiten, erforderlichePorts, erforderliche UDP-Ports, srcPort, dstPort,Protokoll, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, VulnPubDate, modifiedTime, md5	Gibt die Liste der aus Tenable importierten Felder an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc REST-Nachricht zu Schwachstellen

Die Tenable.sc Schwachstellen-REST-Nachricht ruft Informationen zu Schwachstellen aus der Tenable.sc Integration ab. Änderungen an der Methode zum Abrufen von REST-Nachrichten zum Abrufen von Schwachstellen oder zum Abrufen von gepatchten Schwachstellen oder, beginnend mit v14.0 Vulnerability Response und v2.2 der Tenable Vulnerability-Integration, am Datensatz „Auffüllung von Schwachstellen abrufen“ wirken sich auf die Anforderungen aus, die an Tenable.sc zum Abrufen von Informationen zu Schwachstellen gestellt werden.

Tenable.sc REST-Nachricht zum Scannen der Anmeldeinformationen

Tenable.sc REST-Nachricht für Richtlinie

Die POST-REST-Nachricht Tenable.sc policy fügt eine Richtlinie für angeforderte Plugins hinzu. Die generierte Richtlinie wird in Scan-Anforderungen für Tenable.sc verwendet.

Tenable.sc REST-Nachricht scannen

Die POST-REST-Nachricht Tenable.sc scan fügt einen Scan hinzu, der vom Zugriff und der Berechtigung abhängt, die im Anforderungstext der REST-Nachricht definiert sind. Es verwendet Richtlinie, Plugin-ID und IP(s) im Anforderungstext für die Scan-Anforderung.

Tenable.sc REST-Nachricht Scan-Ergebnis

Die Tenable.sc Scan-Ergebnis-GET-REST-Nachricht enthält Scan-Details des Scans, der mit der Scan-REST-Nachricht generiert wurde. Verwendet die scanResultId in der Antwort auf die Scan-REST-Nachrichten und ruft Scan-Details für den ausgelösten Scan ab.

Tenable.sc Anmeldeinformationen scannen

Mit der REST-Nachricht zum Scannen der Anmeldeinformationen Tenable.sc werden die Anmeldeinformationen von Tenable.scabgerufen. Änderungen am Datensatz der REST-Nachrichtmethode „Import“ wirken sich auf die Anforderungen aus, die an Tenable.sc zum Abrufen der Anmeldeinformationen gestellt werden.

Parametername	Wert	Beschreibung
Felder	ID, Name, Beschreibung, Typ	Gibt die Liste der Felder an, die aus importiert werden Tenable.sc
Filter	verwendbar	Gibt an, dass die Integration nur verwendbare Anmeldeinformationen aus abruft Tenable.sc Änderungen an einem der Parameter werden nicht empfohlen.

Datentransformation für die Tenable Vulnerability-Integration

Nachdem Sie die zu importierenden Daten identifiziert haben, werden sie vom Tenable-Produkt abgerufen und über eine Reihe von Datenquellen und Transformationen in Ihrer -Instanz verarbeitet.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „Normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen wandeln importierte Tenable-Schweregrade in Standard-Schweregrade zur Verarbeitung in Ihrer Instanz um. Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Vulnerability Response-Schweregradzuordnungen erstellen in der Dokumentation Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Asset-Import

Importierte Asset-Daten werden zuerst in die Tenable.io-Asset-Importtabelle [sn_vul_tenable_io_asset_import] geladen.

Die Tenable.io Asset Integration-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach `Tenable.io Asset Transform`.

In den folgenden Tabellen sind die Transformationszuordnungsfelder nach Integration geordnet.

Tenable.io-Asset-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Tenable bietet eine eindeutige ID für Assets und Zuordnungen zum erkannten Elementdatensatz und wird für die CI-Suche verwendet.
u_ipv4s	ip_address	Ordnet den ersten IP-Wert dem Feld ip_address im Datensatz des erkannten Elements zu.
u_mac_addresses	mac_address	Ordnet den ersten Wert von „mac_address“ dem MAC-Adressfeld im Datensatz des erkannten Elements zu.
u_fqdns	fqdn	Ordnet den ersten FQDN-Wert dem FQDN-Feld im Datensatz des erkannten Elements zu.
u_netBIOS_Names	NetBIOS	Ordnet den ersten NetBIOS-Wert dem NetBIOS-Feld im Datensatz des erkannten Elements zu.
u_operating_systems	os	Ordnet den ersten Betriebssystemwert dem Feld „BS“ im Datensatz des erkannten Elements zu.
(Vor v14.0 Vulnerability Response und v2.2 der Tenable Vulnerability-Integration)u_last_scan_time	last_scan_date	Zuordnung zum Feld „last_scan_date“ im Datensatz des erkannten Elements.
u_last_authenticated_scan_date	last_auth_scan_date	Zuordnung zum Feld „last_auth_scan_date“ im Datensatz des erkannten Elements.
[Skript]	name	Ordnet den Hostnamen mithilfe der Logik des Skripts zu.
u_tags		Die Tags werden in „sn_sec_cmn_host_tag“ gespeichert. Die Zuordnung von Tags zu Assets wird in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Asset-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
		„sn_sec_cmn_m2m_src_ci_tag“ gespeichert.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Timing und Zweck des Skripts für die Tenable.io-Asset-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Eine Funktion, die verwendet wird, um Werte auf dem Host zu aktualisieren und zu überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Importsatz. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Integration von Tenable.io-Plugins

Die Transformationszuordnung für Tenable.io-Plugins wird zum Transformieren von aus Tenable.io importierten Plugins verwendet.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Art und Weise, wie von den Tenable-Plugins empfangene Daten verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach dem Tenable.io-Plugin Transformieren.

Die Nutzlast der Plugins „tenable.io“ enthält alle Felder in der Spalte „u_attributes“ der Tabelle sn_vul_tenable_io_plugin_import. Das Feld „Attribute“ wird analysiert und den Datensätzen der Drittpartei-Eintragstabelle zugeordnet, wie in der folgenden Tabelle aufgeführt.

Quellenfeld	Zielfeld	Beschreibung
id	id	Ordnet die ID der Quelle zu und fügt ihr das Präfix TEN- hinzu. Wenn beispielsweise die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.
Beschreibung	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Die Quelle für importierte TPE ist Tenable.io.
[Skript]	source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
Familie	Kategorie	Ordnet die Plugin-Familie der Kategoriespalte zu
plugin_modification_date	last_modified	Ordnet „plugin_modification_date“ dem zuletzt geänderten Feld zu.
plugin_publication_date	date_published	Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu.
has_patch	remediation_type	Ordnet den Korrekturtyp dem has_patch-Wert zu.
synopsis	Bedrohung	Ordnet die Bedrohungsinformationen für diese Schwachstelle zu.
cvss_base__score	Punktzahl	Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
solution	solution	Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu.
Exploit_available	Exploit	Ordnet den vom Scanner bereitgestellten Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu
vpr.Punktzahl	source_risk_score	Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu.
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		• 4 – 7 – Mittel • 0–4: Niedrig
vpr.drivers.age_of_vuln	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner der Spalte „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.exploit_code_maturity	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.product_coverage	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner den Bedrohungsquellen in der Drittparteitabelle zu.
vpr.drivers.threat_intensity_last28	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.
vpr.drivers.threat_recency	Threat_recency	Ordnet die Bedrohungsaktualitätsinformationen vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Ordnet die cvss3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
cvss_temperal_score	cvss_temperal_score	Ordnet die temporäre Punktzahl für CVSS v2 zu.
cvss_v3_template_score	v3_zeitlich_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
risk_factor	source_severity	Entspricht dem Quellschweregrad in der Drittpartei-Eintragstabelle.
name	name	Ordnet den Namen des Plugins einem Namen in der Drittpartei-Eintragstabelle zu.
stig_severity	stig_severity	Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu.
plugin_type	check_type	Ordnet den Plugin-Typ „check_type“ in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
unsupported_by_vendor	unsupported_by_vendor	Ordnet das Feld „unsupported_by_vendor“ der Spalte „unsupported_by_vendor“ zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.

Zusätzlich zu den direkten Feldern werden Drittparteieinträgen weitere Informationen als zugehörige Listen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie unter „sn_vul_m2m_entry_cve“.
bid	Die Liste der Fehler-Traqs wird als Referenz hinzugefügt.
siehe_also	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Eine Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Drittanbietereintrag. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Die TenableIOPluginsImportProcessor-Skripteinbindung wird vom onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe der Tenable.io-Plugin-Integration und wandelt sie in Now Platform Schwachstelleneinträge von Drittparteien um. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.io-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

Tenable.io-Schwachstellenimport

Die Tenable.io-Transformationszuordnung für angreifbare Elemente wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus Tenable.io importiert wurden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Art und Weise, wie Daten aus dem Import von Tenable-Schwachstellen verarbeitet werden.

Die gleiche Transformationszuordnung wird für die Tenable.io-Integration für feste Schwachstellen und die Tenable.io-Integration für offene Schwachstellen verwendet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Transformationszuordnung für angreifbare Tenable.io-Elemente.

Quellenfeld	Zielfeld	Beschreibung
u_asset.uuid	id	Uuid wird dem ID-Feld des cmdb_ci-Datensatzes zugeordnet.
u_asset.ipv4	ip_address	Das Feld ipv4 wird dem IP-Adressfeld des cmdb_ci-Datensatzes zugeordnet.
u_asset .last_authenticated_results	last_auth_scan_date	Das Datum des letzten authentifizierten Scans wird dem Datum des letzten Authentifizierungsscans des cmdb_ci-Datensatzes zugeordnet.
u_asset.mac_address	mac_address	Die MAC-Adresse wird dem Host-MAC-Adressfeld des Datensatzes „cmdb_ci“ zugeordnet.
u_asset.netBIOS_Name	NetBIOS	NetBIOS wird dem NetBIOS-Feld des cmdb_ci-Datensatzes zugeordnet.
u._plugin.cvss3_base_score	v3_base_score	Die CVSS v3-Basispunktzahl wird der v3-Basispunktzahl des Drittpartei-Eintragsdatensatzes zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u._plugin.cvss3_template_score	v3_zeitlich_Punktzahl	Die temporäre CVSS v3-Punktzahl wird der v3 Temporary-Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u._plugin.cvss_base_score	Punktzahl	Die CVSS-Basispunktzahl wird dem Punktzahlfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u._plugin.cvss_template_score	temporal_score	Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_plugin.description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_plugin.family	Kategorie	Ordnet die Plugin-Familie der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu.
u_plugin.modification_date	last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittparteieintrags zugeordnet.
u_plugin.publication_date	date_published	Das Veröffentlichungsdatum wird dem Feld „Veröffentlichungsdatum“ des Drittpartei-Eintragsdatensatzes zugeordnet.
u_plugin.risk_factor	source_severity	Der Risikofaktor wird dem Feld „source_severity“ des Drittpartei-Eintragsdatensatzes zugeordnet.
u_plugin.solution	solution	Die Lösung wird dem Lösungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u_plugin.synopsis	Bedrohung	Die Synopse wird dem Bedrohungsfeld des Drittpartei-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Eintragsdatensatzes zugeordnet.
u_severity_id	Priorität	Die Priorität wird der Schweregrad-ID aus der Nutzlast zugeordnet. Der Standardwert ist 5.
u_plugin.exploit_available	Exploit	Ordnet den vom Scanner bereitgestellten Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
vpr.Punktzahl	source_risk_score	Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu.
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch • 4 – 7 – Mittel • 0–4: Niedrig
u_plugin.vpr.drivers.age_of_vuln	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.exploit_code_maturity	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.product_coverage	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner Bedrohungsquellen in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.threat_intensity_last28	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_plugin.vpr.drivers.threat_recency	Threat_recency	Ordnet die Informationen zur Bedrohungsaktualität vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Ordnet die CVSS3 v3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
u_plugin.type	check_type	Ordnet den Plugin-Typ „check_type“ in der Drittpartei-Eintragstabelle zu.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Ordnet das Feld „unsupported_by_vendor“ im Plugin der Spalte „unsupported_by_vendor“ zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.
u_plugin.family_id	Family_id	Ordnet die Plugin-Familien-ID der Spalte „family_id“ in der Drittpartei-Eintragstabelle zu.
port	port	Der Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
protocol	protocol	Das Protokoll wird dem Protokollfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_first_found	first_found	„Zuerst gefunden“ wird dem Feld „Zuerst gefunden“ des Datensatzes des angreifbaren Elements zugeordnet.
u_last_found	last_found	„Zuletzt gefunden“ wird dem Feld „Zuletzt gefunden“ des Datensatzes des angreifbaren Elements zugeordnet.
u_state	state	Der Status wird dem Feld „Status“ im Datensatz des angreifbaren Elements zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die Quelle der aus dieser Integration erstellten angreifbaren Elemente ist Tenable.io.
[Skript]	integration_instance	„integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_plugin.name	name	Ordnet den Namen des Plugins einem Namen in der Eintragstabelle einer Drittpartei zu.
u_plugin.stig_severity	stig_severity	Ordnet den STIG-Schweregrad des Plugins der Spalte „STIG-Schweregrad“ in der Drittpartei-Eintragstabelle zu

Zusätzlich zu den direkten Feldern werden Drittparteieinträgen weitere Informationen als zugehörige Listen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie unter „sn_vul_m2m_entry_cve“.
bid	Die Liste der Fehler-Traqs wird als Referenz hinzugefügt.
siehe_also	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation löst den TenableIOVulnerabilitiesProcessor aus, der Daten aus Tenable.io mithilfe des Importsatzes importiert und jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle der angreifbaren Elemente und die Schwachstellentabelle der Drittpartei lädt.Zur internen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	Verwendung. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Eine Funktion zum Überprüfen, ob der Drittpartei-Eintrag und die Erkennungen bereits vorhanden sind. Andernfalls werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Anzahl der CIs, VIs und Erkennungen zu aktualisieren, wie sie aus Tenable.io importiert wurden. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Tenable.sc-Asset-Import

Aus Tenable.sc importierte Asset-Daten werden zuerst in die Tabelle „Tenable.sc-Asset-Import“ (sn_vul_tenable_sc_asset_import) geladen. Die Transformationszuordnung Tenable.sc Asset Integration wird zum Transformieren der importierten Asset-Informationen verwendet. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach Tenable.sc Asset Transformieren.

Quellenfeld	Zielfeld	Beschreibung
u_uuid	id	uuid wird nicht von der Tenable-API ausgefüllt, daher wird das Attribut „u_uniqueness“ verwendet, um ein eindeutiges uuid-Feld für Assets zu erstellen und es dem cmdb_ci-Datensatz zuzuordnen.
u_ip	ip_address	Ordnet das IP-Feld aus der API dem Feld „ip_address“ in einem cmdb_ci-Datensatz zu.
u_macaddress	mac_address	Ordnet das Feld „macaddress“ aus der API dem Adressfeld im Datensatz „cmdb_ci“ zu.
u_dnsname	fqdn	Ordnet das Feld „dnsname“ aus der API dem Feld „fqdn“ im Datensatz „cmdb_ci“ zu.
u_netBIOSName	NetBIOS	Ordnet das NetBIOS-Feld aus der API dem NetBIOS-Feld im cmdb_ci-Datensatz zu.
u_oscpe	os	Die BS-Informationen werden aus dem Attribut oscpe in der Nutzlast extrahiert und dem Feld os im Datensatz cmdb_ci zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_lastauthrun	last_auth_scan_date	Ordnet das Feld „lastauthrrun“ aus der API dem Feld „last_auth_scan_date“ im Datensatz des erkannten Elements zu.
u_lastauthrun und u_lastunauthrun	last_scan_date	„lastauthrun“ wird aus der Tenable-API oder „lastunautrun“ extrahiert. Je nachdem, welcher Wert in der Nutzlast angezeigt wird, wird das Feld „last_scan_date“ im Datensatz des erkannten Elements gefüllt.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Funktion, die verwendet wird, um die Werte auf dem Host zu aktualisieren und zu überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Importsatz. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Import von Tenable.sc-Plugins

Aus Tenable.sc importierte Plugins-Daten werden zuerst in die Tabelle „Tenable.sc-Plugin-Import“ (sn_vul_tenable_sc_plugin_import) geladen. Die Tenable.sc-Plugin-Transformationszuordnung wird verwendet, um die importierten Plugin-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Plugin-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Tenable.sc-Plugin-Transformationszuordnung.

Quellenfeld	Zielfeld	Beschreibung
u_id	id	Ordnet die ID aus der Quelle zu und fügt das Präfix TEN- hinzu. Wenn beispielsweise die empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_description	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Das aus dieser Integration importierte TPE hat Tenable.sc als Quelle.
[Skript]	source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
u_family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte zu.
u_plugin_modification_date	last_modified	Ordnet „plugin_modification_date“ dem zuletzt geänderten Feld zu.
u_plugin_publication_date	date_published	Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu.
u_has_patch	remediation_type	Ordnet den Korrekturtyp dem has_patch-Wert zu.
u_synotisi	Bedrohung	Ordnet die Bedrohungsinformationen für diese Schwachstelle zu.
u_cvss_base_score	Punktzahl	Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
u_solution	solution	Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu.
u_cvss_temperal_score	cvss_temperal_score	Ordnet die temporäre Punktzahl für CVSS v2 zu.
u_cvss_v3_template_score	v3_zeitlich_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
u_risk_factor	Quellenschweregrad	Entspricht dem Quellschweregrad in der Drittpartei-Eintragstabelle.
u_cvss_v3_base_score	v3_base_score	Ordnet die CVSS-Basispunktzahl in der Drittpartei-Eintragstabelle zu.
u_exploit_available	Exploit	Ordnet das vom Scanner bereitgestellte ExploitAvailable der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
u_vpr_score	source_risk_score	Ordnet die VPR-Punktzahl vom Scanner der Quellrisiko-Punktzahl in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch • 4 – 7 – Mittel • 0–4: Niedrig
u_vpr_context[id=age_of_vuln]	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=exploit_code_maturity]	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=product_coverage]	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_sources_last_28”]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner zu „bedrohten Quellen“ in der Drittparteitabelle zu.
u_vpr_context[id=”threat_intensity_last_28”]	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_recency”]	Threat_recency	Ordnet die Informationen zur Bedrohungsaktualität vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Ordnet die CVSS v3-Auswirkungspunktzahl vom Scanner zu „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
u_name	name	Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu.
u_stig_severity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Eintragstabelle der Drittpartei zu.
u_check_type	check_type	Ordnet den Schecktyp „check_type“ in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_family.id	family_id	Ordnet das Plugin „family_id“ dem Plugin „family_id“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.

Zusätzlich zu den direkten Feldern werden Drittparteieinträgen weitere Informationen als zugehörige Listen hinzugefügt.

Quellenfeld	Beschreibung
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_see_also	Die Liste der URLs wird als Referenz hinzugefügt.
u_exploit_frameworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Drittanbietereintrag. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von erstellten und ignorierten Plugins festzulegen. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Die TenableSCPluginsImportProcessor-Skripteinbindung wird vom onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe aus der Tenable.sc-Plugin-Integration und wandelt sie in ServiceNow-Schwachstelleneinträge von Drittparteien um. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.sc-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Import von Tenable.sc-Schwachstellen

Die Transformationszuordnung Tenable.sc Open Vulnerabilities wird zum Transformieren importierter Daten aus der Tenable.sc-Integration für offene Schwachstellen verwendet, und die Transformationszuordnung Tenable.sc und behobene Schwachstellen wird zum Transformieren importierter Daten aus der Tenable.sc-Integration für feste Schwachstellen verwendet.

Hinweis:
Änderungen an diesen Transformationszuordnungen ändern die Art und Weise, wie Daten aus dem Import fester/offener Tenable-Schwachstellen verarbeitet werden.

Um auf die Transformationszuordnungen für offene und feste Schwachstellen von Tenable.sc zuzugreifen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationsinstanzen** > **Integration fester/offener Tenable.sc-Schwachstellen** > **Datenquellen** > **Offene/behobene Schwachstellen in Tenable.sc** > **Transformiert**.

Quellenfeld	Zielfeld	Beschreibung
u_pluginID	ID	Wird als Bezeichner für das Plugin verwendet. Dieses Feld ist der Plugin-ID im Datensatz des Drittparteieintrags zugeordnet.
u_riskfactor	source_severity	Dieses Feld ist „source_severity“ im Drittpartei-Eintragsdatensatz zugeordnet.
u_severity	Priorität	Das Prioritätsfeld ist dem Schweregrad zugeordnet. Der Standardwert ist 5.
u_hasbeenmitigated	state	Wurde dem Statusfeld des Schwachstellen-Datensatzes zugeordnet. Bei der Integration mit behobenen Schwachstellen befinden sich alle AEs im Status „Geschlossen“.
u_ip	ip_address	Die IP-Adresse wird dem Host-IP-Feld der Tabelle „cmdb_ci“ zugeordnet.
u_port	port	Der Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_protocol	protocol	Das Protokoll wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_firstSeen	first_found	Der erste erkannte Wert wird dem ersten gefundenen Feld des VI-Datensatzes zugeordnet.
u_lastSeen	last_found	Der zuletzt erkannte Wert wird dem zuletzt gefundenen Feld des VI-Datensatzes zugeordnet.
u_exploitVerfügbar	Exploit	ExploitAvailable wird dem Exploit-Feld im Drittpartei-Eintragsdatensatz zugeordnet.
u_synotisi	Bedrohung	Die Synopse wird dem Bedrohungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_solution	solution	Die Lösung wird dem Lösungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_basescore	Punktzahl	BaseScore wird dem Punktzahlfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_temperalPunktzahl	temporal_score	Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_cvssv3basescore	v3_base_score	Cvssv3basescore wird der v3-Basispunktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_cvsstemperalScore	v3_zeitlich_Punktzahl	Die Cvssv3-Punktzahl wird der temporären v3-Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_pluginpubdate	date_published	Das Plugin-Veröffentlichungsdatum wird dem Plugin-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Veröffentlichungsdatum im Drittpartei-Eintragsdatensatz zugeordnet.
u_pluginmoddate	last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittparteieintrags zugeordnet.
u_dnsname	fqdn	DnsName wird dem FQDN-Feld des cmdb_ci-Datensatzes zugeordnet.
u_macaddress	mac_address	„MacAddress“ wird dem Feld „mac_address“ des Datensatzes „cmdb_ci“ zugeordnet.
u_netBIOSName	NetBIOS	NetBIOSName wird dem NETBIOS-Feld des cmdb_ci-Datensatzes zugeordnet.
u_ip	ip	IP wird dem IP-Feld des cmdb_ci-Datensatzes zugeordnet.
hostUniqueness	uuid	Die Eindeutigkeit des Hosts wird keinem Feld zugeordnet, sondern wird verwendet, um uuid für den Host zu bestimmen.
u_family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu.
u_plugintext	Nachweis	Plugin-Text wird dem Nachweis im TPE-Datensatz zugeordnet.
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die Quelle der angreifbaren Elemente, die aus dieser Integration erstellt werden, ist Tenable.sc.
[Skript]	integration_instance	„integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_vpr_score	source_risk_score	Ordnet die VPR-Punktzahl vom Scanner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		der Quellrisiko-Punktzahl in der Drittpartei-Eintragstabelle zu.
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch • 4 – 7 – Mittel • 0–4: Niedrig
u_vpr_context[id=age_of_vuln]	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=exploit_code_maturity]	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=product_coverage]	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_sources_last_28]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner Bedrohungsquellen in der Drittparteitabelle zu.
u_vpr_context[id=”threat_intensity_last_28]	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_recency”]	Threat_recency	Ordnet die Informationen zur Bedrohungsaktualität vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Ordnet die CVSS v3-Auswirkungspunktzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		vom Scanner zu „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
u_pluginname	name	Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu.
u_stigseverity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Eintragstabelle der Drittpartei zu.
u_checktype	check_type	Ordnet den Schecktyp „check_type“ in der Drittpartei-Eintragstabelle zu.
u_family.id	family_id	Ordnet das Plugin „family.id“ dem Plugin „family_id“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Tabelle „ third_party_entry“ wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.

Quellenfeld	Beschreibung
u_cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie unter sn_vul_m2m_entry_cve.
u_bieten	Die Liste der Fehler-Traqs wird als Referenz hinzugefügt.
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_seealso	Die Liste der URLs wird als Referenz hinzugefügt.
u_xrefs	Die Liste der X-REFs wird als Referenz hinzugefügt.
u_exploitframeworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Funktion, die verwendet wird, um die Werte in der Schwachstelle zu aktualisieren und zu überprüfen, ob die Schwachstelle bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einer Tabelle angreifbarer Elemente. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten VIs und von VIs, die aktualisiert und ignoriert wurden, festzulegen. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Legen Sie zusätzliche Filterparameter für Tenable.io -Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Tenable Vulnerability Integration an, um die mit dem Produkt Tenable.io importierten Schwachstellendaten weiter zu verfeinern.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, um nur bestimmte Schwachstellendetails überprüfen zu können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach `cidr_range`, `num_assets`, `indexed_at`und `plugin_family`gefiltert werden. Oder Sie möchten eine Tenable.io -Integration so ausführen, dass eine Ausführung alle vier Stunden nur kritische Schwachstellen importiert und eine andere alle 24 Stunden ausführt, um alle anderen nicht kritischen Schwachstellen abzurufen.

Um diese Daten beim Sammeln dieser Daten zu unterstützen, können Sie von Tenable unterstützte Parameter hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Mit dieser Funktion können Sie Ihre HTTP-Anforderungsinformationen mit Tenable-Parametern in Now Platformanpassen, ohne zusätzliche API-Aufrufe oder Codierung hinzuzufügen. Die folgenden Tenable.io Integrationen unterstützen die Filterung durch Bereitstellung von JSON-Inhalten im Anforderungstext:

- Assets Integration
- Integration behobener Schwachstellen
- Integration offener Schwachstellen

Sie sollten wissen, wie JSON -Zeichenfolgen für diese Funktion verwendet werden.

Erforderliche Rolle: sn_vul.vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Suchen Sie die vom Produkt Tenable.io unterstützten Parameter auf der Entwickler-Site, die Sie für die Filterung verwenden möchten.

   Parameter und Werte, die Sie aus dem Produkt Tenable.io eingeben, werden nur auf Ebene der Integrationsinstanz unterstützt.

2. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
3. Klicken Sie auf der Listenseite „Tenable Integrations“ (Tenable-Integrationen) auf den Datensatz für die Integration Tenable.io, die Sie öffnen möchten.
4. Klicken Sie bei ausgewählter Registerkarte Tenable-REST-Methoden auf das Informationssymbol (I) für die REST-Methode und anschließend auf **Datensatz öffnen**.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Um den Datensatz zu bearbeiten, klicken Sie oben auf der Seite auf den Link in. Um den Datensatz zu bearbeiten, klicken Sie **hier**.
7. Geben Sie im Datensatz REST-Methode im Feld Inhalt den JSON-Inhalt ein, der Teil des Anforderungstexts sein soll.

   Beispielsweise können Sie den Schweregradparameter für importierte Schwachstellen für die Tenable.io Assets-Integration auf `{"filters": {"severity": ["critical"]}}` festlegen, damit nur kritische Schwachstellen importiert werden (CVSS-Punktzahl 10,0).

   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Tenable.io weitere Informationen zum Trennen der einzelnen Werte.

8. Klicken Sie auf **Aktualisieren**.

Berichterstellung für Tenable Vulnerability Integration

Zeigen Sie Berichte über Schwachstellen und angreifbare Elemente in den Dashboards Vulnerability Response an.

Datenvisualisierungen in den -Arbeitsbereichen Vulnerability Response .

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad aktiver Schwachstellen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen anzeigen, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.

Vorherige Versionen von Vulnerability Response

Das Übersichts-Dashboard für Vulnerability Response (Schwachstellenmanagement) bietet eine Ausführungsansicht für Schwachstellen und angreifbare Elemente, damit der Schwachstellenadministrator Problembereiche schnell erkennen kann. Das Vulnerability Response-Nachbesserungsdashboard (Nachbesserung von Schwachstellen) ermöglicht Nachbesserungsspezialisten, sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren, für die sie verantwortlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..

Erforderliche Rolle: Korrekturbesitzer.

Persona-Rollen und granulare Rollen sind verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Um das Dashboard anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Korrekturübersicht**.

Statusdiagramm der Integrationsausführung für die Tenable-Schwachstellen-Integration

Das Modul „Tenable Integration Run Status“ (Status der Tenable-Integrationsausführung) bietet Ihnen eine grafische Ansicht des Status der Tenable-Integrationsausführungen.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein Teil des Balkendiagramms klicken, wird eine Liste mit detaillierteren Informationen geöffnet.

Erforderliche Rolle: Schwachstellen-Administrator

Persona-Rollen und granulare Rollen sind verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

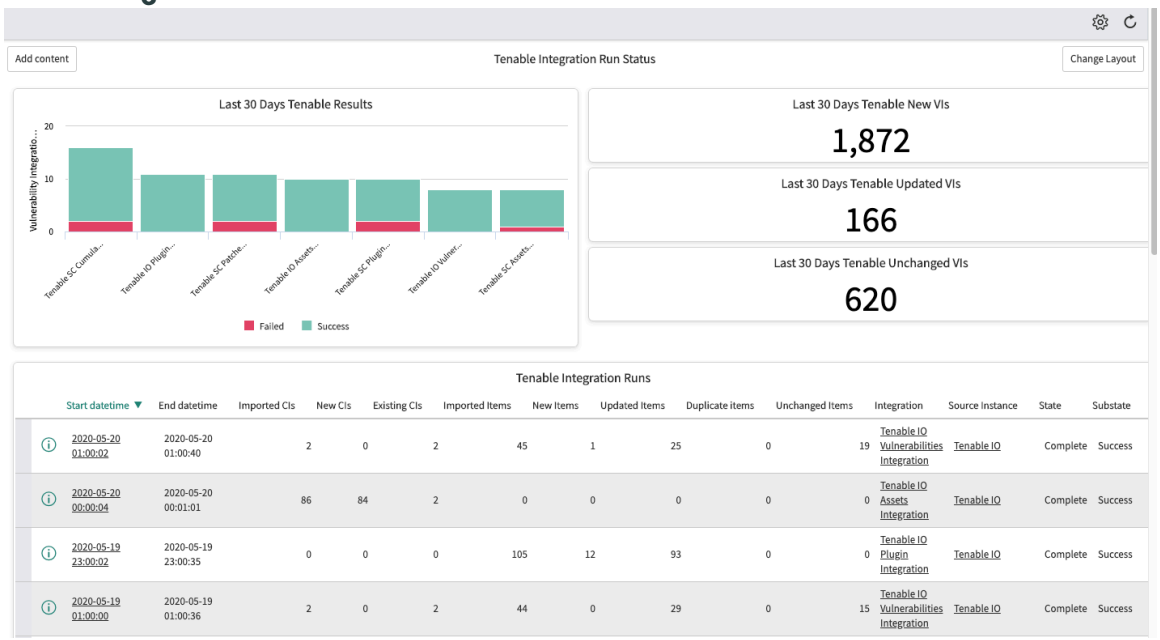
Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausführungsstatus



Diagrammberichte zum Status der Tenable-Integrationsausführung

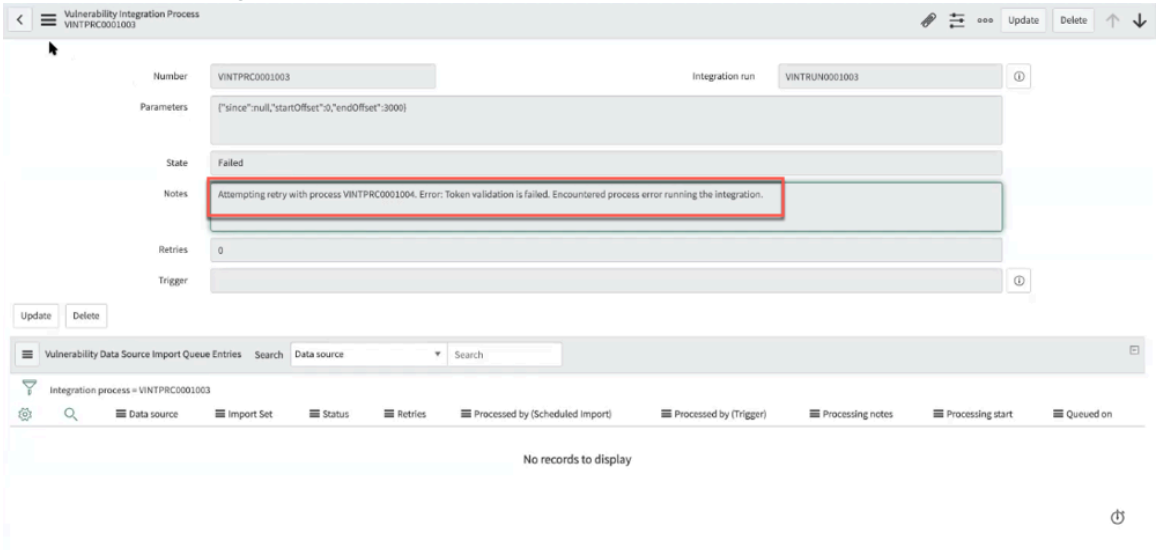
Name	Beschreibung
Tenable-Ergebnisse der letzten 30 Tage	Die Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Jede Ausführung wird als Balken im Diagramm angezeigt.
Neue Tenable-VIs der letzten 30 Tage	Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Aktualisierte Tenable-VIs der letzten 30 Tage	Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Unveränderte Tenable-VIs der letzten 30 Tage	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Tenable-Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle *sn_vul_detection*. Während die Integration ausgeführt wird, ändert sich möglicherweise die Anzahl der Erkennungen oder Ergebnisse. In diesem Bericht wird die Anzahl der Erkennungen in der Spalte „Anzahl bis Datum“ in der Instanz nach Abschluss der Integrationsausführung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ablauf der Tokenvalidierung

Wenn eine Tenable.sc-Integrationsausführung aus irgendeinem Grund fehlschlägt, läuft das Authentifizierungstoken für Tenable.sc automatisch ab, und im Datensatz des Vulnerability-Integrationsprozesses wird eine Meldung angezeigt.

Nachricht über abgelaufenes Token



Für den nächsten Integrationsprozess wird automatisch ein neues Token generiert. Alle Integrationsprozesse – fehlgeschlagen und erfolgreich – werden auf der Registerkarte Vulnerability Integration Process (Schwachstellenintegrationsprozess) im Datensatz „Schwachstellenintegrationsprozess“ angezeigt.

Initiieren Sie den erneuten Scan für die Tenable.sc -Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie erneut Scans auf der Tenable-Plattform initiieren. Sie können bei Bedarf von Ihrer Instanz Now Platform® aus einen erneuten Scan auf angreifbare Elemente für das Produkt Tenable.sc initiieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.write_all oder sn_vul.write_assigned

Hinweis:
Tenable.sc bietet keine Unterstützung für das erneute Scannen auf Agent-basierten Computern.

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum erneuten Scannen über -Arbeitsbereiche finden Sie unter Scannen Sie die angreifbaren Elemente Tenable.io und Tenable.sc aus den Arbeitsbereichen Vulnerability Response erneut.

Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Um den Aufwand und das Volumen zu reduzieren, die mit geplanten, vollständigen Scans verbunden sind, können Nachbesserungsbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen für Assets (Konfigurationselemente) in ihren Umgebungen initiieren.
Sie können erneute Scans von angreifbaren Elementen (VIs), Korrekturaufgaben (RTs),

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Drittparteieinträgen (TPE) oder von Datensätzen erkannter Elemente in Ihrer Instanz Now Platform initiieren.

Durch erneute Scans können Ihre für die Korrektur Verantwortlichen und Schwachstellenanalysten überprüfen, ob Ihre Korrekturaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben haben.

Beispielsweise wird Ihre gesamte Umgebung alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Now Platform für angreifbare Elemente vom Typ Tenable.sc initiieren.

Hinweis:

Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.sc Integration für Scan-Anmeldeinformationen importiert und aktualisiert die Scanner-Anmeldeinformationen aus dem Produkt Tenable.sc in Ihrer -Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationen zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten. Die ServiceNow® Tenable.sc Integration zum Scannen von Anmeldeinformationen wird automatisch über den Setup-Assistenten in Ihrer Instanz aktiviert (Aktiv), wenn Sie die Integrationen für Tenable.sc Schwachstellen (Tenable.sc Integrationen offener und fester Schwachstellen) konfigurieren.

Beachten Sie die folgenden Informationen zu den Anmeldeinformationen, die Sie importieren, damit Ihre Benutzer sie bei Bedarf aus Ihrer Instanz Now Platform anzeigen können:

- Mit der -Administrator-Anwenderrolle Tenable.sc erstellte Anmeldeinformationen sind für Anwender in allen Ihren Organisationen verfügbar.
- Mit der Organisationsbenutzerrolle Tenable.sc erstellte Anmeldeinformationen sind nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in den Now Platform importiert, es sei denn, sie werden für den Account des Benutzers freigegeben, der für die Verbindung mit der Instanz verwendet wird.

Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.sc.

Weitere Informationen zum Konfigurieren der Anwendung Tenable.sc finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten. Um weitere Informationen zur Integration der Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Integrationen** > **Integration von Tenable.sc-Scan-Anmeldeinformationen**.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, von dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Sie können erneute Scans nur für VIs mit Tenable.sc als Quelle initiieren. Überprüfen Sie, ob Tenable.sc in der Spalte **„Quelle“** in den VI-Listenansichten oder in den Feldern **„Quelle“** in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol **Liste personalisieren** (Zahnradsymbol), und verwenden Sie den Slushbucket, um **die Quelle** von **Verfügbar** in **Ausgewählt**zu verschieben.

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Korrekturaufgabe bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die Schaltfläche **Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem Produkt Tenable.sc stammen und sich in einem anderen Status als **Geschlossen befinden**. Bei mehreren VI-Datensätzen müssen alle VIs aus dem Tenable.sc-Produkt stammen und sich in einem anderen Status als **Geschlossen befinden**.
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem beliebigen anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Tenable.sc stammen.
   - In einem TPE-Datensatz (Drittparteieintrag) muss der Datensatz über mindestens einen zugeordneten VI-Datensatz aus dem Produkt Tenable.sc in einem anderen Status als **Geschlossen**verfügen.

4. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie werden aufgefordert, die Scanner-Anmeldeinformationen für den Zugriff auf den Scanner auszuwählen. Dies sind die Anmeldeinformationen, die von der Tenable.sc Integration mit Scan-Anmeldeinformationen importiert werden.

5. Wählen Sie im Dialogfeld die gewünschten Filter und Anmeldeinformationstypen aus.
6. Klicken Sie auf **Scan anfordern**.

Es wird eine Nachricht angezeigt, die anzeigt, dass Ihre Prüfung verarbeitet wird. Der Status für alle erneut gescannten Elemente kann jederzeit unter den zugehörigen Scan-Listen in den VI-, RT- und TPE-Datensätzen gefunden werden, mit denen Sie die erneut gescannten Elemente gestartet haben. Klicken Sie in der Nachricht **auf Details anzeigen**, um den Status des erneuten Scans und alle anderen von einem bestimmten Datensatz gestarteten erneuten Scans anzuzeigen.

Das Feld „Status“ im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt). Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde. Alle AEs, die in den Status „ **Geschlossen“/„Behoben“** übergegangen sind oder werden, werden mit dem nächsten geplanten Import der Tenable.sc-Integration für feste Schwachstellen importiert.

Initiieren Sie den erneuten Scan für die Tenable.io -Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie erneut Scans auf der Tenable-Plattform initiieren. Sie können bei Bedarf von Ihrer Instanz Now Platform® aus einen erneuten Scan auf angreifbare Elemente für das Produkt Tenable.io initiieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.write_all oder sn_vul.write_assigned

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

Warum und wann dieser Vorgang ausgeführt wird

- Siehe und Scannen Sie Datensätze und Korrekturaufgaben im erneut Vulnerability Manager Workspace und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace, um in den Vulnerability Response-Arbeitsbereichen einen erneuten Scan zu initiieren.
- Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Hinweis:
Tenable.io bietet keine Unterstützung für das erneute Scannen auf Agent-basierten Computern.

Um den Aufwand und das Volumen geplanter, vollständiger Scans zu reduzieren, können Sie als Besitzer der Remediation, IT-Spezialist, Schwachstellenanalyst oder Schwachstellenmanager bei Bedarf gezielte erneute Scans initiieren. können Sie Assets (Konfigurationselemente) in Ihren Umgebungen auf bestimmte Schwachstellen scannen. Sie können erneute Scans aus Datensätzen von angreifbaren Elementen (VI),

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgaben (VUL), Drittparteieinträgen (TPE) oder erkannten Elementen (SDI) in der Instanz Now Platform initiieren. Durch erneute Scans können Sie überprüfen, ob durch Ihre Nachbesserungsaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben wurden.

Hinweis:
Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.io Integration für Scan-Anmeldeinformationen importiert und aktualisiert die Scanner-Anmeldeinformationen aus dem Produkt Tenable.io in Ihrer -Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationen zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten.

Im Folgenden werden die Anmeldeinformationen beschrieben, die Sie importieren, damit Ihre Benutzer sie je nach Bedarf aus Ihrer Instanz Now Platform sehen können:

- Mit der -Administrator-Anwenderrolle Tenable.io erstellte Anmeldeinformationen sind für Anwender in allen Ihren Organisationen verfügbar.
- Mit der Organisationsbenutzerrolle Tenable.io erstellte Anmeldeinformationen sind nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in den Now Platform importiert, es sei denn, sie werden für den Account des Benutzers freigegeben, der für die Verbindung mit der Instanz verwendet wird.

  Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.io.

- Die Tenable.io Template Integration und die Tenable.io Scan Credential Integration müssen aktiviert werden, bevor erneute Scans initiiert werden können. Um weitere Informationen zur Integration der Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationen** > **Integration von Tenable.io Scan-Anmeldeinformationen**.

  Standardmäßig sind die Integrationen für Vorlagen- und Scan-Anmeldeinformationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für Tenable.ioeingeben, werden alle Tenable.io Integrationen automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

  1. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
  2. Suchen Sie in der angezeigten Liste nach den Tenable.io Integrationsdatensätzen, die Sie benötigen.
  3. Öffnen Sie jeden Datensatz, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren.
  4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
  5. Kehren Sie zum Setup-Assistenten zurück, um mit der Konfiguration für Tenable Vulnerability Integration mit Vulnerability Responsefortzufahren.

Weitere Informationen zum Konfigurieren der Produkte Tenable.io und Tenable.sc finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten.

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Now Platform für angreifbare Elemente vom Typ Tenable.io initiieren.

Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration behobener Schwachstellen initiiert haben.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, von dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

Hinweis:
Wenn Sie den Scanner Tenable.io verwenden, können Sie erneute Scans für VIs nur mit Tenable.io als Quelle initiieren. Überprüfen Sie, ob Tenable.io in der Spalte **„Quelle“** in den VI-Listenansichten oder in den Feldern **„Quelle“** in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol **Liste personalisieren** (Zahnradsymbol), und verwenden Sie den Slushbucket, um **die Quelle** von **Verfügbar** in **Ausgewählt**zu verschieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Datensätze, die Sie für den erneuten Scan verwenden möchten.

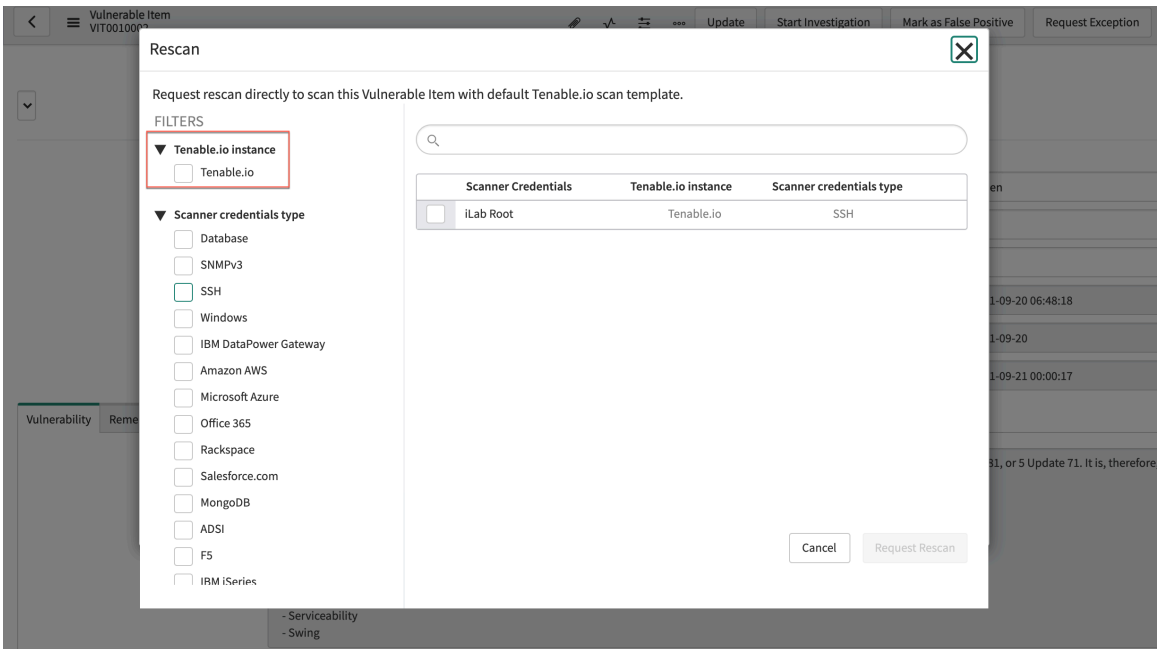
   Abhängig von Ihrer Auswahl ist die Schaltfläche **Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss sich das VI in einem anderen Status als **„Geschlossen“**befinden. Bei mehreren VI-Datensätzen müssen alle VIs aus dem Produkt Tenable.io stammen und sich in einem anderen Status als **Geschlossen befinden**.
   - Für Korrekturaufgaben-Datensätze werden nur Korrekturaufgaben in einem anderen Status als **„Geschlossen“** unterstützt. Alle zugeordneten VIs müssen sich in einem anderen Status als **„Geschlossen“** befinden und Tenable.io als Quelle verwenden.
   - In einem TPE-Datensatz (Drittparteieintrag) muss der Datensatz über mindestens einen zugeordneten VI-Datensatz aus dem Produkt Tenable.io in einem anderen Status als **Geschlossen**verfügen.
   - Bei Datensätzen erkannter Elemente muss dem Datensatz mindestens ein VI-Datensatz aus dem Produkt Tenable.io in einem anderen Status als **„Geschlossen“**zugeordnet sein.
   - In der Liste „Angreifbare Elemente“ können Sie einzelne angreifbare Elemente auswählen, die Sie erneut scannen möchten. Verwenden Sie das Menü Aktionen für ausgewählte Zeilen unten links im Bildschirm, um den erneuten Scan zu starten. Sie werden aufgefordert, Ihre Anmeldeinformationen einzugeben.

4. Klicken Sie oben rechts in einem Datensatz **auf Erneut scannen**.
   Sie werden aufgefordert, die Instanz(en) für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind diejenigen, die von der Tenable.io Integration zum Scannen von Anmeldeinformationen importiert wurden.

5. Wählen Sie im Dialogfeld die Instanz und/oder Instanzen und die Anmeldeinformationstypen aus, die Sie verwenden möchten.

   In der folgenden Abbildung ist eine Integrationsinstanz, Tenable.io, zu sehen. Wenn Sie mehr als eine Instanz Tenable.io haben, werden sie alle im Abschnitt „Tenable.io“ im Formular angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Erneutes Scannen anfordern**.

   Es wird eine Nachricht angezeigt, die anzeigt, dass Ihr Scan verarbeitet wird und ein übergeordneter Scan-Datensatz erstellt wird. Der Status für alle untergeordneten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, Korrekturaufgaben-, TPE- und SDI-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht **auf Details anzeigen**, um den Status des erneuten Scans und alle anderen von einem bestimmten Datensatz gestarteten erneuten Scans anzuzeigen.

   Das Feld „Status“ im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Jeder Scan unterstützt eine eindeutige Kombination aus Integrationsinstanz, TPE, IP und Netzwerk-ID. Möglicherweise werden in einem übergeordneten Scan-Datensatz mehrere untergeordnete Scans angezeigt. Beispiel: Die maximale Anzahl von IP-Adressen, die ein untergeordneter Scan unterstützen kann, beträgt 1000. Wenn für ein angreifbares Element 1002 IPs vorhanden sind, werden zwei untergeordnete Scans erstellt und in der zugehörigen Liste „Scans“ aufgeführt, um die Anforderung zu unterstützen. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans, und sein Status spiegelt den Status der untergeordneten Scans wider.

   Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt). Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde. Alle AEs, die in **den Status „Geschlossen“/ „Behoben“** überführt wurden oder werden, werden mit dem nächsten geplanten Import der Tenable.io Integration behobener Schwachstellen importiert.

   Bei Scans, bei denen ein Fehler auftritt, können Sie die untergeordneten Scans im übergeordneten Scan-Datensatz überprüfen. Zeigen Sie den Fehler in der Antwortnutzlast des untergeordneten Scans an.

   Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration behobener Schwachstellen initiiert haben.

Aktualisieren Sie Configuration Items mit dem Netzwerkpartitionsbezeichner für Tenable Vulnerability Integration

Erstellen Sie eindeutige Configuration Items (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um weitere Details zu Ihren Schwachstellen zu erhalten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig können Sie Ihre Assets in der Anwendung Vulnerability Response anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch in Ihrer CMDB als ein CI gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie in den folgenden Tabellen gezeigt, können beispielsweise mehrere Assets (CI) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, verfügen jedoch über eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche in der Regel als einzelnes CI (CI 1) identifiziert und gespeichert.

Standardmäßige IP-Suche und CI-Erstellung

Quelle	IP-Adresse	Network_id	Konfigurationselement
Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	Repository-ID	Konfigurationselement
Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse aufweisen, um sie als unterschiedliche Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die geplante Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzu. Von der IRE erstellte vorhandene CIs werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Wenn Sie ein Upgrade ab v14.0 von Vulnerability Response und v2.2 der Tenable-Schwachstellenintegration durchführen, werden die CMDB-CI-Klassenmodelle (1.0.21.) unterstützt. Die -Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

Option	Beschreibung
Geplante Aufgaben bei Bedarf ausführen.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Tenable-Daten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartitionsbezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und

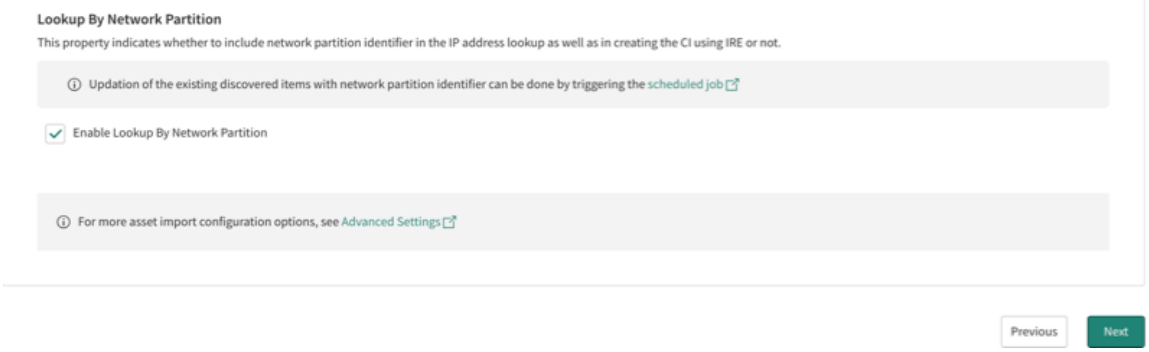
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Option	Beschreibung
	Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.
Warten Sie mit den nächsten geplanten Aufgaben auf Importe neuer Daten aus den Integrationen.	Erstellen Sie CIs für jedes neue Asset unter Verwendung des Netzwerkpartitionsbezeichners, beginnend mit der nächsten geplanten Aufgabe. CI, angreifbares Element und Erkennungsdatensätze werden mit der neuen Granularität aktualisiert. Neue CIs werden erstellt, wenn keine exakte Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Tenable.io integrations oder Tenable.sc integrations (Integrationen) aus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Auswahlvorgang **Konfiguration des Asset-Imports**.
5. Auswahlvorgang **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen aus **Suche nach Netzwerkpartition aktivieren** Abschnitt.



6. Klicken Sie auf **Next (Weiter)**.

Die Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY _ID sind enthalten und aktualisieren vorhandene CIs oder erstellen CIs mit der nächsten geplanten Aufgabe.

Bezeichnerattribut der Netzwerkpartition, das in die IP-Suche und CI-Erstellung einbezogen wird

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI2

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI2

Mit der nächsten geplanten Aufgabe fügen die Suchregeln für IP-Adresse und unvollständige IP-Adressen-CI-Identifizierung das Attribut für den Netzwerkpartitionsbezeichner für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc automatisch hinzu.

Nachdem Sie die Systemeigenschaft aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie die geplanten Aufgaben bei Bedarf starten.

Importieren Sie Änderungen für die Tenable Vulnerability-Integration

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Importintegration für Tenable-Schwachstellen in der Tenable-Schwachstellen-Integration ServiceNow®.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Gruppe von Aufgaben erfordert Programmierkenntnisse und fortgeschrittene Kenntnisse über Now Platform.

Führen Sie diese Schritte aus, um domänengetrennte Importe für die Tenable Vulnerabilities-Integrationen zu erstellen. Das folgende Beispiel bezieht sich auf die Integration „Tenable.io Open Vulnerabilities“, der Inhalt gilt jedoch auch für die anderen Tenable-Integrationen.

Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede von Ihnen erstellte Domäne einen Anwender, und weisen Sie ihn dieser Domäne zu.

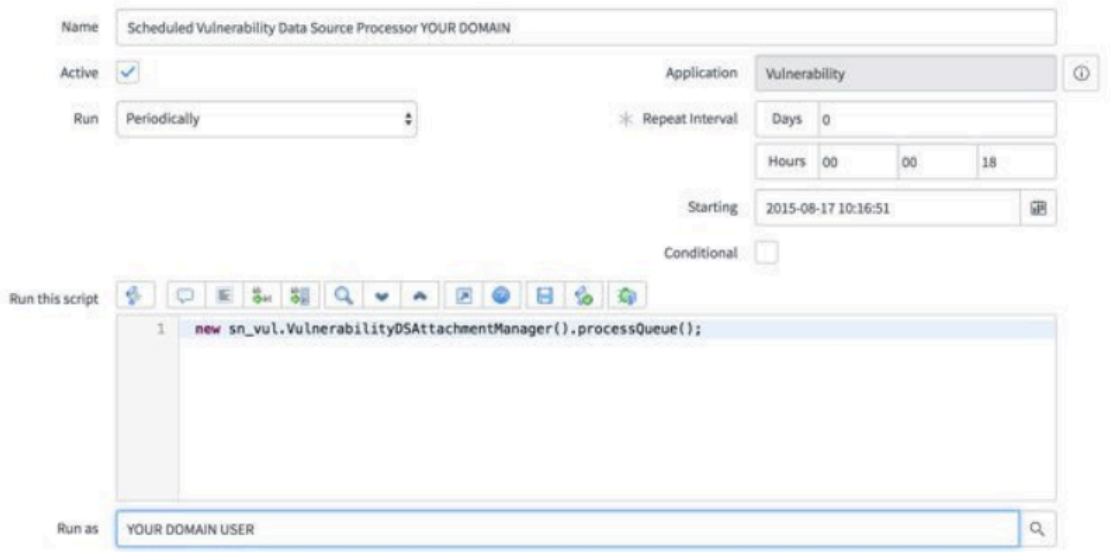
   Stellen Sie sich diesen Benutzer als run_as-Platzhalter für die Domäne in Tenable.io vor.
3. Integration offener Schwachstellen.
   Der -Benutzer entspricht dem VR.System-Benutzer in der globalen Domäne und muss die folgenden Rollen aufweisen: sn_vul.tenable_configure_integration, import_admin und sn_vul.vulnerability_write. Dieser Anwender benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   Hinweis:
   Betrachten Sie diesen Anwender als spezifisch für diese Rolle. Der Anwender darf keinen anderen Zweck haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie in jeder Domäne eine geplante Aufgabe, indem Sie den Prozessor für die geplante Schwachstellen-Datenquelle kopieren, den Sie unter finden **Systemdefinition** > **Geplante Aufgaben**.
5. Fügen Sie die Domäne an den Namen an, um die geplante Aufgabe zu identifizieren.
6. Ändern Sie den Benutzer run_as in den Benutzer, den Sie im vorherigen Schritt erstellt haben.

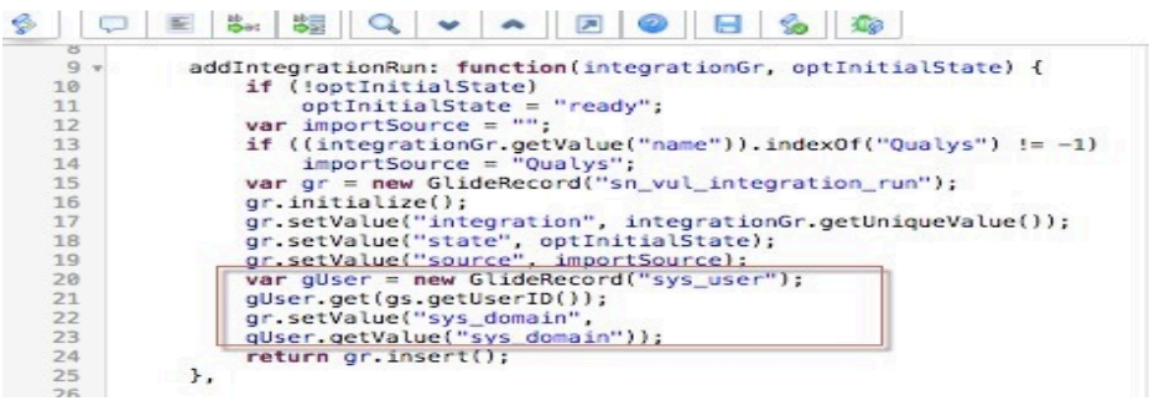
Hinweis:
Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Benutzerdomäne run_as ausgeführt wird.



7. Bearbeiten Sie die UI-Aktion „Jetzt ausführen“ in der Tenable.io Open Vulnerabilities-Integration, um diesen Codeblock am Anfang der Datei hinzuzufügen.
```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Hinweis:
Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in der Benutzerdomäne „run_as“ ausgeführt wird.

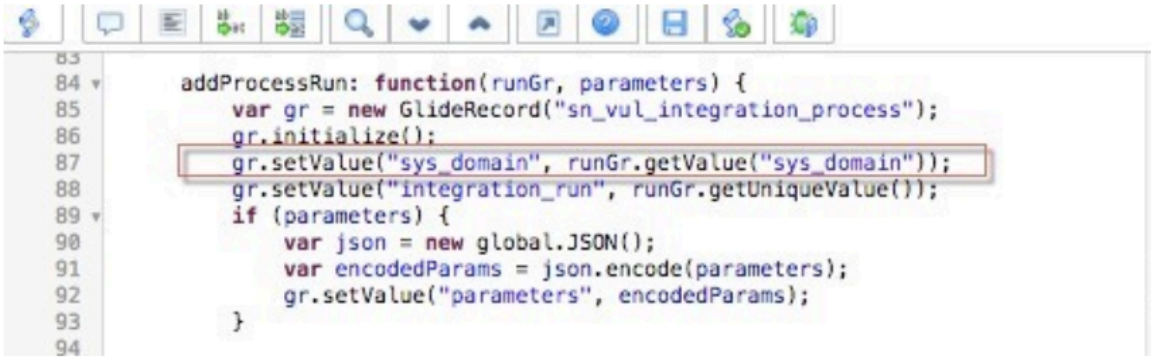
8. Bearbeiten Sie die Skripteinbindungsmethode addIntegrationRun für VulnerabilityIntegrationUtils, um den hervorgehobenen Code hinzuzufügen.



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Bearbeiten Sie die Skripteinbindungsmethode addProcessRun für VulnerabilityIntegrationUtils, um den hervorgehobenen Code hinzuzufügen.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Bearbeiten Sie die DataSourceVulnReportRefreshProcessor-Skripteinbindungsmethode _processFromDataSourceGroups, um diesen ursprünglichen Code zu ändern: Ursprünglicher _processFromDataSourcesGroups-Code in Bearbeiteter _processFromDataSourcesGroups-Code.
11. Bearbeiten Sie die Skripteinbindungsmethode VulnerabilityDSAttachmentManager, queueItem, um die folgenden hervorgehobenen Codeblöcke hinzuzufügen: queueItem, _getNext, _processQueueEntry.

Sie sind bereit für Importe der domänengetrennten Hosterkennung.

Rechner vor dem Import deaktivieren

Befolgen Sie diese Schritte, um den Standardrechner zu deaktivieren, wenn er nicht verwendet wird. Wenn Sie keine Schwachstellen-Rechner verwenden, deaktivieren Sie am besten die Standard-Rechner zusätzlich zu den anderen, die Sie definiert haben. Sicherheitsrisiko-Rechner werden jedes Mal ausgeführt, wenn auf den Datensatz eines angreifbaren Elements zugegriffen wird, und können sich auf die Leistung der Instanz auswirken.

Erforderliche Rolle: sn_vul.vulnerability_admin.

12. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellen-Rechner**.
13. Öffnen Sie die Gruppe „Schwachstellenauswirkung“.
14. Öffnen Sie den Rechner für punktzahl- und servicebasierte Auswirkung.
15. Deaktivieren Sie das Feld Aktiv, um den Rechner zu deaktivieren.
16. Klicken Sie auf Aktualisieren.

Sie haben den Standardrechner deaktiviert.

Deaktivieren Sie auf Benachrichtigungen basierende Business-Regeln vor dem ersten Import

Befolgen Sie diese Schritte, um Benachrichtigungsbezogene Business-Regeln vor dem ersten Datensatzimport zu deaktivieren. Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln viele Benachrichtigungen generieren, was sich auf die Leistung auswirkt. Diese Business-Regeln müssen geändert werden, um sie während des Imports zu deaktivieren.

Erforderliche Rolle ist sn_vul.vulnerability_admin.

17. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
18. Suchen Sie nach betroffenen CI-Benachrichtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

19. Öffnen Sie die Geschäftsregel, und fügen Sie die folgende Bedingung ein: `current.sys_class_name != “sn_vul_vulnerable_item"`.
20. Klicken Sie auf **Aktualisieren**.
21. Wiederholen Sie dieses Verfahren für die folgenden Geschäftsregeln:
    - Benachrichtigungen für betroffene Kostenstellen
    - Betroffene Gruppenbenachrichtigungen
    - Benachrichtigungen zum betroffenen Standort

Hinweis:
Nach Abschluss des ersten Datensatzimports können Sie diese Business-Regeln erneut aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und sich auf die Leistung Ihrer Instanz auswirken.

Ändern Sie ein anfängliches Startdatum

Führen Sie diese Schritte aus, um ein anfängliches Startdatum zu ändern. Während der Installation legen Sie mit dem Setup-Assistenten ein anfängliches Startdatum für die Tenable-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen, wie in den folgenden Schritten gezeigt.

22. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
23. Klicken Sie auf eine beliebige Integration.
24. Klicken Sie auf Integrationsdetails.
25. Legen Sie das Feld Startzeit auf einen Wert in der Vergangenheit fest, damit alle seit dieser Zeit gescannten und erkannten Schwachstellen erkannt werden.

    Wenn Sie Tenable mit dem Setup-Assistenten konfiguriert haben, ist das Feld Startzeit vorab ausgefüllt, zunächst bis drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum. Hinweis: Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass große Datenmengen die Tenable-API-Quotenbeschränkungen überschreiten und Ausführungszeitüberschreitungen ausgelöst werden.

26. Klicken Sie auf **Absenden** oder **Aktualisieren**.
27. **Wahlweise:** Klicken Sie auf **Jetzt ausführen**, um die Ausführung sofort zu starten.

Tenable-Erkennungen basierend auf der Schwachstelleninstanz aufteilen, um angreifbare Elemente aufzuteilen

ServiceNow® Vulnerability Response ermöglicht die Aufteilung von Erkennungen von Tenable-Scannern, wodurch für jede erkannte Schwachstelleninstanz ein spezifisches angreifbares Element (Unique VIT) erstellt werden kann. Diese Aufteilung ermöglicht die Zuweisung von VITs zu verschiedenen Nachbesserungsteams, wodurch die Verwaltung und Nachverfolgung von Schwachstellen verbessert wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Nutzlast des Tenable-Scanners enthält Erkennungsdaten, wobei jeder Pfad innerhalb des Nachweises zur Aufteilung der Erkennungen verwendet wird. Das Ausgabe-Tag in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutzlast gibt den Ort der Schwachstelle an und erleichtert so die genaue Identifizierung und Verwaltung von Schwachstellen entsprechend ihren spezifischen Pfaden.

Prozedur

1. Legen Sie in der Tabelle „Drittparteiintegrationen“ [sn_sec_int_integration] den Wert **Nachweis in VI-Schlüsselspalte einschließen** für Tenable.io und Tenable.scauf true fest.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.
3. Aktivieren Sie im Formular „Port einbeziehen“ das Kontrollkästchen **Port einbeziehen**, und wählen Sie den Link **Hier klicken**.
4. Wählen Sie in der Liste Nachweis zu VI-Schlüssel hinzufügen die **Option Neu**aus.
5. Fügen Sie im Formular „Nachweis zum VI-Schlüssel hinzufügen – Neuer Datensatz“ im Feld **Schwachstelle** die Tenable-ID hinzu, für die Sie den Nachweis einschließen möchten.

   Hinweis:
   Sie können die Erkennungen nur basierend auf Pfadinformationen oder durch Kombination von Pfad- und Versionsdetails aufteilen. Weitere Informationen finden Sie im Abschnitt „Erkennungen von Tenable-Scannern aufteilen“ auf dieser Seite.

6. Im Feld **Regulärer Ausdruck zur Aufteilung von Tenable-VITs** :
   - Teilen Sie die Erkennung nur basierend auf dem Pfad auf, indem Sie Pfad\s+:\s+([A \n]+) eingeben.
   - Teilen Sie die Erkennung basierend auf dem Pfad sowie den installierten und festen Versionen auf, indem Sie Pfad\s+:\s+([A\n]+)\n\s+linstalliert\s+version\s+:\s+([A\n]+) eingeben. \n\s+Repariert\s+Version\s+:\s+([A\n]+).
7. Wählen Sie **Absenden**.

Example: Erkennungen von Tenable-Scannern aufteilen

Die folgende Erkennung von einem Tenable-Scanner zeigt im Ausgabe-Tag einen Nachweis, der sowohl Pfad- als auch Versionsinformationen enthält.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                     "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                "tracked": true


            "output": "In                    C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                    Path
            "plugin":
                "bid":
                    123456


                "checks_for_default_account": false,
               "checks_for malware": false,

                 "coe":
                "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"


                 "cvSs3_base_score": 7.8,
                "cvss3 temporal score": 7.0,

                "cvss3_temporal_vector": {
                    "exploitability": "Proof-of-Concept",
                    "remediation level": "Official Fix",
                     "report_confidence": "Confirmed",
                     "raw": "E: P/RL:0/RC: C"
```


Integration von Atlassian Jira mit Vulnerability Response

Die Atlassian Jira -Integration mit Vulnerability Response ermöglicht Ihnen die Nutzung verschiedener Problemverfolgungs- und Agile-Verwaltungstools für die Nachverfolgung von Maßnahmen zur Nachbesserung von Schwachstellen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht

ServiceNow® Vulnerability Response ist in Atlassian Jira integriert, um Probleme zu erstellen, die Schwachstellen entsprechen, und synchronisiert die Problementität in Jira und die Entität des angreifbaren Elements in Vulnerability Response bidirektional, um die neuesten Updates widerzuspiegeln. Schwachstellenmanager erfordern, dass in ServiceNow Vulnerability Response vorhandene Schwachstellenelemente erstellt und den Nachbesserungsbenutzern (Entwicklern im Fall von Application Vulnerability Response) in ihrem bevorzugten Datensatzsystem und Problem-Management-Tool wie Atlassian Jirazugewiesen werden. Jeder Fortschritt, der für die Schwachstellen im Problemmanagement-Tool erzielt wurde, sollte in ServiceNow Vulnerability Response aktualisiert werden, damit er für Schwachstellenmanager sichtbar ist. Darüber hinaus müssen alle von Schwachstellenmanagern in Vulnerability Response vorgenommenen Aktualisierungen für angreifbare Elemente an das Problem-Management-Tool weitergegeben werden, damit die Transparenz für Nachbesserungsbenutzer gewährleistet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response	Versionshinweise zur Integration von Vulnerability Response
Vulnerability Response und Configuration Compliance für Container	Versionshinweise zu Container Vulnerability Response
Jira-Spoke	Versionshinweise zur Jira-Spoke

Jira Schwachstellen-Integrationen

Um die Jira Vulnerability-Integration anzuzeigen, navigieren Sie zu **Alle** > **Agile-Management für VR** > **Agile-Tools konfigurieren** .

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig nicht alle aktiv.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um die Integrationen automatisch der Reihe nach auszuführen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Vorbereitung der Jira Vulnerability Response -Integration

Eine erfolgreiche Jira Vulnerability-Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Die Jira Vulnerability Response -Integration setzt voraus, dass Sie mit dem Produkt und der API Jira vertraut sind.

Mit Agile Integration for Vulnerability Response und Jira Integration for Vulnerability Response installierte Komponenten

Bei der Aktivierung des Plugins „Agile Integration for Vulnerability Response“ und „Jira Integration for Vulnerability Response“ werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Anwenderrollen.

Installierte Rollen

Rollentitel [name]	Beschreibung
Agile-Tool-Administrator [sn_vul_agile.agile_tool_admin]	Ermöglicht die Erstellung einer Konfigurationsregel für Agile Management, um Probleme zu erstellen oder zu aktualisieren. Erstellen Sie Regelkonfigurationen für Agile Management.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen (Fortsetzung)

Rollentitel [name]	Beschreibung
JIRA-Administrator [sn_vul_jira.admin]	Ermöglicht die Auswahl des Agile-Tools, um Probleme für die ausgewählte Entitätstabelle zu erstellen.

Installierte Tabellen

Tabelle	Beschreibung
Agile-Tool-Konfiguration [sn_vul_agile_tool_rule_config]	Enthält Konfigurationsregeln zum Erstellen von Problemen auf der Agile-Plattform.
Agile-Tool-Feldzuordnung [sn_vul_agile_tool_field_mapping]	Enthält die Feldzuordnung der Konfigurationsregel.
Zuordnung des Agile-Tool-Status [sn_vul_agile_tool_state_mapping]	Enthält die Statuszuordnung des Jira-Problemstatus mit dem Status „Angreifbares Anwendungselement“, „Angreifbares Container-Element“, „Anwendungskorrekturaufgabe“ und „Container-Korrekturaufgabe“.
Agile-Tool-Manifest [sn_vul_agile_tool_manifest]	Enthält die Nutzlast für die Problemerstellung.
Agile-Tool-Datenressource [sn_vul_agile_tool_data_resource]	Enthält die Informationen zum erstellten Jira-Problem.
JIRA-Administrator [sn_vul_jira.admin]	Ermöglicht die Auswahl des Agile-Tools, um Probleme für die ausgewählte Entitätstabelle zu erstellen.

Installieren Sie Vulnerability Response Integration mit Jira

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Jira ordnungsgemäß in Application Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Erforderliche Rolle: admin.

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	• Jira Integration for Vulnerability Response erfordert die Anwendung Vulnerability Response. • Stellen Sie für die aktuelle Version von Jira Integration for Vulnerability Response sicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben. Weitere Informationen finden Sie unter KB0856498 – Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen. • Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass das Integration Hub-Plugin installiert ist.	• Für Jira Spoke ist Integration Hub erforderlich. • Informationen zur Installation von Integration Hub finden Sie in KB1112383. • Weitere Informationen finden Sie unter Gesetzliche Zeitpläne für IntegrationHub – Übersicht.
Stellen Sie sicher, dass die neueste Version von Jira Spoke installiert ist.	Informationen zur Installation von Jira Spoke finden Sie in KB0792632.
Vergewissern Sie sich, dass Vulnerability Response Integration with Agile Management installiert ist.	Vulnerability Response Integration with Atlassian Jira erfordert diese Integration.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie die -Integration Jira Vulnerability Response installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Vulnerability Response integration with Jira.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Konfigurieren Sie Regeln in der Agile-Tool-Konfiguration

Jira -Probleme werden auf der Plattform Jira erstellt, wenn die in Angreifbares Anwendungselement, Angreifbares Container-Element, Anwendungskorrekturaufgabe und Container-Korrekturaufgabe erstellten Datensätze mit den in der Agile-Tool-Konfiguration erstellten Regeln übereinstimmen.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin.

Prozedur

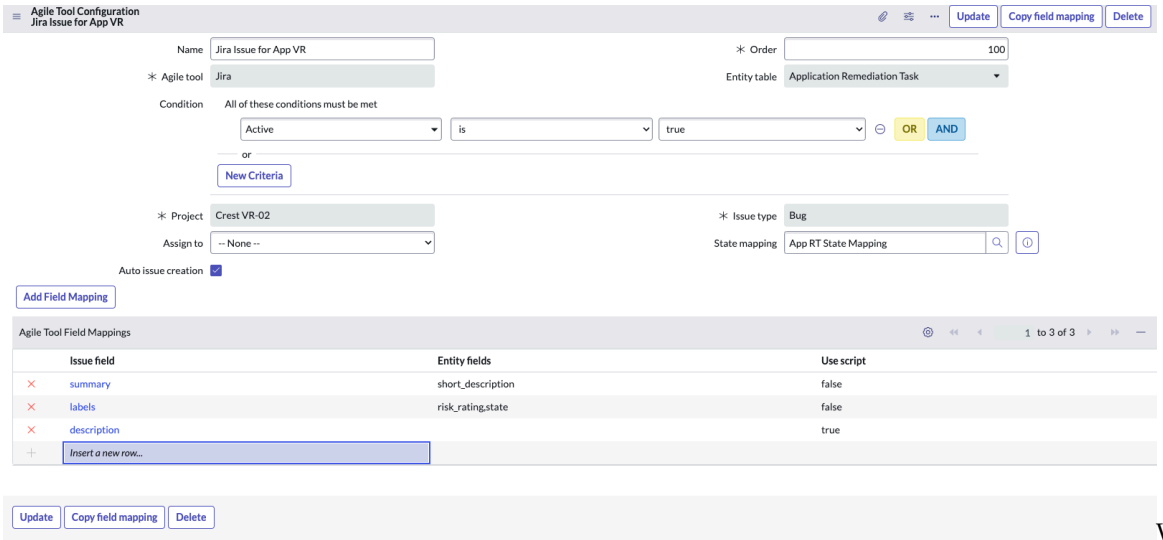
1. Navigieren zu **Alle** > **Agile-Management für VR** > **Agile-Tools konfigurieren**.
2. Um eine neue Konfigurationsregel in der Agile-Tool-Konfiguration zu erstellen, wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular zur Konfiguration des Agile-Tools

Feld	Beschreibung
Name	Name der Agile-Tool-Konfiguration.
Bestellung	Reihenfolge der Agile-Tool-Konfiguration.
Agile-Tool	Das Agile-Tool zum Erstellen von Problemen auf der spezifischen Agile-Plattform.
Entitätstabelle	Tabelle, auf die die Konfigurationsregel angewendet werden soll.
Bedingung	Filterbedingung in der ausgewählten Entitätstabelle, um Probleme auf der Agile-Plattform zu erstellen.
Automatische Problemerstellung	Die Konfigurationsregel wird abgefragt, wenn in der ausgewählten Entitätstabelle ein neuer Datensatz erstellt wird (nur dann, wenn das Kontrollkästchen aktiviert ist). **Hinweis:** Der Anwender muss die Listenaktion verwenden, um Probleme für vorhandene Entitätsdatensätze zu erstellen.
Projekt	Das Projekt, in dem das Jira-Problem erstellt wird.
Problemtyp	Der Typ des Problems, das in einem bestimmten Projekt erstellt werden soll.
Zuweisen an	Der Beauftragte, dem das Problem beim Erstellen des Problems zugewiesen werden soll. Damit die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erstellten Probleme nicht zugewiesen bleiben, wählen Sie „Keine“ aus.
Statuszuordnung	Die vorhandenen Statuszuordnungen aus der Tabelle „Agile-Tool-Statuszuordnung“ oder erstellen eine neue Statuszuordnung zwischen dem Problemstatus in der agilen Plattform und den Status der Entitätstabelle ServiceNow.



Wenn die Anwendung installiert ist, werden Anwendungskorrekturaufgabe und Container-Korrekturaufgabe standardmäßig im Feld Entitätstabelle im Formular „Agile-Tool-Konfiguration“ angezeigt.

4. Um das angreifbare Anwendungselement und das angreifbare Container-Element in der Auswahlliste „Entitätstabelle“ hinzuzufügen, navigieren Sie zu **„Systemeigenschaften“** > **„sn_vul_agile.tablesToShow“**, und fügen Sie alle im Feld „Wert“ hinzu.

Formular für Systemeigenschaften

Feld	Beschreibung
Auswahlmöglichkeiten	Durch Kommas getrennte Werte für eine Auswahlliste.
Wert	Legen Sie den gewünschten Wert für die Eigenschaft fest. Alle Eigenschaftswerte werden als Zeichenfolgen gespeichert. Wenn Sie Eigenschaften mit der Methode gs.getProperty() abrufen, behandeln Sie die Ergebnisse als Zeichenfolgen. Beispielsweise gibt die Eigenschaft „true|false“ „wahr“ oder „falsch“ (Zeichenfolgen) zurück, nicht das boolesche Äquivalent.

5. Wählen Sie den vorhandenen Statuszuordnungsdatensatz aus, oder erstellen Sie eine neue Statuszuordnung im Agile-Tool-Statuszuordnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Zuordnung des Agile-Tool-Status“.

Feld	Beschreibung
Name	Fügen Sie den eindeutigen Namen für die Statuszuordnung ein.
Agile-Tool	Wählen Sie das Agile-Tool aus.
Entitätstabelle	Wählen Sie die Quelltabelle aus, für die die Statuszuordnung erstellt wird.
Projekt	Wählen Sie das Projekt aus, in dem der Status zugeordnet werden soll.
ServiceNow-Entitätsstatus	Wählen Sie den Status aus, den Sie dem Agile-Tool-Status zuordnen möchten.
Agile-Tool-Status	Wählen Sie aus den Status der angreifbaren Elemente den Status aus, den Sie zuordnen möchten.

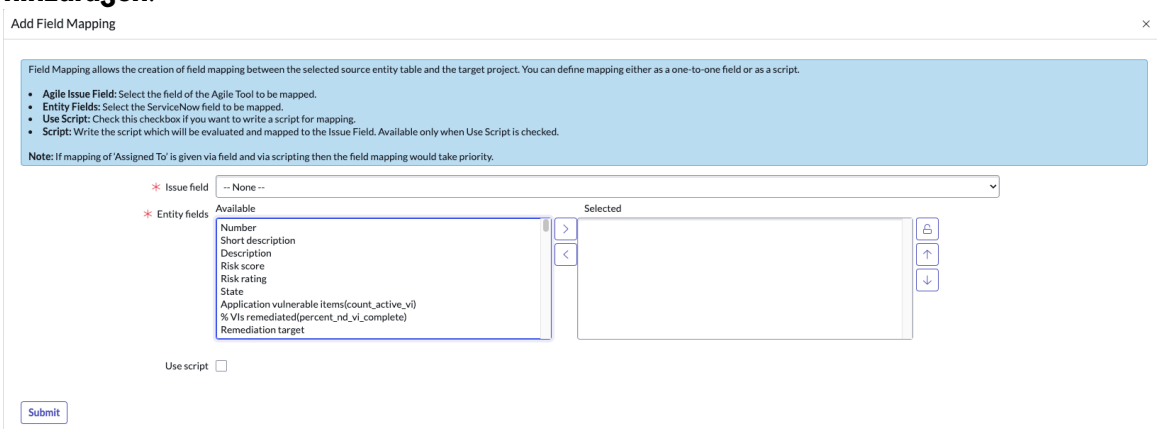
6. Klicken Sie auf **„Projekte speichern und abrufen“,** um die Projekte im Feld „Projektkonfigurationsregel“ abzurufen und die Anmeldeinformationen des Agile-Tools zu validieren.

   Tipp:
   Sie können die Systemeigenschaft **„projectsPageSize“** so festlegen, dass eine bestimmte Anzahl von Projekten pro Seite abgerufen wird.

7. Navigieren Sie zu **„Systemeigenschaften“** > **„sn_vul_jira.projectsPageSize“**, und fügen Sie im Feld „Wert“ für Jira Cloud die Anzahl der Projekte hinzu, die pro Seite abgerufen werden sollen.
8. Wählen Sie in der Konfigurationsregel Projekt, Problemtyp und Zuweisen an aus, nachdem die Projekte abgerufen wurden.

   Die Standardfeldzuordnung wird in der eingebetteten Liste der Agile-Tool-Feldzuordnungen ausgefüllt. Standardmäßig sind die Felder „Zusammenfassung“ und „Beschreibung“ von Problemen zugeordnet.

9. Um weitere Problemfelder den Feldern ServiceNow zuzuordnen, klicken Sie auf **Feldzuordnung hinzufügen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Sie dürfen nur Felder vom Typ „Zeichenfolge“ und „Auswahl“ zuordnen.
- Stellen Sie sicher, dass alle Problem-Pflichtfelder aus dem Agile-Tool ordnungsgemäß dem Entitätsfeld zugeordnet sind.

Formular „Zuordnung des Agile-Tool-Status“.

Feld	Beschreibung
Problemfeld	Enthält die Problemfelder des aktuell ausgewählten Projekts und des Problemtyps in der Konfigurationsregel.
Entitätsfelder	Enthält die Felder der in der Konfigurationsregel ausgewählten Entitätstabelle.
Verwenden Sie das Skript	Wählen Sie diese Option aus, um das Skript für die Zuordnung der Problemfelder zu Entitätsfeldern zu verwenden.
Skript	Skript zum Zuordnen des Problemfelds zu Entitätsfeldern.

10. Klicken Sie im Glide-Modal **auf Absenden**, um den Feldzuordnungsdatensatz in der Tabelle „Agile-Tool-Feldzuordnungen“ zu übermitteln.

    Hinweis:
    Wenn Sie die Pflichtfelder nicht zuordnen, werden für diese Konfigurationsregel keine Probleme erstellt.

    Obligatorische Felder werden oben im Formular „Agile-Tool-Konfiguration“ angezeigt.
    Alle Feldzuordnungen für eine bestimmte Konfigurationsregel werden in der eingebetteten Liste der Tabelle „Agile-Tool-Feldzuordnung“ in der Tabelle „Agile-Tool-Konfiguration“ angezeigt.

11. Klicken Sie mit der rechten Maustaste in den Header, um Ihre Änderungen zu speichern.
    Der gespeicherte Datensatz wird in der Tabelle „Agile-Tool-Konfiguration“ angezeigt. Wenn ein Datensatz erstellt wird, der mit einer Konfigurationsregel übereinstimmt, wird das Problem für den Datensatz entsprechend der Zuordnung in der Konfigurationsregel erstellt.

12. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.cloudBulkSize**, und legen Sie im Feld Wert die Anzahl der Probleme fest, die pro Batch erstellt werden sollen.

    Hinweis:
    Die maximale Anzahl von Problemen, die pro Batch in Jira Cloud erstellt werden können, beträgt 50.

    Sie können die Batchgröße für die Erstellung von Problemen in Jira Server festlegen.

13. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.onPremBulkIssue**, und legen Sie im Feld **Wert** die Anzahl der Probleme fest, die pro Batch erstellt werden sollen.
    Sie können die Fehleranzahl auch im Feld „Wert“ in der Systemeigenschaft festlegen, um die Datensätze in der Manifesttabelle zu verarbeiten und Jira-Probleme bis zu einer bestimmten Fehleranzahl zu erstellen.

14. Navigieren Sie zu **„Systemeigenschaften“** > **„sn_vul_agile.ManifestErrorCount** “, und legen Sie die maximale Anzahl fest, bis zu der das Manifest mit Fehler verarbeitet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Agile-Problem manuell mithilfe einer Listenaktion

Wenn die Listenaktion „Jira-Problem erstellen“ ausgelöst wird, sollten Datensätze, die den Regelkonfigurationskriterien entsprechen, für „Jira-Problem erstellen“ berücksichtigt werden. Diese Datensätze sollten in der Tabelle „sn_vul_agile_tool_manifest“ mit der in der Konfigurationsregel ausgewählten Zuordnung erfasst werden.

Vorbereitungen

Erforderliche Rolle: sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Containerelemente**.
2. Wählen Sie mehrere Datensätze aus, um Jira-Probleme zu erstellen, und klicken Sie auf **Jira-Problem erstellen**.
   Die ausgewählten Datensätze sollten die Feldzuordnung und die Statuszuordnung des zugehörigen Agile-Tools berücksichtigen.
   Die ausgewählten Datensätze, die die Konfigurationsregelbedingung erfüllen, müssen für die Erstellung von Jira-Problemen geeignet sein, und diese Datensätze müssen der Tabelle `sn_vul_agile_tool_manifest` hinzugefügt werden.

Erstellen Sie ein Agile-Problem manuell mithilfe einer Formularaktion

Erstellen Sie manuell ein Agile-Problem mit einer Formularaktion. Wenn der Datensatz mit einer Konfigurationsregelbedingung übereinstimmt, wird ein Popup-Feld mit Werten gefüllt, die in der Konfigurationsregel ausgewählt sind. Wenn er keinen Kriterien entspricht, kann der Anwender Werte für vordefinierte auswählen Felder.

Vorbereitungen

Stellen Sie sicher, dass alle Problem-Pflichtfelder aus dem Agile-Tool ordnungsgemäß dem Entitätsfeld zugeordnet sind.

Erforderliche Rolle: sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Containerelemente**.
2. Wählen Sie einen beliebigen Datensatz aus, um manuell ein Agile-Problem zu erstellen.
3. Wählen Sie **Agile-Problem erstellen aus**.
4. Fügen Sie gültige Details für die genannten Felder ein.

   Wenn der Datensatz die Bedingung einer Konfigurationsregel erfüllt, sollten die folgenden Felder mit dem konfigurierten Wert ausgefüllt werden, und der Anwender kann die Feldwerte ändern.

Feld	Beschreibung
Projekt	Wählen Sie das Projekt aus, in dem das Jira-Problem erstellt wird.
Problemtyp	Wählen Sie die Art des Problems aus, das in einem bestimmten Projekt erstellt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuweisen an	Wählen Sie den Beauftragten aus, dem das Problem beim Erstellen des Problems zugewiesen werden soll.
Feldzuordnung	Wählen Sie die Problemtypfelder des Agile-Tools aus, und fügen Sie die direkten Werte für das ausgewählte Feld ein.

5. Wählen Sie **Agile-Problem erstellen aus,** um den Datensatz zu übermitteln.
   Nach dem Senden des Datensatzes wird der Datensatzeintrag in der Tabelle „sn_vul_agile_tool_manifest“ erstellt.

Synchronisieren Sie manuell den Status des Problems Jira .

Aktualisieren Sie den Status des einzelnen Datensatzes, indem Sie im Kontextmenü des Formulars auf die Schaltfläche **Agile-Status synchronisieren** klicken, und aktualisieren Sie die Status mehrerer Datensätze, indem Sie in auf die Listenaktion **Agile-Status des angreifbaren Anwendungselements, des angreifbaren Container-Elements und der Korrekturaufgabentabelle synchronisieren** klicken Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen
Erforderliche Rolle: sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Warum und wann dieser Vorgang ausgeführt wird
Der Status wird von ServiceNow mit dem Agile-Tool synchronisiert, wenn der Entitätsstatus in ServiceNow geschlossen oder wenn eine Entität erneut geöffnet wird (d. h. Status ist Offen). Alle anderen Status werden vom Agile-Tool an ServiceNowwidergespiegelt. Der Anwender darf den Status für die Datensätze, deren zugehörige konfigurierte Regel keine Statuszuordnung hat, oder die Probleme, die direkt über die Formularaktion erstellt wurden, nicht synchronisieren.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Containerelemente**.
2. Wählen Sie mehrere Datensätze aus, um Jira-Probleme zu erstellen, und klicken Sie auf **„Agile-Status synchronisieren“**.
   Die Status der Datensätze, für die bereits Probleme erstellt wurden, werden aktualisiert, wenn sich der Datensatz nicht im Status „Geschlossen“ befindet und die Statuszuordnung für die ausgewählten Datensätze in der Konfigurationsregel vorhanden ist.
3. Öffnen Sie einen Datensatz, und der **Status der Agile-Synchronisierung** wird im Formular-Kontextmenü angezeigt, wenn die folgenden Bedingungen erfüllt sind.
   - Für den Datensatz wurde ein Problem erstellt, und der Datensatz befindet sich nicht im Status „Geschlossen“.
   - Für den Datensatz ist eine Statuszuordnung vorhanden
4. Klicken Sie auf **Agile-Status synchronisieren**, um den Agile-Status mit dem zugeordneten Status zu synchronisieren.
   Sie können die Systemeigenschaft festlegen, um die Batchgröße zum Abrufen des Problemstatus aus Jira festzulegen.
5. Navigieren Sie zu **Systemeigenschaft** > **sn_vul_jira.bulkIssueStatusSize**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Jira Server die maximale Anzahl der zurückzugebenden Probleme (standardmäßig 50). Der maximal zulässige Wert wird durch die Jira-Eigenschaft „jira.search.views.default.max“ vorgegeben. Wenn Sie einen höheren Wert als diese Zahl angeben, werden Ihre Suchergebnisse abgeschnitten).
- Wenn das Problem aus einer Formularaktion erstellt wird oder die konfigurierte Regel keine Statuszuordnung aufweist, werden diese Datensätze für die Statussynchronisierung nicht berücksichtigt.

Konfigurieren Sie den Scheduler so, dass Probleme automatisch erstellt werden

Konfigurieren Sie den Scheduler so, dass er die Probleme Jira für die in der Tabelle sn_vul_agile_tool_manifest erstellten Datensätze ausführt und automatisch erstellt.

Vorbereitungen
Erforderliche Rolle: admin oder schedule_admin.

Warum und wann dieser Vorgang ausgeführt wird
Alle in der Tabelle „sn_vul_agile_manifest“ erstellten Datensätze für angreifbares Anwendungselement, angreifbares Container-Element, Anwendungskorrekturaufgabe und Container-Korrektur werden für die Problemerstellung Jira berücksichtigt.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Erstellen Sie Jira-Probleme**.
2. Sie können die Felder Ausführung, Zeitzone und Zeit im Skript Geplant ändern.

Formular „Geplante Skript-Ausführung“

Feld	Beschreibung
Ausführen	Zeitintervall für die Ausführung der geplanten Aufgabe: ○ Täglich: Wird täglich zu einer festgelegten Zeit ausgeführt. ○ Wöchentlich: Wird wöchentlich zu einer festgelegten Uhrzeit und an einem bestimmten Tag ausgeführt. ○ Monatlich: Wird monatlich zu einer bestimmten Zeit und an einem bestimmten Tag im Monat ausgeführt. ○ Regelmäßig – Wird in einem festgelegten Wiederholungsintervall ausgeführt. ○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt. ○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt. ○ Geschäftskalender: Eintragsstart – Wird an den Starteintragsdaten für den im Feld ausgewählten Geschäftskalender ausgeführt. Für das Startdatum jedes Geschäftseintrags, den Sie für den Geschäftskalender definiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	haben, wird eine regelmäßige Aufgabe ausgeführt. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt. ○ Geschäftskalender: Eintragsende – Wird für das Enddatum für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge. **Hinweis:** Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offsettyp und Offset. Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie unter Create a business calendar und Define business calendar entries .
Tag	Tag, an dem die geplante Aufgabe ausgeführt werden soll ○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus. ○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus. Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen.
Wiederholungsintervall	Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein. ○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein. ○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein.
Zeit	Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag.
Zeitzone	Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus: ○ **Keine**: Verwenden Sie die Standardzeitzone für den angemeldeten Anwender, der die geplante Aufgabe erstellt. Die geplante Aufgabe wird beispielsweise um 16:45 Uhr US-Pazifik-Zeit ausgeführt, wenn es sich um die für den Benutzer zugewiesene Zeitzone handelt und wenn Sie 16:45 in das Feld Zeit eingeben. ○ **Zeitzone des Systems verwenden**: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt wird. Die regelmäßige Aufgabe wird beispielsweise um 22:15 Uhr Londoner Zeit ausgeführt, wenn Europa/London die standardmäßige Systemzeitzone für die Instanz ist und Sie 22:15 in das Feld Zeit eingeben. ○ Tatsächliche Zeitzone. ○ Beispiel: Die regelmäßige Aufgabe wird um 13:30 Uhr in der Zeitzone USA Ost ausgeführt, wenn Sie US/Ost auswählen und im Feld Zeit 13:30 eingeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
run_as	Standardmäßig muss „run_“ als Feldwert leer sein. Der Benutzer kann den Wert als Domänenbenutzerwert festlegen, um ein Problem für eine bestimmte Domäne zu erstellen.

Konfigurieren Sie den Scheduler so, dass Probleme automatisch aktualisiert werden

Konfigurieren Sie den Scheduler so, dass die Probleme Jira für die Datensätze, die der Tabelle sn_vul_agile_tool_manifest hinzugefügt wurden, automatisch aktualisiert werden.

Vorbereitungen
Erforderliche Rolle: admin oder schedule_admin.

Warum und wann dieser Vorgang ausgeführt wird
Alle in der Tabelle „sn_vul_agile_manifest“ erstellten Datensätze für angreifbares Anwendungselement, angreifbares Container-Element, Anwendungskorrekturaufgabe und Container-Korrektur werden für die Problemaktualisierung Jira berücksichtigt. Wenn der Datensatz geschlossen wird und Kommentare hinzugefügt werden, sollten diese Werte auch auf das zugehörige Problem Jira aktualisiert werden.

Hinweis:

- Die geplante Aufgabe „Probleme aktualisieren“ aktualisiert den Status Jira nicht, wenn der Workflow für das ausgewählte agile Problemprojekt verhindert, dass ein Anwender den Status direkt aus einem anderen Status ändert.
- Wenn Sie einen Entitätsdatensatz mit zusätzlichen Kommentaren schließen, wird zum Zeitpunkt der Aktualisierung nur der letzte Kommentar berücksichtigt. Bei der nächsten Aktualisierung werden alle Kommentare dem zugehörigen Jirahinzugefügt.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Aktualisiert Jira-Probleme**.
2. Sie können die Felder **Ausführung**, **Zeitzone**und **Zeit** im Skript Geplant ändern.

Formular „Geplante Skript-Ausführung“

Feld	Beschreibung
Ausführen	Zeitintervall für die Ausführung der geplanten Aufgabe: ○ Täglich: Wird täglich zu einem bestimmten Zeitpunkt ausgeführt ○ Wöchentlich: Wird wöchentlich zu einer bestimmten Zeit und an einem bestimmten Tag ausgeführt. ○ Monatlich: Wird monatlich zu einer bestimmten Zeit und an einem bestimmten Tag im Monat ausgeführt. ○ Regelmäßig: Wird in einem vorgegebenen, sich wiederholenden Intervall ausgeführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt ○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt ○ Geschäftskalender: Eintragsstart: Wird für die Anfangseintragsdaten für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Für das Startdatum jedes Geschäftseintrags, den Sie für den Geschäftskalender definiert haben, wird eine regelmäßige Aufgabe ausgeführt. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt. ○ Geschäftskalender: Eintragsende: Wird für das Enddatum für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge. **Hinweis:** Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offsettyp und Offset. Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie unter und Create a business calendar Define business calendar entries .
Tag	Tag, an dem die geplante Aufgabe ausgeführt werden soll ○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus. Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen.
Wiederholungsintervall	Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel: ○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein. ○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein. ○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein.
Zeit	Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag.
Zeitzone	Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus: ○ Keine: Verwenden Sie die Standardzeitzone für den angemeldeten Benutzer, der die geplante Aufgabe erstellt. Beispiel: Die geplante Aufgabe wird um 16:45 Uhr ausgeführt. US-Pazifik-Zeit, wenn es sich um die zugewiesene Zeitzone des Benutzers handelt und Sie im Feld Zeit 16:45 eingeben. ○ Zeitzone des Systems verwenden: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	wird. Beispiel: Die regelmäßige Aufgabe wird um 22:15 Uhr Londoner Zeit ausgeführt, wenn Europa/London die standardmäßige Systemzeitzone für die Instanz ist, und Sie geben im Feld „Zeit“ 22:15 Uhr ein. ○ Tatsächliche Zeitzone. ○ Beispiel: Die regelmäßige Aufgabe wird um 13:30 Uhr in der Zeitzone USA Ost ausgeführt, wenn Sie US/Ost auswählen und im Feld Zeit 13:30 eingeben.
run_as	Standardmäßig ist das Feld **run_as** leer. Sie können den Wert auf einen Domänenbenutzer festlegen, um ein Problem für eine bestimmte Domäne zu erstellen.

Konfigurieren Sie den Scheduler, um den Status Jira automatisch mit ServiceNow® zu synchronisieren

Konfigurieren Sie den Scheduler, um den Status von Problemen Jira mit angreifbaren Elementen in der Anwendung, angreifbaren Container-Elementen und Aufgaben in der Tabelle sn_vul_agile_manifest zu synchronisieren.

Vorbereitungen
Erforderliche Rolle: schedule_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Der Zeitplaner wird automatisch gemäß dem konfigurierten Zeitplan ausgeführt. Der Status der Datensätze, die in der Tabelle „Angreifbares Anwendungselement“, „Angreifbares Container-Element“, „Anwendungskorrekturaufgabe“ und „Container-Korrekturaufgabe“ erstellt wurden und in denen Probleme in Jira erstellt wurden, wird entsprechend dem aktuellen Status des Problems auf der Plattform Jira basierend auf aktualisiert Statuszuordnung in der Konfigurationsregel.

Alle in der Tabelle „sn_vul_agile_manifest“ erstellten Datensätze für angreifbare Anwendungselemente, angreifbare Container-Elemente, Anwendungskorrekturaufgaben und Container-Korrekturelemente werden für die Problemerstellung Jira berücksichtigt.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Synchronisierungsstatus**.
2. Sie können die Felder Ausführung, Zeitzone und Zeit im Skript Geplant ändern.

Formular „Geplante Skript-Ausführung“

Feld	Beschreibung
Ausführen	Zeitintervall für die Ausführung der geplanten Aufgabe:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Täglich: Wird täglich zu einem bestimmten Zeitpunkt ausgeführt ○ Wöchentlich: Wird wöchentlich zu einer bestimmten Zeit und an einem bestimmten Tag ausgeführt. ○ Monatlich: Wird monatlich zu einer bestimmten Zeit und an einem bestimmten Tag im Monat ausgeführt. ○ Regelmäßig: Wird in einem vorgegebenen, sich wiederholenden Intervall ausgeführt ○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt ○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt ○ Geschäftskalender: Eintragsstart: Wird an den Anfangseintragsdaten für den im Feld ausgewählten Geschäftskalender ausgeführt. Für das Startdatum jedes Geschäftseintrags, den Sie für den Geschäftskalender definiert haben, wird eine regelmäßige Aufgabe ausgeführt. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt. ○ Geschäftskalender: Eintragsende: Wird für das Enddatum für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge. **Hinweis:** Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offsettyp und Offset. Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	unter Create a business calendar und Define business calendar entries .
Tag	Tag, an dem die geplante Aufgabe ausgeführt werden soll ○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus. ○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus. Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen.
Wiederholungsintervall	Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel: ○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein. ○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein. ○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein.
Zeit	Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag.
Zeitzone	Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus: ○ -Keine-: Verwenden Sie die Standardzeitzone für den angemeldeten Benutzer, der die regelmäßige Aufgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erstellt. Die geplante Aufgabe wird beispielsweise um 16:45 Uhr US-Pazifik-Zeit ausgeführt, wenn es sich um die für den Benutzer zugewiesene Zeitzone handelt und wenn Sie 16:45 in das Feld Zeit eingeben. ○ Zeitzone des Systems verwenden: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt wird. Beispiel: Die regelmäßige Aufgabe wird um 22:15 Uhr Londoner Zeit ausgeführt, wenn Europa/London die standardmäßige Systemzeitzone für die Instanz ist, und Sie geben im Feld „Zeit“ 22:15 Uhr ein. ○ Tatsächliche Zeitzone. ○ Beispiel: Die regelmäßige Aufgabe wird um 13:30 Uhr in der Zeitzone USA Ost ausgeführt, wenn Sie US/Ost auswählen und im Feld Zeit 13:30 eingeben.
run_as	Standardmäßig ist das Feld run_as leer. Sie können den Wert als Wert des erforderlichen Domänenbenutzers festlegen, um ein Problem für eine bestimmte Domäne zu erstellen.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Integration

Mit der Prisma-Cloud-Computing-Integration können Sie Hosts scannen, um Schwachstellen zu erkennen.

Ab Version 24.02.0 von Vulnerability Responsekönnen Sie die Prisma-Cloud-Computing-Integration verwenden, um Schwachstellen auf den laufenden Hosts zu importieren. Die Prisma-Host-APIs ermöglichen das Abrufen umfassender Schwachstelleninformationen für einen bestimmten Host und liefern außerdem einen Snapshot der Host-Schwachstellen zu einem bestimmten Zeitpunkt. Diese API ermöglicht die regelmäßige Synchronisierung zwischen Prisma- und ServiceNow-Instanz. Da Prisma sowohl als Software-as-a-Service-Lösung (SaaS) als auch als lokale Lösung angeboten wird, ist die Verwendung eines MID Servers erforderlich, um Prisma-APIs aus der ServiceNow-Instanz aufzurufen. Darüber hinaus müssen Sie ein MID-Server -Element verwenden, wenn sich das Produkt Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute und Ihre Instanz Now Platform nicht in derselben Umgebung befinden. Weitere Informationen finden Sie unter Systemanforderungen für MID-Server .

Berichte zu Schwachstellen und angreifbaren Elementen können Sie auch in den Dashboards Vulnerability Response anzeigen. Diese Schwachstellen können dann priorisiert und behoben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen anzeigen

Sie können die Integrationen anzeigen, die Teil von Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Computesind. Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Integrationen**.

Die folgenden Integrationen sind verfügbar.

Ausführungssequenz	Zeitplan	Integration	Beschreibung
1	Täglich	Integration mit Prisma-Cloud-Computing-Hosts	Ruft Schwachstellen von Hosts ab und erstellt VITs, Erkennungen und erkannte Elemente für Hosts.

Hinweis:
Wenn das Plugin „Container Vulnerability Response“ installiert ist, können Sie auch Integrationen im Zusammenhang mit Container Vulnerability Response anzeigen.

Prisma-Integration , Prozess

Wenn Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ausgeführt wird, wird geprüft, ob in der Tabelle der National Vulnerability Database (NVD) ein Common Vulnerability and Exposure (CVE) vorhanden ist. Wenn sie bereits vorhanden ist, werden die vorhandenen Informationen verwendet. Wenn das CVE jedoch nicht gefunden wird, werden in der NVD-Tabelle Platzhalterdatensätze generiert. Beim Erstellen dieser Platzhalter-NVD-Datensätze werden zunächst nur das CVE und sein Name ausgefüllt. Andere Details werden nicht mit der Annahme ausgefüllt, dass die NVD-Integration diese Details später ausfüllt. Wenn der Parameter der Integrationsinstanz *update_nvd* auf true festgelegt ist, werden die Platzhalter-NVD-Datensätze aktualisiert. Standardmäßig ist der Instanzparameter auf „falsch“ festgelegt. Zumindest bis die NVD-Integration ausgeführt wird und diese Details ausfüllt, sind jedoch ein gewisses Verständnis des CVE, z. B. sein Schweregrad oder einige grundlegende Informationen über das Problem erforderlich. Um diese Anforderung zu erfüllen, werden die Felder **Exploit vorhanden** und **Korrekturhinweise** mit den aus Prisma erhaltenen Details ausgefüllt. Darüber hinaus ist diese Konfiguration anpassbar, sodass Sie beliebige andere Felder angeben können, die Sie im NVD-Eintrag basierend auf den von Prisma bereitgestellten Informationen ausfüllen möchten.

Vorbereitung auf das Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Sie können sich auf den Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute vorbereiten, indem Sie Setupaufgaben ausführen.

Bevor Sie beginnen

Zur Installation und Konfiguration der Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute können Sie die folgende Prüfliste drucken. Stellen Sie sicher, dass die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und die Schwachstellendaten in Ihre Instanz Now Platform® importieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration

Aufgabe	Beschreibung
☐	Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen: • API-Basis-URL • Anwendername und Passwort. Diese Anmeldeinformationen werden verwendet, um die Schwachstellen aus der Prisma-Cloud-Computing-Integration abzurufen. Weitere Informationen finden Sie unter https://pan.dev/compute/api/ **Hinweis:** MID-Server ist optional. Die für die Prisma-Cloud-Computing-Integration verwendeten Anwenderanmeldeinformationen benötigen die Berechtigung zum Überwachen der Images. Siehe folgenden Code: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Wenn die Anwendung Vulnerability Response [] noch nicht installiert und aktiviert ist, installieren Sie die Anwendung , bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher.
☐	Rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in Ihrer Instanz Now Platform® herunter.
☐	Schätzen Sie die Anzahl der zu importierenden angreifbaren Elemente. Vergewissern Sie sich, dass Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie voraussichtlich importieren werden. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support ServiceNow von .
☐	Stellen Sie sicher, dass Sie über die folgenden Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und die angreifbaren Elemente zu korrigieren: **Administrator** Installieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Wenn dies nicht zugewiesen ist, weist der Administrator den Container-Schwachstellen-Administrator (sn_vul_container.vulnerability_admin) und andere Rollen zu. **sn_vul_container.vulnerability_admin**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
	Schließt die Konfiguration der Prisma-Cloud-Computing-Integration ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Container Vulnerability Response (CVR) und ihre Datensätze. Dieser Administrator konfiguriert Integrationen und Regeln in Container Vulnerability Response. **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben sn_vul.read_all und sn_vul_container.read_all. **Besitzergruppe für Container-Korrektur** Standardmäßig ist die Gruppe „Besitzer der Container-Korrektur“ verfügbar. Anwender, die dieser Gruppe zugewiesen sind, erben sn_vul_container.remediation_owner. Der Container-Korrekturbesitzer behebt Container-Schwachstellen, die ihm oder einer Gruppe, der er angehört, zugewiesen sind. **Schwachstellenanalyst** Benutzer, die der Gruppe der Container-Schwachstellenanalysten zugewiesen sind, erben die Eigenschaft „sn_vul.vulnerability_analyst“. Der Schwachstellenanalyst überwacht die Behebung aller angreifbaren Elemente. Wenn dies noch nicht geschehen ist, können Sie zusätzliche Gruppen erstellen und Benutzer mit dem -Benutzerverwaltungsmodul in Ihrer -Instanz hinzufügen. Weitere Informationen finden Sie unter Benutzergruppen erstellen .
☐	Installieren Sie die Integration Vulnerability Response mit NVD, und führen Sie die Integration der US-Schwachstellendatenbank (National Vulnerability Database Integration) des NIST API – API (nur CVE) aus.

Sie sind bereit für Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ..

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren

Bevor Sie die Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit das Produkt Prisma Cloud Compute ordnungsgemäß in Vulnerability Response und Container Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in der Anwendung ServiceNow Storenach der Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie bei Bedarf die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Aktualisieren Sie die Felder **Instanzname** und **Grund für die Instanz**, und klicken Sie auf **Instanz validieren**.
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.

Ergebnisse
Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Nächste Maßnahme
Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ..

Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute .

Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute, um Daten aus Prisma Cloud Compute zu importieren. Sie können die importierten Daten verwenden, um Schwachstellen für Ihre Hosts zu priorisieren und zu beheben.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die E-Mail von ServiceNow, die Sie zur Integration erhalten haben.
2. Melden Sie sich bei Ihrer -Instanz als Administrator an.
3. Befolgen Sie die Anweisungen in der E-Mail, um Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Computeabzurufen.
4. Navigieren zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**. Füllen Sie die Felder im Formular „Prisma-Cloud-Computing-Konfiguration“ aus. Weitere Informationen finden Sie unter Formular „Prisma-Cloud-Computing-Konfiguration“.
5. Wählen Sie in der Projektliste entweder **Alle Projekte** oder **Bestimmte Projekte** aus, um entweder alle Projekte oder ausgewählte Projekte zu konfigurieren.
   Wenn Sie **Bestimmte Projekte**auswählen, können Sie die Projekte aus der Liste Verfügbar auswählen.
6. Schließen Sie die Konfiguration ab, indem Sie entweder **Fertigstellen** oder **Anmeldeinformationen speichern und testen**auswählen.
   - Wenn Sie ein Projekt konfiguriert haben, wählen Sie **Fertig stellen**aus.
   - Wenn Sie kein Projekt konfiguriert haben, wählen Sie **Anmeldeinformationen speichern und testen aus**
7. Zeigen Sie die neu erstellte Instanz an, indem Sie zu navigieren **Prisma-Cloud-Computing-Integration** > **Administration** > **Integrationsinstanzen**.
8. Zeigen Sie die Projekte an, die Sie zuvor konfiguriert haben, indem Sie **Integration Instance Parameters**ausgewählt haben.
9. Führen Sie die neu erstellte Integrationsinstanz aus, um die angreifbaren Elemente zu importieren.
   Die VITs werden basierend auf der Granularität weiter erstellt.
10. Konfigurieren Sie die Granularität eines angreifbaren Elements.

    a. Navigieren zu **Prisma-Cloud-Computing-Integration** > **Image-Schwachstellenschlüssel konfigurieren**

    b. Konfigurieren Sie die Granularität der VITs, indem Sie die erforderlichen Kontrollkästchen aktivieren. Die angreifbaren Elemente werden basierend auf den ausgewählten Schlüsseln während des nächsten Imports erstellt.

> **Hinweis:**
> Standardmäßig wird eine VIT für eine Kombination aus Image-Repository,] Schwachstelle und Image-Tag erstellt. Sie können dem Schlüssel Komponenten hinzufügen, um die Granularität zu erhöhen. Sie können beispielsweise ein CVIT für eine Kombination aus Image-Repository, Schwachstelle, Image-Tag und Cluster erstellen. Sobald die angreifbaren Elemente oder die Ergebnisse zu angreifbaren Elementen erstellt wurden, können die Kontrollkästchen nicht mehr bearbeitet werden.

Statusdiagramm der Integrationsausführung für die Prisma-Cloud-Computing-Integration

Das Modul „Prisma Cloud Compute Integration Ausführungsstatus“ bietet Ihnen eine grafische Ansicht des Status der Ausführungen von Prisma Cloud Compute Integration.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein Teil des Balkendiagramms klicken, wird eine Liste mit detaillierteren Informationen geöffnet.

Erforderliche Rolle: Schwachstellen-Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rollen und granulare Rollen sind verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

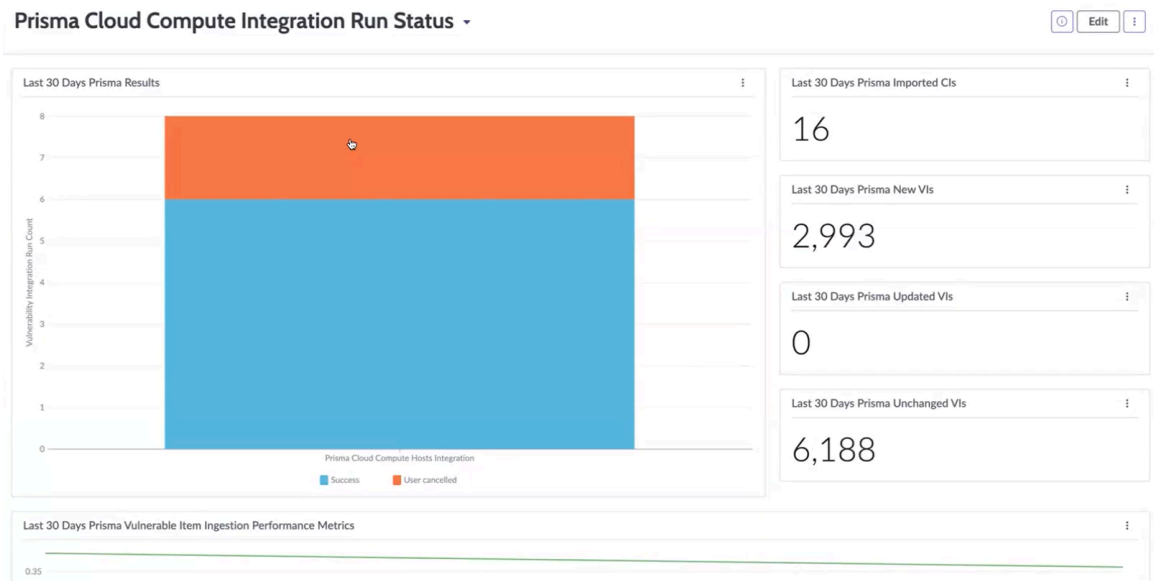
Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Ausführungsstatus



Diagrammberichte zum Status der Prisma-Cloud-Computing-Integration

Name	Beschreibung
Prisma-Ergebnisse der letzten 30 Tage	Die Anzahl der Integrationsausführungen, die für die Integration abgeschlossen wurden. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Jede Ausführung wird als Balken im Diagramm angezeigt.
Von Prisma importierte CIs der letzten 30 Tage	Die Anzahl der Configuration Items (CIs), die von Prisma in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Neue Prisma-VIs der letzten 30 Tage	Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Von Prisma aktualisierte AEs der letzten 30 Tage	Anzahl der aktualisierten angreifbaren Elemente (VIs), die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Unveränderte Prisma-VIs der letzten 30 Tage	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Angreifbares Prisma-Element – Erfassungsleistungsmetriken der letzten 30 Tage	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage.

Erstellen Sie manuell eine Schwachstellen-Integration

Schwachstellen-Integrationen bieten Kunden und Lieferanten die Möglichkeit, die Schwachstellendaten in ihrer Instanz durch Abrufen von Daten aus externen Systemen und Lieferanten zu ergänzen. Diese Funktion kann den Lebenszyklus der Schwachstellenkorrektur vereinfachen, indem die Instanz mit anderen Schwachstellenmanagementsystemen synchronisiert wird.

Ausführliche Anweisungen zum Erstellen von Integrationen finden Sie unter Definieren Sie eine neue Schwachstellenintegration.

Definieren Sie eine neue Schwachstellenintegration

Eine Schwachstellen-Integration ruft Berichtsdaten aus einem Drittanbietersystem ab (im Allgemeinen, um Schwachstellendaten abzurufen) und verarbeitet diese Berichtsdaten mithilfe von Datenquellen oder einem anwenderdefinierten Prozessor.

Vorbereitungen

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder nach Bedarf aus.

Schwachstellenintegration

Feld	Beschreibung
Name	Ein beschreibender Name für die Integration.
Aktiv	Gibt an, ob die Integration aktiv ist. Wenn er für einen bestimmten Zeitraum nicht ausgeführt werden soll, können Sie die zu verwendenden Parameter einrichten und den Auftrag deaktivieren.
Ausführen	Die Häufigkeit, mit der die Integration ausgeführt werden soll: Täglich, Wöchentlich, Regelmäßig usw. Wie bereits erwähnt, werden nachfolgende Felder basierend auf Ihrer Einstellung in diesem Feld angezeigt.
Tag	Der Tag, an dem die Integration ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wenn Sie **Wöchentlich** im Feld **Ausführen** ausgewählt haben, zeigt dieses Feld die Wochentage an. ○ Wenn Sie **Monatlich** im Feld **Ausführen** ausgewählt haben, zeigt dieses Feld die Tage des Monats an.
Zeit	Zeitpunkt, zu dem die Integration starten soll. Dieses Feld wird nur angezeigt, wenn Sie im Feld **AusführenTäglich**, **Wöchentlich** oder **Monatlich** ausgewählt haben.
Anwendung	[Schreibgeschützt] Der Name der Anwendung, für die diese Integration erstellt wurde.
Wiederholungsintervall	Wenn Sie im Feld **Ausführendie Option Regelmäßig** ausgewählt haben, zeigt dieses Feld die Anzahl der Tage und Stunden an, bis die Integration erneut ausgeführt wird.
Wird gestartet	Wenn Sie im Feld **Ausführen** die **Option Regelmäßig** ausgewählt haben, zeigt dieses Feld Datum und Uhrzeit an, die als Ausgangspunkt für regelmäßige Aktualisierungen verwendet werden sollen.
Bedingt	Wählen Sie dieses Feld aus, wenn Sie bedingte Parameter hinzufügen möchten.
Bedingung	Wenn Sie das **Kontrollkästchen** Bedingung aktiviert haben, geben Sie die Bedingungen hier ein.
Integrationsdetails	
Integrationsskript	Wählen Sie die Skripteinbindung aus, die die VulnerabilityIntegrationBase erweitert, die bei der Ausführung der Integration ausgeführt werden soll. Dieses Skript definiert, wie Daten aus einem Drittparteisystem abgerufen werden.
Integrationswerksskript	Geben Sie ein Skript ein, das definiert, wie die für das **Integrationsskript**ausgewählte Skripteinbindung erstellt wird. Weitere Informationen finden Sie unter Skriptfelder für Integrationswerk. **Hinweis:** Skripts erfordern Kenntnisse in den Bereichen ServiceNow und Vulnerability Response.
Berichtsprozessorstrategie	Wählen Sie die Strategie aus, die Sie für die Verarbeitung der vom Integrationsskript zurückgegebenen Daten verwenden möchten, wenn die Integration ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wählen Sie **Datenquellenanhang**, wenn Sie Daten mit einer Datenquelle verarbeiten möchten. ○ Wählen Sie **Benutzerdefinierter Berichtsprozessor,** um einen anwenderdefinierten Bearbeiter auszuwählen.
Berichtsprozessor-Skript	Wenn Sie **Benutzerdefinierter Berichtsprozessor** im Feld **Berichtsprozessorstrategie** ausgewählt haben, wählen Sie die Skripteinbindung aus, die die Skripteinbindung VulnerabilityReportProcessorBase erweitert, die bei der Ausführung der Integration ausgeführt werden soll. Dieses Skript definiert, wie die vom Integrationsskript zurückgegebenen Daten verarbeitet werden.
Prozessorwerksskript	Geben Sie ein Skript ein, das definiert, wie die für den **Berichtsprozessor**ausgewählte Skripteinbindung erstellt wird.

4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Skript zur Integration von Schwachstellen

Berichtsprozessorstrategien

Skriptfelder für Integrationswerk

Führen Sie manuell eine Schwachstellen-Integration aus

Skript zur Integration von Schwachstellen

Im Formular „Schwachstellenintegration“ ist das Integrationsskript ein Verweis auf eine Skripteinbindung, die die Skripteinbindung VulnerabilityIntegrationBase erweitert.

Die in diesem Skript enthaltene Funktionalität wird vom VulnerabilityIntegrationController aufgerufen, um zu verwalten, wie Daten aus einer externen Datenquelle abgerufen werden. Jede Unterklasse von VulnerabilityIntegrationBase hat Zugriff auf kontextbezogene Informationen zum aufrufenden Prozess. Diese Informationen sind über die folgenden Mitgliedsvariablen verfügbar:

- integrationGr – ein GlideRecord des Schwachstellen-Integrationsdatensatzes, der die Ausführung der Integration angefordert hat.
- integrationProcessGr – ein GlideRecord, der Kontextinformationen für den aktuellen Prozess einer Integration bereitstellt.

Der Schwachstellenprozess enthält spezielle Parameter, die innerhalb einer Integration verwendet werden, im Allgemeinen für Paginierungszwecke. Jeder Ausführung einer Schwachstellen-Integration (die auch als Vulnerability-Integrationsausführung bezeichnet wird) ist mindestens ein Prozess für die Schwachstellen-Integration zugeordnet. Bei

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrfachaufruf-Integrationen gibt es für jede Schwachstellen-Integrationsausführung einen oder mehrere Schwachstellen-Integrations-Prozessdatensätze.

Die Skripteinbindung muss eine Implementierung für die RetrieveData()- Methode bereitstellen und ein Objekt zurückgeben, das vom Skript des Berichtsprozessors verarbeitet wird. Das von AbrufenDaten zurückgegebene Objekt ist ein einfaches Objekt mit Eigenschaften für Inhalt, Inhaltstyp und Erweiterung.

Hier ist ein Screenshot von VulnerabilityIntegrationBase.retrieveData():

VulnerabilityIntegrationBase.Daten abrufen()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

Die Logik in RetrieveData() hängt von der Schnittstelle ab, die zum Abrufen der Daten erforderlich ist. Wenn beispielsweise die Quelle der abgerufenen Daten über eine REST API verfügt, kann der Textkörper dieser Methode den REST-Endpunkt aufrufen, wahrscheinlich über RESTMessageV2. Die Antwort auf den Anruf kann dann analysiert oder in einen Anhang eingefügt werden, und die Details können zum Erstellen des Rückgabeobjekts verwendet werden.

Einzelaufruf-Integrationen

Einzelaufruf-Integrationsskripts (einzelne Seite) sind die einfachsten Arten von Integrationen. Sie benötigen einen Aufruf, häufig an eine externe Datenquelle, um Daten abzurufen. Für Einzelseiten-/Einzelaufruf-Integrationen muss nur „retrieveData()“ implementiert werden.

Es folgt ein Beispiel, das ein einfaches Integrationsskript für Einzelaufrufe demonstriert. Es erstellt eine RESTMessageV2 und führt sie aus. Anschließend wird ein Objekt zurückgegeben, bei dem der Antworttext zusammen mit einem angenommenen Inhaltstyp und einer Erweiterung als Inhalt verwendet wird.

Skript für Einzelaufruf-Integration

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrfachanruf-Integrationen

Integrationsskripts mit mehreren Aufrufen (oder mehreren Seiten) sind etwas komplizierter. Sie erfordern mehrere Aufrufe einer Datenquelle, um Daten abzurufen.

Wie bei einer Einzelaufruf-Integration muss auch für eine Mehrfachaufruf-Integration die Funktion RetrieveData() implementiert sein. Im Textkörper von abrufenDaten() verwendet die Integration die von VulnerabilityIntegrationBase bereitgestellten Methoden hasMoreData() und setNextRunParameters().

Die Methode hasMoreData() akzeptiert einen einzelnen booleschen Wert, der den VulnerabilityIntegrationController anweist, weitere Prozesse einzufügen, um mehr Daten abzurufen. Bei der Übergabe von „wahr“ an hasMoreData() erfolgt ein Aufruf von setNextRunParameters(), um Kontext für den nächsten Prozess bereitzustellen.

Die Methode setNextRunParameters() akzeptiert ein einzelnes Objekt, das Kontextinformationen bereitstellt, die beim nächsten Aufruf von Abrufen von Daten verwendet werden sollen. Dieses Objekt wird verwendet, um den Status an nachfolgende Aufrufe von Abrufen von Daten () zu übergeben. Ein Beispiel-Anwendungsfall ist die Übergabe eines Objekts an einen Webservice, das die aktuelle Seitenzahl und Seitengröße angibt.

Bei Mehrfachaufruf-Integrationen prüft jeder RetrieveData()-Aufruf zuerst die aktuellen Prozessparameter. Die Methode _getProcessParameters() wird allen VulnerabilityIntegrationBases zur Verfügung gestellt, um die vom vorherigen Prozess festgelegten Parameter abzurufen. Wenn keine Parameter vorhanden sind, weist dies darauf hin, dass es sich um den ersten Prozess handelt.

Es folgt ein Screenshot eines Beispielskripts für die Mehrfachanruf-Integration. Dieses Skript erweitert das Beispiel für die Einzelaufruf-Integration und demonstriert die Durchführung von Aufrufen an einen REST-Endpunkt mit grundlegender Unterstützung für Paginierung. Es zeigt, wie Sie eine einzelne Seite mit Daten abrufen, erkennen, dass weitere Daten abzurufen sind, und dann dem nächsten Prozess mitteilen, welche Seite abgerufen werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skript für Mehrfachanruf-Integration

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Anhänge als abrufenDaten() -Rückgabewerte

Manchmal ist es besser, einen Anhang von abrufenDaten () zurückzugeben. Die Logik zum Erstellen und/oder Abrufen eines Anhangs ist Implementierungsspezifisch, aber nachdem der Anhang bekannt ist, können seine Informationen zurückgegeben werden.

Um einen Anhang bereitzustellen, gibt abrufenDaten() ein Objekt zurück wie:

```
{
    contents: "attachment-sys-id",
    contentType: "sys_attachment"
}
```

Ein Beispiel, das das vorherige Beispielerweitert, aber den Antworttext der REST-Nachricht im folgenden Integrationsprozess-Datensatz speichert. Anschließend wird dieser Anhangsbezeichner als Inhalt des Rückgabeobjekts zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gibt den Anhang aus abrufenDaten zurück

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Berichtsprozessorstrategien

Das Feld **„Strategie für Berichtsprozessor“** im Formular „Schwachstellenintegration“ wird verwendet, um die Methode zur Verarbeitung der vom Skript für die Schwachstellenintegration zurückgegebenen Daten auszuwählen, wenn der Schwachstellenintegrationsprozess ausgeführt wird.

Der Standardwert ist **Datenquellenanhang**. Diese Methode ist die Baselineimplementierung, die die abgerufenen Daten an eine Datenquelle übergibt, um sie in das System zu importieren. Wenn Sie **Benutzerdefinierter Berichtsprozessor** auswählen, können Sie ein anwenderdefiniertes Prozessorskript für die Verarbeitung der Daten auswählen.

Strategie zur Verarbeitung des Anhangsberichts der Datenquelle verwenden

Die Berichtsprozessorstrategie „Datenquellenanhang“ wird verwendet, um vom Integrationsskript abgerufene Daten an konfigurierte Datenquellen zu übergeben.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen** und erstellen Sie eine neue Integration.
2. Wählen Sie im Feld **Strategie für Berichtsprozessordie Option Datenquellenanhang**aus.
3. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie **Speichern**aus.
4. Klicken Sie in der zugehörigen Liste **„Datenquellen für Schwachstellenintegration“** auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Definieren Sie die zu verwendende Datenquelle.
6. Klicken Sie auf **Absenden**.
7. Wiederholen Sie die Schritte 4 bis 6, wenn Sie zusätzliche Datenquellen benötigen.
   Achten Sie darauf, die Reihenfolge anzugeben, in der die verschiedenen Datenquellen Informationen im Feld **Reihenfolge** senden.
8. Klicken Sie auf **Aktualisieren**.

Über anwenderdefinierte Berichtprozessorskripts

Im Formular „Schwachstellenintegration“ ist der Berichtsprozessor ein Verweis auf eine Skripteinbindung, die die Skripteinbindung VulnerabilityReportProcessorBase erweitert. Die in diesem Skript enthaltene Funktionalität wird vom VulnerabilityIntegrationController aufgerufen und definiert die Art und Weise, wie die vom Integrationsskript zurückgegebenen Daten verarbeitet werden.

Jede Unterklasse von VulnerabilityReportProcessorBase hat Zugriff auf kontextbezogene Informationen zum aufrufenden Prozess. Diese Informationen sind über die folgenden Mitgliedsvariablen verfügbar:

- integrationGr – ein GlideRecord des Datensatzes der Schwachstellenintegration, der die Ausführung der Integration angefordert hat.
- integrationProcessGr: GlideRecord des Schwachstellenprozesses, der Kontextinformationen für den aktuellen Prozess einer Integration bereitstellt.

Die Skripteinbindung muss eine Implementierung für die Methode `processReport()` bereitstellen. Das an processReport() übergebene Objekt ist das von Abrufen vonDaten zurückgegebene Objekt und als solches ein einfaches Objekt mit den Eigenschaften „Inhalt“, „Inhaltstyp“ und „Erweiterung“. Die tatsächliche Logik in processReport() ist Implementierungsspezifisch und abhängig von den bereitgestellten Berichtsdaten.

Hier ist ein Screenshot von VulnerabilityReportProcessorBase.processReport():

Anwenderdefiniertes Berichtsprozessorskript

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Skriptfelder für Integrationswerk

Das Formular „Schwachstellenintegration“ enthält das Integrations-Factory-Skript und, wenn die Berichtsprozessorstrategie **„Custom Report Processor“** ausgewählt ist, das Prozessor-Factory-Skript. Diese Felder werden verwendet, um die Logik zum Tatsächlichen Instanziieren des Objekts bereitzustellen, das durch die Referenzfelder der Skripteinbindung, das Integrationsskript und den Berichtsprozessor definiert wird.

Wenn die Skripteinbindung ausgewählt ist, werden beide Felder vorab mit einem Konstruktoraufruf ohne Argument ausgefüllt. Oft reicht dies aus, aber es kann Fälle geben, in denen mehr Logik erforderlich ist, um das Skriptobjekt zu instanziieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der integrationProcessGr-Datensatz wird für die Factory-Skriptfelder verfügbar gemacht, sodass bei Bedarf prozessspezifische Informationen verwendet werden können.

Führen Sie manuell eine Schwachstellen-Integration aus

Eine Schwachstellenintegration wird so konfiguriert, dass sie auf Zeitplanbasis ausgeführt wird. Sie können sie jedoch bei Bedarf manuell ausführen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_write

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen**.
2. Öffnen Sie die Integration, die Sie ausführen möchten.
3. Klicken Sie auf **Jetzt ausführen**.

Manuelle Erfassung von Schwachstellen

Erfassen Sie Schwachstellen manuell in der Anwendung Vulnerability Response, damit Sie sie schnell beheben können, ohne auf die Ergebnisse des Scanners warten zu müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scanner von Drittparteien wie Rapid7 helfen beim Import von Schwachstellendaten in Vulnerability Response und verarbeiten die Daten, um die Ergebnisse zu melden. Mit der Integration zur manuellen Erfassung können Sie Schwachstellen proaktiv erfassen und beheben, anstatt darauf zu warten, dass Scanner die gefährdeten Assets melden. Durch die manuelle Erfassung von Schwachstellen werden Assets effektiv vor unbekannten Bedrohungen wie Zero-Day-Angriffen geschützt.

Manuelle Erfassung von Schwachstellen

Sie können die Schwachstellendaten importieren, indem Sie eine Vorlage in den folgenden Dateiformaten hochladen:

- Excel
- Kommagetrennter Wert (CSV)

Um auf die Vorlage zuzugreifen und sie herunterzuladen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Datei hochladen – UI**.

Stellen Sie sicher, dass Sie die folgenden wichtigen Punkte befolgen, wenn Sie die Datensätze in der Vorlage ausfüllen:

- Machen Sie keine Tippfehler in den Datensätzen der Spalte „Schweregrad/Status“. Bei einem Eingabefehler wird der Datensatz übersprungen.
- Ändern Sie die Spaltennamen nicht.
- Geben Sie Spaltennamen in keine Zeile außer in die erste Zeile ein.
- Ändern Sie nicht die Reihenfolge der Blätter in der Vorlage Microsoft Excel. Die Schwachstellendaten müssen immer im zweiten Blatt vorhanden sein.
- Geben Sie Details zu Schwachstellen auf keinem Blatt mit Ausnahme des Blatts „Manuelle Erkennungen eingeben“ ein.
- Verwenden Sie nur alphanumerische Zeichen und Sonderzeichen wie Bindestrich (-), Punkt (.), Pluszeichen (+), Unterstrich (_), Leerzeichen, Klammern „(“ „)“ und das At-Symbol (@) für Dateiname

Anweisungen zum Ausfüllen der Daten in der Vorlage finden Sie unter Vorlage für die manuelle Erfassung von Schwachstellen.

Ab v24.0.6 von Vulnerability Responsekönnen Sie auch zusätzliche Spalten in der Vorlage Microsoft Excel erstellen. Weitere Informationen finden Sie unter KB1646630 .

Integrationen für manuelle Erfassung

Die Integration wird ausgelöst, wenn eine Datei hochgeladen wird. Basierend auf dem Typ der hochgeladenen Datei wird die zugehörige Integration ausgelöst.

Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen**.

Die folgenden Integrationen für manuelle Erfassung im Basissystem sind standardmäßig verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen

Integrationstyp	Beschreibung
Excel-Integration für manuelle Erfassung	Ruft Daten ab, indem die zuletzt hochgeladene Datei Microsoft Excel aus der Push-Warteschlange für Schwachstellenerfassung abgerufen wird, und kopiert den Anhang in die entsprechende Integrationsausführung.
CSV-Integration für manuelle Erfassung	Ruft Daten ab, indem die zuletzt hochgeladene CSV-Datei aus der Push-Warteschlange für Schwachstellenerfassung abgerufen wird, und kopiert den Anhang in die entsprechende Integrationsausführung.

Die Drittanbieterintegration „Manuelle Erfassung“ erstellt standardmäßig eine Integrationsinstanz mit den folgenden beiden Integrationsinstanzparametern:

- max_input_records: Definiert die Anzahl der Datensätze, die in der Vorlage erstellt werden können. Wenn Sie mehr Datensätze hinzufügen, als in diesem Parameter angegeben sind, werden die zusätzlichen Datensätze übersprungen. Die Anzahl der Datensätze kann in der Spalte „Wert“ aktualisiert werden. Die empfohlene Anzahl von Datensatzerstellungen in der Vorlage beträgt 1000. Alles über diesem Wert kann zu Leistungsproblemen führen.
- insert_fixed: Importiert behobene Schwachstellenerkennungen.

Um die Parameter der Integrationsinstanz anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen** und klicken Sie auf die Quellinstanz einer beliebigen Integration. Alternativ können Sie zu navigieren **Alle** > **Vulnerability Response** > **Integrationsinstanzen** und klicken Sie auf **Manuelle Erfassung**.

Schwachstellen manuell erfassen

Erfassen Sie Schwachstellen manuell, indem Sie eine Vorlage mit Schwachstellendaten hochladen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Datei hochladen – UI**.
2. Klicken Sie auf den Excel- oder CSV-Link, und laden Sie die Vorlage im entsprechenden Format herunter.
3. Geben Sie in der Vorlage die Schwachstellendaten in den Datensätzen ein.
   Anweisungen zum Ausfüllen der Daten in der Vorlage finden Sie unter Vorlage für die manuelle Erfassung von Schwachstellen.
4. Klicken Sie auf **Datei importieren**, und laden Sie die aktualisierte Vorlage hoch.
5. Klicken Sie auf **Absenden**.
   Die Seite „Veröffentlichungswarteschlangen für Integration von Schwachstellen“ wird angezeigt. Sie können die Liste der Integrationsinstanzen, den Status der Integrationsausführungen und Protokollnotizen anzeigen, nachdem die Integrationsausführung abgeschlossen wurde.

Nächste Maßnahme

Navigieren Sie nach dem Hochladen der Datei zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen**. Stellen Sie sicher, dass die Integrationsausführung erfolgreich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verifizieren Sie die manuelle Integrationsausführung

Stellen Sie sicher, dass die Integrationsausführung erfolgreich ist. Zeigen Sie die Anzahl der einzelnen Erkennungen und die angreifbaren Elemente (VIs) an, die während der Integrationsausführung erstellt oder aktualisiert wurden.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen**.
2. Klicken Sie auf den Namen der Integration basierend auf dem hochgeladenen Dateityp.
3. Klicken Sie auf die Registerkarte **Integrationsausführungen für Schwachstellen**.
4. Klicken Sie auf die Nummer der Integrationsausführung.
5. Klicken Sie auf die Registerkarte **Elemente**.
6. Überprüfen Sie die Informationen auf der Registerkarte **Elemente**.

Registerkarte „Elemente“.

Registerkarte/Feld	Beschreibung
Registerkarte „Elemente“.	Zeigt die Gesamtanzahl der importierten VIs an. Sie können die Gesamtzahl der importierten Erkennungen anzeigen, indem Sie die auf der Registerkarte Erkennungen aufgeführten Zahlen hinzufügen.
Neue Elemente	Zeigt die Anzahl der angreifbaren Elemente an, die bei dieser Integrationsausführung erstellt werden.
Importierte Elemente	Zeigt die Summe aller Felder in diesem Abschnitt an.
Doppelte Elemente	Zeigt doppelte Elemente an. Dieses Feld ist nicht mehr ausgefüllt.
Aktualisierte Elemente	Zeigt an, wie oft angreifbare Elemente während dieser Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als 2 aktualisierte Elemente angezeigt.
Unveränderte Elemente	Zeigt angreifbare Elemente an, die während der Integrationsausführung gefunden wurden und in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

Nächste Maßnahme

Nachdem Sie sich verifiziert haben, dass die Integrationsausführung erfolgreich ist, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Verlauf hochgeladener Dateien**. Überprüfen Sie, ob in den Notizen fehlerhafte Datensätze vorhanden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Manuelle Erkennungen für automatisches Schließen konfigurieren

Aktivieren Sie das automatische Schließen manueller Erkennungen, um veraltete manuelle Erkennungen automatisch zu schließen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Datei hochladen – UI**.
2. Klicken Sie auf **Konfiguration für automatisches Schließen ändern**.
3. Klicken Sie auf die Registerkarte **Manuelle Erkennungen**.
4. Stellen Sie sicher, dass das Kontrollkästchen **Manuelle Erkennungen automatisch schließen** aktiviert ist.
5. Geben Sie im Feld **Zuletzt gefundene manuelle Erkennungen (vor Tagen)** die Anzahl der Tage ein, nach denen die manuellen Erkennungen geschlossen werden sollen.
   Der Standardwert ist 90 Tage. Sie können einen beliebigen positiven Wert für die Anzahl der Tage eingeben.

Überprüft den Upload-Status

Überprüfen Sie, ob die Ausführung der Schwachstellenintegration erfolgreich, teilweise erfolgreich oder fehlgeschlagen war.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Verlauf hochgeladener Dateien**.
2. Überprüfen Sie in der Tabelle „Push-Warteschlangen für Schwachstellenintegration“ in den Spalten Erstellt und Status die Uhrzeit des Uploads und den Status des Uploads.
3. **Wahlweise:** Zeigen Sie im Feld **Notizen** den Grund für den Fehler an.

Vorlage für die manuelle Erfassung von Schwachstellen

Die Vorlage enthält Spalten, die mit Daten zu Schwachstellen und Configuration Item (CI) gefüllt werden müssen. Nachdem die Vorlage ausgefüllt und hochgeladen wurde, werden die Daten verarbeitet.

Anweisungen zum Ausfüllen der Vorlage

Um die Details in die Vorlage einzugeben, befolgen Sie die Anweisungen in der folgenden Tabelle.

Vorlagenanweisungen

Spalte	Erforderlich/ optional?	Zeichenfolgenlänge (max.)/gültige Werte	Beschreibung
Asset-ID	Optional	255	Universally Unique Identifier (UUID) oder Asset-ID. Dies kann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorlagenanweisungen (Fortsetzung)

Spalte	Erforderlich/ optional?	Zeichenfolgenlänge (max.)/gültige Werte	Beschreibung
			der von einem Scanner generierte Wert sein.
Geben Sie Informationen in mindestens eine der folgenden fünf Spalten ein:			
MAC-Adresse	Erforderlich	24	Host- oder Asset-Informationen. Die Kombination aller angegebenen Werte muss für ein Asset eindeutig sein.
FQDN	Erforderlich	255	
NETBIOS	Erforderlich	255	
IP-Adresse	Erforderlich	255	
Host-Name	Erforderlich	255	
Die verbleibenden Spalten sind nicht voneinander abhängig.			
Schwachstellen-ID	Erforderlich	255	Stellt eine Schwachstelle in der National Vulnerability Database (NVD) oder eine ID dar, die von einem Drittanbieterscanner zurückgegeben wird.
Schwachstellenzusammenfassung	Optional	512	Kurze Beschreibung der Schwachstelle. Sie wird der Datenbank nur hinzugefügt, wenn die Schwachstellen-ID nicht verfügbar ist.
Schweregrad	Optional	kritisch, hoch, mittel, niedrig, keine	Schweregrad der Schwachstelle. Sie wird der Datenbank nur hinzugefügt, wenn die Schwachstellen-ID nicht verfügbar ist. Wenn der Datensatz leer ist, wird er standardmäßig als kritisch betrachtet.
Port	Optional	Nicht zutreffend	Port, von dem die Schwachstelle erkannt wird. Der Wert muss eine gültige Ganzzahl sein. Bei einer ungültigen Eingabe wird der Datensatz übersprungen.
Protokoll	Optional	40	Typ des verwendeten Netzwerkprotokolls.
Nachweis	Optional	4000	Stellt den Speicherort oder Systempfad der Schwachstelle dar.
Status	Optional	offen, behoben	Status der Erkennung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorlagenanweisungen (Fortsetzung)

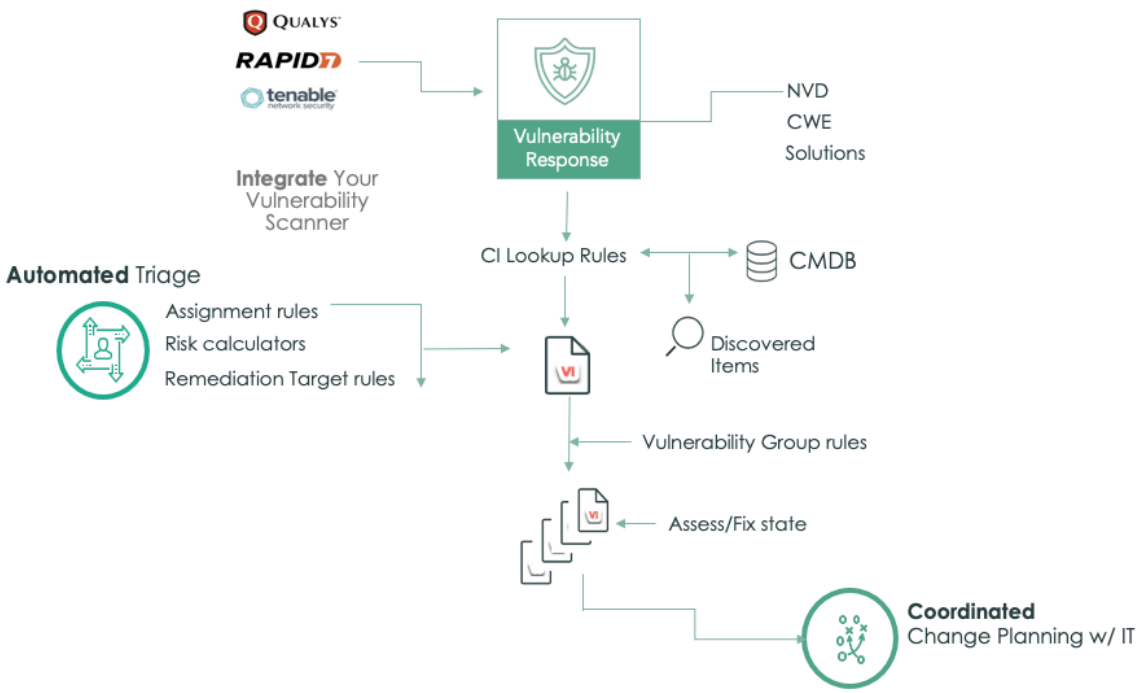
Spalte	Erforderlich/ optional?	Zeichenfolgenlänge (max.)/gültige Werte	Beschreibung
			Wenn der Datensatz leer ist, gilt er standardmäßig als geöffnet.

Vulnerability Response Übersicht über Nachbesserung

Vulnerability Response Die Nachbesserung ist ein phasenweiser Prozess, der aus der Überprüfung des Importabschlusses, der Selektierung neuer Schwachstellen und der Überwachung des Fortschritts bis zum Abschluss besteht. Auf diese Weise wird die Nachbesserung verwaltbar, rechtzeitig und in vielerlei Hinsicht automatisiert.

Wenn Sie Ihre Sicherheitslage für alle Unternehmens-Assets kennen, können Sie die kritischsten Schwachstellen identifizieren, die behoben werden müssen. Dieser Nachbesserungsprozess erfordert, dass Vulnerability Response und eine Drittanbieterintegration wie Qualys Vulnerability Integration installiert und konfiguriert sind.

Prozess-Flow für Vulnerability Response-Integration



Überprüft den erfolgreichen Abschluss von Importen von Drittparteiintegrationen

Die erste Phase in diesem Prozess besteht darin, sicherzustellen, dass alles wie vorgesehen funktioniert. Vulnerability Response ist zum Herunterladen von Schwachstellen in der National Vulnerability Database (NVD) und Common Enumeration Weakness (CWE) voreingestellt. Durch Importe von Drittparteien erhalten Sie die Daten, die Sie zum Erstellen angreifbarer Elemente und für Korrekturaufgaben benötigen. Eine erfolgreiche Nachbesserung hängt vom konsistenten und erfolgreichen Import von Schwachstellen und angreifbaren Elementen ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Imports gleichen CI-Suchregeln Assets von Drittparteien mit Assets in Configuration Management Database (CMDB)ab. Alle Assets werden im Modul „Erkannte Elemente“ gespeichert. CI-Informationen sind für die Implementierung der Lösung von entscheidender Bedeutung.

Hinweis:
Sobald eine Drittanbieterintegration installiert und konfiguriert wurde, kann ein Import in einigen Fällen fehlschlagen, z. B. wenn der Drittanbieter seine API-Aufrufe drosselt. Wenn beim Import ein Fehler auftritt, ist sofortige Aufmerksamkeit erforderlich.

Im Lieferumfang der -Anwendungen enthaltene Berichte zur Integrationsstatusausführung für unterstützte Drittanbieterintegrationen bieten Ihnen eine grafische Übersicht über Ihre Importe. Verwenden Sie diesen Bericht, oder erstellen Sie einen eigenen, um auf einfache Weise zu bestimmen, ob Ihr letzter Import erfolgreich war. Weitere Informationen zu unterstützten Integrationen finden Sie unter Vulnerability Response-Integrationen.

Überprüfen und selektieren Sie Schwachstellen und angreifbare Elemente

Die nächste Phase der Nachbesserung erfordert die Überprüfung auf neue Schwachstellen und angreifbare Elemente. Ein angreifbares Element (VI) ist eine erkannte Kombination aus Schwachstelle und Konfigurationselement (Configuration Item, CI). Bei der Bildung angreifbarer Elemente werden verschiedene Regeln ausgeführt, die VIs zuweisen, das Risiko bestimmen, das sie darstellen, und Korrekturziele festlegen. Passen Sie alle Regeln nach Bedarf an, um sicherzustellen, dass die angreifbaren Elemente erfolgreich selektiert wurden.

Überwachen Sie den Fortschritt der Nachbesserung vorhandener Schwachstellen

Die letzte Phase der Nachbesserung besteht in der Überwachung Ihres Fortschritts.

- Überprüfen Sie den Status von Importen für Patch-Implementierungen, die nicht angezeigt wurden, und wenden Sie sich an die IT-Abteilung.
- Verfolgen Sie den Fortschritt bei der Erfüllung gesetzlicher Compliance-Verpflichtungen, und stellen Sie deren Erfüllung sicher.
- Überprüfen Sie den Status zurückgestellter Elemente, und überarbeiten oder implementieren Sie Korrekturen.
- Überwachen Sie die Dashboards für Schwachstellenmanagement. Um Trends zu überprüfen, Berichte in Echtzeit anzuzeigen und Metriken zu verwenden, mit denen Sie Ihre Nachbesserungsziele nachverfolgen, können Sie Ihre Prozesse mit der Anwendung Performance Analytics for Vulnerability Response überwachen.
- Veraltete Erkennungen in werden geschlossen Vulnerability Response.

Überprüft den erfolgreichen Abschluss von Vulnerability Response Integrationsimporten

Am einfachsten können Sie feststellen, ob Ihre Importe erfolgreich waren, indem Sie ein Dashboard für den Integrationsausführungsstatus verwenden. Das Dashboard „Status der Integrationsausführung“ bietet ein Beispiel für eine grafische Ansicht des Status von Integrationsausführungen von Drittanbietern.

Die Schwachstellen-Integrationen Qualys und Rapid7 verfügen über ein Status-Dashboard für die Integrationsausführung. Ausführliche Informationen zum Diagramminhalt finden Sie unter Qualys Statusdiagramm der Integrationsausführung oder Rapid7 Vulnerability-Integration Statusdiagramm für die Ausführung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Diagramme für Integrationen, die nicht von ServiceNow® bereitgestellt werden, können aus Berichten in einem Dashboard erstellt werden, erfordern jedoch möglicherweise ServiceNow -Kenntnisse. Weitere Informationen zum Erstellen von Berichten und Dashboards finden Sie unter Erste Schritte mit Berichten und Dashboards.

Zeigen Sie Vulnerability Response Erkennungsdaten für angreifbare Elemente an

Die vollständigen Daten, die von Ihren Drittanbieter-Scanner-Integrationen mit Vulnerability Response gesammelt wurden, werden auf den Registerkarten Erkennungen und Erste Erkennungen in den Datensätzen zu angreifbaren Elementen (VIT) angezeigt. Es wird auch in Erkennungsdatensätzen in der Liste „Erkennung angreifbarer Elemente“ in Ihrer Instanz Now Platform® angezeigt.

Vorbereitungen

Drittanbieterintegrationen rufen Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, die von den Scannern gemeldet werden. Erkennungsdaten werden mit angreifbaren Elementen gekoppelt, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn kein VI gefunden wird, wird ein neues erstellt. Erkennungen werden nur durch Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden wurden.

Erforderliche Rolle:

- sn_vuln.admin initiiert Integrationsausführungen und zeigt Daten zur Erkennung angreifbarer Elemente an.
- sn_vul.remediation_owner ist angreifbare Elemente zugewiesen, die aus Erkennungen angreifbarer Elemente erstellt wurden, und zeigt Daten in VI-Datensätzen an.

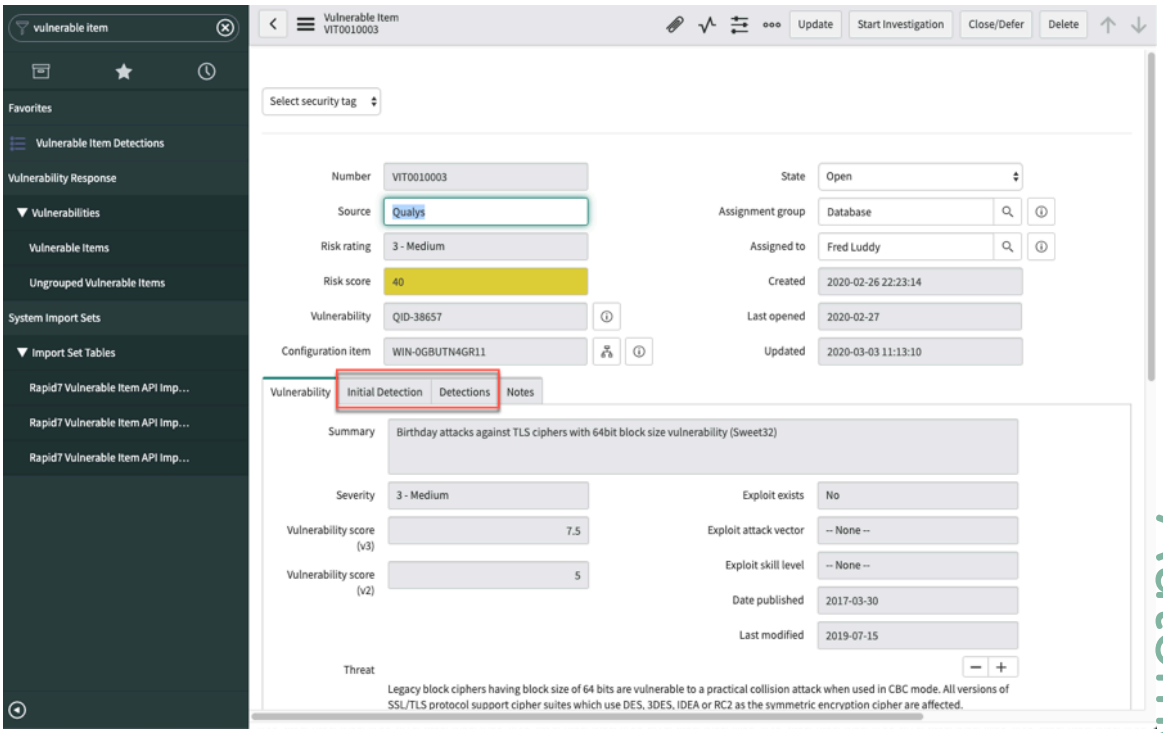
Prozedur

1. Um die Erkennungsdaten für angreifbare Elemente anzuzeigen, navigieren Sie zu einem Datensatz für ein angreifbares Element, und öffnen Sie ihn.

   Der Datensatz wird mit den Registerkarten Anfängliche Erkennungen und Erkennungen angezeigt.

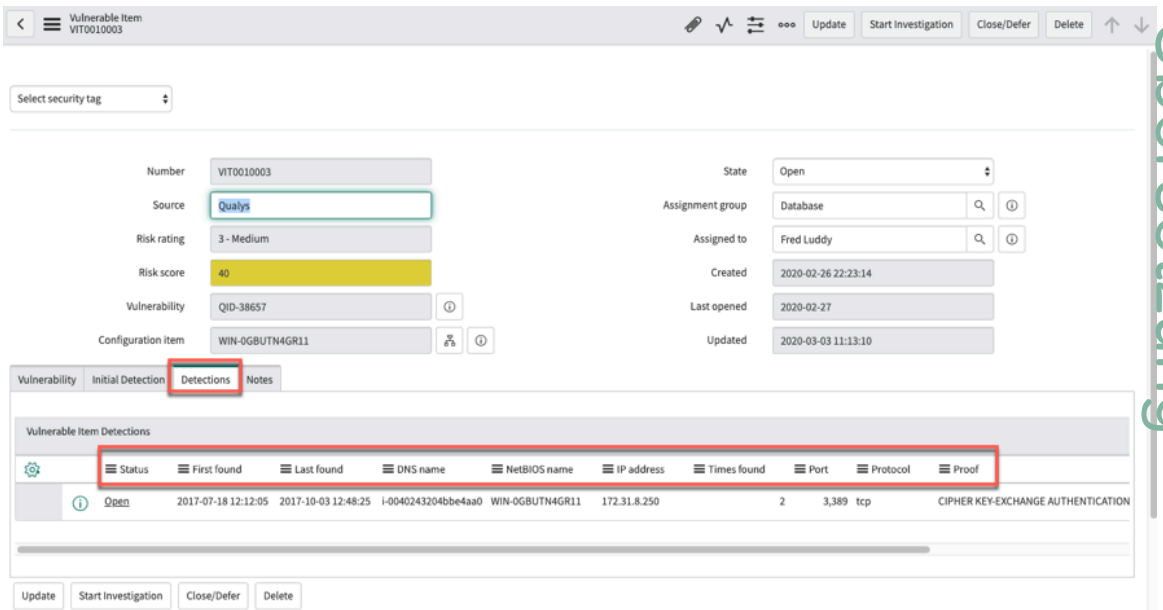
   Hinweis:
   Daten, die zuvor auf der Registerkarte Konfigurationsdetails angezeigt wurden, werden zusammen mit anderen Erkennungsdaten auf den Registerkarten Anfängliche Erkennung und Erkennungen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf die Registerkarte **Erkennungen**.

Wenn ein angreifbares Element anhand der Ergebnisse eines Drittanbieterscans erstellt wird, werden die Daten des Scans im Erkennungsdatensatz angezeigt (siehe folgende Abbildung).



Jede Zeile im Abschnitt „Erkennungen von angreifbaren Elementen“ stellt Daten aus einer eindeutigen Erkennung dar. In der Spalte Zuerst gefunden wird das Datum angezeigt, an dem das angreifbare Element zum ersten Mal vom Scanner erkannt wurde. In der Spalte Zuletzt gefunden wird das Datum der aktuellsten Erkennung angezeigt. Im Feld Quelle wird der Scanner angezeigt, der die Daten abgerufen hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für Qualyssind mit Erkennungen angreifbarer Elemente die folgenden Felder im VI-Datensatz veraltet und werden nicht mehr ausgefüllt:

- Qualys Schweregrad
- Zuletzt aktualisiert von Quelle

Auch für Qualyswird wie in der vorherigen Abbildung gezeigt Folgendes gilt: Wenn ein VI aus einem Scan erstellt wird, wird der Wert aus dem Scan nach Ergebnissen in der Spalte Nachweis im Erkennungsdatensatz angezeigt. Dieser Wert wird jedoch nicht im oberen Teil des VI-Datensatzes angezeigt.

Wenn für Rapid7 ein AE aus einem Scan erstellt wird, kann der Wert für „Nachweis aus dem Scan“ sowohl in der Nachweisspalte im Erkennungsdatensatz als auch im oberen Teil des AE-Datensatzes angezeigt werden, jedoch nicht standardmäßig. Um diesen Wert im oberen Teil des VI-Datensatzes anzuzeigen, wählen Sie das Feld Nachweis im Formularlayout aus.

3. **Wahlweise:** Führen Sie die folgenden Schritte aus, um das Layout der Registerkarte Erkennungen im Datensatz zu konfigurieren.

   a. Die folgenden Spalten werden standardmäßig auf der Registerkarte Erkennungen angezeigt.

   - Status
   - Zuerst gefunden (Daten)
   - Zuletzt gefunden (Datum)
   - DNS-Name
   - Net-BIOS-Name
   - IP-Adresse
   - Mal gefunden
   - Port
   - Protokoll
   - Nachweis
   - SSL

   Hinweis:

   (Optional) Hinweis: Wenn in einer Spalte kein Wert vorhanden ist, wurden die Daten für dieses Feld vom Scanner nicht erkannt.

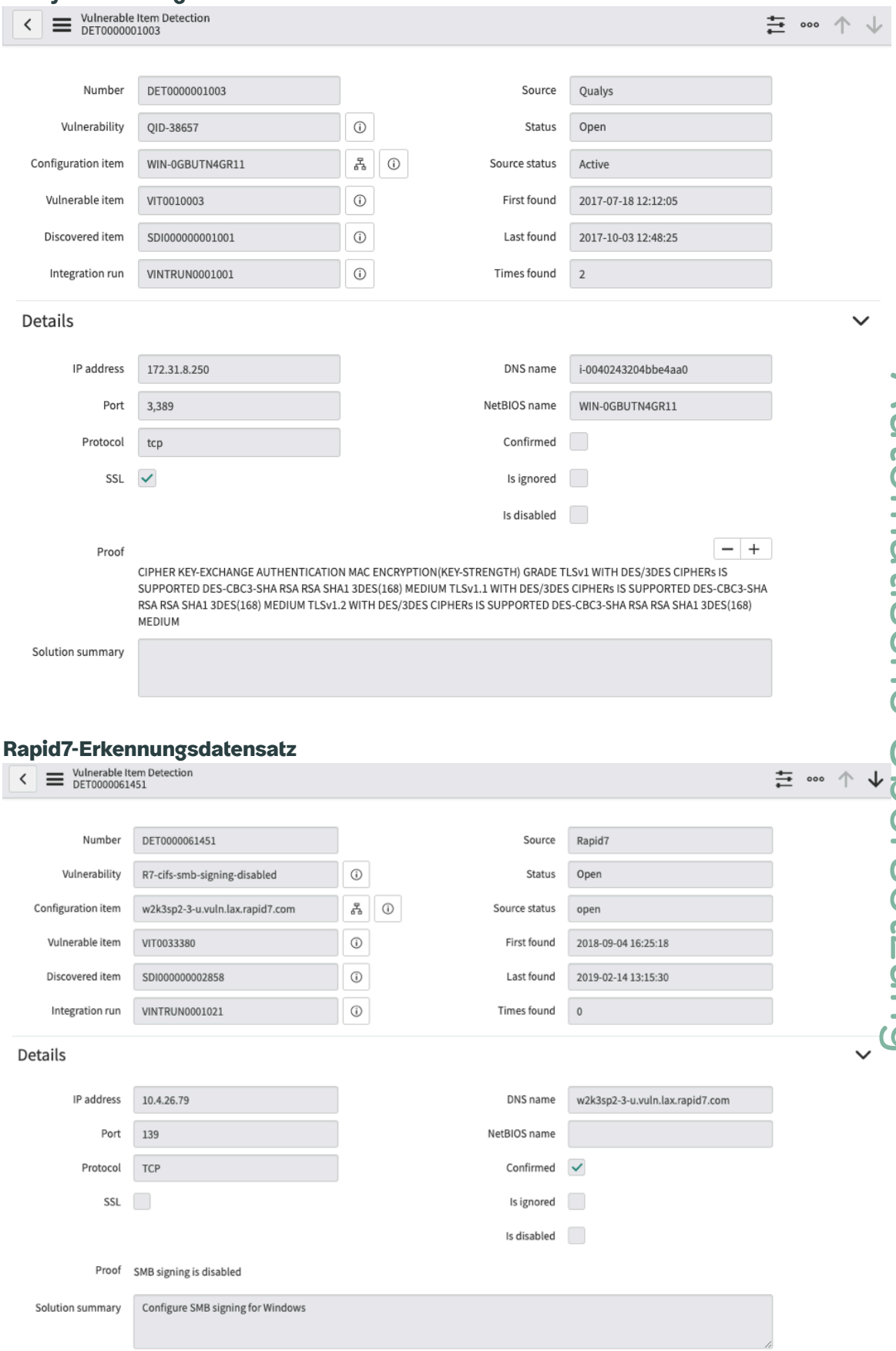
   b. Klicken Sie auf das Zahnradsymbol ( ), um Ihre Ansicht zu personalisieren.

   c. Wählen Sie die Spalten aus dem Slushbucket aus, um bestimmte Daten anzuzeigen, und klicken Sie auf **OK**.

4. Klicken Sie bei ausgewählter Registerkarte Erkennungen in der Spalte Status auf ein Element, um den Erkennungsdatensatz zu öffnen und die Details anzuzeigen, die diesem angreifbaren Element zugeordnet sind, einschließlich einer Lösungszusammenfassung (nur Rapid7 InsightVM-Integration).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys Erkennungsdatensatz



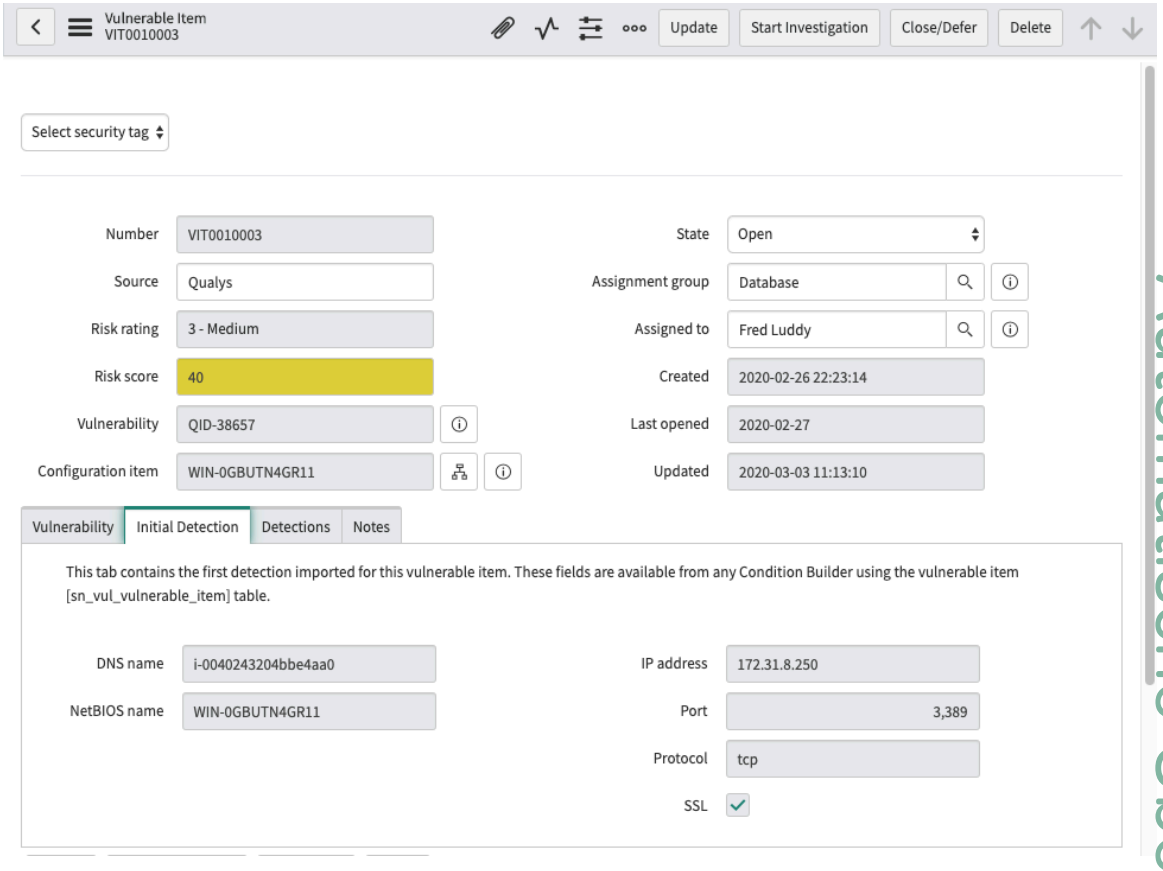
Rapid7-Erkennungsdatensatz

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Kehren Sie zum Datensatz zurück, und wählen Sie die Registerkarte Ursprüngliche Erkennung aus.

   Auf der Registerkarte Anfängliche Erkennungen werden die Daten angezeigt, die beim ersten Vorkommen der Erkennung vom Scanner des Drittanbieters importiert wurden. Diese Informationen auf der Registerkarte „Ersterkennung“ ändern sich nicht, wenn Erkennungsdaten aktualisiert werden.

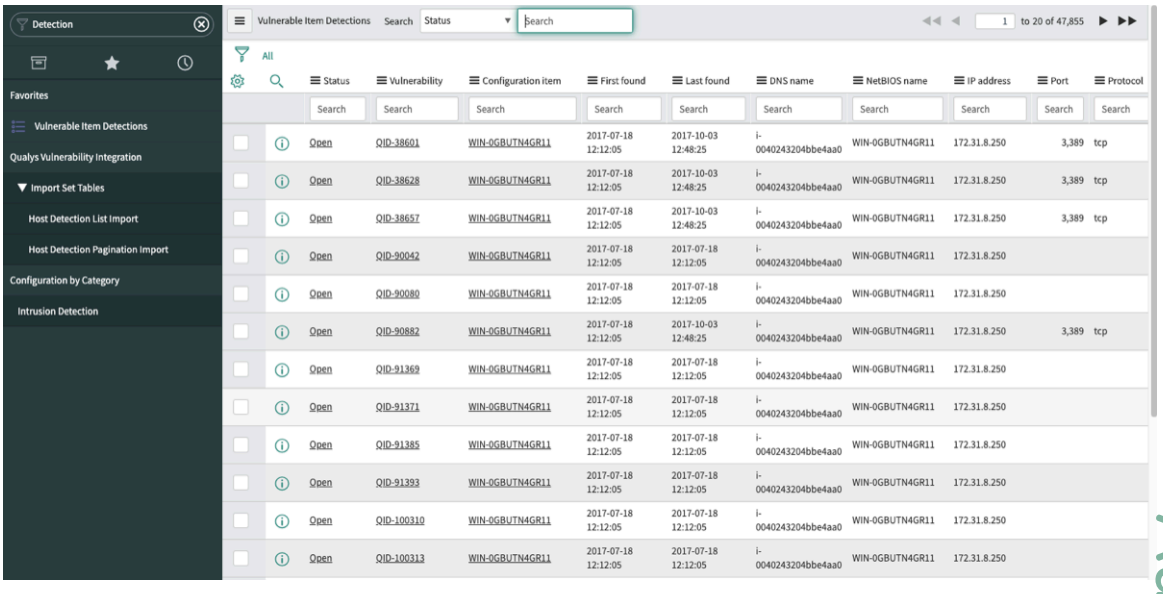


6. **Wahlweise:** Navigieren Sie zu Angreifbares Element Erkennungen, um die Erkennungsliste für angreifbare Elemente anzuzeigen.

   (Optional) Die Liste „Erkennung angreifbarer Elemente“ wird angezeigt. Jede Zeile in der Liste „Erkennungen angreifbarer Elemente“ steht für eine eindeutige Erkennung. Die Spalten zeigen dieselben Daten an wie der VI-Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erkennungen werden nur durch Daten geöffnet oder geschlossen, die von einem Scanner gefunden wurden. Es findet kein Rolldown von VIs statt. Beim Import von Erkennungen werden VIs erstellt und die Status von VIs aktualisiert. Wenn alle Erkennungen für ein angreifbares Element geschlossen sind, wird dieses angreifbare Element geschlossen. Im VI-Datensatz ist der Status „Geschlossen“ und der Substatus „ Fest“.

Hinweis:
Fehler werden protokolliert während:

- Vom Scanner abgerufene Anhänge werden verarbeitet.
- Erkennungen oder angreifbare Elemente werden erstellt oder aktualisiert.

Informationen zur Behandlung von Erkennungsfehlern finden Sie unter Fehlerbehandlung für Erkennungen.

Wenn alle VIs für eine Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen.

Geschlossene VIs mit dem Substatus „ **Repariert** “ oder **„Veraltet“** werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIs mit der neuen Schwachstelle abgeglichen werden können.

Angreifbare Elemente, die in Ihrer Instanz auf **„Gelöst“** festgelegt sind, aber durch die nachfolgenden Integrationsausführungen nicht in den **Status „Geschlossen“/„Behoben“** versetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Wenn alle VIs für eine Korrekturaufgabe geschlossen sind, wird der Datensatz geschlossen.

Angreifbare Elemente, die in Ihrer Instanz auf „Gelöst“ festgelegt sind, aber von den nachfolgenden Integrationsausführungen nicht in den Status „Geschlossen/Behoben“ versetzt werden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Für Rapid7 -Erkennungen ist auf der Rapid7-Konfigurationsseite in Ihrer -Instanz jetzt eine Option verfügbar, um gelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden VIs, die auf **„Gelöst“** gesetzt, aber dann nicht von nachfolgenden Scans auf **„Geschlossen“/„Behoben“** gesetzt wurden, nach der von Ihnen eingegebenen Anzahl von Tagen zurück in den Status „ **Offen“** geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Scanner für Qualys Erkennungen weiterhin VIs findet, die auf „Gelöst“ festgelegt wurden, dann aber nicht durch nachfolgende Scans in den Status **„Geschlossen“/ „Behoben“** geändert wurden, werden diese VIs zurück in den Status „Offen **“ verschoben**, wenn das Datum der letzten Suche nach dem Datum „Gelöst“ liegt.

Nächste Maßnahme

Um weitere Daten, einschließlich Element- und Erkennungsanzahlen, anzuzeigen, können Sie Überprüfen Sie Vulnerability Response die Erkennungsdaten für angreifbare Elemente in Integrationsausführungsdatensätzen (VINTRUN)..

Überprüfen Sie Vulnerability Response die Erkennungsdaten für angreifbare Elemente in Integrationsausführungsdatensätzen (VINTRUN).

In den Datensätzen der Integrationsausführung in Ihrer Instanz Now Platform® können Sie Erkennungsdaten für angreifbare Elemente von Drittanbieterintegrationen basierend auf dem Datum und der Uhrzeit der Scans suchen. Überprüfen Sie, ob der Scan erfolgreich abgeschlossen wurde, und zeigen Sie die Anzahl (Anzahlen) der einzelnen Erkennungen sowie alle angreifbaren Elemente (VIs) an, die direkt als Ergebnis der Scans erstellt oder aktualisiert werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vuln.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Möglicherweise möchten Sie die Informationen zur Integrationsausführung, entweder Datum und Uhrzeit des Scans, oder die Datensatznummer der Integrationsausführung (VINTRUN#) aus dem angreifbaren Element oder den Erkennungsdatensätzen, um bestimmte Datensätze in den folgenden Listen finden zu können.

Prozedur

1. Wählen Sie eine, um fortzufahren.

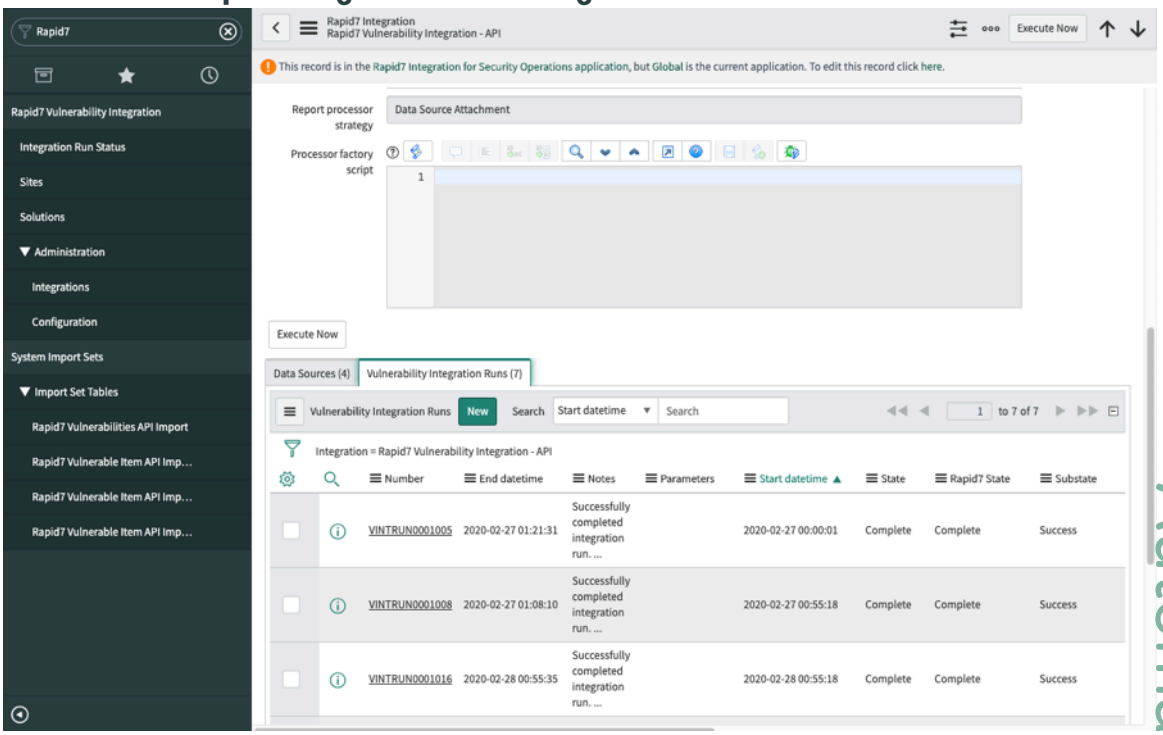
2. Klicken Sie unten auf der angezeigten Seite auf die Registerkarte **Integrationsausführungen für Schwachstellen**.

3. Klicken Sie auf ein Element in der Spalte Anzahl oder Importquelle, um einen Datensatz zu öffnen.

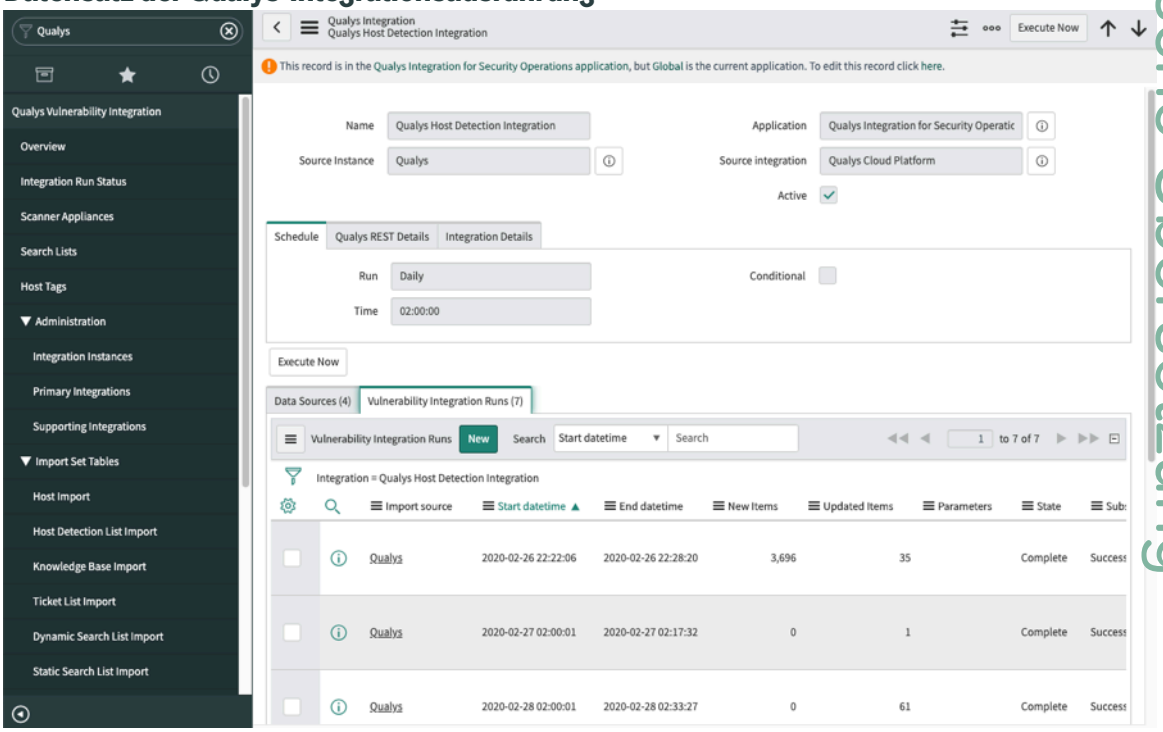
   Der Datensatz der Integrationsausführung wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatz der Rapid7-Integrationsausführung

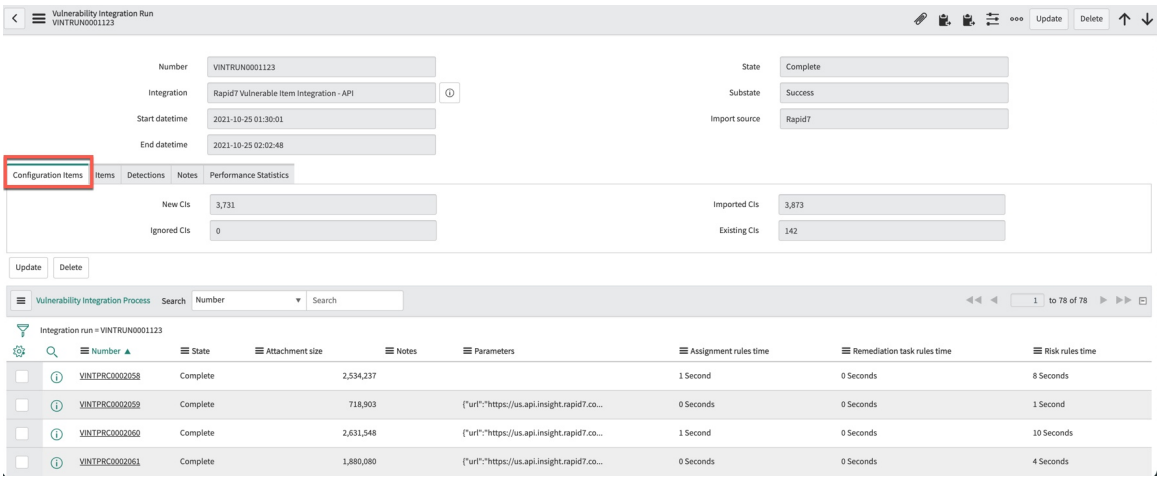


Datensatz der Qualys-Integrationsausführung



Der Datensatz der Integrationsausführung wird angezeigt. Ob die Integration erfolgreich ausgeführt wurde, können Sie im Feld Status überprüfen. Wählen Sie die Registerkarte **Konfigurationselemente** aus.

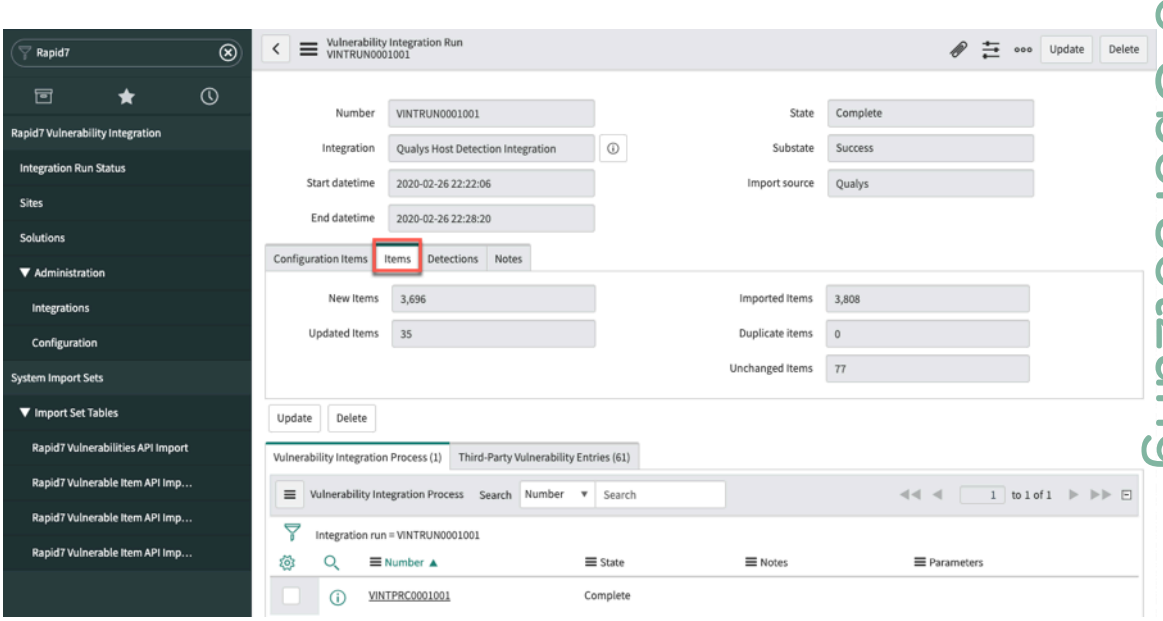
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Registerkarte Konfigurationselemente werden die folgenden Informationen angezeigt:

- Auf der Registerkarte Konfigurationselemente wird die Gesamtzahl der importierten Konfigurationselemente angezeigt.
- Das Feld Neue CIs zeigt die Anzahl der CIs an, die als Teil dieser Integrationsausführung erstellt wurden.
- Das Feld Importierte CIs zeigt die Summe aller CIs in diesem Abschnitt an.
- Der Wert des Felds Ignorierte CIs ist für die Vulnerability Response Integrationen immer 0.
- Das Feld Vorhandene CIs zeigt die Gesamtzahl der bereits vorhandenen CIs an.

Klicken Sie auf die Registerkarte **Elemente**.



Auf der Registerkarte Elemente werden die folgenden Informationen angezeigt:

- Auf der Registerkarte „Elemente“ wird die Gesamtzahl der importierten AEs angezeigt. Sie können die Gesamtzahl der importierten Erkennungen anzeigen, indem Sie die auf der Registerkarte Erkennungen aufgeführten Zahlen hinzufügen.
- Das Feld Neue Elemente zeigt die Anzahl der angreifbaren Elemente an, die bei dieser Integrationsausführung erstellt werden.
- Das Feld Importierte Elemente zeigt die Summe aller Felder in diesem Abschnitt an.

Automatische Übersetzung

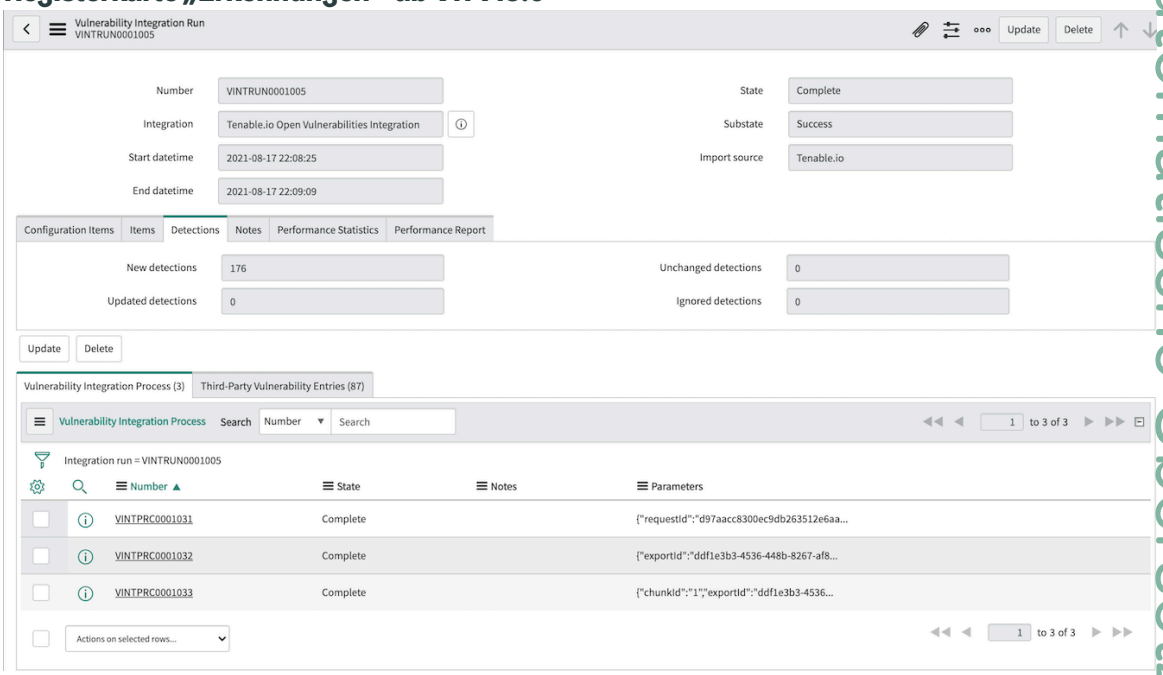
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Feld „Elemente duplizieren“ ist nicht mehr ausgefüllt.
- Das Feld Aktualisierte Elemente zeigt an, wie oft angreifbare Elemente während dieser Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als 2 aktualisierte Elemente angezeigt.
- Das Feld Unveränderte Elemente zeigt angreifbare Elemente, die während der Integrationsausführung gefunden wurden und bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

4. Klicken Sie auf die Registerkarte **Erkennungen**.

Diese Registerkarte wird nur angezeigt, wenn für die Integrationsausführung Erkennungen vorhanden sind. Sie können die Gesamtzahl der importierten Erkennungen überprüfen, indem Sie die aufgeführten Zahlen hinzufügen.

Registerkarte „Erkennungen “ ab VR v15.0



Hinweis:
Vor v15.0 gab es kein Feld für ignorierte Erkennungen.

Auf der Registerkarte Erkennungen werden die folgenden Informationen angezeigt:

- Ab v15 wurde ein neues Feld Ignorierte Erkennungen hinzugefügt, um die zuvor ignorierten Erkennungen nachzuverfolgen. Mit dieser Implementierung werden die Anzahl der importierten Erkennungen und die in Datensätzen der Integrationsausführung nachverfolgte Anzahl konsistent. Diese Funktionalität wurde für alle Scanner implementiert, d. h. Qualys Vulnerability Integration, Rapid7 Vulnerability-Integration, Tenable Vulnerability Integration und MicrosoftMicrosoft Azure Event Hubs TVM.
- Im Feld Neue Erkennungen werden neue Erkennungen angezeigt, die während dieser Integrationsausführung erstellt werden.
- Im Feld Unveränderte Erkennungen werden während der Integrationsausführung gefundene Erkennungen angezeigt, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Feld Aktualisierte Erkennungen zeigt an, wie oft Erkennungen während dieser Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der aktualisierten eindeutigen Erkennungen. Wenn beispielsweise eine Erkennung im Rahmen der Integrationsausführung zweimal aktualisiert wird, wird sie zweimal gezählt und als 2 aktualisierte Erkennungen angezeigt.

Hinweis:
Erkennungen, die in diesen Anzahlen nicht angezeigt werden, sind Erkennungen, die sich im Status „Geschlossen“ (Behoben) befinden, da feste Datensätze zum Aktualisieren vorhandener VIs verwendet werden. Wenn Sie diese Erkennungsdatensätze transparenter machen möchten, können Sie die geschlossenen VIs anzeigen, die erstellt werden, wenn kein passendes VI im Status „Offen“ vorhanden ist. Weitere Informationen zu Schwachstellen im festen Status, die Sie im Setup-Assistenten für die Qualys-Integration aktivieren können, finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

5. Klicken Sie auf ein Element in der Spalte Anzahl oder Importquelle, um einen Datensatz zu öffnen.

Anzeigen von Patch-Daten und Planen von Patches in Vulnerability Response

Ab v16.1 von Vulnerability Responsekönnen Sie Patches planen und Patchdaten zusammen mit Lösungs- und anderen Schwachstelleninformationen in Datensätzen sowohl in der klassischen Umgebung als auch in den Vulnerability Response -Arbeitsbereichen in Ihrer Instanz Now Platform anzeigen.

Erforderliche Rollen

Benutzer benötigen Rollen, die für die Patch Orchestration-Integration spezifisch sind, die Sie zum Importieren Ihrer Patches verwenden, um Daten anzuzeigen und Patches zu planen. Weitere Informationen finden Sie unter den unterstützten Integrationen.

- Informationen zur Integration der HCL BigFix Patch Orchestration in mit Vulnerability Responseund Informationen zur Integration der Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM.
- Patch-Orchestrationsdaten werden in den Dashboards Vulnerability Response angezeigt in der klassischen Umgebung.
- Daten zu Bewertungslisten im Vulnerability Response Arbeitsbereicheanzeigen.

Planen von Patches

Sie können Patches von den folgenden Datensätzen aus planen:

- Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkanntes Element (SDI)

Patchen Sie Daten in der klassischen Umgebung

In der klassischen Umgebung in der Anwendung Vulnerability Response :

- Um Patch-Update-Datensätze anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Patches**.
- Um Lösungen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Lösungen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um Ihnen zugewiesene VIs mit Patches anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir zugewiesen mit Patches**.
- Um Korrekturaufgaben anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir zugewiesen mit Patches**
- Um Datensätze erkannter Elemente anzuzeigen, navigieren Sie zu **Alle** > **Security Operations** > **Erkannte Elemente**.

Patchen Sie Daten und Status-Rollup für die Patch-Orchestrierung in Vulnerability Response

Ab v16.1 von Vulnerability Response werden Patch-Daten und -Status für Patch-Update und andere Datensätze in der Anwendung Vulnerability Response zusammengefasst.

Patch-Update-Datensätze in den Arbeitsbereichen in der klassischen Umgebung in Vulnerability Response

Informationen zu Patches, Schwachstellenlösungen und Schwachstellen sind alle in der Anwendung Vulnerability Response verbunden.

Patch-Daten und Patch-Rollup-Daten sowie deren Status werden für die Datensätze in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit Vulnerability Responseenthalten. Zeigen Sie VPU-Datensätze (Patch) in Vulnerability Response-Arbeitsbereichen in der Listenansicht im IT-Nachbesserungs-Arbeitsbereich an. Die Patch-Update-Datensätze in der klassischen Ansicht und in Vulnerability Response-Arbeitsbereichen enthalten die folgenden Daten:

- Daten und Informationen zur Schwachstellenlösung von Patch-Lieferanten, die von der Anwendung Vulnerability Solution Management importiert werden.
- Quellkorrekturstatus, der die Gesamtzahl der Geräte mit einer Schwachstelle umfasst, die durch einen Patch behoben werden kann, sowie alle Geräte, für die Updates fehlen.
- Korrekturstatus, der den Prozentsatz der korrigierten VIs und die Gesamtzahl der VIs enthält, die einen Patch als bevorzugten Patch haben.
- Zugehörige Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen für zugehörige Links zu Datensätzen in der Klassenansicht. Diese Daten werden auf Registerkarten in Datensätzen in Vulnerability Response-Arbeitsbereichen angezeigt.
- Patch-Anforderungen, die von Korrekturbesitzern zur Genehmigung übermittelt wurden.

Erforderliche Rollen

Benutzer benötigen Rollen, die für die Patch Orchestration-Integration spezifisch sind, die Sie zum Anzeigen von Daten und Planen von Patches verwenden. Weitere Informationen finden Sie unter den unterstützten Integrationen.

- Informationen zur Integration der HCL BigFix Patch Orchestration in mit Vulnerability Responseund Informationen zur Integration der Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM.
- Patch-Orchestrationsdaten werden in den Dashboards Vulnerability Response angezeigt in der klassischen Umgebung.
- Daten zu Bewertungslisten im Vulnerability Response Arbeitsbereicheanzeigen.

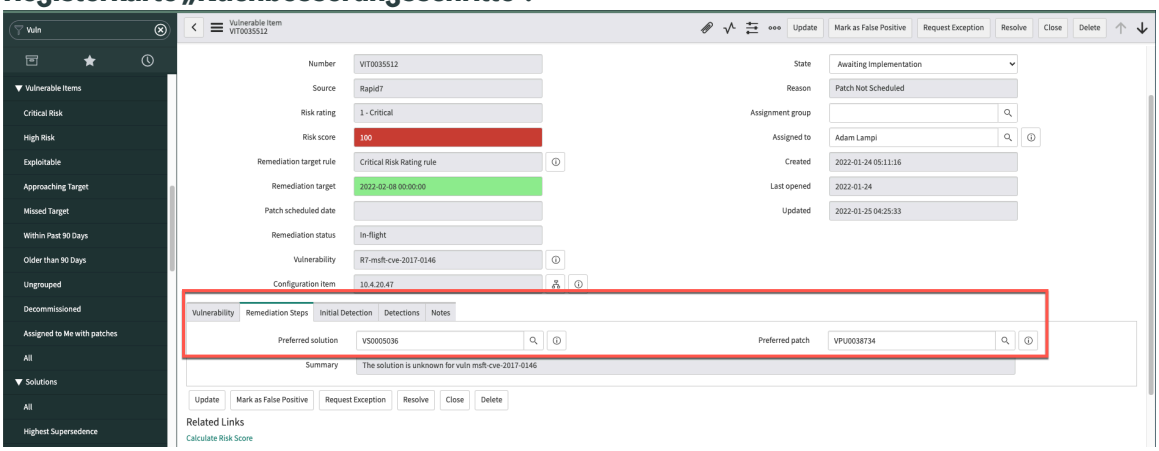
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Patchen Sie Daten und Status-Rollup

Um die angreifbaren Elemente anzuzeigen, für die Patches vorhanden sind und die Ihnen in der klassischen Umgebung zugewiesen sind, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir zugewiesen mit Patches**.

Wenn der Datensatz eines angreifbaren Elements mit einem bevorzugten Patch gefüllt ist, wechselt er nur dann automatisch in **den Status Warten auf Implementierung**, wenn der Status des VI nicht **Geschlossen**, **Gelöst**, **Zurückgestellt** oder **In Überprüfung**lautet. Um einen Drilldown in die Daten durchzuführen und die bevorzugte Lösung und andere Daten anzuzeigen, klicken Sie im VI-Datensatz auf die Registerkarte **Nachbesserung**.

Registerkarte „Nachbesserungsschritte“.



Ein AE mit einem bevorzugten Patch geht in den folgenden Fällen in **den Status „Warten auf Implementierung“** über:

- Wenn ein Patch für die Bereitstellung in einem CI geplant ist, das Teil eines Sammlungsimports ist, und dem CI ein VI zugeordnet ist, lautet der Grund für das VI **Warten auf ImplementierungPatch Geplant**.
- Status von Das AE lautet **Warten auf Implementierung,** und der Grund ist **„Patch geplant (fehlendes Zieldatum)“**als Grund.
- Wenn ein Patch nicht für die Bereitstellung in einem CI geplant ist, das Teil eines Sammlungsimports ist, lautet der Status des AE „ **Warten auf Implementierung“**mit dem Grund für **„Patch nicht geplant“**.

Klicken Sie auf das Symbol **Preferred Patch** Information (Bevorzugter Patch), um die Patch-Updates zu öffnen und die folgenden Informationen in den zugehörigen Links anzuzeigen:

Angreifbare Elemente

Angreifbare Elemente, die diesem Patch zugeordnet sind.

Zugeordnete Geräte

Geräte mit Updates und Geräte ohne Updates.

Patch-Bereitstellungen

Für diesen Patch geplante Bereitstellungen auf einzelnen Computern (Assets) oder auf Gruppen von Assets.

Patch-Anforderungen

Eine Liste der Patch-Anforderungen, die zur Genehmigung gesendet wurden, bevor sie für die Bereitstellung geplant sind

Potenzielle Patches

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Patches, die eine Schwachstelle beheben können.

Klicken Sie auf das Symbol **„Informationen zu bevorzugtem Patch“**, um den Datensatz zu öffnen und die zuvor aufgeführten Informationen sowie die folgenden Patch-Update-Daten anzuzeigen:

Quellenkorrekturstatus

Die Gesamtzahl der Geräte, die diesen Patch benötigen, sowie die Gesamtzahl der Geräte, auf denen der Patch fehlt.

Nachbesserungsstatus

Der Status (VIs insgesamt, % behoben, VIs zurückgestellt) für die VIs, die über diesen bevorzugten Patch verfügen.

Bevorzugte Patches und Lösungen

Wenn eine importierte Schwachstelle mit einem Asset in Ihrem Configuration Management Database (CMDB)übereinstimmt, wird in Vulnerability Responseein angreifbares Element (VI) erstellt. Wenn das diesem VI zugeordnete Konfigurationselement (Configuration Item, CI) auch von einem Drittanbieter-Patch importiert wird und für dieselbe Schwachstelle ein Patch fehlt, wird ein bevorzugter Patch aufgelistet und ein Rollup für Ihre Lösungen durchgeführt. Diese Informationen informieren Sie darüber, dass für ein Asset (CI) die Korrektur aus einem verfügbaren Patch verfügbar ist, die am besten zu seiner Schwachstelle passt.

Patches ohne Lösungen werden angezeigt

Wenn nach einem Import keine Daten zur Schwachstellenlösung verfügbar sind, bleibt das Feld **Schwachstellenlösung** im Patch-Update-Datensatz leer. Weitere Informationen zum Anzeigen von Informationen für diese Patch-Typen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Zeigen Sie Patches ohne Lösungen in an Vulnerability Response

Ab v16.0 von Vulnerability Responsesucht das System für Patches, für die nach einem Import keine Lösungen vorhanden sind, in den Schwachstellen-Referenzdaten nach Patch-IDs, damit Sie diese Patches in den Schwachstellen-Datensätzen anzeigen können.

Patches ohne Lösungen

Erforderliche Rolle: sn_vul.vulnerability_admin.

Die aus den Patch-Orchestration- und Schwachstellenlösungs-Anwendungen sowie den Patchscanner-Integrationen importierten Daten werden verarbeitet, verbunden und in der Anwendung Vulnerability Response in den Patch-Update-Datensätzen angezeigt.

Wenn für eine Schwachstelle eine Lösung vorhanden ist, werden die zugehörigen Informationen in Ihrer Instanz korreliert und von den Patches über Lösungen für Schwachstellen bis hin zu Schwachstellen zusammengefasst. Um diese Informationen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**.

Wenn nach einem Import keine Daten zur Schwachstellenlösung verfügbar sind, bleibt das Feld **Schwachstellenlösung** im Patch-Update-Datensatz leer. Damit Sie die zugehörigen Lösungsinformationen für diese Patches anzeigen können, ist in Ihrer Instanz standardmäßig die Systemeigenschaft „**sn_vul_patch_orch.no_solution_patch_rollup**“ aktiviert. Diese Eigenschaft sucht nach Bulletin-IDs und Artikel-IDs in den Schwachstellen-Referenzdaten aus Scanner-Importen. Wenn eine Übereinstimmung gefunden wird,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden die zugehörigen Daten in der Tabelle „Potenzielle Patches“ ausgefüllt, und diese Informationen werden in den zugehörigen Listen der Schwachstellen-Datensätze angezeigt.

Wenn Sie eine große Anzahl von Schwachstellen haben oder die Ausführung der geplanten Rollup-Aufgabe lange dauert, empfiehlt es sich, diese Systemeigenschaft zu deaktivieren, um mögliche Leistungsprobleme zu vermeiden. Beachten Sie jedoch, dass importierte Lösungsdaten weder gesucht noch für Schwachstellen ohne Lösungen zusammengefasst werden, wenn Sie diese Systemeigenschaft deaktivieren.

Um die Systemeigenschaft zu deaktivieren, gehen Sie als Benutzer mit der Rolle sn_vul.vulnerability_admin wie folgt vor:

1. Navigieren zu **sys.properties.list**.
2. Suchen Sie **sn_vul_patch_orch.no_solution_patch_rollup,** und klicken Sie darauf, um den Datensatz zu öffnen.
3. Im Feld Wert geben Sie falseein.
4. Klicken Sie auf **Aktualisieren**.

Patch-Orchestrationsdaten werden in den Dashboards Vulnerability Response angezeigt

Ab v16.1 können Sie Patch-Update-Daten in der klassischen Umgebung in den in der Anwendung Vulnerability Response enthaltenen Dashboards anzeigen.

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad aktiver Schwachstellen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen anzeigen, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Siehe Vulnerability Manager Workspace und IT Remediation Workspace erkunden, um weitere Informationen zu erhalten.

Sie können diese Daten auch in den Dashboards für CISO und Schwachstellenmanagement (PA) anzeigen, wenn Sie ein -Abonnement für Performance Analyticshaben.

Sie können Patch-Daten auch in der klassischen Umgebung anzeigen. Weitere Informationen zu den erforderlichen Rollen und zum Anzeigen von Daten in den Vulnerability Response -Dashboards in der klassischen Umgebung, die in der Anwendung Vulnerability Response enthalten sind und ein separates Abonnement erfordern, finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..

Zeigen Sie eine Lösung an

Zeigen Sie alle Lösungen, Lösungen mit höchster Ersatzlösung und Lösungen an, die angreifbaren Elementen zugeordnet sind, um Ihre Korrekturaktivitäten zu planen.

Vorbereitungen

Erforderliche Rolle: sn_vul.read, sn_vul.vulnerability_admin oder sn_vul.remediation_owner
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenanalyst oder Korrekturbesitzer können Sie verschiedene Lösungssätze anzeigen, die sich auf angreifbare Elemente beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Lösungsdatensätze sind schreibgeschützt, außer unter **Notizen** im Abschnitt **Interne Hinweise** oder von Anwendern erstellte Lösungen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Lösungen**.
2. Wählen Sie eine Lösungsliste.

   Hinweis:
   Sie können eine Lösungsliste mithilfe von Platzhaltern für den Produktnamen filtern.

3. Klicken Sie zum Überprüfen auf die einzelnen Elemente.
4. **Wahlweise:** Geben Sie auf der Registerkarte **Notizen** Notizen ein, und klicken Sie mit der rechten Maustaste **auf Speichern**, um auf der Seite zu bleiben, oder klicken Sie auf **Aktualisieren,** um zu speichern und zur Liste **der Schwachstellenlösungen** zurückzukehren.

   Hinweis:
   Wenn Sie nur über die Rolle „sn_vul.read“ verfügen, können Sie diesen Schritt nicht ausführen.

Erstellen Sie eine Schwachstellenlösung

Erstellen Sie eine Schwachstellenlösung, damit Sie Schwachstellenlösungen nachverfolgen können, die nicht durch Lösungsinhalte von Drittanbietern abgedeckt werden.

Vorbereitungen

Erforderliche Rolle: admin, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder vulnerability.write Vulnerability Solution Management ist eine Funktion, die in der Anwendung Vulnerability Response verfügbar ist. Vulnerability Solution Management erfordert ein separates Abonnement.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Lösung aus einer beliebigen Lösungsliste erstellen. Bevor Sie eine Lösung erstellen können, müssen Sie die Anwendung Vulnerability Solution Management installieren.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Lösungen**.
2. Wählen Sie eine Lösungsliste aus: **Alle**, **Höchste Ersatzlösung** oder **Mit angreifbaren Elementen**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die bearbeitbaren Felder im Formular entsprechend aus.
   Sie können alle nicht verwendeten Felder leer lassen. Weitere Informationen zu einzelnen Feldern finden Sie unter Lösungsformularfelder.
5. Klicken Sie im Header mit der rechten Maustaste **auf Speichern**.
   Der Lösungsdatensatz wird hinzugefügt und standardmäßig in den Listen **Alle** und Ersetzung durch **höchste Ersetzung** angezeigt.
6. Die zugehörigen Listen werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese Lösung den folgenden zugehörigen Listen zuordnen: **Angreifbare Elemente**,**Schwachstellen von Drittparteien**, **CVEs**, **Ersatzlösungen** und **Vorhergehende Lösungen**. Wählen Sie eine Schwachstelle oder Lösung aus, und klicken Sie auf **Absenden**.

Hinweis:

Vulnerability Solution Management ordnet angreifbare Elemente und Korrekturaufgaben automatisch Lösungen zu, wenn Schwachstellen-Datensätze manuell Lösungen zugeordnet werden.

Angreifbare Elemente, die manuell einer anderen Lösung zugewiesen wurden, werden nicht automatisch mit Lösungsänderungen auf Schwachstellenebene aktualisiert.

Wenn Sie die Beziehung zwischen einer Drittanbieterschwachstelle und einer Lösung ausschließen möchten, da sie für das zu korrigierende CI nicht relevant ist oder in Ihrer Umgebung kein Problem darstellt, lesen Sie Schließen Sie manuell Lösungen aus Datensätzen von Drittparteien oder umgekehrt aus.

Schließen Sie manuell Lösungen aus Datensätzen von Drittparteien oder umgekehrt aus

Schließen Sie die Beziehung zwischen einer Drittanbieterschwachstelle und einer Lösung aus, da sie für das zu korrigierende CI nicht relevant ist oder in Ihrer Umgebung kein Problem darstellt. Schließen Sie Lösungen manuell aus, indem Sie entweder eine Drittpartei-Schwachstelle oder einen Lösungsdatensatz verwenden.

Vorbereitungen

Erforderliche Rolle:

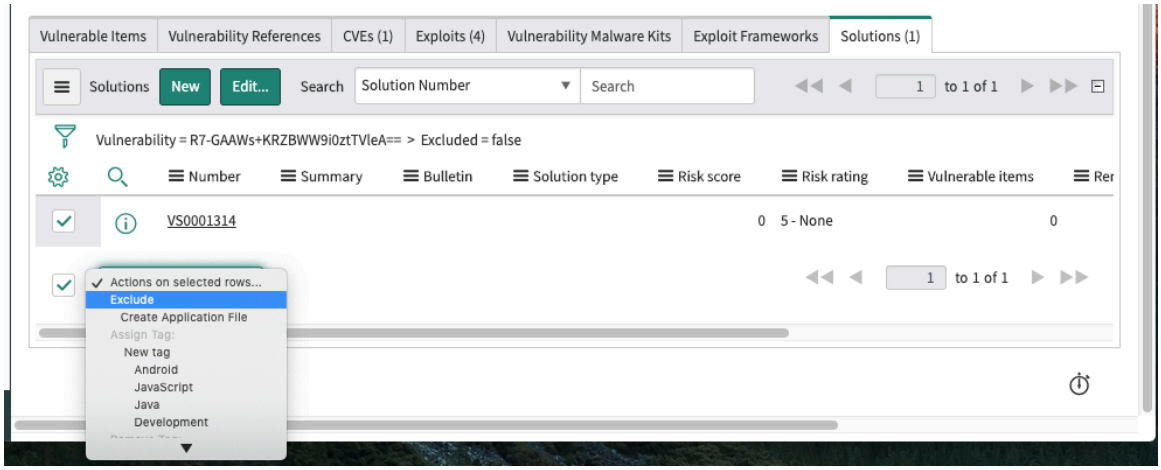
- sn_vul.write
- sn_vul.remediation_owner

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **Drittpartei** oder **Vulnerability Response** > **Alle Lösungen**
2. Öffnen Sie eine Schwachstelle oder einen Lösungsdatensatz einer Drittpartei.
   a. Für einen Drittpartei-Datensatz: Wählen Sie die zugehörige Registerkarte **Lösungen**.
   b. Für einen Lösungsdatensatz: Wählen Sie die Registerkarte Zugehörige **Schwachstellen von Drittparteien**.
3. Aktivieren Sie das Kontrollkästchen neben jeder Schwachstelle oder jedem Lösungsdatensatz, den Sie ausschließen möchten.
4. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen** die **Option Ausschließen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Drittpartei- oder Lösungsdatensatz wird nicht mehr auf der zugehörigen Registerkarte angezeigt.

Beziehungen von Drittpartei-Schwachstellen mit Lösungen werden ebenfalls ausgeschlossen, wenn Lösungen aktualisiert werden oder wenn die nächtliche Aufgabe aktiviert ist.

Schwachstellenbeziehungen von Drittparteien zu Lösungen werden während der nächtlichen geplanten Aufgabeausgeschlossen.

Wenn Sie Schwachstellen von Drittparteien ausschließen, ist die Lösung kein Faktor mehr bei der Bewertung einer bevorzugten Lösung. Ausschlussauswirkungen:

- Alle Zählungen für Lösungen seit der Drittpartei-Schwachstelle, angreifbare Elemente (VIs) und Konfigurationselemente (CIs), die an die Drittpartei-Schwachstelle angehängt sind, werden nicht mehr auf die Lösung angerechnet.
- Ermittlung der bevorzugten Lösung für die Drittanbieter-Schwachstelle und damit verbunden der bevorzugten Lösung aller angehängten AEs und Korrekturaufgaben, die die AEs enthalten.

Schwachstellen automatisch selektieren

Um eine erfolgreiche Behebung sicherzustellen, müssen neue Schwachstellen überprüft und selektiert werden. Transformieren Sie Importe von Schwachstellen in Korrekturaufgaben mit automatisierter Zuweisung von angreifbaren Elementen (VI), Risikoberechnung, Korrekturzielen und VI-Gruppierung.

Beginnen Sie mit importierten Schwachstellen, gleichen Sie die nicht in der CMDB gefundenen Assets ab, priorisieren Sie die Ergebnisse, übersetzen Sie dies in automatisch zugewiesene Korrekturaktivitäten, orchestrieren Sie den Korrekturprozess, und bestätigen Sie den Abschluss mit einem Validierungsscan.

Neue angreifbare Elemente werden normalerweise beim Import basierend auf den Regeln für Korrekturaufgaben in Korrekturaufgaben sortiert. Manchmal können angreifbare Elemente nicht gruppiert werden oder sie enthalten kein erkanntes Konfigurationselement.

Übersicht über den Schwachstellenselektierungsprozess:

- Melden Sie sich bei der Vulnerability Response-Instanz an.
- Validieren Sie, ob Ihre Regeln (CI-Suche, Zuweisung) für angreifbare Elemente wie erwartet funktionieren. Informationen zum Überarbeiten von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien. Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Aufgrund des großen Datenimportvolumens ist bei der automatisierten Zuweisung angreifbarer Elemente Vorsicht geboten.

- Überprüfen Sie, ob Ihre Korrekturziele korrekt sind. Informationen dazu, wie Korrekturzielregeln funktionieren und wie sie überarbeitet werden können, finden Sie unter Vulnerability Response Korrekturzielregeln.
- Zeigen Sie nicht gruppierte angreifbare Elemente an.
  - Angesichts der nicht gruppierten angreifbaren Elemente sollten Sie ggf. Ihre Gruppenregeln überarbeiten und einen erneuten Scan durchführen. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben.
  - Gruppieren Sie die angreifbaren Elemente manuell. Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response, um weitere Informationen zu erhalten.
  - Überarbeiten Sie die Risikopunktzahlen für die angreifbaren Elemente in Ihren Korrekturaufgaben. Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.
  - Schließen Sie ältere angreifbare Elemente, die nicht kürzlich von Ihren Drittanbieterintegrationen erkannt wurden. Weitere Informationen finden Sie unter Automatisches Schließen von angreifbaren Elementen und Erkennungen.
- Nicht abgeglichene Konfigurationselemente anzeigen und neu klassifizieren.
- Untersuchen, was zur Behebung getan werden muss.

  Dieser Schritt kann Folgendes umfassen:

  - Bestimmen Sie, womit Sie sich jetzt befassen und was Sie zurückstellen können. Diese Bestimmung basiert häufig auf der Risikopunktzahl, den betroffenen Systemen und Patches mit Change-Fenstern.

    Hinweis:
    Korrekturzielregeln gehören zu angreifbaren Elementen. Diese Regeln werden ausgeführt, wenn das angreifbare Element importiert wird. Diese Regeln wurden zuvor im Setup-Assistenten erstellt.

  - Aktualisieren Sie bei Bedarf die angreifbaren Elementeund Zeigen Sie den Nachbesserungszielstatus eines angreifbaren Elements Vulnerability Response an.
  - Erstellen Sie eine **Change-Anforderung**, und weisen Sie die Korrekturaufgabe zur Korrektur einer Zuweisungsgruppe (IT-Betrieb) zu.

    Hinweis:
    Wenn die Schwachstelle einen Security Incident darstellt und das Plugin Security Incident Response (com.snc.security_incident) aktiviert ist, können Sie stattdessen Security Incident-Datensätze aus den Korrekturaufgaben erstellen.

  - Nachdem Sie eine oder mehrere Change-Anforderungen übermittelt haben, ändern Sie den Gruppenstatus in „Wird untersucht“.

Führen Sie eine Massenbearbeitung von angreifbaren Elementen in durch Vulnerability Response

Bearbeiten Sie angreifbare Elemente massenweise , um Zeit zu sparen, indem Sie Felder auswählen und eine asynchrone Massenbearbeitung im Hintergrund ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Wichtig:
Die Massenbearbeitungsfunktion ist für angreifbare Host-Elemente in Vulnerability Manager Workspaceverfügbar. Weitere Informationen finden Sie unter Massenbearbeitung in verwenden Vulnerability Manager Workspace.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Schwachstellen** > **Angreifbare Elemente**.
2. Wählen Sie die angreifbaren Elemente aus, indem Sie eine der folgenden Aktionen ausführen:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld #unique_131_Connect_42_entry-be-record-selection verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option **Alle angreifbaren Elemente, die dem Filter entsprechen** im Feld #unique_131_Connect_42_entry-be-record-selection verwenden.
3. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
4. Füllen Sie die Felder im Modal „Massenbearbeitung“ aus.

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte angreifbare Elemente ○ Alle angreifbaren Elemente, die dem Filter entsprechen ○ Nachbesserungsaufgabe ○ Schwachstelleneintrag
Status	Change für den **Status** im angreifbaren Element. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nicht aktualisieren ○ Öffnen ○ Wird untersucht ○ Warten auf Implementierung ○ Zurückgestellt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ▪ Wenn Sie diese Option auswählen, werden die Felder Grund, Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt. ▪ Wenn Sie VITs zurückstellen, wird eine Korrekturaufgabe erstellt, und diese Aufgabe wird zur Genehmigung gesendet. ○ Geschlossen **Hinweis:** ▪ Wenn Sie diese Option auswählen, um die Datensätze als falsch positiv zu markieren, werden die Felder Grund, Kurzbeschreibung, Bisund Zusätzliche Informationen angezeigt. ▪ Wenn Sie die Datensätze als falsch positiv markieren, wird eine Korrekturaufgabe erstellt und zur Genehmigung gesendet. ○ Gelöst
Bevorzugte Lösung	Lösung zur Korrektur aller angreifbaren Elemente, die für die Massenbearbeitung ausgewählt sind. Wählen Sie den Change für das Feld **Preferred Solution (Bevorzugte Lösung)** im angreifbaren Element (VITs) aus. Die Auswahlmöglichkeiten stammen aus einer Nachschlageliste der verfügbaren bevorzugten Lösungen für die ausgewählten VITs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ◦ Der Satz der verfügbaren bevorzugten Lösungen ist eine Schnittmenge aller potenziellen Lösungen für die Schwachstellen in allen ausgewählten VITs. ◦ Beim Auswählen von **Datensatzauswahl** > **Schwachstelleneintrag** Bei einer Massenbearbeitung werden alle VITs für die Schwachstelle auf die ausgewählte bevorzugte Lösung festgelegt. **Hinweis:** Durch diesen Vorgang wird die **bevorzugte Lösung** nicht auf der Ebene des Schwachstelleneintrags festgelegt. Durch das Festlegen der **bevorzugten Lösung** auf der Ebene des Schwachstelleneintrags wird die **bevorzugte Lösung** für alle neuen VITs in Zukunft festgelegt. Durch die Massenbearbeitung wird nur der aktuelle Satz von VITs geändert. ◦ Eindeutige Schwachstellen, die über die Auswahlkriterien hinweg auf 500 beschränkt sind. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, werden Sie in einer Warnmeldung aufgefordert, VITs mit unterschiedlichen Kriterien für die Festlegung der **Lösung Preferred**auszuwählen. ◦ Die Gesamtzahl der Lösungen, die in der Suchliste angezeigt werden können, ist auf 170 beschränkt. Wenn mehr als 170 Lösungen vorhanden sind, wird eine Warnmeldung angezeigt. Der aktualisierte Wert wird in der Listenansicht der angreifbaren Elemente angezeigt.
Bevorzugter Patch	Patch, das auf die Korrektur aller für die Massenbearbeitung ausgewählten Schwachstellenelemente abzielt. **Hinweis:** ◦ Sie müssen Patch Orchestration installieren, um die Liste der bevorzugten Patches anzuzeigen. ◦ Der Satz der verfügbaren bevorzugten Patches ist eine Schnittmenge aller potenziellen Patches für alle ausgewählten VITs. ◦ Eindeutige Schwachstellen, die über die Auswahlkriterien hinweg auf 500 beschränkt sind. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, werden Sie in einer Warnmeldung aufgefordert, VITs mit unterschiedlichen Kriterien für die Festlegung des **bevorzugten Patch**auszuwählen. ◦ Die Gesamtzahl der Patches, die in der Suchliste angezeigt werden können, ist auf 170 beschränkt. Wenn mehr als 170 Patches vorhanden sind, wird eine Warnmeldung angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Grund	Grund für das Zurückstellen von Datensätzen: ○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige Grund für das Schließen von Datensätzen: ○ Falsch positiv **Hinweis:** ▪ Wenn Sie diese Option auswählen, werden die Felder Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt. ▪ Eine Korrekturaufgabe wird erstellt, wenn Sie die Datensätze als Falsch positiv markieren und diese Aufgabe zur Genehmigung gesendet wird. ○ Storniert ○ Behoben **Hinweis:** Dieses Feld wird angezeigt, wenn Sie als Status Zurückgestellt oder Geschlossen auswählen.
Kurzbeschreibung	Kurze Notiz, in der der Grund für Zurückstellungen und als falsch positiv geschlossene Anforderungen beschrieben wird. Diese Informationen werden im Feld Beschreibung der Korrekturaufgabe angezeigt, die für Zurückstellungs- und „Falsch positiv geschlossen“-Anforderungen erstellt wird. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie als Status Zurückgestellt und Geschlossen – Falsch positiv auswählen.
Bis	Datum, bis zu dem der Datensatz zurückgestellt bleibt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie als Status Zurückgestellt auswählen.
Zusätzliche Information	Alle weiteren erforderlichen Informationen. Diese Informationen werden im Feld Zusätzliche Informationen auf der Registerkarte Übersicht angezeigt. Wenn Ihre Zurückstellungsanforderung genehmigt wird, werden diese zusätzlichen Informationen als Zurückstellungsnotizen sowohl in der VIT als auch in der Korrekturaufgabe angezeigt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie als Status Zurückgestellt und Geschlossen – Falsch positiv auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuweisung aufheben	Die Zuweisung aller ausgewählten Elemente wird für die Zuweisungsgruppe und den Korrekturbesitzer aufgehoben. Weitere Informationen dazu, wie ein Korrekturbesitzer die Zuweisungen von angreifbaren Elementen entfernen kann, finden Sie unter Zuweisungen von angreifbaren Elementen für Sie oder Ihre Gruppen entfernen. **Hinweis:** ○ Dieses Feld wird angezeigt, wenn Sie als Status Nicht aktualisieren auswählen. ○ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt, und diese Aufgabe wird zur Genehmigung gesendet.
Zuweisungsgruppe	Zuweisungsgruppe für die VIT. Wählen Sie manuell aus, oder verwenden Sie Zuweisungsempfehlungen, wenn diese Option aktiviert ist. **Hinweis:** Dieses Feld wird deaktiviert, wenn Sie das Kontrollkästchen **Zuweisung** aufheben aktivieren.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

5. Wählen Sie **OK**.
   Ein asynchroner Massenbearbeitungsauftrag aktualisiert die ausgewählten Datensätze. Die Auftragsnummer mit einem Link wird auf der Seite „Angreifbare Elemente“ angezeigt, auf der Sie den Status anzeigen können. Eine Korrekturaufgabe wird mit den ausgewählten angreifbaren Elementen erstellt, wenn Sie angreifbare Elemente massenweise zurückstellen, die Zuweisung aufheben oder sie schließen (falsch positiv). Und diese Korrekturaufgabe wird zur Genehmigung gesendet.

Nicht gruppierte Vulnerability Response angreifbare Elemente

Angreifbare Elemente werden beim Import automatisch einer Korrekturaufgabe zugewiesen. Wenn jedoch ein angreifbares Element (VI) manuell erstellt wird, kann es manchmal jedoch zu einem verwaisten Element werden. Das Modul **Nicht gruppierte** angreifbare Elemente listet diese angreifbaren Elemente ohne Gruppe auf.

Hinweis:
Automatisierte Integrationsprozesse erstellen keine verwaisten Elemente, daher wird erwartet, dass dieser Anwendungsfall klein ist.

Das Aufheben der Gruppierung tritt auf, wenn ein angreifbares Element ohne Schwachstelle erstellt wurde oder keine Regel für Korrekturaufgaben vorhanden ist, die das VI einer Gruppe zuweist.

Überprüfen Sie in diesem Fall die Liste der nicht gruppierten angreifbaren Elemente, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Nicht gruppiert**.

Nach der Überprüfung lauten Ihre Auswahlmöglichkeiten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben, um alle Elemente zu erfassen, die in dieser Liste angezeigt werden.
- Sie können Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response und manuell Elemente aus dieser Liste zur Gruppe hinzufügen oder eine Bedingung definieren, die diesen Elementen entspricht.
- Sie können eine vorhandene Korrekturaufgabe öffnen und der Gruppe alle relevanten angreifbaren Elemente hinzufügen, solange sie sich im Status „Offen“ oder „Wird untersucht“ befindet.

Hinweis:
Manuell hinzugefügte angreifbare Elemente werden durch Regeln für Korrekturaufgaben oder Gruppenbedingungen nicht automatisch aus Korrekturaufgaben entfernt.

Weitere Informationen zum Verhalten von Korrekturaufgaben und Aufgabenregeln finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

Zeigen Sie nicht gruppierte Vulnerability Response angreifbare Elemente an

Angreifbare Elemente, die keiner Gruppe zugewiesen sind, werden in einer sichtbaren Liste platziert.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Schwachstellen** > **Nicht gruppierte angreifbare Elemente**.
2. Überprüfen Sie die angreifbaren Elemente in der Liste.
3. Klicken Sie auf die einzelnen angreifbaren Elemente, um sie anzuzeigen und zu bestimmen, wie sie in eine Gruppe aufgenommen werden sollen.

Fügen Sie manuell ein angreifbares Element zu einer Korrekturaufgabe hinzu

Wenn ein angreifbares Element nicht gruppiert wird, können Sie es einer Korrekturaufgabe hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Notieren Sie die Nummer der Schwachstelle.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
3. Wählen Sie eine Korrekturaufgabe (VUL) für das angreifbare Element aus.
4. Wählen Sie **Bearbeiten** unten rechts.
5. Geben Sie die Nummer **des angreifbaren Elements** in das Suchfeld für Sammlung ein.
6. Wählen Sie das angreifbare Element aus der Sammlung aus, und fügen Sie es der Liste hinzu.
7. Klicken Sie auf **Speichern**.

Entfernen Sie Zuweisungen von angreifbaren Elementen

Datensätze für angreifbare Elemente in den Anwendungen Vulnerability Response und Application Vulnerability Response neu zuweisen.

Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie feststellen, dass sich angreifbare Elemente (VITs) nicht in Ihrem Korrekturbereich befinden, oder wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen nicht korrekt zugewiesen wurden, können Sie sich oder Ihre Gruppen aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** entfernen für Datensätze zu angreifbaren Elementen und Korrekturaufgaben.

Die Schaltfläche **„Zuweisung aufheben"** wird für die folgenden Datensätze in jedem anderen Status als „Geschlossen" oder „Gelöst" angezeigt:

- Korrekturaufgaben (VULs) sowohl in der klassischen Umgebung als auch in den Vulnerability Response -Arbeitsbereichen. Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, werden die Felder **Zugewiesen an** und**Zuweisungsgruppe** für alle zugehörigen VITs ebenfalls gelöscht.
- Angreifbare Elemente (VITs) in der klassischen -Umgebung und in den -Arbeitsbereichen Vulnerability Response.
- Angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs)
- Angreifbare Container-Elemente (CVITs)

Wichtig:
Sie können die Zuweisung angreifbarer Host-Elemente in Vulnerability Manager Workspacemassenweise aufheben. Weitere Informationen finden Sie unter Massenbearbeitung in verwenden Vulnerability Manager Workspace.

Prozedur

1. Navigieren Sie entweder in der klassischen Umgebung oder im Arbeitsbereich des IT-Korrekturverantwortlichen zu einem Ihnen zugewiesenen Datensatz für angreifbare Elemente (VIT), der sich in einem anderen Status als „Geschlossen" oder „Gelöst" befindet.
2. Um die Felder **Zugewiesen an** und **Zuweisungsgruppe** zu löschen, wählen Sie oben im Datensatz **Zuweisung aufheben**aus.
3. **Wahlweise:** Alternativ können Sie zu einem AVIT navigieren, das Ihnen oder Ihren Gruppen zugewiesen ist, und **auf Zuweisung aufheben** klicken, um die Zuweisungsfelder zu löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie im Dialogfeld „Zuweisung aufheben“ Arbeitsnotizen an, und wählen Sie **Absenden aus**.
5. **Wahlweise:** Wenn Sie die Zuweisungsfelder für mehrere VITs in einer Liste löschen möchten, wählen Sie die gewünschten VITs aus, und wählen Sie dann **Massenbearbeitung**aus.

   a. Wählen Sie im Dialogfeld „Massenbearbeitung von angreifbaren Elementen“ im Feld **Datensatzauswahl** die **Option Nur ausgewählte angreifbare Elemente** aus, aktivieren Sie das Kontrollkästchen **Zuweisung aufheben**, und wählen Sie **OK**aus.
   Weitere Informationen zu Massenbearbeitungen finden Sie unter Massenbearbeitung von angreifbaren Elementen in Vulnerability Response.

   b. Wählen Sie die ID der Korrekturaufgabe aus, die in der Benachrichtigung angezeigt wird.

6. Zeigen Sie die folgenden Informationen an:
   - Die von Ihnen bereitgestellten Arbeitsnotizen werden im Abschnitt „Notizen“ angezeigt.
   - Auf der Registerkarte **Change-Genehmigung im Status** wird der Datensatz für die Status-Change-Genehmigung mit dem Status Wird überprüft angezeigt, wodurch der Genehmigungs-Workflow nachverfolgt werden kann.
   - Auf der Registerkarte **Angeforderte Genehmigungen** wird Ihr Antrag auf Entfernung von Ihnen oder Ihrer Zuweisungsgruppe im Status Angefordert angezeigt.

Ergebnisse

Die Anforderung wird mithilfe eines standardmäßigen, einstufigen Genehmigungsworkflows genehmigt. Weitere Informationen finden Sie unter Anforderungen in Arbeitsbereichen des Schwachstellenmanagers genehmigen.

- Wenn Ihre Anforderung genehmigt wird, werden der Statusänderungsgenehmigungsdatensatz und der Datensatz für die angeforderte Genehmigung in den Status Genehmigt geändert. Sie und Ihre Gruppen werden aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** entfernt. Nicht zugewiesen wird im Feld **Zuweisungstyp** angezeigt, und die Korrekturaufgabe und VITs werden in der Liste des nicht zugewiesenen Moduls für Konfigurations-Compliance angezeigt.

  Benachrichtigungen, dass die Zuweisung von Datensätzen aufgehoben wird, werden automatisch an Schwachstellenmanager oder Analysten in der Benachrichtigungsgruppe „Zuweisung aufheben“ gesendet. Informationen zur Konfiguration der Genehmigungskennzeichnung, von Benachrichtigungen und der Standardzuweisungsgruppe finden Sie unter Zuweisungen von angreifbaren Elementen und Korrekturaufgaben entfernen.

- Wenn Ihre Anforderung abgelehnt wird, wird der Status des Change-Genehmigungsdatensatzes und des angeforderten Genehmigungsdatensatzes in den Status Abgelehnt geändert.

Hinweis:
Als Schwachstellenadministrator können Sie die Systemeigenschaft `sn_vul.unassign_vr.approval_required` auf **„false“** festlegen, um den Genehmigungsprozess zu deaktivieren.

Nächste Maßnahme

Navigieren Sie zu den Nicht zugewiesenen Modulen für die Anwendungen Vulnerability Response und Application Vulnerability Response Container Vulnerability Response, überwachen Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

alle nicht zugewiesenen Datensätze auf Elemente, die in Ihren Bereich fallen könnten, und weisen Sie sie sich selbst neu zu.

Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in, oder lehnen Sie sie ab Vulnerability Response

Genehmigen Sie Anforderungen zum Entfernen angreifbarer Elemente aus einer Zuweisungsgruppe oder einem einzelnen Benutzer in der Anwendung Vulnerability Response.

Vorbereitungen

Erforderliche Rolle: Zum Aufheben der Zuweisung von Genehmigungen ist ein Genehmiger in der Gruppe „Genehmiger – Ebene 1“ erforderlich.

- sn_vul.unassign_approver für AVITs und VITs
- sn_vul_container.unassign_approver für CVITs

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt, und es wird eine Genehmigungsgruppe zum Aufheben der Zuweisung erstellt. Benutzer der Gruppe „Genehmigerzuweisung aufheben – Ebene 1“ können die Anforderung genehmigen. Diese Gruppe enthält standardmäßig die Genehmiger-Rolle zum Aufheben der Zuweisung, sn_vul.unassign_approver. Sie können eine neue Gruppe erstellen oder ändern und die Genehmigungskonfiguration aktualisieren. Um eine Genehmigungsregel zu konfigurieren, wählen Sie im Modul Genehmigungsregeln eine der folgenden Genehmigungsregeln aus, und navigieren Sie zur Genehmigungskonfiguration auf der Registerkarte **Genehmigungskonfigurationen** :

- *`Vulnerable item field change request`* für ein angreifbares Element.
- *`Vulnerability field change request`* für eine Korrekturaufgabe.
- *`Application vulnerability field change request`* für ein angreifbares Anwendungselement (Application Vulnerable Item, AVIT)
- *`Approval for container management`* für ein angreifbares Containerelement (CVIT).

Weitere Informationen zu Genehmigungsregeln und -konfigurationen finden Sie unter Konfigurationen des Genehmigungsworkflows für Anforderung zum Aufheben der Zuweisung.

Wichtig:
Sie können Anforderungen in Vulnerability Manager Workspacegenehmigen oder ablehnen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Genehmigungen** für VITs und AVITs. Alternativ navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen** für CVITs.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie ab, indem Sie die entsprechenden Kommentare hinzufügen.

Automatisches Schließen von angreifbaren Elementen und Erkennungen

Sie können veraltete Erkennungen und angreifbare Elemente (VIs), die stillgelegten CIs zugeordnet sind, mithilfe des Moduls für Regeln zum automatischen Schließen automatisch schließen.

In den folgenden Szenarien können Sie veraltete Erkennungen und VIs automatisch schließen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Veraltete Erkennungen in automatisch schließen Vulnerability Response
- Schließt angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch

Informationen zum Arbeiten mit deaktivierten Configuration Items finden Sie unter Arbeiten mit deaktivierten Configuration Items und Erstellen Sie Regeln für das automatische Schließen.

Arbeiten mit deaktivierten Configuration Items

Außer Betrieb genommene Configuration Items (CIs) werden in den Status „Stillgelegt", „Archiviert" oder „Gelöscht" in Configuration Management Database (CMDB)verschoben. Vulnerability Response enthält angreifbare Elemente (VIs), die aus CIs bestehen. Wenn der Status eines CI auf „Deaktiviert" aktualisiert wird, werden die zugehörigen VIs mit dem Substatus „CI außer Betrieb genommen" geschlossen.

Hinweis:
Ab v25.0.3 von Vulnerability Responsewird die neue Regel für das automatische Schließen des Typs „CI außer Betrieb genommen" eingeführt, um die angreifbaren Elemente und Erkennungen im Zusammenhang mit außer Betrieb genommenen CIs zu schließen.

Wenn die CMDB den Status der Lebenszyklusphase eines CI in „Deaktiviert" ändert, können Sie die zugehörigen VIs automatisch schließen. Weitere Informationen zum automatischen Schließen der zugehörigen VIs finden Sie unter Schließt angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch.

Das stillgelegte CI wird schließlich archiviert oder dauerhaft aus CMDBgelöscht.

Auswirkung der Außerkraftsetzung der CIs:

- **Auswirkung auf erkannte Elemente:** Wenn das CI außer Betrieb genommen wird, wird das zugehörige erkannte Element (DI) als „CI außer Betrieb genommen" markiert.
- **Auswirkung auf angreifbare Elemente:** Wenn der Status eines DI auf „CI stillgelegt" aktualisiert wird, wird das zugehörige VI geschlossen und der Abschnitt „Hinweise" wird automatisch aktualisiert.

Hinweis:
Der Status eines DI wird automatisch auf „CI stillgelegt" aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Umgekehrt wird der Status eines VI nur dann auf „Geschlossen" aktualisiert, wenn die Option **VIs, die mit stillgelegten CIs verknüpft sind, automatisch schließen** aktiviert ist. Weitere Informationen zum automatischen Schließen der zugehörigen VIs finden Sie unter Schließt angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch.

Die regelmäßige Aufgabe `Close detections/VIs for decommissioned CIs` wird täglich für die aktualisierten DIs ausgeführt. Wenn die Konfigurationsoption für das automatische Schließen für stillgelegte CIs aktiviert ist, wird das DI identifiziert, das ein stillgelegtes CI enthält, und das zugehörige VI wird mit dem Substatus „CI außer Betrieb genommen" geschlossen. Wenn alle VIs in einer Korrekturaufgabe geschlossen sind und ihr Substatus „CI außer Betrieb genommen" ist, wird die Korrekturaufgabe ebenfalls mit dem Substatus „Abgebrochen" geschlossen. Um die außer Betrieb genommenen VIs anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Angreifbare Elemente** > **Außer Betrieb genommen**.

Hinweis:
Wenn ein CI aus dem Status „Stillgelegt" in den ursprünglichen Status zurückkehrt, wird auch der Eintrag „Erkannte Elemente" aktualisiert. VIs werden automatisch geöffnet, wenn Daten erneut vom Scanner erfasst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schließt angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch

Wenn Configuration Management Database (CMDB) den Status der Lebenszyklusphase eines Configuration Item (CI) in „Deaktiviert“ ändert, können Sie die zugehörigen angreifbaren Elemente (VIs) und Erkennungen automatisch schließen.

Vorbereitungen
Erforderliche Rolle: sn_vul.admin

Warum und wann dieser Vorgang ausgeführt wird
Ab v22.0 von Vulnerability Responsemüssen Sie zum automatischen Schließen der zugehörigen VIs und Erkennungen die Systemeigenschaft *sn_vul_cmn.auto_close_vis_linked_retired_cis* zum automatischen Schließen von VIs aktivieren, die stillgelegten CIs zugeordnet sind. Um die Option zu aktivieren, setzen Sie das Feld „Wert“ auf „1“. Um die Option zu deaktivieren, setzen Sie umgekehrt das Feld „Wert“ auf „0“.

Wenn während eines Upgrades die Systemeigenschaft *sn_vul_cmn.auto_close_vis_linked_retired_cis* in v21.0 von Vulnerability Responseausgewählt ist, bleibt der Wert „1“. Wenn diese Option aktiviert ist, werden neue oder vorhandene AEs und Erkennungen, die für dasselbe CI gemeldet werden, automatisch erstellt oder mit dem Status „Geschlossen“ aktualisiert. Dies basiert auf der Asset-ID in der Scanner-Payload und dem Status des Eintrags „Erkannte Elemente“. Weitere Informationen zu den Auswirkungen stillgelegter CIs finden Sie unter Arbeiten mit deaktivierten Configuration Items

.

Hinweis:

- Der Status eines DI wird bei jeder Aktualisierung des Lebenszyklusstatus eines CI auf „CI außer Betrieb genommen“ aktualisiert. Umgekehrt wird der Status eines VI nur dann auf „Geschlossen“ aktualisiert, wenn die Option **VIs, die mit stillgelegten CIs verknüpft sind, automatisch schließen** aktiviert ist.
- Die im folgenden Verfahren enthaltenen Informationen gelten nur für Versionen vor v22.0 von Vulnerability Response. Ab v22.0 von Vulnerability Responsekönnen Sie zusätzliche Suchoptionen konfigurieren. Weitere Informationen finden Sie unter Erstellen Sie Regeln für das automatische Schließen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Konfiguration für automatisches Schließen** > **Konfigurationselement-Lebenszyklus**.
2. Um angreifbare Elemente, die den stillgelegten CIs zugeordnet sind, automatisch zu schließen, aktivieren Sie das Kontrollkästchen **VIs, die mit stillgelegten CIs verknüpft sind, automatisch schließen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Aktualisieren**.

Hinweis:
Wenn ein CI bereits stillgelegt ist, bevor die Option **VIs automatisch schließen, die mit stillgelegten CIs verknüpft sind** aktiviert wird, werden VIs nur für neue Erkennungen von Scannern erstellt. Der Status dieser VIs ist „Geschlossen“, und der Substatus ist „CI außer Betrieb genommen“.

Sie können VIs mit dem Status „CI außer Betrieb genommen“ nicht manuell mit den Optionen **Erneut** öffnen oder **Massenbearbeitung erneut** öffnen.

Geschlossene VIs mit dem Substatus „Repariert“ oder „Veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIs mit der neuen Schwachstelle abgeglichen werden können. Weitere Informationen finden Sie unter Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente.

Veraltete Erkennungen in werden geschlossen Vulnerability Response

Mit dem Modul Veraltete Erkennungen automatisch schließen können Sie ältere, veraltete angreifbare Erkennungen, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden, automatisch bereinigen. Wenn Sie diese Erkennungen in den Status „Geschlossen“ verschieben, reduzieren Sie die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben in Ihrer Instanz Now Platform und helfen Ihnen, Assets in Ihrer CMDB abzugleichen.

Übersicht und Schlüsselbegriffe

Um ein genaueres Rollup von Erkennungsdaten für Ihre angreifbaren Elemente durchzuführen, hilft Ihnen das Modul Veraltete Erkennungen automatisch schließen dabei, ältere, veraltete Erkennungen von angreifbaren Elementen zu bereinigen, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden. Weitere Informationen zu dieser Funktion finden Sie im Anwendungsfall unten und im Artikel Veraltete Erkennungen automatisch schließen [KB 0958638] .

In früheren Versionen von Vulnerability Responsehat das Modul Angreifbare Elemente automatisch schließen angreifbare Elemente, die nicht kürzlich von Ihren Drittanbieter-Scanner-Integrationen gefunden oder aktualisiert wurden, automatisch in Geschlossen – Veraltet überführt.

Bevor Sie die Funktion Veraltete Erkennungen automatisch schließen aktivieren, lesen Sie die folgenden Begriffe, das Rollup von Status für angreifbare Elemente und Korrekturaufgaben und die Voraussetzungen für Ihre Drittanbieterintegrationen, die Erkennungsdaten importieren.

Informationen zum Aktivieren dieser Funktion finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

Wichtige Begriffe

Veraltete Erkennungen

Bezieht sich auf Erkennungen, die angreifbaren Elementen in Ihrer Instanz Now Platform® zugeordnet sind, veraltet sind und längere Zeit nicht von Integrationsscans von Drittanbietern gefunden, aktualisiert oder erkannt wurden.

Zuletzt gefundene Erkennungen

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner eines Drittanbieters bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuellste oder späteste Datum und die neueste Uhrzeit, zu der Erkennungen vom Scanner erneut gefunden wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuletzt gescannte Assets

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner eines Drittanbieters bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuelle Datum und die aktuelle Uhrzeit, zu der ein Asset zuletzt von einem Drittanbieter-Scanner gescannt wurde.

Anwendungsfall

Manchmal werden Assets (Konfigurationselemente) in Ihrer Umgebung außer Betrieb genommen oder von Drittanbieterscannern gelöscht, und die zugehörigen Erkennungen werden nicht durch Erkennungen angreifbarer Elemente aktualisiert. Dies hat zur Folge, dass die Erkennungen und die zugehörigen angreifbaren Elemente in der Anwendung Vulnerability Response nicht aktualisiert werden und inaktiv (veraltet) werden.

Um diese veralteten Erkennungen mit unveränderten Daten zu angreifbaren Elementen zu schließen und anschließend die Anzahl der aktiven AEs und Korrekturaufgaben zu reduzieren, aktivieren Sie Veraltete Erkennungen automatisch schließen. Diese Funktion schließt automatisch Erkennungen von angreifbaren Elementen, die nicht kürzlich von Ihren Scanner-Integrationen von Drittanbietern gefunden oder aktualisiert wurden, basierend auf Suchkriterien und einem von Ihnen festgelegten Alter in Tagen.

Angenommen, ein bestimmtes Konfigurationselement (Configuration Item, CI) weist mehrere Asset-IDs auf, und eine dieser IDs wurde in den letzten 90 Tagen nicht für eine Erkennung von einem Drittanbieterscanner importiert. Diese Funktion schließt automatisch diese Erkennung, die keine neuen Schwachstellendaten aufweist, sodass das zugehörige VI geschlossen werden kann.

Da einem VI mehr als eine Erkennung zugeordnet sein kann, überträgt diese Funktion nur die Erkennungen, die durch die von Ihnen festgelegten Parameter als veraltet eingestuft werden. Wenn einem VI beispielsweise vier Erkennungen zugeordnet sind und zwei Erkennungen veraltet sind (d. h. in den letzten 90 Tagen keine neuen Schwachstellendaten importiert wurden), schließt diese Funktion nur die veralteten Erkennungen. Bevor das AE geschlossen werden kann, müssen Sie zuerst die beiden anderen offenen Erkennungen korrigieren.

Rollup von Erkennungsstatus zu VIs

Um die automatisch geschlossenen Erkennungen von Erkennungen zu unterscheiden, die von Drittanbieterscannern geschlossen wurden, wurde ein neuer Wert für das Feld Status, Veraltet, hinzugefügt. Die möglichen Werte für dieses Feld sind: Offen, Geschlossen und Veraltet. Veraltet gibt an, dass eine Erkennung von der Erkennungsfunktion zum automatischen Schließen geschlossen wurde.

Statusrangfolge: Offen > Geschlossen > Veraltet.

1. Wenn Erkennungen Offen sind, bleibt der zugehörige VI-Status Offen.
2. Wenn keine Erkennungen Offen, einige Erkennungen Geschlossen und Veraltet sind, wechselt der zugehörige VI-Status zu Geschlossen – Behoben.
3. Wenn alle Erkennungen Veraltet sind, wechselt der zugehörige VI-Status zu Geschlossen – Veraltet.

   Ab Vulnerability Response 20.0 gilt: Wenn die Erkennung veraltet ist und sich das zugehörige VI im Status „Geschlossen“ befindet, wechselt der Status des VI nicht in „Geschlossen – Veraltet“. Dies dient dazu, zu verhindern, dass das VI erneut geöffnet wird, wenn eine neue Erkennung erkannt wird, damit Sie nicht den gesamten Anforderungs- und Genehmigungsprozess für falsch positive Meldungen durchlaufen müssen. Um dieses Verhalten umzukehren, deaktivieren Sie im Formular „Konfiguration für automatisches

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schließen“ das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren**. Weitere Informationen finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

Rollup von VI-Status zu Korrekturaufgaben (VUL)

Statusvorrang: Offen > Geschlossen – Repariert > Geschlossen – Veraltet.

1. Wenn VIs in einer VUL (Korrekturaufgabe) Offen sind, wird der VUL-Status nicht geändert.
2. Wenn mindestens ein VI Geschlossen – Repariert ist und die übrigen Geschlossen – Veraltet sind, geht der VUL-Status in Geschlossen – Repariert über.
3. Wenn alle VIs in einer VUL Geschlossen – Veraltet sind, wechselt der Status der VUL zu Geschlossen – Abgebrochen.

Erkennungen für das automatische Schließen und Anforderungen für die Integration von Drittparteien

Microsoft TVM-Benutzer und veraltete Erkennungen automatisch schließen

Prüflistenelement	Beschreibung
Die Microsoft TVM-Schwachstellen-Integration	Wenn Sie bei Microsoft TVM Vulnerability Integration **Zuletzt gefundene Erkennungen** als Grundlage für Ihre Suche auswählen, erfordert diese Funktion eine erfolgreiche Ausführung von Microsoft TVM Machine Vulnerabilities Integration (Vollständiger Import) innerhalb der letzten sieben Tage. Diese Integration wird wöchentlich ausgeführt. Wenn das automatische Schließen veralteter Erkennungen aktiviert und für **die zuletzt gefundenen Erkennungen**konfiguriert ist und die Microsoft TVM-Integration für maschinelle Schwachstellen deaktiviert ist oder ein Datenimport innerhalb der letzten sieben Tage nicht erfolgreich abgeschlossen wurde, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, außer in Ausnahmefällen veraltete Erkennungen werden möglicherweise nicht wie erwartet geschlossen. Wenn Sie **„Zuletzt gescannte Assets“** als Grundlage für Ihre Suche auswählen, ist die Ausführung der Microsoft TVM-Integration für maschinelle Schwachstellen nicht erforderlich. So aktivieren Sie diese Integration: 1. Navigieren zu **Microsoft TVM-Schwachstellenintegration** > **Administration** > **Integration**. 2. Suchen und aktivieren Sie **Microsoft TVM Machine Vulnerabilities Integration (Vollständiger Import)**.
(Optional) Stellen Sie mehrere Instanzen der Microsoft TVM-	Sie können optional mehrere Instanzen der Integrationen in Ihrer Umgebung bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüflistenelement	Beschreibung
Integrationen in Ihrer Umgebung bereit.	Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und wird in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden auf Instanzen, für die Integrationsausführungen erfolgreich abgeschlossen wurden, automatisch in den Status Veraltet überführt. Wenn Veraltete Erkennungen automatisch schließen aktiviert ist und Sie die Integrationen deaktivieren, die wöchentlich in einer Instanz ausgeführt werden, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt. Einige Erkennungen werden jedoch möglicherweise nicht wie erwartet automatisch in den Status Veraltet geändert.

Qualys Benutzer verwalten und veraltete angreifbare Elemente automatisch schließen

- Alle aktivierten Qualys Drittparteiintegrationen, die Erkennungsdaten abrufen, können mit diesem Modul ausgeführt werden. Es sind keine bestimmten Qualys -Anwendungen erforderlich.
- Sie können optional mehrere Instanzen der Qualys -Integrationen in Ihrer Umgebung bereitstellen.
- Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und wird in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden auf allen Instanzen automatisch in den Status Veraltet überführt.

Rapid7 Benutzer und Veraltete Erkennungen automatisch schließen

Prüflistenelement	Beschreibung
Die Rapid7 Schwachstellen-Integration	Wenn Sie **Zuletzt gefundene Erkennungen** als Grundlage für Ihre Suche auswählen, erfordert diese Funktion eine erfolgreiche Ausführung einer der Rapid7 Comprehensive Vulnerable Item Integrations (Comprehensive Vulnerable Item Integrations) innerhalb der letzten sieben Tage. Diese umfassenden Integrationen werden wöchentlich ausgeführt: • Für das Data Warehouse Rapid7 Nexpose ist eine erfolgreiche Ausführung von Rapid7 Comprehensive Vulnerable Item Integration erforderlich. • Für Rapid7 InsightVMist eine erfolgreiche Ausführung von Rapid7 Comprehensive Vulnerable Item Integration – API erforderlich. Wenn Veraltete Erkennungen automatisch schließen aktiviert und für **zuletzt gefundene Erkennungen**konfiguriert ist und die Rapid7 Comprehensive Vulnerable Item Integrations deaktiviert sind oder ein Datenimport innerhalb der letzten sieben Tage nicht erfolgreich abgeschlossen wurde, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, aber Einige

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüflistenelement	Beschreibung
	veraltete Erkennungen werden möglicherweise nicht wie erwartet geschlossen. Wenn Sie **Zuletzt gescannte Assets** als Grundlage für Ihre Suche auswählen, ist keine umfassende Integrationsausführung Rapid7 erforderlich. So aktivieren Sie diese Integrationen: 1. Navigieren zu **Rapid7 Vulnerability-Integration** > **Administration** > **Integration**. 2. Suchen und aktivieren Sie die Rapid7 Comprehensive Vulnerable Item Integration, die Sie benötigen. **Hinweis:** Zusätzlich zu den Integrationen, die wöchentlich ausgeführt werden, verfügen Rapid7 Nexpose und Rapid7 InsightVM jeweils über täglich ausgeführte VI-Integrationen, die Rapid7 Vulnerable Item Integration und die Rapid7 Vulnerable Item Integration – API. Wenn sowohl die tägliche als auch die wöchentliche Rapid7 Integration aktiviert sind, wird jeweils nur eine Integration ausgeführt. Wenn eine dieser Integrationsaufgaben ausgeführt wird, wird die Aufgabe für die andere Integration bis zur nächsten geplanten Aufgabe übersprungen.
(Optional) Stellen Sie mehrere Instanzen der -Integrationen Rapid7 in Ihrer Umgebung bereit.	Sie können optional mehrere Instanzen der umfassenden Integrationen in Ihrer Umgebung bereitstellen. Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und wird in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden auf Instanzen, für die Integrationsausführungen erfolgreich abgeschlossen wurden, automatisch in den Status Veraltet überführt. Wenn Veraltete Erkennungen automatisch schließen aktiviert ist und Sie die Integrationen deaktivieren, die wöchentlich in einer Instanz ausgeführt werden, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt. Einige Erkennungen werden jedoch möglicherweise nicht wie erwartet automatisch in den Status Veraltet geändert.

Benutzer von Tenable Vulnerability Integration und Veraltete angreifbare Elemente automatisch schließen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle aktivierten Integrationen aus der Tenable-Schwachstellen-Integration, die Erkennungsdaten abrufen, können mit diesem Modul ausgeführt werden. Es sind keine spezifischen Tenable-Schwachstellen-Integrationen erforderlich.
- Sie können optional mehrere Instanzen der Tenable Vulnerability-Integration in Ihrer Umgebung bereitstellen.
- Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und wird in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden auf allen Instanzen automatisch in **den Status Veraltet** überführt.

Nachdem Sie verifiziert haben, dass Ihre Integrationen ordnungsgemäß konfiguriert sind, rufen Sie Veraltete Erkennungen in automatisch schließen Vulnerability Response auf, um die Funktion zu aktivieren.

Upgrade-Informationen von „Veraltete angreifbare Elemente automatisch schließen“ auf „Veraltete Erkennungen automatisch schließen“.

Für das Modul Veraltete Erkennungen automatisch schließen, wenn Sie zuvor Veraltete angreifbare Elemente automatisch schließen verwendet haben:

- Der Wert für die Anzahl der Tage, die Sie für die Option **Zuletzt gescannte Assets** unter Veraltete angreifbare Elemente automatisch schließen eingegeben haben, wird für **zuletzt in Veraltete Erkennungen automatisch schließende Assets** gescannt automatisch beibehalten.
- Der Wert für die Anzahl der Tage, die Sie für die Option **Zuletzt gefundene angreifbare Elemente** unter Veraltete angreifbare Elemente automatisch schließen, wird automatisch für **zuletzt** unter Veraltete Erkennungen automatisch schließen verwendete Erkennungen beibehalten.
- Vorhandene offene Erkennungen mit „Geschlossen – Veraltet“ für angreifbare Elemente werden gemäß den Konfigurationseinstellungen für automatisches Schließen in „Veraltet“ geändert, wenn die geplante Aufgabe `Auto-Close Stale Detections` nach dem Upgrade ausgeführt wird.

Rollup-Informationen

- Wenn ein angreifbares Element vor dem Upgrade Geschlossen – Veraltet war und alle Erkennungen nach dem Upgrade als Veraltet markiert werden, bleibt der VI-Status Geschlossen – Veraltet.
- Wenn ein angreifbares Element vor dem Upgrade den Status „Geschlossen – Veraltet“ hatte und nur einige seiner Erkennungen nach dem Upgrade als „Veraltet“ markiert werden und die restlichen vom Scanner geschlossen wurden, wird das angreifbare Element gemäß der Rollup-Logik in „Geschlossen – Behoben“ geändert.

Veraltete Erkennungen in automatisch schließen Vulnerability Response

Aktivieren Sie Veraltete Erkennungen automatisch schließen, um veraltete angreifbare Erkennungen, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden, automatisch zu schließen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vuln.admin (veraltet) oder ein Schwachstellenmanager mit der granularen Rolle sn_vul.manage_auto_close_stale_vi.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu dieser Funktion, zu wichtigen Begriffen und zu allen Setups, die für Ihre Drittanbieterintegrationen zum Importieren von Erkennungsdaten erforderlich sind, finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response.

Hinweis:
Die im folgenden Verfahren enthaltenen Informationen gelten nur für Versionen vor v22.0 von Vulnerability Response. Ab v22.0 von Vulnerability Responsekönnen Sie zusätzliche Suchoptionen konfigurieren. Weitere Informationen finden Sie unterErstellen Sie Regeln für das automatische Schließen.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Konfiguration für automatisches Schließen** > **Veraltete Erkennungen**.
   Das Formular „Veraltete Konfiguration automatisch schließen“ wird angezeigt.
2. Füllen Sie die Felder aus.
3. Wählen Sie für das Feld **Veraltete Erkennungen automatisch schließen basierend auf** eine Option für Ihre Suche aus.

   Beide Suchen gleichen das Alter älterer, veralteter Erkennungen in Tagen mit einem von Ihrem Scanner bereitgestellten Datum ab.

   Hinweis:
   Ab v22.0 von Vulnerability Responsewerden die Optionen **Zuletzt gefundene Erkennungen** und **Zuletzt gescannte Assets** als Liste erstellt.

   - **Zuletzt gefundene Erkennungen**. Mit dieser Option wird nach dem aktuellen oder spätesten Datum gesucht, an dem Erkennungen vom Scanner erneut gefunden wurden.

     Hinweis:
     Für Rapid7 - und MicrosoftMicrosoft Azure Event Hubs TVM-Benutzer wird eine Warnmeldung angezeigt, dass aktuelle Erkennungsinformationen erforderlich sind.

     Wenn Sie **Zuletzt gefundene Erkennungen** als Grundlage für Ihre Suche auswählen, erfordert diese Funktion eine erfolgreiche Integrationsausführung einer der Rapid7 Comprehensive Vulnerable Item Integrations innerhalb der letzten sieben Tage.

     Wenn Sie **Zuletzt gefundene Erkennungen** als Grundlage für Ihre Suche auswählen, erfordert diese Funktion eine erfolgreiche Integrationsausführung der Microsoft TVM Machine Vulnerabilities-Integration (vollständiger Import) innerhalb der letzten sieben Tage.

   - **Zuletzt gescannte Assets**. Mit dieser Option wird das aktuellste Datum gesucht, an dem ein Asset zuletzt von einem Drittanbieter-Scanner gescannt wurde.
4. Stellen Sie nur für die TVM-Benutzer Rapid7 und MicrosoftMicrosoft Azure Event Hubs sicher, dass alle erforderlichen Integrationen aktiviert sind.
   Siehe Rapid7 Vulnerability-Integration verstehen und Informationen zur Schwachstellenintegration von Microsoft Threat and Vulnerability Management, um weitere Informationen zu erhalten.
5. Um das Modul zu aktivieren, klicken Sie auf das Kontrollkästchen Aktiv, um es auszuwählen.
6. Geben Sie im Feld **Zuletzt gefundene Erkennungen (vor Tagen)** das Alter älterer, veralteter Erkennungen in Tagen ein.

   Der Standardwert ist 90 Tage. Sie können einen beliebigen positiven Wert für die Anzahl der Tage eingeben. Dieser Wert wird verwendet, um ein von Ihrem Scanner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bereitgestelltes Datum abzugleichen. Wenn 90 und **Zuletzt gefundene Erkennungen** angezeigt werden, werden alle Erkennungen, die in den letzten 90 Tagen nicht gefunden wurden, automatisch geschlossen. Wenn 90 und **Zuletzt gescannte Assets** angezeigt werden, werden Erkennungen, die Assets zugeordnet sind, die in den letzten 90 Tagen nicht gescannt wurden, automatisch geschlossen.

Hinweis:

Es besteht eine Beziehung zwischen dem Feld **„Zuletzt gefundene Erkennungen/ Zuletzt (vor Tagen) gescannte Assets“** für diese Funktion und dem Feld „ **Importieren seit** “ in der Integration von Rapid7 Comprehensive Vulnerable Item Integration – API und Microsoft TVM Machine Vulnerabilities-Integration.

Für diese Integrationen ist das Feld **Importieren seit** auf den Konfigurationsseiten standardmäßig leer.

Wenn Sie keinen Wert eingeben oder das Feld keinen Wert enthält, werden die Daten für die Anzahl der Tage verwendet, die im Feld **Zuletzt gefundene Erkennungen/Zuletzt gescannte Assets (vor Tagen)** konfiguriert sind.

Wenn beispielsweise die Anzahl der im Konfigurationsformular für das automatische Schließen definierten Tage 90beträgt und das Feld **Importieren seit** auf den Konfigurationsseiten der Integration leer ist, werden bei der ersten Integrationsausführung die Daten der letzten 90 Tage importiert. Die Felder **„Importieren seit“** für Rapid7 Integration von Comprehensive Vulnerable Item Integration – API und die Integration von Microsoft TVM Machine Vulnerabilities können bearbeitet werden, sodass Sie auch beliebige Werte angeben können. Der 90-Tage-Wert wird als Standard angegeben, wenn das Feld leer bleibt, damit die Funktion zum automatischen Schließen der Falschmeldungen nicht schließt.

Diese Beziehung zwischen diesen Feldern gilt nur für die erste Integrationsausführung. Danach hat eine Änderung des Felds **Zuletzt gefundene Erkennungen/Zuletzt gescannte Assets (vor Tagen)** im Formular „Veraltete angreifbare Erkennungen automatisch schließen“ keine Auswirkung auf das Feld **Importieren seit** auf den Konfigurationsseiten der Integration. Das Feld wird in die Startzeit der ersten Ausführung geändert, sodass die nachfolgenden Integrationsausführungen nur die Delta-Informationen importieren.

7. **Wahlweise:** Aktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für zurückgestellte VIs ignorieren**, um veraltete Erkennungen zu ignorieren, die zurückgestellten VIs oder VIs zugeordnet sind, die derzeit für eine Zurückstellung überprüft werden.

   (Optional) Wenn Sie diese Option deaktiviert lassen, werden alle Erkennungen geschlossen, die Ihren Kriterien entsprechen und zurückgestellten VIs zugeordnet sind oder VIs zugeordnet sind, die zur Zurückstellung überprüft werden. Die zurückgestellten oder in Überprüfung befindlichen AEs, die diesen Erkennungen entsprechen, werden basierend auf der Rollup-Logik ebenfalls automatisch geschlossen. Weitere Informationen zur Rollup-Logik finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response.

   Wenn Sie diese Option aktivieren, werden alle Erkennungen, die Ihren Kriterien entsprechen und zurückgestellten VIs zugeordnet sind oder VIs, die zur Zurückstellung überprüft werden, während des automatischen Schließens übersprungen.

8. **Wahlweise:** Deaktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Standardmäßig ist dieses Kontrollkästchen aktiviert, damit das geschlossene AE nicht erneut geöffnet wird, wenn eine neue Erkennung im Zusammenhang mit diesem geschlossenen AE identifiziert wird. Weitere Informationen zur Rollup-Logik finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response.

9. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

Die regelmäßige *Auto-Close Stale Detections*-Aufgabe wird täglich ausgeführt. Die Aufgabe bestimmt, ob Sie das Datum ausgewählt haben, an dem Erkennungen zuletzt gefunden wurden, oder das Datum, an dem Assets zuletzt gescannt wurden. Anschließend werden die entsprechenden Erkennungen in den Status Veraltet versetzt. Es ist wichtig zu beachten, dass die Funktion Veraltete Erkennungen automatisch schließen nur veraltete Erkennungen für aktive Integrationsinstanzen schließt. Angreifbare Elemente und Erkennungen, die aktiven Integrationsinstanzen zugeordnet sind, werden geschlossen. Ab v22.0 von Vulnerability Response wurde die geplante Aufgabe geändert, um die allgemeine Tabelle [sn_vul_cmn_auto_close_rule] zu berücksichtigen.

Nachdem die Erkennungen als Veraltet markiert wurden und der Scanner meldet, dass diese Erkennung erneut gefunden wurde, wechselt das Feld Status der Erkennungen in Offen. Die entsprechenden angreifbaren Elemente der Erkennung werden ebenfalls erneut geöffnet.

Wenn die Erkennung als Veraltet markiert ist und der Scanner feststellt, dass sie behoben ist, geht die Erkennung außerdem in den Status Geschlossen über. Der Status wird auch bis zu den VIs hochgerollt.

Erstellen Sie Regeln für das automatische Schließen

Verwenden Sie Regeln zum automatischen Schließen, um ältere Erkennungen basierend auf den von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: sn_vul.manage_auto_close_stale_vi

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für automatisches Schließen**.

   Das -Basissystem stellt die folgenden Regeln für das automatische Schließen bereit:

   - **Zuletzt gescannte Assets**: Erkennungen, die Assets zugeordnet sind, die in den letzten 90 Tagen nicht gescannt wurden, werden in den Status **„Veraltet“** versetzt.
   - **Zuletzt gefundene manuelle Erkennungen**: Manuelle Erkennungen, die in den letzten 90 Tagen nicht gefunden wurden. Wenn Sie den **zuletzt gefundenen Datensatz für Erkennungen** aktivieren, erfordert diese Funktion eine erfolgreiche Integrationsausführung von Rapid7 Comprehensive Vulnerable Item Integrations und Microsoft TVM Machine Vulnerabilities Integration (Vollständiger Import) innerhalb der letzten sieben Tage.
   - **Zuletzt gefundene Erkennungen**: Erkennungen, die in den letzten 90 Tagen nicht gefunden wurden.

2. Wählen Sie **Neu** aus, um eine neue Regel für das automatische Schließen zu erstellen.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Name	Name der Regel zum automatischen Schließen.
Aktiv	Option zum Aktivieren der Regel. Wenn aktiviert, werden Erkennungen automatisch geschlossen, die den Filterkriterien entsprechen.
Zurückgestellte Elemente ignorieren	Wenn diese Option ausgewählt ist, werden Erkennungen, die den Status **„Wird überprüft“** oder **„Zurückgestellt“** zugeordnet sind, ignoriert und nicht geschlossen. Wenn Sie diese Option deaktivieren, werden alle Erkennungen geschlossen, die Ihren Kriterien entsprechen.
Ausführungsreihenfolge	Eindeutiger Wert für die Ausführung der Regel zum automatischen Schließen. Dieser Wert bestimmt die Reihenfolge der Ausführung. Der Standardwert ist 100.
Beschreibung	Beschreibung der Regel zum automatischen Schließen.
Bedingung	Filterbedingungen, die zum Identifizieren von Erkennungen verwendet werden, die geschlossen werden sollten.

4. Wählen Sie **Absenden**.

   Die regelmäßige *Auto-Close Stale Detections*-Aufgabe wird täglich ausgeführt. Identifiziert Erkennungen basierend auf den angegebenen Bedingungen und versetzt die übereinstimmenden in den Status **Veraltet**. Die Aufgabe verarbeitet die folgenden Szenarien:

   - Wenn alle Erkennungen in einem angreifbaren Element (VIT) als veraltet markiert sind, wird das VIT mit dem Substatus „Veraltet“ geschlossen.
   - Wenn es mindestens eine Erkennung gibt, die innerhalb einer VIT geöffnet bleibt, während sich andere im Status „Veraltet“ befinden, bleibt die VIT offen.
   - In Fällen, in denen in einer VIT Erkennungen mit den Status „Geschlossen“ und „Veraltet“ vorhanden sind, wird die VIT mit dem Substatus „Behoben“ geschlossen.

   Wenn Sie ein Upgrade auf die neueste Version von Vulnerability Responsedurchführen, werden auch die in Ihren Regeln für das automatische Schließen festgelegten Bedingungen entsprechend aktualisiert. Wenn die Regeln außerdem verschiedenen Domänen zugeordnet sind, werden sie speziell innerhalb dieser Domänen erstellt.

Klassifizieren Sie nicht klassifizierte Hardware neu

Klassifizieren Sie nicht klassifizierte Hardware neu, indem Sie die CI-Suchregeln aktualisieren.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.admin

Warum und wann dieser Vorgang ausgeführt wird
In der Tabelle „Host-Importzuordnung“ [sn_sec_cmn_src_cmdb_map] werden die eingehenden Variablen der Nutzlast und die entsprechenden Zuweisungen in der Tabelle „Erkannte Elemente“ angezeigt. Gelegentlich können Diskrepanzen in den Namenskonventionen zwischen Scanner und Discovery dazu führen, dass die Hardware nicht klassifiziert wird. Stellen Sie beim Erstellen eines neuen nicht klassifizierten Hardware-CI sicher, dass der Name in der Nutzlast nur den Hostnamen enthält. Später, wenn Discovery das Asset identifiziert hat, kann es in die entsprechende CI-Klasse neu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

klassifiziert werden. Bei Bedarf kann ein Skript geschrieben werden, um einen abgeleiteten Wert zu generieren, der mit dem CI-Namen in Discovery und Configuration Management Database (CMDB) übereinstimmt.

Wenn die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

Prozedur

1. Navigieren Sie zur Tabelle „Hostimportzuordnungen“ [sn_sec_cmn_src_cmdb_map].
2. Wählen Sie eine Quelle aus.
3. Wählen Sie in der Liste Zielfeld **die Option Name**aus.
   Die Checkbox **Use script (Skript verwenden)** wird sichtbar.

   Hinweis:
   - Das Skript ist nur verfügbar, wenn **Name** in der Liste Zielfeld ausgewählt wird.
   - Um ein Skript für andere Optionen in der Liste des Zielfelds hinzuzufügen, müssen Sie die UI-Richtlinie wie folgt deaktivieren:
     - „Festlegen von „Skript verwenden“ auf „falsch““ wird deaktiviert.
     - „Skriptverwendung anzeigen oder ausblenden“ wird deaktiviert.
     - Die Bedingung „Zielfeld ist Name“ in „Skriptrichtlinie anzeigen oder ausblenden“ wird entfernt.
   - Die Tabelle „Host-Importzuordnungen“ wird mit zwei neuen Spalten aktualisiert: Skript und Skript verwenden.

4. Aktivieren Sie die Checkbox **Skript verwenden**.
   Im Feld **Skript** wird das Standardskript angezeigt, Sie können jedoch ein anwenderdefiniertes Skript erstellen. In diesem Feld können Sie die Quell- und abgeleiteten Werte angeben, um sie an die Namenskonvention der Datenbank anzupassen. Der vom Skript generierte Wert wird in sourcePayload['DERTIVED'][rule.source_field] gespeichert. Stellen Sie sicher, dass die CI-Suchregeln so angepasst sind, dass beim Einchecken in die entsprechenden Tabellen die Quellnutzlast sowie abgeleitete und zielgerichtete Attributwerte verwendet werden.
5. Um das Skript auf ältere doppelte Datensätze anzuwenden, gehen Sie wie folgt vor:
   a. Navigieren zu **Alle** > **Vulnerability Response** > **Erkannte Elemente**.
   b. Wählen Sie die doppelten Datensätze aus.
   c. Wählen Sie in der Liste Aktion für ausgewählte Zeilen **die Option CI-Suchregeln erneut anwenden aus**.
      Zeigt eine Übereinstimmung mit einem vorhandenen Asset an.
6. Um das Skript für Tenable.ioanzuwenden, gehen Sie wie folgt vor:
   a. Navigieren zu **Vulnerability Response Host-Importzuordnungen**.
   b. Wählen Sie das Skript für die Zeile mit NetBIOS, HOSTNAMES und FQDNS-Namen als **Quellfeld** aus.
   c. Aktualisieren Sie das Skript für jedes Element.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für Tenable.iogibt der Scanner ein Array für NetBIOS, HOSTNAMES und FQDNS-Namen zurück, für das das Skript nicht wie erwartet funktioniert.

Da die Host-Importzuordnung für Tenable.io im Feld **„Quelle" denWert „netBIOS_name"** enthält, müssen Sie ein Skript schreiben. Während der Suche wird ein anderes Quellfeld **(NETBIOS)** verwendet, das ein Array von Werten enthält. Daher wird in der Tabelle eine neue Zeile hinzugefügt, und die gleiche Logik muss in einer Schleife im Skript geschrieben werden. Entsprechendes gilt für **FQDNS** und **HOSTNAMES**.

7. Um das Skript für Rapid7anzuwenden, gehen Sie wie folgt vor:
   a. Navigieren zu **Alle** > **Vulnerability Response Host-Importzuordnungen**.
   b. Aktualisieren Sie für Rapid7 Zeilen mit FQDN und HostName die Suchmethode auf Skript.

Hinweis:
Für Rapid7ist die CI-Suchmethode auf Feldübereinstimmung für FQDN und Hostname festgelegt, wodurch verhindert wird, dass das Skript verwendet wird.

Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response

Das manuelle Erstellen einer Korrekturaufgabe erfolgt, wenn Sie angreifbare Elemente nach etwas anderem als den Kriterien für Korrekturaufgabenregeln gruppieren möchten. Sie können beispielsweise Aufgaben für einen bestimmten Manager oder für aktive, neue Exploits wie Ransomware erstellen, die verschiedene Schwachstellen beinhalten. Sie können sie auch verwenden, um nicht gruppierte angreifbare Elemente zu gruppieren.

Wichtig:
Wo können Sie Host-Korrekturaufgaben erstellen?

- Vulnerability Manager Workspace als Benutzer mit der Rolle sn_vul.vulnerability_analyst, oder sn_vul.vulnerability_admin festlegen.
- IT Remediation Workspace als Benutzer mit der Rolle sn_vul.remediation_owner.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.

   Die Regeln für Korrekturaufgaben funktionieren genauso wie zuvor die Regeln für Korrekturaufgaben und stehen Ihnen weiterhin zur Verfügung. Möglicherweise möchten Sie die Regeln für Korrekturaufgaben jedoch inaktiv lassen, da Sie sich an die Funktionen geübt haben, die Ihren Sicherheitsmanagern und IT-Teams in den Arbeitsbereichen zur Verfügung stehen.

2. Wählen Sie eine der Kategorien für Aufgaben aus, um die Liste zu öffnen.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.
   Informationen zu bestimmten Feldern finden Sie unter Formularfelder für Korrekturaufgaben.
5. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Aufgabe erstellt wird, sucht die zugehörige Liste **„Angreifbares Element“** mit dem Filtertyp **„Bedingung“** oder **„Filtergruppe“** nach allen übereinstimmenden angreifbaren Elementen und zeigt sie an.

Sie können den zugehörigen Link **Erneut nach Schwachstellen scannen** verwenden, um einen ServiceNow® – initiierten Scan manuell auszulösen. Informationen zum Konfigurieren eines Schwachstellenscanners finden Sie unter Konfigurieren und verwalten Sie Qualys Schwachstellenscanner und Scans.

Für eine Qualys Vulnerability Integration ist im Modul **Schwachstellenscanner** ein Standardscanner vorinstalliert. Dieser Scanner ist standardmäßig deaktiviert. Aktivieren Sie die Kontrollkästchen **Aktiv** und **Standard**, um den Qualys-Scanner für die Verwendung mit dem zugehörigen Link Auf **Schwachstellen scannen** auf den Formularen für Korrekturaufgaben und angreifbare Elemente zu aktivieren.

Der zugehörige Link **Update-Status** zeigt Datum und Uhrzeit der letzten Aktualisierung an. Er fasst Informationen aus den VIs in der Korrekturaufgabe zusammen. Weitere Informationen finden Sie unter Formularfelder für Korrekturaufgaben. Wenn eine Aufgabe auf Grundlage einer bestimmten Schwachstelle erstellt wird, wird diese Schwachstelle im Formular für Korrekturaufgaben aufgeführt.

Wenn Sie ein zugeordnetes angreifbares Element öffnen, werden alle zugehörigen Korrekturaufgabeneinträge unter der Registerkarte der zugehörigen Liste **„Korrekturaufgabe“** angezeigt.

Fügen Sie der Vulnerability Response-Gruppe Benutzer hinzu

Wenn die Funktion „Schließen/Zurückstellen“ verwendet wird, um ein angreifbares Element zurückzustellen oder zu schließen, ohne dass ein Scan erforderlich ist, wird die Gruppe Vulnerability Response benachrichtigt, um die Anforderung zu genehmigen oder abzulehnen. Sie können die entsprechenden Benutzer zuweisen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**.
2. Öffnen Sie die Gruppe Vulnerability Response.
3. Klicken Sie auf die zugehörige Liste **Gruppenmitglieder** und anschließend auf **Bearbeiten**.
4. Wählen Sie einen oder mehrere Namen in der Liste **Sammlung** aus.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Einen Benutzer erstellen

Verwalten Sie einzelne angreifbare Elemente manuell

Angreifbare Elemente stellen ein Configuration Item (CI) mit einer bestimmten Schwachstelle dar. Angreifbare Elemente werden aus Drittanbieterquellen oder mithilfe der SAM-NVD-Informationen (Link) importiert, um Schwachstelleneinträge mit Softwaredatensätzen zu vergleichen, die aus dem Modul „Software“ Asset-Management abgerufen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbare Elemente sind in Korrekturaufgaben enthalten, die durch Schwachstellenregeln definiert werden. Normalerweise sind Korrekturaufgaben der Ort, an dem Gruppen angreifbarer Elemente zugewiesen werden und an dem gearbeitet wird.

Angreifbare Elemente können im Modul **„Angreifbare Elemente“** massenweise angezeigt und bearbeitet werden. Datensätze zu angreifbaren Elementen zeigen auf der Registerkarte Schwachstelle Informationen aus der **Schwachstelle** an. Diese Registerkarte kann angeben, ob öffentliche oder aktive Exploits dafür vorhanden sind. Außerdem wird angezeigt, ob dies durch einen Patch, eine Konfigurationsänderung oder eine Kombination aus beidem behoben werden kann. Wenn während der Deduplizierung IP-Adressen gefunden werden, werden sie in einer zugehörigen Liste angezeigt.

Wenn ein CI aus der CMDB entfernt wird, werden auch alle zugehörigen angreifbaren Elemente entfernt.

Wenn ein angreifbares Element zu einer Korrekturaufgabe hinzugefügt wird, wird die Gruppe in der Liste **Korrekturaufgaben** der angreifbaren Elemente angezeigt.

Wenn eine Aufgabe erstellt wird, die ein angreifbares Element betrifft, wird die Aufgabe in der zugehörigen Liste **„Betroffene Aufgaben“** der angreifbaren Elemente angezeigt.

Angreifbare Elemente können manuell erstellt werden. Sie können Security Incidents oder Change-Anforderungen erstellen und manuell schließen oder zurückstellen. Regeln für Korrekturaufgaben können auf manuell erstellte angreifbare Elemente angewendet werden.

Korrekturaufgaben und Regeln für Korrekturaufgaben wurden erweitert und übernehmen nun die Aufgabenfunktionalität. Angreifbare Elemente können nicht als übergeordnete Aufgabe verknüpft werden.

Erstellen Sie Vulnerability Response angreifbare Elemente

Mehrere Methoden erstellen angreifbare Elemente (VIs, Vulnerable Items). Meistens wird eine Integration in einen Schwachstellenscanner so installiert und konfiguriert, dass die Ergebnisse nächtlich importiert werden. Es gibt Fälle, z. B. bei physischen Sicherheitsschwachstellen, in denen Sie Datensätze für angreifbare Elemente möglicherweise manuell hinzufügen möchten.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Warum und wann dieser Vorgang ausgeführt wird

Manuell erstellte VIs und automatisch erstellte VIs werden durch Korrekturaufgabenregeln und Gruppenbedingungen automatisch zu Korrekturaufgaben hinzugefügt und daraus entfernt.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Wählen Sie eine Kategorie aus, um die Liste zu öffnen.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.
   Informationen zu den Feldern für angreifbare Elemente finden Sie unter Vulnerability Response Formularfelder für angreifbare Elemente.
5. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.

   Die Regeln für Korrekturaufgaben werten das angreifbare Element aus und fügen es einer vorhandenen Aufgabe hinzu oder erstellen eine neue Aufgabe. Wenn die Bewertung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

fehlschlägt, wird das angreifbare Element der Liste **„Nicht gruppierte angreifbare Elemente“** hinzugefügt.

Wenn Sie ein neues angreifbares Element speichern, werden alle aktivierten Rechner ausgeführt.

Hinweis:
Pro **Zielfeld** darf jeweils nur ein Rechner aktiv sein. Wenn Sie eines aktivieren, werden alle anderen mit demselben **Zielfeld** deaktiviert.

6. Sie können auf jede der zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

   Sie können den zugehörigen Link **Auf Schwachstellen scannen** verwenden, um manuell einen ServiceNow® -initiierten Scan auszulösen. Informationen zum Konfigurieren eines Schwachstellenscanners finden Sie unter Konfigurieren und verwalten Sie Qualys Schwachstellenscanner und Scans.

   Für eine Qualys Vulnerability Integration ist im Modul **Schwachstellenscanner** ein Standardscanner vorinstalliert. Dieser Scanner ist standardmäßig deaktiviert. Aktivieren Sie die Kontrollkästchen **Aktiv** und **Standard**, um den Qualys-Scanner für die Verwendung mit dem zugehörigen Link Auf **Schwachstellen scannen** auf den Formularen für Korrekturaufgaben und angreifbare Elemente zu aktivieren.

   In der Kopfzeile sind die folgenden Bearbeitungs- und Korrekturoptionen verfügbar:

   - Aktualisieren: Speichert Aktualisierungen im Formular.
   - Security Incident erstellen: Erstellt einen Security Incident.
   - Schließen: Schließt das Element. Wenn alle Elemente in der Gruppe geschlossen sind, wird die Korrekturaufgabe automatisch geschlossen.
   - Ausnahme anfordern: Sendet eine Anforderung zum Zurückstellen eines Elements.
   - Lösen: Löst das Element auf.
   - Löschen: Entfernt das angreifbare Element.

Zugehörige Informationen

Führen Sie eine Massenbearbeitung von angreifbaren Elementen in durch Vulnerability Response

Ein angreifbares Element zurückstellen

Wenn Sie feststellen, dass das mit einem angreifbaren Element (VIT) verbundene Problem ein geringes Risiko aufweist und ohne weitere Analyse sofort zurückgestellt werden kann, können Sie die Funktion **Zurückstellen** verwenden.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Täglich wird eine geplante Aufgabe ausgeführt, um nach zurückgestellten angreifbaren Elementen zu suchen, deren Wiedereröffnungsdatum erreicht ist. An dem Tag, an dem die Zurückstellung des AE abläuft, wird der Datensatz erneut geöffnet.

Ab Vulnerability Response v20.0 prüft die geplante Aufgabe „Angreifbares Element und Gruppen-Aufschubablauf prüfen“ vor dem erneuten Öffnen eines zurückgestellten AE, ob eine Ausnahmeregel für ein zurückgestelltes AE gilt, und aktualisiert die Felder **„Grund** “ und **„Bis“** gemäß der Ausnahmeregel. Der Status des AE bleibt bis zum spätesten Ablaufdatum zurückgestellt.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie auf **Ausnahme anfordern**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Bis	Wählen Sie das Datum aus, an dem der Status „Zurückgestellt“ abläuft und die Korrekturaufgabe erneut aktiviert wird. **Hinweis:** Ab Version 18.0 von Vulnerability Response (VR) wird der Status der VIT unter Berücksichtigung des aktiven Ausnahmefensters in den Status „Zurückgestellt“ geändert, wenn ein zurückgestelltes angreifbares Element von einem Scanner geschlossen und erneut geöffnet wird, bevor das Ausnahmefenster abläuft. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft sn_vul.auto_defer_vit_in_active_exception_window auf „wahr“ fest. Außerdem bleibt das zurückgestellte Bis-Datum auch dann erhalten, wenn das angreifbare Element geschlossen wird oder die Ausnahme abgelaufen ist. Die erforderliche Rolle für Lese- und Schreibzugriff lautet sn_vul.manage_exception_configuration. Nachdem der Datensatz übermittelt wurde und E-Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Vulnerability Response eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird das angreifbare Element auf „Offen“ zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Falsch positiv ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Klicken Sie auf **Absenden**.
   Die Gruppe wird **als In Überprüfung**markiert. Der zugehörige Link **Erneut öffnen** wird angezeigt. Das Datum und der Grund der Wiedereröffnung werden in den Arbeitsnotizen unter der Registerkarte **Change-Genehmigungen** anzeigen angezeigt.

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht wird. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Öffnen Sie ein zurückgestelltes angreifbares Element.
3. Wählen Sie **Verlängerung anfordern**aus.

Hinweis:
Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Elements Zurückgestellt ist.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	angreifbaren Elements verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

   Hinweis:
   - Die Anforderung durchläuft zwei Genehmigungsebenen.
   - Wenn eine zurückgestellte Ausnahmeregel erneut verlängert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden die Hinweise Bis, Grund und Zurückstellung aktualisiert.

Aktualisieren Sie Vulnerability Response angreifbare Elemente

Der zugehörige Link **Status aktualisieren** wird verwendet, um angreifbare Elemente zu überprüfen und festzustellen, ob zusätzliche angreifbare Elemente vorhanden sind, die zu einer Korrekturaufgabe gehören. Verwenden Sie diese Option, wenn ein Update außerhalb der geplanten Aufgabe erforderlich ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write oder, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Der zugehörige Link **„Status aktualisieren“** kann im Formular für Korrekturaufgaben nur im Status **„Offen“** oder **„Wird untersucht“** mit einer Filtergruppe oder mit dem Filtertyp „Bedingung“ bearbeitet werden. Diese Inspektion wird unabhängig vom Status des Kontrollkästchens **Angreifbare Elemente automatisch aktualisieren** durchgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab v22.0 von Vulnerability Responseist die Schaltfläche **Status aktualisieren** in der Datensatzansicht für Korrekturaufgaben in Vulnerability Manager Workspace und IT Remediation Workspaceverfügbar.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie einen beliebigen -Datensatz im Status „ **Offen“** oder **„Wird untersucht“**.
3. Klicken Sie auf den Link **Status aktualisieren**.
   Neue angreifbare Elemente werden unter der Registerkarte **„Angreifbare Elemente“** angezeigt.

Identifizieren und eskalieren Sie Sicherheitsprobleme in Software von Drittparteien

Sie können Softwareschwachstellen anzeigen, die von Einträgen von Drittanbietern zurückgegeben wurden, um die Nachbesserung zu bestimmen. Verwenden Sie diese Informationen, um die Einträge verwundbarer Software mit einem Software-Discovery-Modell Asset-Management abzugleichen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Bibliotheken** > **Drittpartei**.
   Eine Liste der heruntergeladenen angreifbaren Software wird angezeigt.
2. Klicken Sie auf einen Softwaredatensatz, um Informationen zu Schwachstellen anzuzeigen.
3. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zur Identifizierung von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie bei Bedarf Lösen Sie Korrekturaufgaben.

Erkennen und eskalieren Sie Sicherheitsprobleme mithilfe von NVD

Wenn CVE-ID-Datensätze (Common Vulnerability and Exposures Identifier) aus der National Vulnerability Database (NVD) heruntergeladen werden, werden sie mit der Software in Ihrem Unternehmensnetzwerk verglichen, die vom Software-Asset-Discovery-Modell identifiziert wurde. Wenn eine CVE-ID mit einer angreifbaren Software oder einem Konfigurationselement in Ihrem Netzwerk übereinstimmt, wird ein angreifbares Element erstellt. Sie verwenden die Informationen im CVE-ID-Datensatz, um zu entscheiden, ob das angreifbare Element zur Korrektur eskaliert werden soll.

Vorbereitungen

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **NVD**.
   Eine Liste der CVE-IDs, die vom NVD heruntergeladen wurden, wird angezeigt. Updates vom NVD können bei Bedarf und durch geplante Ausführungen aus den Datensätzen Integration der US-Schwachstellendatenbank (National Vulnerability Database Integration) des NIST unter durchgeführt werden **Alle** > **Administration** > **Integrationen**.
2. Klicken Sie auf einen CVE-Datensatz, um die folgenden Informationen anzuzeigen:
   - Eine Zusammenfassung für die CVE-ID
   - ein Verweis auf einen Eintrag in der Common Weakness Enumeration (CWE), falls zutreffend.
   - die Schwachstellenpunktzahl der CVE-ID im Common Vulnerability Bewertungssystem (CVSS). Weitere Informationen zu CVSS finden Sie auf der Website der National Vulnerability Database .
3. Klicken Sie auf die zugehörigen Listen, um weitere Informationen zu Schwachstellen zu erhalten.

   Verwundbarkeitsreferenzen

   Name, Beschreibung und URL für die angegebene Schwachstelle sowie Verweis darauf.

   Exploits

   Detailinformationen

   Schwachstellen

   Liste der CWE-Schwachstellen.
4. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zur Identifizierung von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie bei Bedarf Lösen Sie Korrekturaufgaben.

Identifizieren und eskalieren Sie Sicherheitsprobleme mit CWE

Zeigen Sie die Bibliothek der Common Weakness Enumeration (CWE)-Datensätze aus der National Vulnerability Database (NVD) an, um zu verstehen, wie sie sich auf die Common Vulnerability and Exposure-Datensätze (CVE) beziehen. Verwenden Sie dann diese Informationen, um die Einträge verwundbarer Software mit einem Software-Discovery-Modell Asset-Management abzugleichen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Bibliotheken** > **CWE**.
   Eine Liste der heruntergeladenen angreifbaren Software wird angezeigt.
2. Klicken Sie auf einen CWE-Softwaredatensatz, um Informationen zu Schwachstellen anzuzeigen.
3. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zur Identifizierung von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie bei Bedarf Lösen Sie Korrekturaufgaben.

Zeigen Sie den Nachbesserungszielstatus eines angreifbaren Elements Vulnerability Response an

Wenn ein angreifbares Element sein durch eine Korrekturzielregel definiertes Korrekturzieldatum fast erreicht (oder überschritten) hat, wird der Datensatz des angreifbaren Elements mit einem Status aktualisiert. Diese Informationen können dem Analysten helfen, bevorstehende Korrekturaktivitäten proaktiv zu überwachen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules [schreibgeschützt]

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Die geplante Aufgabe **„Korrekturziele auswerten“** wird einmal pro Tag ausgeführt, um das aktuelle Datum mit dem Korrekturdatum für angreifbare Elemente zu vergleichen, das in der zugehörigen Korrekturzielregel angegeben ist. Wenn das aktuelle Datum innerhalb der Anzahl der Tage liegt, bevor die Remediation überfällig ist, wird dem Datensatz des angreifbaren Elements ein Remediationsstatus hinzugefügt.

Weitere Informationen zu Korrekturzielregeln finden Sie unter Vulnerability Response Korrekturzielregeln.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Angreifbare Elemente**.
2. Klicken Sie auf das angreifbare Element, das Sie überprüfen möchten.
   Wenn das Korrekturdatum für das angreifbare Element im Bereich der in der Korrekturzielregel festgelegten Bedingungen liegt, wird die Registerkarte **Korrekturzielstatus** angezeigt.
3. Klicken Sie auf die Registerkarte **Korrekturzielstatus**.
4. Klicken Sie auf den Statusdatensatz des Korrekturziels, um ihn zu überprüfen.

Hinweis:
Informationen zum Anzeigen der Anzahl der angreifbaren Elemente, die sich dem Ziel nähern, sich in der Ausführung befinden und in der Vergangenheit liegen, finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln

Arbeiten mit nicht abgeglichenen CIs

Als Schwachstellenmanager und Analyst können Sie nicht abgeglichene Configuration Items (CIs) anzeigen und neu klassifizieren, erkannte Elemente abgleichen, die nicht abgeglichen wurden, CI-Suchregeln erneut auf die ausgewählten erkannten Elemente anwenden und vorhandene CIs deduplizieren.

Nicht abgeglichene Konfigurationselemente anzeigen und neu klassifizieren

Configuration Items (CIs), die nicht in Configuration Management Database (CMDB) gefunden wurden, werden in einer sichtbaren Liste erkannter Elemente platziert. Diese Liste bietet eine praktische Möglichkeit, nicht abgeglichene CIs neu zu klassifizieren.

Vorbereitungen

Erforderliche Rolle:

sn_vul.read (Minimum zum Anzeigen von nicht abgeglichenen CIs)

und

itil oder Asset (zur Neuklassifizierung)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenanalyst können Sie nicht abgeglichene CIs anzeigen.

Die Aktion zum erneuten Klassifizieren ist nur für CIs der Klasse `sn_sec_cmn_unmatched_ci` verfügbar, wenn Sie entweder die Rolle itil oder asset innehaben. Sobald ein CI erneut klassifiziert wurde, kann es über die Anwenderoberfläche nicht erneut klassifiziert werden. Sie können über das CI-Formular oder die CI-Listenansicht neu klassifizieren, indem Sie den **Klassenwert** ändern. Weitere Informationen finden Sie unter Reclassify a CI .

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Erkannte Elemente**.
2. Klicken Sie zum Überprüfen auf die einzelnen Elemente.
3. Um Korrekturen an den Informationen in den Feldern des Formulars **„Erkanntes Element“** vorzunehmen, bearbeiten Sie sie auf dieser Seite, und klicken Sie mit der rechten Maustaste **auf Speichern**.
   Alle Daten, die diesen Feldern hinzugefügt werden oder darin verbleiben, werden bei der erneuten Klassifizierung an das resultierende **Konfigurationselement** übertragen.
4. Wenn alles richtig aussieht, klicken Sie auf **Erneut klassifizieren**.
5. Wählen Sie in der Auswahlliste einen **Klassennamen** aus, und klicken Sie auf **Absenden**.
   Die **Klassedes erkannten Elements** wird aktualisiert, das Feld **„Status“** wird in „Neu klassifiziert“ geändert, und alle Daten befinden sich in der CMDB.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht übereinstimmende erkannte Elemente abstimmen

Erstellen Sie eine regelmäßige Aufgabe, um nicht abgeglichene erkannte Elemente abzugleichen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Ein angreifbares Element (VI) besteht aus einer Schwachstelle und einem Konfigurationselement (Configuration Item, CI). Wenn ein VI erstellt wird, ist das zum Zeitpunkt der Erstellung hinzugefügte CI möglicherweise veraltet. Nicht abgeglichene CI-Informationen werden nicht abgeglichen, wenn sich die Informationen in der CMDB ändern. Um abzugleichen, wenden Sie die Suchregeln für Configuration Item (CI) auf die Elemente an, die sich in einem nicht abgeglichenen Status befinden, wenn die CMDB mit den neuesten CIs aktualisiert wird.

Sie können einen Bedarf für eine geplante Aufgabe ausführen, um die CI-Übereinstimmungsregel für erkannte Elemente in einem nicht abgeglichenen Status erneut anzuwenden. Wenn sich das CI nach dem erneuten Anwenden der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Betroffene Erkennungen und angreifbare Elemente werden ebenfalls aktualisiert. Details finden Sie unter CI-Changes für erkannte Elemente.

Prozedur

1. Navigieren zu **Alle** > **Security Operations > Nicht übereinstimmende erkannte Elemente abgleichen**.
2. Klicken Sie auf der Seite „Hintergrundaufträge“ **auf Abgleichsauftrag erstellen**.
3. Füllen Sie die Felder des Formulars aus.

Hinweis:
Sie können nur das Feld **„Parameter“** bearbeiten.

Formular „Hintergrundauftrag“.

Feld	Beschreibung
Nummer	Eindeutige Auftragsnummer.
Erstellt von	Benutzer, der den Auftrag erstellt hat.
Parameter	Parameter zum Abgleichen der nicht abgeglichenen erkannten Elemente: ○ limit: Maximale Anzahl erkannter Elemente, die abgeglichen werden sollen. Wenn Sie keinen Wert eingeben, werden 10.000 erkannte Elemente abgeglichen. ○ firstDiscovereditem: Erstes erkanntes Element, das abgeglichen werden muss. Wenn Sie keinen Wert eingeben, beginnt der Abgleichsprozess mit dem ersten erkannten Element.
Status	Aktueller Status des Hintergrundauftrags.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Statusbeschreibung	Beschreibung des aktuellen Status des Hintergrundauftrags.
Auftragstyp	Typ des Auftrags. Der Wert lautet **Abgleich nicht übereinstimmender erkannter Elemente**.
Gestartet um	Zeit, zu der der Auftrag gestartet wurde.
Endete um	Zeitpunkt, zu dem der Auftrag abgeschlossen wurde.
Auftragsdauer	Gesamtzeit, die für den Abschluss des Auftrags benötigt wurde.
Substatus	Substatus für den ausgewählten Status.
Notizen	Anzahl der Datensätze, die verarbeitet wurden.

4. Klicken Sie auf **Absenden**.

Hinweis:

- Um die Ausführung des Auftrags zu beenden, klicken Sie auf **Abbrechen**.
- Sie können nicht abgeglichene CIs nicht abgleichen oder CI-Suchregeln erneut anwenden, während Sie Hosts oder angreifbare Elemente importieren.

Wenden Sie die CI-Suchregeln erneut auf ausgewählte erkannte Elemente an

Wenden Sie die Suchregeln für das Configuration Item (CI) erneut auf ausgewählte erkannte Elemente aus den Auswahlaktionen der Listenansicht für erkannte Elemente an. Wenn sich das CI ändert, nachdem Sie die Regeln erneut angewendet haben, werden die erkannten Elemente mit dem neuen CI und den betroffenen Erkennungen aktualisiert. Angreifbare Elemente werden ebenfalls aktualisiert.

Vorbereitungen

Erforderliche Rolle: admin

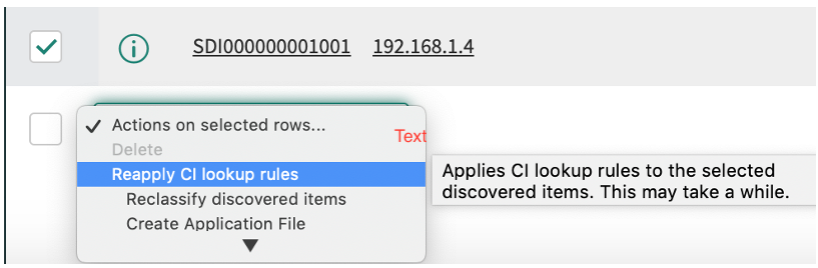
Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen finden Sie unter CI-Changes für erkannte Elemente.

Weitere Informationen zu den Konzepten des CI-Abgleichs und der CMDB, zur Suche erkannter Elemente, zur regelbasierten Identifizierung sowie weitere detaillierte Informationen zur Funktionsweise des CI-Abgleichs finden Sie im Artikel CI-Abgleich in Vulnerability Response [KB0998706] in der HI Knowledge Base.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Erkannte Elemente**.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und klicken Sie auf **Aktion für ausgewählte Zeilen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie in der Liste **CI-Suchregeln erneut anwenden aus**.

Hinweis:

Ab Vulnerability Response v24.0.6 können Sie die erneute Anwendung von CI-Suchregeln auf erkannte Elemente mit dem Substatus „CI außer Betrieb genommen“ überspringen, indem Sie die Systemeigenschaft *sn_sec_cmn.skipItemsWithCIDecommissioned*aktivieren.

Die Regeln werden erneut auf diese erkannten Elemente angewendet.

4. Klicken Sie in der Nachricht **auf Status anzeigen**.

Der Status wird im Hintergrundauftragsformular angezeigt.

Hinweis:

Im Feld **„Hinweise“** gibt das Attribut „Erkannte Elemente konnten aufgrund eines Ausnahmeattributs nicht verarbeitet werden“ mit einem Wert ungleich Null an, dass beim erneuten Anwenden einer CI-Suchregel ein Fehler oder eine Ausnahme aufgetreten ist. Weitere Details finden Sie in den Systemprotokollen.

Wenden Sie die Erweiterungen der CI-Suchregeln erneut an

Wenden Sie die Suchregeln für Configuration Item (CI) erneut auf ausgewählte erkannte Elemente wie Betriebssystem und NetBIOS an.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

- In Quelldaten vorhandene BS- und NetBIOS-Werte werden vor dem Konfigurationselement ausgefüllt, während diese Felder im erkannten Element ausgefüllt werden.
- Bei leeren Werten für Betriebssystem und NETBIOS in den Quelldaten werden die Werte aus dem Konfigurationselement übernommen, während diese Felder in der Tabelle für erkannte Elemente ausgefüllt werden.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Erkannte Elemente**.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und wählen Sie **Aktion für ausgewählte Zeilen**aus.
3. Wählen Sie in der Liste **CI-Suchregeln erneut anwenden aus**.

Die Regeln werden erneut auf diese erkannten Elemente angewendet.

Schritte zum Verhindern von doppelten oder verwaisten Datensätzen nach dem Ausführen von Vulnerability Response CI-Suchregeln

Ergreifen Sie Maßnahmen, um zu verhindern, dass doppelte oder verwaiste Datensätze durch den Abgleich von (Configuration Items (CI)) in CMDBentstehen.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die zum Iterieren und Abgleichen in der CMDB verwendete Logik kann zu langen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verarbeitungszeiten führen. Gründliches Testen und Debuggen von Verarbeitungsskripts in den Regeln trägt dazu bei, das Risiko von Problemen später im Prozess zu minimieren.

Doppelte oder verwaiste Datensätze verhindern

- Verwenden Sie kleine Teilmengen von Daten, die für die zu testende CI-Suchregel spezifisch sind.
  - Setzen Sie alle CI-Suchregeln, mit Ausnahme der gerade getesteten, auf inaktiv.
  - Analysieren Sie die importierten CIs, um sicherzustellen, dass sie das erwartete Verhalten aufweisen und die Übereinstimmung ordnungsgemäß erfolgt.
- Übereinstimmende CIs überprüfen
  - Überprüfen Sie die Anzahl der übereinstimmenden im Vergleich zu den nicht übereinstimmenden CIs. Stellen Sie sicher, dass der Prozentsatz akzeptabel ist. Sehen Sie sich nicht nur die erste Seite an, sie ist wahrscheinlich die erste, die eingefügt wird.
  - Suchen Sie manuell nach einigen CIs.
  - Überprüfen Sie, ob Benennungs- oder Feldprobleme vorliegen (z. B. Suche nach einer bestimmten Domäne).

    Wenn es angemessen erscheint, fügen Sie zusätzliche Übereinstimmungsregeln hinzu.
- Überprüfen Sie nicht abgeglichene CIs
  - Navigieren Sie zur Tabelle Nicht abgeglichene CIs.
  - Nach Klasse des Konfigurationselements gruppieren.
  - Überprüfen Sie alle Klassen, die nicht richtig aussehen (Zertifikate, Netzwerkkarten, Bilder).
    - Finden Sie heraus, warum sie nicht mit dem richtigen CI übereinstimmen?
    - Soll die Klasse ausgeschlossen werden?
    - Soll die Klasse zu einer zugehörigen Klasse hochgestuft werden?
- Überprüfen Sie CI-Status wie **Deaktiviert**.
- Entfernen Sie Testdaten
  - Sobald Sie beginnen, das richtige oder erwartete Verhalten beim CI-Abgleich zu beobachten, beginnen Sie von vorne.
  - Beginnen Sie erneut mit: Löschen der zum Testen verwendeten Daten: (siehe Abschnitt **„Daten aus Tabellen löschen** “)
    - Erkannte Elemente
    - Angreifbare Elemente
    - Korrekturaufgaben
  - Alle CI-Übereinstimmungsregeln werden manuell erneut ausgeführt.

Weitere Informationen zu CI-Suchregeln und Qualysfinden Sie im Artikel KB0750656 .

Weitere Informationen zu CI-Suchregeln und Rapid7finden Sie in KB0818096 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten werden aus Tabellen gelöscht

Manchmal haben Sie Daten importiert und stellen fest, dass etwas nicht stimmt. Wenn in einer Entwicklungs- oder Leistungsumgebung etwas nicht stimmt, können Sie aus einer besseren Umgebung erneut klonen. Dies ist jedoch nicht immer eine Option.

Hinweis:
Das Ausführen dieser Aktionen erfordert das Fachwissen ServiceNow.

Es gibt vier Optionen zum Löschen von Daten aus Tabellen:

- **Alle Datensätze löschen** in **der Tabellenkonfiguration**verwendet.
- Konfigurieren Sie die **Tabellenbereinigung**, indem Sie zu **Automatisch Leerungen** (sys_auto_flush.list) navigieren und einen neuen Datensatz **für die automatische Leerung** erstellen.
- Kürzen Sie gs.truncateTable mit einem Hintergrundskript.

  Wenn Sie `truncateTable` verwenden, müssen Sie das Kontrollkästchen „Datensatz für Rollback“ in den Hintergrundskripts deaktivieren. Andernfalls wird eine Kopie der Tabelle und zugehöriger kaskadierender Tabellen erstellt, was zu lange dauert und höchstwahrscheinlich fehlschlägt.

  Hinweis:
  Verwenden Sie `truncateTable` niemals in einer Produktionsumgebung. Wenden Sie sich an Ihren Support-Mitarbeiter, bevor Sie große Löschungen in Produktionsumgebungen oder gemeinsam genutzten Umgebungen ausführen.

Vorhandene Konfigurationselemente werden dedupliziert

Immer wenn Configuration Items (CIs) durch eine Deduplizierungsaufgabe aktualisiert werden, werden auch die erkannten Elemente (DIs) aktualisiert, die sich auf diese CIs beziehen. Die angreifbaren Elemente (VIs) und Erkennungen werden ebenfalls mit dem CI aktualisiert.

Weitere Informationen finden Sie unter CI-Changes für erkannte Elemente.

Zugehörige Informationen

Deduplizierungsaufgaben nachbessern

Lösen Sie Korrekturaufgaben

Die in Vulnerability Response enthaltene Flexibilität ermöglicht es Ihnen, Schwachstellen auf die Weise zu beheben, die für Ihre Sicherheitsorganisation geeignet ist.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sobald Sie benachrichtigt werden, dass eine Change-Anforderung gelöst wurde, ändern Sie den Status der Korrekturaufgabe in Gelöst, und warten Sie auf den nächsten Scan. Erneute Scans werden automatisch durch den im Setup-Assistenten konfigurierten Importzeitplan einer Drittpartei ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn die Statussynchronisierung aktiviert ist, werden Korrekturaufgaben automatisch in den Status Gelöst verschoben, nachdem eine Change-Anforderung, die einer Korrekturaufgabe (VUL) zugeordnet ist und sich im Status Überprüfen befindet, implementiert wird. Weitere Informationen finden Sie unter Change Management für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Mir zugewiesen**.
2. Klicken Sie auf einen Datensatz, der sich im Status Öffnen befindet.

   Der Status „Offen“ gibt an, dass der Datensatz noch nicht bearbeitet wurde. Im Formular wird Folgendes angezeigt:
   - Informationen zur Korrekturaufgabe
   - Gruppenkonfigurationsdetails
   - Notizen
   - Zugehörige angreifbare Elemente
   - Aufgaben-SLAs
   - Change-Anforderungen
3. Führen Sie Ihre Analyse für die Gruppe durch.
4. Wenn Sie bereit sind, mit der Arbeit am Datensatz zu beginnen, wählen Sie eine der folgenden Optionen aus.

Option	Bezeichnung
Wenn das angreifbare Element ein Risiko für Ihre IT-Umgebung darstellt, erstellen Sie einen CHG-Datensatz, und eskalieren Sie das Problem an das Change-Management- Team.	Weisen Sie die Gruppe der entsprechenden Gruppe oder Person zu, und klicken Sie auf **Change erstellen**.
Wenn das angreifbare Element ein potenzielles Sicherheitsrisiko für Ihre Organisation darstellt, erstellen Sie einen Datensatz für den Security Incident, und eskalieren Sie das Problem an das Team Security Incident Response.	Klicken Sie auf **Security Incident erstellen**. Diese Schaltfläche wird nur angezeigt, wenn Security Incident Response aktiviert ist. Es wird eine Berechnung der Geschäftsauswirkung angewendet, der Incident zugewiesen und der Security Incident erstellt.

   Nachdem Sie eine Change-Anforderung erstellt haben, wird der entsprechende Datensatz in der zugehörigen Liste **„Change-Anforderungen“** im Formular „Schwachstellengruppe“ angezeigt.
5. Wenn Sie feststellen, dass das Problem ein geringes Risiko aufweist und zurückgestellt werden kann, klicken Sie auf **Ausnahme anfordern**.
   Weitere Informationen zum Zurückstellen einer Korrekturaufgabe finden Sie unter Korrekturaufgabe zurückstellen.
6. Wenn Sie feststellen, dass das Problem ohne weitere Analyse sofort geschlossen werden kann, klicken Sie auf **Schließen**.
   Weitere Informationen zum Schließen einer Korrekturaufgabe finden Sie unter Schließen Sie eine Korrekturaufgabe. Ab v23.0 von Vulnerability Responsewurde die Schaltfläche **Schließen** für Korrekturaufgaben entfernt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine regelmäßige Aufgabe für die Integration einer Drittpartei aktualisiert und scannt Datensätze automatisch in einem festgelegten Intervall. Die angreifbaren Elemente werden zum nächsten geplanten Datum und zur nächsten geplanten Uhrzeit gescannt. Alternativ können Sie einen Schwachstellen-Scan manuell über den zugehörigen Link **Nach Schwachstellen suchen** initiieren.

Wenn der Scan die Schwachstelle im Konfigurationselement erneut findet und nicht als Behoben markiert, wird das angreifbare Element in den Status „Wird untersucht“ zurückversetzt. Wenden Sie sich an die IT-Abteilung, um die Change-Anforderung erneut zu öffnen.

Wenn der Scan die Schwachstelle nicht findet und zurückgibt, dass das angreifbare Element als Behoben markiert wurde, geht das angreifbare Element in den Status Geschlossen – Behoben über und wird während des Imports geschlossen.

Nur wenn sich alle angreifbaren Elemente in einer Aufgabe im Status „Geschlossen – Behoben“ befinden, wird die Korrekturaufgabe automatisch geschlossen. Korrekturaufgaben mit angreifbaren Elementen in anderen geschlossenen Status als „Behoben“ müssen manuell geschlossen werden.

Korrekturaufgabe zurückstellen

Wenn Sie feststellen, dass das mit einer Korrekturaufgabe (VUL) verbundene Problem eine niedrige Priorität hat und ohne weitere Analyse sofort zurückgestellt werden kann, können Sie die Funktion **Ausnahme** anfordern verwenden.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Korrekturaufgabe aus einem Korrekturaufgabendatensatz in den Vulnerability Response Arbeitsbereichen zurückstellen. Nachdem Sie die Anforderung gesendet haben, wird sie zur Genehmigung gesendet. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Täglich wird eine regelmäßige Aufgabe ausgeführt, um nach zurückgestellten Korrekturaufgaben zu suchen, deren Datum für die Wiedereröffnung erreicht ist. An dem Tag, an dem die Zurückstellung der Aufgabe abläuft, wird die Aufgabe erneut geöffnet.

Hinweis:
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder aus einer Korrekturaufgabe entfernen kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben Korrekturaufgaben jedoch nicht automatisch aus den Status „Geschlossen“ oder „Zurückgestellt“.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie einen Datensatz.
3. Klicken Sie auf **Ausnahme anfordern**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bis	Wählen Sie das Datum aus, an dem der Status „Zurückstellen“ abläuft und die Korrekturaufgabe erneut aktiviert wird. Nachdem der Datensatz übermittelt wurde und E-Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Vulnerability Response eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird die Korrekturaufgabe auf **„Offen“** zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Falsch positiv ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Klicken Sie auf **Absenden**.
   Die Gruppe wird als In Überprüfung markiert. Der zugehörige Link **Erneut öffnen** wird angezeigt. Das Datum und der Grund der Wiedereröffnung werden in den Arbeitsnotizen unter der Registerkarte **Change-Genehmigungen** anzeigen angezeigt.

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe an

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor das Datum für „Zurückgestellt bis“ erreicht wird. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status „Zurückstellen“ abläuft und die Korrekturaufgabe erneut aktiviert wird.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Elemente übertragen, die Teil der Korrekturaufgabe sind. Die angreifbaren Elemente müssen sich jedoch im Status „Zurückgestellt“ befinden, und ihre aktuellen Bis-Daten müssen vor dem „Aktualisiert bis“-Datum liegen. Außerdem wird bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers eine E-Mail ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Korrekturaufgabe erneut verlängert wird, erhöht sich die Anzahl der Zurückstellungen verlängern im Back-End.

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das mit einer Korrekturaufgabe verbundene Problem ohne weitere Analyse sofort geschlossen werden kann, können Sie die Funktion **Schließen** verwenden. Ab v23.0 von Vulnerability Responsewurde die Schaltfläche **„Schließen“** für Korrekturaufgaben entfernt, und das Schließen einer Korrekturaufgabe wird vom Scanner gesteuert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

In den Vulnerability Response -Arbeitsbereichen durchläuft eine Korrekturaufgabe dieselben Status wie eine Korrekturaufgabe in früheren Versionen von Vulnerability Response. Wenn alle angreifbaren Elemente (VITs) in einer Korrekturaufgabe geschlossen wurden, geht die Korrekturaufgabe in den Status „Inaktiv“ über.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder aus einer Korrekturaufgabe entfernen kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben Korrekturaufgaben jedoch nicht automatisch aus den Status „Geschlossen “ oder „Zurückgestellt“.

Prozedur

1. Öffnen Sie den Datensatz, für den Sie eine Überprüfung anfordern möchten.
2. Wählen Sie die Schaltfläche **Schließen/Zurückstellen** aus.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Status	Wählen Sie einen Status aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ Zurückgestellt ○ Abgeschlossen
Bis	Nur im Popup-Fenster **„Zurückstellen** “ verfügbar. Wählen Sie das Datum aus, an dem der Status **„Zurückstellen** “ abläuft und die Korrekturaufgabe erneut aktiviert wird. Nachdem der Datensatz übermittelt wurde und E-Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Vulnerability Response eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird das angreifbare Element auf **„Offen“** zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet.
Grund	Geben Sie den Grund für das Schließen des Problems ein.
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

4. Wählen Sie **Absenden**.
   Die Korrekturaufgabe wird als **Geschlossen**markiert.

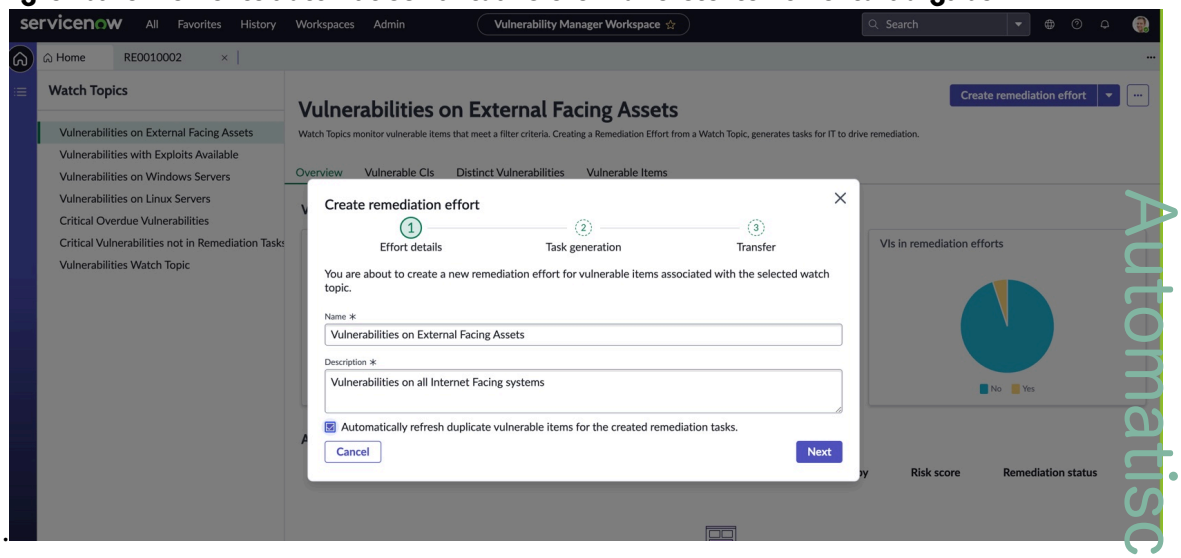
Doppelte angreifbare Elemente werden von mehreren Scannern identifiziert

Wenn Sie mehrere Scanner für dasselbe Asset verwenden, um Schwachstellen zu erkennen, können mehrere angreifbare Elemente (VIs) erstellt werden. Sie können diese doppelten VIs identifizieren, um sicherzustellen, dass den Korrekturbesitzern keine doppelten Schwachstellen zugewiesen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Lösung ist nur möglich, wenn dieselben Schwachstellen erkannt werden, z. B. dieselben Common Vulnerabilities and Exposures (CVE). Die Schwachstellenkombination hängt von den verwendeten Scannern ab. Qualys und Tenable haben beispielsweise jeweils eigene Schwachstellentypen, d. h. Einträge von Drittparteien (TPEs), und andere Scanner wie Microsoft Defender for Endpoint erkennen Schwachstellen basierend auf CVEs.

Ab v 17.1 können Sie beim Erstellen einer Korrekturmaßnahme doppelte angreifbare Elemente in den erstellten Korrekturaufgaben automatisch aktualisieren. Um die doppelten angreifbaren Elemente automatisch zu aktualisieren, müssen Sie die Option **Doppelte angreifbare Elemente automatisch aktualisieren für erstellte Korrekturaufgaben** auswählen.



Doppelte VIs anzeigen: Identifizieren Sie doppelte angreifbare Elemente, die von mehreren Scannern im System gemeldet wurden. Sie können das duplizierte VI als Gelöst markieren. Weitere Informationen finden Sie unter Doppelte Schwachstellen automatisch beheben. Doppelte Einträge werden nur angezeigt, wenn die Kombination von Schwachstellen mithilfe von CVEs erstellt wird. Weitere Informationen finden Sie unter Vulnerability Response-Korrekturaufgabe und Status angreifbarer Elemente.

Potenzielle Duplikate werden für die folgenden Schwachstellen-Kombinationen identifiziert:

Scanner-Kombination	Typ der Schwachstelle
Scanner 1 und Scanner 2	CVE
Scanner 1 und Scanner 2	CVE und TPE

Doppelte Schwachstellen automatisch beheben

Ab Vulnerability Response (VR) v17.1 können Sie doppelte Schwachstellen in einem Asset automatisch beheben.

Wenn ein Asset mit mehreren Scannern gescannt wird, besteht die Möglichkeit, dass die verschiedenen Scanner dieselbe Schwachstelle als Duplikate identifizieren. Wenn beispielsweise die Scanner von Qualys und Microsoft dieselbe Schwachstelle identifizieren, können Sie festlegen, dass das Duplikat automatisch behoben wird.

Beispielszenario

VR erstellt einen Datensatz, VI1, für Schwachstelle 1 vom Microsoft Defender für Endpunkt-Scanner. Ein zweiter Datensatz, VI2, wird vom Qualys-Scanner für dieselbe Schwachstelle erstellt. Das Nachbesserungsteam wendet die Patches an, die möglicherweise die VI1- und VI2-Datensätze beheben. Wenn Sie den Qualys-Scanzeitplan

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

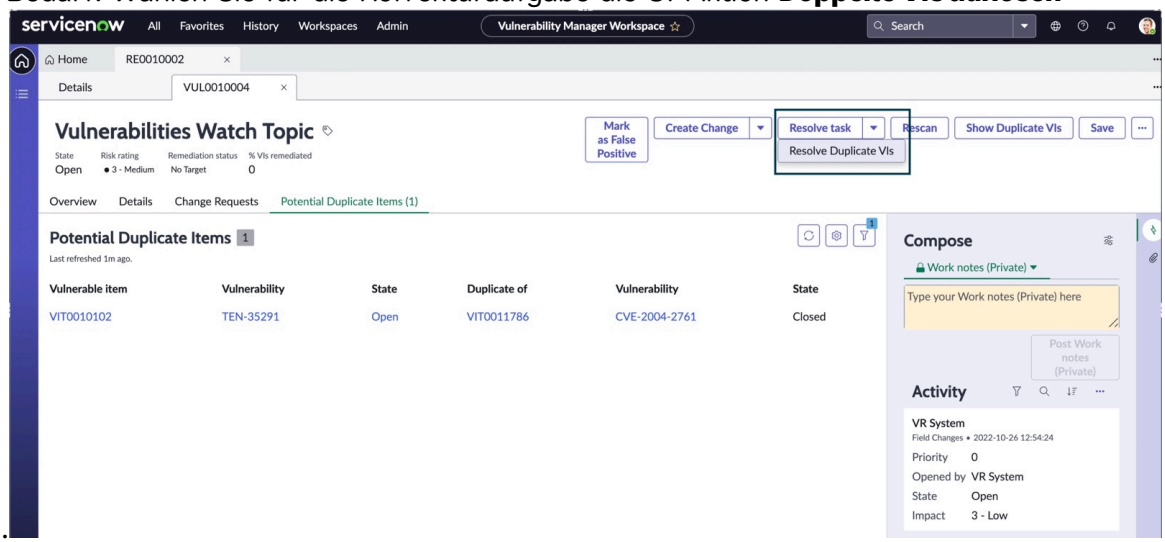
über einen Tag hinaus konfigurieren, liefert Microsoft Defender zu diesem Zeitpunkt die behobenen Schwachstelleninformationen, und VR schließt den VI1-Datensatz als Geschlossen/Behoben.

In diesem Szenario befindet sich der VI2-Datensatz noch im Status „Offen“, und VR wartet auf die Qualys-Scan-Ergebnisse. In dieser Situation verbleiben AE-Datensätze vom zweiten Scanner im Status „Offen“, auch wenn der Patch angewendet wird und das AE vom anderen Scanner als behoben bestätigt wird.

Um diese Situation zu beheben, können Sie den doppelten Schwachstellen-Datensatz basierend auf der Bedingung beheben, dass die Schwachstelle vom ersten Scanner geschlossen wird.

Gehen Sie wie folgt vor, um Schwachstellen zu beheben:

- Bei Bedarf: Wählen Sie für die Korrekturaufgabe die UI-Aktion **Doppelte VIs auflösen** aus.



- Automatisiert: Aktivieren Sie die Systemeigenschaft `sn_vul.auto_resolve_duplicate_vit`, um doppelte angreifbare Elemente automatisch aufzulösen. Die tägliche geplante Aufgabe „Doppelte VITs in Korrekturaufgabe aktualisieren und beheben“ aktualisiert die doppelten Elemente automatisch.

Die doppelten AEs werden dann als gelöst markiert.

Hinweis:
Der Datensatz des gelösten Schwachstellenelements wird erneut geöffnet, wenn der Scanner es als **Nicht behoben**identifiziert.

Erstellen und bearbeiten Sie eine Klassifizierungsgruppe

Erstellen Sie Gruppen, damit die zugrunde liegenden Regeln dieser Gruppe die Tabellendatensätze basierend auf den Bedingungen klassifizieren können. Die Regeln können verwendet werden, um jedes Feld in der entsprechenden Tabelle auszuwählen.

Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

Prozedur

1. Navigieren Sie zur Tabelle Systemeigenschaften.
2. Fügen Sie in der Systemeigenschaft `sn_sec_cmn.classificationTables` den Namen der Tabelle hinzu, für die Sie die Klassifizierungsgruppe erstellen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie eine neue Geschäftsregel, indem Sie der Geschäftsregel in der in der Gruppe definierten Tabelle das folgende Codefragment hinzufügen:
```
var KlassifizierungCalc = Neu
sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_group','sn_vul_classification_rule');
KlassifizierungCalc.calculate();
```

Hinweis:
Geschäftsregeln werden bereitgestellt, um die Klassifizierung während der Erfassung für die Tabellen „Erkannte Elemente“ und „Schwachstelleneintrag“ auszuführen. Damit andere Tabellen über die Klassifizierungsregeln bei der Erfassung verfügen, müssen Sie die Geschäftsregeln hinzufügen.

4. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Klassifizierungsregeln**.
5. Klicken Sie im Kontextmenü Klassifizierungsgruppen auf **Neu**.
6. Füllen Sie die Felder des Formulars aus.

Formular „Schwachstellenklassifizierungsgruppe“.

Feld	Beschreibung
Name	Name der neuen Klassifizierungsgruppe.
Aktiv	Option zum Aktivieren der Gruppe.
Beschreibung	Beschreibung der neuen Klassifikationsgruppe.
Tabelle	Tabelle, auf deren Grundlage die Regeln ausgeführt werden. **Hinweis:** Das Vulnerability Response-Basissystem enthält Klassifizierungsgruppen für erkannte Elemente und Schwachstellen.

Erstellen und bearbeiten Sie eine Klassifizierungsregel

Erstellen Sie Regeln, um eingehende Schwachstellen automatisch den richtigen Teams zur Korrektur zu klassifizieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

Warum und wann dieser Vorgang ausgeführt wird
Wenn sie erstellt werden, klassifizieren diese Regeln die Schwachstellen als zu einer Plattform oder zu einer Anwendung gehörend. Sie können diese Regeln konfigurieren, um den Wert eines bestimmten Felds im Schwachstelleneintrag zu ersetzen.
Verwenden Sie diese Regeln, um die Berechnung vorgelagert in die Tabelle „Eintrag von Drittpartei-Schwachstellen“ zu verschieben, um die Wiederverwendung von Inhalten zu ermöglichen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Klassifizierungsregeln**.
2. Um eine Klassifizierungsgruppe anzuzeigen, klicken Sie auf diese Gruppe.
3. Klicken Sie im Kontextmenü Klassifizierungsregeln auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die Felder des Formulars aus.

Formular „Klassifizierungsregel für Schwachstellen“.

Feld	Beschreibung
Name	Name der neuen Klassifizierungsregel.
Aktiv	Option zum Aktivieren der Regel.
Beschreibung	Beschreibung der neuen Klassifizierungsregel.
Ausführungsreihenfolge	Reihenfolge, in der die Regel ausgeführt werden soll.
Erweiterte Ansicht	Option zum Anzeigen zusätzlicher Felder in den Abschnitten mit Registerkarten.
Wenn diese Bedingung erfüllt ist	
Bedingungstyp	Typ der Bedingung für die Regel. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Filter**: Grundlegende Filterbedingungen, um zu bestimmen, ob die Regel verwendet werden soll oder nicht. ○ **Filtergruppe**: Satz von mehreren Bedingungen, die zusammen verwendet werden. Die Regel wird basierend auf den in der Filtergruppe definierten Bedingungen ausgewertet. ○ **Skript**: Geskriptete Bedingung, mit der bestimmt wird, wann diese Regel angewendet werden soll. Dieses Feld wird nur angezeigt, wenn die Option **Erweiterte Ansicht** ausgewählt ist.
Bedingung	Bedingung für die Regel. Definieren Sie Bedingungen basierend auf der Spalte, die in der erforderlichen Spalte des Schwachstelleneintrags ausgewählt ist. Sie können mehrere Bedingungen hinzufügen, um die Regel zu verfeinern. Dieses Feld wird nur angezeigt, wenn **Filter** im Feld **Bedingungstyp** ausgewählt wird. **Hinweis:** Wenn Sie mehrere Bedingungen oder Vorlagen definieren, können Sie nur aus einer übergeordneten und einer untergeordneten Tabelle auswählen. Sie können nicht aus zwei oder mehr untergeordneten Tabellen auswählen.
Filtergruppe	Gruppe von Filtern. Die Gruppe wird definiert, wenn ein Satz von Bedingungen wiederholt an mehreren Stellen verwendet wird. Klicken Sie mithilfe des Listensymbols ( ) auf die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Suche, um die Filtergruppe auszuwählen. Weitere Informationen finden Sie unter Filtergruppen in Security Operations erstellen und definieren. Dieses Feld wird nur angezeigt, wenn im Feld **Bedingungstyp** die **Option Filtergruppe** ausgewählt wird.
Skript	Skript, das ausgewertet wird, um zu bestimmen, wann diese Regel angewendet werden soll. Sie können Ihren Code schreiben und die Antwort entweder auf „true“ oder „false“ festlegen. Dieses Feld wird nur angezeigt, wenn im Feld **Bedingungstypdie Option Skript** ausgewählt wird
Diese Werte festlegen	
Klassifizierung	Klassifizierung der Regel. Um eine Option auszuwählen, klicken Sie auf das Glühbirnensymbol ( ). In der Liste werden die Optionen für Plattform und Anwendung angezeigt. Alternativ können Sie eine eigene Klassifizierung eingeben, die nicht in der Liste enthalten ist.
Klassifizierungstyp	Typ der Klassifizierung. Dieses Feld zeigt die gefilterte Liste der Klassifizierungstypen basierend auf dem Wert, den Sie für das Feld **Klassifizierung** ausgewählt haben.
Werttyp	Typ des Werts, der mithilfe dieser Regel zugewiesen wird. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Vorlage**: Wählen Sie eine Vorlage. Sie können eine erforderliche Vorlage verwenden. ○ **Skript**: Wählen Sie ein bereits vorhandenes Skript aus, oder schreiben Sie ein eigenes anwenderdefiniertes Skript. Dieses Feld wird nur angezeigt, wenn die Option **Erweiterte Ansicht** ausgewählt ist.
Vorlage	Andere Bedingung für die Regel neben den Feldern **Klassifizierung** und **Klassifizierungstyp**. Wählen Sie eine Kombination aus Feldern und Werten aus, die festgelegt werden sollen, wenn die Regel ausgewertet wird. Dieses Feld wird nur angezeigt, wenn im Feld **Werttyp** die **Option Vorlage** ausgewählt wird.
Skriptwert	Skript zum Festlegen von Werten für den aktuellen Datensatz. Dieses Feld definiert, welche Werte für die Felder in Schwachstelleneinträgen festgelegt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden. Dieses Feld wird nur angezeigt, wenn im Feld **Werttypdie Option Skript** ausgewählt wird.

5. Um die neue Regel zu erstellen, klicken Sie auf **Absenden**.

Example:
Verwenden Sie VR-Klassifizierungsregeln, um die Logik zu vorgelagerten Tabellen wie „Schwachstelle“ und „Erkannte Elemente“ hinzuzufügen und zu berechnen. Sie können die Ausgabe mehrmals wiederverwenden und dadurch die Leistung von Regeln wie Zuweisungsregeln verbessern. Klassifizieren Sie beispielsweise den Drittpartei-Eintrag (TPE) als Java, und verwenden Sie die Ausgabe mehrmals in Zuweisungsregeln. Beispiel für eine Zuweisungsregel:

```
VI.TPE.Classfication Type
        | IS | Java
```

Wenden Sie eine Regel auf eine vorhandene Schwachstelle an

Wenn Sie eine Klassifizierungsregel ändern, führen Sie alle aktiven Regeln für alle Schwachstelleneinträge erneut aus. Sie können die vorhandenen Schwachstellen auch nachbessern, indem Sie die neu erstellten Klassifizierungsregeln auf die vorhandenen Schwachstellen anwenden.

Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Klassifizierungsregeln für Schwachstellen**.
2. Um eine Regel auszuwählen, aktivieren Sie das Kontrollkästchen neben der Regel.
3. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
4. Klicken Sie auf **Erneut anwenden**.

Deaktivieren oder löschen Sie eine Klassifizierungsregel

Deaktivieren oder löschen Sie eine Klassifizierungsregel, wenn sie nicht mehr benötigt oder relevant wird.

Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

Warum und wann dieser Vorgang ausgeführt wird
Wenn eine Klassifizierungsregel deaktiviert oder gelöscht wird, verbleiben die Daten, die in den Feldern **Klassifizierung** und **Klassifizierungstyp** durch diese gelöschte Regel gefüllt wurden, in den jeweiligen Tabellen.

Wenn Sie diese Daten löschen möchten, erstellen Sie eine Regel mit leeren Werten in den Feldern **„Klassifizierung“** und **„Klassifizierungstyp“,** und wenden Sie die Gruppe erneut an. Sobald diese neue Regel erneut angewendet wird, werden die Änderungen in allen Datensätzen angezeigt, für die diese Regel gilt, basierend auf den Bedingungen der Regel.

Ab v24.0.6 von Vulnerability Responsewird eine gelöschte oder deaktivierte Klassifizierungsregel nicht mehr auf das erkannte Element oder den Schwachstelleneintrag

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angewendet, und die Daten in den Feldern **Klassifizierung** und **Klassifizierungstyp** werden gelöscht.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Klassifizierungsregeln für Schwachstellen**.
2. Um die zu löschende Regel auszuwählen, klicken Sie auf das Kontrollkästchen neben der Regel.
3. Um die Regel zu löschen, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Liste Aktion für ausgewählte Zeilen **auf Löschen**.
   - Wählen Sie die Regel aus, und klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.

Hinweis:
Wenn Sie nicht auf diese Schaltfläche klicken, ist die Regel weiterhin im System vorhanden. Schwachstellen, auf die von der Regel verwiesen wird, verweisen weiterhin auf sie.

Erstellen Sie eine Ausschlussregel

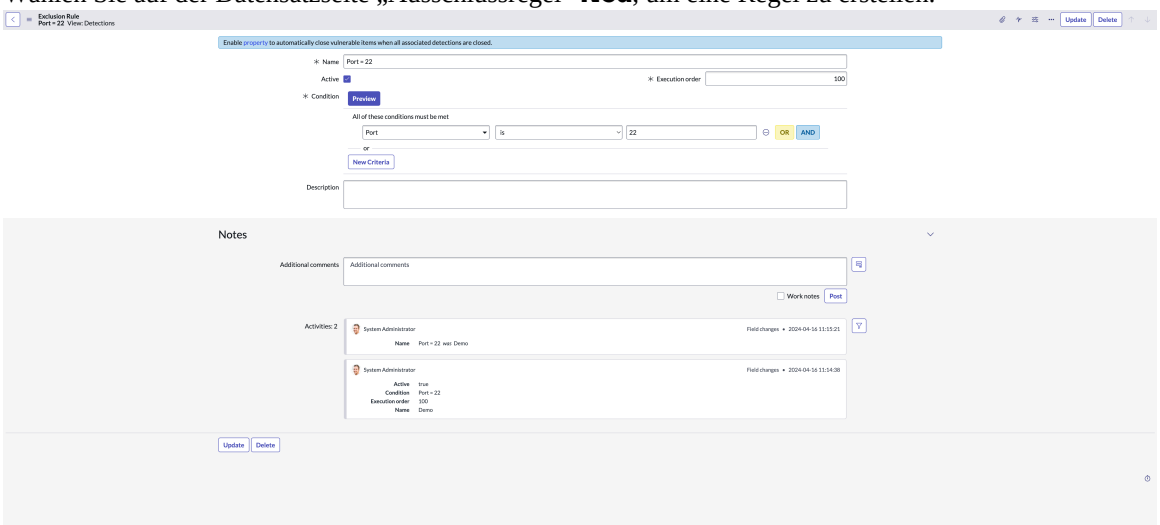
Erstellen Sie eine Regel, um Erkennungen während der Erfassung von der Konvertierung in angreifbare Elemente (VITs) auszuschließen.

Vorbereitungen
Erforderliche Rolle: Schwachstellen-Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Ausschlussregeln**.
2. Wählen Sie auf der Datensatzseite „Ausschlussregel“ **Neu**, um eine Regel zu erstellen.



Die Meldung „Eigenschaft zum automatischen Schließen angreifbarer Elemente aktivieren, wenn alle zugeordneten Erkennungen geschlossen werden“ wird angezeigt. Standardmäßig ist diese Eigenschaft deaktiviert. Wählen Sie zum Aktivieren den Eigenschaftslink aus, und geben Sie im Feld **Wert** den Wert Wahr ein.

3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausschlussregel“.

Feld	Beschreibung
Name	Name der Ausschlussregel.
Aktiv	Option zum Aktivieren der Ausschlussregel.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausschlussregel.
Bedingung	Filterbedingungen für die Erkennungen, die bei der Verarbeitung definiert werden können. **Hinweis:** Sie können keine Bedingungen für das Feld „Ausschlussregel“ oder „Angreifbares Element“ auswählen.
Beschreibung	Beschreibung der Ausschlussregel.

4. Wählen Sie **Absenden**.
   Die Aktivität wird im System aufgezeichnet.

Hinweis:
Sobald eine Ausschlussregel erstellt wurde, wird sie für Erkennungen ab der nachfolgenden Erfassung wirksam.

Change-Management Aufgaben für Vulnerability Response

Erstellen Sie aus Korrekturaufgaben (RTs) Change-Anforderungen, ordnen Sie RTs zu vorhandenen Change-Anforderungen zu oder teilen Sie Korrekturaufgaben in neue Aufgaben mit Teilmengen von angreifbaren Elementen (VI) auf.

Erstellen und verwalten Sie Change-Anforderungen direkt aus einer Korrekturaufgabe, wenn ein manueller und kontrollierter Prozess jeglicher Art zum Ändern oder Entfernen unterstützter Konfigurationselemente (Configurations Items, CI) in Ihrer CMDB erforderlich ist. Wenn Sie Change-Anforderungen direkt aus einem Datensatz erstellen und verwalten, können Sie Schwachstellen schnell untersuchen und beheben.

Unter Change Management für Vulnerability Response finden Sie eine Übersicht über die Funktionsweise des Change-Managements mit der Anwendung Vulnerability Response und die Systemanforderungen.

In den folgenden Themen erfahren Sie, wie Sie Change-Anforderungen erstellen, Korrekturaufgaben vorhandenen Change-Anforderungen zuordnen und Korrekturaufgaben aufteilen. Unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben finden Sie Informationen dazu, wie Statusfelder in Change-Anforderungen (CHG) Korrekturaufgaben automatisch lösen.

Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe

Erstellen Sie als IT-Korrekturbesitzer eine Change-Anforderung (CHG) direkt aus einer Korrekturaufgabe (VUL) für alle angreifbaren Elemente in der Gruppe. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, einschließlich der bevorzugten Lösung, um Ihre Untersuchung auf Schwachstellen zu beschleunigen, die ein manuelles Eingreifen erfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Zum Erstellen einer Change-Anforderung: jeder Benutzer mit der Rolle „itil“. Die Rolle sn_vul.remediation_owner wird auch automatisch zugewiesen, wenn die Rolle itil einem Benutzer zugewiesen wird.

Erforderliche Rolle: Für die Genehmigung von Change-Anforderungen: Benutzer mit den Rollen itil, admin, sn_change_write, change_manager.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Erstellen einer Change-Anforderung in den Arbeitsbereichen Vulnerability Response finden Sie unter Erstellen Sie eine Change-Anforderung im IT Remediation Workspace.

Führen Sie die unten aufgeführten Schritte aus, um eine Change-Anforderung in der klassischen Umgebung zu erstellen.

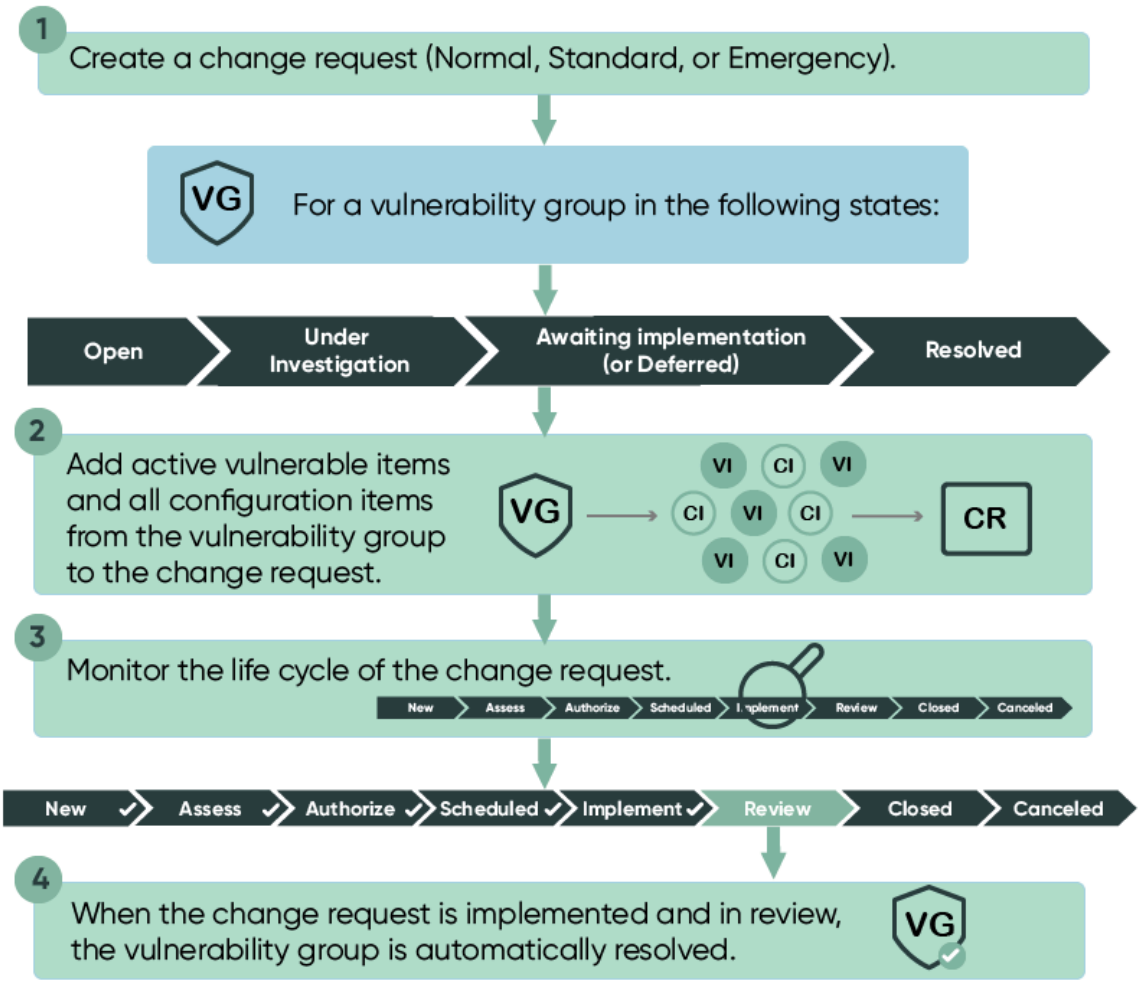
Sie können Change-Anforderungen direkt von einer Korrekturaufgabe aus erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

- Standard Ein zuvor autorisierter Change, der als risikoarm und relativ gängig gilt und anhand eines festgelegten Verfahrens oder einer festgelegten Arbeitsanweisung implementiert wird.
- Normal Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsebenen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall Ein Change zur Lösung eines schwerwiegenden Incident.

Die folgende Abbildung zeigt den Basis-Flow zum Erstellen einer Change-Anforderung aus einer VUL (Korrekturaufgabe). Die detaillierten Schritte für diesen Flow finden Sie in der Abbildung.

Der Datensatz für die Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben als Schwachstellengruppen (VG) bezeichnet. In den folgenden Abbildungen ist VG= Korrekturaufgabe oder VUL-Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Hinweis:
Wichtige Punkte zum Erstellen neuer Change-Anforderungen:

- Sie können neue Change-Anforderungen für jede Korrekturaufgabe (VUL) in einem anderen Status als Geschlossenerstellen.
- Stellen Sie sicher, dass Sie einen Genehmiger für andere Change-Anforderungen als Standard-Change-Anforderungen (vorab genehmigt) haben, die Sie erstellen oder einer VUL zuordnen. Dies beschleunigt das Verschieben der VUL bis zur Lösung. Weitere Informationen zum Hinzufügen von Benutzern finden Sie unter Fügen Sie der Vulnerability Response-Gruppe Benutzer hinzu.
- Bevor eine Korrekturaufgabe gelöst werden kann, müssen alle Aufgaben in mindestens einem CHG, das der VUL zugeordnet ist, abgeschlossen werden, damit die Change-Anforderung implementiert und in den Status „Überprüfung“ versetzt werden kann.

Prozedur

1. Um eine vollständige Change-Anforderung aus einem vorhandenen Korrekturaufgaben-Datensatz zu erstellen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.
   Die Liste der Korrekturaufgaben, die Ihrer Zuweisungsgruppe zugewiesen sind, wird angezeigt.
2. **Wahlweise:** Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturübersicht** um das Dashboard „Remediationsübersicht“ anzuzeigen und eine VUL zu suchen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Alternativ können Sie in der Spalte Nummer auf eine Korrekturaufgabe klicken, um den Datensatz zu öffnen und die Details anzuzeigen.
   Der Datensatz wird angezeigt.
4. Klicken Sie bei angezeigten VUL-Datensatz, für den Sie die Change-Anforderung erstellen möchten, oben rechts im Datensatz **auf Change erstellen**.
   Das Formular „Change-Anforderung erstellen“ wird angezeigt.
5. Füllen Sie die Felder aus.

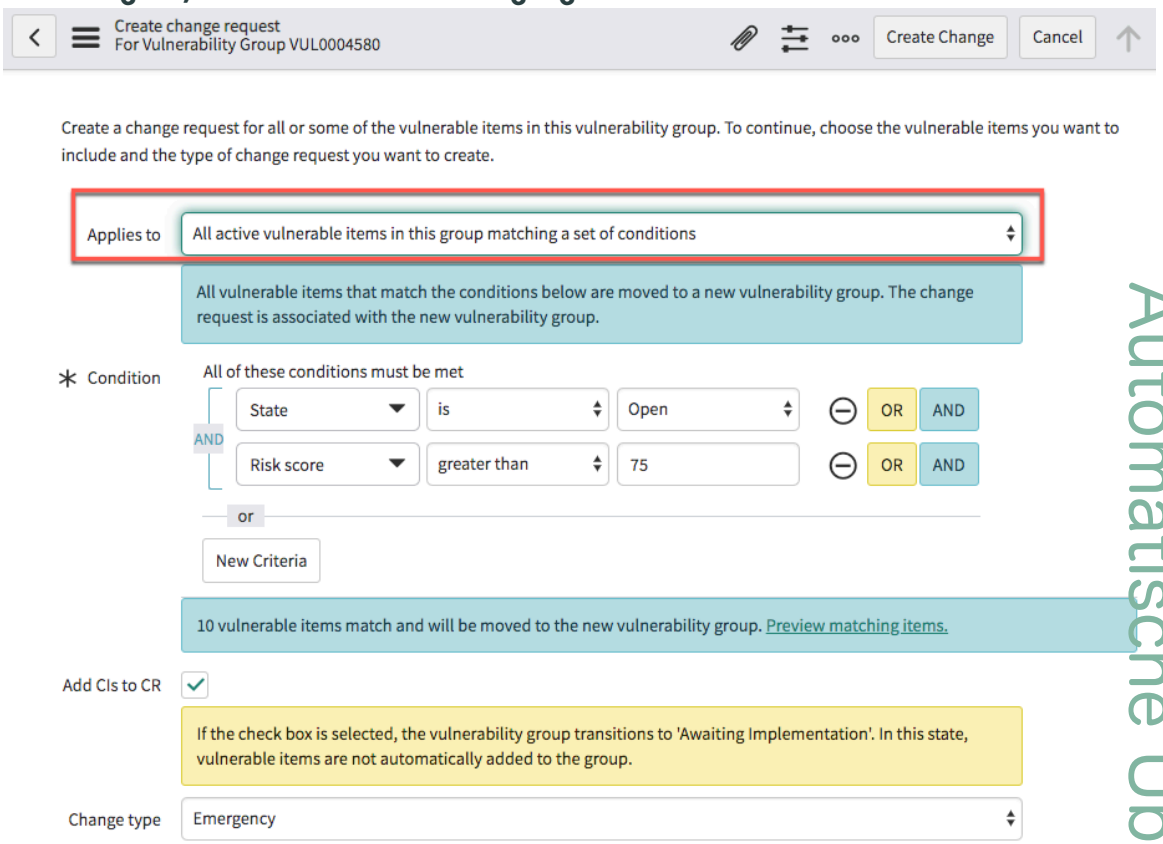
   a. Wählen Sie in der Auswahlliste des Felds Gilt für eines aus, um fortzufahren.

Option	Beschreibung
Alle aktiven angreifbaren Elemente in dieser Gruppe	Wenn diese Option ausgewählt ist, werden alle aktiven angreifbaren Elemente aus dieser Korrekturaufgabe mit einem anderen Status als „Geschlossen“ automatisch der Change-Anforderung hinzugefügt, nachdem Sie **auf Change erstellen**klicken.
Alle angreifbaren Elemente in dieser Gruppe, die eine Reihe von Bedingungen erfüllen	Wenn diese Option ausgewählt ist, wird der Bedingungsgenerator wie in der zweiten Abbildung unten angezeigt. Geben Sie Filterkriterien ein, um die angreifbaren Elemente zu identifizieren, die Sie für die neue Change-Anforderung verwenden möchten. Ein Beispiel für einen Filter könnte nur angreifbare Elemente enthalten, die bestimmten Suchkriterien entsprechen: **Status ist „Offen“** und **Risikopunktzahl größer als 75**. Nachdem Sie Ihre Bedingungen eingegeben haben, wird eine Nachricht mit der Anzahl der VIs angezeigt, die Ihren Kriterien entsprechen (10). Es wird ein Link (**Vorschau passende Elemente anzeigen**) zur Vorschau der übereinstimmenden Elemente angezeigt. Wenn keine Elemente Ihren Filterbedingungen entsprechen, wird unter dem Bedingungsgenerator eine Meldung angezeigt, in der Sie aufgefordert werden, den Filter anzupassen. Nachdem Sie auf **Change erstellen**geklickt haben, werden alle angreifbaren Elemente, die diesem Bedingungsfilter entsprechen, in eine neue Korrekturaufgabe verschoben. Diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Change-Anforderung ist mit der neuen Korrekturaufgabe verknüpft.

Erstellen Sie ein Change-Anforderungs-Formular für angreifbare Elemente in einer Aufgabe, die eine Reihe von Bedingungen erfüllen



b. Wahlweise: Wenn sie im Formular angezeigt wird, klicken Sie auf den Link **Vorschau passende Elemente anzeigen,** um eine Liste der VIs anzuzeigen, die Ihren Filterkriterien entsprechen.
Die Vorschau der Korrekturaufgabenliste wird angezeigt. Sie können Elemente in dieser Vorschauliste auswählen und UI-Aktionen dafür ausführen. Diese Aktionen werden jedoch auch für die VUL ausgeführt. Wenn Sie beispielsweise ein VI aus der Vorschauliste löschen, wird dieses VI auch aus der VUL gelöscht.

c. Schließen Sie nach Abschluss der Vorschau das Browserfenster, um zum Formular „Change-Anforderung“ zurückzukehren.

d. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen aus, um fortzufahren.

Option	Beschreibung
Das Kontrollkästchen CIs zu CR hinzufügen ist aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle Configuration Items (CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, zu dieser Change-Anforderung hinzugefügt. Die VUL wechselt automatisch in den Status Warten auf Implementierung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Das Kontrollkästchen „CIs zu CR hinzufügen“ ist deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass die CIs aus den aktiven angreifbaren Elementen aus dieser Korrekturaufgabe dem neuen Change Request hinzugefügt werden. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit der VUL synchronisiert, und die VUL verbleibt in ihrem aktuellen Status.

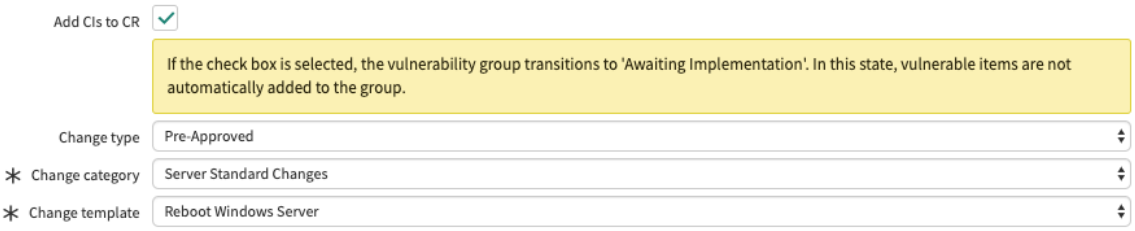
e. Wählen Sie aus der Auswahlliste für das Feld Change-Typ einen aus, um fortzufahren.

Änderungstyp	Beschreibung
Notfall	Ein Change zur Lösung eines schwerwiegenden Incident.
Normal	Ein Change-Typ, mit dem Changes an einem Service implementiert werden, bei denen es sich nicht um Standard- oder Notfall-Changes handelt.
Standard	Eine vorab autorisierte Change-Anforderung mit geringem Risiko, die häufig implementiert wird. Genehmigte Standard-Change-Anforderungen können in einem Vorlagenkatalog vordefiniert werden, um den Zugriff auf und die Anfrage eines Standard-Changes effizienter zu gestalten. Wenn diese Option ausgewählt ist, werden zwei Felder angezeigt (siehe folgende Abbildung). Wählen Sie in jeder Auswahlliste eines aus, um diese Felder auszufüllen: ▪ Change-Kategorie: Wählen Sie eine Kategorie für den Change aus Ihrem vorhandenen Katalog aus, z. B. Hardware, Server-Standard-Changes, Software. In diesem Beispiel ist Patchen von Standard-Changes ausgewählt. ▪ Change-Vorlage: Wählen Sie eine verfügbare Vorlage für Change-Anforderungen mit vordefinierten unterstützenden Aufgaben aus Ihrem Katalog aus. In diesem Beispiel wird die Vorlage „Microsoft Monatlicher Patchzyklus“ ausgewählt. Weitere Informationen zu Kategorien, Vorlagen und Change-Typen von ITSM-Change-Anforderungen finden Sie unter Change-Typen .

Die Funktion liest automatisch die Typen von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change Management eingerichtet haben. Wenn Sie beispielsweise

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Namen für Ihre Standard-Change-Anforderungen in ITSM von Standard in Vorgenehmigtändern, wird Ihr neuer Name automatisch in der Auswahlliste Change type (Change-Typ) unter Change Request erstellen (Change-Anforderung erstellen) angezeigt (siehe folgende Abbildung).



Die Felder im Abschnitt „Vorschau auf Change-Anforderung“ des Formulars sind bereits mit Informationen aus der VUL ausgefüllt. Bei Bedarf können diese Feldwerte bearbeitet werden. Überprüfen Sie beispielsweise die Werte in den Feldern in der folgenden Abbildung:

Geplantes Enddatum

Dieses Datum (10.10.2019) ist derselbe Wert, der im Feld Korrekturzieldatum der VUL angezeigt wird. Dieser Wert wird vom frühesten Korrekturzieldatum der angreifbaren Elemente abgeleitet, die zur VUL gehören. Wenn Sie eine Change-Anforderung für ein kritisches Problem erstellen, das ein früheres Korrekturdatum erfordert, können Sie diesen Wert und den Wert im Feld Priorität bearbeiten.

Begründung

Dieses Feld zeigt die Anzahl der CIs an, die dem CHG hinzugefügt wurden. Wenn Sie zusätzliche Informationen hinzufügen möchten, können Sie diesen Text bearbeiten. Beispielsweise können Sie in diesem Feld eine Notiz zu dem Filter hinzufügen, den Sie zum Erstellen der neuen VUL verwendet haben, z. B. Risikopunktzahl größer als 75. Dieser Text kann Ihnen helfen, Ihre neue Change-Anforderung und Korrekturaufgabe zu finden.

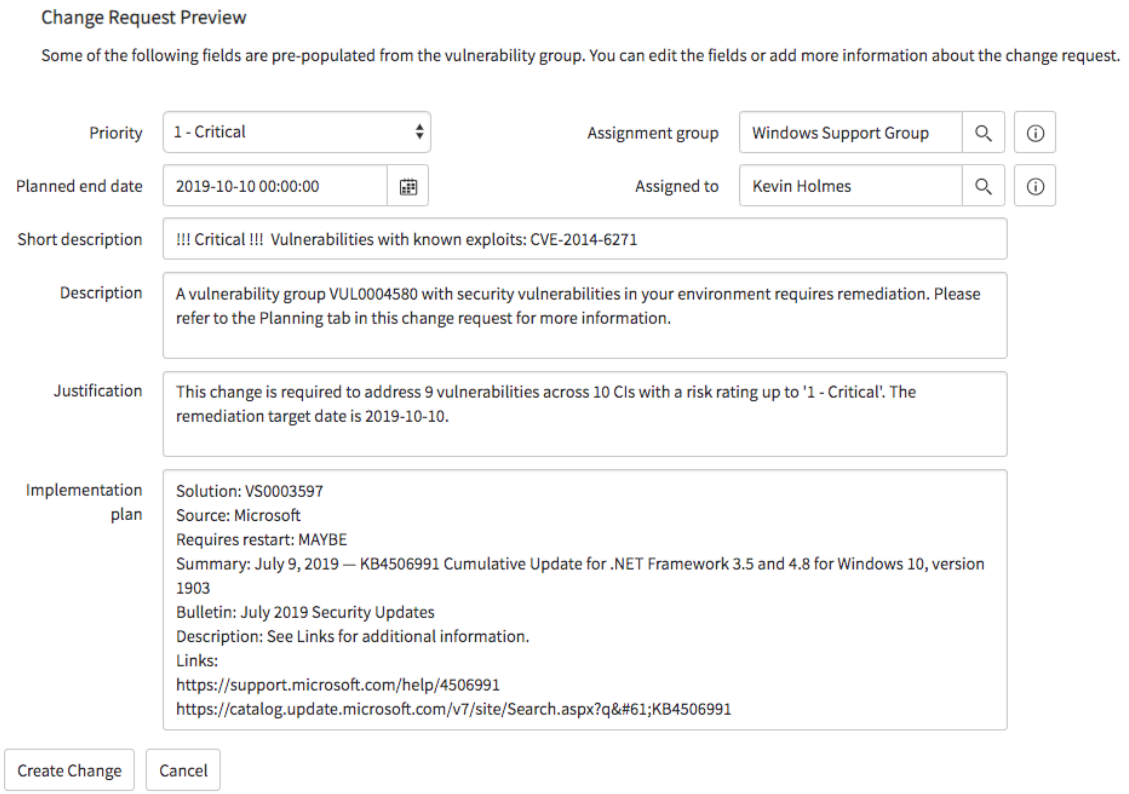
Implementierungsplan

In diesem Feld wird die bevorzugte Lösung für die Schwachstelle angezeigt.

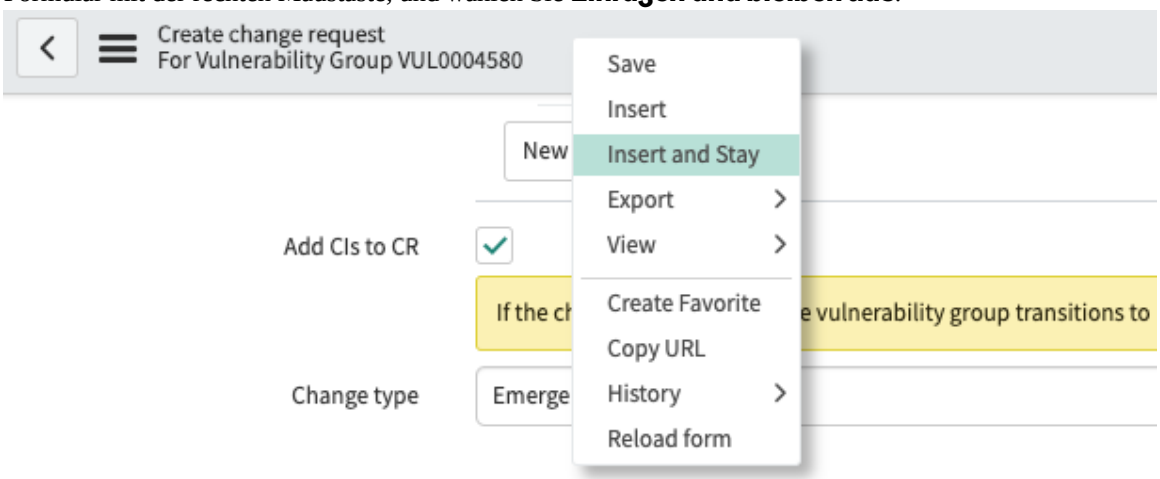
Zuweisungsgruppe und Zugewiesen an

Bearbeiten Sie diese Felder, um die Zuweisungsgruppe zu ändern, oder weisen Sie diese Change-Anforderung einem Anwender in einer Ihrer Zuweisungsgruppen neu zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



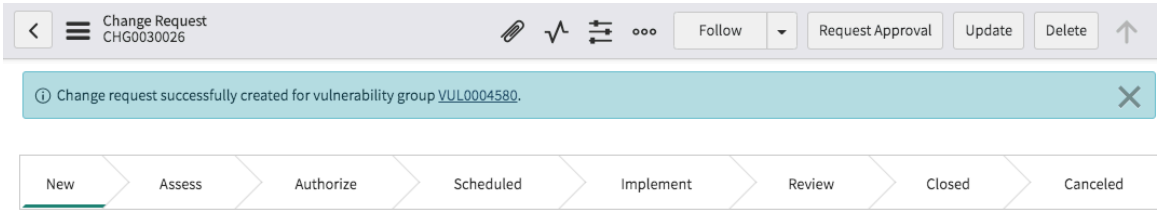
6. Zeigen Sie eine Vorschau an, und bearbeiten Sie die Felder nach Bedarf.
7. Um Ihre Änderungen zu speichern und auf dieser Seite zu bleiben, klicken Sie im grauen Banner oben im Formular mit der rechten Maustaste, und wählen Sie **Einfügen und bleiben aus**.



8. Nachdem Sie Ihre Änderungen abgeschlossen haben, wählen Sie eine aus, um fortzufahren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

Bei einer Korrekturaufgabe im Status Offen, bei der die Felder Zuweisungsgruppe und Zugewiesen an nicht zugewiesen sind (leer), wird der aktuell angemeldete Benutzer automatisch der Aufgabe zugewiesen, nachdem Sie auf **Change erstellen**geklickt haben. Außerdem muss das Kontrollkästchen CIs zu CR hinzufügen aktiviert sein. Oben in der VUL wird eine blaue Bestätigungsmeldung angezeigt, die auf diese Zuweisung hinweist.

Nächste Maßnahme

Überwachen Sie die Change-Anforderung und die Change-Aufgaben, um sicherzustellen, dass sie abgeschlossen und die Change-Anforderung implementiert wird. Nachdem dieses CHG implementiert und in den Status Überprüfen versetzt wurde und die Statussynchronisierung aktiviert ist, wird die VUL automatisch in den Status Gelöstverschoben. Weitere Informationen zur Statussynchronisierung finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Als IT-Korrekturbesitzer vermeiden Sie die Erstellung von doppelten Change-Anforderungen (CHG), während Sie an der Lösung Ihrer Korrekturaufgaben arbeiten, indem Sie eine Korrekturaufgabe (VUL) einer bereits in Ihrer -Instanz verfügbaren Change-Anforderung zuordnen.

Vorbereitungen

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: Jeder, der über die Rolle „itil“ verfügt. Die Rolle sn_vul.remediation_owner wird einem Benutzer automatisch zugewiesen, wenn die Rolle itil zugewiesen wird.

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung finden Sie unter Erstellen Sie eine Change-Anforderung im IT Remediation Workspace.

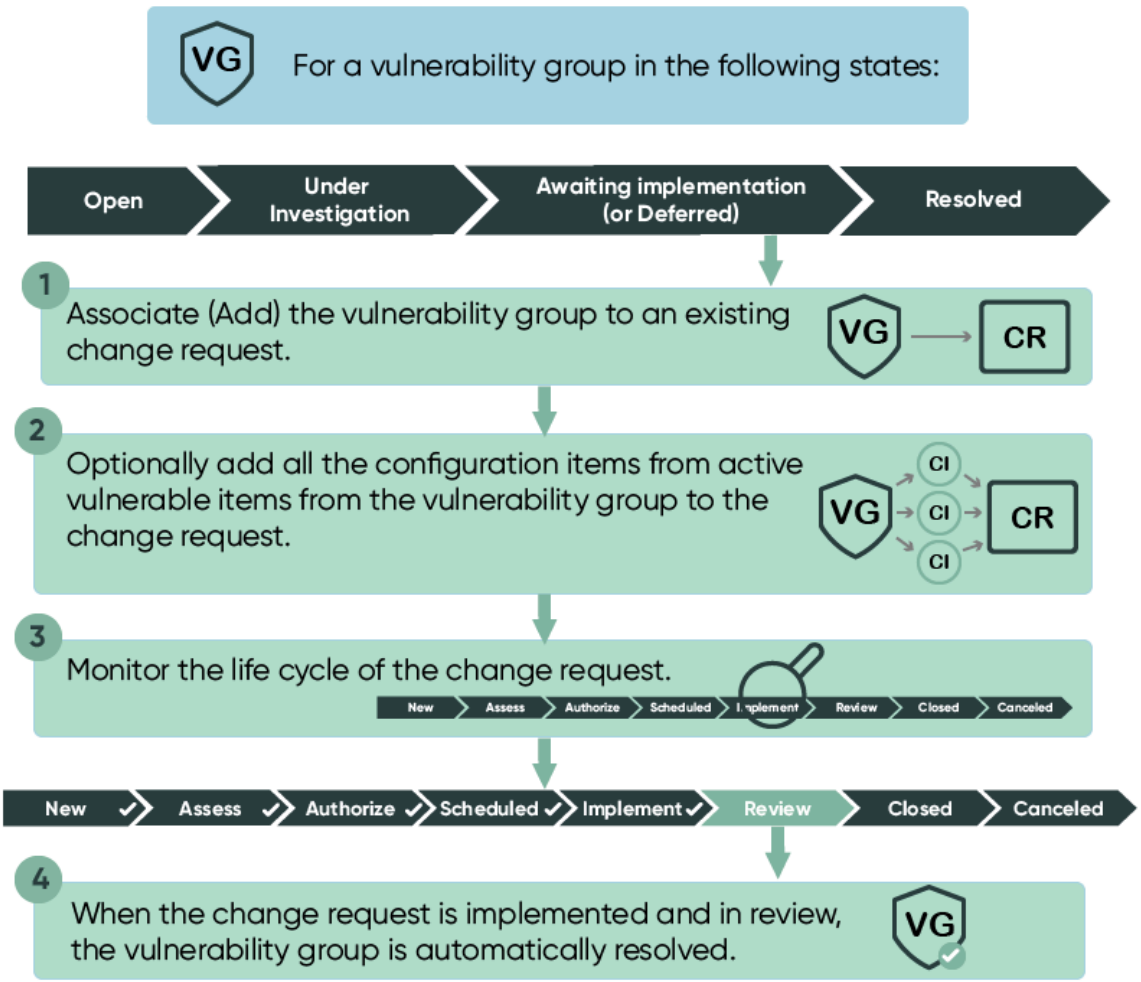
Der Datensatz für die Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben als Schwachstellengruppen (VG) bezeichnet. In den folgenden Abbildungen ist VG= Korrekturaufgabe oder VUL-Datensatz.

Weitere Informationen zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung finden Sie unter Erstellen Sie eine Change-Anforderung im IT Remediation Workspace.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Korrekturbesitzer können Sie Korrekturaufgaben, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, vorhandenen Change-Anforderungen direkt aus den Korrekturaufgaben-Datensätzen zuordnen. Die folgende Abbildung zeigt den Basis-Flow für die Zuordnung einer Change-Anforderung zu einer vorhandenen VUL (VG). Die detaillierten Schritte für diesen Flow finden Sie in der Abbildung.

Workflow zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung



Hinweis:
Sie können einer VUL in jedem Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „Geschlossen“ und „Zurückgestellt“) eine vorhandene Change-Anforderung zuordnen. Wenn Sie einer vorhandenen VUL einen Change Request zuordnen, werden dem Change Request nur die aktiven AEs hinzugefügt.

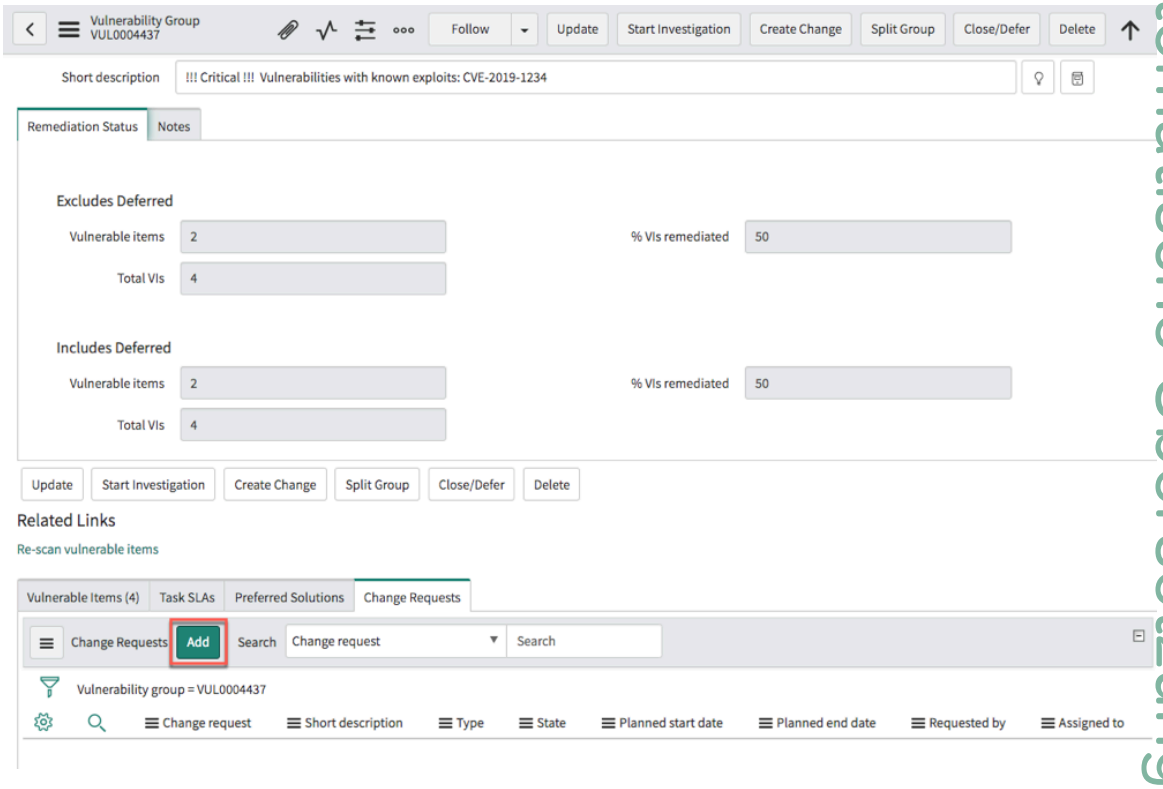
Bevor Sie beginnen, sollten Sie, um die Erstellung von doppelten Change-Anforderungen zu vermeiden, ggf. die vorhandenen Change-Anforderungen anzeigen, die bereits einer VUL zugeordnet sind. Um die Anzahl der Change-Anforderungen, die sich auf eine bestimmte VUL beziehen, einfach nachzuverfolgen, konsultieren Sie die Spalte CR-Anzahl in der Liste der Korrekturaufgaben. Falls nicht angezeigt, klicken Sie auf das Einstellungssymbol ( ) oben rechts. Verschieben Sie die Spalte CR-Anzahl von Verfügbar in Ausgewählt, und klicken Sie auf **OK**.

Um die neue Spalte automatisch auszufüllen, führen Sie für Kunden mit vorhandenen Daten in dieser Tabelle die geplante Aufgabe aus: Neue CR-Anzahlspalte ausfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

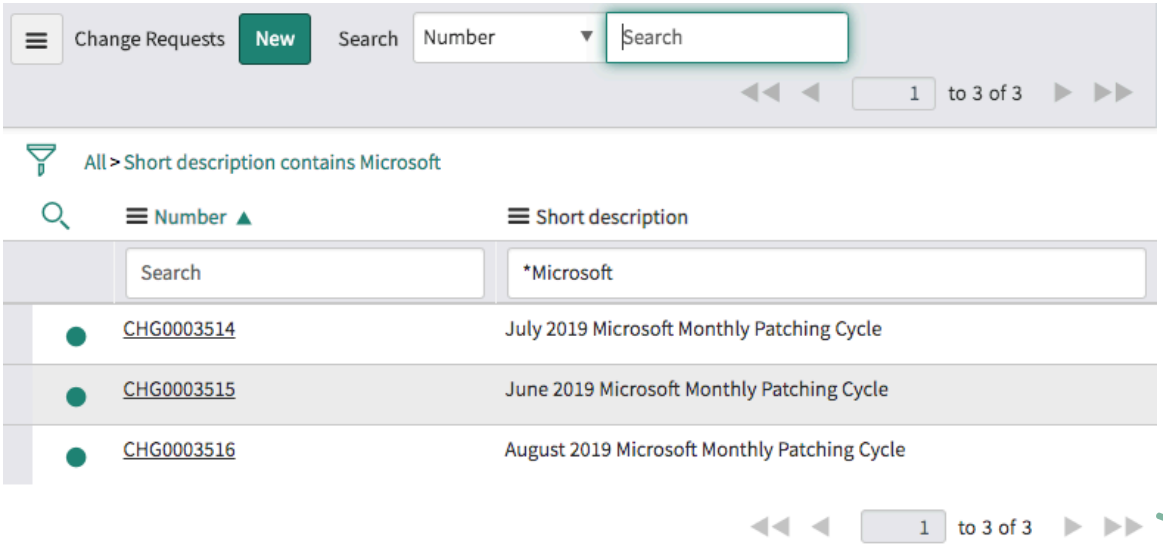
1. Um einer vorhandenen Change-Anforderung eine Korrekturaufgabe zuzuordnen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Suchen Sie die Korrekturaufgabe, mit der Sie arbeiten.
3. **Wahlweise:** Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturübersicht** um das Dashboard „Remediationsübersicht“ anzuzeigen und eine VUL zu suchen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen ist.
4. Klicken Sie in der Spalte Nummer auf einen VUL-Datensatz, um ihn zu öffnen.
   Der VUL-Datensatz wird angezeigt.
5. Scrollen Sie bei angezeigtem geöffneten Datensatz zur zugehörigen Liste Change-Anforderungen, und wählen Sie sie aus.
   Alle Change-Anforderungen, die der VUL zugeordnet sind, werden zusammen mit der Schaltfläche **Hinzufügen** angezeigt. In der folgenden Abbildung sind dieser VUL noch keine Change-Anforderungen zugeordnet.



6. Klicken Sie auf **Hinzufügen**, um die VUL einem vorhandenen CHG zuzuordnen.
   Das Formular „Vorhandene Change-Anforderung zu Korrekturaufgabe hinzufügen“ wird angezeigt.
7. Klicken Sie im Formular auf das Suchsymbol.
   In einem neuen Fenster wird eine Listenansicht der vorhandenen Change-Anforderungen angezeigt (siehe folgende Abbildung).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Wählen Sie ein Element aus der angezeigten Liste aus, oder klicken Sie alternativ auf den Filter ( ), und geben Sie Bedingungen ein, um Ihre Suchergebnisse einzuschränken.
9. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen aus, um fortzufahren.

Hinweis:
Diese Checkbox wird nur für vorhandene Change-Anforderungen im Status Neu angezeigt.

Option	Beschreibung
Das Kontrollkästchen CIs zu CR hinzufügen ist aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle Configuration Items (CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, zu dieser Change-Anforderung hinzugefügt. Wenn diese Option ausgewählt ist, wird der Status der Change-Anforderung mit der VUL synchronisiert. Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.
Das Kontrollkästchen „CIs zu CR hinzufügen“ ist deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass die CIs aus den aktiven angreifbaren Elementen aus dieser Korrekturaufgabe dem neuen Change Request hinzugefügt werden. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit der VUL synchronisiert, und die VUL verbleibt in ihrem aktuellen Status.

10. Klicken Sie im Feld Search for Change Request (Nach Change-Anforderung suchen) auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die VUL wird angezeigt. Oben im Datensatz wird eine blaue Bestätigungsmeldung angezeigt, die anzeigt, dass die ausgewählte Change-Anforderung erfolgreich der VUL zugeordnet wurde.

Hinweis:
Bei einer VUL im Status Offen mit nicht zugewiesenen Feldern Zuweisungsgruppe und Zugewiesen an (leer) wird der aktuell angemeldete Benutzer automatisch der VUL zugewiesen, nachdem Sie auf **Hinzufügen**geklickt haben. Außerdem muss das Kontrollkästchen CIs zu CR hinzufügen aktiviert sein. Oben in der VUL wird eine blaue Bestätigungsmeldung angezeigt, die anzeigt, dass der aktuelle Benutzer zugewiesen ist.

Nächste Maßnahme
Überprüfen Sie den VUL-Datensatz. Klicken Sie in der Spalte „Change-Anforderung“ in der zugehörigen Liste „Change-Anforderungen“ auf den Link für das neue CHG, um den CR-Datensatz anzuzeigen. Im geöffneten CHG-Datensatz können Sie den Status des Change Request überwachen. Die betroffenen Configuration Items (CI) und die Korrekturaufgaben werden in den zugehörigen Listen Betroffene CIs und Korrekturaufgaben angezeigt.

Teilen Sie eine Korrekturaufgabe auf

Identifizieren Sie als IT-Korrekturbesitzer aus einer vorhandenen Korrekturaufgabe (VUL) eine Teilmenge der angreifbaren Elemente (VI), die Sie in eine neue Gruppe verschieben möchten.

Vorbereitungen
Hinweis:

Anwendungsfälle für die Aufteilung von VIs aus vorhandenen VULs in neue Korrekturaufgaben können die folgenden Beispiele umfassen:

- Wenn Sie eine Change-Anforderung oder Change-Anforderungen für eine Aufgabe aufteilen möchten.
- Wenn Sie eine aufgeteilte Gruppe einem anderen Benutzer in Ihrer Zuweisungsgruppe neu zuweisen.
- Wenn Sie eine Zurückstellung oder eine Ausnahme für eine aufgeteilte Aufgabe anfordern, weil Sie wissen, dass einige Schwachstellen in bestimmten Configuration Items (CI) nicht innerhalb eines bestimmten Zeitrahmens behoben werden können.

Erforderliche Rolle: Jeder Benutzer mit der Rolle itil zum Aufteilen einer VUL.

Hinweis:
Die Rolle sn_vul.remediation_owner wird auch automatisch zugewiesen, wenn die Rolle itil einem Benutzer zugewiesen wird.

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zum Aufteilen von Korrekturaufgaben in den Arbeitsbereichen Vulnerability Response finden Sie unter Teilen Sie eine Korrekturaufgabe in in IT Remediation Workspace.

Dient zum Aufteilen einer Korrekturaufgabe in der klassischen Umgebung oder für Versionen von Vulnerability Response.

Sie können vorhandene Korrekturaufgaben mit mehr als einem angreifbaren Element aufteilen, das sich im Status Offen, Wird untersucht oder Warten auf Implementierung befindet. Durch das Erstellen einer neuen VUL mit angreifbaren Elementen, die bestimmten Kriterien entsprechen, können Sie mit einer bestimmten Gruppe von angreifbaren Elementen arbeiten, ohne die ursprüngliche Korrekturaufgabe zu beeinträchtigen.

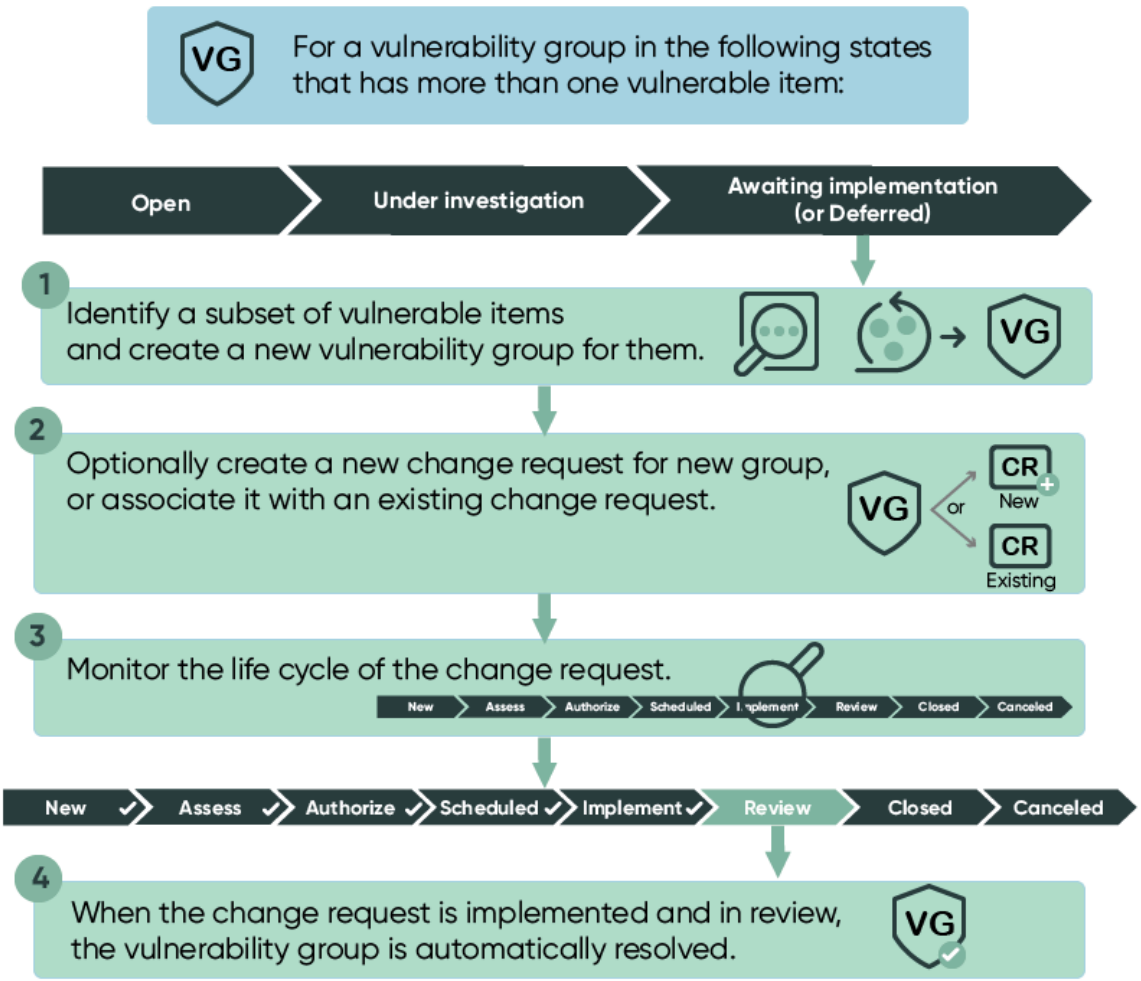
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Bedingungen für die angreifbaren Elemente angeben, die Sie mit dem Bedingungsgenerator in eine neue Korrekturaufgabe verschieben möchten, werden nur die aktiven VIs, die Ihren Kriterien entsprechen, in die neue Gruppe verschoben.

Sie müssen keine Change-Anforderungen (CHG) erstellen, wenn Sie eine VUL aufteilen. Sie können eine VUL gleichzeitig mit der Erstellung einer Change-Anforderung aufteilen oder eine VUL aufteilen, ohne eine Change-Anforderung zu erstellen. Die folgende Abbildung zeigt den Basis-Flow für die Aufteilung einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow finden Sie in der Abbildung.

Der Datensatz für die Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben als Schwachstellengruppen (VG) bezeichnet. In den folgenden Abbildungen ist VG= Korrekturaufgabe oder VUL-Datensatz.

Workflow zum Aufteilen einer Korrekturaufgabe

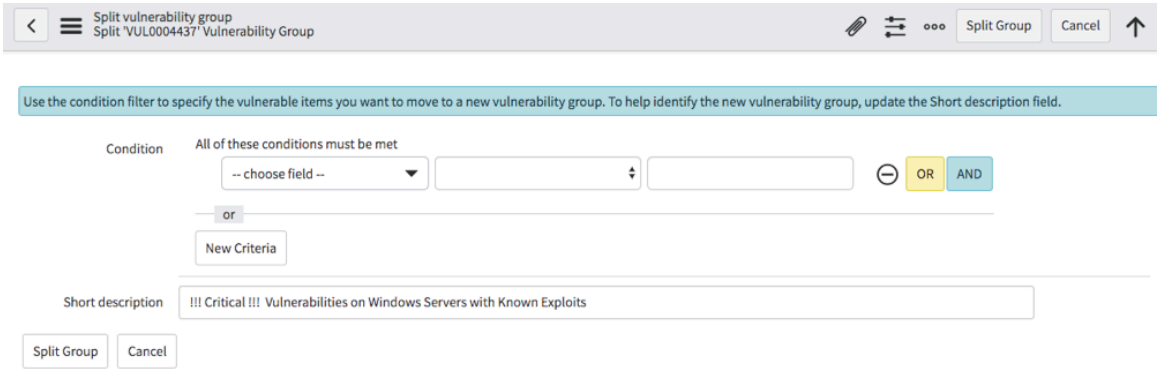


Automatische Übersetzung

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.
   Die Liste der Korrekturaufgaben wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf einen Datensatz, um ihn zu öffnen.
   Der Datensatz wird angezeigt.
3. Klicken Sie oben rechts in der VUL **auf Aufgabe aufteilen**.
   Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

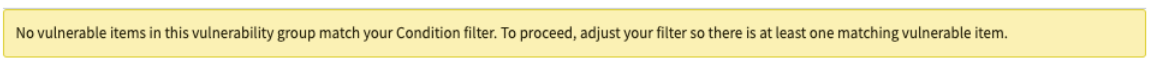


4. Geben Sie bei angezeigtem Bedingungsfilter die Bedingungen für die angreifbaren Elemente an, die Sie in eine neue Aufgabe verschieben möchten.
   Beispielsweise können Sie nur angreifbare Elemente herausfiltern, die den folgenden Bedingungen entsprechen:
   - Status „In Offen “.
   - Risikopunktzahlen größer als 80.
   - Configuration Items, die „WINSV“ enthalten.
   - Standort: San Diego.

   Für Bedingungen können Sie beispielsweise Folgendes eingeben:
   - Status – ist – Offen
   - Risikopunktzahl – ist größer als oder gleich – 80
   - Konfigurationselement. Name – enthält – WINSV
   - Konfigurationselement. Standort – ist – San Diego

   Wenn angreifbare Elemente nach Eingabe der Bedingungen Ihrem Filter entsprechen, wird eine Nachricht mit der Anzahl der übereinstimmenden angreifbaren Elemente angezeigt.

   Hinweis:
   Wenn eine Meldung angezeigt wird, dass keine angreifbaren Elemente Ihrem Filter entsprechen, passen Sie die Bedingungen so an, dass mindestens ein angreifbares Element Ihren Filterkriterien entspricht.

5. **Wahlweise:** Passen Sie den Filter nach Bedarf an.
6. **Wahlweise:** Damit Sie die neue VUL nach ihrer Erstellung leichter identifizieren können, aktualisieren Sie möglicherweise das Feld Kurzbeschreibung.
   Wenn bearbeitet, verwenden Sie das Kurzbeschreibungsfeld als Suchkriterium für die neue VUL, um sie nach der Erstellung leichter zu finden, z. B.LOCATED IN SAN DIEGO.
7. **Wahlweise:** Um eine Vorschau der Details zu den angreifbaren Elementen anzuzeigen, die Ihren Filterkriterien entsprechen, führen Sie die folgenden Schritte aus, bevor Sie auf **Aufgabe aufteilen** klicken, um die neue VUL zu erstellen.
   Diese Details umfassen vorhandene Change-Anforderungen, die bereits dieser Teilmenge zugeordnet sind, und VULs mit diesen angreifbaren Elementen. Wenn Sie diese Informationen in der Vorschau anzeigen, können Sie möglicherweise keine doppelten VULs erstellen.

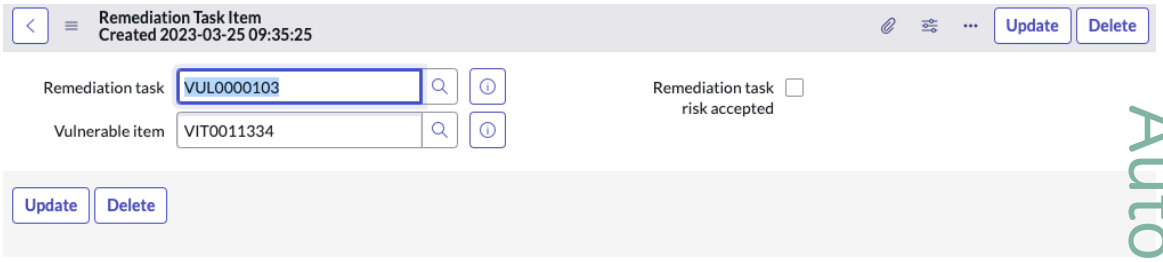
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der blauen Bestätigungsmeldung im Formular „Korrekturaufgabe aufteilen **“ auf Vorschau passende Elemente**.
Die Liste „Element der Korrekturaufgabe“ wird in einem neuen Fenster in Ihrem Browser mit einer Liste angreifbarer Elemente angezeigt, die Ihren Bedingungen entsprechen.

b. Klicken Sie in der Spalte Nummer auf ein Element, um den Datensatz zu öffnen.

c. Klicken Sie im angezeigten Datensatz rechts neben den Feldern „Schwachstellengruppe“ oder „Angreifbares Element“ auf das Informationssymbol für das angreifbare Element, um die Datensätze anzuzeigen.



d. Klicken Sie im angezeigten Dialogfeld **auf Datensatz öffnen**.
Informationen zum Zieldatum der Korrektur werden angezeigt. Klicken Sie im Abschnitt „Zugehörige Listen“ auf eine zugehörige Liste, um weitere Informationen zum AE anzuzeigen.

8. Wenn Sie bereit sind, die neue VUL mit den VIs zu erstellen, die Ihren Bedingungen entsprechen, schließen Sie das Vorschaufenster, um zum Formular „Aufgabe teilen“ im anderen Fenster zurückzukehren, und klicken Sie oben im Formular **auf Aufgabe teilen**.

Hinweis:

Bei weniger als 200 AEs wird der Teilungsvorgang synchron durchgeführt.

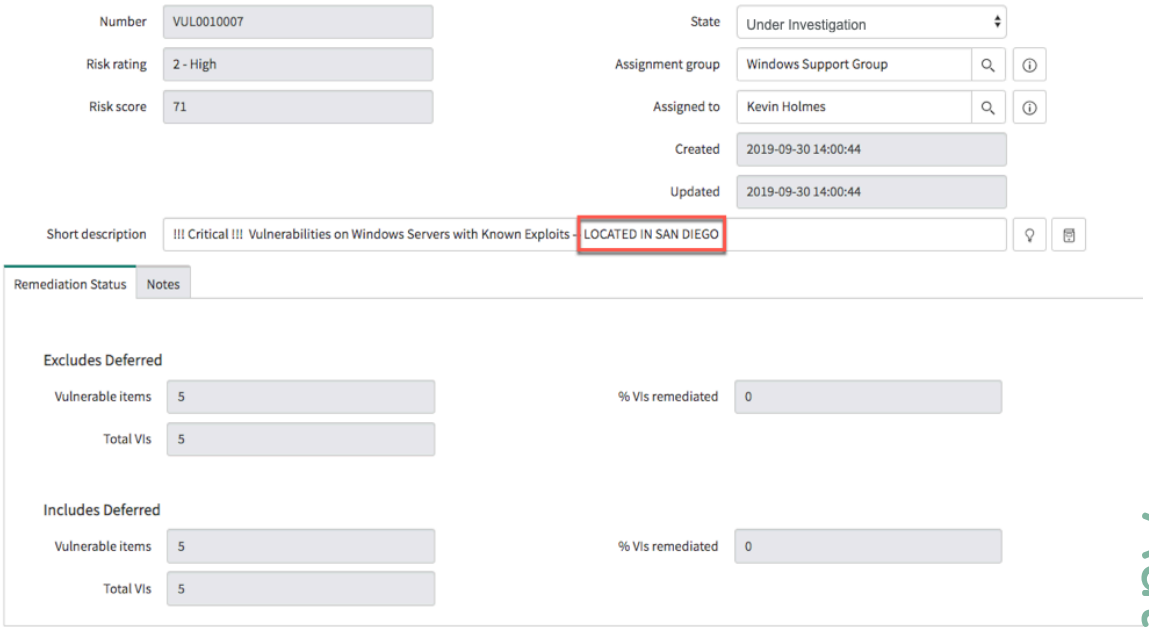
Bei über 200 VIs wird der Aufteilungsvorgang asynchron im Hintergrund durchgeführt, und es kann einige Sekunden dauern, bis die VIs in der neuen Gruppe angezeigt werden.

Es wird eine Bestätigungsmeldung angezeigt, die alle aktiven AEs anzeigt, die in die neue Gruppe verschoben wurden. Die Nummer der neuen Korrekturaufgabe wird ebenfalls angezeigt. Wenn er sich nicht bereits im Status „Wird untersucht“ befindet, wird der VUL zu „Wird untersucht“ verschoben. Überprüfen Sie das Feld Kurzbeschreibung auf den Text, den Sie für die neue VUL in (SORTIMENT IN SAN DIEGO) eingegeben haben.

Rollup-Berechnungen für die neue Gruppe werden durchgeführt, um die neue Risikopunktzahl, das Korrekturzieldatum und andere Feldwerte zu berechnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die angreifbaren Elemente, bevorzugten Lösungen und Change-Anforderungen werden in den zugehörigen Listen unten im Datensatz angezeigt. Verarbeiten und überwachen Sie diese neue Aufgabe wie jede Korrekturaufgabe.

9. **Wahlweise:** Scrollen Sie zur zugehörigen Liste **„Notizen“**, und klicken Sie darauf, um sie auszuwählen. Bestätigen Sie, dass die Anzahl der angreifbaren Elemente aus der ursprünglichen Korrekturaufgabe in die neue Gruppe im Aktivitätenstrom verschoben wurde.
10. **Wahlweise:** Um auf der neuen VUL die VIs aus der zugehörigen Liste „Angreifbare Elemente“ erneut auszuwählen und aufzuteilen, scrollen Sie zum Ende des Korrekturaufgaben-Datensatzes und wählen Sie in der Spalte Angreifbares Element der zugehörigen Liste „Angreifbare Elemente“ die zu verschiebenden VIs aus Wählen Sie in der Auswahlliste Aktionen für ausgewählte Zeilen die **Option Aufgabe aufteilen**aus. Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.
11. Um die Gruppe erneut aufzuteilen und die ausgewählten Elemente in eine neue Gruppe zu verschieben, klicken Sie auf **Aufgabe aufteilen**.
    Die ausgewählten VIs werden in eine andere Korrekturaufgabe verschoben, die Bestätigungsmeldung wird angezeigt, und die neue Gruppe wird angezeigt.
12. Wählen Sie eine aus, um die Untersuchung oder Korrektur fortzusetzen.

Nächste Maßnahme

Überwachen Sie den Status einer neuen VUL, um ihre Lösung zu beschleunigen.

Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

Es besteht eine synchronisierte Beziehung zwischen den Statusfeldern von Korrekturaufgaben (VULs) und den Statusfeldern von Change-Anforderungen (CHG) im Produkt Vulnerability Response. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie automatisch auch den Status aller zugehörigen Korrekturaufgaben.

Statussynchronisierung

Der Datensatz für die Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

als Schwachstellengruppen (VG) bezeichnet. In den folgenden Abbildungen ist VG= Korrekturaufgabe oder VUL-Datensatz.

Die Statussynchronisierung wird standardmäßig in Ihrer -Instanz durch eine Systemeigenschaft (sn_vul.cr_state_synch) aktiviert, wenn Sie die Anwendung Vulnerability Response herunterladen.

Wenn die Statussynchronisierung aktiviert ist, ändert das Feld CHG Status das Feld Status der Korrekturaufgabe in den folgenden Fällen automatisch:

- Wenn ein neues CHG für eine Korrekturaufgabe (VUL) erstellt wird und sich nicht im Status „Warten auf Implementierung“befindet, wird der VUL-Status in „Warten auf Implementierung“geändert.
- Wenn ein vorhandenes CHG einer VUL zugeordnet ist und sich nicht im Status „Warten auf Implementierung“befindet, wird der VUL-Status in „Warten auf Implementierung“verschoben.
- Nachdem die Aufgaben in einem CHG abgeschlossen wurden (Implementiert) und das CHG in den Status Überprüfen versetzt wird, wird die VUL in den Status Gelöstverschoben.

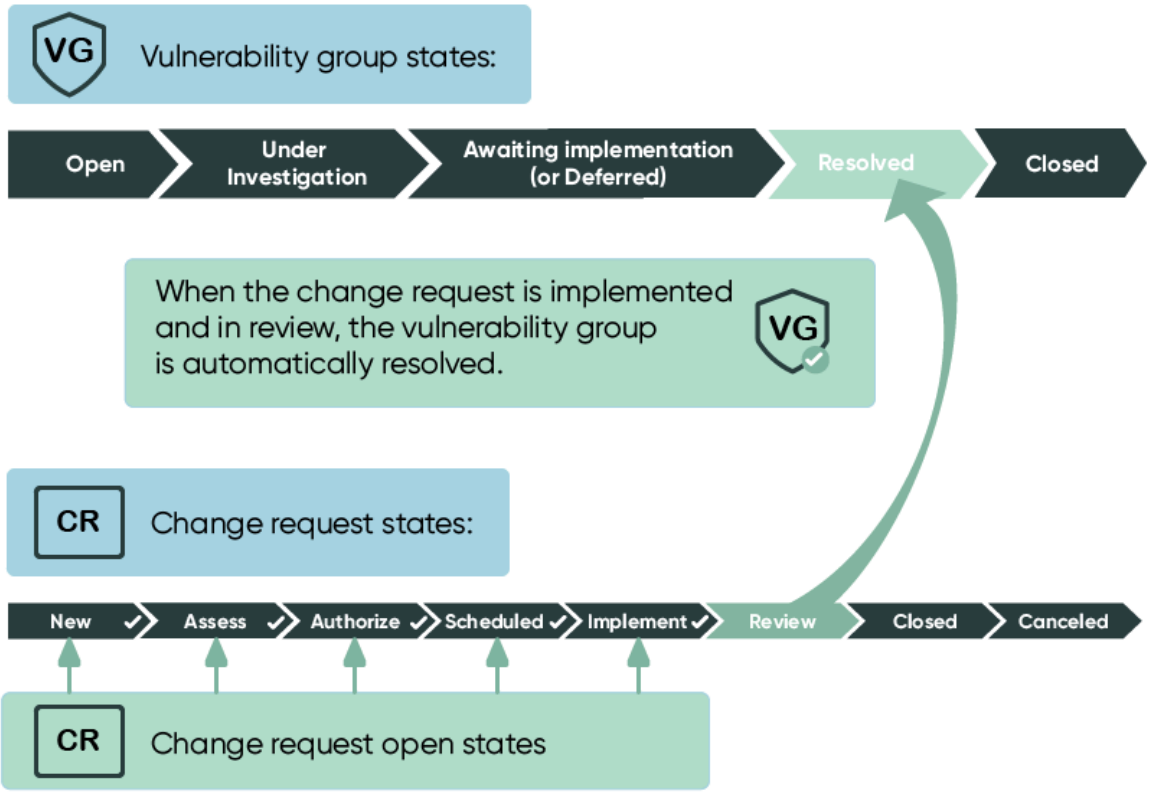
Weitere Informationen und Beispiele zur Statussynchronisierung finden Sie in den folgenden Abschnitten.

Hinweis:
Sie können CHGs und VULs weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist. Wenn das System jedoch registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder aus einem VUL entfernen, Status Die Synchronisierung kann Ihren manuellen Eingriff möglicherweise überschreiben. Die Status von Change-Anforderungen verschieben die VUL jedoch nicht automatisch aus den Status „Geschlossen“ oder „Zurückgestellt“.

Statussynchronisierung weiterleiten

Die folgende Abbildung zeigt, wie CHG-Status VUL-Status in einem Lebenszyklus automatisch verschieben, also von Offen zu Gelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können neue Change-Anforderungen für jede Korrekturaufgabe in einem anderen Status als Geschlossenerstellen. Die Statussynchronisierung verschiebt die VUL automatisch bidirektional durch die Status Offen, Wird untersucht, Warten auf Implementierungund Gelöst. Diese Verschiebung basiert auf bestimmten Werten des Statusfelds im Change Request. Die Statussynchronisierung zwischen Change-Anforderung und Korrekturaufgabe wird automatisch aktiviert, es sei denn, das Kontrollkästchen (CIs zu CR hinzufügen) wird in einem Formular angezeigt und Sie deaktivieren das Kontrollkästchen.

Die VUL wird nicht nach „Gelöst“ verschoben, wenn sich ein CHG im Status „Offen“ befindet. Alle CHGs in den Status vor der Überprüfung in ihrem Lebenszyklus, z. B. Neu, Bewerten, Autorisieren, Geplant oder Implementieren, wie in der vorherigen Abbildung gezeigt, gelten als offene Status für die CHG. Offene Status verschieben das Statusfeld in der VUL nicht, da Untersuchungen oder Aufgaben im CHG nicht abgeschlossen sind. Die Statussynchronisierung wird aufgerufen, wenn ein CHG für die VUL erstellt oder ihr zugeordnet wird oder wenn sich der Status einer vorhandenen Beziehung für das CHG ändert. Die abgeschlossenen CHG-Status sind „Überprüfung“ und „Erfolgreich geschlossen“. Wenn ein CHG erfolgreich geschlossen wird, lauten seine Geschlossencodes: Erfolgreichoder Erfolgreich mit Problemen. In diesem Fall wird die VUL in den Status Gelöstversetzt.

Rückwärts gerichtete Statussynchronisierung

Da ein CHG während seines Lebenszyklus verarbeitet wird, kann es irgendwann abgebrochen werden. Wenn CHG in diesem Fall Abgebrochenoder Geschlossen ist (mit dem Abschlusscode Nicht erfolgreich), wird die VUL automatisch zurück in den Status „Wird untersucht“verschoben. Die VUL wird zurück in den Status „Wird untersucht“verschoben, da kein aktiver Plan zur Nachbesserung der Schwachstelle vorhanden ist.

Wenn sich eine VUL im Status „Gelöst“ befindet und Sie eine neue CHG erstellen oder sie einer vorhandenen CHG in einem der anfänglichen offenen Status zuordnen, wechselt die VUL automatisch zurück in den Status „Warten auf Implementierung“. Die VUL wird in diesen Status zurückversetzt, da dem CHG jetzt mehr Arbeit zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VULs mit mehr als einem CHG

Wenn einer VUL mit dem Status „ Warten auf Implementierung“ mehr als ein CHG zugeordnet ist, basiert die Statussynchronisierung auf dem Status des CHG im frühesten Status seines Lebenszyklus. Beispielsweise sind einer VUL vier CHGs zugeordnet, CHG1, CHG2, CHG3 und CHG4, wie in der folgenden Tabelle gezeigt.

CHG-Nummer	CHG-Status
1	Implementieren
2	Abgebrochen
3	Geschlossen (Lösungscode von „Nicht erfolgreich“)
4	Geschlossen (Lösungscode erfolgreich)

Die Statussynchronisierung zwischen CHG und VUL basiert in diesem Fall auf CHG1, dem frühesten Status der vier CHGs (Implementieren). In diesem Fall verbleibt die VUL im Status Warten auf Implementierung.

In einem anderen Beispiel: Wenn sich eine VUL im Status „Gelöst“ befindet und über ein vorhandenes CHG verfügt, das implementiert wurde und sich im Status „Überprüfung“ befindet, und ein neues CHG erstellt wird, wird die VUL von „Gelöst“ zurück zu „Warten auf Implementierung“verschoben. Die Statussynchronisierung basiert auf dem CHG im Status „Neu“, dem CHG im frühesten Status.

CHG-Nummer	CHG-Status
1	Prüfung
2	Neu

Wenn VULs mehr als ein CHG aufweisen, wechselt der Status des VUL außerdem in den folgenden Fällen automatisch:

- Wenn ein CHG zur Überprüfungwechselt und alle anderen der VUL zugeordneten CHGs sich im Status „Überprüfung“ oder „Geschlossen“ befinden (mit einem erfolgreichen Abschlusscode), wechselt die VUL automatisch in den Status „Gelöst“. Alle anderen zugehörigen CHGs, die abgebrochen oder nicht erfolgreich geschlossen wurden, werden ignoriert.
- Wenn ein CHG in den Status „Abgebrochen“ oder„Geschlossen“ (Abschlusscode „ Nicht erfolgreich“ wechselt und alle anderen dem VUL zugeordneten CHGs sich im selben Status befinden, wird das VUL automatisch in den Status „Wird untersucht“zurückversetzt).

Weitere Informationen zu den Status von Korrekturaufgaben und den möglichen Aktionen in den einzelnen Status finden Sie unter Vulnerability Response Korrekturaufgabe und Status angreifbarer Elemente.

Bewerten Sie Ihre Gefährdung durch angreifbare Software

Sie können den Herausgeber und Produktinformationen im Modul „Risikobewertung“ angeben, um die Zero-Day-Anfälligkeit (aktueller Tag) Ihrer Assets gegenüber angreifbarer Software mithilfe der Anwendung ITSM Software Asset Management (SAM) Foundation zu bewerten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Sie können die Bewertung des Gefahrenpotenzials nach Software und Common Vulnerabilities and Exposures (CVE) durchführen, um die zusätzlichen Funktionen im Arbeitsbereich der Schwachstellenbewertung zu nutzen. Weitere Informationen finden Sie unter Erkunden Sie den Arbeitsbereich der Schwachstellenbewertung.

Vorbereitungen

Erforderliche Rolle: Schwachstellen-Administrator (sn_vulnerability_write)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Halten Sie die folgenden Informationen über die angreifbare Software bereit, die Sie bewerten möchten:

- Herausgeber
- Version
- Produkt
- Edition

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zu den Systemanforderungen finden Sie unter Konfigurieren Sie die Bewertung des Gefahrenpotenzials für Schwachstelle ..

Zeigen Sie das Modul zur Bewertung des Softwarerisikos an, und erstellen und bearbeiten Sie bei Bedarf Datensätze zur Risikobewertung für angreifbare Software in Ihrer Instanz Now Platform®.

Sie verwalten die Vulnerability Response-Aktivitäten für einen großen Betrieb, der für viele Assets verantwortlich ist. Sie werden vom Security Operations Center (SOC) in Ihrem Betrieb kontaktiert, weil festgestellt wurde, dass eine Version einer Software angreifbar ist. Sie stellen fest, dass kürzlich ein Scan Ihrer Assets abgeschlossen wurde und diese Schwachstelle nicht gefunden wurde. Das SOC-Team hat durch eine zuverlässige Quelle außerhalb der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder der anderen Drittanbieterbibliotheken in Ihrer Instanz von dieser Schwachstelle erfahren, und Sie befürchten, dass Ihr Schwachstellenscanner Folgendes getan hat: Das Plugin dafür wurde noch nicht hinzugefügt.

Sie sind zuversichtlich, dass die Daten für diese Schwachstelle im NVD aktualisiert und in Kürze importiert werden, damit Ihr Scanner diese Schwachstelle beim nächsten Scan erkennen kann. Da Sie jedoch über den Umfang Ihres potenziellen Risikos betroffen sind, möchten Sie heute herausfinden, ob Sie haben Assets in Ihrem Netzwerk, auf denen diese Software installiert ist.

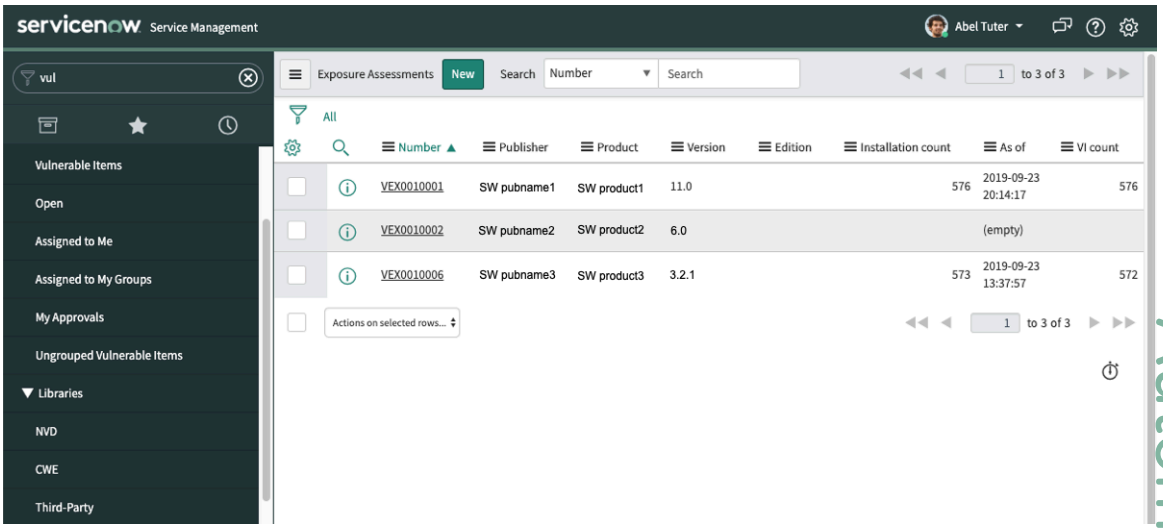
Ab v23.0 von Vulnerability Responsewerden Sie, wenn Sie das Pro- oder Enterprise-Abonnement haben, je nach Ihrer Rolle zur Seite **„Risikobewertung“** in den Arbeitsbereichen weitergeleitet, wenn Sie im Menü **„Alle“** auf den Link **„Risikobewertung“** klicken. Weitere Informationen finden Sie unter Konfigurieren Sie die Bewertung des Gefahrenpotenzials für Schwachstelle ..

Automatische Übersetzung

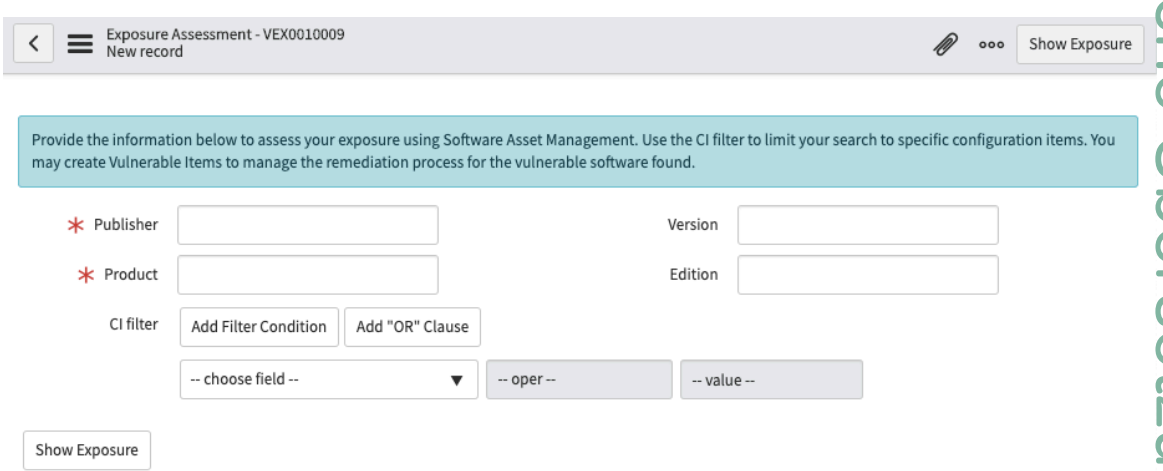
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um eine neue Bewertung des Gefahrenpotenzials zu erstellen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Bewertung des Gefahrenpotenzials**.
   Die Liste der Bewertungen des Gefahrenpotenzials wird angezeigt.



2. Wählen Sie **Neu**.
   Das Formular „Bewertung des Gefahrenpotenzials“ wird angezeigt.



3. Füllen Sie das Formular aus.

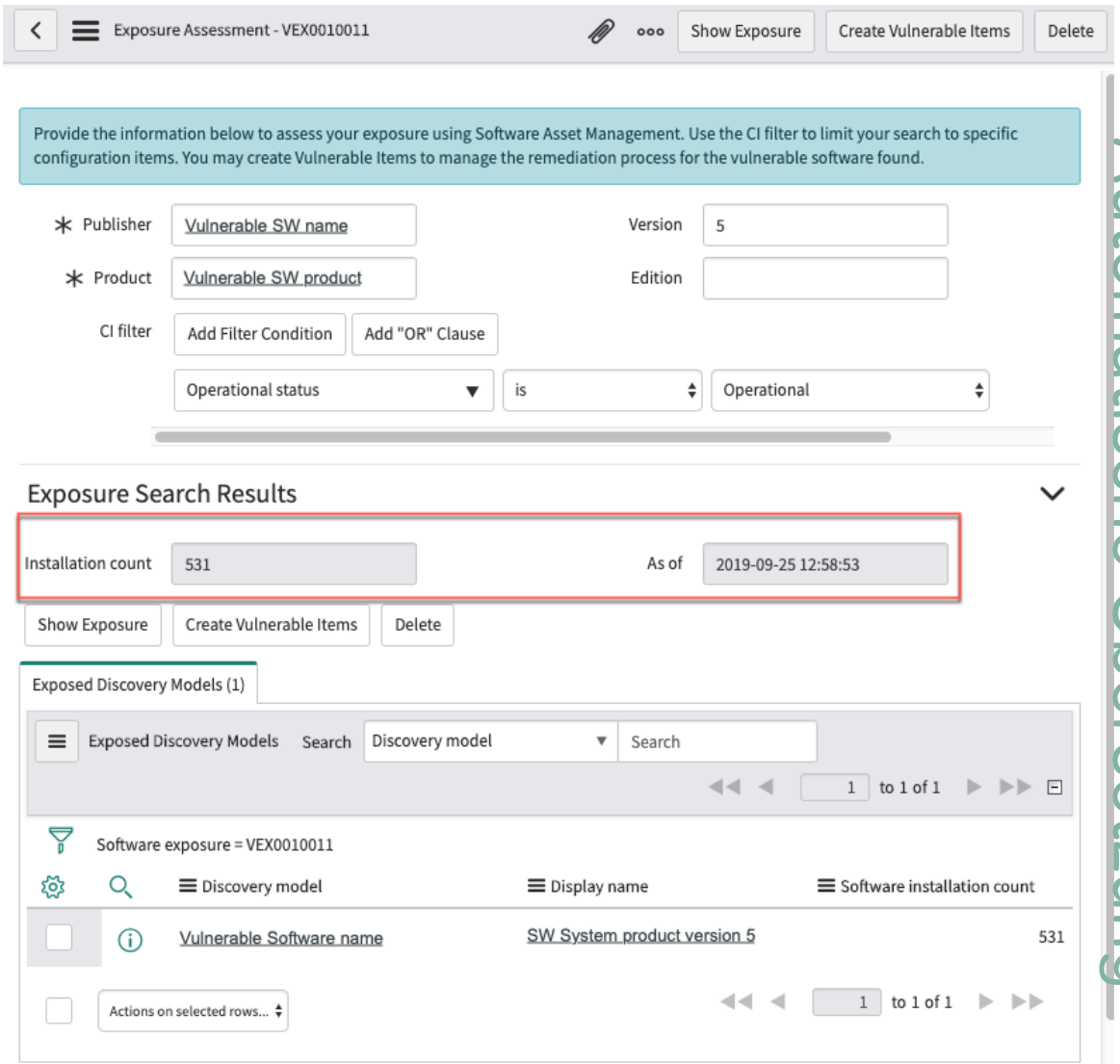
Feld	Beschreibung
Herausgeber	Name des Softwareherausgebers.
(Optional) Version	Geben Sie die Versionsnummer ein, um die Suche nach Ihren Assets einzugrenzen.
Produkt	Name des Softwareprodukts.
(Optional) Edition	Geben Sie die Edition ein, um die Suche nach Ihren Assets einzugrenzen.
CI-Filter	Verwenden Sie die Auswahllisten für den Filter Configuration Item (CI), um Ihre Suche auf bestimmte Configuration Items (Assets) zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	beschränken. Sie können beispielsweise eine Abfrage nur für aktive Assets senden, auf denen diese Software installiert sein darf: Der Betriebsstatus ist „Operativ“.

4. Wählen Sie **Risiko anzeigen**.
   Der Risikobewertungsdatensatz mit Ihrem Discovery-Modell und die Anzahl der Softwareinstallationen auf Ihren Assets ab dem angegebenen Datum wird angezeigt.



5. Wählen Sie eine, um fortzufahren.

6. **Wahlweise:** Erstellen Sie ein angreifbares Element für Ihr Suchergebnis.

> **Hinweis:**
> Nachdem Sie angreifbare Elemente erstellt haben, können Sie die Suchkriterien für diesen Risikodatensatz nicht mehr ändern.

7. Alternativ können Sie Ihre Filterbedingungen überarbeiten und Ihre Suchergebnisse weiter verfeinern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Führen Sie die folgenden Schritte aus, um angreifbare Elemente zu erstellen:

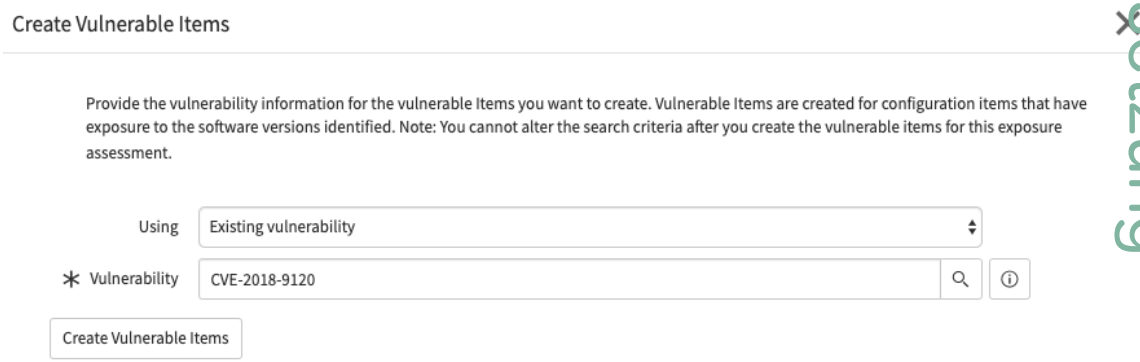
a. Wählen Sie **Angreifbare Elemente erstellen aus**.
Das Dialogfeld „Angreifbare Elemente erstellen“ wird angezeigt.

b. Füllen Sie die Felder aus.

Feld	Beschreibung
Arbeiten mit	Wählen Sie aus der Auswahlliste eine aus, um fortzufahren. ▪ **Vorhandene Schwachstelle**. Klicken Sie rechts neben dem Feld Schwachstelle auf das Suchsymbol. Wählen Sie in der angezeigten Liste die CVE-ID aus, oder geben Sie Suchkriterien ein, um die vorhandene CVE-ID zu finden, z. B. CVE 2018-9120. **Hinweis:** Dies kann eine CVE-ID aus einer anderen Schwachstellendatenbank als der NVD sein. ▪ **Neue Schwachstelle**. Geben Sie die CVE-ID für Ihre neue Schwachstelle im Format „xxxx-xxxx“, „xxxx-xxxxxx“ oder „xxxx-xxxxxx“ ein.
Schwachstellenzusammenfassung (nur für neue Schwachstelle)	Geben Sie eine Zusammenfassung für die neue Schwachstelle ein, z. B. Ein Angreifer kann ein Skript im Browser eines ahnungslosen Benutzers ausführen.

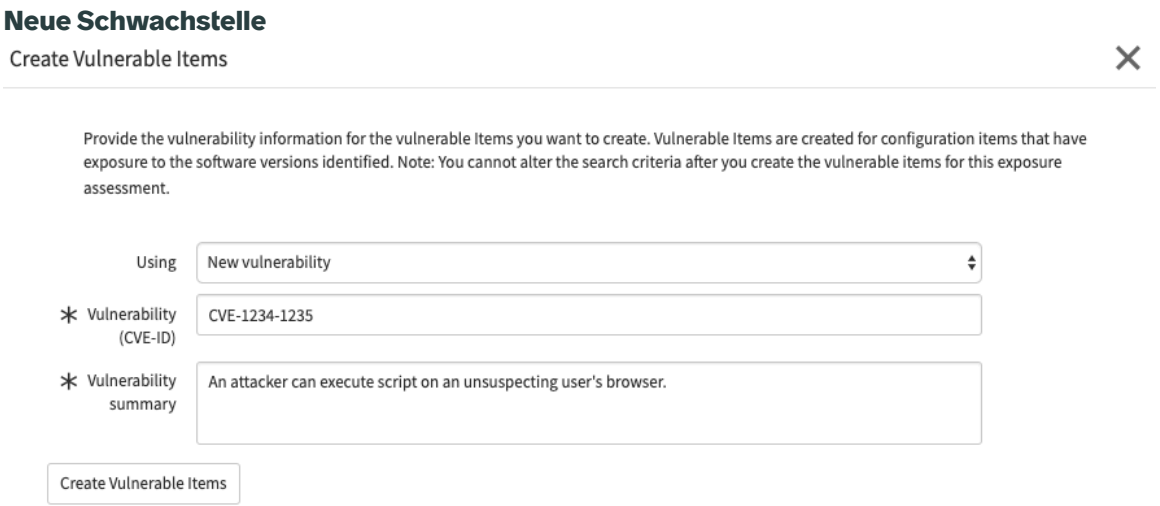
Die folgenden Abbildungen zeigen Beispiele des ausgefüllten Formulars für eine vorhandene und eine neue Schwachstelle.

Vorhandene Schwachstelle



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



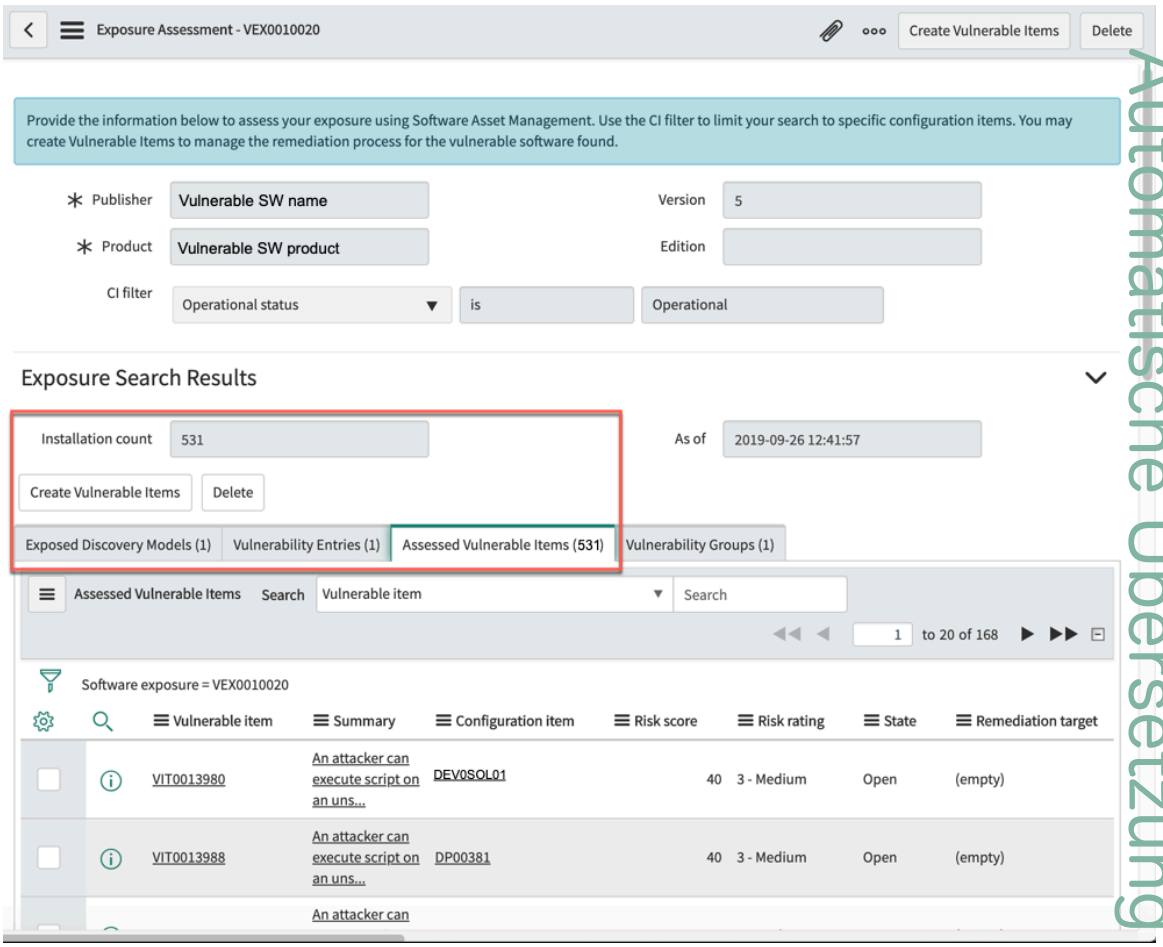
c. Wählen Sie **Angreifbare Elemente erstellen**.
Der Datensatz der Bewertung des Gefahrenpotenzials wird mit einer Statusmeldung angezeigt, die darauf hinweist, dass angreifbare Elemente erstellt werden.

d. Klicken Sie nach einigen Sekunden mit der rechten Maustaste auf den grauen Banner oben im Formular, um die Seite neu zu laden.
Die neuen angreifbaren Elemente werden auf der Registerkarte Bewertete angreifbare Elemente (531) wie in der folgenden Abbildung angezeigt. Die neue Korrekturaufgabe, die für diese angreifbaren Elemente erstellt wurde, wird auf der Registerkarte „Korrekturaufgabe“ (1) angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In diesem Beispiel wird eine Korrekturaufgabe gemäß den Gruppenregeln und Bedingungen aus der Regel für Korrekturaufgaben mit der Bezeichnung Vulnerability erstellt. Diese Gruppenregel ist die standardmäßige Regel für Korrekturaufgaben, die mit dem Produkt Vulnerability Response in Ihrer Instanz Now Platform® installiert wird. In diesem Beispiel haben die Bedingungen dieser Gruppenregel alle angreifbaren Elemente in einer einzigen Korrekturaufgabe platziert. Wenn Sie mehr als eine Korrekturaufgabe für die angreifbaren Elemente erstellen möchten, die Ihren Suchergebnissen der Bewertung des Gefahrenpotenzials entsprechen, können Sie zusätzliche Regeln für Korrekturaufgaben einrichten. Durch das Erstellen weiterer Korrekturaufgaben können Sie möglicherweise vermeiden, dass Korrekturaufgaben mit einer großen Anzahl angreifbarer Elemente erstellt werden. Weitere Informationen zu Regeln für Korrekturaufgaben finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben.

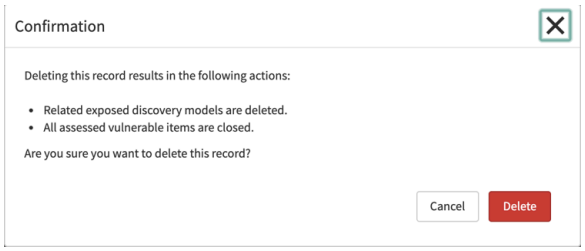


Automatische Übersetzung

9. Wählen Sie eine, um fortzufahren.

Option	Beschreibung
Korrekturaufgaben	Klicken Sie bei ausgewählter Registerkarte Korrekturaufgaben in der Nummernspalte, um den Datensatz zu öffnen, die zu überprüfen und die zu korrigierende Aufgabe zuzuweisen. Weitere Informationen zu Zuweisungsgruppen finden Sie unter Creating groups .
Bewertete angreifbare Elemente	Klicken Sie bei ausgewählter Registerkarte Bewertete angreifbare Elemente in der Spalte Angreifbares Element, um die Datensätze

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	zu öffnen und einzelne angreifbare Elemente zu überprüfen und zuzuweisen.
Löschen	Löschen Sie den Risikobewertungsdatensatz. Ein Bestätigungsdialogfeld wird angezeigt. **Hinweis:** Wenn Sie den Risikodatensatz löschen, nachdem Sie angreifbare Elemente erstellt haben, werden alle angreifbaren Elemente, die Sie für diesen Datensatz erstellen und die nicht mit einem anderen Risikodatensatz verknüpft sind, automatisch in den Status Geschlossen versetzt. Der Grund für den Abschluss ist „Abgebrochen“.
	

Nächste Maßnahme

Reagieren Sie auf Zero-Day-Bedrohungen (aktueller Tag) basierend auf Ihrer Bewertung des Gefahrenpotenzials. Weitere Informationen zu Korrekturaufgaben und Change-Management für Vulnerability Responsefinden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Change Management für Vulnerability Response.

Zuweisungsempfehlungen werden angezeigt

Eine Zuweisungsgruppe wird normalerweise mithilfe von Zuweisungsregeln einem angreifbaren Element zugewiesen. Diese Regeln werden vom Schwachstellenadministrator konfiguriert, um basierend auf den Daten, die er von Drittanbieterscannern erhalten hat, die richtigen Zuweisungsgruppen zuzuweisen.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Wenn keine passende Zuweisungsgruppe verfügbar oder falsch ist, können Sie mit Empfehlungen für die Zuweisung von Schwachstellen alternative Zuweisungsgruppen anzeigen.

Verwenden Sie Empfehlungen für die Zuweisung von Schwachstellen für die folgenden Aktionen:

- Fordert Zuweisungsgruppenempfehlungen für ein angreifbares Element an.
- Empfehlungen für Zuweisungsgruppen für mehrere angreifbare Elemente anfordern.
- Fordert Zuweisungsgruppenempfehlungen für eine Korrekturaufgabe an.

Fordert Zuweisungsgruppenempfehlungen für ein angreifbares Element an

Fordern Sie Empfehlungen für die Zuweisung von Schwachstellen an, damit Sie Empfehlungen für Zuweisungsgruppen anzeigen können. Sie können Empfehlungen anfordern, wenn keine übereinstimmende Zuweisungsgruppe für ein angreifbares Element (VI) verfügbar ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** und öffnen Sie ein VI.
   Das Element muss sich im Status „Offen“, „Zurückgestellt“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf das Empfehlungssymbol ( ) neben dem Feld **Zuweisungsgruppe,** um Zuweisungsvorschläge für dieses AE anzuzeigen.
3. Wählen Sie im Dialogfeld „Empfehlungen für Zuweisungsgruppe“ eine Empfehlung aus, die auf der Vertrauensbewertung basiert.
   Die Konfidenzpunktzahl sagt vorher, wie relevant die Übereinstimmung für das VI ist. Weitere Informationen finden Sie unter ML-Lösungen (maschinelles Lernen) für Vulnerability Response.
4. Klicken Sie auf **Zuweisen**.

Ergebnisse

Die ausgewählte Gruppe wird im Feld **Zuweisungsgruppe** angezeigt, und der Zuweisungstyp ändert sich in Empfehlung.

Empfehlungen für Zuweisungsgruppen für mehrere angreifbare Elemente anfordern

Verwenden Sie Empfehlungen für die Zuweisung von Schwachstellen, um die Empfehlungen für Zuweisungsgruppen für mehrere angreifbare Elemente (VIs) mithilfe einer Massenbearbeitung anzuzeigen. Wenn mehrere VIs ausgewählt sind, wird eine Vorhersage für eine zufällige Stichprobe der ausgewählten VIs durchgeführt.

Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Die Empfehlungen und ihre Konfidenzwerte können sich je nach Aufruf leicht unterscheiden, je nachdem, welche Beispiele aus den ausgewählten VIs genommen wurden. Die Vertrauensbewertung bewertet, ob das System davon ausgeht, dass die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist. Verwenden Sie die Systemeigenschaft „assignment_recommendation_batchsize“, um die Batchgröße festzulegen, wenn Sie Empfehlungen für die Zuweisung von Schwachstellen für Korrekturaufgaben (VULs) und VIs mithilfe der Massenbearbeitungsoption anfordern. Der Standardwert dieser Systemeigenschaft ist auf optimale Vorhersageleistung festgelegt.

Hinweis:
Wenn Sie den Standardwert erhöhen, ändert sich möglicherweise die Antwortzeit für Empfehlungen für die Zuweisung von Schwachstellen für diese Fälle.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbares Element** und wählen Sie mehrere AEs aus.
   Die Elemente müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf **Massenbearbeitung**.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular: Massenangreifbare Elemente angreifbare Elemente

Feld	Beschreibung
Datensatzauswahl	Datensätze, die für die Massenbearbeitung ausgewählt werden sollen.
Zuweisungsgruppe	Zuweisungsgruppe, die für die ausgewählten angreifbaren Elemente festgelegt werden soll. Um die empfohlenen Zuweisungsgruppen anzuzeigen, klicken Sie auf das Empfehlungssymbol ( ) neben dem Feld. Wählen Sie eine Empfehlung basierend auf der Vertrauensbewertung aus, und klicken Sie auf **Zuweisen**.
Arbeitsnotizen	Hinzuzufügende Hinweise.

4. Klicken Sie auf **OK**.

Ergebnisse

Die ausgewählte Gruppe wird im Feld **Zuweisungsgruppe** angezeigt, und der Zuweisungstyp ändert sich für alle ausgewählten VIs in Empfehlung.

Fordert Zuweisungsgruppenempfehlungen für eine Korrekturaufgabe an

Verwenden Sie Empfehlungen für die Zuweisung von Schwachstellen, um Empfehlungen für Zuweisungsgruppen für eine Korrekturaufgabe (VUL) anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Systemeigenschaft „assignment_recommendation_batchsize“, um die Batchgröße festzulegen, wenn Sie Empfehlungen für die Zuweisung von Schwachstellen für VULs und angreifbare Elemente (VIs) mithilfe der Massenbearbeitungsoption anfordern. Der Standardwert dieser Systemeigenschaft ist auf optimale Vorhersageleistung festgelegt.

Hinweis:
Wenn Sie den Standardwert erhöhen, ändert sich möglicherweise die Antwortzeit für Empfehlungen für die Zuweisung von Schwachstellen für diese Fälle.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** und wählen Sie eine VUL aus.
   Die Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf das Empfehlungssymbol ( ) neben dem Feld **Zuweisungsgruppe**, um die Zuweisungsgruppenempfehlungen für die ausgewählte VUL anzuzeigen.
   Im Dialogfeld „Empfehlungen für Zuweisungsgruppe“ werden die empfohlenen Zuweisungsgruppen mit der durchschnittlichen Vertrauensbewertung für alle VIs in dieser Gruppe angezeigt.
3. Wählen Sie basierend auf der Vertrauensbewertung eine Empfehlung aus der Liste Zuweisungsgruppe aus.
   Die Konfidenzpunktzahl sagt vorher, wie relevant die Übereinstimmung für die ausgewählte VUL ist.
4. Klicken Sie auf **Zuweisen**.
   Die ausgewählte Gruppe wird im Feld **Zuweisungsgruppe** angezeigt.
5. Speichern Sie die Korrekturaufgabe mit den aktualisierten Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Alle VIs mit derselben Zuweisungsgruppe wie die VUL werden der ausgewählten Zuweisungsgruppe zugewiesen. Der Zuweisungstyp wird für die VUL sowie für alle geänderten AEs in Empfehlung geändert.

Ausnahme wird angefordert und genehmigt

Sie können anfordern, die Korrektur eines angreifbaren Elements oder einer Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist. Genehmiger mit Zugriffsrechten können Anforderungen anderer Benutzer genehmigen.

Sie können Ausnahmen in den Arbeitsbereichen Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

- Fordern Sie eine Ausnahme für ein angreifbares Element an
- Fordern Sie eine Ausnahme für eine Korrekturaufgabe an
- Fordern Sie eine Massenausnahme an

Sie können Richtlinienausnahmen auch mit GRC: Richtlinien- und Compliance-Managementanfordern:

- Fordern Sie mit eine Ausnahme an GRC: Richtlinien- und Compliance-Management
- Fordern Sie mit eine Massenausnahme an GRC: Richtlinien- und Compliance-Management

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail mit dem Hinweis, dass eine Ausnahme angefordert wurde.

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Fordern Sie eine Ausnahme für ein angreifbares Element an

Fordern Sie eine Ausnahme für ein angreifbares Element (VI) an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wichtig:
Sie können Ausnahmen in den Arbeitsbereichen des Schwachstellenmanagers und der IT-Korrektur anfordern. Weitere Informationen finden Sie unter Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace und Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Sie können Ausnahmen für VIs auch in der klassischen Umgebung anfordern.

Hinweis:

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle**.
2. Wählen Sie den Artikel aus, für den Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Klicken Sie im Formular „Angreifbares Element“ **auf Ausnahme anfordern**.
4. Wenn Vulnerability Response im Bildschirm „Ausnahmeverwaltung“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in ausgewählten Dauer liegen **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status Offen zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Ab Version 18.0 von Vulnerability Response (VR): Wenn ein angreifbares Element mithilfe der Ausnahmeverwaltungsfunktion zur Korrektur zurückgestellt wurde und es vom Scanner erneut geöffnet wird, bleibt das für die Schwachstelle festgelegte Zurückstellungsdatum weiterhin erhalten. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft `sn_vul.auto_defer_vit_in_active_exception_win` auf „true“ fest. Außerdem bleibt das zurückgestellte **Bis-** Datum auch dann erhalten, wenn das angreifbare Element geschlossen wird oder die Ausnahme abgelaufen ist. Die erforderliche Rolle für Lese- und Schreibzugriff lautet sn_vul.manage_exception_configuration.
Grund	Grund für die Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige Informationen zum Hinzufügen neuer Gründe finden Sie unter Definieren Sie die Zuordnung von Richtliniengrund.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Besitzer der Korrektur aktualisiert werden.

5. Senden Sie die Ausnahmeanforderung, indem Sie **auf Genehmigung anfordern**klicken.

Ergebnisse

Der Status des angreifbaren Elements ändert sich in Wird überprüft. Verwenden Sie die Registerkarte **Change-Genehmigung**, um den Status der Ausnahmeanforderung zu verfolgen.

Fordern Sie eine Ausnahme für eine Korrekturaufgabe an

Fordern Sie eine Ausnahme an, um eine Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort gelöst werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Wichtig:

Sie können die Ausnahmen in den Arbeitsbereichen des Schwachstellenmanagers und in den Arbeitsbereichen für IT-Korrekturen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können Ausnahmen für Korrekturaufgaben auch in der klassischen Umgebung anfordern.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Alle**.
2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Wählen Sie im Datensatz der Korrekturaufgabe (VUL) **die Option Ausnahme anfordern**aus.
4. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in der Konfiguration definierten Ausnahmedauer liegen.
Grund	Begründung für das Anfordern einer Ausnahme.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Korrektur aktualisiert werden.

5. Klicken Sie auf **Genehmigungs-Engine**.

Fordern Sie eine Massenausnahme an

Verwenden Sie die Massenbearbeitungsoption, um eine Ausnahme für mehrere angreifbare Elemente (VITs) anzufordern, anstatt jedes Element manuell auszuwählen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst

Warum und wann dieser Vorgang ausgeführt wird

Wenn mehrere VITs ausgewählt werden, wird eine Korrekturaufgabe (VUL) mit diesen Elementen erstellt. Weitere Informationen zum Bearbeiten mehrerer VITs finden Sie unter Führen Sie eine Massenbearbeitung von angreifbaren Elementen in durch Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Sie können eine Ausnahme anfordern für:

- ein VIT aus Vulnerability Manager Workspace und IT Remediation Workspace. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.
- mehrere VITs aus Vulnerability Manager Workspace. Weitere Informationen finden Sie unter Massenausnahme im Arbeitsbereich des Schwachstellenmanagers anfordern.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle** und wählen Sie die Artikel aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählten Elemente müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf **Massenbearbeitung**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Massenbearbeitung für angreifbares Element“.

Feld	Beschreibung
Datensatzauswahl	Datensätze, die Sie für eine Massenbearbeitung ausgewählt haben.
Status	Status des angreifbaren Elements. Wählen Sie den Status Zurückgestellt aus, um eine Ausnahme für die ausgewählten Artikel anzufordern.
Grund	Substatus für den von Ihnen ausgewählten Status.
Kurzbeschreibung	Name der Korrekturaufgabe, die Sie erstellen.
Bis	Enddatum, das Sie für Ihre Ausnahmeanforderung angeben.
Zusätzliche Information	Weitere Details, die Sie angeben möchten, um den Genehmiger über die Gründe für Ihre Anforderung zu informieren.
Bevorzugte Lösung	Lösung zur Korrektur aller angreifbaren Elemente, die Sie für eine Massenbearbeitung ausgewählt haben.
Zuweisungsgruppe	Zuweisungsgruppe für das AE. Sie können eine Gruppe manuell auswählen oder Zuweisungsempfehlungen verwenden, wenn diese Funktion aktiviert ist.
Arbeitsnotizen	Hinzuzufügende Hinweise.

4. Klicken Sie auf **OK**.
   Es wird eine Korrekturaufgabe erstellt, die die von Ihnen ausgewählten VIs enthält. Diese Korrekturaufgabe wird zur Genehmigung übermittelt.

Fordern Sie mit eine Ausnahme an GRC: Richtlinien- und Compliance-Management

Fordern Sie mit der Funktion zur Verwaltung von Richtlinienausnahmen GRC in der Anwendung Richtlinien- und Compliance-Management innerhalb von Vulnerability ResponseRichtlinienausnahmen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Bevor Sie die Integration für Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Richtlinien- und Compliance-Management von ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können Ausnahmen auch in der klassischen Anwenderoberfläche anfordern:

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** (oder **Korrekturaufgaben**) >**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular **auf Ausnahme anfordern**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Richtlinie	Richtlinie für Schwachstellenmanagement, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von Zurückgestellt in Offen wechselt. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage),** die Sie für die Richtlinie in Richtlinien und Compliance festgelegt haben, nicht überschreiten. Weitere Informationen finden Sie unter Richtlinie erstellen.
Grund	Grund für das Anfordern einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Besitzer der Remediation ausgefüllt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Korrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Fordern Sie mit eine Massenausnahme an GRC: Richtlinien- und Compliance-Management

Wählen Sie eine Gruppe angreifbarer Elemente aus, und senden Sie eine Massenausnahme.

Vorbereitungen

Bevor Sie mit der Integration für Richtlinienausnahmen Massenausnahmen anfordern können, müssen Sie die Anwendung GRC: Richtlinien- und Compliance-Management von ServiceNow Storeherunterladen.

Hinweis:
Um diese Funktion zu verwenden, müssen Sie GRC: Richtlinien- und Compliance-Management vor dem Upgrade von Vulnerability Responseaktualisieren. Wenn Sie Vulnerability Response bereits vor GRC: Richtlinien- und Compliance-Managementaktualisiert haben und diese Funktion verwenden möchten, müssen Sie die Upgrade-Verfahren erneut in der richtigen Reihenfolge ausführen.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können Ausnahmen auch in der klassischen Umgebung in Vulnerability Responseanfordern.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Alle** und wählen Sie die Artikel aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählten Elemente müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf **Massenbearbeitung**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Massenbearbeitung für angreifbares Element“.

Feld	Beschreibung
Datensatzauswahl	Datensätze, die Sie für eine Massenbearbeitung ausgewählt haben.
Status	Status des angreifbaren Elements. Wählen Sie den Status Zurückgestellt aus, um eine Ausnahme für die ausgewählten Artikel anzufordern.
Kurzbeschreibung	Name der Aufgabe, die Sie erstellen.
Bevorzugte Lösung	Lösung, die Sie zur Korrektur aller angreifbaren Elemente verwenden, die Sie für die Massenbearbeitung ausgewählt haben.
Zuweisungsgruppe	Zuweisungsgruppe für das AE. Sie können eine Gruppe manuell auswählen oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zuweisungsempfehlungen verwenden, wenn diese Funktion aktiviert ist.
Arbeitsnotizen	Hinzuzufügende Hinweise.

4. Klicken Sie auf **OK**.
   Es wird eine Korrekturaufgabe mit den ausgewählten angreifbaren Elementen erstellt.
5. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Richtlinie	Richtlinie für Schwachstellenmanagement, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme startet. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von Zurückgestellt in Offen wechselt. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Dauer der Ausnahme (Tage),** die Sie für die Richtlinie in GRC: Richtlinien- und Compliance-Managementfestgelegt haben, nicht überschreiten. Weitere Informationen finden Sie unter Richtlinie erstellen.
Grund	Grund für das Anfordern einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Besitzer der Remediation ausgefüllt werden.

6. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Korrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management.

Genehmigen Sie eine Ausnahmeanforderung in, oder lehnen Sie sie ab Vulnerability Response

Genehmigen Sie die Ausnahmeanforderungen für angreifbare Elemente oder Korrekturaufgaben, die nicht sofort korrigiert werden können, oder lehnen Sie sie ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie müssen diese Anforderungen auf Risiken bewerten und dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Wichtig:

Sie können die Ausnahmeanforderungen im Vulnerability Manager Workspacegenehmigen oder ablehnen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

Sie können Ausnahmeanforderungen auch in der klassischen Umgebung genehmigen.

Hinweis:

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Arbeiten mit einer Ausnahmeregel

Sie können eine Ausnahme für Schwachstellen, angreifbare Elemente (VIs) oder Konfigurationselemente (CIs) anfordern, die nicht sofort behoben oder zurückgestellt werden können. Durch Automatisierung des VI-Zurückstellungsprozesses können Sie die übereinstimmenden VIs basierend auf der Regel zurückstellen, wenn sie vom System identifiziert werden.

Sie können die folgenden Aufgaben für eine Ausnahmeregel ausführen:

- Ausnahmeregel erstellen
- Antrag auf Ausnahmeregel genehmigen
- Ausnahmeregel aktivieren
- Öffnen Sie eine Ausnahmeregel erneut
- Aktualisiert eine genehmigte Ausnahmeregel
- Ausnahmeregel löschen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Ausnahmeregel erstellen

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe von angreifbaren Elementen (VIs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser VIs basiert. Mit dieser Regel können Sie neue und vorhandene VIs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Regel wird vom „Gültig ab“-Datum bis zum „Gültig bis“-Datum angewendet.
Die Korrekturaufgabe (VUL) wird erstellt, wenn die Regel genehmigt wird. Die Gruppierungsmethode für diese VUL wird als Ausnahmeregel bezeichnet. Die VUL wird im Status „Zurückgestellt“ erstellt. Sie können diese VUL nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete VIs werden zurückgestellt und dieser VUL vom „Gültig ab“-Datum hinzugefügt, bis die Gruppe am „Gültig bis“-Datum abläuft.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmeregel-Workflows gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung übermittelt wurde.

Hinweis:

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung einreichen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Klicken Sie auf der neuen Datensatzseite „Ausnahmeregel“ auf **Neu**, um eine Regel zu erstellen.
3. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahmeregel“.

Feld	Beschreibung
Name	Name der Ausnahmeregel.
Gültig ab	Datum, ab dem diese Regel aktiv ist, um die AEs zurückzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gültig bis	Datum, ab dem die Korrekturaufgabe die Annahme neuer AEs beendet.
Grund	Grund für die Erstellung dieser Ausnahmeregel.
Zuweisungsgruppe	Gruppe, der die zur Nachverfolgung der zurückgestellten AEs erstellte Korrekturaufgabe zugewiesen ist.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen.
Bedingung	Filterbedingung für die VIs, die während der Verarbeitung der VIs definiert werden kann.
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für bereits vorhandene Daten ausführen können.
Workflow-Phase	Aktueller Genehmigungsstatus der Ausnahmeregel.
Status	Status der Ausnahmeregel.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel.
Zurückgestellt bis	Datum, bis zu dem die VULs und VIs zurückgestellt werden. An diesem Datum wird die erstellte VUL geschlossen, alle VIs werden aus der Gruppe entfernt, und Gruppenregeln werden erneut angewendet.

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Senden Sie das Formular zur Genehmigung.
   Der Status der Anforderung ändert sich in Überprüfung. Bis Sie die Ausnahmeregel nicht absenden, verbleibt sie im Status Entwurf.

Antrag auf Ausnahmeregel genehmigen

Bewerten Sie Anforderungen für Ausnahmeregeln von Anwendern, um diese Anforderungen genehmigen oder ablehnen zu können.

Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

Warum und wann dieser Vorgang ausgeführt wird

Mitglieder der Benutzergruppe „Ausnahmegenehmiger Ebene 1“ können die Anforderungen der Ausnahmeregel der Ebene 1 genehmigen. In ähnlicher Weise können Mitglieder der Benutzergruppe, die Ausnahmegenehmiger der Ebene 2 sind, die Anforderungen einer Ausnahmeregel der Ebene 2 genehmigen. Beide Benutzergruppen erben standardmäßig die Rolle des Ausnahmegenehmigers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit ab, und erläutern Sie, warum Sie die Anforderung genehmigt oder abgelehnt haben.
   Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe (RT) im Status „Zurückgestellt“ erstellt. Ab dem Datum „Gültig ab“ wird diese Regel für alle VIs ausgeführt, die erstellt werden, und auch für diejenigen, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden. AEs, die den definierten Bedingungen entsprechen, werden dem RT hinzugefügt und für den angegebenen Zeitraum zurückgestellt.

   Hinweis:
   Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung einreichen.

Ausnahmeregel aktivieren

Eine Regel wird an ihrem „Gültig ab“-Datum aktiviert. Nach der Aktivierung automatisiert es den Ausnahmeprozess für angreifbare Elemente (VIs, Vulnerable Items).

Die Ausnahmeregel folgt diesem Lebenszyklus:

1. Die neuen angreifbaren Elemente (VIs), die Sie erstellen oder erneut öffnen und die die angegebene Bedingung erfüllen, werden zurückgestellt. Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wenn Sie die Ausnahmeregel zum ersten Mal ausführen, werden alle aktiven und nicht zurückgestellten VIs, die der Ausnahmeregelbedingung entsprechen, in die neu erstellte Korrekturaufgabe (RT) verschoben, und ihr Status wird geändert auf „Zurückgestellt“
2. Wenn ein neu erstelltes AEs der Bedingung der Ausnahmeregel entspricht, wird es in die zurückgestellte RT verschoben, die der Regel zugeordnet ist, und die Gruppenregel wird nicht dafür ausgeführt.
3. Am Datum „Gültig ab“ werden vorhandene VIs hinzugefügt, wenn Sie die Option Für vorhandene Daten ausführen aktivieren.
4. Die RT akzeptiert keine neuen VIs mehr, wenn die Regel am „Gültig bis“-Datum abläuft. Die RT bleibt bis zum Datum „Zurückgestellt bis“ bestehen.
5. Die Ausnahmeregel läuft am „Gültig bis“-Datum ab.

Fordern Sie eine Verlängerung für eine Ausnahmeregel an

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht ist. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Ausnahmeregeln**.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein. Zur Auswahl stehen: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und Zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Korrekturaufgaben und angreifbaren Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktualisiert. Außerdem wird bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers eine E-Mail ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Ausnahmeregel erneut verlängert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.
- Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Öffnen Sie eine Ausnahmeregel erneut

Öffnen Sie eine Ausnahmeregel erneut, die abgelehnt wurde, Sie möchten jedoch erneut übermitteln. Durch erneutes Öffnen wird die Regel in den Status Entwurf versetzt.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Regel dann aktualisieren und erneut zur Genehmigung einreichen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Suchen Sie die Regel, die Sie erneut öffnen möchten, und klicken Sie auf **Erneut öffnen**.
3. Aktualisieren Sie das Formular, und senden Sie es erneut zur Genehmigung.

Aktualisiert eine genehmigte Ausnahmeregel

Brechen Sie eine genehmigte Regel ab, um sie aktualisieren zu können. Bevor Sie beispielsweise Daten ändern oder einer genehmigten Regel eine Bedingung hinzufügen können, müssen Sie sie abbrechen, damit die Korrekturaufgabe (VUL) gelöscht wird und die angreifbaren Elemente (VIs) in den Status Offen versetzt werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Gruppenregeln werden erneut auf diese AEs angewendet. Senden Sie die Regel, nachdem Sie die Änderungen vorgenommen haben, damit sie den Genehmigungsprozess erneut durchläuft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie abbrechen möchten, und klicken Sie auf **Abbrechen**.
3. Klicken Sie im Dialogfeld „Regel abbrechen“ auf **Regel abbrechen**.
   Die Regel wird zurück in den Status Entwurf verschoben, und die zugehörige VUL wird gelöscht. Die zugehörigen VIs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen VIs angewendet.

Ausnahmeregel löschen

Löschen Sie eine Ausnahmeregel, die nicht mehr erforderlich ist. Sie können beispielsweise eine Regel löschen, wenn Sie ein angreifbares Element (VI) während der Erfassung nicht zurückstellen möchten.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch das Löschen einer Regel wird die zugehörige Korrekturaufgabe (VUL) abgebrochen. Die zugehörigen VIs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen VIs angewendet.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Klicken Sie im Dialogfeld „Regel löschen **“ auf Regel löschen**, um die ausgewählte Regel zu löschen.
   Die zugehörige Korrekturaufgabe wird ebenfalls gelöscht. Die zugehörigen VIs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen VIs angewendet.

Falsch positives Ergebnis wird markiert und genehmigt

Angreifbare Elemente (VIs) und Korrekturaufgaben (VULs) können als falsch positive Meldungen markiert werden. Genehmiger mit Schreibzugriff können solche Anforderungen von anderen Benutzern genehmigen.

- Als falsch positiv markieren
- Massenbearbeitung für falsch positive Meldung
- Genehmigen Sie , oder lehnen Sie ein falsch positives Ergebnis ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des falsch positiven Workflows gesendet und enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise ein VI oder eine Korrekturaufgabe als falsch positiv markiert wird, erhält die anfordernde Person eine Bestätigungs-E-Mail. Gleichzeitig erhält der Genehmiger eine E-Mail, in der angegeben wird, dass ein VI oder eine Korrekturaufgabe als falsch positiv markiert wurde.

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Als falsch positiv markieren

Markieren Sie ein angreifbares Element (VI) oder eine Korrekturaufgabe (VUL) als falsch positiv, wenn die vom Scanner ausgegebene Warnung kein tatsächliches Problem darstellt. Wenn beispielsweise ein Configuration Item außer Betrieb genommen wurde, der Scanner jedoch immer noch ein damit zusammenhängendes Problem auslöst, markieren Sie es als falsch positiv.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Sie können falsch positive Meldungen aus den -Arbeitsbereichen Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an.

Sie können auch falsch positive Meldungen in der klassischen Umgebung anfordern:

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente (oder Korrekturaufgaben)** > **Alle**.
2. Öffnen Sie das VI oder die VUL, das bzw. die Sie als falsch positiv markieren möchten, und klicken Sie auf **Als falsch positiv markieren**.
   Das VI oder die VUL muss sich im Status **„Offen“** befinden.
3. Geben Sie im Formular „Falsch positiv“ unter **Zusätzliche Informationen** Details ein, und klicken Sie auf **Genehmigung anfordern**.
   Die Anforderung wird zur Genehmigung gesendet, und der Status des VI oder VUL ändert sich **in Überprüfung**.

Massenbearbeitung für falsch positive Meldung

Verwenden Sie eine Massenbearbeitung, um mehrere angreifbare Elemente (VITs) als falsch positiv zu kennzeichnen. Wenn mehrere VITs ausgewählt sind, wird mit diesen Elementen eine Korrekturaufgabe erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Als Administrator oder Analyst können Sie im Arbeitsbereich des Schwachstellenmanagers die Massenbearbeitungsfunktion verwenden, um mehrere VITs als falsch positiv zu kennzeichnen. Weitere Informationen finden Sie unter Massenbearbeitung für falsch positive Werte im Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Sie können auch falsch positive Meldungen in der klassischen Umgebung anfordern:

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle** und wählen Sie die Elemente aus, die Sie als falsch positiv markieren möchten.
   Die ausgewählten Elemente müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf **Massenbearbeitung**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Massenbearbeitung für angreifbares Element“.

Feld	Beschreibung
Datensatzauswahl	Datensätze, die für die Massenbearbeitung ausgewählt werden sollen.
Status	Status der angreifbaren Elemente. Wählen Sie Geschlossen aus, um als falsch positiv zu markieren.
Grund	Substatus für den ausgewählten Status. Wenn Sie als Status „Geschlossen“ ausgewählt haben, wählen Sie hier Falsch positiv, um als falsch positiv zu markieren.
Zuweisung aufheben	Senden Sie eine Anforderung, um die Felder „Zugewiesen an“ und „Zuweisungsgruppe“ zu löschen.
Bevorzugte Lösung	Ziellösung für die Korrektur aller für die Massenbearbeitung ausgewählten angreifbaren Elemente.
Zuweisungsgruppe	Zuweisungsgruppe für das AE. Wählen Sie manuell oder mithilfe von Zuweisungsempfehlungen aus, wenn diese Option aktiviert ist.
Arbeitsnotizen	Hinzuzufügende Hinweise.

4. Klicken Sie auf **OK**.
   Eine neue Korrekturaufgabe mit den ausgewählten AEs wird erstellt und zur Genehmigung gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigen Sie , oder lehnen Sie ein falsch positives Ergebnis ab

Als falsch positiver Genehmiger können Sie falsch positive Anforderungen von anderen Anwendern genehmigen oder ablehnen.

Wichtig:

Als falsch positiver Genehmiger können Sie die falsch positiven Anforderungen in Vulnerability Manager Workspacegenehmigen oder ablehnen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.false_positive_approver für angreifbare Elemente
- sn_vul.app_false_positive_approver für angreifbare Anwendungselemente

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellen** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Hinweis:
Ein falsch positives Ergebnis kann zeitgebunden sein. Nur der Genehmiger kann das Enddatum festlegen.

Analytics- und Reporting-Lösungen für Vulnerability Response

Die Überwachung der Nachbesserung von Schwachstellen umfasst das Anzeigen von Trends, das Verwalten von Risiken und das Überwachen von Zuweisungsgruppen. Sie können Probleme mit hohem Risiko, Arbeitsauslastungen für Zuweisungsgruppen, Zurückstellungen und wiederkehrende Schwachstellen überprüfen. Vulnerability Response bietet Tools, Berichte und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

Datenvisualisierungen in den -Arbeitsbereichen Vulnerability Response .

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad aktiver Schwachstellen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen anzeigen, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Manager Workspace und IT Remediation Workspace erkunden.

Schwachstellenanalysten können unter auch Standarddashboards Vulnerability Response verwenden **Alle** > **Vulnerability Response** > **Übersicht**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Ab Version 19.0 von Vulnerability Responsekann dieses Dashboard auch in der New Experience UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das **Dashboard** -Symbol. Je nach Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdownliste neben dem Namen des Dashboards. Weitere Informationen finden Sie unter Dashboards im Arbeitsbereich des Schwachstellenmanagers und Dashboards im Arbeitsbereich für IT-Fehlerkorrekturen.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Vulnerability Response Nachbesserungsprozess

Die meiste Nachbesserung von Schwachstellen wird über den Korrekturaufgaben-Datensatz in den Vulnerability Response -Arbeitsbereichen durchgeführt. Von den Korrekturaufgaben (RTs) im Status „Wird untersucht“ aus können Sie mehrere Aufgaben ausführen.

- Erstellen Sie Change-Anforderungen.
- Fügen Sie Arbeitsnotizen und Beschreibungen von Schwachstellen innerhalb der Korrekturaufgabe hinzu.
- Verschieben Sie die Korrekturaufgabe und die darin enthaltenen angreifbaren Elemente auf einen späteren Zeitpunkt.
- Schließen Sie die Korrekturaufgabe.
- Verfolgen Sie neue Complianceverpflichtungen nach, die normalerweise zeitabhängig sind.

- Melden Sie sich bei der Vulnerability Response-Instanz an.
- Überprüfen Sie Ihr Schwachstellenmanagement sowie die Dashboards und Berichte von Drittparteien, um Problembereiche zu lokalisieren. Zeigen Sie beispielsweise Dashboards an, die das Altern von Korrekturaufgaben nach Status oder angreifbare Elemente mit hohem Risiko nach ihrem Korrekturzieldatum anzeigen.
- Überprüfen Sie den Status der Korrekturaufgaben in der Reihenfolge des Risikos.
- Überarbeiten Sie die Priorisierung für die Aufgaben, indem Sie Ihre Risikopunktzahl-Rechner anpassen, wenn die Risikopunktzahl nicht richtig berechnet wird, oder indem Sie VIs oder RTs nach Bedarf zurückstellen. Weitere Informationen zu diesen Optionen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners oder Korrekturaufgabe zurückstellen.
- Überprüfen Sie zurückgestellte angreifbare Elemente, um sie erneut zu öffnen und nach Bedarf weitere Maßnahmen zu ergreifen. Wenn Sie Change-Aktivitäten für Ihre Assets, Korrekturaufgaben und die entsprechenden angreifbaren Elemente initiieren und nachverfolgen möchten, finden Sie weitere Informationen unter Change Management für Vulnerability Response.
- Überprüfen Sie das Feedback von IT Operations.

  Sobald Sie benachrichtigt werden, dass eine Change-Anforderung gelöst wurde, warten Sie auf den nächsten Scan. Scans werden automatisch durch den im Setup-Assistenten konfigurierten Importzeitplan einer Drittpartei ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn nach einem Scan der Status Repariert lautet, werden angreifbare Elemente während des Imports automatisch geschlossen. Die Gruppe wird geschlossen, wenn alle angreifbaren Elemente in der Gruppe behoben sind.
- Wenn der Status nach dem Scan nicht Fest ist, wird das VI automatisch zurück in den Status Wird untersucht verschoben.

- Angreifbare Elemente, die in Ihrer Instanz auf „Gelöst“ festgelegt sind, aber von den Integrationsausführungen der Drittpartei nicht in den Status „Geschlossen/Behoben“ versetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

  Wenn der Scanner für Qualys -Erkennungen weiterhin VIs findet, die auf „Gelöst“ gesetzt wurden, dann aber nicht durch nachfolgende Scans in den Status „Geschlossen/Behoben“ überführt wurden, kehren diese VIs zu „Offen“ zurück, wenn das zuletzt gefundene Datum nach dem liegt Datum der Lösung.

  Für Rapid7 -Erkennungen ist auf der Konfigurationsseite Rapid7 in Ihrer -Instanz jetzt eine Option verfügbar, um gelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden AEs, die auf „Gelöst“ gesetzt werden, dann aber nicht durch nachfolgende Scans in „Geschlossen/Behoben“ geändert werden, nach der von Ihnen eingegebenen Anzahl von Tagen wieder in den Status „Offen“ geändert.

Vulnerability Solution Management Fortschritt bei der Bereitstellung

Umfassende Bereitstellungsmetriken für Korrekturaufgaben und Schwachstelleneinträge sind in Vulnerability Solution Management unter **Korrekturstatus** in Schwachstellen, angreifbare Elemente enthalten. Identifizieren Sie auf einfache Weise, welche Korrekturaufgabe oder Schwachstelle den Lösungsfortschritt verlangsamt. Zeigen Sie Detailinformationen dazu an, wie die Schwachstelle identifiziert wurde oder welche Aspekte der betroffenen Assets das Korrekturproblem verursachen können. Aktualisieren Sie den Status Ihrer Metriken mithilfe des zugehörigen Links **Status aktualisieren** in den Formularen für Schwachstellen, Lösungen und Korrekturaufgaben.

Verwendung der Standard-Dashboards Vulnerability Response .

Das Übersichts-Dashboard Vulnerability Response (Schwachstellenmanagement) bietet eine Ausführungsansicht für Schwachstellen und angreifbare Elemente und hilft dem Schwachstellen-Administrator, Problembereiche schnell zu identifizieren. Das Vulnerability Response Nachbesserungs-Dashboard (Nachbesserung von Schwachstellen) ermöglicht Nachbesserungsspezialisten, sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren, für die sie verantwortlich sind.

Datenvisualisierungen in den -Arbeitsbereichen Vulnerability Response .

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad aktiver Schwachstellen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen anzeigen, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Vulnerability Manager Workspace und IT Remediation Workspace erkunden.

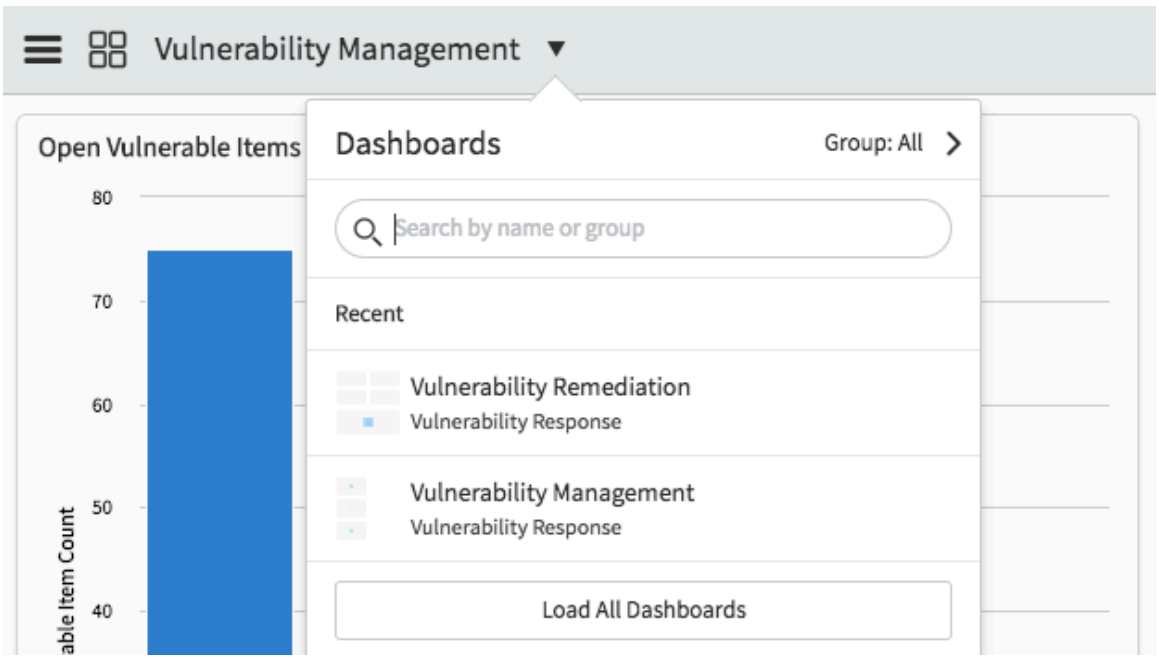
Schwachstellenanalysten können auch Standard-Dashboards Vulnerability Response verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst sowie Benutzer mit sn_vul.vulnerability_read (oder die die Rolle sn_vul.vulnerability_read erben) und pa_viewer.

Die standardmäßigen Vulnerability Response -Dashboards in der Legacy-Umgebung

Diese Berichte sind als Teil der Anwendung Performance Analytics for Vulnerability Response enthalten und erfordern kein separates Abonnement. Um eines zu öffnen, wählen Sie die Auswahlliste aus, um sie zu erweitern, und wählen Sie ein Dashboard aus. Alternativ geben Sie den Namen eines Dashboards in das Suchfeld ein.



Hinweis:

Wenn das Inhaltspaket Performance Analytics für die Anwendung Vulnerability Response installiert und aktiviert ist, wird das Dashboard für Schwachstellenmanagement (PA) automatisch im Modul „Übersicht“ angezeigt. Dieses Dashboard enthält Berichte, die alle Phasen des Lebenszyklus des Schwachstellenmanagements abdecken.

Informationen zu den Berichten, die im Performance Analytics-Inhaltspaket für Vulnerability Responseenthalten sind, finden Sie unter Dashboard für Schwachstellenmanagement [PA].

Weitere Informationen zum CISO-Dashboard und zu Berichten zur Scan-Abdeckung finden Sie unter CISO-Dashboard für Schwachstellenmanagement.

Dashboard für Schwachstellenmanagement

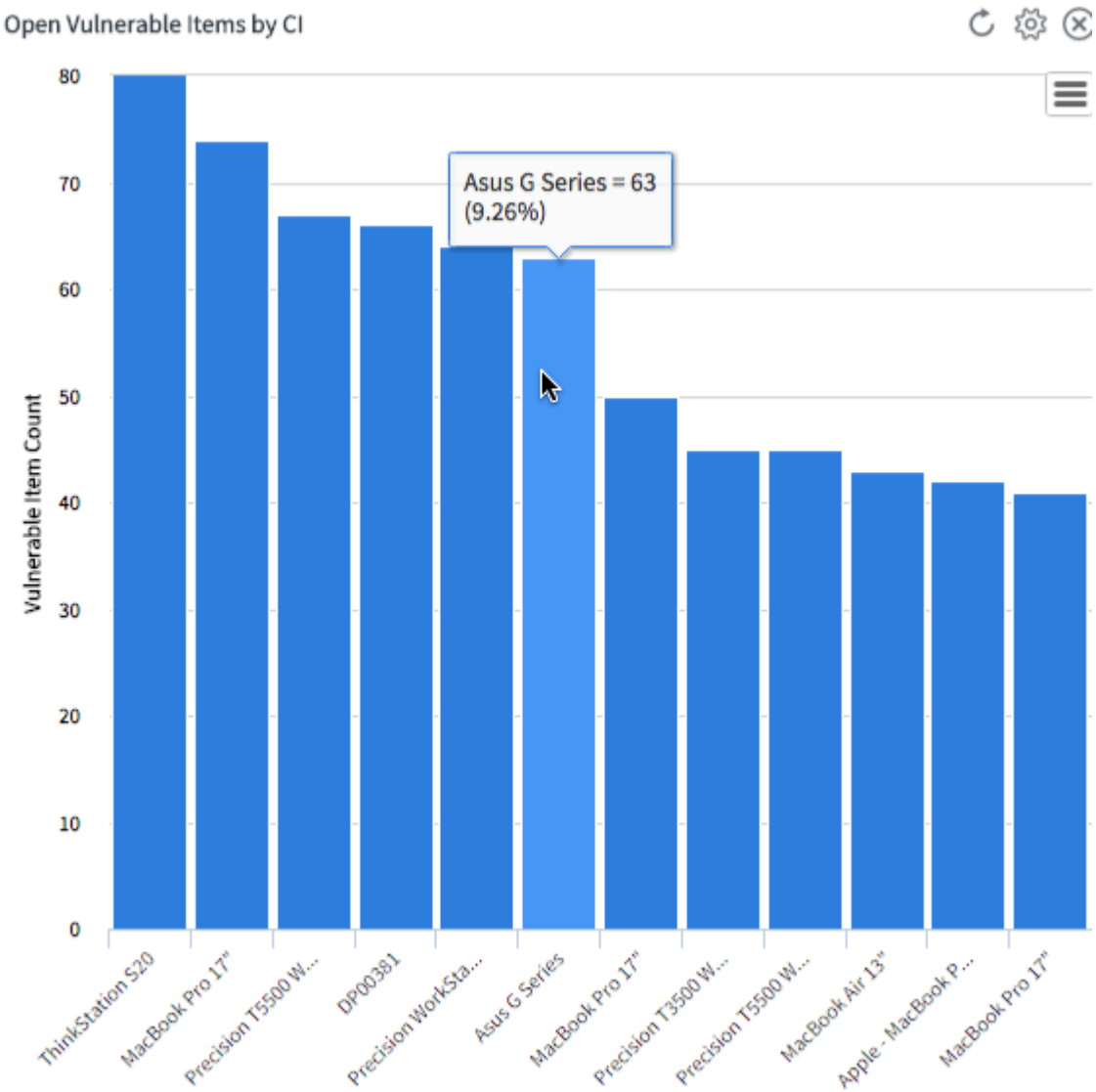
In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms (Balken, Kreis, Datenpunkt usw.) zeigen, um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn anwenderdefinierte Dashboards benötigt werden, finden Sie weitere Informationen unter Dashboards erstellen und verwenden .



Berichte mit Schwachstellenübersicht

Name	Visuell	Beschreibung
Offene angreifbare Elemente nach CI	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente an, die für jedes Configuration Item (CI) aufgezeichnet wurden, von den höchsten bis zu den niedrigsten.
Angreifbare Elemente nach Korrekturzielstatus	Balkendiagramm	Zeigt die Anzahl der angreifbaren Elemente an, die sich dem Ziel nähern, sich in der Ausführung befinden und über das Ziel hinausgehen. **Hinweis:** Elemente im Status „Zurückgestellt“, „Gelöst“ oder „Geschlossen“ werden nicht berücksichtigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte mit Schwachstellenübersicht (Fortsetzung)

Name	Visuell	Beschreibung
Zurückgestellte angreifbare Elemente, die diese Woche ablaufen	Diagramm	Zeigt die Anzahl der zurückgestellten angreifbaren Elemente an, die innerhalb von sieben Tagen reaktiviert werden sollen.
Offene angreifbare Elemente nach Schwachstelle	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente für jede Schwachstelle an, von den meisten bis zu den wenigsten.
Schwachstellen nach Modell	Balkendiagramm	Zeigt die Anzahl der für jedes Modell (CI-Klasse) erfassten angreifbaren Elemente an, von der höchsten bis zur niedrigsten.
Schwachstellen nach Woche	Trenddiagramm	Zeigt die Anzahl der pro Woche aufgezeichneten Schwachstelleneinträge an.
Modelle mit den meisten Schwachstellen	Ring	Zeigt Modelle (CI-Klassen) mit den angreifbarsten Elementen an.
Schwachstellen nach Herausgeber	Balkendiagramm	Zeigt die Anzahl der für jeden Herausgeber aufgezeichneten angreifbaren Elemente an, von der höchsten zur niedrigsten.
Schwachstellen nach Impact	Balkendiagramm	Zeigt die Anzahl der Schwachstelleneinträge für betroffene Netzwerktypen an.
Herausgeber mit den meisten Schwachstellen	Ring	Zeigt die Herausgeber mit den angreifbarsten Elementen an.
CIs mit den meisten Schwachstellen	Ring	Zeigt CIs mit den angreifbarsten Elementen an.
Schwachstellen nach Punktzahl	Balkendiagramm	Zeigt die Anzahl der Schwachstelleneinträge anhand der Schwachstellenpunktzahlen an.
Erneut geöffnete angreifbare Elemente	Liste	Listet die erneut geöffneten angreifbaren Elemente und deren Alter auf.
CIs mit den meisten Schwachstellen nach Klasse	Ring	Zeigt CIs mit den angreifbarsten Elementen an.
Alter des angreifbaren Elements	Liste	Listet die Anzahl der Tage seit dem letzten Öffnen angreifbarer Elemente auf.
CIs mit Schwachstelle nach Datum	Liste	Listet Konfigurationselemente auf, die innerhalb der letzten 30 Tage gescannt wurden.
CIs nicht gescannt	Liste	Listet Konfigurationselemente auf, die noch nie auf Schwachstellen gescannt wurden.

Dashboard für Schwachstellenkorrekturen

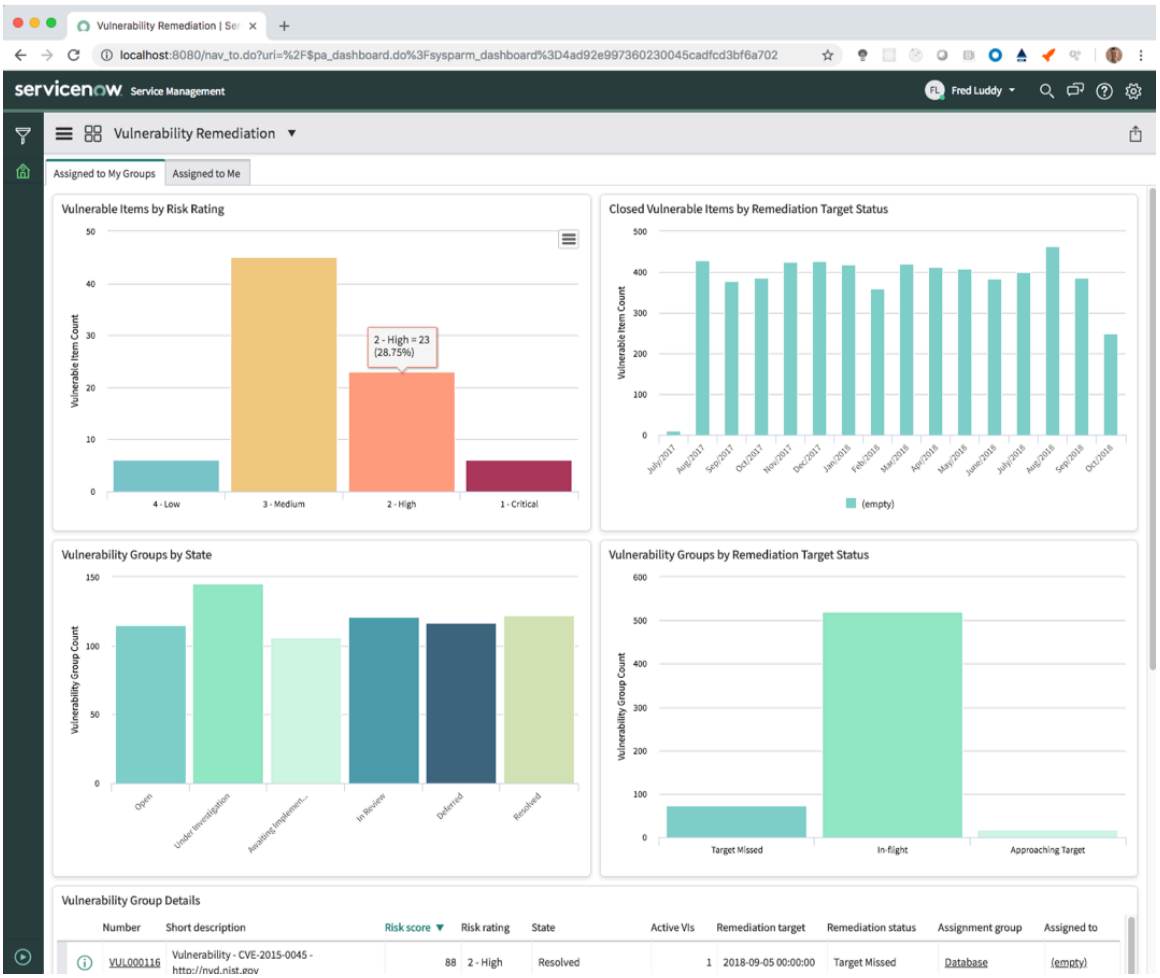
Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Dashboard für Schwachstellenkorrekturen enthält die folgenden Registerkarten: **Meinen Gruppen zugewiesen**, **Mir zugewiesen**und **Von mir angefordert**. Auf den Registerkarten Meinen Gruppen zugewiesen und Mir zugewiesen werden dieselben Berichte angezeigt. Die erste Registerkarte enthält Berichte nach den Zuweisungsgruppen, denen Sie angehören, und die zweite nach angreifbaren Elementen oder Korrekturaufgaben, die Ihnen zugewiesen sind. Auf der Registerkarte Von mir angefordert werden die von Ihnen angeforderten Falschmeldungen und Ausnahmen gemeldet.

Dashboard für Schwachstellenkorrekturen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte

„Meine Gruppen zugewiesen“ und „Mir zugewiesen“.

Name	Visuell	Beschreibung
Angreifbare Elemente nach Risikobewertung	Balken	Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne.
Geschlossene angreifbare Elemente nach Korrekturzielstatus	Balken	Anzahl der geschlossenen angreifbaren Elemente, gruppiert nach Nachbesserungszielstatus für die ausgewählte Zeitspanne.
Korrekturaufgaben nach Status	Balken	Anzahl der aktiven Korrekturaufgaben (RTs), gruppiert nach Status.
Korrekturaufgaben nach Status des Korrekturziels	Balken	Anzahl der aktiven RTs, gruppiert nach Status des Korrekturziels. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.
Details zur Korrekturaufgabe	Liste	Details zum Datensatz der Korrekturaufgabe in einer Liste.

Angefordert von mir

Name	Visuell	Beschreibung
Status von Ausnahme- und falsch positiven Anforderungen	Balken	Anzahl der aktiven Anforderungen von Ihnen.
Ablaufende zurückgestellte und falsch positive Korrekturaufgaben	Balken	Anzahl der zurückgestellten und falsch positiven Korrekturaufgaben (RTs), gruppiert nach Bis-Datum.

Dashboard „Schwachstellengenehmigungen“.

Das Dashboard „Schwachstellengenehmigungen“ enthält die folgenden Berichte für Ausnahme- und falsch positive Genehmiger.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Name	Visuell	Beschreibung
Ausnahme- und falsch positive Anforderungen nach Alter meiner ausstehenden Genehmigungen	Balken	Anzahl der für Sie ausstehenden Genehmigungen, gruppiert nach Erstellungsdatum.
Meine Genehmigung und Abgelehnte Ausnahme- und Falsch-positiv-Anforderungen	Balken	Anzahl der genehmigten oder abgelehnten Genehmigungsanforderungen, gruppiert nach Genehmigungsstatus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Visuell	Beschreibung
Alle Korrekturaufgaben nach Risikobewertung – Genehmigung ausstehend	Balken	Anzahl der Korrekturaufgaben mit ausstehender Genehmigung, gruppiert nach Risikobewertung.
Alle ausstehenden und falsch positiven Genehmigungsanforderungen gruppiert nach Grund	Balken	Anzahl der ausstehenden Genehmigungsanforderungen, gruppiert nach Grund.

Platform Analytics-Lösungen für Schwachstellenmanagement

Platform Analytics-Lösungen enthalten vorverpackte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten. Mit dieser Analytics- und Reporting-Lösung können Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse über die Erkennung bis zur Eindämmung oder Behebung nachverfolgen. Sie können Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern.

Das Inhaltspaket Performance Analytics for Vulnerability Response wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Es ist unter ServiceNow Store als separates Abonnement verfügbar.

Performance Analytics for Vulnerability Response enthält zwei Dashboards:

- Dashboard für Schwachstellenmanagement (PA).
- Risikomanagement-Dashboard „Leitender Informationssicherheitsbeauftragter“ (CISO).

Erforderliche Rollen, Installation und Anzeige der Dashboards

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Informationen zur Installation dieser Anwendung finden Sie unter Anwendung Performance Analytics for Vulnerability Response [PA] installieren und konfigurieren.

Hinweis:
Richten Sie Analytics and Reporting-Lösungen in einer Instanz außerhalb der Produktion ein, und testen Sie sie, bevor Sie sie in der Produktion aktivieren.

Lösungen für Analytik und Berichterstellung bieten alle für die Analyse von Standardanwendungen erforderlichen Konfigurationsdatensätze. Passen Sie diese Datensätze zur Verwendung in Ihrer Produktionsumgebung an. Weitere Informationen finden Sie unter Analytics and Reporting-Lösungen konfigurieren .

Um das Dashboard für Schwachstellenmanagement (PA) anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Übersicht** > **.**

Um das CISO-Dashboard für Schwachstellenmanagement anzuzeigen, navigieren Sie zu **Vulnerability Response** > **CISO-Dashboard** > **.**

Wichtige Begriffe

Performance Analytics (PA)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösung, die Managementdashboards und Berichte zu KPIs und Metriken erstellt und wichtige geschäftliche Fragen beantwortet, um die Qualität zu erhöhen und Kosten zu senken.

Angreifbares Element (VI)

Eine Sicherheitsschwachstelle, die von einem Schwachstellenscanner einer Drittpartei gemeldet wurde und für ein Konfigurationselement bzw. Configuration Item (CI) vorhanden ist

Nachbesserungsaufgabe

Korrekturaufgaben werden erstellt und automatisch IT-Teams basierend auf der Gruppe zugewiesen, die den angreifbaren Elementen in einer Korrekturmaßnahme zugeordnet ist. IT-Teams und Korrekturbesitzer zeigen Korrekturaufgaben im IT-Korrekturarbeitsbereich an. Weitere Informationen finden Sie unter Vulnerability Response Arbeitsbereiche .

.

PA-Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen von einem Business-Service, einer Aktivität oder einem Organisationsverhalten durchgeführt wird, z. B. Nicht zurückgestellte überfällige kritische angreifbare Elemente.

PA-Indikatorquelle

Datensätze, die Datensätze aus einer Tabellen- oder Datenbankansicht filtern, z. B. AE Aktiv.

Zeigen Sie Datenvisualisierungen in Echtzeit an

Um zu sehen, was heute mit den wichtigsten Elementen in Ihrer Anwendung Vulnerability Response geschieht, können Sie bestimmte Berichte im Dashboard für Schwachstellenmanagement (PA) in Echtzeit anzeigen. Durch die Anzeige dieser Berichte in Echtzeit können Sie Ihre wichtigsten angreifbaren Elemente verwalten und schnell nachbessern. Sie können die folgenden Berichte in Echtzeit anzeigen:

- Registerkarte „Übersicht“ – Angreifbare Elemente nach Zuweisungsgruppe
- Registerkarte „Angreifbare CIs“.
  - Angreifbare Configuration Items (CIs) ohne Besitzer
  - Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs
- Registerkarte Ausnahmen
  - Zurückgestellte angreifbare Elemente nach Grund
  - In Kürze ablaufende Zurückstellungsanforderungen
  - Nach CIO-Manager zurückgestellte angreifbare Elemente
- Registerkarte „Nachbesserung“ – Nicht zugewiesene angreifbare Elemente

Weitere Informationen finden Sie unter Performance Analytics for Vulnerability Response-Berichte [PA] in Echtzeit anzeigen.

Zugehörige Informationen

Analytics- und Reporting-Lösungen

Vulnerability Management CISO- Dashboard

Zeigen Sie im Vulnerability Management CISO- Dashboard Daten wie Key Performance Metrics (KPIs) zur Nachbesserung von Schwachstellen an, sehen Sie sich die höchsten Risiken an, überprüfen Sie die Scan-Abdeckung, und erfahren Sie, wie Sie Risiken senken können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Now Platform-Rollen

- sn_vul.vulnerability_c iso, um das Dashboard anzuzeigen.
- sn_vul.c iso_write, um das Dashboard zu bearbeiten.

CISO-Dashboard wird aktiviert

Um das CISO-Dashboard zu aktivieren, müssen Sie Performance Analytics für Vulnerability Response installieren und den entsprechenden Performance Analytics-Auftrag aktivieren. Weitere Informationen finden Sie unter Analytics and Reporting-Lösungen für Vulnerability Response.

Anwendungsfälle

Anwender	Dashboard-Verwendung
Chief Information Security Officers (CISOs)	Chief Information Security Officers (CISOs) können das CISO-Dashboard verwenden, um Einblicke in das Schwachstellenmanagementprogramm für ihre Organisationen zu erhalten. Das Dashboard stellt Daten bereit, mit denen sie Daten auf einen Blick erkennen können, um die Schwachstellen in ihren Umgebungen zu verringern.

Verwenden des CISO-Dashboards

Führende Benutzer, wie die Chief Information Security Officers (CISOs) in Ihrer Organisation, können das CISO-Dashboard für Vulnerability Response anzeigen, um zu verstehen, wie effektiv ihr Programm für Schwachstellenmanagement ist. Sie können das CISO-Dashboard anzeigen, indem Sie zu navigieren **Vulnerability Response** > **CISO-Dashboard**. Verwenden Sie die Filter der obersten Ebene, um Berichte nach Risikobewertung, Altersbereich oder Internetzugriff zu filtern. Einige Berichte zeigen Trenddaten über einen bestimmten Zeitraum an. Sie können den Trend der wichtigen Metriken regelmäßig anzeigen, das allgemeine Sicherheitsrisiko des Unternehmens analysieren und die Bereiche identifizieren, die verbessert werden müssen.

Ab Version 19.0 von Vulnerability Responsekann dieses Dashboard auch in der New Experience UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das **Dashboard** -Symbol. Je nach Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdownliste neben dem Namen des Dashboards. Weitere Informationen finden Sie unter Dashboards im Arbeitsbereich des Schwachstellenmanagers und Dashboards im Arbeitsbereich für IT-Fehlerkorrekturen.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Die Ausführung der geplanten Aufgaben

Führen Sie die geplanten Aufgaben in dieser Reihenfolge aus, um die Daten in den Berichten zu aktualisieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aktualisieren Sie Dashboard-Tabellen
2. [PA VR] CISO-Dashboard

Geplante Aufgaben für das CISO-Dashboard

Name der geplanten Aufgabe	Beschreibung
Aktualisieren Sie Dashboard-Tabellen	Tägliche geplante Aufgabe, die Sie vor der Aufgabe [PA VR] CISO Dashboard ausführen müssen, damit Sie die CISO-Daten erfassen können. Durch Ausführen dieser geplanten Aufgabe aktualisieren Sie die Berichte zur Scan-Abdeckung. Die aktualisierten Informationen umfassen die operativen Configuration Items (CIs), die in den letzten 90 Tagen gescannt wurden, ihre Klassen und die Gesamtzahl der operativen CIs, die diesen Klassen entsprechen. Durch die Ausführung dieser geplanten Aufgabe werden auch die Berichte auf der Registerkarte **„Empfohlene Aktionen“** aktualisiert. **Hinweis:** Operative CIs beziehen sich auf CIs, die über den Betriebsstatus Funktionsfähigverfügen.
[PA VR] CISO-Dashboard	Nachdem die geplante Aufgabe „Dashboard-Tabellen aktualisieren“ abgeschlossen ist, führen Sie diese geplante Aufgabe aus, um alle Berichte auf der Registerkarte **„CISO-Übersicht“** auszufüllen.

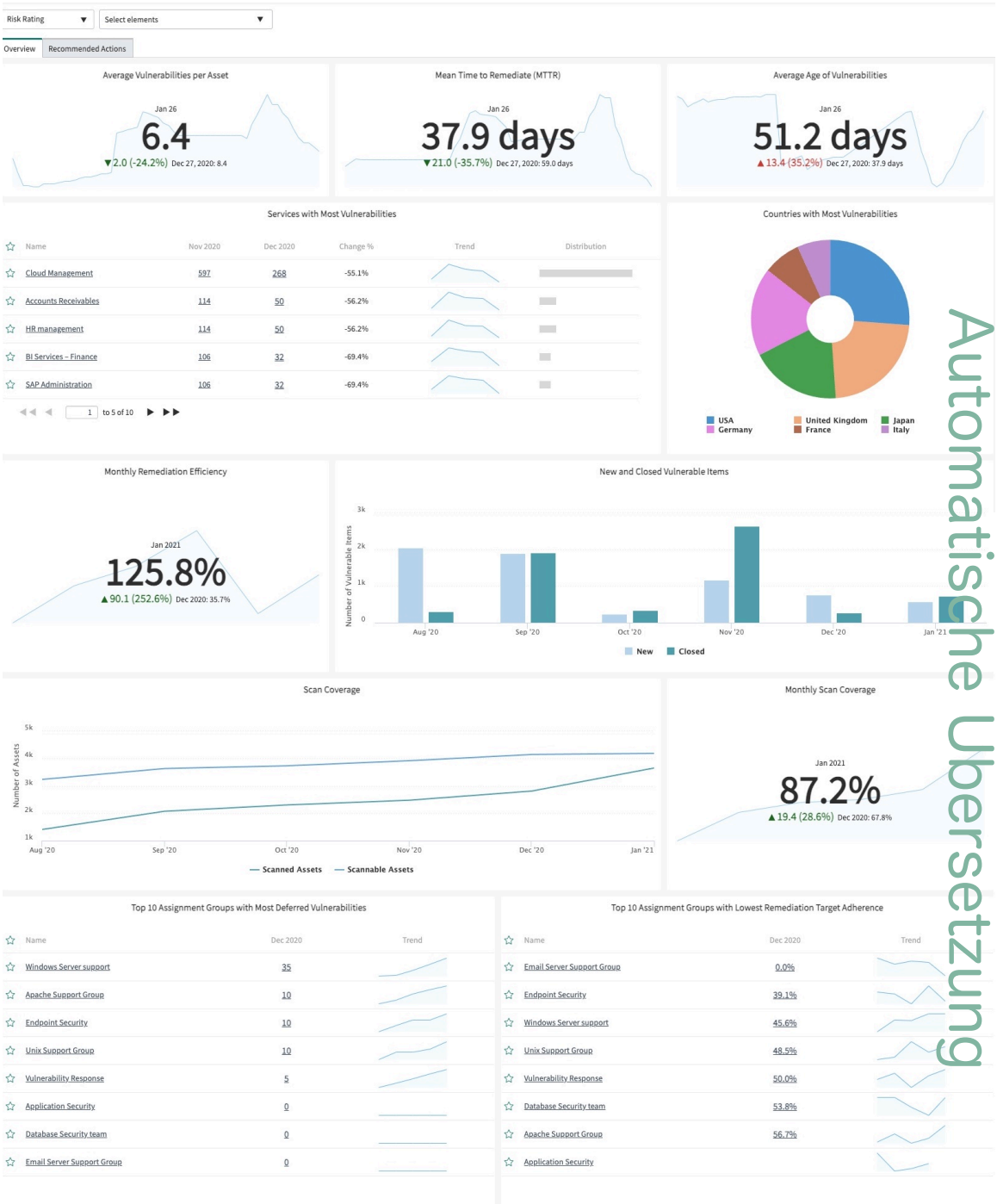
CISO-Dashboard-Registerkarten

Dieses Dashboard bietet einen Einblick in die Risiken in Schwachstellenmanagement. Sie können Schwachstellen und die zugehörigen Daten nach Region, Alter, Services und anderen Aufgliederungen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Übersicht“

Die Registerkarte „Übersicht“ enthält Berichte, die die Sicherheitslage Ihrer Organisation auf einen Blick zeigen.



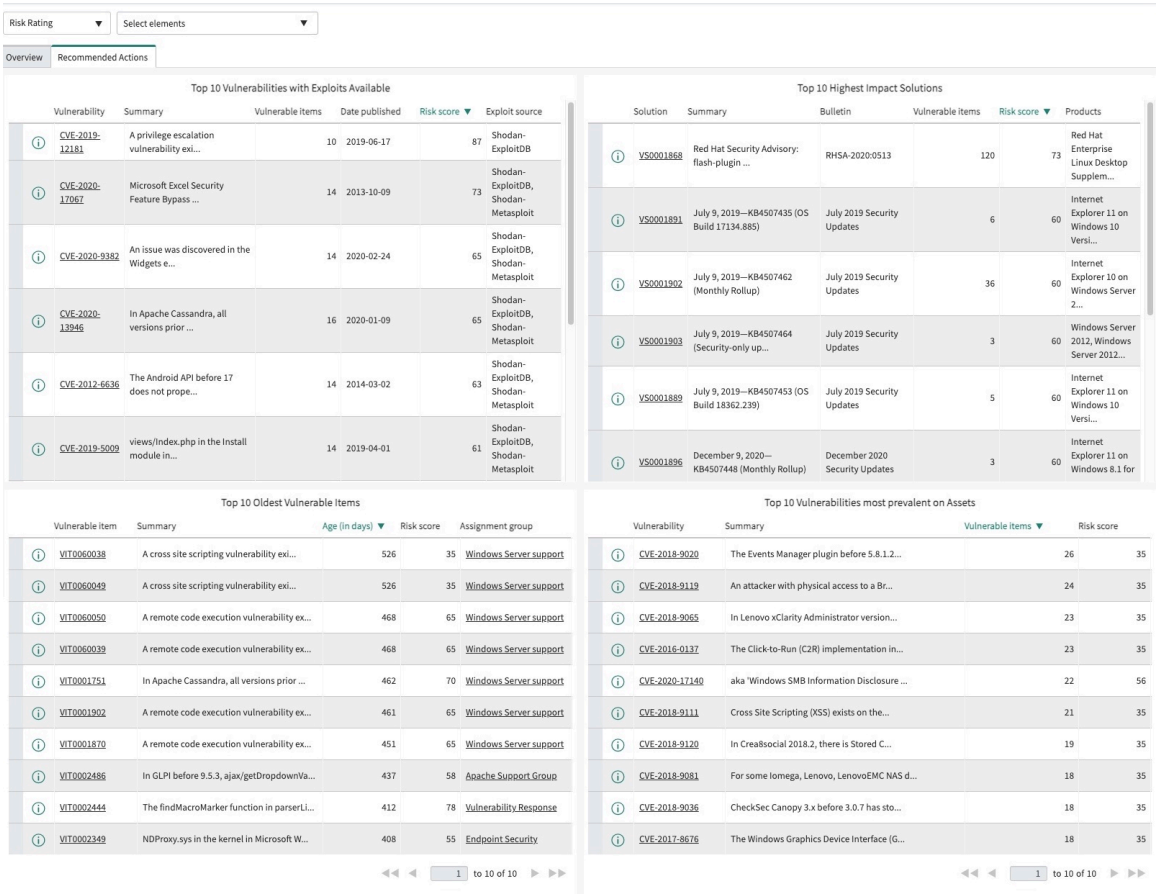
Automatische Übersetzung

Hinweis:
Der Filter der obersten Ebene kann nur für einige Berichte verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Empfohlene Aktionen“.

Die Registerkarte „Empfohlene Aktionen“ enthält Berichte, die Einblicke in ausnutzbare, veraltete und vorherrschende Schwachstellen bieten. Sie enthält auch Lösungen, die Aktionen zur Reduzierung der Risiken empfehlen. Führen Sie die regelmäßige Aufgabe **CISO-Dashboard-Tabellen aktualisieren** aus, um die Berichte auf dieser Registerkarte zu aktualisieren.



Indikatoren

Um die -Indikatoren anzuzeigen, navigieren Sie zu **Performance Analytics** > **Indikatoren**.

1. Suchen Sie auf der Seite „Indikatoren“ in der Spalte Name nach dem Namen des erforderlichen Indikators.
2. Klicken Sie auf den Namen des Indikators, um den Datensatz zu öffnen und seine Details anzuzeigen.

   Die Indikatoren für das CISO-Dashboard erfassen standardmäßig keine Datensätze. Sie können Datensätze sammeln, indem Sie das Kontrollkästchen Datensätze sammeln aktivieren.

Summierte Dauer der geschlossenen angreifbaren Elemente

„Gesamtdauer von geschlossenen AEs“ wird täglich in Tagen gemessen. Das Ziel dieses Indikators besteht darin, die Punktzahl zu minimieren.

Scannbare Assets

„Gescannte Assets“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

Services mit den meisten Schwachstellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Services mit den meisten Schwachstellen“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht darin, die Punktzahl zu minimieren.

Durchschnittliche Schwachstellen pro Asset

[[Aktive angreifbare Elemente]] / [[Aktive angreifbare Konfigurationselemente]

Geschlossene angreifbare Elemente

„Geschlossene angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

Durchschnittliche Zeit bis zur Fehlerkorrektur für angreifbare Elemente

[[Summierte Dauer der geschlossenen angreifbaren Elemente]]/[[Geschlossene angreifbare Elemente]]

Aktuelle Scan-Abdeckung

Berechnet die aktuelle Scan-Abdeckung als Prozentsatz.

Gescannte Assets

„Gescannte Assets“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

Geschlossene angreifbare Elemente (Ziel erfüllt)

„Geschlossene angreifbare Elemente (Ziel erfüllt)“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

% der geschlossenen angreifbaren Elemente, die das Ziel erfüllt haben

[[Geschlossene angreifbare Elemente (Ziel erfüllt) / Nach Monat SUM]] / [[Geschlossene angreifbare Elemente / Nach Monat SUM]] *100

Aktive angreifbare Elemente

„Aktive angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht darin, die Punktzahl zu minimieren.

Durchschnittliches Alter der angreifbaren Elemente

„Durchschnittliches Alter aktiver AEs“ wird täglich als Einheit „Tage“ gemessen. Das Ziel dieses Indikators besteht darin, die Punktzahl zu minimieren.

Hinweis:
Das Anpassen des Alters und der Berechnung des Alters der geschlossenen Elemente für angreifbare Elemente kann zu einem starken Anstieg oder Rückgang der PA-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von Alter und Alter geschlossen für VIs finden Sie im KB-Artikel KB1703270 .

Aktive angreifbare Konfigurationselemente

„Aktive angreifbare CIs“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht darin, die Punktzahl zu minimieren.

Effizienz der monatlichen Fehlerbehebung

[Anzahl der während eines Monats geschlossenen angreifbaren Elemente] / [Anzahl neuer oder erneut geöffneter angreifbarer Elemente im selben Monat]

Neue angreifbare Elemente

„Neue angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht darin, die Punktzahl zu minimieren.

Zurückgestellte angreifbare Elemente

„Zurückgestellte AEs“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht darin, die Punktzahl zu minimieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederungen

- Zuweisungsgruppe: Gilt für einige VI-Berichte.
- Risikobewertung: Gilt für AE-Berichte.
- Altersbereich: Gilt für AE-Berichte.
- Alter geschlossen: Gilt für Berichte für geschlossene VIs.
- Mit Internetzugriff: Gibt an, ob das CI zur Hardwareklasse gehört und mit dem Internet verbunden ist.
- Region: Der verwendete CMDB-CI-Parameter ist Standort. Dieser Ort gibt das Ursprungsland des Konfigurationselements an.

Hinweis:
Das Anpassen des Alters und der Berechnung des Alters der geschlossenen Elemente für angreifbare Elemente kann zu einem starken Anstieg oder Rückgang der PA-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von Alter und Alter geschlossen für VIs finden Sie im KB-Artikel KB1703270 .

Datenvisualisierungen

Name	Typ	Beschreibung
Durchschnittliche Schwachstellen pro Asset	Einzelne Punktzahl	Durchschnittliche Anzahl aktiver angreifbarer Elemente pro Konfigurationselement.
Durchschnittliche Zeit bis zur Nachbesserung (MTTR)	Einzelne Punktzahl	Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements, angezeigt als laufender 30-Tage-Durchschnitt. **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum von „Zuletzt geöffnet“ und dem Datum und der Uhrzeit der Erfassungsaufgabe.
Durchschnittliches Alter von Schwachstellen	Einzelne Punktzahl	Durchschnittliches Alter aktiver angreifbarer Elemente in Tagen.
Services mit den meisten Schwachstellen	Liste und Position	Monatlicher Durchschnitt der aktiven angreifbaren Elemente für Services in der Organisation. **Hinweis:** Informationen zum Definieren der Serviceklassifizierungen, die in den Vulnerability Response-Berichten und zugehörigen Listen angezeigt werden sollen, finden Sie auf der Registerkarte „Services“ im Dashboard für Schwachstellenmanagement [PA].
Länder mit den meisten Schwachstellen		Top 10 der Länder mit der höchsten Anzahl angreifbarer Elemente.
Effizienz der monatlichen Fehlerbehebung	Einzelne Punktzahl	Prozentsatz geschlossener angreifbarer Elemente geteilt durch neue angreifbare Elemente im aktuellen Monat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Neue und geschlossene angreifbare Elemente	Balken	Anzahl der neu importierten angreifbaren Elemente und Anzahl der geschlossenen angreifbaren Elemente in einem Monat.
Scan-Abdeckung	Linie	Anzahl der gescannten Assets im Vergleich zur Gesamtanzahl der scannbaren Assets im Zeitverlauf. Die im Widget enthaltenen CI-Klassen werden im Modul Konfiguration der Scan-Abdeckung angegeben. Informationen zur Konfiguration des Moduls „Scan-Abdeckung“ finden Sie unter Berichte zur Scan-Abdeckung konfigurieren.
Monatliche Scan-Abdeckung	Einzelne Punktzahl	Prozentsatz der gescannten Assets geteilt durch die Gesamtzahl der scannbaren Assets für den aktuellen Monat. Informationen zur Konfiguration des Moduls Scan-Abdeckung finden Sie unter Berichte zur Scan-Abdeckung konfigurieren
Top 10 der Zuweisungsgruppen mit den meisten zurückgestellten Schwachstellen	Liste und Position	Top 10 der Zuweisungsgruppen mit der höchsten Anzahl zurückgestellter angreifbarer Elemente, zurückgestellt basierend auf dem monatlichen Durchschnitt.
Top 10 der Zuweisungsgruppen mit den der niedrigsten Einhaltung des Nachbesserungsziels	Liste und Position	Top 10 Zuweisungsgruppen, deren angreifbare Elemente die geringste Einhaltung ihrer Korrekturziele aufweisen.

Empfohlene Aktionen

Name	Typ	Quelltabelle	Beschreibung
Top 10 Schwachstellen mit verfügbaren Exploits	Liste	Häufigstes Schwachstellenelement [sn_vul_analytics_top_item]	Aktive Schwachstellen mit Exploits, die für alle Threat Intelligence-Anbieter verfügbar sind, die das VR-Exploit-Framework verwenden.
Top 10 Lösungen mit der höchsten Auswirkung	Liste	Häufigstes Schwachstellenelement [sn_vul_analytics_top_item]	Bevorzugte Lösungen oder Patches mit den höchsten Risikopunktzahlen für aktive angreifbare Elemente. Dieser Bericht nutzt die Fähigkeiten von Vulnerability Solution Management (VSM), das Patches von Microsoft und Red Hat mit Schwachstellen in der Umgebung korreliert. VSM hilft bei der Identifizierung der bevorzugten Lösung für Schwachstellen.
Top 10 der ältesten angreifbaren Elemente	Liste	Häufigstes Schwachstellenelement [sn_vul_analytics_top_item]	Aktive angreifbare Elemente mit dem höchsten Alter. Lösen Sie diese Elemente, um das durchschnittliche Alter von Schwachstellen auf der Registerkarte Übersicht zu senken.
Die 10 häufigsten	Liste	Häufigstes Schwachstellenelement [sn_vul_analytics_top_item]	Aktive angreifbare Elemente, die für die höchste Anzahl von Assets verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Empfohlene Aktionen (Fortsetzung)

Name	Typ	Quelltabelle	Beschreibung
Schwachstellen für Assets			

Konfigurieren Sie Berichte zur Scan-Abdeckung

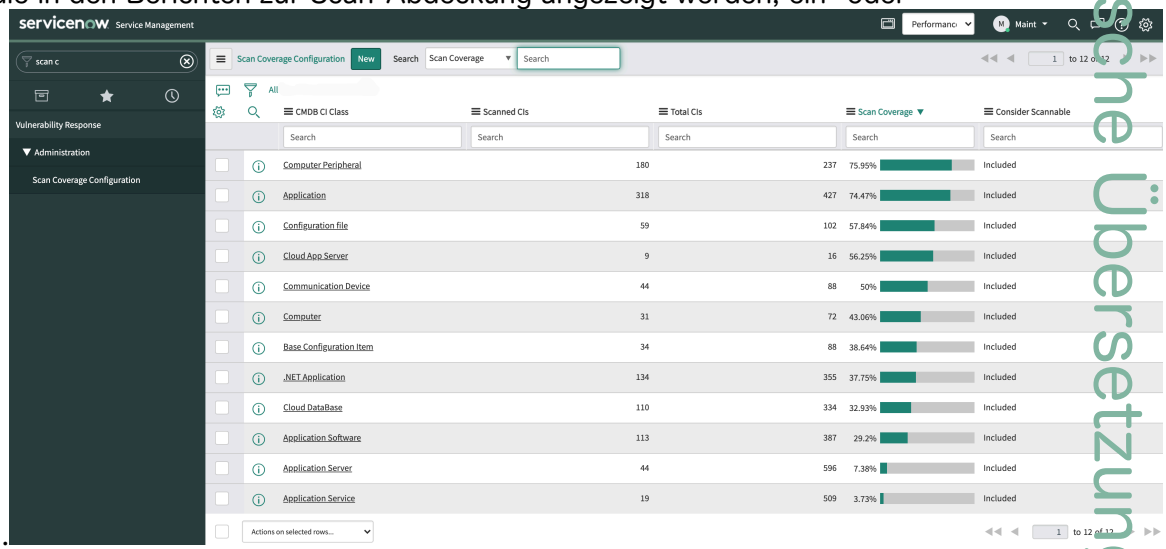
Ermöglichen Sie Ihren Anwendern, Berichte zur Scan-Abdeckung über das CISO-Dashboard auszuführen. Mit diesen Berichten können Ihre Benutzer sehen, wie hoch die Scan-Abdeckung der Organisation über einen bestimmten Zeitraum ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Warum und wann dieser Vorgang ausgeführt wird

Die Scan-Abdeckung zeigt die Anzahl der Assets an, die in den letzten 90 Tagen von den Schwachstellenscannern für die verschiedenen Klassen gescannt wurden. Diese Assets werden mit der Anzahl scannbarer Assets in Configuration Management Database (CMDB)verglichen. Standardmäßig enthält das Modul „Konfiguration der Scan-Abdeckung“ CI-Klassen CMDB, mit denen mindestens ein gescanntes Asset abgeglichen wurde. Sie können eine CI-Klasse aus CMDB zum Bericht „Scan-Abdeckung“ hinzufügen, der im CISO-Dashboard angezeigt wird. Sie können CMDB CI-Klassen, die in den Berichten zur Scan-Abdeckung angezeigt werden, ein- oder ausschließen.



Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Konfiguration der Scan-Abdeckung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Konfiguration der Scan-Abdeckung“.

Feld	Beschreibung
CMDB-CI-Klasse	CI-Klasse, die dem Bericht zur Scan-Abdeckung im CISO-Dashboard hinzugefügt werden muss.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn eine CI-Klasse bereits im Modul „Konfiguration der Scan-Abdeckung“ vorhanden ist, wird sie nicht in diese Liste aufgenommen.
Als scannbar betrachten	Option zum Definieren, ob die CI-Klasse enthalten sein muss oder nicht. Fügen Sie eine CI-Klasse hinzu, wenn deren Daten den Scan-Abdeckungsberichten hinzugefügt werden sollen. Wenn dies ausgeschlossen ist, werden die Daten für diese CI-Klasse nicht hinzugefügt.

4. Klicken Sie auf **Absenden**.

Konfigurieren Sie die PA-Indikatoren für das CISO-Dashboard

Überwachen Sie die automatisierten und formulierten CISO-Indikatoren, damit Sie die Schwachstellendaten in Ihrer Instanz verwalten können.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response verfügt sowohl über automatisierte als auch formulierte Indikatoren.

Wichtige Begriffe

Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen von einem Business-Service, einer Aktivität oder einem Organisationsverhalten durchgeführt wird. Ein Beispiel ist ein aktives angreifbares Element.

Indikatorquelle

Datensätze, die aus Datensätzen bestehen, die aus einer Tabellen- oder Datenbankansicht gefiltert wurden, um die Effizienz zu erhöhen. Ein Beispiel ist AE.Aktiv (mit Internetzugriff).

Aufgliederungen

Aufgliederungen filtern und gruppieren Indikatorpunktzahlen anhand qualitativer Attribute wie Priorität, Kategorie und Zuweisungsgruppe.

Geplante Aufgaben

Geplante Aufgaben werden ausgeführt, um die Indikatorquelldaten zu füllen. Die tägliche geplante Aufgabe „[PA VR] CISO Dashboard“ ist standardmäßig deaktiviert. Sie müssen es aktivieren, um Indikatorpunktzahlen für das CISO-Dashboard zu sammeln.

Prozedur

1. Navigieren zu **Alle** > **Performance Analytics** > **Indikatoren** und wählen Sie eine der folgenden Optionen:
   - Automatisierte Indikatoren
   - Formelindikatoren

   Weitere Informationen zu -Indikatoren finden Sie unter Performance Analytics-Indikatoren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Suchen Sie auf der Seite „Indikatoren“ in der Spalte Name nach dem Namen des erforderlichen Indikators.
3. Klicken Sie auf den Namen des Indikators, um den Datensatz zu öffnen und seine Details anzuzeigen.

Die Indikatoren für das CISO-Dashboard erfassen standardmäßig keine Datensätze. Sie können Datensätze sammeln, indem Sie das Kontrollkästchen **Datensätze sammeln** aktivieren.

Hinweis:
Das Aktivieren der Datensätze erfassen in einem Indikator kann zu Leistungsproblemen führen, da z. B. viel mehr Zeit und Arbeitsspeicher benötigt werden, als für die Ausführung des Datensammlungsauftrags erforderlich ist.

Die maximale Anzahl von Zeilen, die Sie für eine Indikatorquelle abrufen können, beträgt 1.000.000.

Integritäts-Dashboard von SecOps Vulnerability Response

Das Dashboard für die Vulnerability Response-Integrität ist ein Tool, mit dem Unternehmen umfassende Einblicke in die Implementierung und Verwendung ihrer Vulnerability Response-Anwendungen erhalten können.

Die allgemeine Integritätsbewertung wird durch die Zusammenfassung verschiedener kritischer Faktoren für Konfiguration, Implementierung, Integration, Leistung, Daten und Prozess bestimmt. Zeigen Sie das Aggregierte Dashboard für jede Kategorie für die folgenden Anwendungen an:

- Vulnerability Response
- Application Vulnerability Response
- Container Vulnerability Response
- Konfigurations-Compliance

Installieren des SecOps Vulnerability Response Health-Dashboards

Um das SecOps Vulnerability Response Health Dashboard für Vulnerability Response -Anwendungen in Ihrer Now Platform-Instanz zu installieren und zu konfigurieren, navigieren Sie zu ServiceNow® Store, und aktivieren Sie das Plugin „SecOps Health Analytics“ (sn_sec_analytics).

Erforderliche Now Platform-Rollen

Erforderliche Rolle: sn_sec_analytics.admin, sn_sec_analytics.read

Geplante Aufgabe

Um die geplante Aufgabe anzuzeigen, navigieren Sie zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben** > **Erfassen Sie Metriken des Integritätsdashboards**. Die geplante Aufgabe „Dashboard-Metriken zur Integrität erfassen“ wird täglich um 00:00 Uhr ausgeführt. Es generiert die Daten für das Dashboard „Dashboard SecOps Vulnerability Response Health“. Sie können die geplante Aufgabe auch manuell ausführen.

Anwendungsfälle

Beispiele dafür, wie Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie in den folgenden Anwendungsfällen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
Schwachstellenadministrator	Hilft Ihnen, die Integritätspunktzahl der Vulnerability Response -Anwendungen zu verstehen. Es ist auch hilfreich, die Bereiche hervorzuheben, die verbessert werden müssen. Das Vulnerability Response Health-Dashboard befasst sich nur mit der Integrität von Implementierung und Nutzung. Es unterstützt nicht die Verwaltung von Schwachstellen oder Assets.
Supportadministrator	Hilft Ihnen, Leistungs-, Anpassungs- und Konfigurationsprobleme mithilfe von KPIs zu identifizieren. Basierend auf der Anwendungsintegrität können Sie eine zusätzliche Analyse durchführen oder den Benutzern eine Empfehlung geben.
Implementierungspartner	Hilft Ihnen, die Integrität der Vulnerability Response -Implementierung für Konfigurationen, Add-Ons, Anpassungen und Integrationen zu bewerten und Verbesserungsempfehlungen für die Benutzer bereitzustellen.

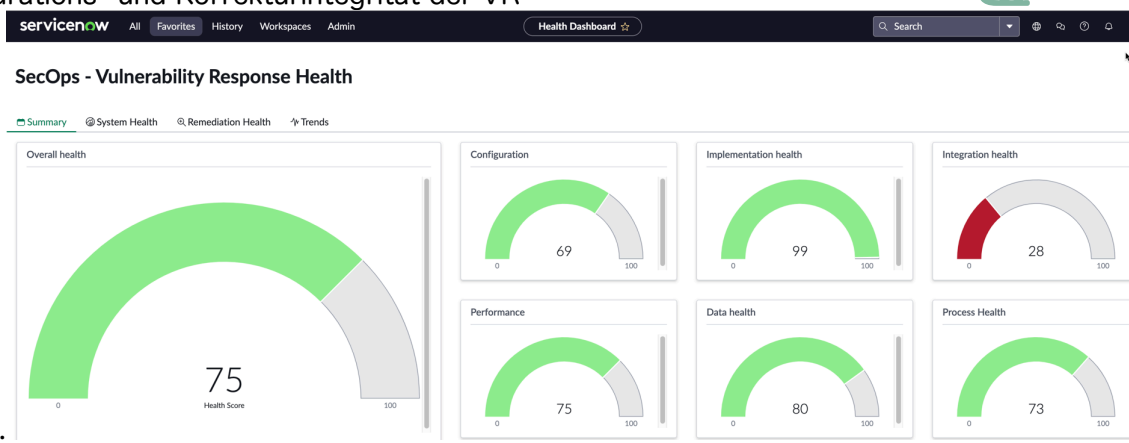
Die Registerkarten des SecOps Vulnerability Response-Integritäts-Dashboards

Um das Dashboard für die Integrität von SecOps Vulnerability Response anzuzeigen, navigieren Sie zu **Security Operations-Integrität** > **Vulnerability Response-Integrität**. Jede Farbe im Dashboard steht für Folgendes:

- Grün: Sicher
- Gelb: Warnung
- Rot: Kritisch

Registerkarte „Zusammenfassung“

Dieses Dashboard kommuniziert die Gesamtintegritätspunktzahl für die Konfigurations- und Korrekturintegrität der VR-Anwendungen.

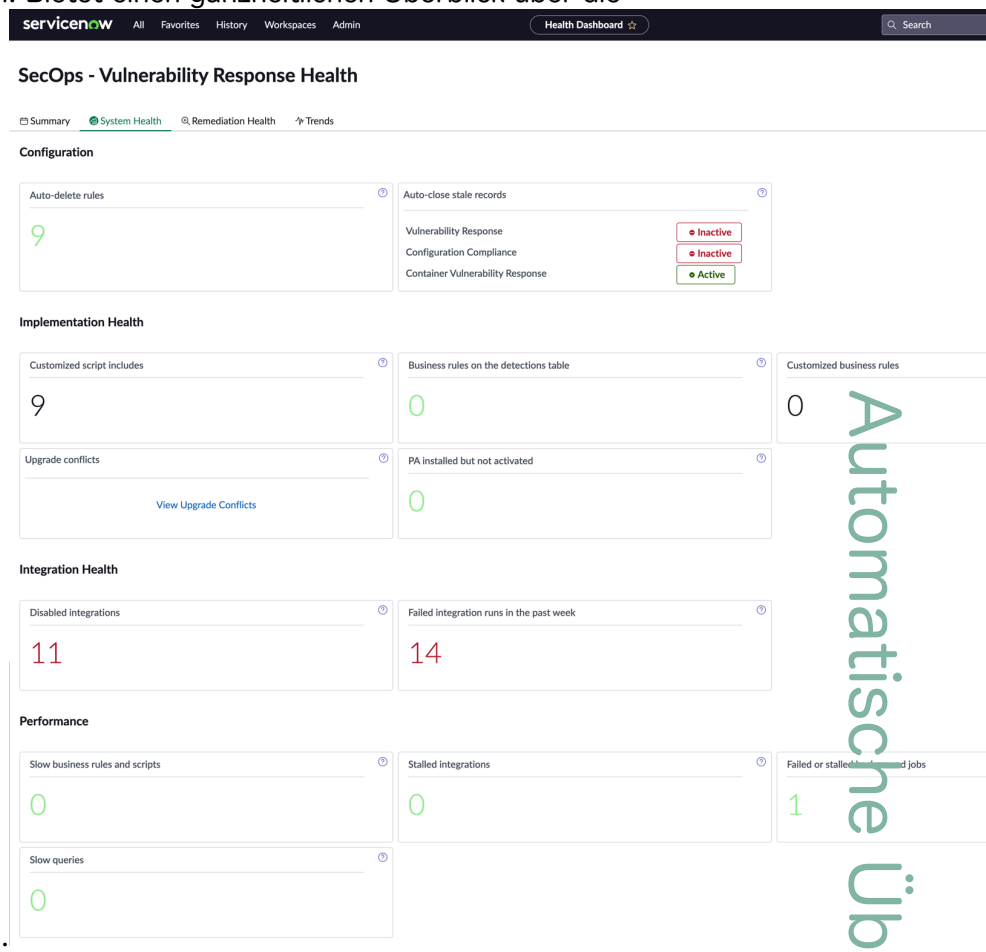


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Systemintegrität“.

Dieses Dashboard zeigt die Konfigurations- und Integrationsintegrität Ihrer -Implementierung an. Bietet einen ganzheitlichen Überblick über die Implementierungsleistung.

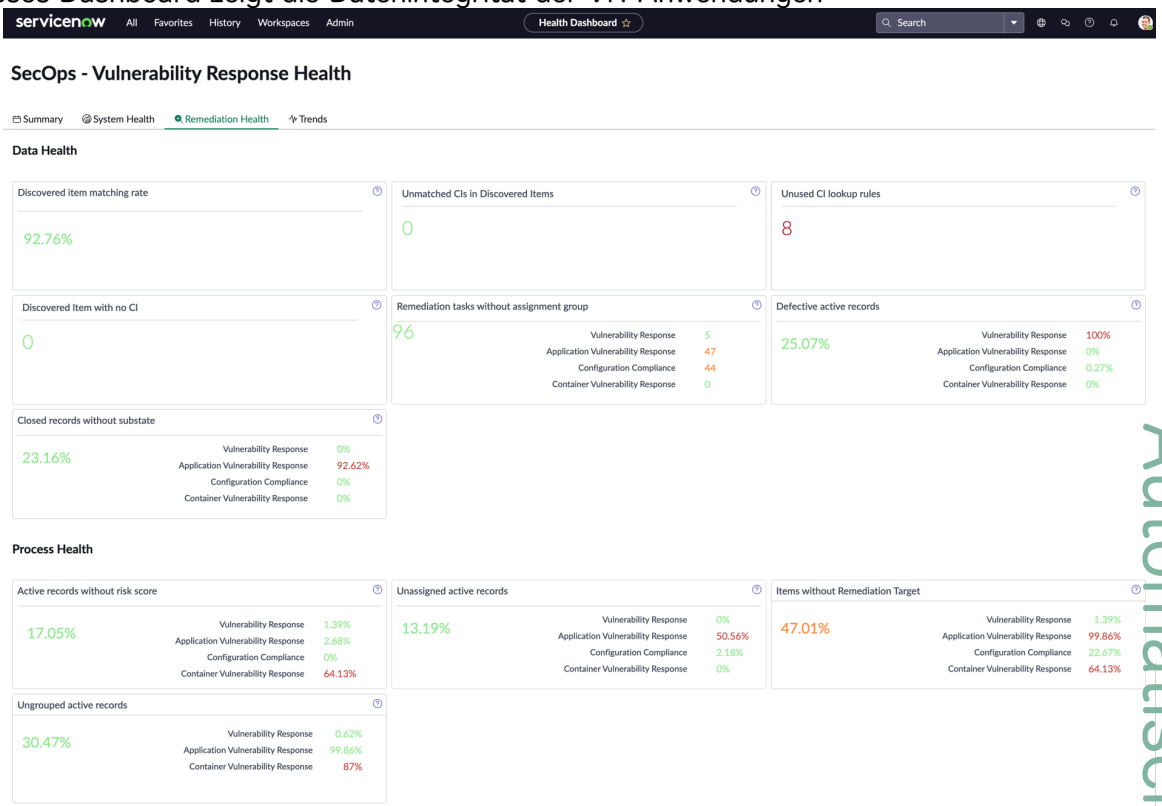


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte Korrekturintegrität

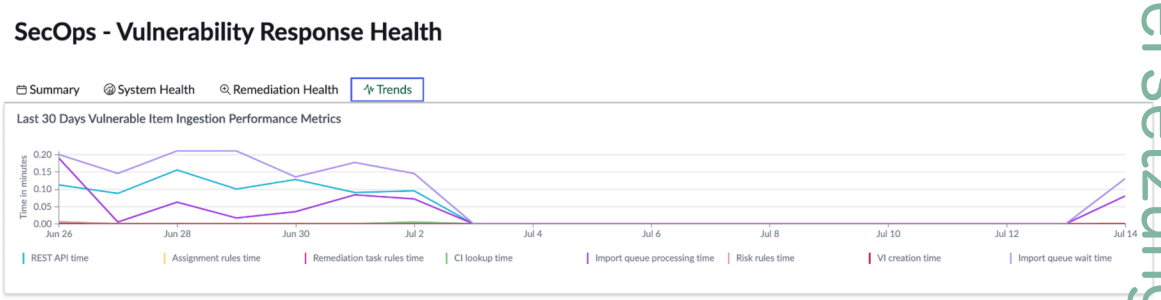
Dieses Dashboard zeigt die Datenintegrität der VR-Anwendungen



an.

Registerkarte „Trends“.

Dieses Dashboard zeigt die Trends für die Leistungsmetriken zur Erfassung angreifbarer Elemente in den letzten 30 Tagen für die VR-Anwendungen



an.

Berichte

Hinweis:
Die Schwellenwerte sind Teil des Basissystems. Sie können die Werte entsprechend Ihren Anforderungen konfigurieren.

Zusammenfassung

Titel	Beschreibung
Integrität gesamt	Gesamtintegritätspunktzahl für die VR-Anwendungen. Weitere Informationen finden Sie in den Berichten für die Metriken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenfassung (Fortsetzung)

Titel	Beschreibung
Konfiguration	Gesamtkonfigurationsintegrität der VR-Anwendungen.
Integrität der Implementierung	Gesamtintegrität der Implementierung der VR-Anwendungen.
Integrität der Integration	Gesamtintegritätsintegrität der VR-Anwendungen.
Performance	Gesamtpunktzahl zur Leistungsintegrität der VR-Anwendungen.
Datenintegrität	Gesamtdatenintegrität der VR-Anwendungen.
Prozessintegrität	Gesamtpunktzahl der Prozessintegrität der VR-Anwendungen.

Systemintegrität

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
Konfiguration				
Regeln für automatische Löschung	Zeigt die Anzahl der aktivierten Regeln für die automatische Löschung an.	Überprüfen und lösen Sie die inaktiven Regeln für die automatische Löschung.	3	1
Veraltete Datensätze automatisch schließen	Schließt veraltete Erkennungen automatisch. Weitere Informationen finden Sie im Thema „Veraltete Erkennungen in Vulnerability Response automatisch schließen“ in servicenow.com/docs.	Reduzieren Sie die Menge der veralteten Erkennungen. Aktivieren Sie diese Option, um die veralteten Erkennungen zu schließen, die nicht von den Scannern geschlossen werden.	3	1
Integrität der Implementierung				
Anwenderdefinierte Skripteinbindungen	Anzahl der „Skripteinbindungen“ angepasst.	Minimieren Sie anwenderdefinierte Skripteinbindungen, um Upgrades zu erleichtern.	10	12
Business-Regeln in der Erkennungstabelle	Anzahl der anwenderdefinierten Business-	Minimieren Sie Business-Regeln, um Upgrades zu erleichtern.	4	8

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemintegrität (Fortsetzung)

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
	Regeln in der Erkennungstabelle.			
Anwenderdefinierte Business-Regeln	Anzahl der anwenderdefinierten Business-Regeln vor der Erstellung von Datensätzen in der CMDB.	Standard-Business-Regeln für Datensätze verwenden.	5	8
Upgrade-Konflikte	Konflikte wie Business-Regeln und Skripts wurden bei einem Upgrade identifiziert.	Überprüfen und lösen Sie die Upgrade-Konflikte.	10	15
PA installiert, aber nicht aktiviert	Gibt an, ob das Performance Analytics-Dashboard nicht aktiviert ist.	Aktivieren Sie das PA-Dashboard.	10	15
Integrität der Integration				
Deaktivierte Integrationen	Anzahl der Integrationen, die deaktiviert wurden.	Überprüfen und aktivieren Sie die erforderlichen Integrationen.	6	9
Fehlgeschlagene Integrationsausführungen in der letzten Woche	Anzahl der Integrationsausführungen, die in der letzten Woche nicht erfolgreich waren.	Überprüfen und beheben Sie die Ursache der fehlgeschlagenen Integrationsausführungen.	9	12
Performance				
Langsame Geschäftsregeln und Skripts	Business-Regeln und Skripts mit einer durchschnittlichen Ausführungszeit von mehr als 10 ms und einer Ausführungsanzahl von mehr als 10.000.	Überprüfen und beheben Sie langsam laufende Business-Regeln.	10	15
Stillgelegte Integrationen	Anzahl der Integrationen, bei denen vor dem Abschluss eine Zeitüberschreitung aufgetreten ist.	Überprüfen und beheben Sie die Ursache der blockierten Integrationen.	10	15

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemintegrität (Fortsetzung)

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
Fehlgeschlagene oder angehaltene Hintergrundaufträge	Fehlgeschlagene oder abgelaufene Hintergrundaufträge in der letzten Woche.	Überprüfen und beheben Sie die Ursache der fehlgeschlagenen Aufgaben.	5	10
Langsame Abfragen	Abfragen mit einer durchschnittlichen Ausführungszeit von mehr als 10 ms und einer Ausführungsanzahl von mehr als 10.000.	Überprüfen und beheben Sie langsam laufende Business-Regeln.	10	15

Integrität der Korrektur

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
Datenintegrität				
Übereinstimmungsrate des erkannten Elements	Anzahl der erkannten Elemente, die vorhandenen CIs entsprechen.	Überprüfen Sie den Zustand Ihrer CMDB und der Logik der CI-Suchregeln.	50	20
Nicht abgeglichene CIs in erkannten Elementen	Erkannte Elemente in nicht abgeglichenem Status.	Überprüfen Sie den Zustand Ihrer CMDB und der Logik der CI-Suchregeln.	9	12
Nicht verwendete CI-Suchregeln	CI-Suchregeln, die keinem erkannten Element zugeordnet sind.	Ändern Sie den Status der nicht verwendeten CI-Suchregeln in inaktiv.	4	6
Erkanntes Element ohne CI	Erkanntes Element ohne Konfigurationselement	Überprüfen Sie die CI-Suchregeln, und wenden Sie sie erneut an.	9	12
Fehlerhafte aktive Datensätze	Datensätze ohne Konfigurationselement oder Schwachstelle.	CIs mit der CMDB-Option für CI-Lebenszyklusmanagement außer Kraft setzen.	40	60

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrität der Korrektur (Fortsetzung)

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
		Hinweis: Das direkte Löschen von CIs kann zu verwaisten VITs führen.		
Korrekturaufgaben ohne Zuweisungsgruppe	Aktive Korrekturaufgaben, deren Zuweisungsgruppe noch zugewiesen werden muss.	Weisen Sie einer Zuweisungsgruppe Korrekturaufgaben zu, und überprüfen Sie die vorhandenen Zuweisungsregeln.	40	60
Geschlossene Datensätze ohne Substatus	Datensätze, die ohne Substatus geschlossen werden.	Geben Sie Informationen im Feld Grund an, wenn Sie die Datensätze schließen.	40	50
Prozessintegrität				
Aktive Datensätze ohne Risikopunktzahl	Aktive Datensätze mit einer Risikopunktzahl von 0 oder ohne zugewiesene Risikopunktzahl.	Überprüfen und lösen Sie die Risikoregeln.	40	60
Nicht zugewiesene aktive Datensätze	Datensätze ohne eine Zuweisungsgruppe.	Weisen Sie den Datensätzen eine Gruppe zu, und überprüfen Sie die vorhandenen Zuweisungsregeln.	30	50
Elemente ohne Korrekturziel	Elemente ohne Korrekturzieldatum.	Überprüfen und lösen Sie die Korrekturzielregeln. Diese Regeln müssen alle Datensätze enthalten.	30	50
Nicht gruppierte aktive Datensätze	Datensätze, die nicht in einer Regel für Korrekturaufgaben enthalten sind.	Überprüfen Sie die Regeln für Korrekturaufgaben.	40	60

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trends

Titel	Beschreibung
Leistungsmetriken zur Erfassung von angreifbaren Elementen in den letzten 30 Tagen	Durchschnittliche Zeit, die in den letzten 30 Tagen für die Erfassung angreifbarer Elemente und die Verarbeitung mehrerer Regeln benötigt wurde.

Die Schwellenwerte werden geändert

Sie können die Schwellenwerte für die Daten des Dashboards „SecOps VR Health“ entsprechend Ihren Anforderungen ändern.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Security Operations-Integrität** > **Konfiguration** > **Metriken**.
2. Öffnen Sie auf der Datenseite des Integritäts-Dashboards den Datensatz, den Sie ändern möchten.
3. Aktualisieren Sie den Datensatz, und speichern Sie ihn.

Vulnerability Management (PA) -Dashboard

Verfolgen Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Behebung. Sie können Berichte beispielsweise nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern. Erhalten Sie schnell Einblicke in Ihre Schwachstellen und die betroffenen Business Services.

Erforderliche Now Platform-Rollen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst und Benutzer mit sn_vul.vulnerability_read (oder Erben der Rolle sn_vul.vulnerability_read) und pa_viewer.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
IT-Manager, IT-Analysten, Verantwortliche für die Nachbesserung von Schwachstellen	Unterstützen Sie Ihre Organisation bei der Bewältigung der Zunahme von Security Incidents aufgrund von ausgenutzten Schwachstellen, indem Sie effizient ermitteln, welche angreifbaren Elemente das meiste Risiko darstellen. Diese Dashboards bieten eine grafische Ansicht der Aktivität angreifbarer Elemente und helfen beim Entwerfen von Korrekturplänen und Statusfortschritten. Sie können sich auf die KPIs konzentrieren, die kritischen betroffenen Assets und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind.

Um das Dashboard für Schwachstellenmanagement (PA) anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Übersicht**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sehen Sie sich Berichte an, die Trenddaten im Zeitverlauf zeigen. Berichte mit Echtzeitdaten werden unten aufgelistet. Zeigen Sie regelmäßig Trends wichtiger Metriken an, um Ihre allgemeinen Geschäftsprozesse zu analysieren und Verbesserungsbereiche zu identifizieren.

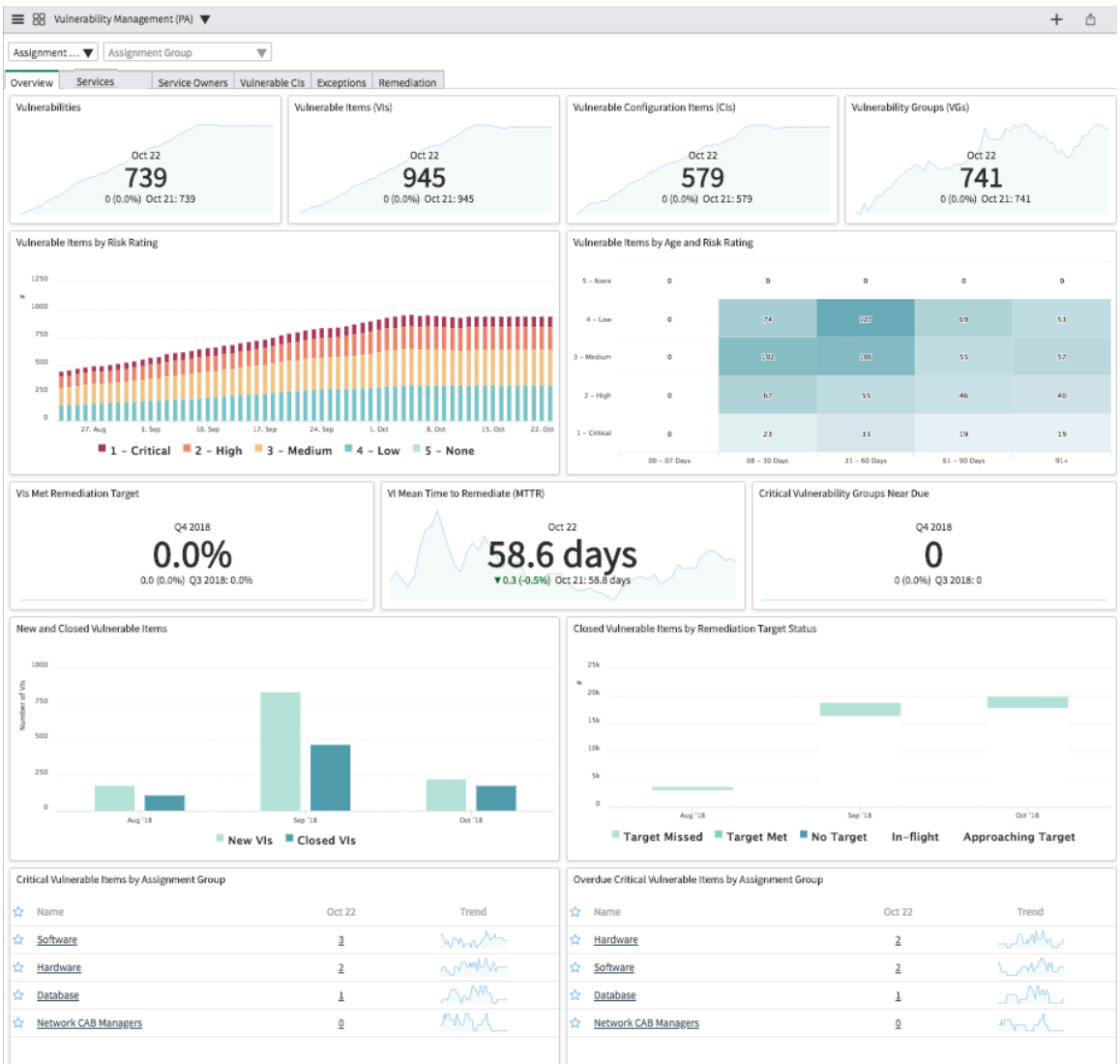
Weitere Informationen zum Anzeigen Ihrer PA-Berichte mit Echtzeit-Punktzahlen finden Sie unter Performance Analytics for Vulnerability Response-Berichte [PA] in Echtzeit anzeigen.

Registerkarten des Dashboards für Schwachstellenmanagement [PA].

Registerkarte „Übersicht“

Dieses Dashboard kommuniziert KPIs für Schwachstellenrisiko und -verbreitung, betroffene Assets, Einhaltung der Korrekturziele und Fortschritt der Korrektur.

Auf der Registerkarte „Übersicht“ können Sie den Bericht „Kritische angreifbare Elemente nach Zuweisungsgruppe“ anzeigen, der basierend auf der geplanten Aufgabe ausgeführt wird.

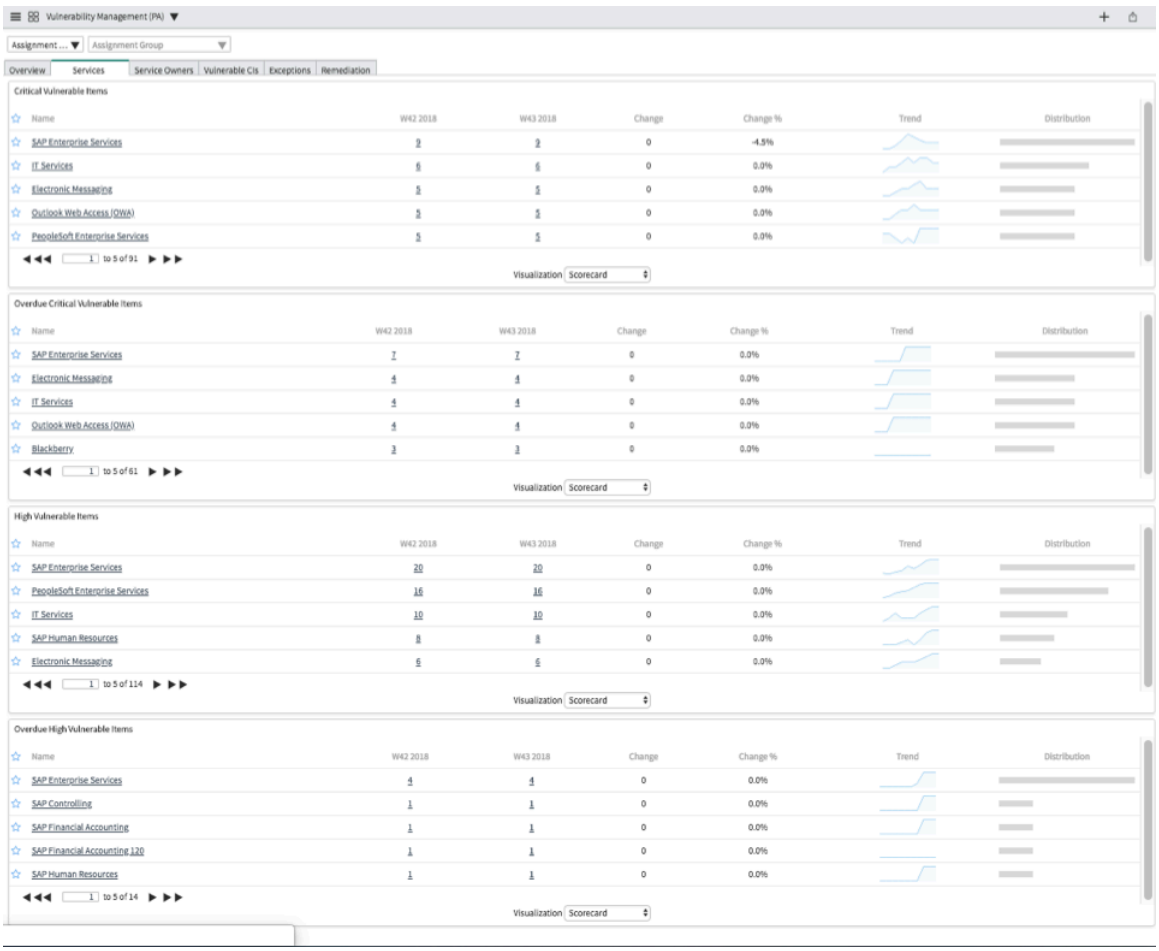


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Business-Services“.

Dieses Dashboard macht Schwachstellenrisiken auf Business-Service-Ebene verfügbar. Die Weitergabe dieser Informationen im gesamten Unternehmen kann Servicemanager dabei unterstützen, Schwachstellen schnell und proaktiv zu beheben, und das Unternehmen zu einem Modell der geteilten Verantwortung für die Informationssicherheit führen.

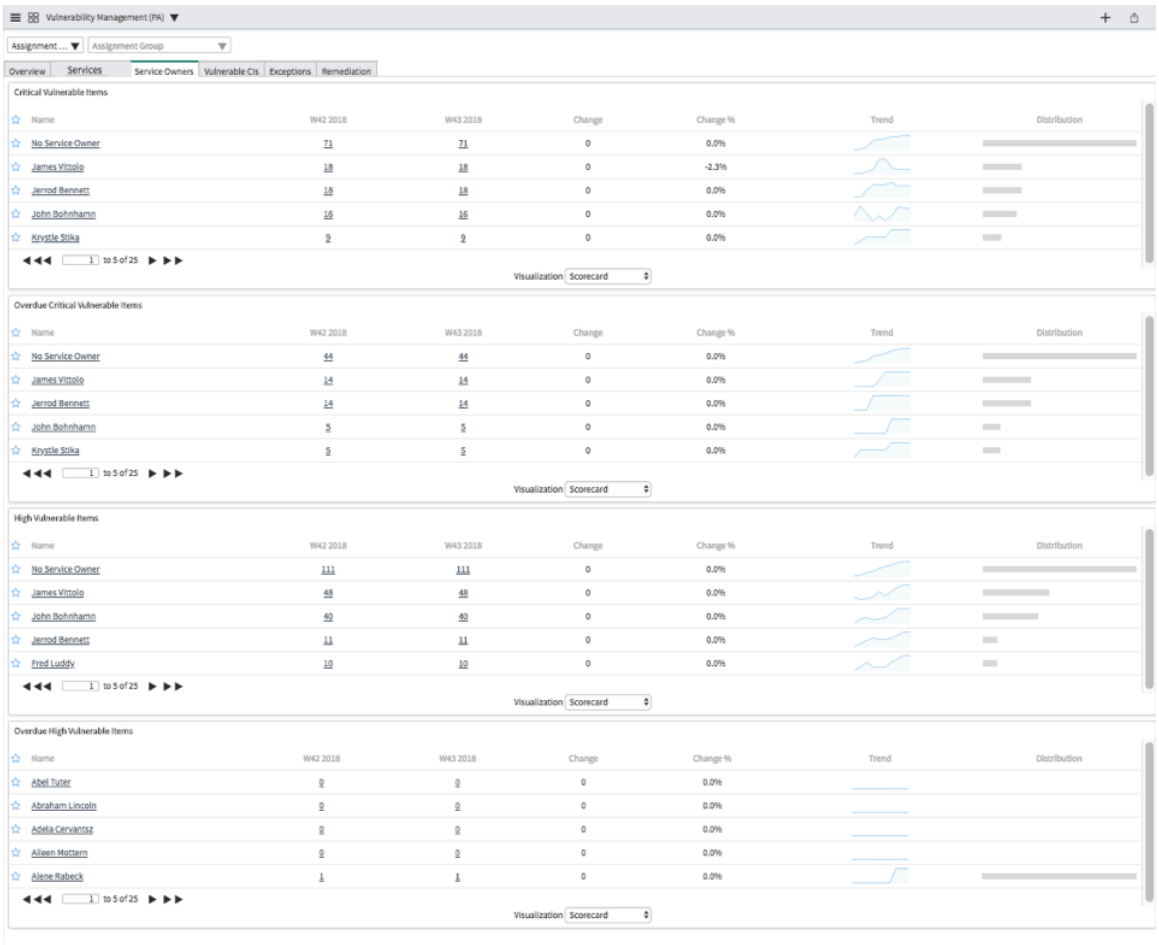
Mit der Systemeigenschaft `sn_vul.service_classifications`können Sie die Serviceklasse in technische Services oder Anwendungsservices ändern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Serviceverantwortliche“.

Dieses Dashboard fasst das Schwachstellenrisiko von der Business-Serviceebene bis zu den Serviceverantwortlichen zusammen – den Führungskräften, die für diese Business-Services verantwortlich sind. Zeigt an, welche Führungskräfte das meiste Schwachstellenrisiko übernehmen und welche möglicherweise die meiste Hilfe benötigen, um sofortige Korrekturmaßnahmen zu fördern.



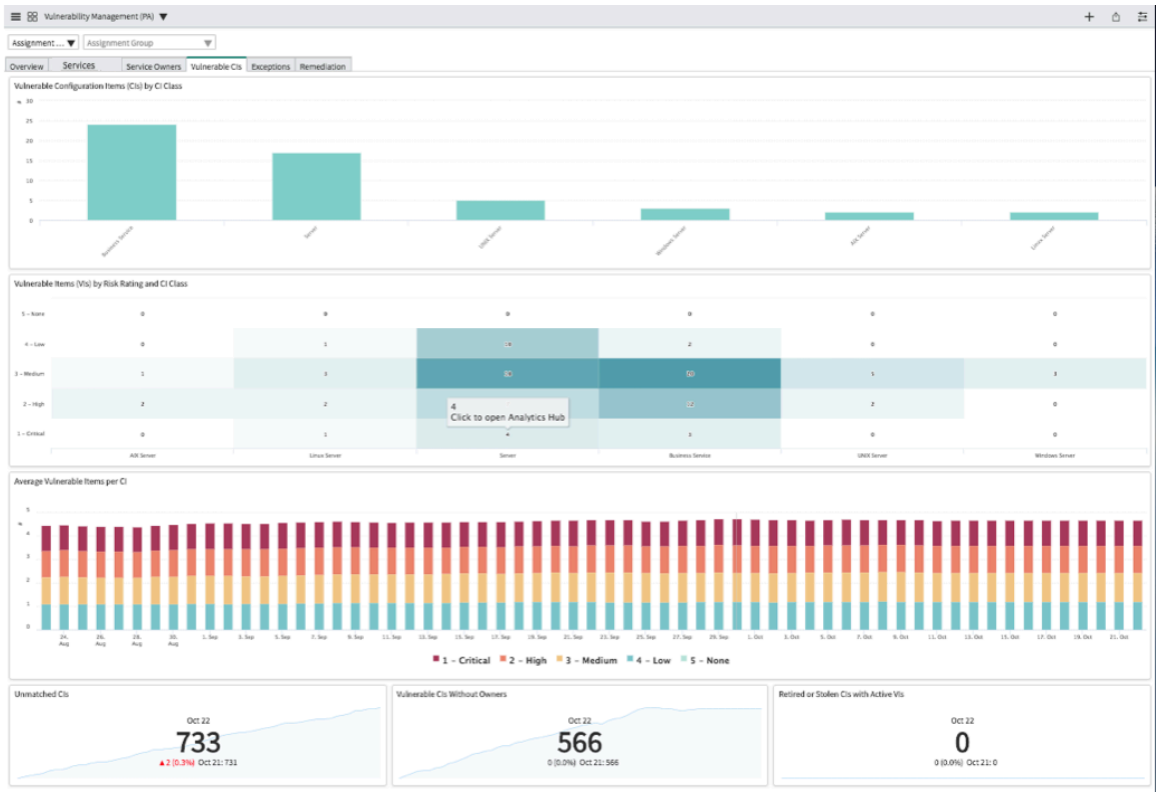
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Angreifbare CIs“.

Dieses Dashboard zeigt Umfang und Zusammensetzung von CIs mit aktiven Schwachstellen und welche Kategorien von CIs die meiste Aufmerksamkeit erfordern. Identifizieren Sie außer Betrieb genommene Assets mit aktiven angreifbaren Elementen, und bestätigen Sie, dass die Assets außer Betrieb genommen wurden. Zeigen Sie die Anzahl der angreifbaren CIs ohne Besitzerinformationen an, damit Sie proaktiv Besitzer für diese Assets identifizieren können, bevor eine kritische Schwachstelle diese Systeme betrifft.

Auf der Registerkarte „Angreifbare CIs“ können Sie die Berichte zu angreifbaren CIs ohne Besitzer und zu stillgelegten oder gestohlenen CIs mit aktiven AEs in Echtzeit anzeigen.

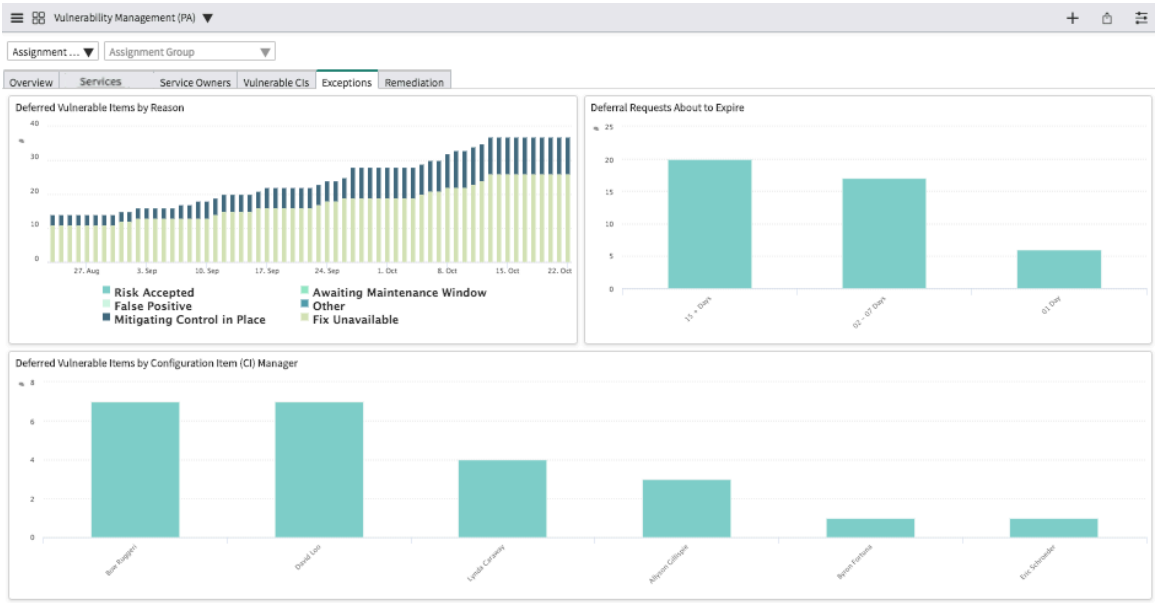


Registerkarte Ausnahmen

Dieses Dashboard hilft Ihnen zu verstehen, wo Ihre Organisation aufgrund potenziell übermäßiger Zurückstellungen Risiken eingeht, und hilft Ihnen, Abhilfemaßnahmen zu überdenken.

Sie können die Berichte „Zurückgestellte angreifbare Elemente nach Grund“, „Ablaufende Zurückstellungsanforderungen“, „Ausnahmen für kritische angreifbare Elemente nach Zuweisungsgruppe“ und „Ausnahmeanforderungen nach anfordernder Person“ anzeigen.

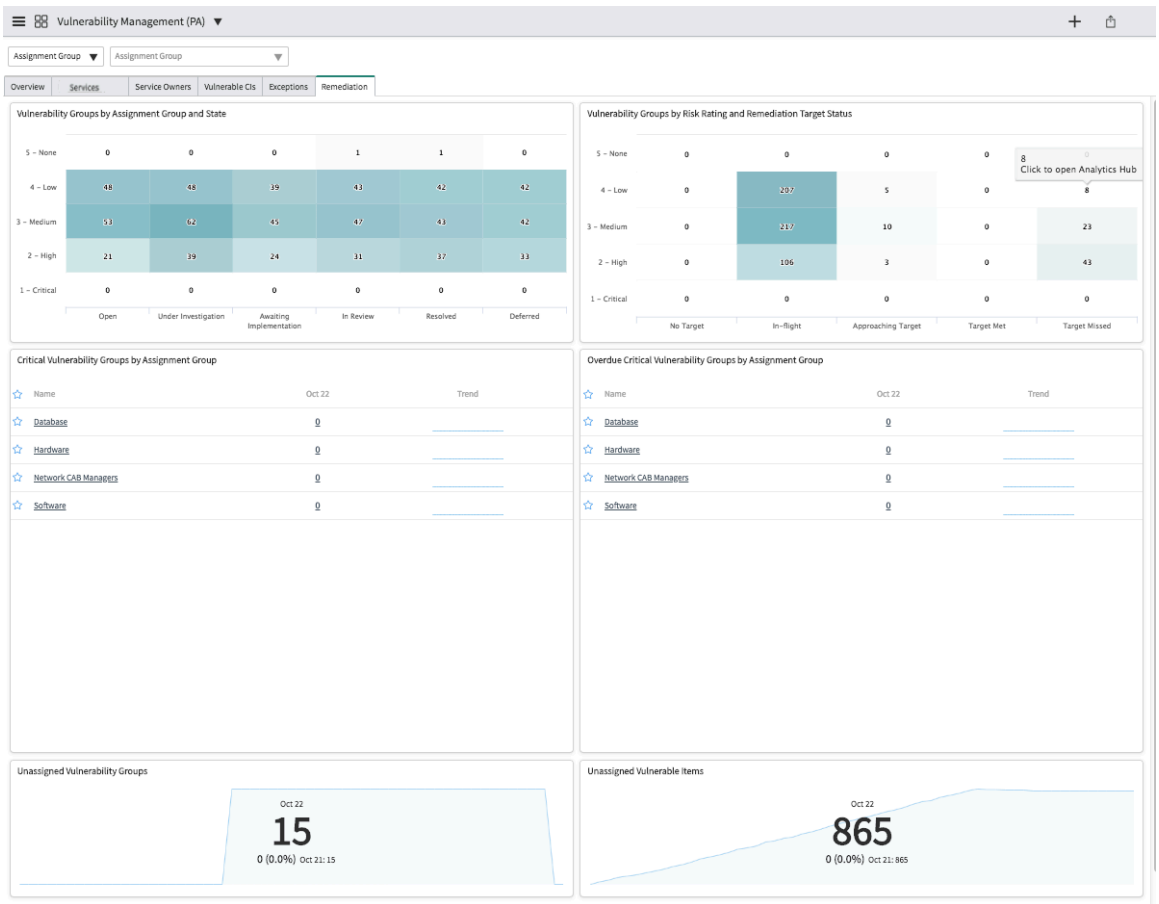
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Registerkarte „Remediation“

Dieses Dashboard hilft Ihnen, den Fortschritt Ihrer Korrekturmaßnahmen nachzuvollziehen und zu verstehen, welche Supportteams bei der Durchführung am meisten Unterstützung benötigen.

Auf der Registerkarte „Nachbesserung“ können Sie den Bericht „Nicht zugewiesene angreifbare Elemente“ in Echtzeit anzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Indikatoren

Vulnerability Response – Indikatoren

Es gibt eine Reihe von Indikatoren, mit denen Sie den Fortschritt der Nachbesserung von Schwachstellen in der Anwendung Vulnerability Response messen und nachverfolgen können.

Die Option Datensätze sammeln für -Indikatoren ist für die Anwendung Vulnerability Response standardmäßig deaktiviert. Diese Option ist deaktiviert, sodass bestimmte Berichte in Echtzeit angezeigt werden können. Die von diesen Indikatoren verwendeten Trendinformationen sind weiterhin verfügbar, wenn Sie Datensätze manuell erfassen und die Datensätze anzeigen möchten, aus denen sich die Punktzahlen zusammensetzen.

Eindeutige Schwachstellen

Eindeutige Schwachstellen mit count_active_vi > 0. Ziel ist die Minimierung.

Nicht zurückgestellte überfällige kritische angreifbare Elemente

Dies ist die Anzahl der Datenquelle „AE.Aktiv“, die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

% der angreifbaren Elemente mit erfülltem Korrekturziel

([[Geschlossene angreifbare Elemente > Korrekturziel = Ziel erfüllt]] / [[Geschlossene angreifbare Elemente]]) * 100. Ziel ist die Maximierung.

Nicht zugewiesene angreifbare Elemente

Alle aktiven angreifbaren Elemente, bei denen die Felder „Zuweisungsgruppe“ und „Zugewiesen an“ leer sind. Ziel ist die Minimierung.

Kritische angreifbare Elemente (Services)

Dies ist die Anzahl der Datenquelle „Aktive AEs (Services)“, welche die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

Weit überfällige angreifbare Elemente (Services)

Dies ist die Anzahl der Datenquelle „Aktive AEs (Services)“, welche die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

Nicht zugewiesene Korrekturaufgaben

Alle aktiven Korrekturaufgaben, bei denen die Felder „Zuweisungsgruppe“ und „Zugewiesen an“ leer sind. Ziel ist die Minimierung.

Kritische angreifbare Elemente

Dies ist die Anzahl der Datenquelle „AE.Aktiv“, die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Angreifbare Elemente

Dies ist die Anzahl der Datenquelle „AE.Aktiv“, die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Neue angreifbare Elemente

Dies ist die Anzahl der Datenquelle „AE.Neu“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Angreifbare Konfigurationselemente

Dies ist die Anzahl eindeutiger Werte in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Summierte Dauer der geschlossenen angreifbaren Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies ist die Summe in der Datenquelle „VI.Closed“, die die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Nicht zurückgestellte Korrekturaufgaben

Dies ist die Anzahl der Datenquelle „VG.Active“, welche die Tabelle sn_vul_vulnerability verwendet. Ziel ist die Minimierung.

Durchschnittliche Zeit bis zur Fehlerkorrektur für angreifbare Elemente

[[Summierte Dauer der geschlossenen angreifbaren Elemente]]/[[Geschlossene angreifbare Elemente]]

Kritische überfällige angreifbare Elemente (Services)

Dies ist die Anzahl der Datenquelle „Aktive AEs (Services)“, welche die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

Stillgelegte Konfigurationselemente

Dies ist die Anzahl eindeutiger Werte in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Zurückstellungsanforderungen

Dies ist die Anzahl der Datenquelle „Aktive Zurückstellungsanforderungen“, welche die folgende Tabelle verwendet: sn_vul_change_approval. Ziel ist die Minimierung.

Angreifbare Elemente nach Konfigurationselementen

Dies ist die Anzahl der Datenquellen-CIs mit aktiven AEs, die die folgende Tabelle verwenden: sn_vul_analytics_vi_ci_class. Ziel ist die Minimierung.

Geschlossene angreifbare Elemente

„Geschlossene angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel besteht in der Maximierung.

Nicht abgeglichene Konfigurationselemente

Listet die Hosts auf, die von Schwachstellenscannern einer Drittpartei erkannt wurden und keinen vorhandenen CIs in der CMDB entsprechen.

Nicht zurückgestellte überfällige kritische Korrekturaufgaben

Dies ist die Anzahl der Datenquelle „VG.Active“, welche die Tabelle sn_vul_vulnerability verwendet. Ziel ist die Minimierung.

Angreifbare Konfigurationselemente ohne Supportgruppe

Dies ist die Anzahl der Datenquelle „VI.Open“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Nicht zurückgestellte kritische Korrekturaufgaben

Dies ist die Anzahl der Datenquelle „VG.Active“, welche die Tabelle sn_vul_vulnerability verwendet. Ziel ist die Minimierung.

Zurückgestellte angreifbare Elemente

Dies ist die Anzahl der Datenquelle „AE.Aktiv“, die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Hoch angreifbare Elemente (Services)

Dies ist die Anzahl der Datenquelle „Aktive AEs (Services)“, welche die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

Eindeutige Konfigurationselemente mit aktiven angreifbaren Elementen

Dies ist die Anzahl eindeutiger Werte in Datenquellen-CIs mit aktiven AEs, welche die folgende Tabelle verwendet: sn_vul_analytics_vi_ci_class. Ziel ist die Minimierung.

Durchschnittliche Anzahl angreifbarer Elemente pro Konfigurationselement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[[Aktive angreifbare Elemente]] / [[angreifbare CIs]]. Ziel ist die Minimierung.

Korrekturaufgaben

Dies ist die Anzahl der Datenquelle „VG.Active“, welche die Tabelle sn_vul_vulnerability verwendet. Ziel ist die Minimierung.

Kritische zurückgestellte angreifbare Elemente

Dies ist die Anzahl der Datenquelle „AE.Aktiv“, die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

Zurückstellungsanforderungen (erstellt)

Dies ist die Anzahl der Datenquelle „Closed.Requests“, die folgende Tabelle verwendet: sn_vul_change_approval. Ziel ist die Minimierung.

Aufgliederungen

Die folgenden Aufgliederungsnamen gelten für die -Indikatoren im Dashboard:

- Alter
- Geschlossen mit Alter
- Zuweisungsgruppe
- CI-Klasse
- CI-Manager
- Zurückstellungsalter
- Aufschiebungsgrund
- Ausnahme für anfordernde Person
- Exploit-Angriffsvektor
- Exploit vorhanden
- Exploit-Kompetenzniveau
- Korrekturzielregel
- Nachbesserungszielstatus
- Nachbesserungszielstatus (geschlossen)
- Risikobewertung
- Service
- Servicerelevanz
- Serviceverantwortlicher
- Schweregrad
- Status

Hinweis:
Das Anpassen des Alters und der Berechnung des Alters der geschlossenen Elemente für angreifbare Elemente kann zu einem starken Anstieg oder Rückgang der PA-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von Alter und Alter geschlossen für VIs finden Sie im KB-Artikel KB1703270 .

Aufgliederungsquelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zuweisungsgruppe: Gilt für AE- oder und RT-Berichte
- Exploit vorhanden: Gilt für VI-Berichte.
- Exploit-Angriffsvektor: Gilt für VI-Berichte.
- Exploit-Kompetenzniveau: Gilt für AE-Berichte.
- Korrekturzielstatus: Gilt für VI- und RT-Berichte.
- Risikobewertung: Gilt für AE- und RT-Berichte.
- Status: Gilt für VI- und RT-Berichte.

Datenvisualisierungen

Titel	Typ	Beschreibung
Schwachstellen	Einzelne Punktzahl	Anzahl der Schwachstellen, die mit einem oder mehreren aktiven angreifbaren Elementen verknüpft sind.
Angreifbare Elemente (AEs)	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) angreifbaren Elemente.
Angreifbare Konfigurationselemente (CIs)	Einzelne Punktzahl	Anzahl der Configuration Items (CIs), die mindestens einem aktiven angreifbaren Element zugeordnet sind.
Korrekturaufgaben	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) Korrekturaufgaben.
Angreifbare Elemente nach Risikobewertung	Balken	Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne.
Angreifbare Elemente nach Alter und Risikobewertung	Heatmap	Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung und Alter (in Tagen).
AEs mit erfülltem Korrekturziel	Einzelne Punktzahl	Prozentsatz der geschlossenen angreifbaren Elemente, deren Nachbesserungszieldaten im aktuellen und vorherigen Quartal eingehalten wurden. Korrekturziele werden aus dem Datum von „Zuletzt geöffnet“ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.
Durchschnittliche Zeit bis zur Korrektur von AEs (MTTR)	Einzelne Punktzahl	Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		angezeigt als laufender 30-Tage-Durchschnitt. **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe.
Kritische Korrekturaufgaben kurz vor der Fälligkeit	Einzelne Punktzahl	Anzahl der aktiven Korrekturaufgaben, deren Korrekturzieldatum näher rückt. Das Korrekturzieldatum einer Korrekturaufgabe wird auf das nächstliegende Fälligkeitsdatum festgelegt, das zu einem aktiven angreifbaren Element in der Gruppe gehört. Korrekturziele werden aus dem Datum von „Zuletzt geöffnet“ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. Dieser Bericht schließt zurückgestellte Korrekturaufgaben aus.
Neue und geschlossene angreifbare Elemente	Balken	Anzahl neuer und geschlossener angreifbarer Elemente über die ausgewählte Zeitspanne. **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe.
Geschlossene angreifbare Elemente nach Korrekturzielstatus	Balken	Anzahl der geschlossenen angreifbaren Elemente, gruppiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

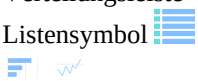
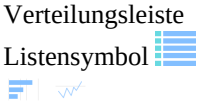
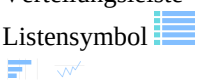
Titel	Typ	Beschreibung
		nach Nachbesserungszielstatus für die ausgewählte Zeitspanne. **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe.
Kritische angreifbare Elemente nach Zuweisungsgruppe	Liste und Position	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Zuweisungsgruppe.
Überfällige kritische angreifbare Elemente nach Zuweisungsgruppe	Liste und Position	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Zuweisungsgruppe. Korrekturziele werden aus dem Datum von „Zuletzt geöffnet“ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.

Business-Services

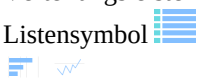
Name	Typ	Beschreibung
Kritische angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Business-Service. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Business-Services (Fortsetzung)

Name	Typ	Beschreibung
Überfällige kritische angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol 	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Business-Service. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.
Hoch angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol 	Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, gruppiert nach Business-Service. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.
Überfällige hoch angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol 	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Business-Service. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.

Serviceverantwortliche

Name	Typ	Beschreibung
Kritische angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol 	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Business-Service-Besitzer. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Serviceverantwortliche (Fortsetzung)

Name	Typ	Beschreibung
		Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.
Überfällige kritische angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Business-Service-Verantwortlicher. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.
Hoch angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, gruppiert nach Business-Service-Besitzer. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.
Überfällige hoch angreifbare Elemente	Liste, Position und Verteilungsleiste Listensymbol	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Business-Service-Verantwortlicher. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilerleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.

Angreifbare CIs

Name	Typ	Beschreibung
Angreifbare Konfigurationselemente (CIs) nach CI-Klasse	Balken	Anzahlen der Konfigurationselemente mit aktiven Schwachstellen, gruppiert nach CI-Klasse in der CMDB.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbare CIs (Fortsetzung)

Name	Typ	Beschreibung
Angreifbare Elemente (AEs) nach CI-Klasse	Treemap	Anzahl der aktiven AEs, aufgeschlüsselt nach CI-Klasse.
Durchschnittliche angreifbare Elemente pro CI	Balken	Durchschnittliche Anzahl von angreifbaren Elementen, die zu einem Konfigurationselement gehören, gruppiert nach Risikobewertung.
Nicht abgeglichene CIs	Einzelne Punktzahl	Anzahl der importierten Konfigurationselemente, die keinem vorhandenen CI in der CMDB entsprechen.
Angreifbare CIs ohne Supportgruppe	Einzelne Punktzahl	Anzahl der angreifbaren Konfigurationselemente, denen keine Supportgruppe zugewiesen ist.
Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs	Einzelne Punktzahl	Anzahl der Konfigurationselemente, die in der CMDB **als außer Kraft gesetzt** oder **gestohlen** markiert wurden und aktive angreifbare Elemente aufweisen.

Ausnahmen

Name	Typ	Beschreibung
Zurückgestellte angreifbare Elemente nach Grund	Balken	Anzahl der zurückgestellten angreifbaren Elemente, gruppiert nach Zurückstellungsgrund.
In Kürze ablaufende Zurückstellungsanforderungen	Balken	Anzahl der Zurückstellungsanforderungen, die Korrekturaufgaben oder angreifbaren Elementen zugeordnet sind und zur Überprüfung erneut geöffnet werden. Sie werden nach der Anzahl der Tage gruppiert, die bis zur erneuten Öffnung verbleiben. Wenn E-Mail-Benachrichtigungen definiert sind, wird eine E-Mail gesendet.
Zurückgestellte angreifbare Elemente nach Configuration Item (CI) Manager	Balken	Anzahl der zurückgestellten angreifbaren Elemente, die vom Manager für das zugehörige Konfigurationselement gruppiert wurden.

Korrektur

Name	Typ	Beschreibung
Korrekturaufgaben nach Risikobewertung und Status	Heatmap	Anzahl der aktiven Korrekturaufgaben, gruppiert nach Risikobewertung und Status.
Korrekturaufgaben nach Risikobewertung und Status des Korrekturziels	Heatmap	Anzahl der aktiven Aufgaben, gruppiert nach Risikobewertung und Status des Korrekturziels. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrektur (Fortsetzung)

Name	Typ	Beschreibung
Kritische Korrekturaufgaben nach Zuweisungsgruppe	Liste und Position	Anzahl der aktiven Korrekturaufgaben mit kritischer Risikobewertung, gruppiert nach Zuweisungsgruppe. Dieser Bericht schließt zurückgestellte Korrekturaufgaben aus.
Überfällige kritische Korrekturaufgaben nach Zuweisungsgruppe	Liste und Position	Anzahl der aktiven Korrekturaufgaben mit kritischer Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Zuweisungsgruppe. Dieser Bericht schließt zurückgestellte Korrekturaufgaben aus.
Nicht zugewiesene Korrekturaufgaben	Einzelne Punktzahl	Anzahl der aktiven Korrekturaufgaben ohne einen Beauftragten oder eine Zuweisungsgruppe.
Nicht zugewiesene angreifbare Elemente	Einzelne Punktzahl	Anzahl der aktiven angreifbaren Elemente ohne einem Beauftragten oder einer Zuweisungsgruppe.

Zeigen Sie Performance Analytics for Vulnerability Response [PA]-Berichte in Echtzeit an

Um Ihre wichtigsten angreifbaren Elemente (VIs) zu verwalten und schnell zu beheben, zeigen Sie bei Bedarf Berichte in Echtzeit im Dashboard für Schwachstellenmanagement (PA) an. Die Anwendung Performance Analytics for Vulnerability Response ist mit einem von ServiceNow Storegetrennten Abonnement verfügbar.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Weitere Informationen zu den Berichten für Performance Analytics for Vulnerability Responsefinden Sie unter Dashboard für Schwachstellenmanagement [PA].

Weitere Informationen zum Setup und zur Installation der Anwendung Performance Analytics for Vulnerability Response finden Sie unter Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA]..

Wenn es nicht angezeigt wird, navigieren Sie zum Anzeigen des Dashboards zu **Vulnerability Response** > **Übersicht**. Oben im Dashboard werden die Registerkarten für Berichte angezeigt.

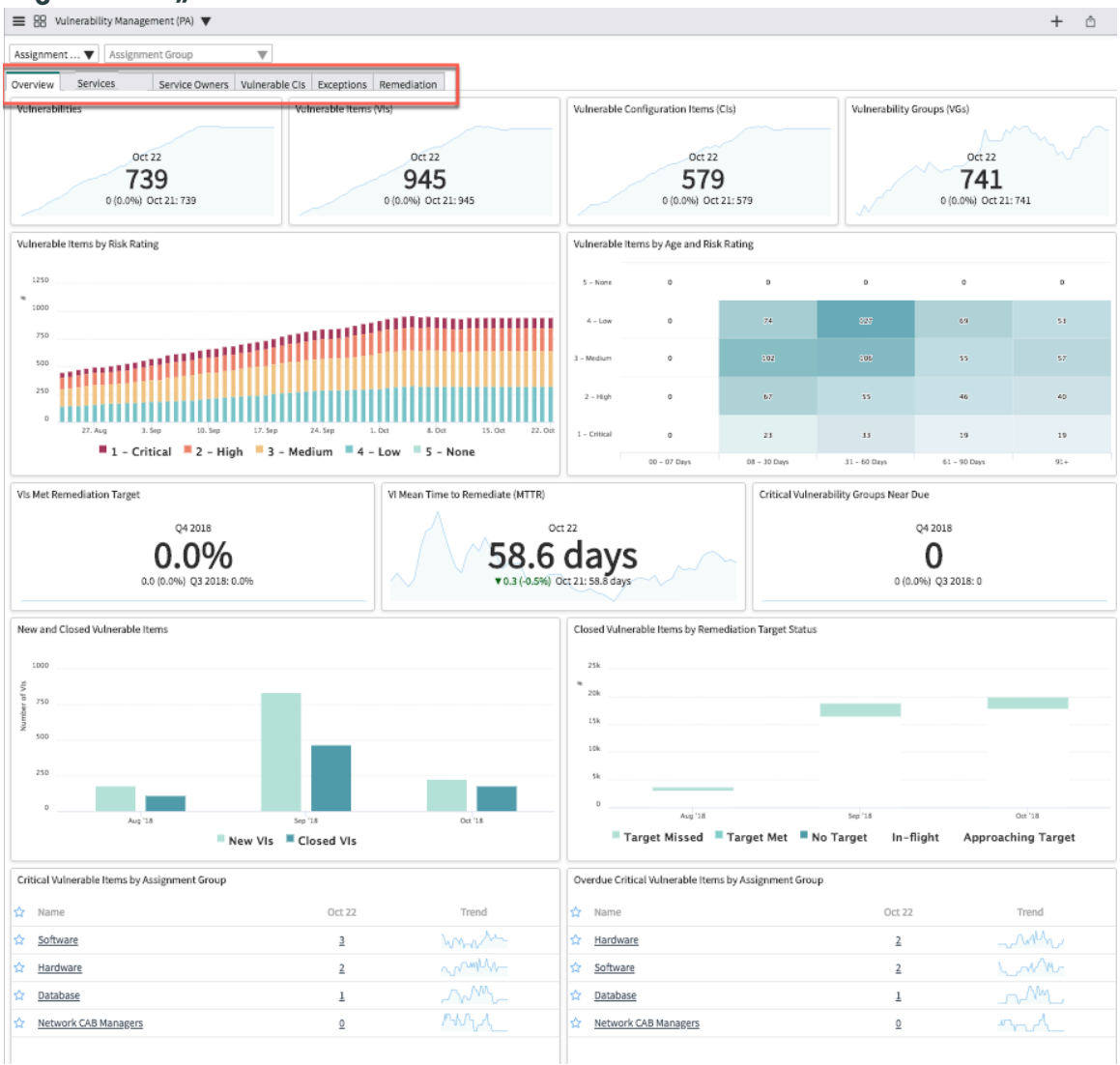
Ab Version 19.0 von Vulnerability Responsekann dieses Dashboard auch in der New Experience UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das **Dashboard** -Symbol. Je nach Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdownliste neben dem Namen des Dashboards. Weitere Informationen finden Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

unter Dashboards im Arbeitsbereich des Schwachstellenmanagers und Dashboards im Arbeitsbereich für IT-Fehlerkorrekturen.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Registerkarte „Übersicht“



Zeigen Sie die folgenden Berichte auf den Registerkarten des Dashboards für Schwachstellenmanagement (PA) in Echtzeit an.

- Registerkarte „Übersicht“
  - Kritische angreifbare Elemente nach Zuweisungsgruppe
- Registerkarte „Angreifbare CIs“:
  - Angreifbare CIs ohne Besitzer
  - Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs
- Registerkarte „Ausnahmen“:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

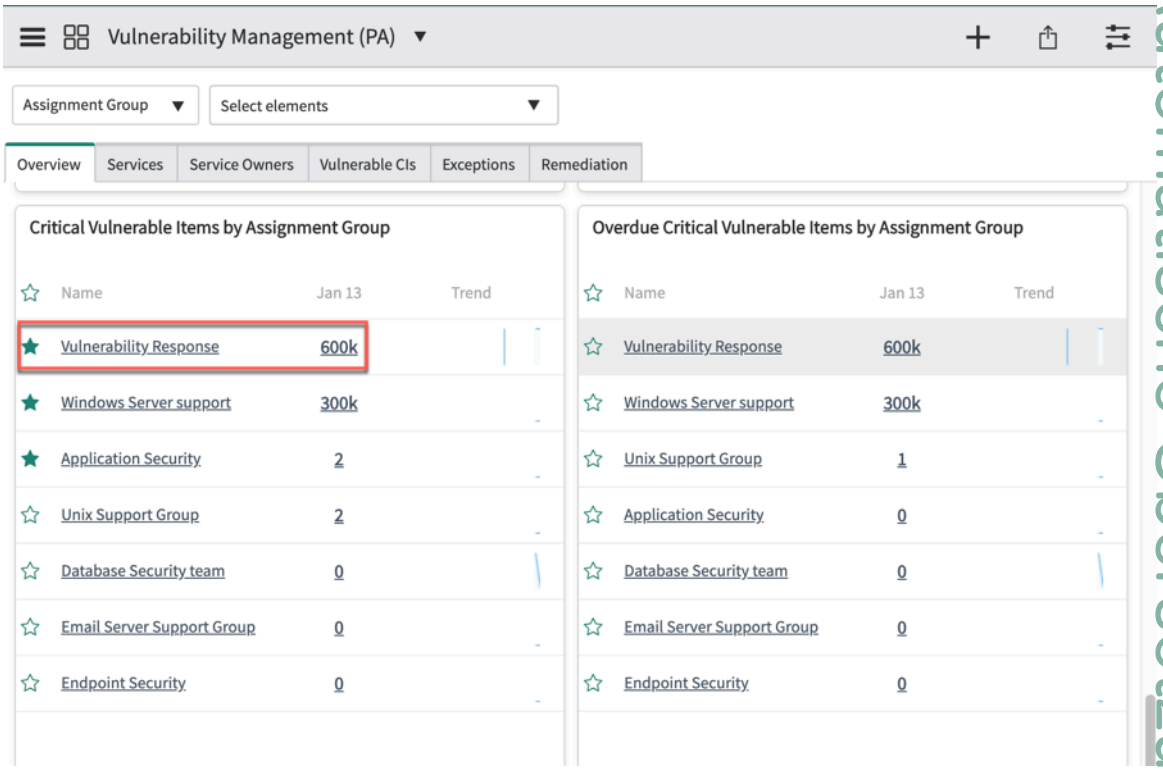
- Zurückgestellte angreifbare Elemente nach Grund
- In Kürze ablaufende Zurückstellungsanforderungen
- Nach CIO-Manager zurückgestellte angreifbare Elemente

- Registerkarte „Nachbesserung“:
  - Nicht zugewiesene angreifbare Elemente

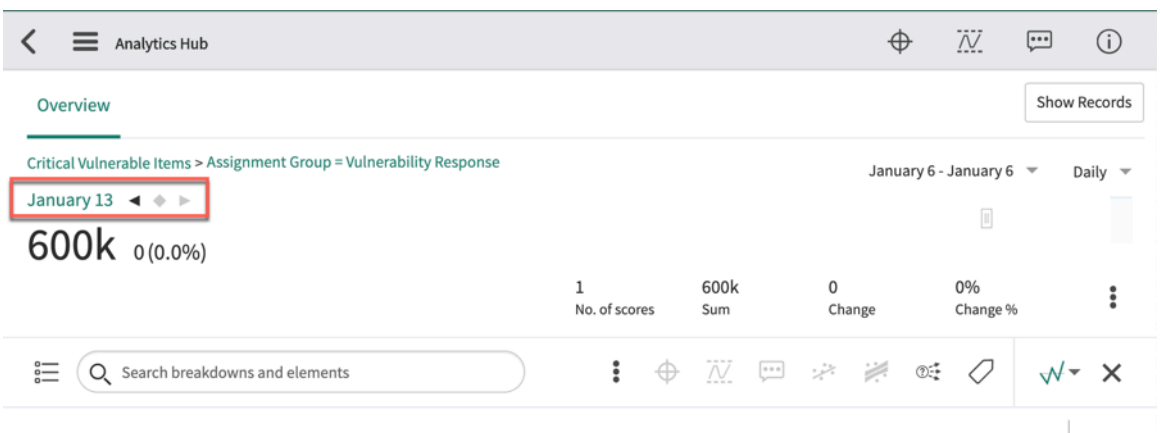
Um Echtzeit-Punktzahlen anzuzeigen, führen Sie bei gleichzeitig ausgewählter Registerkarte, die Echtzeitberichte enthält, die folgenden Schritte aus:

Prozedur

1. Klicken Sie im Bericht, z. B. Kritische angreifbare Elemente nach Zuweisungsgruppe, auf einen der angezeigten Links.



2. Klicken Sie im angezeigten Datensatz auf das Datum.

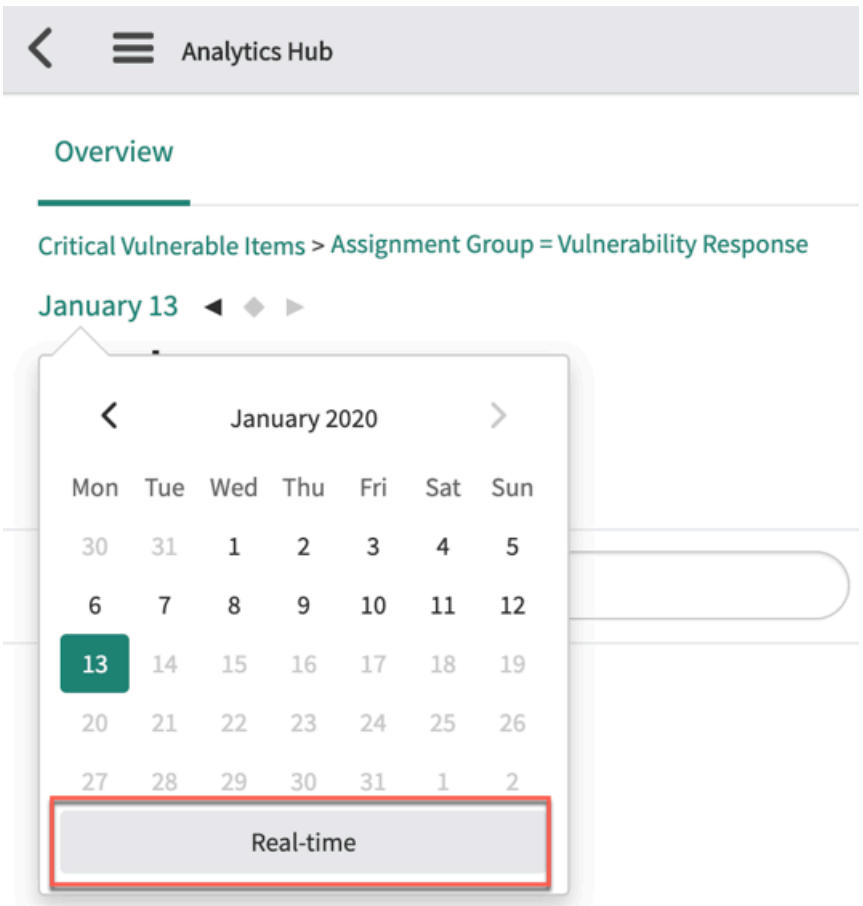


Automatische Übersetzung

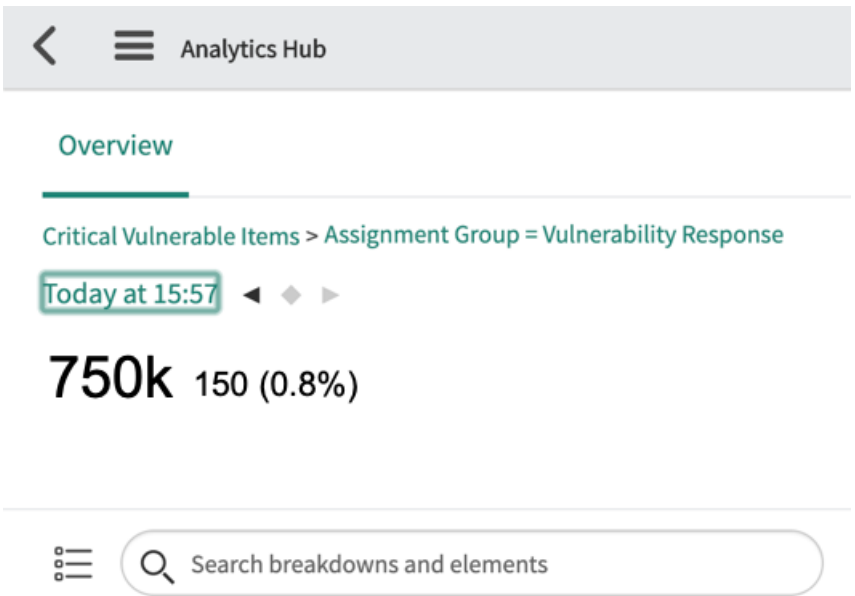
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie im angezeigten Kalender auf Echtzeit.

   Wenn ein Bericht keine Echtzeit-Punktzahl unterstützt, wird die Schaltfläche „Echtzeit“ nicht im Kalender angezeigt.



Es kann einige Minuten dauern, bis der Wert aktualisiert wird. Das aktuelle Datum, die Datensätze, die Anzahl der neuen Datensätze seit dem letzten Bericht und die prozentuale Änderung im Vergleich zum letzten Bericht werden ebenfalls angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. **Wahlweise:** Um die Datensätze, aus denen der Bericht besteht, anzuzeigen, klicken Sie bei angezeigtem Echtzeitbericht oben rechts **auf Datensätze anzeigen**.
   Eine Liste der Datensätze, aus denen sich die Punktzahl zusammensetzt, wird angezeigt.

Performance Analytics -Indikatoren für Vulnerability Response [PA] anzeigen

Zeigen Sie automatisierte und formulierte Performance Analytics -Indikatoren an, die die Schwachstellendaten in Ihrer Instanz darstellen.

Vorbereitungen

Standardmäßig ist die Option zum Sammeln von Datensätzen für -Indikatoren für die Anwendung „Performance Analytics – Content Pack Vulnerability Response“ deaktiviert. Diese Option ist deaktiviert, sodass bestimmte Berichte in Echtzeit angezeigt werden können. Die von diesen Indikatoren verwendeten Trendinformationen sind weiterhin verfügbar, wenn Sie Datensätze manuell erfassen und die Datensätze anzeigen möchten, aus denen sich die Punktzahlen zusammensetzen.

Hinweis:
Das Aktivieren von Datensätzen erfassen in einem Indikator kann sich auf Ihre Leistung auswirken und die für die Ausführung des Datensammlungsauftrags erforderliche Zeit und Speicher erheblich verlängern.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder pa.viewer

Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response verfügt sowohl über automatisierte als auch formulierte Indikatoren.

Wichtige Begriffe

PA-Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen von einem Business-Service, einer Aktivität oder einem Organisationsverhalten durchgeführt wird, z. B. Nicht zurückgestellte überfällige kritische angreifbare Elemente.

PA-Indikatorquelle

Datensätze, die Datensätze aus einer Tabellen- oder Datenbankansicht filtern, z. B. AE Aktiv.

Datensätze erfassen

Wenn diese Option aktiviert ist, werden Datensätze im Arbeitsspeicher gespeichert und haben Zugriff auf Analytics Hub.

Aufgliederungen

Aufgliederungen filtern und gruppieren gesammelte Datensätze. Aufgliederungen können die Speichernutzung erhöhen, insbesondere wenn ihre Anzahl und Vielfalt zunehmen.

Aufgliederungsausschlüsse

Durch Ausschlüsse werden bestimmte Aufgliederungen entfernt, was den Speicherverbrauch reduzieren kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

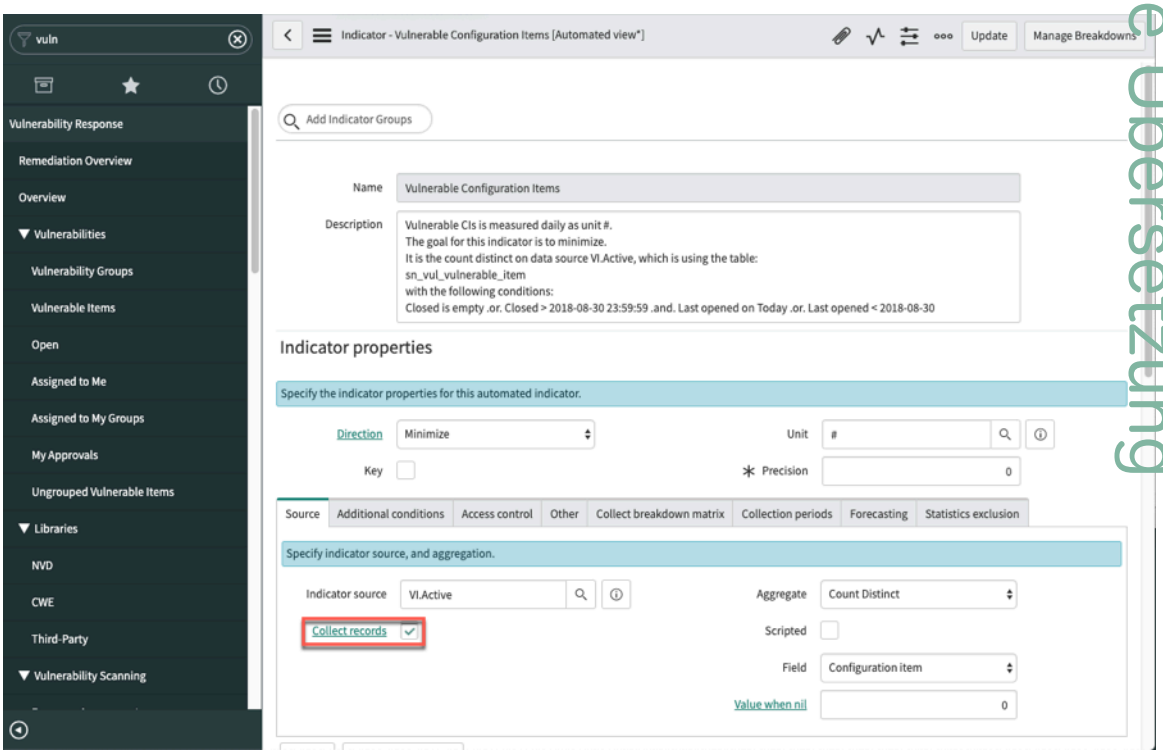
1. Navigieren Sie für automatisierte Indikatoren zu **Performance Analytics** > **Indikatoren** > **Automatisierte Indikatoren**.
2. Navigieren Sie für formulierte Indikatoren zu **Performance Analytics** > **Formelindikatoren**.

   Ausführliche Informationen zu -Indikatoren finden Sie unter Performance Analytics-Indikatoren .
3. Suchen Sie in beiden Fällen am **Anwendung** > **Performance Analytics**.

   Hinweis:
   Wenn es sich nicht in Ihrer Standardansicht befindet, fügen Sie die Spalte **Anwendung** mithilfe des Zahnradsymbols ( ) in der oberen linken Ecke der Seite hinzu. Die Spalte Anwendung wird dann im Dropdown-Menü Suche angezeigt.
4. **Wahlweise:** Um Datensätze sammeln für einen Indikator in Performance Analytics für Vulnerability Response zu aktivieren, gehen Sie wie folgt vor:

   a. Klicken Sie bei angezeigter Liste der automatisierten Indikatoren in der Spalte Name auf den Indikator, für den Sie die Erfassung von Datensätzen aktivieren möchten.
   Der Indikatordatensatz wird angezeigt.

   b. Aktivieren Sie im Abschnitt Indikatoreigenschaften bei ausgewählter Registerkarte Quelle das Kontrollkästchen Datensätze sammeln.



   c. Wählen Sie eine, um fortzufahren.

Automatische Übersetzung

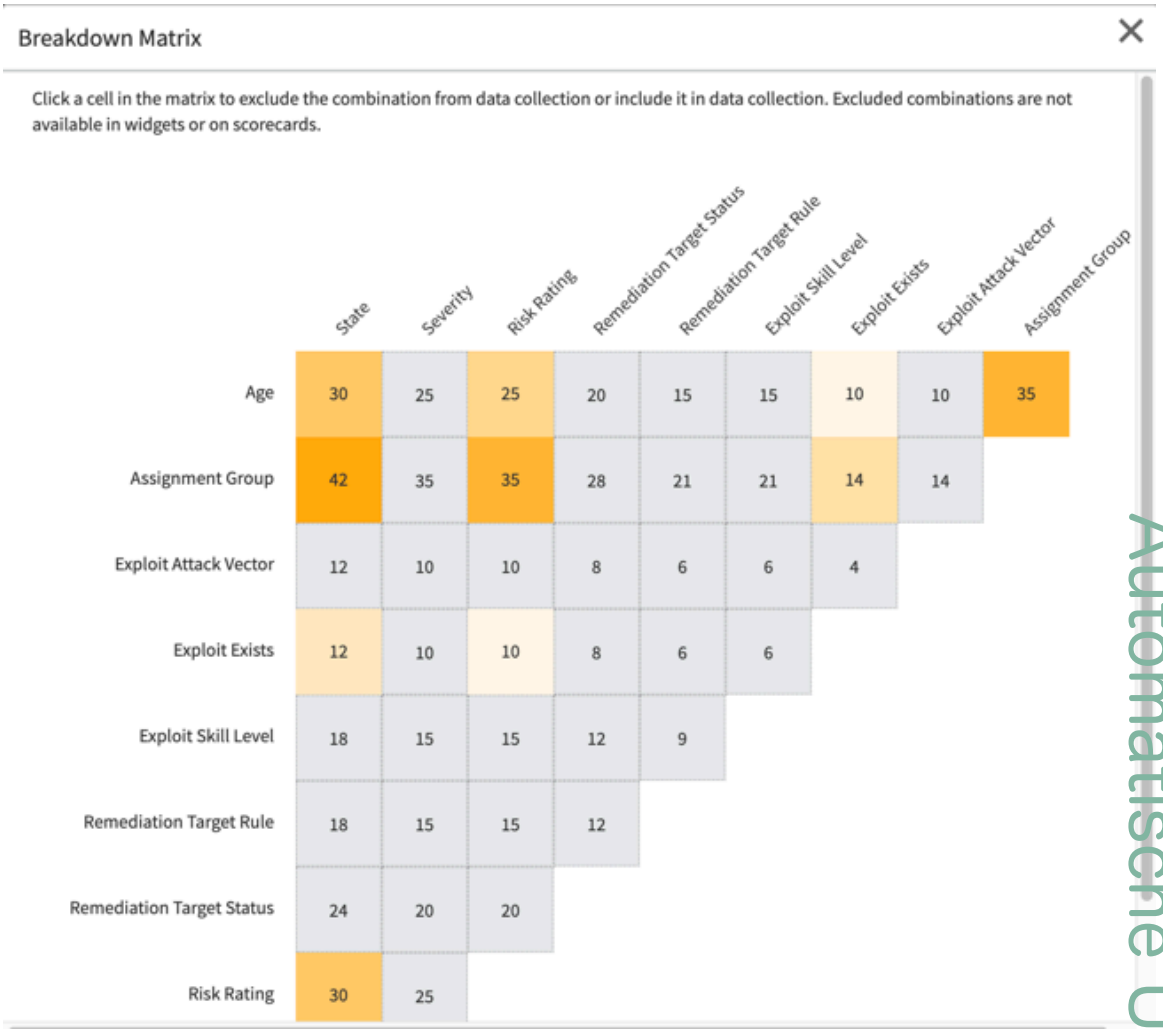
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Aktualisieren	Speichern Sie Ihre Änderungen, und kehren Sie zur Liste der Indikatoren zurück.
Aufgliederungen verwalten **Hinweis:** Wenn Sie Aufgliederungen der zweiten Ebene reaktivieren, kann dies den Speicherverbrauch erheblich erhöhen und den Datensammlungsauftrag verlangsamen. Standardmäßig wurden Aufgliederungsausschlüsse der zweiten Ebene auf die folgenden Indikatoren angewendet: ▪ Angreifbare Konfigurationselemente ▪ Stillgelegte CIs ▪ Zurückgestellte AEs	Reaktivieren Sie Aufgliederungen der zweiten Ebene für die aufgeführten Indikatoren, oder bearbeiten Sie Aufgliederungen für andere Indikatoren. (Optional) Weitere Informationen zu Performance Analytics-Aufgliederungen finden Sie unter Performance Analytics-Aufgliederungen.

d. Klicken Sie auf **Aufgliederungen verwalten**.

e. Klicken Sie im angezeigten Formular **auf Konfigurieren Aufgliederungsmatrix**.
Das Formular „Aufgliederungsmatrix“ wird angezeigt. Ausgeschlossene Kombinationen werden ausgewählt und mit Farben angezeigt, wie in der folgenden Abbildung dargestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



f. Um den Ausschluss zu entfernen und eine ausgeschlossene Kombination erneut zu aktivieren, klicken Sie auf eine ausgewählte Zelle.

g. Klicken Sie oben rechts im Formular **auf Schließen**, um zum Formular „Aufgliederung verwalten“ zurückzukehren.

h. Klicken Sie auf den Zurückpfeil, um zum Indikatordatensatz zurückzukehren.

i. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Liste der Indikatoren zurückzukehren.

Framework für zusammengefasste Berichte

Mit dem Framework für aggregierte Berichte können Sie Berichte für die Daten erstellen, die komplexe und zeitaufwändige On-the-fly-Abfragen beinhalten, um eine bessere Leistung zu erzielen.

Das Framework für aggregierte Berichte verbessert die Leistung durch:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ressourcenverbrauch und Berichte werden schneller erstellt,
- die Daten zusammenzufassen und Zusammenfassungen und Aufgliederungen wiederzuverwenden (Gruppieren nach) und
- Dadurch werden weniger Abfragen an die Datenbank durchgeführt

Wenn Sie mehr als eine Million angreifbarer Elemente haben, verwenden Sie zusätzlich zu den Standardberichten das Framework für aggregierte Berichte in Vulnerability Response Common.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- Now Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics -Administrator (pa_admin): Zusammenfassungen, Widgets und Dashboards überprüfen Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- VR-Lesevorgang (sn_vul_cmn.read): Überprüfen Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- Schwachstellenanalyst (sn_vul.vulnerability_analyst): Aggregierte Ergebnisse überprüfen.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Um die Leistung eines bestimmten Aspekts in einem Geschäftsprozess zu analysieren, der in einer Tabelle ServiceNow aufgezeichnet ist, erstellen Sie eine spezifische Zusammenfassung für den Aspekt und einen Bericht für diese Zusammenfassung.

Vorbereitungen

Erforderliche Rolle: sn_vul_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Zusammengefasste Berichte** > **Zusammenfassungsdefinitionen** > **Alle** und klicken Sie auf **Neu**.
2. Geben Sie der Zusammenfassung im Feld **Name** einen beschreibenden Namen.
3. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung der Zusammenfassung an.
4. Füllen Sie die Felder auf der Registerkarte **Quelle** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder auf der Registerkarte „Quelle“

Feld	Beschreibung
Tabelle	Tabelle, aus der Sie die Daten für den Bericht abrufen möchten. Diese Dropdownliste enthält nur die Tabellen „App Sec Common“, „App-Vul“, „App-Vulc“, „App-Vul-Container“ und „Anwendungsschwachstelle“.
Aggregatfunktion	Funktion, die auf die in **Feld**ausgewählte Spalte angewendet werden soll. ○ **Anzahl**: Anzahl der Datensätze. ○ **Summe**: Gesamtsumme der Werte in der unter **„Feld“**ausgewählten Spalte. ○ **Durchschnitt**: Durchschnitt aller Werte in einer unter **Feld**ausgewählten Spalte. ○ **Maximum**: Höchstwert in der unter **Feld**ausgewählten Spalte. ○ **Minimum**: Mindestwert der unter **„Feld“**ausgewählten Spalte. ○ **Anzahl eindeutiger Werte**: Eindeutige Werte in der unter **dem Feld**ausgewählten Spalte.
Feld	Spalte, auf die Sie die Funktion anwenden möchten. **Hinweis:** Dieses Feld wird nicht angezeigt, wenn Sie im Feld **„Aggregatfunktion“Anzahl** auswählen.

5. Geben Sie auf der Registerkarte **Zusätzliche Bedingungen** im Feld **Bedingungen** die Bedingung an, um eine bestimmte Gruppe von Datensätzen auszuwählen, für die Sie die aggregierten Ergebnisse abrufen möchten.
6. Wählen Sie auf der Registerkarte **Gruppieren nach** die Spalten der Tabelle aus, nach der Sie die Daten gruppieren oder stapeln möchten.
   Sie können bis zu zwei Aufgliederungen auswählen.

   Wenn Sie die **Datumsspalte** in einem beliebigen Feld für Gruppierung auswählen, wird das Feld **Trend nach** angezeigt. Sie können die Zusammenfassungsergebnisse abrufen, die nach Woche, Tag, Minuten usw. kategorisiert sind, indem Sie die Optionen im Feld **Trend nach** auswählen.
7. Wählen Sie auf der **Registerkarte** Zeitplan einen Zusammenfassungszeitplan aus, oder erstellen Sie einen, der die Häufigkeit definiert, mit der Sie die Zusammenfassung zum Abrufen der Daten ausführen können. Informationen zum Erstellen eines Zusammenfassungszeitplans finden Sie unter Führen Sie mehrere Zusammenfassungen gleichzeitig aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können die Ausführung der Zusammenfassung für eine inaktive Zusammenfassungsdefinition nicht planen.

8. Klicken Sie auf **Absenden**, um die Zusammenfassung zu erstellen.
   Die Zusammenfassung wird in der Zusammenfassungsliste angezeigt. Mit der vordefinierten Häufigkeit wird die Zusammenfassung ausgeführt, und für jede Ausführung wird ein Datensatz zusammen mit einem Ausführungsdatum und einer Ausführungszeit in der zugehörigen Liste „Geplante Ausführungen“ erstellt.
9. Navigieren zu **Alle** > **Zusammengefasste Ergebnisse** und öffnen Sie Ihre Zusammenfassung, um die aggregierten Ergebnisse und geplanten Ausführungen anzuzeigen.
   Die aggregierten Ergebnisse werden in der zugehörigen Liste **„Aggregierte Ergebnisse“** aufgeführt. Wenn die Zusammenfassungsausführung fehlschlägt, finden Sie weitere Informationen in der Spalte **Hinweise** in der zugehörigen Liste **Geplante Ausführungen**.
10. **Wahlweise:** Wählen Sie **Jetzt ausführen aus**, um die Zusammenfassungsergebnisse unabhängig vom Zusammenfassungszeitplan zu sammeln.
    Wenn Sie die geplante Ausführung beenden, während sie ausgeführt wird, werden keine Änderungen an den aggregierten Ergebnissen vorgenommen. Sie können eine Zusammenfassung auch löschen oder deaktivieren.

Nächste Maßnahme

Erstellen Sie einen Bericht mit Ihrer Zusammenfassung. Weitere Informationen zum Erstellen eines Berichts mithilfe einer Zusammenfassung finden Sie unter Erstellen Sie einen Bericht mithilfe einer Zusammenfassung.

Zugehörige Informationen

Framework für zusammengefasste Berichte

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Sie können die Ausführung mehrerer Zusammenfassungen mit einem einzigen Zusammenfassungszeitplan planen.

Vorbereitungen

Erforderliche Rolle: sn_vul_cmn.admin

Warum und wann dieser Vorgang ausgeführt wird

Angenommen, Sie möchten sechs Zusammenfassungen gleichzeitig ausführen. Erstellen Sie einen Zusammenfassungszeitplan, und fügen Sie ihm alle Zusammenfassungen hinzu. Diese Zusammenfassungen werden mit der definierten Häufigkeit und Uhrzeit ausgeführt.

Prozedur

1. Navigieren zu **Alle** > **Zusammengefasste Berichte** > **Zeitplan**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular „Zusammenfassungszeitplan“ aus.

Feld	Beschreibung
Zeitplanname	Name des Zusammenfassungszeitplans.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Regelmäßige Aufgabe	Geplante Skriptausführung, die die Häufigkeit definiert, mit der die Zusammenfassungen ausgeführt werden müssen. Sie können eine geplante Aufgabe erstellen, indem Sie die Schaltfläche **Neu** wählen.

4. Wählen Sie **Absenden**.
   Der Zusammenfassungszeitplan wird in der Liste Zusammenfassungszeitplan angezeigt.
5. Öffnen Sie Ihren Zusammenfassungszeitplan.
6. Wählen Sie **Bearbeiten**, fügen Sie die Zusammenfassungen der **Zusammenfassungsliste**hinzu, und wählen Sie **Speichern**.
   Die ausgewählten Zusammenfassungen werden in der zugehörigen Liste „Zusammenfassungen“ angezeigt.

   Hinweis:
   Wenn Sie einem Zeitplan eine inaktive Zusammenfassung hinzufügen, wird die geplante Ausführung nicht gestartet.

7. Wählen Sie **Aktualisieren**.
   Diese Zusammenfassungen werden mit der im Zusammenfassungszeitplan definierten Häufigkeit ausgeführt.

Zugehörige Informationen

Framework für zusammengefasste Berichte

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Ein neuer Prozessor oder ein Hintergrundauftrag, der Prozessor für das Framework für die zusammengefasste Berichterstellung, wird mit dem Basissystem geliefert, das die geplanten Aufgaben ausführt, die sich auf die Tabelle „Framework für die zusammengefassten Berichte“ beziehen. Dadurch kann das gesamte Subsystem im Hintergrund ausgeführt werden, und die Systemressourcen werden, sofern verfügbar, besser genutzt.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Hintergrundauftrags-Konfiguration – Vulnerability Response Common-Aggregation-Ergebnisrechner**.
2. Definieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig im Feld **Max. gleichzeitige Threads** ausgeführt werden sollen, und wählen Sie **Speichern**aus.
   Standardmäßig werden vier Zusammenfassungen gleichzeitig ausgeführt.
3. Navigieren Sie zur Liste „Prozessorpools für Hintergrundaufträge“, **sn_sec_cmn_background_job_processor_pool.list**, und wählen Sie **Neu**, um einen Hintergrundauftrags-Prozessor für das Framework für aggregierte Berichte zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Erstellen eines Prozessorpools für Hintergrundaufträge finden Sie unter Erweiterte parallele Verarbeitung für Hintergrundaufträge in Vulnerability Response .

Hinweis:
Die Anzahl der Hintergrundauftragsprozessoren muss der Anzahl der maximalen gleichzeitigen Threads entsprechen, die im Formular **„Konfiguration des Hintergrundauftrags – Vulnerability Response Common-Aggregation-Ergebnisrechner“** angegeben sind. Siehe Schritt 2.

Zugehörige Informationen

Framework für zusammengefasste Berichte

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Um die für eine von Ihnen erstellte Zusammenfassung spezifischen Daten zu visualisieren und zu analysieren, generieren Sie einen Bericht, indem Sie im Bedingungsgenerator eine Bedingung für die Zusammenfassung angeben.

Vorbereitungen
Erforderliche Rolle: pa_admin

Prozedur

1. Navigieren zu **Alle** > **Berichte** > **Neu erstellen:**.
2. Füllen Sie die Felder auf der Registerkarte **Daten** aus.

Felder der Registerkarte „Daten“.

Feld	Beschreibung
Berichtname	Name des Berichts.
Quelltyp	Typ der Quelle, aus der Daten abgerufen werden. Wählen Sie **Tabelle** aus.
Tabelle	Name der Tabelle, für die die Zusammenfassung erstellt wird. Wählen Sie die Tabelle mit den aggregierten Ergebnissen **Aggregiertes Ergebnis [sn_vul_cmn_aggregate_result]**aus.

3. Legen Sie im Bedingungsgenerator die Bedingung für die Zusammenfassung fest, für die Sie einen Bericht generieren möchten.

Bedingung im Bedingungsgenerator

Teil	Beschreibung
Feld	Wählen Sie **Zusammenfassung**aus.
Betreiber	Auswählen **ist**.
Wert	Name der Zusammenfassung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie auf der Registerkarte **Datendie Option Weiter**aus.
5. Wählen Sie auf der Registerkarte **Typen** aus, wie die Daten visualisiert werden sollen, und wählen Sie **Weiter**.
   Weitere Informationen zu den Berichtstypen finden Sie unter Berichte erstellen .

   Die unterstützten Visualisierungen sind Balkendiagramm, Kreisdiagramm und Heatmap. Sie können die Liniendiagramme und andere Trendvisualisierungen ändern, um die unterstützten Visualisierungen mit aggregiertem Ergebnis zur Darstellung derselben Daten zu verwenden. Die Listenansicht wird nicht unterstützt.
6. Füllen Sie die Felder auf der Registerkarte **Konfigurieren** aus.

Feld	Beschreibung
Gruppieren nach	Gruppiert die Daten nach dem ausgewählten Feld. Wählen Sie hier das Feld aus, das Sie im Feld **Gruppiert nach 1** auf der Registerkarte #unique_468_Connect_42_group-by der Zusammenfassung ausgewählt haben.
Stapeln nach	Organisiert Daten in Ebenen basierend auf dem ausgewählten Feld. Wählen Sie hier das Feld aus, das Sie im Feld **Gruppiert nach 2** auf der Registerkarte #unique_468_Connect_42_group-by der Zusammenfassung ausgewählt haben. **Hinweis:** Nur Balken- und horizontale Balkenberichte verwenden gestapelte Daten. Andere Berichtstypen ermöglichen nur die Gruppierung.
Aggregation	Wenden Sie **die Minimum-** oder **Maximum** -Funktion auf **den Wert**an.

7. Füllen Sie auf der Registerkarte **Stil** die Felder entsprechend aus, und wählen Sie **Ausführen**aus.
   Weitere Informationen zu den Feldern auf den Registerkarten **Konfigurieren** und **Stil** finden Sie im Video zum Erstellen eines Berichts .
8. Legen Sie im Bedingungsgenerator die Bedingung für die Zusammenfassung fest, für die Sie einen Bericht generieren möchten, und wählen Sie **Ausführen**.

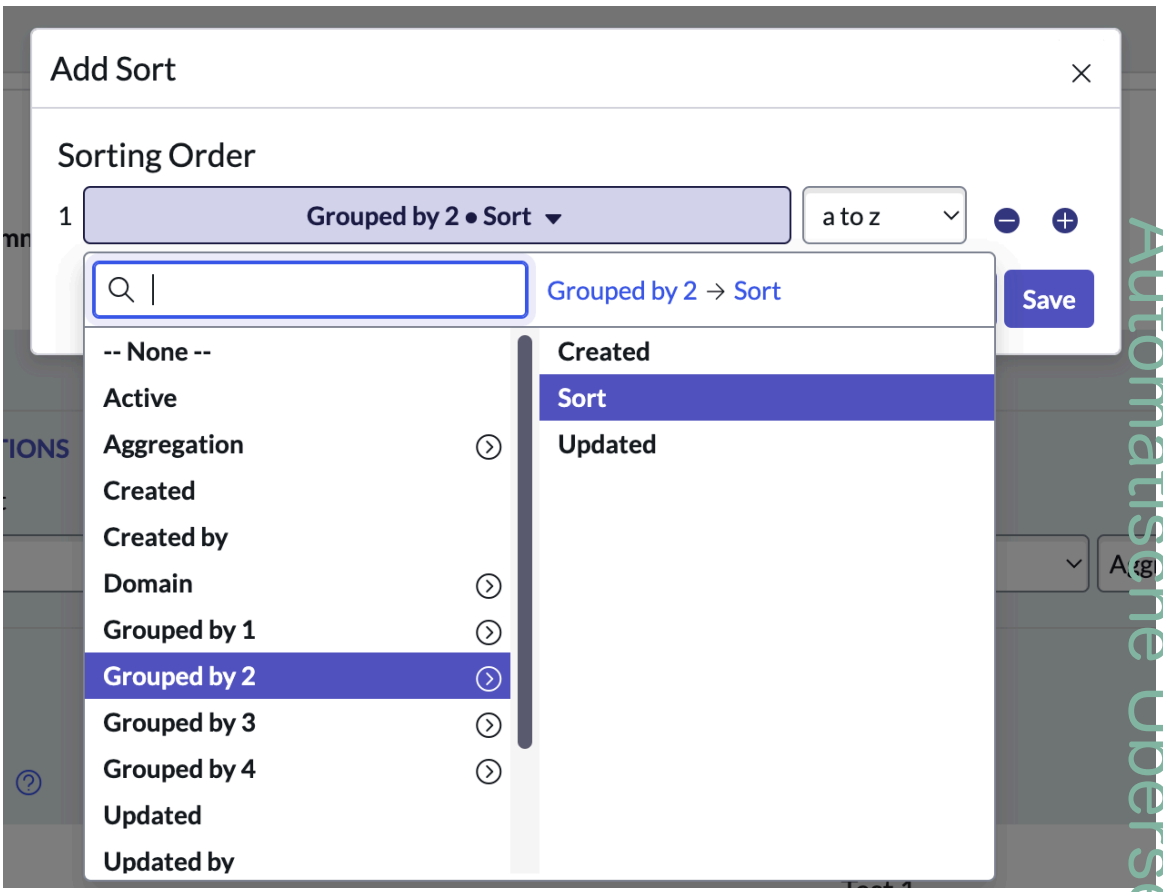
   Der Bericht wird angezeigt.
9. Um die Werte auf der X-Achse zu sortieren, wählen Sie **Sortierung hinzufügen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Geben Sie für Zeichenfolgen die Bedingung **Gruppiert nach > az oder za an,** um die Zeichenfolgen in alphabetischer Reihenfolge zu sortieren.

b. Geben Sie für Werte vom Datentyp „Ganzzahl“ und „Datum“ die Bedingung „ **Gruppiert nach.sortieren > az“ oder „za“** an, um die Werte in aufsteigender bzw. absteigender Reihenfolge zu sortieren.

Ganzzahlen auf der X-Achse werden sortiert

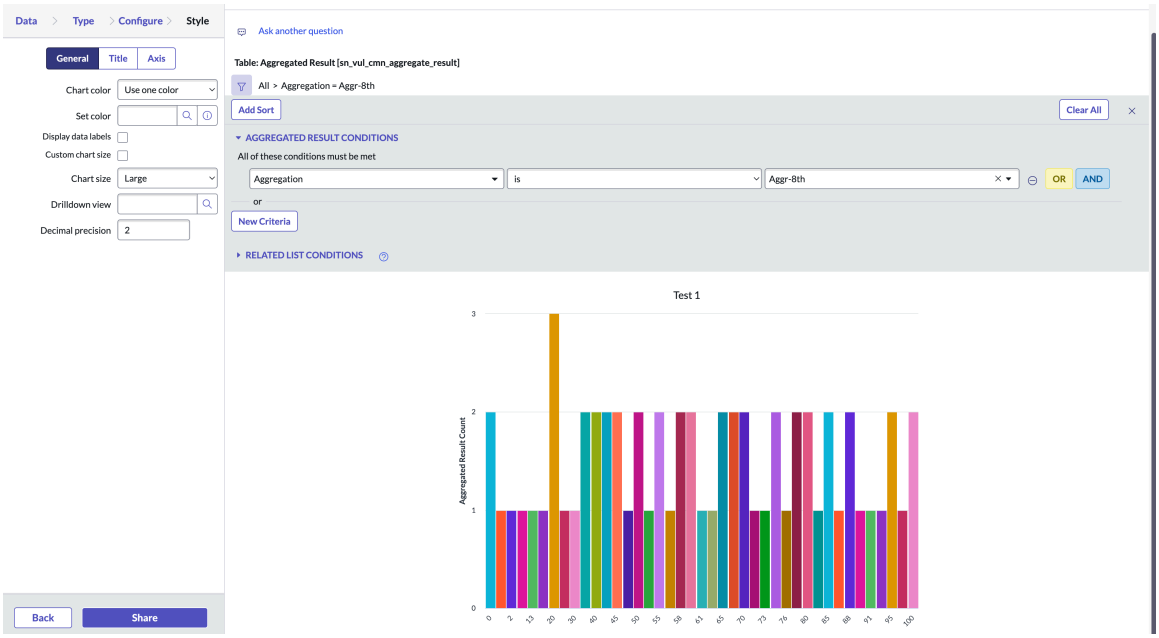


c. Wählen Sie **Ausführen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Ganzzahl- und Datumswerte werden auf der X-Achse sortiert.



10. Wählen Sie **Speichern**, um Ihren Bericht zu speichern.
    Der für eine Zusammenfassung generierte Bericht wird auf der Registerkarte **Ergebnisse** des entsprechenden **Zusammenfassungsformulars** angezeigt.

11. **Wahlweise:** Fügen Sie Ihren Bericht einem Dashboard hinzu.
    Weitere Informationen zum Hinzufügen eines Berichts zu einem Dashboard finden Sie unter Einem reaktionsfähigen Dashboard einen Bericht hinzufügen .

    Das Dashboard **„Schwachstellenmanagement [Aggregiert]“,** das aus Berichten besteht, die mit dem zwischengespeicherten Reporting-Framework erstellt wurden, ist im Lieferumfang des Basissystems enthalten. Um dieses Dashboard anzuzeigen, navigieren Sie zu **Alle** > **Performance Analytics** > **Dashboards** > **Alle** > **Schwachstellenmanagement [Aggregiert]**. Die aktiven Zusammenfassungen, die den Berichten in diesem Dashboard entsprechen, sind im Basissystem enthalten.

12. Geben Sie Ihren Bericht für andere Benutzer frei.
    Weitere Informationen zum Freigeben von Berichten finden Sie unter Berichte verteilen .

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Framework für zusammengefasste Berichte

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Vulnerability Response Referenzinformationen

Die folgenden Themen enthalten Links, Referenzinformationen, Artikel zur Problembehandlung und Wissensartikel sowie Felddaten in den Formularen und Datensätzen in Vulnerability Response.

Nachfolgend finden Sie einige Links zu anderen Ressourcen, die für Sie hilfreich sein könnten, beginnend mit einem Link zu den Knowledge Base-Links für Support- und Problembehandlungs-VR/CC-Artikel in der HI Knowledge Base.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Knowledge Base-Links für Support und Problembehandlung VR/CC
- Weitere Informationen zu Anwendungen und Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen .
- Security Operations-Videos
- Entwicklerschulungen
- Entwicklerdokumentation
- Arbeiten Sie mit einem Implementierungsspezialisten zusammen, um mit dem Customer Success Center die gewünschten Geschäftsergebnisse zu erzielen.
- Nehmen Sie an einem Vulnerability Response-Kurs teil, um Fachwissen aufzubauen und ROI schneller zu erzielen. Besuchen Sie zur Anmeldung die ServiceNow-Schulungs- und -Zertifizierungs-Website .
- Suchen Sie mit einer Anwendung installierte Komponenten
- Vulnerability Response Orchestration
- Tipps zum Schreiben von Integrationen
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Implementierungsprüfliste für die Anwendung Vulnerability Response

Diese Prüfliste listet die Schritte auf, die für eine grundlegende Implementierung der Anwendung Vulnerability Response in Ihrer Instanz Now Platform® von erforderlich sind. Wenn Sie diese Aufgaben abgeschlossen haben, ist das Basissystem betriebsbereit und kann verifiziert werden.

Vorbereitungen

Erforderliche Rolle: „admin“ für das Herunterladen und Aktivieren von Anwendungen und das Zuweisen von Rollen, „sn_vul.vulnerability_admin“ für die Konfiguration von Vulnerability Response.

Prozedur

1. Erwägen Sie, eine PDF-Datei dieser Prüfliste zu erstellen und zu drucken, damit Sie Aufgaben nach dem Abschluss abchecken können.
2. Um eine PDF-Datei zu generieren, klicken Sie oben im Thema auf das Symbol **„Als PDF speichern“** ( ) und dann auf Ausgewähltes Thema.

Vulnerability Response Grundlegende Implementierungsprüflistenaufgaben für Administratoren

Artikel	Beschreibung
☐	Vergewissern Sie sich als Benutzer mit der Rolle admin, dass Sie über Berechtigungen verfügen und die folgenden Anwendungen von ServiceNow® Store auf Ihre Instanz Now Platform herunterladen (**installieren**):

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	○ Vulnerability Response ○ Vulnerability Response Integration in die US-Schwachstellendatenbank (National Vulnerability Database) des NIST ○ Qualys Integration for Security Operations **a.** Um zu überprüfen, ob die Anwendungen in Ihrer Instanz verfügbar sind, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie nach [sn_vul], [sn_vul_nvd] und [sn_vul_qualys]. **b.** Wenn Sie die Anwendungen nicht finden können, finden Sie unter Security Operations und ServiceNow Store weitere Informationen zum Erhalt von Berechtigungen und zum Herunterladen der Anwendungen.
☐	Navigieren Sie als Benutzer mit der Administratorrolle zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung** und aktivieren (**installieren**) Sie die Anwendung Vulnerability Response zusammen mit ihren Abhängigkeiten in Ihrer Instanz Now Platform. **Hinweis:** Während der Installation der Anwendung Vulnerability Response können Sie Demodaten installieren. Demodaten sind erforderlich, wenn Sie automatisierte Tests ausführen möchten, um zu bestätigen, dass Ihre Instanz nach der Installation funktioniert. Führen Sie Tests nur für Entwicklungs-, Test- und andere Instanzen außerhalb der Produktion aus, um Datenbeschädigungen und -ausfälle zu vermeiden. Wenn Demodaten oder Demo-Accounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird. Der Setup-Assistent für Vulnerability Response wird automatisch zusammen mit der Anwendung installiert. Der Setup-Assistent ist erforderlich, um die Anwendung Vulnerability Response zu konfigurieren. Darüber hinaus wird es verwendet, um die in diesem Beispiel verwendete Anwendung Qualys Integration for Security Operations sowie andere Anwendungen, die Vulnerability Responseunterstützen und mit ihnen kompatibel sind, zu installieren und zu konfigurieren. Weitere Informationen zum Installieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren.
☐	Navigieren Sie als Benutzer mit der Administratorrolle im Setup-Assistenten zu **Alle** > **Vulnerability Response-Anwender und -Gruppen** und weisen Sie Anwendern die erforderlichen Vulnerability Response Persona-Rollen zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	a. Zeigen Sie im Setup-Assistenten vorhandene Benutzer und alle bereits zugewiesenen Rollen an, indem Sie auf den Link **des Moduls Benutzeradministration** klicken. **b.** Klicken Sie in der Liste auf einen Anwendernamen, um den Datensatz zu öffnen, und klicken Sie auf die zugehörige Liste **„Rollen“**. Alle diesem Anwender zugewiesenen Rollen werden angezeigt. **c.** Navigieren Sie zurück zu **Vulnerability Response-Anwender und -Gruppen** in Setup-Assistent und folgen Sie den Eingabeaufforderungen, um die Rolle sn_vul.vulnerability_admin zuzuweisen. **Hinweis:** Die Rolle sn_vul.vulnerability_admin ist erforderlich, um mit der Konfiguration fortzufahren. Alternativ können Sie mit der Konfiguration als Benutzer mit der Administratorrolle fortfahren. (Optional) Sie können auch die Rollen Configuration Item (CI)-Manager [sn_vul.ci_manager] und Ausnahmegenehmiger [sn_vul.exception_approver] zuweisen. Diese Personae sind jedoch für die verbleibenden Setupaufgaben nicht erforderlich. Weitere Informationen zum Zuweisen der Persona-Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zu Benutzern und zum Zuweisen von Rollen zu Benutzern und Gruppen finden Sie unter Benutzeradministration.
☐	**a.** Navigieren zu **Alle** > **Administration** > **Integrationen** prüfen, ob die **CWE Comprehensive 2000 Integration** aktiviert ist, und die geplante Aufgabe zum Importieren von Daten ausführen. **b.** Navigieren Sie als Benutzer mit der Administratorrolle zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** und aktivieren (**installieren**) Sie die Anwendung Vulnerability Response Integration with NVD. Führen Sie die NVD- und CWE-Integrationen im Rahmen der Ersteinrichtung von Vulnerability Response und bevor Sie Schwachstellendaten mit dem Scannerprodukt eines Drittanbieters in Ihre Instanz importieren. Weitere Informationen zum Installieren, Konfigurieren und Anzeigen der NVD- und CWE-Bibliotheken finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien und Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus.
☐	Navigieren Sie als Benutzer mit der Administratorrolle zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung** und aktivieren Sie die Anwendung Qualys Integration for Security Operations. Bevor Sie ein Scannerprodukt eines Drittanbieters wie Qualys mit einer Bibliothek installieren und ausführen, müssen Sie zuerst die NVD-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	und CWE-Integrationen installieren und ausführen, um Schwachstellendaten zu erfassen. Weitere Informationen finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.
☐	(Optional) Wenn Sie als Benutzer mit der Administratorrolle Demodaten mit der Anwendung Vulnerability Response installiert haben, können Sie die ATF-Test-Suite Vulnerability Response ausführen, um zu überprüfen, ob die Anwendungen erfolgreich installiert wurden. **Hinweis:** Führen Sie Tests nur für Entwicklungs-, Test- und andere Instanzen außerhalb der Produktion aus, um Datenbeschädigungen und -ausfälle zu vermeiden. Weitere Informationen finden Sie unter Führen Sie die Automated Test Framework-Test-Suite (ATF) für aus Vulnerability Response. Weitere Informationen zu automatisierten Tests finden Sie unter Automated Test Framework (ATF).

3. Fahren Sie mit der Konfiguration der Anwendungen fort, beginnend im Abschnitt „Einstellungen für Vulnerability Response“.

Wenn Sie sich diese Einstellungen ansehen, verstehen Sie, wie Vulnerability Response funktioniert, während Sie mit der Einrichtung Ihrer Umgebung fortfahren. Für die in diesem Beispiel verwendete Scannerintegration müssen Sie die Einstellungen bearbeiten.

Die in diesem Konfigurationsbeispiel verwendeten Konzepte für das Produkt Qualys gelten auch für andere Scanner-Anwendungen.

Zum Konfigurieren der Anwendung werden Ihre Qualys -Anmeldeinformationen benötigt. Stellen Sie sicher, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für Qualys -Produkte von erforderlich sind, damit Sie darauf zugreifen können.

Erforderliche Rolle: sn_vul.vulnerability_admin oder alternativ admin.

Vulnerability Response Grundlegende Implementierungsprüflistenaufgaben für Schwachstellenadministratoren

Aufgabe	Beschreibung
☐	Überprüfen Sie die Zuweisungsregeln für Schwachstellen. Zuweisungsregeln weisen angreifbare Elemente (VIs) automatisch der entsprechenden Zuweisungsgruppe zu. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Weitere Informationen zum Konfigurieren von Vulnerability Response mit dem Setup-Assistenten finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
☐	Überprüfen Sie die Regeln für Korrekturaufgaben. Die Regeln für Korrekturaufgaben gruppieren automatisch angreifbare Elemente (VIs), wenn sie basierend auf bestimmten Bedingungen importiert werden. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.
☐	Überprüfen Sie die Risikorechner. Risikorechner bewerten angreifbare Elemente für die Priorisierung. Sie können Rechner so konfigurieren, dass sie Merkmale des Konfigurationselements (Configuration Item, CI), Exploit-Verfügbarkeit und Schwachstellenschweregrad berücksichtigen, die von Ihrem Lieferanten für Schwachstellenbewertungen (Scanner) gemeldet werden. Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.
☐	Überprüfen Sie die Korrekturzielregeln. Korrekturzielregeln definieren Korrekturzeitleisten für AEs und Korrekturaufgaben. Weitere Informationen finden Sie unter Vulnerability Response Korrekturzielregeln.
☐	Überprüfen Sie im Abschnitt „Integrationskonfiguration“ die Anwendungseinstellungen Qualys, und definieren und planen Sie Ihre Datenimporte. **a.** Klicken Sie auf **Scannerintegrationen**. **b.** Klicken Sie auf der Seite Installierte Anwendungen **auf Bearbeiten**. **c.** Geben Sie Ihre Anmeldeinformationen ein, und klicken Sie auf **Weiter**. **d.** Lesen Sie die Beschreibungen für die KnowledgeBase-Konfiguration. **e.** Überprüfen Sie die Seite „Konfiguration der Host-Erkennung“ auf Importeinstellungen, CI-Suchregeln und Importzeitpläne. **f.** Wenn Sie mit den Einstellungen auf dieser Seite zufrieden sind, klicken Sie auf **Jetzt ausführen**, um Daten zu importieren. Klicken Sie auf den angezeigten Link **Details** anzeigen, um den Ausführungsstatus der Schwachstellenintegration anzuzeigen. **g.** (Optional) Bearbeiten Sie die Konfigurationseinstellungen weiter. **h.** Klicken Sie auf **Fertigstellen**, um die Installation und Konfiguration im Setup-Assistenten abzuschließen. Weitere Informationen zum Konfigurieren der Anwendung Qualys finden Sie unter Qualys Vulnerability Integration mit dem Setup-Assistenten konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Herzlichen Glückwunsch! Sie haben die Anwendung Vulnerability Response erfolgreich installiert und zusammen mit einer Scanner-Anwendung mit dem Setup-Assistenten konfiguriert. Das Basissystem ist jetzt betriebsbereit.

Um andere -Anwendungen für Vulnerability Responseherunterzuladen, zu installieren und zu konfigurieren, befolgen Sie die gleichen Schritte und Konzepte aus der vorherigen Prüfliste. Weitere Informationen finden Sie in den spezifischen Themen für die einzelnen Anwendungen.

Weitere Informationen zu unterstützten Anwendungen, die Ihnen ab ServiceNow Store für Vulnerability Responsezur Verfügung stehen, finden Sie unter Installation von Vulnerability Response und unterstützten Anwendungen.

Weitere Informationen zur Verwendung von Vulnerability Responsefinden Sie unter Die Anwendung Vulnerability Response erkunden.

Vulnerability Response Status der Korrekturaufgaben

Drittanbieterintegrationen importieren Erkennungsdaten für angreifbare Elemente, die neue VITs erstellen oder vorhandene VITs aktualisieren. Erkennungsstatus aktualisieren VIT-Status, sofern sie „Offen“ oder „Geschlossen“ sind.

Weitere Informationen dazu, wie sich der Status einer Erkennung auf den Status einer VIT auswirkt, finden Sie unter Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente.

Mit Change Management für Vulnerability Responsebesteht eine synchronisierte Beziehung zwischen den Statusfeldern der Korrekturaufgaben und den Statusfeldern der Change-Anforderungen (CHG) in Vulnerability Response. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie automatisch auch den Status aller zugehörigen Korrekturaufgaben. Nachdem eine Change-Anforderung implementiert wurde, wird die Korrekturaufgabe automatisch gelöst. Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Hinweis:

Ab v23.0 von Vulnerability Response:

- Der Workflow **„Statusgenehmigung für Korrekturaufgabe“** ist veraltet und wird durch den Flow „Statusgenehmigung für Korrekturaufgabe“ im Flow Designer ersetzt.
- Die Schaltfläche **„Schließen“** wurde für eine Korrekturaufgabe entfernt, und das Schließen einer Korrekturaufgabe wird vom Scanner gesteuert.

In der folgenden Tabelle sind die Korrekturaufgabenstatus und die Aktionen aufgeführt, die Sie für eine Korrekturaufgabe im jeweiligen Status ausführen können:

Status der Korrekturaufgaben

Status	Beschreibung
Öffnen	Status beim Erstellen. In diesem Status können Sie: **Doppelte VIs anzeigen** Identifizieren Sie doppelte VITs, die von mehreren Scannern im System gemeldet wurden. Sie können die doppelte VIT als Gelöst oder Geschlossen markieren. Doppelte Einträge werden nur angezeigt, wenn die Kombination von Schwachstellen mit Common Vulnerabilities and Exposures (CVE)erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Korrekturaufgaben (Fortsetzung)

Status	Beschreibung
	Weitere Informationen finden Sie unter Vulnerability Response Korrekturaufgabe und Status angreifbarer Elemente. **Untersuchung starten** Weisen Sie diese Korrekturaufgabe einer Person oder Gruppe zu, um mit der Untersuchung zu beginnen. **Als falsch positiv markieren** Markieren Sie ein Element oder eine Gruppe als falsch positiv, wenn der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, in Tatsächlich aber keine Schwachstelle vorliegt. **Ausnahme anfordern** Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (Bis) und einen Grund an, und geben Sie optional zusätzliche Informationen an. Verschiebt die Korrektur des Elements oder der Gruppe bis zu dem Datum, an dem eine Ausnahme angefordert wird. **Lösen** Als gelöst markieren, um das Element oder die Gruppe in den Status „Gelöst“ zu versetzen. **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Korrekturaufgabe aufteilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe in in IT Remediation Workspace. **Zurückstellen** Wählen Sie den Status Zurückgestellt, ein Datum der Wiedereröffnung, einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der Wiedereröffnung. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Gruppe.
Wird untersucht	Wird durch die Schaltfläche **„Untersuchung starten“** ausgelöst. In diesem Status können Sie: **Security Incident** Weitere Informationen hierzu finden Sie unter Security Incidents erstellen. **Change erstellen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Korrekturaufgaben (Fortsetzung)

Status	Beschreibung
	Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Aufgabe teilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf. **Erstellt eine Change-Anforderung** Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe. **Warten auf Implementierung** Ändert den Status in „Warten auf Implementierung“. Dieser Status gibt an, dass Korrekturaufgaben außerhalb eines Vulnerability Responseverwiesen wurden. **Zurückstellen** Wählen Sie den Status Zurückgestellt, ein Datum der Wiedereröffnung, einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der Wiedereröffnung. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.
Zurückgestellt	Wird durch die Schaltfläche **„Ausnahme anfordern“** ausgelöst. Im Rahmen des Genehmigungs-Workflows lautet der Status „Zurückgestellt“ „Wird überprüft“ und kann erst geschlossen werden, wenn er genehmigt wurde. In diesem Status können Sie: **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Aufgabe teilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue SG verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf. **Security Incident**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Korrekturaufgaben (Fortsetzung)

Status	Beschreibung
	Weitere Informationen hierzu finden Sie unter Security Incidents erstellen. **Erneut öffnen** Wechseln Sie zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. Aufschubinformationen werden unter der Registerkarte **Schließen/ Zurückstellen** angezeigt. Am Zurückstellungsdatum wird die Gruppe erneut zur Korrektur geöffnet.
Warten auf Implementierung	Wird durch die Schaltfläche **Warten auf Implementierung** ausgelöst. In diesem Status können Sie: **Security Incident** Weitere Informationen hierzu finden Sie unter Security Incidents erstellen. **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Aufgabe teilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf. **Erstellt eine Change-Anforderung** Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe. **Zurückstellen** Wählen Sie den Status Zurückgestellt, ein Datum der Wiedereröffnung, einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der Wiedereröffnung. **Lösen** Fügen Sie Notizen hinzu. Der Status wird zu Gelöst. Hinweise werden unter der Registerkarte **Lösung** angezeigt. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.
Gelöst	Wird über die Schaltfläche **„Lösen“** ausgelöst. In diesem Status können Sie: **Security Incident**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Korrekturaufgaben (Fortsetzung)

Status	Beschreibung
	Weitere Informationen hierzu finden Sie unter Security Incidents erstellen. **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Erneut öffnen** Wechseln Sie zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. Notizen werden unter der Registerkarte **Notizen** angezeigt. Lösungsinformationen werden unter der Registerkarte **Lösung** angezeigt.
Abgeschlossen	Ausgelöst vom Scanner. In diesem Status können Sie: **Security Incident** Weitere Informationen hierzu finden Sie unter Security Incidents erstellen. **Erneut öffnen** Wechseln Sie zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. Abschlussinformationen werden unter der Registerkarte **Schließen/ Zurückstellen** angezeigt.

- Der Korrekturbesitzer kann nur ein angreifbares Element oder eine Korrekturaufgabe als gelöst markieren. Basierend auf der Bestätigung vom Scanner kann dieses gelöste Element oder diese Korrekturaufgabe als geschlossen oder erneut geöffnet markiert werden.
- Die Schaltfläche **Löschen** ist für den Administrator verfügbar, wenn mehrere angreifbare Elemente manuell erstellt wurden und diese geschlossen oder gelöscht werden müssen.
- Wenn Sie feststellen, dass die Elemente ein geringes Risiko darstellen und auf ein Change-Fenster oder einen Patch warten, können Sie die Korrekturaufgabe für eine bestimmte Zeit [] in den Status Zurückstellenrotändern. Mit der Option **„Ausnahme anfordern“** können Sie eine Ausnahme anfordern.

Hinweis:
Wenn Korrekturaufgaben zurückgestellt oder geschlossen werden, können Sie Lösungen angeben, um die Gründe dafür genauer zu definieren.

- Wenn ein VIT manuell oder automatisch erneut geöffnet wird, geschieht Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der VIT-Status ändert sich in Offen. Der ursprüngliche Status der Korrekturaufgabe wird nicht aktualisiert.
- Die VIT wird neu bewertet und in eine neue oder vorhandene Korrekturaufgabe aufgenommen, die auf den aktiven Regeln für Korrekturaufgaben basiert.

Dadurch wird der Verlauf beibehalten, während eine weitere Korrektur ermöglicht wird.

- Wenn eine Korrekturaufgabe erstellt (automatisch oder manuell) oder aufgeteilt wird, werden ihre Felder **Status**, **Grund**und **Bis** ausgewertet. Im Falle der Aktion „Teilen“ werden diese Felder sowohl für die alten als auch für die neuen Korrekturaufgaben ausgewertet. Wenn eine VIT aktualisiert wird, werden die Felder **Status**, **Grund**und **Bis** aller zugehörigen Korrekturaufgaben ausgewertet.
  - Wenn alle VITs in einer Korrekturaufgabe zurückgestellt werden und denselben Grund haben, ändert sich der Status der Korrekturaufgabe in **Zurückgestellt**, und der Grund der VITs wird der Korrekturaufgabe zugewiesen. Wenn sich die VITs im Grund unterscheiden, wird der Grund der Korrekturaufgabe in **Keine**geändert.
  - Das nächstgelegene **Bis-** Datum aller VITs wird im Feld **Bis** der Korrekturaufgabe aktualisiert.
  - Wenn Sie eine VIT erneut öffnen, ändert sich der Status der Korrekturaufgabe in **Offen**.

  Diese Bewertung wird von der geplanten Aufgabe *`Rollup vulnerability item values to vulnerability and group`* durchgeführt, die alle 15 Minuten ausgeführt wird.

Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente

Drittanbieterintegrationen rufen die Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, die von den Scannern gemeldet werden.

Erkennungsdaten werden mit angreifbaren Elementen (VIs, VITs) gekoppelt, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn kein VI gefunden wird, wird ein neues erstellt. Erkennungen werden nur von den Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden wurden.

Wenn alle Erkennungen für ein angreifbares Element geschlossen sind, wird dieses angreifbare Element geschlossen. Im VI-Datensatz lautet der Status Geschlossen/Behoben. Wenn alle VIs für eine Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen. Der Statusfluss bleibt ansonsten derselbe.

Geschlossene VIs mit dem Substatus „Repariert“ oder „Veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIs mit der neuen Schwachstelle abgeglichen werden können.

Ab Version 20.0 von Vulnerability Responsegilt: Wenn eine Erkennung veraltet ist und sich das zugehörige VI im Status „Geschlossen“ befindet, wechselt der Status des VI nicht in „Geschlossen – Veraltet“. Dies dient dazu, zu verhindern, dass das AE erneut geöffnet wird, wenn eine neue Erkennung erkannt wird, damit Sie nicht den gesamten Anforderungs- und Genehmigungsprozess für falsch positive Meldungen durchlaufen müssen. Um dieses Verhalten umzukehren, deaktivieren Sie im Formular „Konfiguration für automatisches Schließen“ das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren**. Weitere Informationen finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

Gemäß der Skripteinbindung *`DetectionBase`*, Methode *`_shouldReOpenVI()`*wird das VI, das zuvor mit dem Substatus „Repariert“, „Veraltet“ oder „CI außer Betrieb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

genommen“ Geschlossen war, erneut geöffnet, und die Erkennung wird der vorhandenen VIT zugeordnet.

Angenommen, das Datum der Schließung eines AE liegt nach dem Datum der letzten Feststellung einer Erkennung. Sie erwarten, dass diese VI-Datensätze geschlossen bleiben. Wenn Sie jedoch sehen, dass ein zuvor geschlossenes VI erneut geöffnet wurde, bedeutet dies, dass das VI von einer früheren Erkennung geschlossen wurde und die Schwachstelle bei einem späteren Scan erneut gefunden wurde. Wenn eine neue Erkennung gefunden wird, die mit der geschlossenen VIT übereinstimmt, die dieselbe Schwachstelle im Configuration Item des VI aufweist, wird das VI erneut geöffnet.

Korrekturaufgaben und Status angreifbarer Elemente

Korrekturaufgaben und der Status angreifbarer Elemente können sich gegenseitig beeinflussen. Meistens wird durch den Status einer Korrekturaufgabe der Status eines angreifbaren Elements aktualisiert, wobei der Status der höchsten Prioritätsaufgabe zur Aktualisierung der angreifbaren Elemente in der Gruppe verwendet wird.

Die Statusrangfolge ist wie folgt.

Zurückgestellt > **Gelöst** > **Warten auf Implementierung** > **Wird untersucht** > **Offen**

- Wenn sich eine Gruppe angreifbarer Elemente in einer Korrekturaufgabe befindet und nicht auf individueller Ebene geändert wird, hat sie denselben Status wie ihre Korrekturaufgabe.
- Wenn die Korrekturaufgabe vom Status „Offen“ in „Warten auf Implementierung“ übergeht, werden alle VIs in der Korrekturaufgabe in den Status Warten auf Implementierung verschoben.
- Wenn die Korrekturaufgabe zurückgestellt wird, wird auch das AEs zurückgestellt.
  Ab Version 16.5 können Sie nachverfolgen, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Die regelmäßige Aufgabe `set deferral counts` wird täglich ausgeführt, um die Anzahl der Datensätze zu erfassen, die in der Spalte Anzahl der Zurückstellungen in den Modulen für mehrere Zurückstellungen für VR, AVR und CVR mehr als einmal zurückgestellt wurden. Alle Anzahlen für VIs, die einer Korrekturaufgabe zugeordnet sind, werden gesammelt und veröffentlicht, wenn eine Korrekturaufgabe mehr als einmal zurückgestellt wird.

Angreifbare Elemente werden nur durch Korrekturaufgaben aktualisiert

Elemente entsprechen dem Status der Korrekturaufgabe, wenn sie nicht einzeln aktualisiert wurden. Ausnahmen:

- Wenn sich der Status der Korrekturaufgabe in Geschlossen und die Lösung in Abgebrochen oder Behoben mit Ausnahme ändert, ist das Element nicht betroffen und nimmt den Status einer anderen Korrekturaufgabe an, die es enthält. Wenn sich das angreifbare Element in keiner anderen Korrekturaufgabe befindet, wird es in den Status „Offen“ zurückversetzt.
- Wenn der Status des angreifbaren Elements Geschlossen/Behoben ist (aktualisiert durch Scan oder Import), bleibt das angreifbare Element im Status Geschlossen/Behoben, wenn die Korrekturaufgabe ihren Status ändert. Diese Bedingung ist unabhängig vom Status der Korrekturaufgabe „wahr“.

Angreifbare Elemente in Status, die einzeln festgelegt werden

Angreifbare Elemente in einem Status, der für das Element aktualisiert wurde, z. B. einzeln geschlossene oder zurückgestellte Elemente, stimmen nicht automatisch mit dem Status der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgabe überein. Stattdessen wird der Status mit dem aller zugeordneten Gruppen verglichen, um den Status mit der höchsten anzuwendenden Priorität zu ermitteln.

Hinweis:
Der Status „Geschlossen“/„Repariert“ ist ein Sonderfall. Wenn bei angreifbaren Elementen, die auf den Status Geschlossen/Behoben festgelegt sind, alle angreifbaren Elemente in einer Korrekturaufgabe auf Geschlossen/Behoben gesetzt sind (z. B. wenn ein Scanner feststellt, dass alle Schwachstellen behoben wurden), wird die Korrekturaufgabe automatisch als gekennzeichnet Geschlossen/Behoben

Korrekturaufgaben enthalten leere Zuweisungsfelder

Wenn sich der Status der VIs in einer Korrekturaufgabe von Gelöst in Offen ändert, wird der Status der Korrekturaufgabe auch von Gelöst in Wird untersucht aktualisiert.

Wenn jedoch die Felder **Zugewiesen an** und **Zuweisungsgruppe** in der Korrekturaufgabe leer sind, verbleibt die Korrekturaufgabe im Status Gelöst und wird nicht in den Status Wird untersucht verschoben.

Die Zuweisungsgruppe für angreifbare Elemente wird nicht immer aktualisiert, wenn ihre Korrekturaufgabe aktualisiert wird

Wenn die Zuweisungsgruppe für ein VI im Status „Offen“ manuell aktualisiert wird, wird sie nicht erneut aktualisiert, wenn die Zuweisungsgruppe für die zugehörige Korrekturaufgabe aktualisiert wird. Diese Informationen werden nicht überschrieben, da die Zuweisungsgruppe für das AE absichtlich aktualisiert wurde und möglicherweise Teil einer anderen Korrekturaufgabe ist.

Status der Korrekturaufgabe für angreifbare Elemente (VIs) in mehreren Gruppen

Wenn sich ein VI in mehreren Korrekturaufgaben befindet (Gruppe in den folgenden Tabellen) und sein eigener Status nicht festgelegt wurde, bestimmt der Gruppenstatus mit höherer Priorität den Status dieses VI (siehe folgende Tabelle).

Beispiele für Status von angreifbaren Elementen

Status der Korrekturaufgabe	Status des angreifbaren Elements
Gruppe A: **Öffnen** > **Wird untersucht** Gruppe B: **Offen**	**Wird untersucht** Wenn für Gruppe A der Status „Wird untersucht“ und für Gruppe B der Status „Offen“ angegeben ist, ändert sich das Feld VI in „Wird untersucht“. Nach der Suche hat Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität.
Gruppe A: **Wird untersucht** Gruppe B: **Öffnen** > **Wird untersucht**	**Wird untersucht** Wenn bei Gruppe B der Status „Wird untersucht“ und bei Gruppe A untersucht wird, bleibt das Feld „Wird untersucht“. Nach der Suche haben sie zwischen Gruppe A und Gruppe B den Status mit der gleichen Priorität.
Gruppe A: **Wird untersucht** Gruppe B: **Wird untersucht** > **Warten auf Implementierung**	**Warten auf Implementierung** Wenn Gruppe B auf Implementierung wartet und Gruppe A untersucht wird, ändert sich das Feld VI in Warten auf Implementierung. Nach

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für Status von angreifbaren Elementen (Fortsetzung)

Status der Korrekturaufgabe	Status des angreifbaren Elements
	der Suche hat Gruppe B zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität.
Gruppe A: **Wird untersucht** > **Zurückgestellt** Gruppe B: **Warten auf Implementierung**	**Zurückgestellt** Wenn Gruppe A auf Zurückgestellt und Gruppe B auf Implementierung wartend gesetzt ist, ändert sich das Feld VI in Zurückgestellt. Nach der Suche hat Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität.

Angreifbares Element in Sonderfällen für mehrere Gruppen

Status der Korrekturaufgabe	Status des angreifbaren Elements
Gruppe A: **Wird untersucht** Gruppe B: **Warten auf Implementierung** > **Geschlossen (repariert oder storniert)**	**Wird untersucht** Wenn Gruppe B den Status „Geschlossen/Repariert“ oder „Geschlossen/Abgebrochen“ hat und für Gruppe A der Status „Wird untersucht“ lautet, ändert sich der AE von „Warten auf Implementierung“ (früher die höchste Priorität) in „Wird untersucht“ (derzeit die höchste Priorität).
Gruppe A: jeder Status Gruppe B: beliebiger Status	Wenn der Status der Quelle des angreifbaren Elements Repariert ist (durch Scan oder Import aktualisiert), ändert sich der Status des angreifbaren Elements in Geschlossen/Repariert, wenn die Gruppe ihren Status ändert. Diese Bedingung ist unabhängig vom Status der anderen zugeordneten Gruppen „wahr“. Die Suche nach angreifbaren Elementen für den Gruppenstatus findet nicht statt.

Wenn ein VI-Status einzeln festgelegt wird, wird sein Status wie bei jeder anderen Korrekturaufgabe bei der Bewertung der Rangfolge berücksichtigt. Wenn ein VI zu mehr als einer Korrekturaufgabe gehört, sind in der folgenden Tabelle die vorgenommenen Aktualisierungen aufgelistet.

Angreifbares Element Status einzeln auf Sonderfälle festgelegt

Status eines angreifbaren Elements innerhalb einer Gruppe	Endstatus des angreifbaren Elements
Status der Gruppe A: **Wird untersucht** Status der Gruppe B: **Wird untersucht** > **Warten auf Implementierung** Ursprünglicher AEs-Status: **Wird untersucht** > **(am AE festgelegt)**	**Warten auf Implementierung** Wenn Gruppe B zu „Warten auf Implementierung“ wechselt und Gruppe A weiterhin „Untersucht“ bleibt, ändert sich der VI in Warten auf Implementierung (höchste Priorität).
Gruppe A: **Wird untersucht**	**Zurückgestellt**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbares Element Status einzeln auf Sonderfälle festgelegt (Fortsetzung)

Status eines angreifbaren Elements innerhalb einer Gruppe	Endstatus des angreifbaren Elements
Gruppe B: **Wird untersucht** > **Warten auf Implementierung** Ursprünglicher AEs-Status: **Zurückgestellt** > **(am AE festgelegt)**	Wenn Gruppe B zu „Warten auf Implementierung“ wechselt und Gruppe A weiterhin „Untersuchung“ bleibt, verbleibt das AE im Status „Zurückgestellt“ (höchste Priorität).

Die folgende Tabelle zeigt, dass, wenn zwei Korrekturaufgaben mit gemeinsamen angreifbaren Elementen zurückgestellt werden, deren Status bis zum Erreichen des spätesten Datums zurückgestellt wird.

Sonderfälle mit zurückgestelltem Status für angreifbares Element

Status eines angreifbaren Elements innerhalb einer Gruppe	Endstatus des angreifbaren Elements
Status der Gruppe A: **Wird überprüft (bis 10. April)** Status der Gruppe B: **Wird untersucht** > **Wird überprüft (bis 30. April)** Ursprünglicher AEs-Status: **Wird überprüft (bis 10. April)** > **(am AE festgelegt)**	**Zurückgestellt (bis 30. April)** Wenn Gruppe B zu „Zurückgestellt“ wechselt (bis 30. April) und Gruppe A weiterhin „Zurückgestellt“ bleibt (bis 10. April), ändert sich das VI von „Zurückgestellt“ (bis 05. April) in den Status „Zurückgestellt“ (bis 30. April).
Gruppe A: **Wird überprüft (bis 15. Juli)** Gruppe B: **Wird untersucht** > **Wird überprüft (bis 10. Juli ...** Ursprünglicher AEs-Status: **Zurückgestellt** > **(bis 15. Juli)**	**Zurückgestellt (bis 15. Juli)** Wenn Gruppe B zu „Zurückgestellt“ wechselt (bis 10. Juli) und Gruppe A weiterhin „Zurückgestellt“ bleibt (15. Juli), bleibt das AEs in „Zurückgestellt“ (bis 15. Juli).

Zusätzliche Einstellungen für Domain Separation

Für eine präzise Ausführung und genaue Ergebnisse sind die folgenden Vorsichtsmaßnahmen und Einstellungen für die Domänentrennung in Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Complianceerforderlich.

Ändern Sie nicht die Geschäftslogiken und -prozesse in der globalen Domäne, um Probleme zu vermeiden, damit bei jedem Upgrade die neuesten Änderungen aktualisiert werden. Duplizieren Sie alle Geschäftslogiken und Prozesse in jeder Domäne separat, und stellen Sie sicher, dass sie in der globalen Domäne inaktiv sind. Andernfalls haben die Geschäftslogiken und -prozesse in der globalen Domäne Vorrang vor der untergeordneten Domäne. Angenommen, Sie haben eine Risikoregel in einer untergeordneten Domäne erstellt, und die globale Domäne verfügt über eine ähnliche Risikoregel. Dann hat die Regel der globalen Domäne Vorrang vor der Regel der untergeordneten Domäne.

Erneute Auswertung von Rechnern und Regeln

Vor v20.0 wird, wenn Sie Rechner oder Regeln erneut anwenden, die Kennzeichnung für die erneute Ausführung auf „Wahr“ gesetzt. Zudem wird eine Business Rule ausgelöst, um eine geplante Aufgabe auszuführen, die die Rechner und Regeln erneut anwendet. Ab v20.0

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

müssen Sie sich nicht mehr auf die Wiederholungskennzeichnung verlassen. Wenn Sie auf die Schaltfläche **Rechner erneut anwenden** klicken, wird ein Hintergrundauftrag ausgelöst, der die Rechner und Regeln erneut anwendet. Auf diese Weise können Sie Rechner und Regeln für alle Domänen erstellen.

Einstellungen für Rollup-Rechner

In einer Domäne darf nur ein Rollup-Rechner für eine Tabelle aktiv sein. Betrachten Sie beispielsweise die Tabelle „Korrekturaufgabe“ *sn_vul_vulnerability* mit dem Rollup-Rechner **Korrekturaufgaben-Rollup** in der globalen Domäne. Wenn Sie diesen Rollup-Rechner duplizieren, indem Sie die Gewichtungen für dieselbe Tabelle in derselben Domäne ändern, treten bei den Rollup-Berechnungen Diskrepanzen auf. Stellen Sie daher sicher, dass Sie nur einen Rollup-Rechner aktivieren, wenn zwei oder mehr Rollup-Rechner für eine Tabelle in derselben Domäne vorhanden sind.

Formularfelder „Erkannte Elemente“.

Assets werden automatisch mit Configuration Items (CIs) in Configuration Management Database (CMDB) abgeglichen, wenn sie mit den CI-Suchregeln importiert werden. Datensätze für nicht abgeglichene CIs werden bei Importen von Drittpartei-Schwachstellenintegrationen automatisch erstellt und in Erkannte Elemente aufgenommen. Für Cloud-Assets, die nicht in CMDB CI vorhanden sind, wird der Datensatz jedoch in der Cloud-Ressourcenklasse erstellt.

Felder „Erkannte Elemente“.

Die Informationen in diesen Datensätzen werden aus den Datensätzen der Drittpartei erfasst und während des Imports klassifiziert.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „Erkannte Elemente“ [sn_sec_cmn_src_ci] aufgeführt sind.

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, benötigen Sie mindestens die Rolle sn_vul.read_all.

Feld	Beschreibung
Nummer	Der dem Datensatz zugewiesene Bezeichner.
Konfigurationselement	Configuration Item, das aus der Quellintegration einer Drittpartei importiert wird. Ab v12.0 ist Configuration Item das neueste CI in der Liste der CIs, nachdem die außer Betrieb genommenen gefiltert wurden.
Klasse	Klasse, die dem CI während des Imports von Vulnerability Responsezugewiesen wurde.
Quelle	Quelle, die aus der Drittanbieterquellenintegration importiert wird.
CI-Übereinstimmungsregel	Die CI-Übereinstimmungsregel, die zum Erstellen des Elements verwendet wurde.
V18.0: Übereinstimmender Typ für DI	Übereinstimmender Typ, der zum Erstellen des erkannten Elements verwendet wird. Die Optionen sind: • Erstellt von VR • Erstellt von IRE • Abgeglichen mit CI-Suche • Abgeglichen mit IRE

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Manuell abgeglichen (Ab v24.0.6 von Vulnerability Responsekönnen Sie diese zusätzliche Option anzeigen. Diese Option wird automatisch festgelegt, wenn Sie ein CI im Formular „Erkanntes Element“ manuell aktualisieren.) Diese Informationen sind nur für Daten verfügbar, die für Vulnerability Response v18.0 und höher ausgefüllt werden. Bei vorhandenen Daten enthält diese Spalte keinen Wert. **Hinweis:** Wenn Sie die CI-Suchregeln erneut anwenden, werden möglicherweise einige CIs auf DIs aktualisiert, was dazu führt, dass diese Spalte ausgefüllt wird.
Andere übereinstimmende CIs	Liste der anderen Konfigurationselemente, die der CI-Suchregel entsprechen.
Status	Status des CI, der während des Imports bestimmt wird. Die Auswahlmöglichkeiten lauten wie folgt: • **Abgeglichen**: In der CMDB wurde ein übereinstimmendes Konfigurationselement gefunden. • **Nicht abgeglichen**: In der CMDB wurde keine Übereinstimmung gefunden. Ein Platzhalterdatensatz wird erstellt.
Erstellt	Datum, an dem der Datensatz für das erkannte Element erstellt wurde.
Aktualisiert	Datum, an dem der Datensatz des erkannten Elements aktualisiert wurde.
Aktualisiert von	Benutzer, der die Daten aktualisiert hat.
Host-Tag	Host-Tags, die diesem erkannten Element während des Imports zugewiesen wurden. Sie können bis zu 31 Host-Tags pro erkanntem Element verwenden.
Vollqualifizierter Domänenname	Daten, die diesem CI zugeordnet sind, wurden in der CMDB gefunden.
MAC-Adresse	Daten, die diesem CI zugeordnet sind, wurden in der CMDB gefunden.
Betriebssystem	Betriebssystem, das diesem CI zugeordnet ist.
NetBIOS	NetBIOS, das aus der Quellintegration der Drittpartei importiert wird.
IP-Adresse	Daten, die diesem CI zugeordnet sind, wurden in der CMDB gefunden.
Quelldaten	Aktuelle Daten, die diesem CI aus der Quelle zugeordnet sind.
V16: Ursprüngliche Quelldaten	Anfängliche Daten, die diesem CI aus der Quelle zugeordnet sind.
V16: CI neu bewerten	Empfängt Daten vom Scanner. Wenn aktualisierte Daten vorhanden sind, wird der Wert auf „wahr“ festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die Quelldatenwerte werden gemäß den aktuellen Quelldaten neu berechnet. Wenn aktualisierte Daten vom Scanner abgerufen werden, werden die Quelldaten aktualisiert. Der vorhandene Quelldatenwert wird in das ursprüngliche Quelldatenfeld verschoben. Um die erkannten Elemente neu auszuwerten, aktivieren Sie die Option CI-Suchregeln erneut anwenden für die geplante Aufgabe Changed Discovered Items (CI-Suchregeln erneut anwenden).
Agent ist vorhanden	Gibt „wahr“ an, wenn der Agent auf dem Asset installiert ist. Wenn die Werte für hostUID und UUID in der Spalte Quelldaten leer sind, wird dieser Wert als trueausgefüllt. **Hinweis:** Dieses Feld wird ab v19.0 von Vulnerability Responseangezeigt.

Ab v23.0 von Vulnerability Responsezeigt die Spalte **Compliance der Testergebnisse in % (CI)** den Prozentsatz der Testergebnisse an, die für das entsprechende CI konform sind. Um diesen Wert zu erhalten, müssen Sie in der geplanten Aufgabe **„Update remediation metrics“ (Remediationsmetriken aktualisieren)** die OptioncalcTRComplianceForCI auf true festlegen.

Hinweis:
Der Wert **Testergebnis-Compliance in % (CI)** wird nur für die erkannten Elemente ausgefüllt, die in der Spalte **Letztes Konfigurations-Compliance-Scandatum** oder **Nicht-Infra Letzter Compliance-Scan Datum** einen nicht leeren Wert haben.

Ab Version 18.0 von Vulnerability Responsekönnen die Scanner Qualys, Tenable for Vulnerability Response und Rapid7 die folgenden zusätzlichen Metadaten für Cloud-Assets empfangen.

Feld	Beschreibung
Cloud-Service-Provider	Name des Cloud-Service Providers, der Cloud-Computing-Services anbietet. Beispiel: Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP).
Cloud-Region	Standort, an dem die Ressource gehostet wurde.
Cloud-Account	Account, der von Cloud-Service Providern wie AWS, GCPusw. für den Zugriff auf Cloud-Computing-Services bereitgestellt wird.
Cloud-Ressourcentyp	Arten von Assets, die in der Cloud vorhanden sind, z. B. Amazon Elastic Compute Cloud-Computer (EC2), AWS S3-Buckets usw.
Ressourcen-ID	Eindeutiger Bezeichner, der einer Ressource in einer Cloud-Computing-Umgebung zugewiesen ist. Diese ID wird zum Identifizieren und Verwalten der Ressource verwendet.
Ressourcenname	Benutzerdefinierter Name, der zum Identifizieren und Verwalten einer Ressource in einer Cloud-Computing-Umgebung verwendet wird.
Image	Das Image eines virtuellen Computers oder Serverimages ist ein vorkonfigurierter virtueller Computer, der ein Betriebssystem, Anwendungen und andere Software enthält. Beispiel: Amazon Machine Image.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die neue CI-Suchregel „Cloud-Ressourcen-ID“ wurde eingeführt, um die Cloud-CIs basierend auf den Cloud-Metadaten abzugleichen.

Vulnerability Response Schwachstellenformularfelder

Schwachstellen werden automatisch erstellt, wenn Datensätze aus der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder Integrationen von Drittanbietern heruntergeladen und unter **Bibliotheken** in Vulnerability Responsegespeichert werden.

NVD-Eintragsfelder

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, benötigen Sie mindestens die Rolle sn_vul.read_all.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „National Vulnerability Database Entries“ [sn_vul_nvd_entry] aufgeführt sind.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Risikobewertung	(Ausgeblendet, wenn der Schwachstelle keine VITs zugeordnet sind) Quantifizierte **Risikopunktzahl,** die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikoeinstufungen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners. **Hinweis:** Diese **Basisrisikobewertung** ist nicht mit der **Risikobewertung des Lösungsdatensatzes identisch.**
Risikopunktzahl	(Ausgeblendet, wenn der Schwachstelle keine VITs zugeordnet sind) Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt. **Hinweis:** Diese Basis- **Risikopunktzahl** ist nicht identisch mit der **Risikopunktzahl des Lösungsdatensatzes.** Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle Schweregradzuordnungen werden für NVD und mit ServiceNow -Drittparteiintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung.
Exploit vorhanden	Ja, wenn dieser Schwachstelle mindestens ein Exploit zugeordnet ist.
Exploit-Kompetenzniveau	Niedrigste Kompetenzstufe, die zum Ausnutzen dieser Schwachstelle erforderlich ist.
Exploit-Angriffsvektor	Angreifbarster Angriffsvektor der Exploits für diese Schwachstelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Verfügbar, wenn SAM NVD aktiviert ist.
Aktive AEs	(Ausgeblendet, wenn der Schwachstelle keine VITs zugeordnet sind) Anzahl der angreifbaren Elemente, die dieser Schwachstelle zugeordnet sind und sich nicht im Status „Geschlossen“ befinden. Wenn für diese Schwachstelle keine aktiven AEs vorhanden sind, werden **Risikobewertung** und **Risikopunktzahl** nicht angezeigt.
CWE-Eintrag	Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Zusammenfassung	Beschreibung der Schwachstelle.
Bedrohungsinformationen (ab Vulnerability Response Version 20.0)	Threat Intelligence bereitgestellt von Qualys. Mit diesen Daten können Sie die Beweggründe, Ziele und das Angriffsverhalten eines Bedrohungsakteurs nachvollziehen.
Schwachstellendetails	
CVSS v2	CVSS v2-Daten importiert
CVSS v3	Importierte CVSS v3-Daten, vor 2015 nicht verfügbar.
Bevorzugte Lösung	(Ausgeblendet, wenn der Schwachstelle keine VITs zugeordnet sind) Höchste Ersatzlösung in der Kette, abgeleitet von den Lösungen, auf die in der Schwachstelle verwiesen wird. Wenn in der Kette mehr als eine höchste Ersatzlösung vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen.
CISA-Exploit (Diese Registerkarte ist nur verfügbar, wenn die Anwendung CISA installiert ist.)	
CISA-Fälligkeitsdatum	Frist für die Behebung der Schwachstelle.
Hinzugefügt am	Datum, an dem die Schwachstelle dem CISA-Katalog hinzugefügt wurde.
Produkt	Produkt, in dem die Schwachstelle identifiziert wurde.
Lieferant/Projekt	Lieferant, der der identifizierten Schwachstelle zugeordnet ist.
Bekannte Ransomware Ab v21.0 von Vulnerability Response.	Wird ausgewählt, wenn das Feld **, von dem bekannt ist, dass es in Ransomware-Kampagnen verwendet wird,** aus dem CISA-Katalog für bekannt ausgenutzte Schwachstellen (KEVs) erfasst wird. Die Kennzeichnung wird auf der Ebene „Allgemeine Schwachstellen und Risiken“ (Common Vulnerabilities and Exposures, CVE) festgelegt und ein Rollup bis zum Drittparteieintrag durchgeführt.
Nachbesserungsstatus	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
AEs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle.
AEs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle.
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle.
Zugehörige Links	
Zustand aktualisieren	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Aktualisiert Folgendes: • Status der Korrekturaufgabe • Risikopunktzahl und Bewertung • Metriken wie „Aktive VITs“, „VITs insgesamt“ aus dem Abschnitt „Korrekturstatus“.
Zugehörige Listen	
Angreifbare Elemente	(Ausgeblendet, wenn der Schwachstelle keine VITs zugeordnet sind) Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind.
Verwundbarkeitsreferenzen	Informationen zur Schwachstelle aus externen Quellen, angegeben von NVD.
Exploits	Exploits, die dieser Schwachstelle zugeordnet sind.
Lösungen	(Ausgeblendet, wenn der Schwachstelle keine VITs zugeordnet sind) Alle Vulnerability Solution Management -Integrationslösungen, die dieser Schwachstelle zugeordnet sind.
Schwachstellen	Importierte **Schwachstellendaten**, die Common Vulnerabilities and Exposures (CVE) zugeordnet sind.
Software mit Schwachstellen	(Ausgeblendet, wenn dem CVE Software zugeordnet ist) Importierte CPE-Daten (Common Platform Enumeration), die der Schwachstelle zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schwachstellen-Malware-Kits	Malware, die aus verschiedenen Scannerquellen für eine Schwachstelle importiert wurde.

Eingabefelder für CWE-Schwachstellen

Diese Felder befinden sich in Datensätzen, die in der Tabelle „CWEs“ [sn_vul_cwe] aufgeführt sind.

Feld	Beschreibung
CWE-ID	Bezeichner für diesen Schwachstelleneintrag. Dieser Bezeichner wird sowohl für Kategorien als auch für Schwachstellen verwendet und ist für die beiden Datensätze eindeutig.
Name	Beschreibender Name, der dieser CWE-ID zugewiesen ist.
Wahrscheinlichkeit der Ausnutzung	Wie wahrscheinlich ist, dass die Schwachstelle ausgenutzt wird, auf einer qualitativen Skala. Einer der folgenden: • Unbekannt • Niedrig • Mittel • Hoch
Position in OWASP Top 10	Die numerische Position dieser Schwachstelle in der OWASP-Top-10-Liste.
SANS bis Position 25	Numerische Position dieser Schwachstelle in der SAN-Top-25-Liste.
Klasse	Typ der Schwachstelle
Status	Einer der folgenden: • Unvollständig • Entwurf • Stabil • Überholt • Veraltet • Unstabil
Zusammenfassung	Einer der folgenden: • Variante • Klasse • Basis • Verbindung
Aktualisiert	Zeitpunkt der letzten Aktualisierung des Datensatzes in der Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Funktionsbereiche	Liste der betroffenen Funktionsbereiche. Beispiel: **Dateiverarbeitung**. Wird nur für 24/862-Schwächen ausgefüllt.
Betroffene Ressourcen	Liste der betroffenen Ressourcen. Zum Beispiel **Datei** oder **Verzeichnis**. Wird nur für 51/863-Schwächen ausgefüllt.
URL	Knowledge Base-Artikel, der dieser Schwachstelle zugeordnet ist.
Beschreibung	Beschreibung der Schwachstelle.
Integrationsausführung	Die Integrationsausführung, in die diese CWE importiert wurde.
Abschnitte	
Zusätzliche Details	Beschreibungen des Softwarekonzepts, die die Schwachstelle weiter erläutern. Beinhaltet: • Erweiterte Beschreibung • Hintergrunddetails • Notizen
Erkennungsmethoden	Details dazu, wie Sie diese Schwachstelle in einer Anwendung erkennen können.
Einführungsmodi	Die Phasen, in denen die Schwachstelle eingeführt wird, z. B. **Implementierung**, **Architektur und Design**usw.
Demo-Beispiele	Codebeispiele der Schwachstelle mit zugehörigen Beschreibungen.
Potenzielle Minderungen	Details dazu, wie die Schwachstelle verhindert werden kann, einschließlich Angabe, in welcher Phase des Anwendungslebenszyklus sie auftritt, und zur Effektivität der Verringerung.
Zugehörige Listen	
Beziehungen	CWEs, die dieser Schwachstelle zugeordnet sind. Listet Beziehungen zwischen dieser CWE und anderen auf. Kann übergeordnetes/untergeordnetes Element, folgt/Vorrang, erforderlich von/erfordert (für zusammengesetzte Schwachstellen), CanAlsoBe, PeerOf, MemberOf einschließen.
Beispiele für Beobachtung	Einige CVEs, die für diese Schwachstelle repräsentativ sind
Häufige Konsequenzen	Konsequenzen eines erfolgreichen Exploits in Bezug auf Umfang und Auswirkung. Zum Beispiel: Geltungsbereich: Vertraulichkeit Auswirkung: Anwendungsdaten werden gelesen
Mitgliedschaften	CWE-Mitgliedschaften mit dieser Schwachstelle.
Anwendbare Plattformen	Plattformen, die dieser Schwachstelle zugeordnet sind.
Anwendungsschwachstelleneinträge	Anderer Anwendungsschwachstelleneinträge, die mit einer verknüpft sind.
Externe Referenzen	Informationen zur Schwachstelle aus externen Quellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eintragsfelder für Drittpartei-Schwachstellen

Diese Felder befinden sich in Datensätzen, die in der Tabelle „Einträge für Drittpartei-Schwachstellen“ [sn_vul_ third_party_entry] aufgeführt sind.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Version 16.0: CVEs	Mehrere gemeinsame Schwachstellen und Risiken (Common Vulnerability and Exposures, CVEs), die dieser Drittpartei-Schwachstelle zugeordnet sind.
Quelle	Ursprung der Schwachstelle – ob Scanner oder physischer Test.
Risikobewertung	Quantifizierte **Risikopunktzahl,** die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikoeinstufungen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners. **Hinweis:** Diese **Basisrisikobewertung** ist nicht mit der **Risikobewertung**des Lösungsdatensatzes identisch
Risikopunktzahl	Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt, basierend auf der Risikopunktzahl. **Hinweis:** Diese Basis- **Risikopunktzahl** ist nicht identisch mit der **Risikopunktzahl des Lösungsdatensatzes.** Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle Schweregradzuordnungen werden für NVD und mit ServiceNow -Drittparteiintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung.
Exploit vorhanden	Ja, wenn dieser Schwachstelle mindestens ein Exploit zugeordnet ist.
Exploit-Kompetenzniveau	Niedrigste Kompetenzstufe, die zum Ausnutzen dieser Schwachstelle erforderlich ist.
Exploit-Angriffsvektor	Angreifbarster Angriffsvektor der Exploits für diese Schwachstelle.
Aktive AEs	Anzahl der angreifbaren Elemente, die dieser Schwachstelle zugeordnet sind und sich nicht im Status „Geschlossen“ befinden.
Kategorie	Von der Drittanbieterintegration bereitgestellte Klassifizierung. Hilft bei der Zuweisung.
Fehlerkorrekturtyp	Arten von Korrekturaktionen. • Patch • Konfigurationsänderung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Patch und Konfigurationsänderung • Gegenmaßnahme
CWE-Eintrag	Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt.
PCI	Wenn das Kontrollkästchen aktiviert ist, wird die Schwachstelle als erhebliches Risiko für die Offenlegung von Zahlungsinformationen gekennzeichnet.
PCI-Schweregrad	Risikostufe für die Offenlegung von Zahlungsinformationen. [Nur Qualys]
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Zusammenfassung	Beschreibung der Schwachstelle.
Schwachstellendetails	
CVSS v2	CVSS v2-Daten importiert
CVSS v3	Importierte CVSS v3-Daten, vor 2015 nicht verfügbar.
Bedrohung	Beschreibung der Bedrohung, die von dieser Schwachstelle ausgeht.
Bevorzugte Lösung	Höchste Ersatzlösung in der Kette, abgeleitet von den Lösungen, auf die in der Schwachstelle verwiesen wird. Wenn in der Kette mehr als eine höchste Ersatzlösung vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen.
Korrekturhinweise	Beschreibung der vom Lieferanten abgerufenen Korrekturlösung.
Nachbesserungsstatus	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
AEs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle.
AEs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle.
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle.
Zugehörige Links	
Zustand aktualisieren	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Aktualisiert Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Status der Korrekturaufgabe • Risikopunktzahl und Bewertung • Metriken wie Aktive AEs, AEs insgesamt aus dem Abschnitt „Korrekturstatus“.
Zugehörige Listen	
Angreifbare Elemente	Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind.
Verwundbarkeitsreferenzen	Informationen zur Schwachstelle aus externen Quellen, angegeben von NVD.
CVEs	Common Vulnerability Enumeration (CVE)-Datensatz, der dieser Schwachstelle zugeordnet ist.
Kategorien	Kategorien, die dieser Schwachstelle zugeordnet sind.
Exploits	Exploits, die dieser Schwachstelle zugeordnet sind.
Schwachstellen-Malware-Kits	Malware-Kits, die dieser Schwachstelle zugeordnet sind.
Lösungen (Rapid7)	Lösungsinformationen aus Rapid7-Lösungsintegrationen. Wird angezeigt, wenn verfügbar.
Exploit-Frameworks	Exploit-Frameworks, die mit dieser Schwachstelle verbunden sind.
Lösungen	Vulnerability Solution Management Lösungen, die dieser Schwachstelle zugeordnet sind.
CISA-Exploit	
CISA vorhanden	CISA-Exploit für die Eintragstabelle für Drittpartei-Schwachstellen vorhanden.
CISA-Fälligkeitsdatum	Frist für die Behebung der Schwachstelle.

Formularfelder für Korrekturaufgaben

Mithilfe von Korrekturaufgaben kann ein Analyst den Fortschritt überwachen und den Mediationsprozess effizienter gestalten.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „Korrekturaufgabe“ [sn_vul_vulnerability] aufgeführt sind.

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, benötigen Sie mindestens die Rolle sn_vul.read_all.

Felder für Korrekturaufgaben

Feld	Beschreibung
Nummer	Die automatisch generierte Nummer des angreifbaren Elements (VI, Vulnerable Item) für diesen Datensatz.
Risikobewertung	Rollup der Risikopunktzahlen von angreifbaren Elementen, getrennt in Bereiche: „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“. Weitere Informationen zu Risikoeinstufungen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgaben (Fortsetzung)

Feld	Beschreibung
	Hinweis: Diese **Basisrisikobewertung** ist nicht mit der **Risikobewertung des Lösungsdatensatzes identisch.**
Risikopunktzahl	Rollup der Risikopunktzahlen aller angreifbaren Elemente, die dieser Korrekturaufgabe zugeordnet sind. Risiko, das die angreifbaren Elemente insgesamt für Ihre Umgebung darstellen. **Hinweis:** Diese Basis- **Risikopunktzahl** ist nicht identisch mit der **Risikopunktzahl des Lösungsdatensatzes.**
Korrekturziel	Datum, bis zu dem die angreifbaren Elemente nachgebessert werden sollten, beginnend mit der ersten Identifizierung. Weitere Informationen zu Korrekturzielen finden Sie unter Vulnerability Response Korrekturzielregeln.
Korrekturstatus	Status der Korrektur für die Aufgabe. Sie wird durch das angreifbare Element mit dem nächsten Fälligkeitsdatum bestimmt. Für offene Gruppen gibt es folgende Status: • In Ausführung • Ziel rückt näher • Ziel fehlt Für geschlossene Gruppen gibt es folgende Status: • Kein Ziel • Ziel erfüllt • Ziel fehlt Für berechnete Korrekturzieldaten wird, wenn die Aufgabe geschlossen ist, der Gesamtkorrekturstatus aller geschlossenen angreifbaren Elemente in der Aufgabe angezeigt. Diese bestimmen, ob die Aufgabe ihr Datum erreicht hat oder nicht. Der Korrekturstatus einer geschlossenen Aufgabe ist **„Kein Ziel“**, wenn keines der geschlossenen Elemente ein Korrekturzieldatum aufwies. Es wird **als Ziel verfehlt angezeigt**, wenn eines der geschlossenen Elemente sein Zieldatum verfehlt hat. Sie ist **„Ziel erfüllt“,** wenn mindestens ein geschlossenes VI sein Ziel erreicht hat und keines der anderen es verfehlt hat.
Status	Fortschrittsstatus der Aufgabe. Status umfassen:

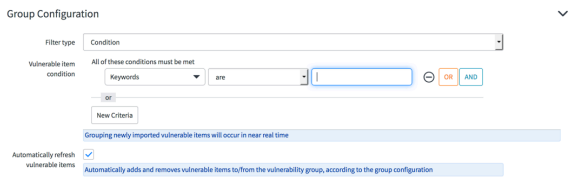
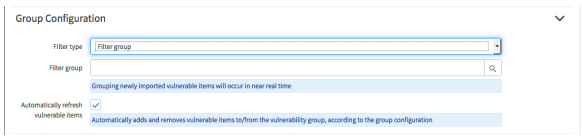
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgaben (Fortsetzung)

Feld	Beschreibung
	• Öffnen • Wird untersucht • Warten auf Implementierung • Zurückgestellt • Wird überprüft • Gelöst • Abgeschlossen Weitere Informationen zu den Status finden Sie unter Vulnerability Response Korrekturaufgabe und Status angreifbarer Elemente.
Bis-Datum für Risikominderung	Datum, an dem die auf die Korrekturaufgabe angewendeten Ausgleichssteuerungen enden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn der Wert verfügbar ist.
Zuweisungsgruppe	Gruppe für die Bearbeitung dieser Korrekturaufgabe ausgewählt.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser Schwachstelle arbeitet.
Erstellt	Datum, an dem diese Korrekturaufgabe erstellt wurde.
Aktualisiert	Datum der letzten Aktualisierung dieser Korrekturaufgabe.
Schwachstelle	Schwachstelle, die für die Aufgabe gilt. (Sichtbar, wenn die Gruppe basierend auf einer einzelnen Schwachstelle gebildet wird.)
Kurzbeschreibung	Kurze Beschreibung dieser Korrekturaufgabe.
Wird überprüft (sichtbar, wenn sich das RT im Status „Wird überprüft“ befindet)	
Angefordert von	Person, die die Zurückstellung angefordert hat.
Gewünschter Grund	Grund für Zurückstellung.
Gewünschter Zustand	Der vom Genehmiger angeforderte Status
Gewünschter Substatus	Der Grund, aus dem vom Genehmiger angefordert wurde.
Zurückstellung(sichtbar, wenn sich die Aufgabe im Status „Zurückgestellt“ befindet)	
Zurückgestellt von	Person, die die Aufgabe zurückgestellt hat.
Ablauf zurückstellen	Datum, an dem die Zurückstellung abläuft.
Grund für das Zurückstellen	Grund für die Zurückstellung.
Lösung (sichtbar, wenn RT den Status „Gelöst“ aufweist)	
Gelöst von	Einzelperson, die die Korrekturaufgabe gelöst hat.
Lösungsdatum	Datum, an dem die Korrekturaufgabe gelöst wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgaben (Fortsetzung)

Feld	Beschreibung
Lösungsnotizen	Zusätzliche Informationen.
Schließen (sichtbar, wenn RT den Status „Geschlossen“ aufweist)	
Geschlossen von	Einzelperson, die die Korrekturaufgabe gelöst hat.
Abgeschlossen	Datum, an dem die Korrekturaufgabe geschlossen wurde.
Abschlussnotizen	Zusätzliche Informationen.
Gruppenkonfiguration (in allen Status sichtbar)	
Filtertyp	Typ der zur Auswahl von Schwachstellen für die Gruppe verwendeten Filterung: **Bedingung**  **Hinweis:** Wird einmal pro Stunde aktualisiert. **Filtergruppe**  **Hinweis:** Wird einmal pro Stunde aktualisiert. **Manuell**
Nachbesserungsstatus	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente in dieser Aufgabe. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
AEs insgesamt	Gesamtzahl der angreifbaren Elemente in dieser Aufgabe. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente in dieser Aufgabe. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente in dieser Aufgabe.
AEs insgesamt	Gesamtzahl der angreifbaren Elemente in dieser Aufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgaben (Fortsetzung)

Feld	Beschreibung
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente in dieser Aufgabe.
Notizen (in allen Status sichtbar)	
Beschreibung	Beschreibung der Gruppen- oder Korrekturaktionen.
Zusätzliche Anmerkungen	Zusätzliche Informationen.
Aktivitäten	Systemhinweise.
Zugehörige Links	
Angreifbare Elemente erneut scannen	Löst einen erneuten Scan der angreifbaren Elemente aus, um zu bestimmen, ob sie repariert wurden.
Aktualisierungsstatus	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Führt ein Rollup für Folgendes aus den AEs in der Aufgabe zusammen: • Status der Korrekturaufgabe • Risikopunktzahlen und Risikobewertungen • Zieldatum und Status der Korrektur (falls zutreffend) • Metriken wie Aktive AEs, AEs insgesamt aus dem Abschnitt „Korrekturstatus“.
Zugehörige Listen	
Angreifbare Elemente	Angreifbare Elemente in dieser Aufgabe.
Aufgaben-SLAs	Plattform-SLAs, die dieser Aufgabe zugeordnet sind.
Bevorzugte Lösungen	Bevorzugte Lösungen der angreifbaren Elemente in dieser Aufgabe.
Change-Anforderungen	Change-Anforderungen, die dieser Aufgabe zugeordnet sind.
Angeforderte Genehmigungen	(Sichtbar, wenn sich die Aufgabe im Status Wird überprüft befindet.) Liste der Genehmiger. Sobald die Zurückstellung genehmigt wurde, wird die Korrekturaufgabe in den Status Zurückgestellt verschoben.

Formularfelder „Fragebogenkonfiguration“.

Sie können einen unterschiedlichen Fragebogen für eine bestimmte Sammlung von Schwachstellen oder Korrekturaufgaben definieren, indem Sie die Schwachstellen bzw. Korrekturaufgaben im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ filtern.

Das Formular „Fragebogenkonfiguration“ wird angezeigt, wenn Sie im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ auf die Schaltfläche **Neu** klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder „Fragebogenkonfiguration“.

Feld	Beschreibung
Name	Name des Fragebogens
Freigaberegel	Genehmigungsregel, für die der Fragebogen gilt. • **Ausnahmeanforderung für Schwachstellen-Gruppen** • **Ausnahmeanforderung für angreifbare Elemente** • **Falsch positiv für Schwachstellen-Gruppen** • **Falsch positiv für angreifbare Elemente** • **Fragebogen für Ausgleichssteuerungen für angreifbare Gruppen** für Risikominderungsanforderungen der Korrekturaufgabe. • **Fragebogen für Ausgleichssteuerungen für angreifbare Elemente** für Risikominderungsanforderungen für angreifbare Elemente.
Beschreibung	Kurzbeschreibung für die Fragebogenkonfiguration.
Bestellung	Der Fragebogen mit der niedrigsten Reihenfolge wird während der Anforderungen angezeigt.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass der Fragebogen verwendet wird.
Tabelle	Tabelle, für die die Genehmigungsregel gilt. • Angreifbares Element [sn_vul_vulnerable_item] für Genehmigungsregeln im Zusammenhang mit angreifbaren Elementen. • Korrekturaufgabe [sn_vul_vulnerability] für die Genehmigungsregeln im Zusammenhang mit Korrekturaufgaben.
Bedingung	Bedingung für die Datensätze, für die der Fragebogen angezeigt werden muss. Sie können die Bedingung auf alle Felder eines angreifbaren Elements und einer Korrekturaufgabe mit Ausnahme **von Grund**anwenden.
Fragebogen	Fragebogen, der angezeigt wird, wenn ein Korrekturbesitzer eine Ausnahme, ein falsch positives Ergebnis oder eine Risikominderung anfordert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurieren Sie die Ausnahmeverwaltung für Vulnerability Response

Konfigurieren Sie den Fragebogen zur Risikominderung

Vulnerability Response Formularfelder für angreifbare Elemente

Angreifbare Elemente werden während des Imports von Drittpartei-Schwachstellenintegrationen automatisch erstellt.

Felder für angreifbare Elemente

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, benötigen Sie mindestens die Rolle sn_vul.read_all.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „Angreifbare Elemente“ [sn_vul_vulnerable_item] aufgeführt sind.

Wenn Sie SAM-NVD-Schwachstellen-Scanning aktiviert haben, werden die Datensätze mit der Software in Ihrem Configuration Management Database (CMDB) verglichen, und es werden Übereinstimmungen mit angreifbarer Software oder Configuration Items (CIs) gefunden.

Feld	Beschreibung
Sicherheits-Tag auswählen	Sicherheits-Tag, um dem Datensatz Metadaten hinzuzufügen oder zu bestimmen, wer Zugriff auf diesen Security Incident-Datensatz haben soll. Dieses Feld wird nur angezeigt, nachdem das angreifbare Element gespeichert wurde.
Nummer	Automatisch generierte Nummer des angreifbaren Elements für diesen Datensatz.
Quelle	Scanner, der dieses angreifbare Element gefunden hat.
Risikobewertung	Quantifizierte **Risikopunktzahl,** die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikoeinstufungen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners. **Hinweis:** Diese **Basisrisikobewertung** ist nicht mit der **Risikobewertung des Lösungsdatensatzes identisch.**
Risikopunktzahl	Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt. **Hinweis:** Diese Basis- **Risikopunktzahl** ist nicht identisch mit der **Risikopunktzahl des Lösungsdatensatzes.** Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.
Schwachstelle	ID der Schwachstelle, die diesem angreifbaren Element zugeordnet ist.
Konfigurationselement	Betroffenes Asset.
Status	Dieses Feld ist standardmäßig auf **Offen eingestellt**. Sie können es jedoch in **„Wird untersucht“** ändern, wenn die Schwachstelle zur sofortigen Korrektur bereit ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bis-Datum für Risikominderung	Datum, an dem die auf das angreifbare Element angewendeten Ausgleichskontrollen ablaufen. **Hinweis:** Dieses Feld wird nur angezeigt, wenn der Wert Ursprüngliche Risikopunktzahl verfügbar ist.
Zuweisungsgruppe	Gruppe für die Bearbeitung dieser Korrekturaufgabe ausgewählt.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser Schwachstelle arbeitet.
Erstellt	Datum, an dem dieses angreifbare Element in Ihrer Instanz erstellt wurde.
Zuletzt geöffnet	Datum, an dem das angreifbare Element zuletzt in Ihrer Instanz geöffnet wurde. Anfangs entspricht dies dem Erstellungsdatum des angreifbaren Elements. Wenn es jedoch geschlossen wurde, enthält das Feld „Zuletzt geöffnet“ das Datum und die Uhrzeit der erneuten Öffnung.
Aktualisiert	Datum des letzten Scans.
Alter	Dauer, für die das AE seit dem Datum, an dem es zuletzt geöffnet wurde, aktiv war. Wenn das AE geschlossen ist, wird der Wert des Felds Alter auf 0 gesetzt. Weitere Informationen zum Feld Alter finden Sie unter Berechnung und Anzeige des Alters von angreifbaren Elementen. Weitere Informationen zum Anpassen der Berechnung der Altersdauer finden Sie im Artikel KB1703270 .
Schwachstelle	
Zusammenfassung	Beschreibung der Schwachstelle.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle Schweregradzuordnungen werden für NVD und mit ServiceNow -Drittparteiintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung.
Schwachstellenpunktzahl (v3)	CVSS v3-Punktzahl.
Schwachstellenpunktzahl (v2)	CVSS v2-Punktzahl.
Exploit vorhanden	Ja, wenn mindestens ein Exploit den Schwachstellen zugeordnet ist, die diesem angreifbaren Element zugeordnet sind.
Exploit-Angriffsvektor	Angreifbarster Angriffsvektor der Exploits für die Schwachstellen, die diesem angreifbaren Element zugeordnet sind.
Exploit-Kompetenzniveau	Niedrigste Kompetenzebene, die zum Ausnutzen der mit diesem angreifbaren Element verbundenen Schwachstellen erforderlich ist.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Bedrohung	Relevante Informationen zur Bedrohung. Aus dem angreifbaren Eintragsdatensatz abgerufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Alle hier vorgenommenen Änderungen aktualisieren den Datensatz des angreifbaren Eintrags.
Korrekturhinweise	Relevante Lösung für die Bedrohung, abgerufen aus dem Datensatz des angreifbaren Eintrags.
Fehlerkorrektur Nur mit Vulnerability Solution Managementverfügbar.	
Bevorzugte Lösung	Bevorzugte Lösung, die aus dem Schwachstellen-Datensatz importiert wurde. **Hinweis:** Alle hier vorgenommenen manuellen Änderungen ändern den Schwachstellendatensatz nicht und bleiben bei nachfolgenden Importen für das VI unverändert.
Zusammenfassung	Zusammenfassung aus dem Lösungsdatensatz importiert.
Lösungstyp	Potenzielle oder bevorzugte Lösung.
Erstmalige Erkennung	
DNS-Name	Name des Domänennamensservice. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, sofern eines vorhanden ist.
NetBIOS-Name	Name des NetBIOS. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, sofern eines vorhanden ist.
IP-Adresse	IPv4- oder IPv6-Adresse. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, sofern eines vorhanden ist.
Port	Adresse des Ports
Protokoll	Name des Protokolls.
SSL	Gibt an, ob die SSL-Verschlüsselung verwendet wird oder nicht.
Erkennungen	
Status	Status der Erkennung.
Zuerst gefunden	Datum, an dem die Drittparteiquelle die Erkennung für dieses Asset zum ersten Mal gefunden hat.
Zuletzt gefunden	Datum, an dem die Drittparteiquelle die Erkennung für dieses Asset zuletzt gefunden hat.
DNS-Name	Name des Domänennamensservice. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, sofern eines vorhanden ist.
NetBIOS-Name	Name des NetBIOS. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, sofern eines vorhanden ist.
IP-Adresse	IPv4- oder IPv6-Adresse. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, sofern eines vorhanden ist.
Port	Adresse des Ports

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Protokoll	Name des Protokolls.
SSL	Gibt an, ob die SSL-Verschlüsselung verwendet wird oder nicht.
Mal gefunden	Anzahl der Erkennungen dieser Schwachstelle für dieses Asset durch die Drittparteiquelle.
Integrationsausführung	Integrationsausführung, über die die Erkennung importiert wurde.
Schließen Verfügbar, sobald das angreifbare Element korrigiert und geschlossen wurde. Die Elemente in diesem Abschnitt sind schreibgeschützt.	
Geschlossen von	Wer das angreifbare Element geschlossen hat.
Abgeschlossen	Datum, an dem das angreifbare Element geschlossen wurde.
Abschlussnotizen	Informationen, die im Abschluss enthalten sind.
Alter der Schließung	Zeitraum, nach dem das AE geschlossen wurde. Wenn das AE erneut geöffnet wird, wird der Wert des Felds Alter geschlossen auf Null gesetzt. Weitere Informationen zur Verwendung des Felds Alter geschlossener finden Sie unter Berechnung und Anzeige des Alters von angreifbaren Elementen. Weitere Informationen zum Anpassen der Berechnung der Dauer der Schließung nach Alter finden Sie im Artikel KB1703270 .
Notizen	
Zusätzliche Kommentare/ Arbeitsnotizen	Alle relevanten Informationen. Aktivieren Sie das Kontrollkästchen, um Zusätzliche Kommentare hinzuzufügen. Ab Vulnerability Response v20.0 können Sie im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Element Arbeitsnotizen hinzufügen.
Aktivität	Wird nur angezeigt, wenn eine Arbeitsnotiz erstellt wurde.
Zugehörige Links	
Risikopunktzahl berechnen	Wenn entweder der **Schwachstellenschweregrad-Rechner** oder **der Risikopunktzahl** -Rechner aktiviert ist, wird das Feld **„Risikopunktzahl“** aktualisiert.

Im Folgenden finden Sie die zugehörigen Listen für angreifbare Elemente.

Zugehörige Liste	Beschreibung
Korrekturaufgaben	Aufgaben, die diesem angreifbaren Element zugeordnet sind.
Betreffende Aufgaben	Aufgaben, die diesem angreifbaren Element zugeordnet sind.
Zugeordnete IP-Adressen	Verfügbar, wenn die Anwendung Qualys Vulnerability Integration Vulnerability Integration installiert ist. IP-Adressen, die während der Deduplizierung gefunden werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Betroffene Services	Business Services, die von diesem angreifbaren Element betroffen sind. Wird angezeigt, wenn diese Informationen im CMDB- Datensatz verfügbar sind. Diese Informationen können manuell oder mit der Anwendung ServiceNow® Service-Mapping eingegeben werden. Weitere Informationen finden Sie unter Service-Mapping. Wenn ein betroffenes CI, das dem angreifbaren Element zugeordnet ist, hinzugefügt oder aktualisiert wird, werden die Informationen in dieser zugehörigen Liste beim Speichern des Datensatzes automatisch aktualisiert.
Genehmigungen der Statusänderung	Status von Change-Anforderungen und andere Genehmigungsinformationen, die der VIT zugeordnet sind.
Qualys-Tickets	Qualys Informationen zur Ticketintegration, die diesem angreifbaren Element zugeordnet sind.

Lösungsformularfelder

Lösungen werden automatisch erstellt, wenn Datensätze aus Lösungsintegrationen von Drittanbietern heruntergeladen und unter **Lösungen** in Vulnerability Responsegespeichert werden.

Eintragsfelder für Lösungsintegration

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

Feld	Beschreibung
Nummer	Bezeichner, der der Lösung zugewiesen ist.
Quelle	Ursprung der Lösung.
Quell-ID	Quellbezeichner für diese Lösung.
Risikobewertung	Unterteilt **die Risikopunktzahl** des Lösungsdatensatzes in Bereiche von „Kritisch“ bis „Kein“. Weitere Informationen zur **Risikobewertung von**Lösungen finden Sie unter Vulnerability Solution Management. **Hinweis:** **Die Risikobewertung** der Lösung ist nicht dasselbe wie die **Risikobewertung**der Datensätze **für angreifbare Elemente**, **Drittpartei-Schwachstellen** und **Korrekturaufgaben**.
Risikopunktzahl	Gewichtete Berechnung basierend auf der **Risikopunktzahl** und der Anzahl angreifbarer Elemente, für die diese Lösung **bevorzugt wird**. Weitere Informationen zur Lösungsrisikopunktzahl finden Sie unter Vulnerability Solution Management. **Hinweis:** **Die Risikopunktzahl** des Lösungsdatensatzes ist nicht dasselbe wie die **Risikopunktzahlides angreifbaren Elements**, **des Drittpartei-Schwachstelleneintrags** und **der Korrekturaufgabendatensätze**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Verfügbar, wenn SAM NVD aktiviert ist. Wenn einer Schwachstelle jedoch keine aktiven angreifbaren Elemente zugeordnet sind, wird die **Risikopunktzahl** der Lösung auf 0 festgelegt.
Höchste Ersatz	Gibt an, dass keine Ersatzlösung vorhanden ist.
Lösungstyp	Art der Lösung. Die Auswahlmöglichkeiten lauten wie folgt: • Workaround • Mitigation • Lieferantenkorrektur • Patch • Rollup • Berechtigung • Wird nicht korrigiert • Keine verfügbar
Neustart erforderlich	Neustart erforderlich. Die Auswahlmöglichkeiten lauten wie folgt: • Ja • Nein • Vielleicht
Veröffentlichungsdatum	Datum, an dem die Schwachstelle nach Quelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt von der Quelle geändert wurde.
Zusammenfassung	Korrekturzusammenfassung für die Lösung.
Bulletin	Security Bulletin, das der Lösung zugeordnet ist.
Produktkategorien	Produktkategorien, für die die Lösung gilt.
Produkte	Produkte, für die die Lösung gilt.
Lösungsdetails	
Beschreibung	Wenn in der Lösungsquelle kein Inhalt verfügbar ist, werden Sie zu einem anderen relevanten Abschnitt oder einer anderen relevanten Lösung weitergeleitet, um weitere Informationen zu erhalten.
Links	Importierte Internetressourcen, die der Lösung zugeordnet sind.
Schwachstellendetails	
Hinweise zu Schwachstellen	Zusammenfassung der durch die Lösung behobenen Schwachstellen.
Nachbesserungsstatus	
Bevorzugte Lösungsziele	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Korrekturstatus für angreifbare Elemente und ihre eindeutigen Configuration Items (CIs), für die dies die bevorzugte Lösung ist. **Hinweis:** Ein eindeutiges CI wird nur einmal gezählt, unabhängig davon, wie vielen VIs es zugeordnet ist.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
AEs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Behobene AEs in Prozent	Abschluss in Prozent für die Korrektur angreifbarer Elemente (VIs, Vulnerable Items) Gilt für VIs, für die diese Lösung bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten AEs.
Verbleibende CIs	Anzahl der eindeutigen CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die CIs zurückgestellter angreifbarer Elemente.
CIs insgesamt	Anzahl der eindeutigen CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die CIs zurückgestellter angreifbarer Elemente.
Behobene CIs in Prozent	Abschluss in Prozent der korrigierten eindeutigen CIs (d. h. alle AEs für dieses CI und diese Lösung wurden korrigiert). Bestimmt durch die Anzahl der korrigierten CIs für die Gesamtzahl der eindeutigen CIs, die angreifbaren Elementen mit der bevorzugten Lösung zugeordnet sind. Diese Anzahl enthält nicht die CIs zurückgestellter angreifbarer Elemente.
Bevorzugte Lösungsziele (einschließlich zurückgestellte) Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs, einschließlich „Zurückgestellt“, für die dies die bevorzugte Lösung ist.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
AEs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
Behobene AEs in Prozent	Abschluss in Prozent für die Korrektur angreifbarer Elemente (VIs, Vulnerable Items) Gilt für VIs, für die diese Lösung bevorzugt wird.
Verbleibende CIs	Anzahl der eindeutigen CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird.
CIs insgesamt	Anzahl der eindeutigen CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird.
Behobene CIs in Prozent	Abschluss in Prozent der korrigierten eindeutigen CIs (d. h. alle AEs für dieses CI und diese Lösung wurden korrigiert). Bestimmt durch die Anzahl der korrigierten CIs für die Gesamtzahl der eindeutigen CIs, die angreifbaren Elementen mit der bevorzugten Lösung zugeordnet sind. Diese Anzahl enthält nicht die CIs zurückgestellter angreifbarer Elemente.
Potenzielle Lösungsziele	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs mit einer Schwachstelle im Zusammenhang mit dieser Lösung.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Verbleibende CIs	Anzahl eindeutiger CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Potenzielle Lösungsziele (einschließlich zurückgestellte) Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs (einschließlich „Zurückgestellt“) mit einer Schwachstelle, die von dieser Lösung behoben werden können, einschließlich der Anzahl der bevorzugten Lösungen.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt.
Verbleibende CIs	Anzahl eindeutiger CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt.
Notizen	
Interne Hinweise	Bearbeitbares Feld für den Korrekturspezialisten.
Zugehörige Links	
Zustand aktualisieren	Datum und Uhrzeit der letzten Aktualisierung des Korrekturstatus. Aktualisiert Folgendes: • Status der Korrekturaufgabe • Risikopunktzahl und Bewertung • Metriken aus dem Abschnitt „Korrekturstatus“.
Zugehörige Listen	
Angreifbare Elemente	Angreifbare Elemente, die dieser Lösung als bevorzugte Lösung für die Korrektur zugeordnet sind.
Schwachstellen von Drittparteien	Mit dieser Lösung verknüpfte Schwachstellen von Drittparteien.
CVEs	Common Vulnerability and Exposure (CVE) – Schwachstellen, die dieser Lösung zugeordnet sind.
Korrekturaufgaben	Korrekturaufgaben, die zugehörige angreifbare Elemente enthalten, wobei diese Lösung zur Korrektur bevorzugt wird.
Vorhergehende Lösungen	Frühere Lösungen, die eine oder mehrere Schwachstellen dieser Lösung beheben.
Ersatzlösungen	Spätere Lösungen, die alle Schwachstellen dieser Lösung beheben. Diese Liste ist leer, wenn das Kontrollkästchen **„Höchste Ersetzung“** aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationen des Genehmigungsworkflows für Anforderung zum Aufheben der Zuweisung

Sie können den Genehmigungsworkflow für das Entfernen von Zuweisungen von angreifbaren Elementen (VIs, VITs), Korrekturaufgaben, angreifbare Elemente in der Anwendung (AVITs) und angreifbare Elemente in Containern (CVITs) für Sie und Ihre Gruppe entwerfen.

VIT, Korrekturaufgabe, AVIT und CVIT haben jeweils eine Standardgenehmigungsregel. Jede Genehmigungsregel hat eine Standardgenehmigungskonfiguration. Jede Genehmigungskonfiguration hat eine standardmäßige Genehmigerebene. Die Genehmigungsregeln für VITs, Korrekturaufgaben, AVIT und CVIT sind standardmäßig aktiviert. Als Administrator können Sie die folgenden Aktionen ausführen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Meine Genehmigungen** > **Genehmigungsregeln** und Auswahl der entsprechenden Genehmigungsregel.

- können Sie eine Genehmigungsregel aktivieren oder deaktivieren.
- Eine Genehmigungskonfiguration erstellen und aktualisieren.
- definieren Sie Bedingungen für angreifbare Elemente und Korrekturaufgaben, für die die Genehmigungsregeln gelten.
- mehrere Genehmigerebenen erstellen und aktualisieren.

Die folgende Tabelle zeigt die standardmäßigen Genehmigungsregeln, Genehmigungskonfigurationen und Genehmigerebenen für VIT, Korrekturaufgabe, AVIT und CVIT, die im Lieferumfang des Basissystems enthalten sind.

Standardgenehmigungsregeln, Genehmigungskonfigurationen und Genehmigerebenen

Typ	Genehmigungsregel	Genehmigungskonfigura	Genehmiger-Ebenen
VIT oder VI	Change-Anforderung für Feld zu angreifbarem Element	Change-Anforderung für Feld zu angreifbarem Element	Anforderung der Aufhebung der Zuweisung der Ebene 1 für AE
Nachbesserungsaufgabe	Schwachstellegruppenfeld Change-Anforderung	Change-Anforderung für Schwachstellenfeld	Ebene 1 – Anforderung der Zuweisungsaufhebung für SG
AVIT	Change-Anforderung für Feld zu angreifbaren Elementen der Anwendung	Change-Anforderung für Anwendungsschwachstellen-Feld	Heben Sie die Zuweisung des angreifbaren App-Elements auf
CVIT	Genehmigung für Container-Verwaltung	Standardkonfiguration – CVIT-Zuweisung aufheben	CVIT-Zuweisung aufheben – Genehmigungsebene 1

Weitere Informationen zum Genehmigen von Anforderungen zum Aufheben von Zuweisungen finden Sie unter Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in, oder lehnen Sie sie ab Vulnerability Response.

Vulnerability Response Beispiele für Regeln für Korrekturaufgaben

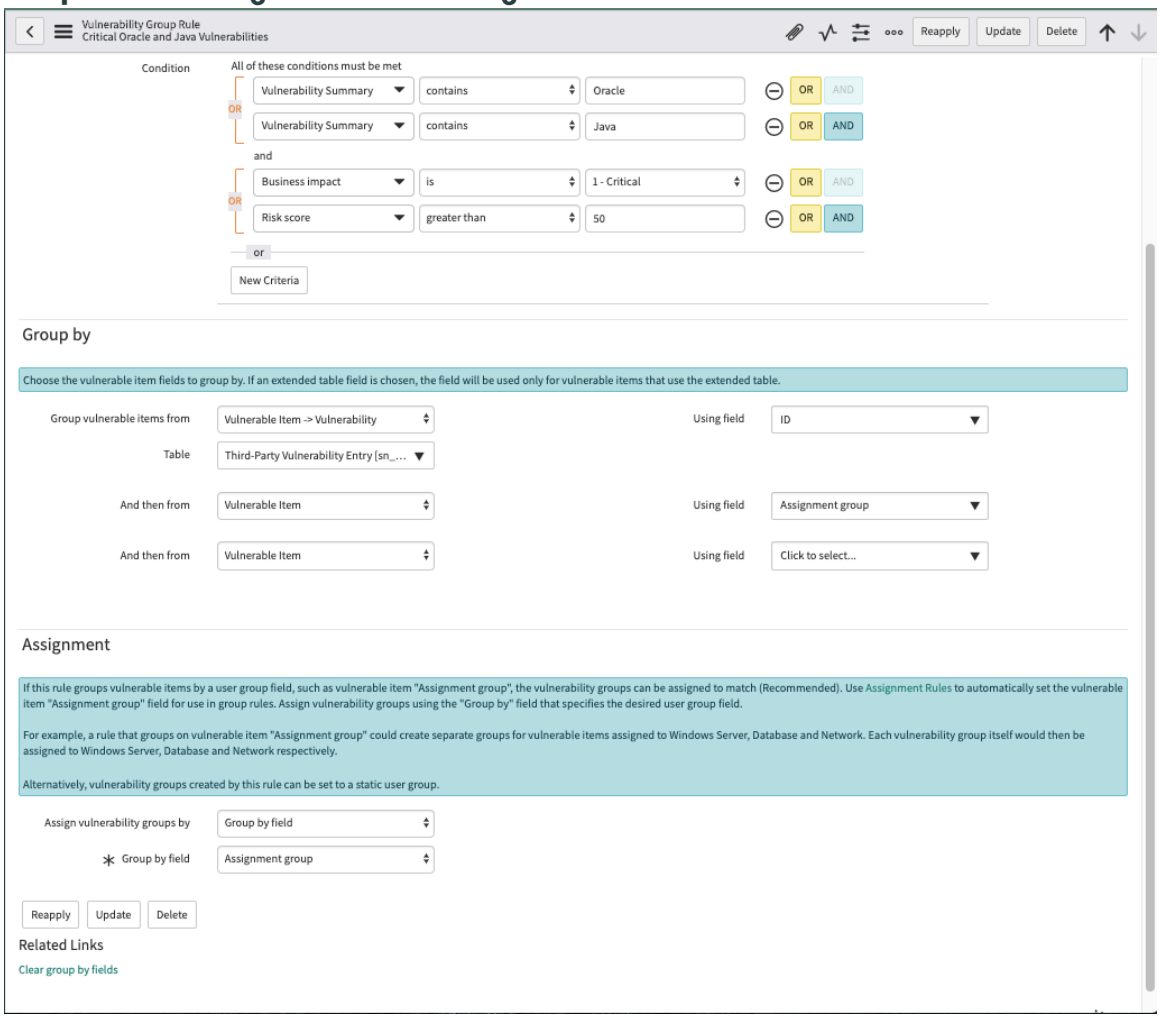
Beispiele für Regeln für Korrekturaufgaben, bei denen Schwachstelle und Risiko, Auswirkung oder Configuration Item (CI) verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regel für Korrekturaufgaben zum Gruppieren von angreifbaren Java- und Oracle-Elementen mit hohem Risiko

Dieses Beispiel zeigt eine Tour durch die Regel, die angreifbare Java- und Oracle-Elemente nach Schwachstelle gruppiert und ihren jeweiligen Supportgruppen zuweist.

Beispiel für eine Regel für Korrekturaufgaben

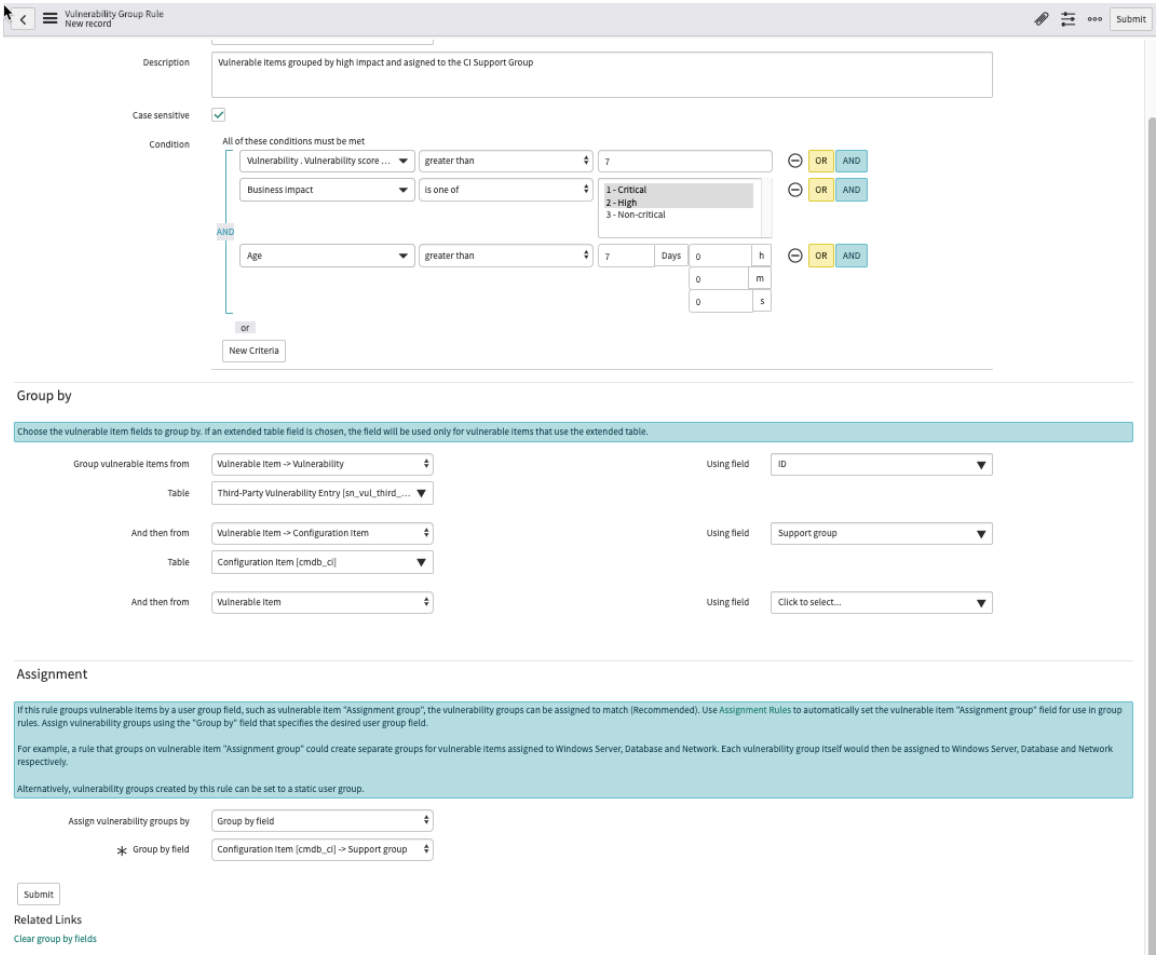


Klicken Sie mit der rechten Maustaste in den Header, um **Speichern**zu wählen.

Regel für Korrekturaufgaben, um alle angreifbaren Elemente mit großer Auswirkung nach Schwachstelle und CI-Supportgruppe zu gruppieren

Dieses Beispiel zeigt die Formularfeldeinstellungen für eine Gruppenregel für angreifbare Elemente mit großer Auswirkung, mit der diese der CI-Supportgruppe zugewiesen werden.

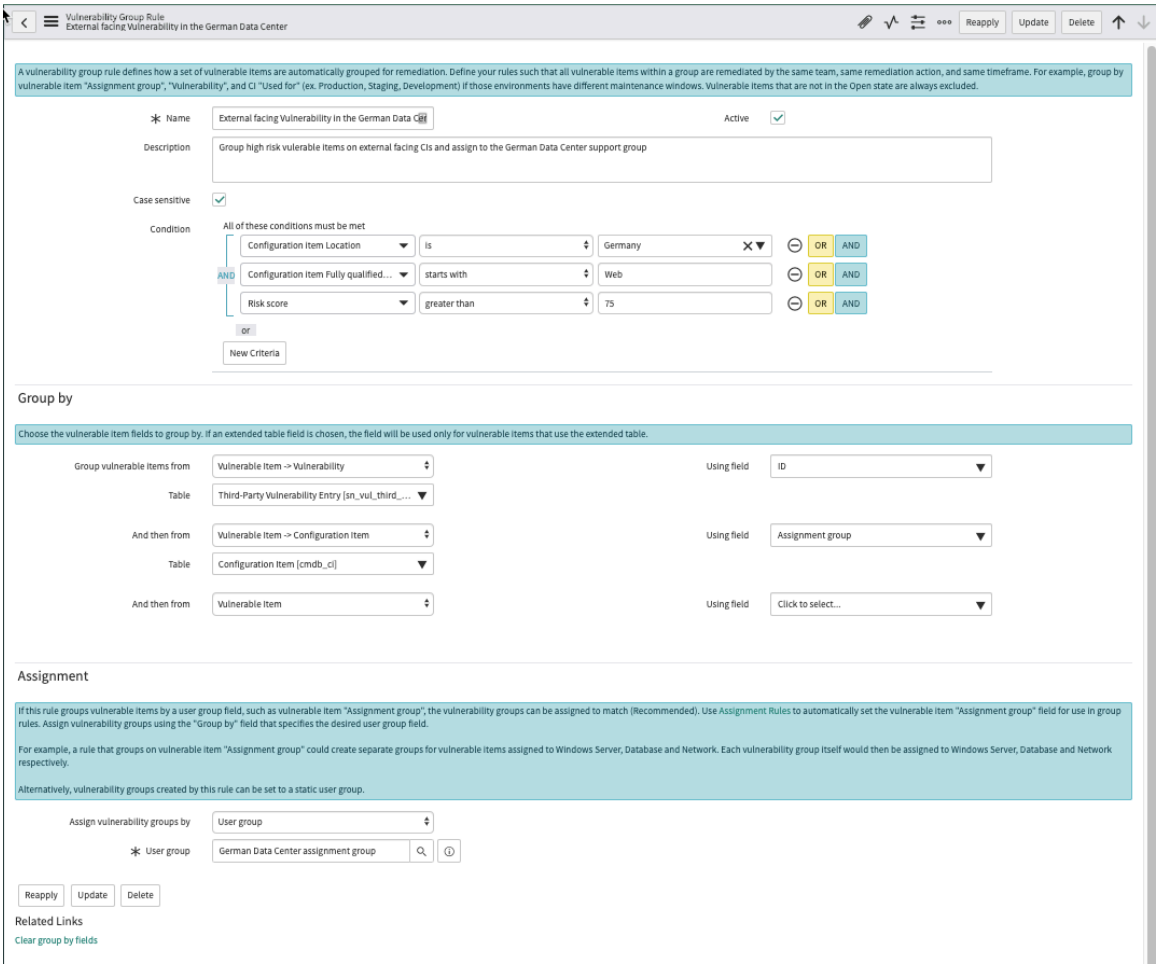
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Regel für Korrekturaufgaben, um alle Schwachstellen mit hohem Risiko in einem externen CI in einem Rechenzentrum in Deutschland zu gruppieren

Dieses Beispiel zeigt die Formularfeldeinstellungen für eine Gruppenregel für Schwachstellen mit hohem Risiko bei extern ausgerichteten CIs in einem Rechenzentrum in Deutschland. Sie sind der Zuweisungsgruppe für das Rechenzentrum in Deutschland zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beispiel für die Berechnung der Risikopunktzahl für Vulnerability Response

Sie können die Risikopunktzahl-Rechner bestimmen, um Risikopunktzahlen zu generieren, die die für Ihre Organisation eindeutigen Schwachstellen- und Asset-Daten verwenden.

Beispiel für die Bestimmung der Punktzahlen von Risikoregelrechnern

Das folgende Beispiel zeigt, wie Punktzahlen für Risikoregel-Rechner ermittelt werden.

Angenommen, ein Risikoregel-Rechner ist mit den Feldern in der folgenden Tabelle konfiguriert:

Feld	Gewichtung	Gewichtungsaufgliederung
Schwachstelle.Schweregrad	50	Standard: 20 1 – Kritisch: 100 2 - Hoch: 80 3 - Mittel: 60 4 - Niedrig: 40 5: Keine: 20
Schwachstelle.Exploit vorhanden	50	Standard: 50

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Gewichtung	Gewichtungsaufgliederung
		Ja: 100 Nein: 0

Angenommen, die in dieser Tabelle aufgeführten angreifbaren Elemente sind auch im System vorhanden:

ID	Schwachstellenschweregrad	Schwachstellen-Exploit ist vorhanden
VIT00001	1 – Kritisch	1: Ja
VIT00002	2 – Hoch	1: Ja
VIT00003	3 – Mittel	2: Nein
VIT00004	4 – Niedrig	2: Nein
VIT00005	5 – Keine	2: Nein

Die Berechnung der Risikopunktzahl für die angreifbaren Elemente basiert auf der folgenden Formel:

`Risikopunktzahl = (W(Schweregrad) * FV (Schweregrad). + W(Exploitexists) * FV(Exploit vorhanden))/100`

wobei **W** die Gewichtung und **FV** der Gewichtungsprozentsatz des Feldwerts ist.

Die resultierende Risikopunktzahl für diese angreifbaren Elemente wird in der folgenden Tabelle beschrieben:

ID	Schwachstellenschwereg (50 %)	Schwachstellen-Exploit vorhanden (50 %)	Resultierende Risikopunktzahl
VIT00001	1 – Kritisch (50 % x 100)	1: Ja (50 % x 100)	100
VIT00002	2 – Hoch (50 % x 80)	1: Ja (50 % x 100)	90.0
VIT00003	3 – Mittel (50 % x 60)	2: Nein (50 % x 0)	30
VIT00004	4 – Niedrig (50 % x 40)	2: Nein (50 % x 0)	20
VIT00005	5 - Keine (50 % x 20)	2: Nein (50 % x 0)	10

Hinweis:
Für VIT00005 wird die Standardgewichtung angewendet, da der Wert des Schweregrads leer ist.

Wenn der Gewichtungsprozentsatz für einen der Feldwerte geändert wird, finden Sie die Ergebnisse in dieser Tabelle:

Feld	Gewichtung	Gewichtungsaufgliederung
Schwachstelle.Schweregrad	50	• Standard: 20 • 1 – Kritisch: 100 • **2 - Hoch: 70** *überarbeiteter Wert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Gewichtung	Gewichtungsaufgliederung
		• 3 - Mittel: 60 • 4 - Niedrig: 40
Schwachstelle.Exploit vorhanden	50	• Standard: 50 • Ja: 100 • Nein: 0

Die Risikopunktzahl für die angreifbaren Elemente nach dem erneuten Anwenden des Rechners wird in der folgenden Tabelle angezeigt:

ID	Schwachstellenschwere (50 %)	Schwachstellen-Exploit vorhanden (50 %)	Resultierende Risikopunktzahl
VIT00001	1 – Kritisch (50 % x 100)	1: Ja (50 % x 100)	100
VIT00002	**2 – Hoch (50 % x 70)** *überarbeiteter Wert	1: Ja (50 % x 100)	**85** *überarbeiteter Wert
VIT00003	3 – Mittel (50 % x 60)	2: Nein (50 % x 0)	30
VIT00004	4 – Niedrig (50 % x 40)	2: Nein (50 % x 0)	20
VIT00005	5 - Keine (50 % x 20)	2: Nein (50 % x 0)	10

Fehlerbehandlung für Erkennungen

Fehler werden beim Erstellen von Erkennungen oder beim Erstellen und Aktualisieren angreifbarer Elemente während der Verarbeitung der Anhänge protokolliert. Wenn ein Schwachstellenintegrationsprozess fehlschlägt, werden die Fehler auf der Registerkarte „Protokoll für Schwachstellenintegrationen“ protokolliert.

Diese Fehler werden mit einer der folgenden Kategorien protokolliert.

Feld	Beschreibung
VI-Erstellung	Fehler beim Erstellen oder Aktualisieren der Erkennung.
Erkennung	Fehler beim Erstellen einer Erkennung.

Mobile Experience für Vulnerability Response

Wenn Sie für die Korrektur von Schwachstellen zuständig sind, können Sie mit Ihrem Android- oder iOS-Mobilgerät auf die Anwendung Vulnerability Response (VR) in Ihrer Now Platform®-Instanz zugreifen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response

Um sich mit den Konzepten von Vulnerability Response und den Möglichkeiten dieses Produkts für Ihre Organisation vertraut zu machen, lesen Sie unter Vulnerability Response verstehen nach.

Hinweis:
Bevor Sie Vulnerability Response Mobile-App mobileinstallieren, machen Sie sich mit vertraut Mobile Agent .

Übersicht

Als Benutzer mit der Rolle „Korrekturbesitzer“ (sn_vul.remediation_owner) können Sie mit dem Vulnerability Response Mobile-App die Schwachstellen, Korrekturaufgaben und Zuweisungen in Ihrer Instanz Now Platform direkt auf Ihrem Mobilgerät Android oder iOS anzeigen und suchen.

Sie werden benachrichtigt, wenn Ihnen oder Ihrer Zuweisungsgruppe Korrekturaufgaben zugewiesen wurden. Diese App bietet einem für die Korrektur Verantwortlichen die Flexibilität, Felder neu zuzuweisen, zu bearbeiten und mit der Korrektur zu beginnen, ohne an den Desktop gebunden zu sein.

Sie haben Zugriff auf Schwachstellen, angreifbare Elemente, Module und alle Lösungen. Sie können die folgenden Aufgaben auf Ihrem Mobilgerät ausführen:

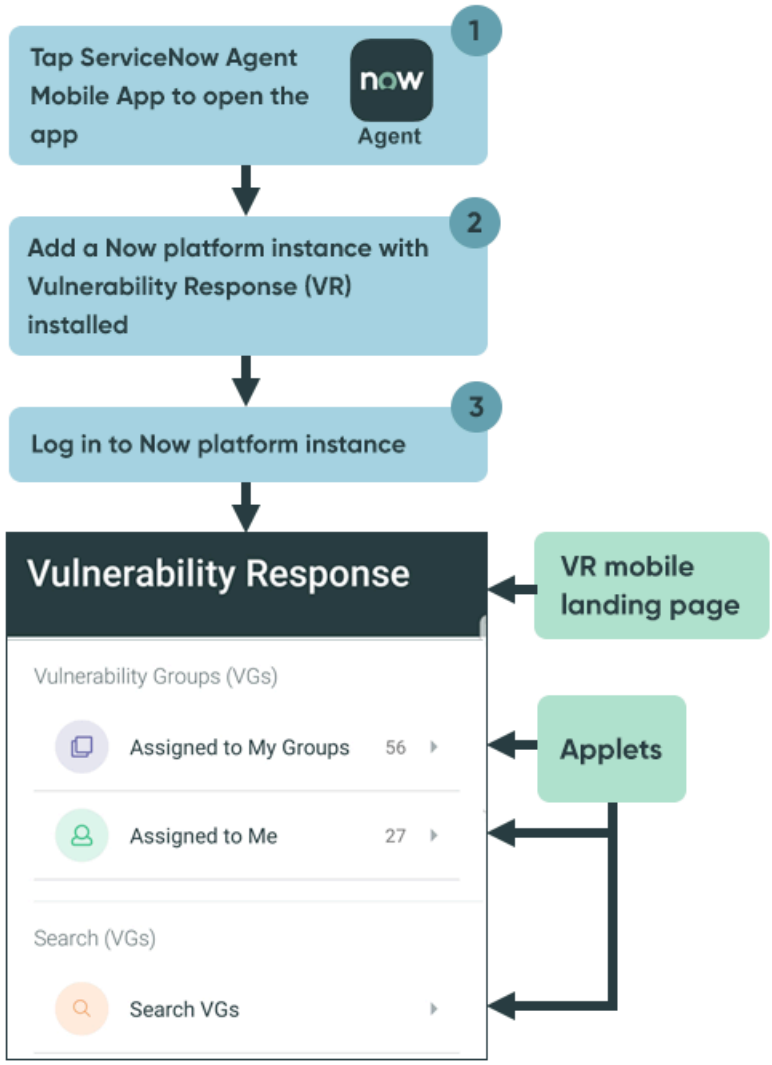
- Korrekturaufgaben anzeigen und aktualisieren.
- Zeigen Sie Change-Anforderungen an.
- Weisen Sie eine Korrekturaufgabe oder ein angreifbares Element einem anderen Mitglied einer Zuweisungsgruppe neu zu.
- Zeigen Sie Benachrichtigungen an, wenn Ihnen oder einer Ihrer Zuweisungsgruppen eine kritische Korrekturaufgabe zugewiesen wird.
- Bearbeiten Sie eine Teilmenge von Feldern in Korrekturaufgaben-Datensätzen.
- Suchen Sie nach Korrekturaufgaben, die bestimmten Suchkriterien entsprechen.

Die folgende Abbildung zeigt, wie Sie sich über Ihr Mobilgerät bei der Instanz Now Platform anmelden und wie der Zielbildschirm von Vulnerability Response Mobile-App nach der Anmeldung angezeigt wird.

Schritt-für-Schritt-Anweisungen zum Einrichten der Instanz Now Platform und zur Installation von Vulnerability Response Mobile-Appfinden Sie unter Richten Sie eine Prüfliste für ein Vulnerability Response Mobile-App. Anweisungen zur Anmeldung finden Sie unter Melden Sie sich bei an Vulnerability Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Mobile-App



Anwendungen

Anwendungen sind die ServiceNow -Softwarekomponenten wie Security Incident Response (SIR), Vulnerability Response (VR), Governance, Risk und Compliance (GRC) und andere ServiceNow -Produkte, die bestimmte Funktionen und Funktionalitäten in Ihrer Instanz Now Platform von bereitstellen. Nachdem Sie Kernanwendungen mit mobilen Apps in Ihrer Instanz Now Platform installiert haben, werden diese Anwendungen als Symbole unten auf Ihrem Mobilgerät angezeigt.

Vulnerability Response-Symbol auf Mobilgerät

Ordner

Jede Anwendung ServiceNow® Mobile enthält Ordner, die die Applets nach Kategorien trennen. In der vorherigen Abbildung sind Korrekturaufgaben und Suche (SG) die Ordner für Vulnerability Response Mobile-App.

Applets

Applets sind die verschiedenen Optionen in der Anwendung. In der vorherigen Abbildung sind die Symbole unter Korrekturaufgaben und Suche (SG) die verfügbaren Applets für Vulnerability Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In den folgenden Themen finden Sie weitere Informationen zu den Applets von Vulnerability Response Mobile-App.

Richten Sie eine Prüfliste für ein Vulnerability Response Mobile-App

Die folgende Prüfliste enthält die Einrichtungsaufgaben, die Sie in der Instanz Now Platform® und auf Ihrem Mobilgerät ausführen müssen, bevor Sie Vulnerability Response Mobile-Appverwenden.

Vorbereitungen
Weitere Informationen folgen jedem Schritt in der rechten Spalte. Geschätzte Zeit für Abschluss dieser Aufgabe: 15–20 Minuten.

Erforderliche Rolle: admin, sn_vul.remediation_owner

Sie haben Ihr Mobilgerät erfolgreich für Vulnerability Response Mobile-Appeingerichtet. Der nächste Schritt besteht darin, sich bei Vulnerability Response Mobile-App anzumelden und Ihrem Mobilgerät eine Instanz Now Platform hinzuzufügen.

Prozedur

1. Sie können diese Prüfliste ausdrucken und sich durch die Aufgaben führen lassen, die zur Installation von Vulnerability Response Mobile-Apperforderlich sind.
2. Stellen Sie sicher, dass alle Elemente in der Liste abgeschlossen sind, damit Sie sich bei Vulnerability Response Mobile-App anmelden und eine Instanz Now Platform hinzufügen können.

Mobile Prüfliste

Artikel	Beschreibung
☐	Stellen Sie als Benutzer mit der Administratorrolle sicher, dass die Kernanwendung Vulnerability Response auf einer Instanz Now Platform von installiert ist. Dies ist die Instanz Now Platform, die Sie auf Ihrem Mobilgerät anzeigen. **Hinweis:** Die Kernanwendung Vulnerability Response und die Instanz Now Platform müssen aus demselben Familien-Release stammen. **a.** Um sicherzustellen, dass die Core-Anwendung auf Ihrer Instanz installiert ist, navigieren Sie zu **Plugins**, und suchen Sie nach Vulnerability Response. **b.** Wenn die Core-Anwendung Vulnerability Response noch nicht installiert ist, klicken Sie auf **Installieren**, um sie zu installieren. Weitere Informationen zur Installation der Kernanwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Weitere Informationen zum Abrufen der Kernanwendung Vulnerability Response auf dem ServiceNow Store, zum Abrufen von Berechtigungen, zur Installation von Kernanwendungen und zum Aktivieren von Abhängigkeiten finden Sie unter Security Operations und ServiceNow Store.
☐	Stellen Sie als Benutzer mit der Administratorrolle sicher, dass Vulnerability Response Mobile-App auf der Instanz Now Platform installiert ist, die Sie auf Ihrem Mobilgerät anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	Hinweis: Die Instanzen Vulnerability Response Mobile-App und Now Platform müssen aus demselben Familien-Release stammen. Die Anwendung Vulnerability Response Mobile-App und Vulnerability Response müssen kompatibel sein. Weitere Informationen zur Kompatibilität der Anwendung Vulnerability Response finden Sie unter Vulnerability Response- und Configuration Compliance-Kompatibilitätsmatrix. Laden Sie Vulnerability Response Mobile-App aus ServiceNow Store in Ihrer Instanz von Now Platform herunter, und installieren Sie es. Wenn Sie Vulnerability Response Mobile-Appinstallieren, werden auch die zugehörigen Abhängigkeiten com.glide.sg und com.glide.sg.agent_native_client installiert. So überprüfen Sie, ob diese Abhängigkeiten installiert sind: **a.** Navigieren zu **Alle** > **Plugins**. **b.** Suchen Sie nach den Plugin-IDs (com.glide.sg und com.glide.sg.agent_native_client). **c.** Wenn sie nicht aktiviert sind, aktivieren Sie diese Plugins. Diese Plugins sind für Vulnerability Response Mobile-Apperforderlich. Weitere Informationen zum Abrufen der Anwendung Vulnerability Response Mobile-App auf dem ServiceNow Store, zum Abrufen von Berechtigungen, zur Installation von Anwendungen und zum Aktivieren von Abhängigkeiten finden Sie unter Security Operations und ServiceNow Store.
☐	Stellen Sie als Benutzer mit der Administratorrolle in Ihrer Instanz Now Platform sicher, dass Sie mobilen Benutzern die erforderlichen Rollen Now Platform zugewiesen haben. **a.** Um die Rollen anzuzeigen, die einem Benutzer zugewiesen sind, navigieren Sie zu **Alle** > **Administration** > **Anwender**. **b.** Wählen Sie den Anwendernamen gefolgt von der zugehörigen Liste „Rollen“ aus. Alle diesem Anwender zugewiesenen Rollen werden angezeigt. **c.** Überprüfen Sie, ob ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der Rolle IT Infrastructure Library (itil) zu. Benutzer mit der Rolle itil können Change-Anforderungen und Korrekturaufgaben erstellen, öffnen, aktualisieren und schließen. Nur Benutzern mit der Rolle itil können Aufgaben zugewiesen werden. **d.** Überprüfen Sie, ob ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der Rolle des Korrekturbesitzers (sn_vul.remediation_owner) zu. Benutzer mit der Rolle sn_vul.remediation_owner können Schwachstellen- und Lösungsdatensätze lesen. Diese Rolle wird automatisch hinzugefügt, wenn Sie die Rolle itil zuweisen. **e.** Stellen Sie sicher, dass Sie alle erforderlichen Zuweisungsgruppen erstellt und diesen Gruppen mobile Benutzer zugewiesen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	Hinweis: Wenn Sie eine große Anzahl von Benutzern für die mobile Anwendung haben, können Sie alternativ die Rolle sn_vul.remediation_owner einer Gruppe zuweisen. Jeder Anwender, den Sie der Gruppe hinzufügen, erbt diese Rolle. Weitere Informationen zu Zuweisungsregeln und -gruppen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Weitere Informationen zu Benutzern und zum Zuweisen von Rollen zu Benutzern und Gruppen finden Sie unter Benutzeradministration.
☐	Laden Sie als Benutzer mit der Rolle des Korrekturbesitzers (sn_vul.remediation_owner) die aktuelle ServiceNow® Agent-App auf Ihr Mobilgerät herunter. Die aktuelle Agent-App ist im App Store von Apple iOS und im Play Store Google verfügbar.
☐	Als Benutzer mit der Rolle sn_vul.remediation_owner müssen Sie überprüfen, ob auf Ihrem Mobilgerät und in der Instanz Now Platform Benachrichtigungen aktiviert sind. Benachrichtigungen informieren Sie, wenn Ihnen oder Ihrer Zuweisungsgruppe kritische Korrekturaufgaben zugewiesen werden. Um Sie bei der rechtzeitigen Korrektur zu unterstützen, klicken Sie nach dem Aktivieren von Benachrichtigungen auf eine Benachrichtigung in Vulnerability Response Mobile-App, und navigieren Sie direkt zum Datensatz. Führen Sie die folgenden Schritte aus, um Benachrichtigungen in Ihrer Instanz Now Platform zu aktivieren, damit sie auf Ihrem Mobilgerät angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	a. Vergewissern Sie sich, dass Sie Vulnerability Response Mobile-App in Ihrer Instanz Now Platform von heruntergeladen und installiert haben. **b.** Überprüfen Sie in den Systemeinstellungen in der Instanz Now Platform unter „Benachrichtigungen“, ob die **Anwendung ServiceNow Mobile**aktiviert ist. Weitere Informationen zum Festlegen von Benachrichtigungen finden Sie unter Setting notification preferences in Core UI . Now Platform -Benachrichtigungen werden auch auf dem Nachrichtenbildschirm Ihres Mobilgeräts angezeigt. Stellen Sie sicher, dass in den Einstellungen Ihres Mobilgeräts auch Benachrichtigungen aktiviert sind.

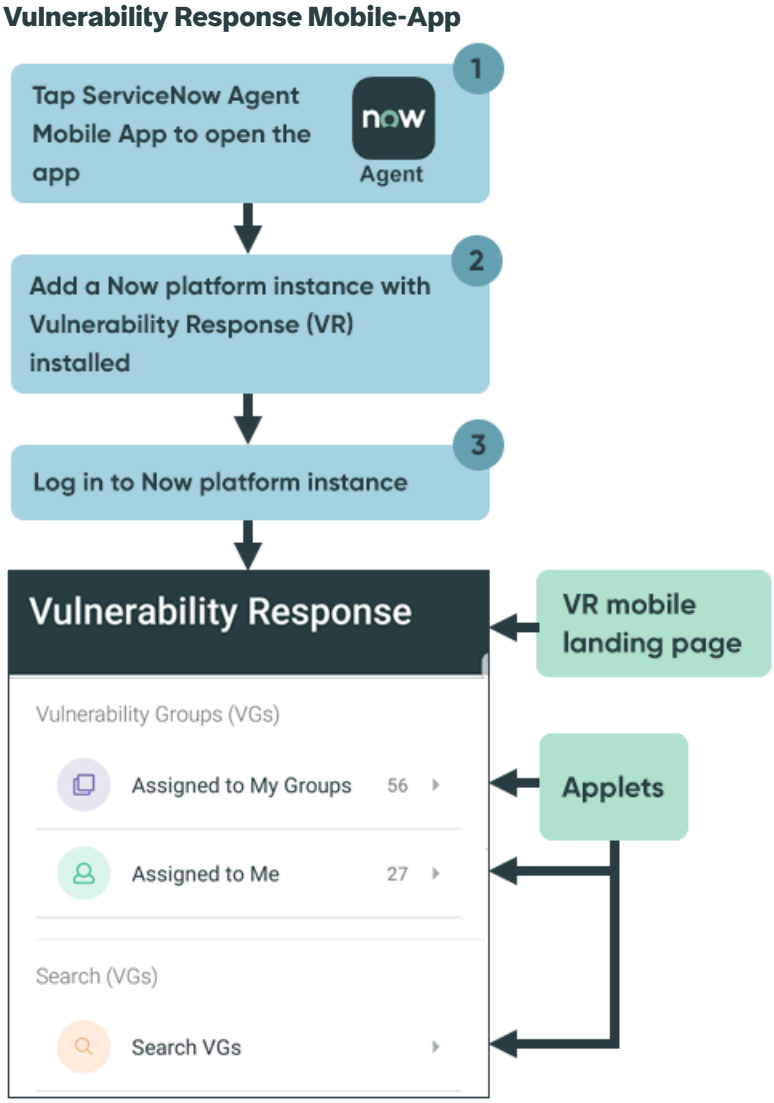
Melden Sie sich bei an Vulnerability Response Mobile-App

Öffnen Sie die App Vulnerability Response Mobile, und fügen Sie auf Ihrem Mobilgerät eine Now Platform-Instanz mit Vulnerability Response hinzu.

Vorbereitungen

Stellen Sie sicher, dass Sie die in Richten Sie eine Prüfliste für ein Vulnerability Response Mobile-Appbeschriebenen Setup-Schritte abgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

Warum und wann dieser Vorgang ausgeführt wird

Dauer für diese Aufgabe: 5–7 Minuten.

Prozedur

1. Tippen Sie auf Ihrem Mobilgerät auf die App **ServiceNow Agent**.

   Wenn Sie noch nicht bei einer Instanz Now Platform angemeldet sind, wird der Bildschirm „Instanzen“ angezeigt.

2. Wenn die Instanz Now Platform mit der Core-Anwendung Vulnerability Response Ihrem Mobilgerät noch nicht hinzugefügt wurde, führen Sie die folgenden Schritte aus, um sie hinzuzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Tippen Sie im angezeigten Bildschirm Instanzen auf das Plus-Symbol ( ).
Ein Bildschirm wird angezeigt, in dem Sie aufgefordert werden, die Adresse einer Now Platform -Instanz einzugeben und zu speichern.

b. Füllen Sie die Felder aus.

Feldname	Beschreibung
Geben Sie die Instanzadresse ein, oder scannen Sie einen QR-Code.	Wählen Sie eine, um fortzufahren: ▪ Geben Sie vor .service-now.comden Namen Ihrer Instanz Now Platform ein, z. B. vrmobilennewjoragent. ▪ Geben Sie eine Adresse ein. Diese Adresse ist die URL der Instanz Now Platform, die Sie auf Ihrem Mobilgerät anzeigen möchten. ▪ Scannen Sie einen QR-Code.
(Optional) Geben Sie einen Kurznamen ein	Geben Sie einen Spitznamen für diese Instanz ein. Wenn dem Gerät mehrere Instanzen hinzugefügt wurden, können Kurznamen Ihnen dabei helfen, eine Instanz Now Platform schnell zu finden.

c. Tippen Sie auf **Speichern und anmelden**

3. Geben Sie im angezeigten Anmeldebildschirm ServiceNow den Anwendernamen und das Passwort für die Instanz Now Platform ein, die Sie hinzufügen möchten, und tippen Sie auf **Anmelden**.
Der Zielbildschirm von Vulnerability Response wird angezeigt. Sie haben sich erfolgreich bei Vulnerability Response Mobile-App angemeldet!

4. Nach der Anmeldung wird überprüft, ob Benachrichtigungen in Vulnerability Response Mobile-Appaktiviert sind.

a. Tippen Sie im Zielbildschirm unten auf **Benachrichtigung**.

b. Tippen Sie im Bildschirm **Benachrichtigungen auf Benachrichtigungen aktivieren**, falls die Option nicht aktiviert ist.
Benachrichtigungen von Now Platform werden auf dem Bildschirm Benachrichtigungen in Vulnerability Response Mobile-Appangezeigt.

5. Nachdem Sie sich auf Ihrem Mobilgerät bei einer Instanz angemeldet haben, ist dies die Standardinstanz Now Platform auf dem Gerät.
Wenn Sie ein anderes Now Platform auf dem Gerät anzeigen möchten, müssen Sie sich von der Standardinstanz abmelden. So melden Sie sich ab:

a. Tippen Sie auf das Symbol **Einstellungen**.

b. Tippen Sie auf **Abmelden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Bildschirm Instanzen wird mit allen Now Platform -Instanzen angezeigt, die Sie dem Mobilgerät hinzugefügt haben.

c. **Wahlweise:** Tippen Sie auf eine andere Instanz, um sich anzumelden, oder folgen Sie alternativ den vorherigen Schritten, um eine weitere Instanz hinzuzufügen.

Ergebnisse

Wenn der Instanzenbildschirm für Vulnerability Response Mobile-App nicht angezeigt wird, nachdem Sie auf die App **ServiceNow Agent** auf Ihrem Gerät getippt haben, vergewissern Sie sich, dass **ServiceNow Agent** als vertrauenswürdige App auf Ihrem Gerät zugelassen ist. Um den Zugriff als vertrauenswürdige App zuzulassen, navigieren Sie auf Ihrem Gerät zu den Einstellungen und zur allgemeinen Geräteverwaltung, und tippen Sie auf die Option (Trust-App usw.), um den Zugriff zuzulassen.

Wenn nach der Eingabe Ihrer Anmeldeinformationen im Anmeldebildschirm eine Fehlermeldung angezeigt wird, überprüfen Sie, ob Anwendername und Passwort für die Instanz Now Platform korrekt sind.

Wenn beim Anzeigen des Zielbildschirms Probleme auftreten, überprüfen Sie Ihre Netzwerkverbindung.

Wenn Sie den Bildschirm „Instanzen“ nicht anzeigen können, nachdem Sie auf die App **ServiceNow Agent** getippt haben, versuchen Sie, sie von Ihrem Gerät zu deinstallieren. Stellen Sie sicher, dass Sie die aktuelle Version der App aus dem Apple App Store iOS oder dem Play Store Google haben, und versuchen Sie, sie erneut zu installieren.

Mit können Sie Korrekturaufgaben anzeigen, zuweisen und bearbeiten Vulnerability Response Mobile-App

Sie können die Felder in den Korrekturaufgaben-Datensätzen, die Ihrer Gruppe zugewiesen sind, anzeigen, zuweisen oder bearbeiten. Navigieren Sie durch Schwachstellen, angreifbare Elemente, Lösungsdatensätze und zugehörige Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

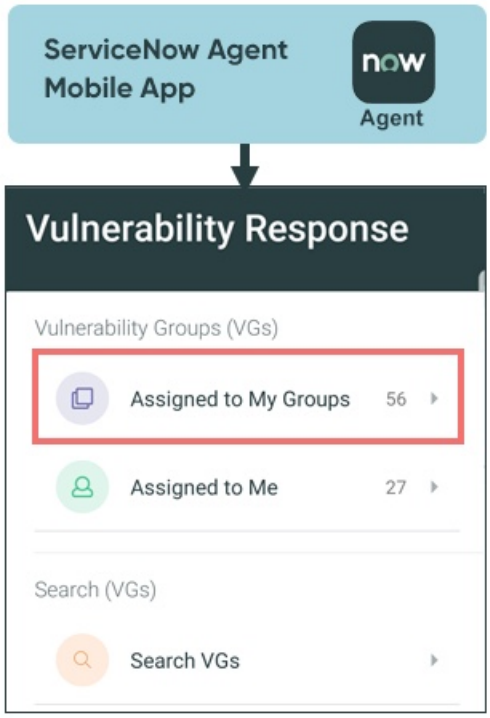
Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie RT-Datensätze (VUL) sich selbst zu, oder weisen Sie sie einem anderen Mitglied Ihrer Gruppe neu zu. Alternativ können Sie sich vor der Bearbeitung, Zuweisung oder Korrektur die Details aktiver Datensätze für Korrekturaufgaben, angreifbarer Elemente (VI), NVD-Schwachstellen und Lösungen anzeigen. Dauer für diese Aufgabe: 5–10 Minuten.

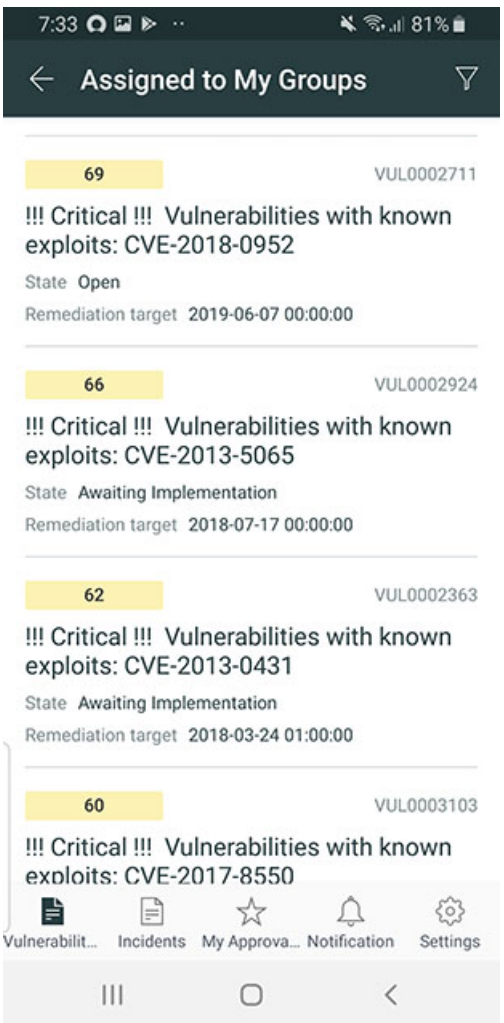
Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei der Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Vulnerability Response Mobile-App.
2. Tippen Sie im angezeigten Vulnerability Response-Zielbildschirm **auf Zugewiesen an Meine Gruppen**. Wenn Sie nach der Anmeldung von Vulnerability Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Liste der offenen Datensätze, die Ihrer Gruppe zugewiesen sind, wird angezeigt.

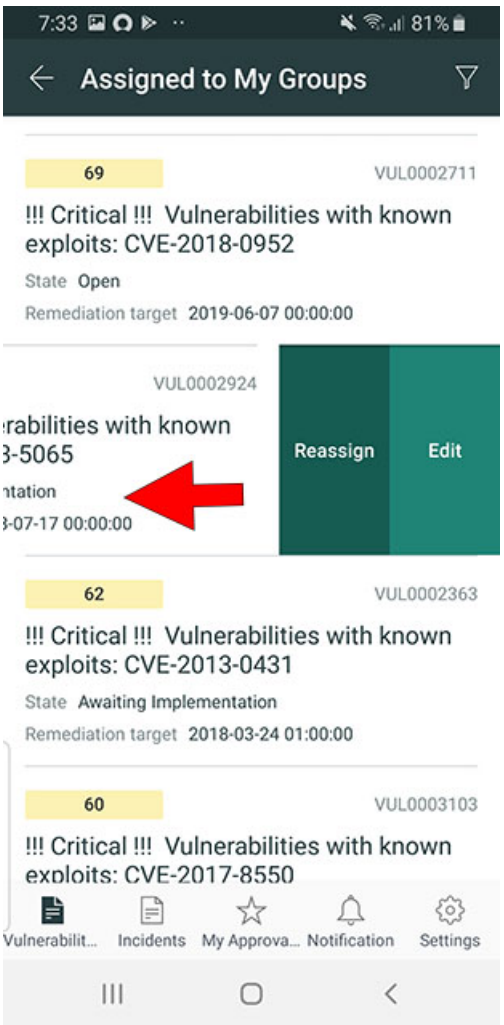


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Informationen zur Suche nach Datensätzen, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App.

4. Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen.
   Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator unter Now Platform.

5. Um einen Datensatz direkt aus der Liste neu zuzuweisen oder zu bearbeiten, wischen Sie bei angezeigter Liste der offenen Datensätze auf einem Datensatz nach links, um das Menü zu öffnen.



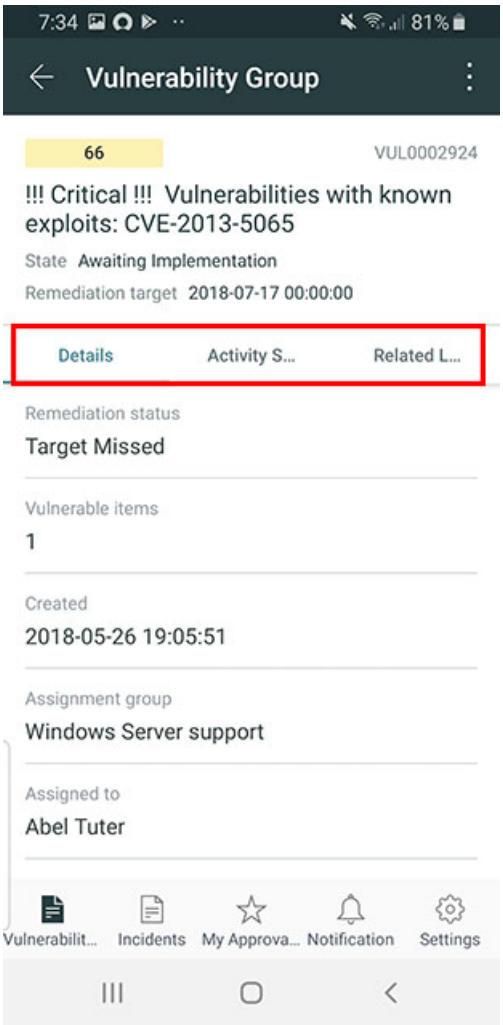
6. Wählen Sie eine aus dem angezeigten Menü, um fortzufahren.

7. Alternativ können Sie zum Anzeigen der Details eines offenen Schwachstellen-Datensatzes und um weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen, tippen Sie bei angezeigtem Bildschirm Zugewiesen an Meine Gruppen auf einen Datensatz in der Liste.

8. Wählen Sie im angezeigten Datensatz für die offene Korrekturaufgabe eine Option aus der folgenden Tabelle aus, um Arbeitsnotizen oder zugehörige Listen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Abbildung zeigt den Navigationspfad vom Datensatz der Korrekturaufgabe zum Datensatz der bevorzugten Lösung für die ausgewählte Schwachstelle. Navigieren Sie durch die Datensätze und zugehörigen Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigationspfad von der Korrekturaufgabe durch einen Lösungsdatensatz

9. Wählen Sie nach dem Überprüfen, Bearbeiten oder Remediieren eine Option aus, um fortzufahren.

Automatische Übersetzung

Mit können Sie Korrekturaufgaben anzeigen, neu zuweisen und bearbeiten, die Ihnen zugewiesen wurden Vulnerability Response Mobile-App

Sie können die Felder in den Ihnen zugewiesenen Korrekturaufgaben-Datensätzen anzeigen oder zuweisen oder bearbeiten. Navigieren Sie durch Datensätze und zugehörige Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

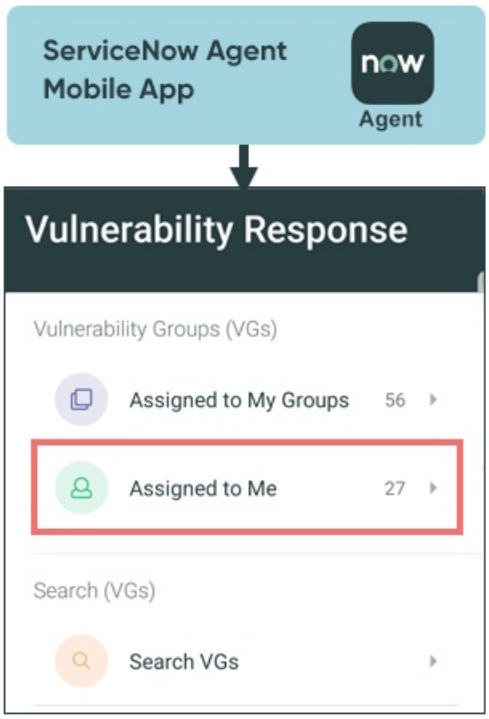
Warum und wann dieser Vorgang ausgeführt wird

Ihnen zugewiesene Datensätze neu zuweisen oder bearbeiten. Zeigen Sie die Details von aktiven Datensätzen für Korrekturaufgaben, Datensätzen von angreifbaren Elementen (VI), Schwachstellen und Lösungen an, bevor Sie sie bearbeiten, zuweisen oder korrigieren. Dauer für diese Aufgabe: 5–10 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

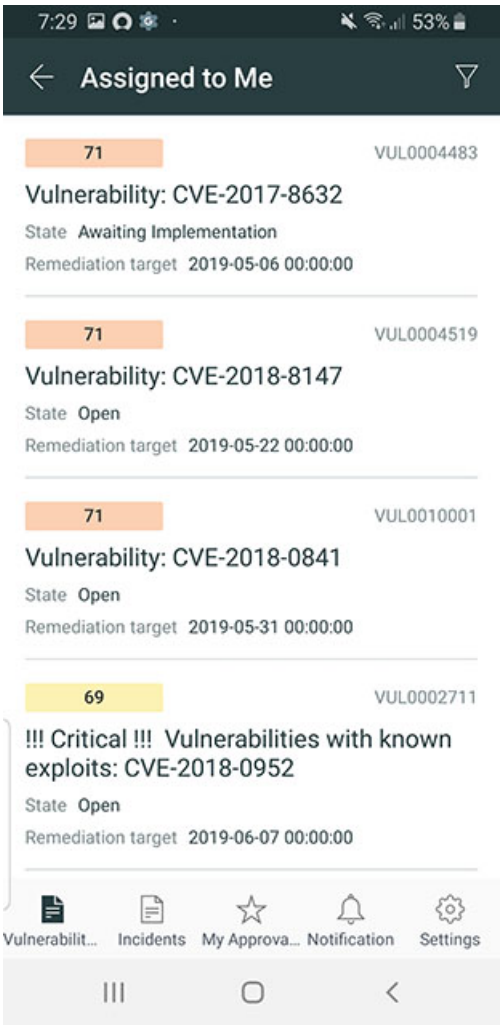
Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei der Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Vulnerability Response Mobile-App.
2. Tippen Sie im angezeigten **Vulnerability Response-** Zielbildschirm **auf Mir zugewiesen**.
   Wenn Sie nach der Anmeldung von Vulnerability Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



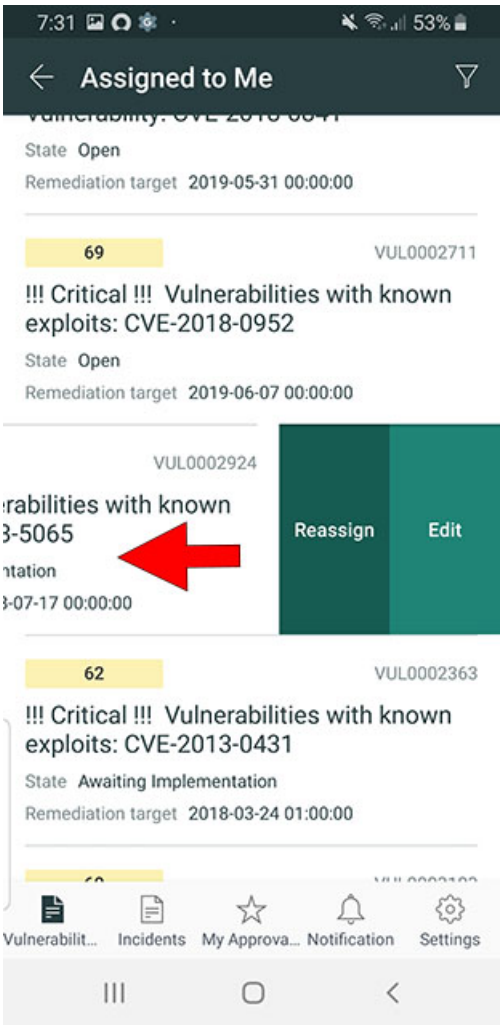
Die Liste der Ihnen zugewiesenen Datensätze für Korrekturaufgaben wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. **Wahlweise:** Informationen zur Suche nach Datensätzen, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App.
4. Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen.
   Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator unter Now Platform.
5. Um den Datensatz direkt aus der Liste neu zuzuweisen oder zu bearbeiten, wischen Sie bei angezeigtem Bildschirm Mir zugewiesen auf einem Datensatz nach links, um das Menü zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

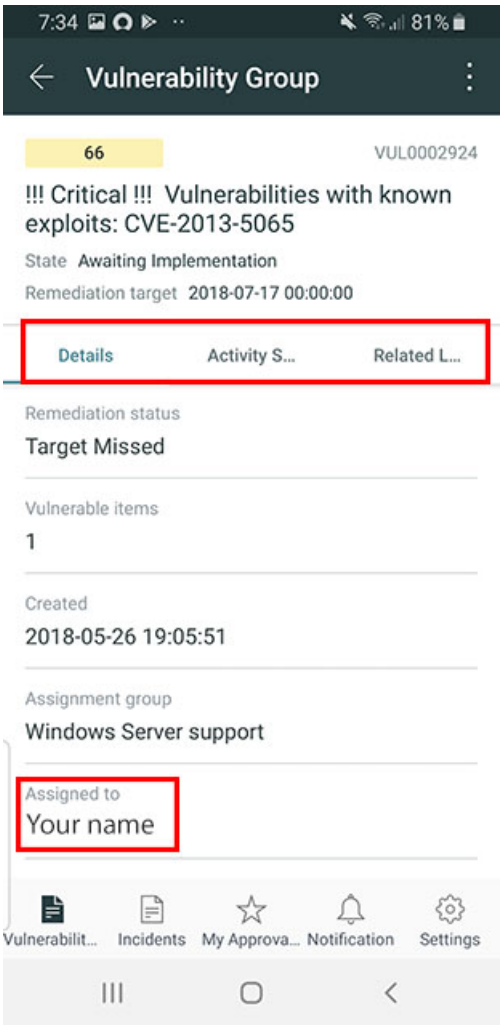


6. Wählen Sie eine, um fortzufahren.

7. Alternativ können Sie zum Anzeigen der Details eines geöffneten Datensatzes und um weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen, tippen Sie bei angezeigtem Bildschirm Mir zugewiesen auf einen Datensatz in der Liste.

8. Wählen Sie im angezeigten Datensatz für die offene Korrekturaufgabe eine Option aus der folgenden Tabelle aus, um Arbeitsnotizen oder zugehörige Listen anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Abbildung zeigt den Navigationspfad vom Datensatz der Korrekturaufgabe zum Datensatz der bevorzugten Lösung für die ausgewählte Schwachstelle. Navigieren Sie durch die Datensätze und zugehörigen Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigationspfad von RT durch einen Lösungsdatensatz

9. Wählen Sie eine, um fortzufahren.

Automatische Übersetzung

Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App

Suchen Sie nach Korrekturaufgaben, die bestimmten von Ihnen ausgewählten Suchkriterien entsprechen.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

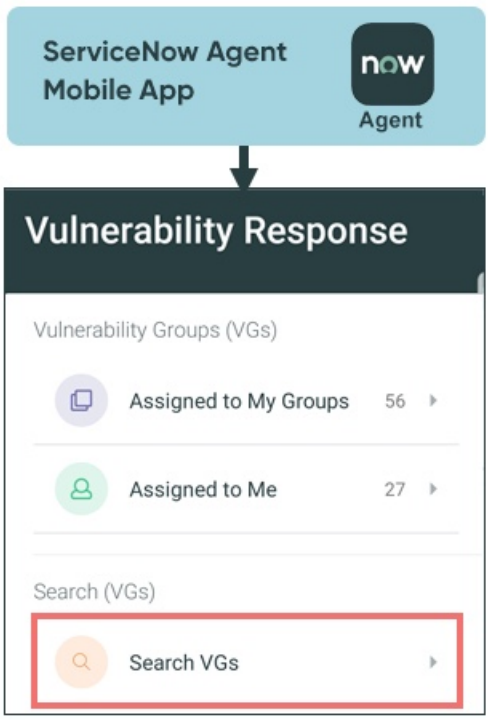
Warum und wann dieser Vorgang ausgeführt wird

Dauer für diese Aufgabe: 5–7 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei der Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Vulnerability Response Mobile-App.
2. Tippen Sie bei angezeigtem **Vulnerability Response-** Zielbildschirm auf **Search RTs (RTs**durchsuchen).
   Wenn Sie nach der Anmeldung von Vulnerability Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



3. Tippen Sie im angezeigten Suchbildschirm auf die Felder, und füllen Sie das Formular mit den gewünschten Suchkriterien aus.

   Befolgen Sie die Anweisungen nach der Tabelle, um Suchkriterien zu bearbeiten, Suchkriterien zu löschen oder eine Suche zu senden.

Tippen Sie auf dieses Feld	So fügen Sie einen Eintrag auf Geräten Android hinzu	So fügen Sie einen Eintrag auf Geräten iOS hinzu
Nummer	Tippen Sie auf den Bildschirm, und geben Sie eine RT-Nummer ein, z. B. (VUL0002372). Diese Nummer wird oben rechts im RT-Datensatz angezeigt. Tippen Sie auf das Häkchen-Symbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs zurückzukehren.	Geben Sie eine RT-Nummer ein, z. B. (VUL0002372). Diese Zahl wird oben rechts im RT-Datensatz angezeigt. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	So fügen Sie einen Eintrag auf Geräten Android hinzu	So fügen Sie einen Eintrag auf Geräten iOS hinzu
Risikobewertung	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.
Korrekturstatus	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.
Status	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.
Grund	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.
Zuweisungsgruppe	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	So fügen Sie einen Eintrag auf Geräten Android hinzu	So fügen Sie einen Eintrag auf Geräten iOS hinzu
	geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.	geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.
Zugewiesen an	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.
Kurzbeschreibung	Tippen Sie auf den Bildschirm, und geben Sie Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf das Häkchen-Symbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.	Geben Sie auf dem Bildschirm Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.
Beschreibung	Tippen Sie auf den Bildschirm, und geben Sie Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf das Häkchen-Symbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.	Geben Sie auf dem Bildschirm Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm SearchRTs zurückzukehren.

Bei Android -Geräten wählen Sie bei angezeigtem Bildschirm Search RTs (RTs durchsuchen) und Eingabe eines Kriteriums eines aus, um fortzufahren.

4. Wählen Sie bei iOS bei angezeigtem Bildschirm Search RTs (RTs durchsuchen) eines aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wahlweise:** Wenn Ihre Suche mehrere Datensätze zurückgibt, können Sie Filtern Sie Datensätze mit Vulnerability Response Mobile-App, um die Suchergebnisse zu verfeinern.

Filtern Sie Datensätze mit Vulnerability Response Mobile-App

Legen Sie zusätzliche Filter fest, um die Anzahl der Datensätze zu begrenzen, die in einem Bildschirm angezeigt werden. Das Filtern von Datensätzen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

Vorbereitungen
Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

Warum und wann dieser Vorgang ausgeführt wird
Dauer für diese Aufgabe: 5 Minuten.

Prozedur

1. Um Ihre Suchergebnisse weiter zu verfeinern oder zusätzliche Filterkriterien in einer beliebigen Liste von Datensätzen einzugeben, die angezeigt wird, tippen Sie auf das Filtersymbol ( ).
2. Tippen Sie bei angezeigtem Filter-Bildschirm auf ein Feld, um es zu erweitern.
   Ein allgemeines Feld zur Eingabe von Suchkriterien für Datensätze von Korrekturaufgaben ist das Feld Status.
3. Tippen Sie in den angezeigten Optionen auf das Kontrollkästchen, oder tippen Sie auf ein Element für Ihren Filter.
   Für viele der Filter können Sie mehr als eine Option auswählen.
4. Tippen Sie auf das Zurück-Symbol (Back) oder **auf FERTIG**, um Ihre Änderungen in einem Feld zu speichern.
   Die von Ihnen ausgewählten Kriterien werden im Filter-Bildschirm angezeigt. Die Anzahl der Datensätze, die Ihren Kriterien entsprechen, wird auch oben im Bildschirm angezeigt. Tippen Sie auf **ZURÜCKSETZEN**, um alle Filter zu entfernen und die Standardeinstellung wiederherzustellen.
5. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 4 bei angezeigtem Bildschirm Filter, um mit dem Festlegen Ihrer Filterkriterien fortzufahren.
6. Tippen Sie auf das Kreuzungssymbol ( ), um UND-Bedingungen festzulegen.
7. Alternativ können Sie auf das Schnittmengensymbol ( ) tippen, um ODER-Bedingungen festzulegen.
8. Nachdem Sie alle gewünschten Kriterien hinzugefügt haben, tippen Sie bei angezeigtem Filter-Bildschirm auf **FERTIG**.
   Auf dem Bildschirm werden nur die Datensätze angezeigt, die Ihren Filterkriterien entsprechen.

Zugehörige Informationen

Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App

Vulnerability Response Orchestration

Mit Workflows und Aktivitäten Vulnerability Response Orchestration von können Sie mithilfe der Workflow-Orchestration mit Windows- oder UNIX-basierten Systemen und Umgebungen interagieren und Daten aus diesen abrufen. Durch das Anreichern von Daten können Sie den Korrekturlebenszyklus verkürzen.

Weitere Informationen zum Bearbeiten oder Erstellen von anwenderdefinierten Workflows finden Sie unter Exploring flows .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Orchestration Workflows und Aktivitäten

Vulnerability Response Orchestrationenthält mehrere Workflows. Workflows und Aktivitäten automatisieren und beschleunigen Ihre -Prozesse. Verwenden Sie Workflows und Aktivitäten, um Scan-Datensätze zu erstellen, angreifbare Elemente zu scannen, Scan-Datensätze zu erstellen und vieles mehr.

Vulnerability Response Workflow zum Scannen auf Schwachstellen

Automatisieren Sie Schwachstellen-Scans für einzelne oder mehrere angreifbare Elemente mit dem Workflow **„Vulnerability Response – Scan Vulnerability“,** der im Basissystem enthalten ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow **„Vulnerability Response – Scan Vulnerability“** erstellt einen Scan-Datensatz für die Schwachstelle oder Gruppe von Schwachstellen, aus der er aufgerufen wurde.

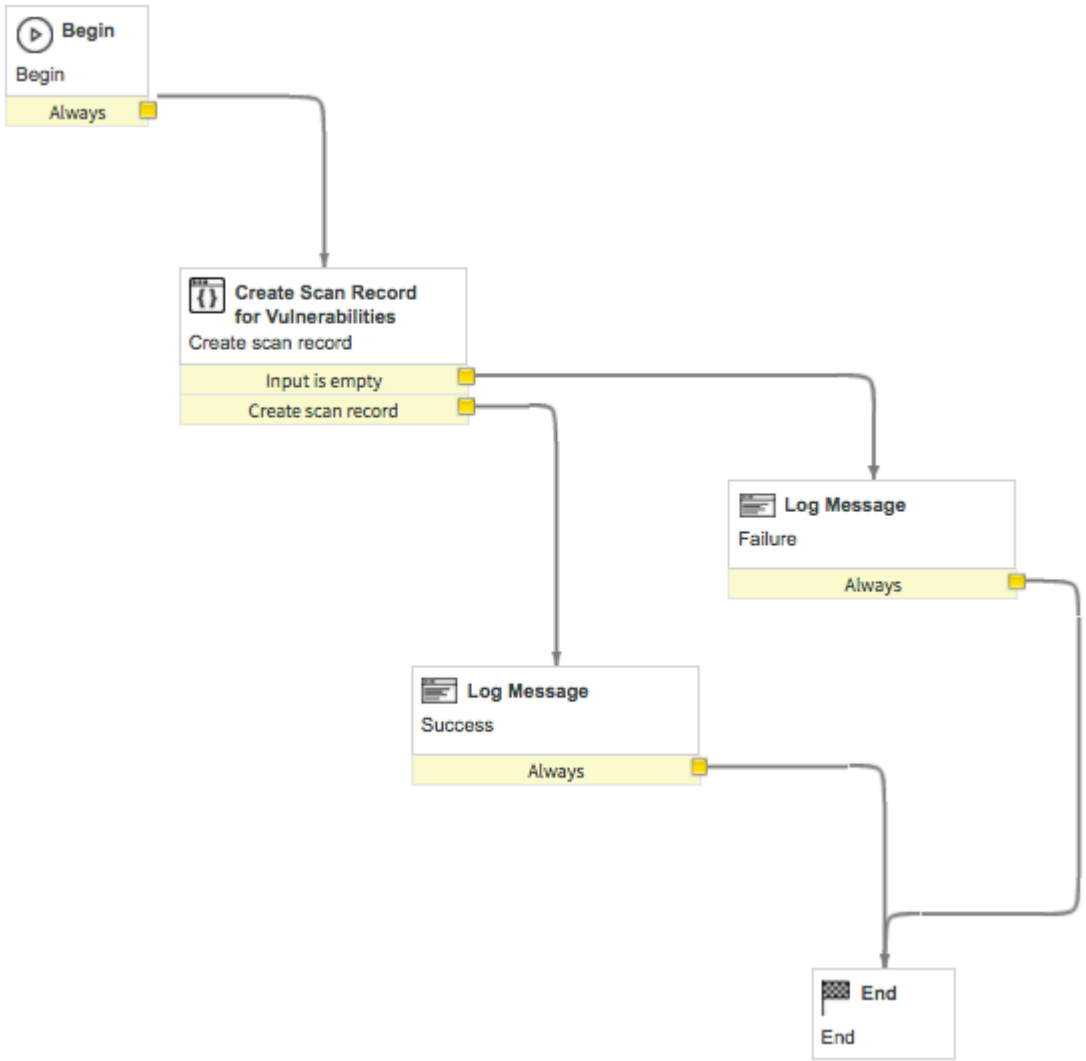
Hinweis:

- Es empfiehlt sich, Schwachstellen oder angreifbare Elemente nach der Korrektur erneut zu scannen, wenn ein Schwachstellen-Patch auf die betroffenen Datensätze angewendet wird. Sie können den erneuten Scan mit der beschriebenen Methode durchführen oder die erneuten Scans automatisieren.
- Ab v23.0 von Vulnerability Responseist der Workflow **„Vulnerability Response – Schwachstelle scannen“** veraltet und wird durch den Flow „Schwachstelle erneut scannen“ im Flow Designer ersetzt.

Zu den Workflow-Aktivitäten gehören Variablen für die Aktivität Scan-Datensatz für Schwachstellen erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response: Workflow zum Scannen auf Schwachstellen



Workflow zum Scannen auf Schwachstellen

Die zugehörigen Listen namens **Vulnerability Response** > **Schwachstelle scannen** Der Workflow scannt eine Korrekturaufgabe erneut.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird von **„Angreifbare Gruppe erneut scannen"** während einer Aktion **„Schließen/Ignorieren"** ausgelöst.

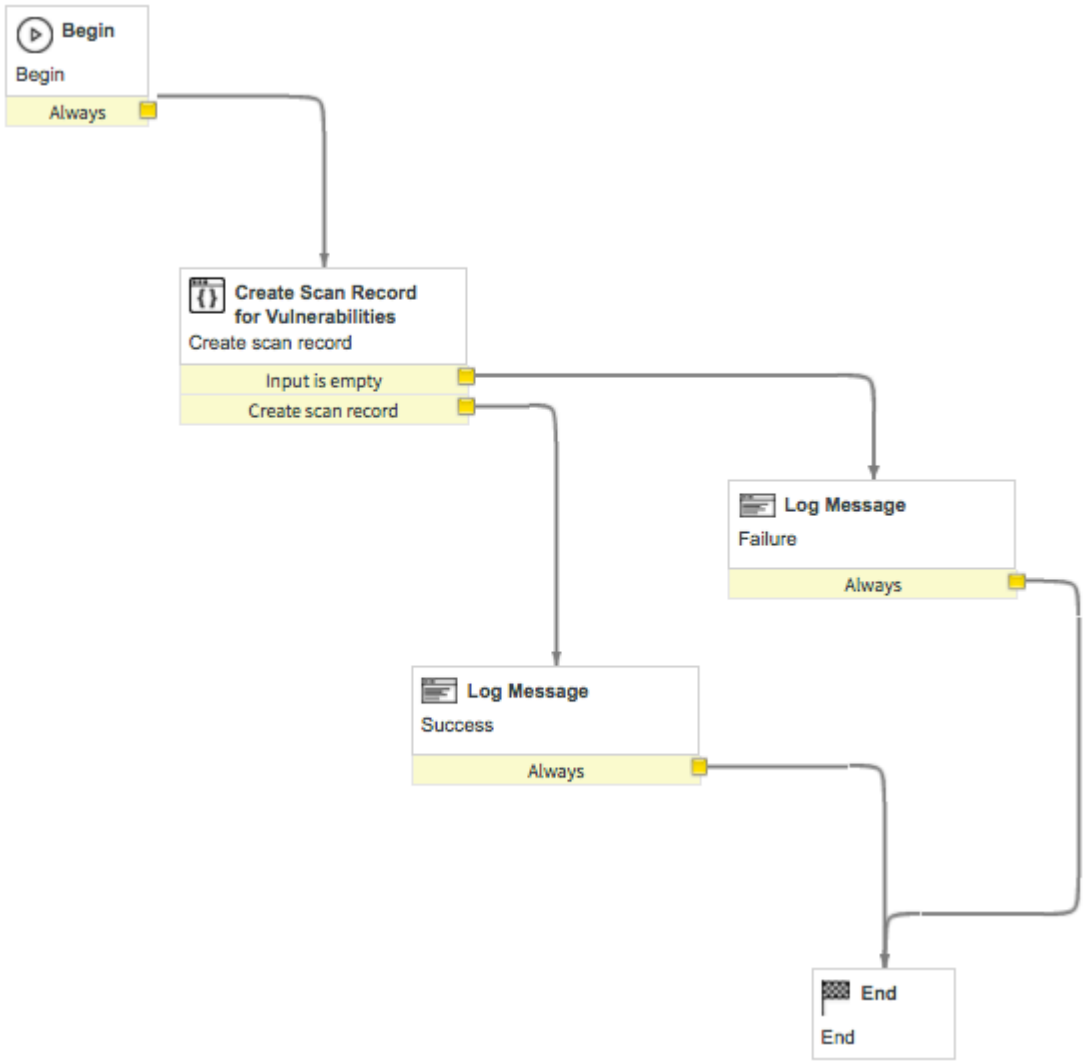
Zu den Workflow-Prozessaktivitäten gehören:

Variablen für die Aktivität Scan-Datensatz für Schwachstellen erstellen

Protokollnachricht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow zum Scannen auf Schwachstellen



Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie einen Aufgabendatensatz (VUL).
3. Klicken Sie auf **Schließen**.
4. Wählen Sie **Geschlossen** für **Gewünschter Status**aus.
5. Wählen Sie **Fest** für den **Substatus**aus.
6. Wählen Sie **Warten auf Bestätigung beim nächsten Scan** für **Jetzt schließen?**
   Für die Korrekturaufgabe und angreifbare Elemente ändert sich der **Status** in **Bestätigung ausstehend**und der **Substatus** in **Fest**und es wird ein erneuter Scan ausgeführt.

Vulnerability Response Workflow zum Scannen angreifbarer Elemente

Automatisieren Sie Schwachstellen-Scans für einzelne oder mehrere angreifbare Elemente mit dem Workflow **„Vulnerability Response – Angreifbare Elemente scannen“,** der im Basissystem enthalten ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
Der Workflow **„Vulnerability Response – Angreifbare Elemente scannen“** erstellt einen Scan-Datensatz für das angreifbare Element oder die Gruppe von Elementen, aus der er aufgerufen wurde.

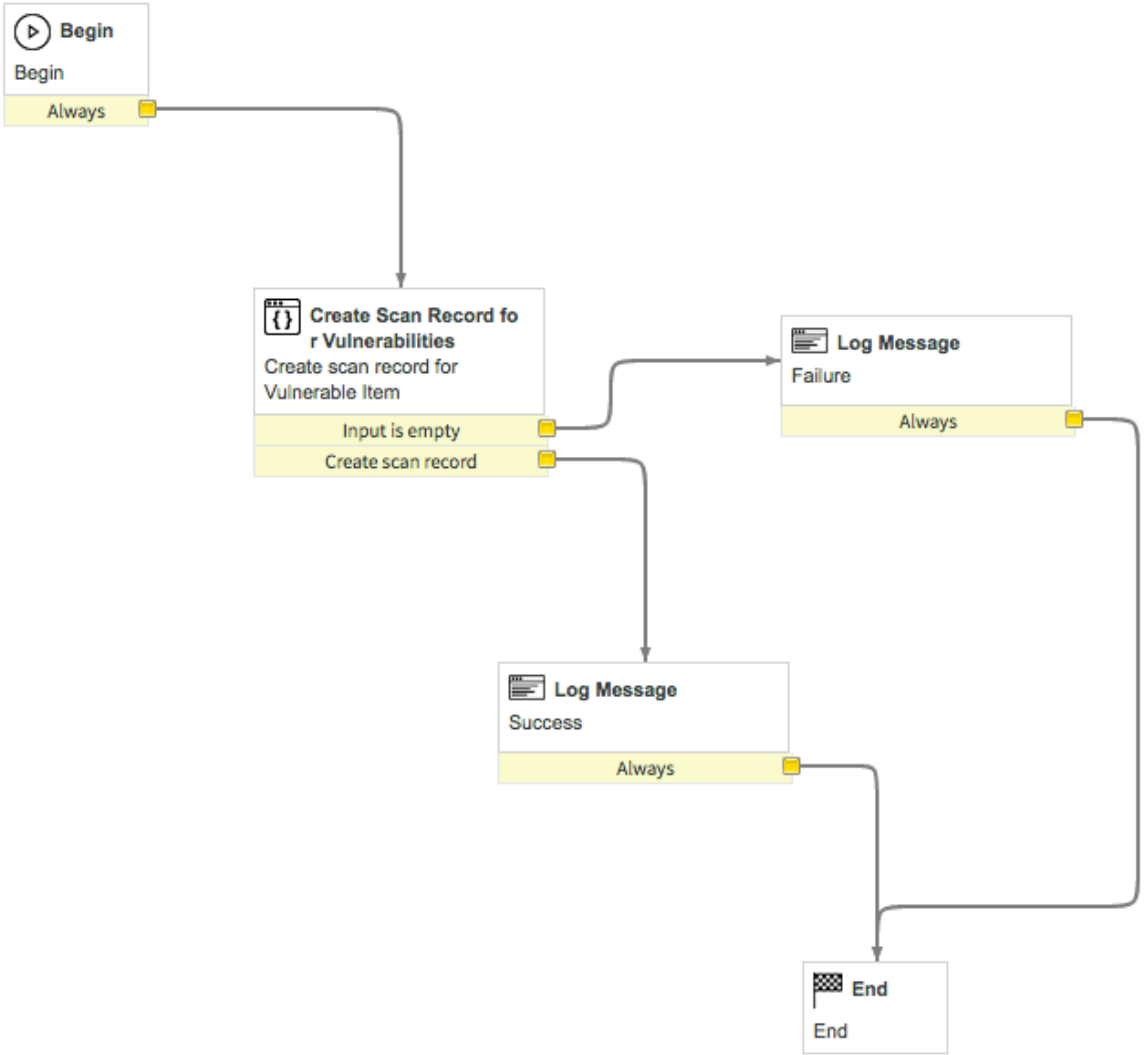
Hinweis:

- Es empfiehlt sich, Schwachstellen oder angreifbare Elemente nach der Korrektur erneut zu scannen, wenn ein Schwachstellen-Patch auf die betroffenen Datensätze angewendet wird. Sie können den erneuten Scan mit der beschriebenen Methode durchführen oder die erneuten Scans automatisieren.
- Ab v23.0 von Vulnerability Responseist der Workflow **„Vulnerability Response – Angreifbare Elemente scannen“** veraltet und wird durch den Flow „Angreifbares Element erneut scannen“ im Flow Designer ersetzt.

Zu den Workflow-Prozessaktivitäten gehören: Variablen für die Aktivität Scan-Datensatz für Schwachstellen erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response: Workflow zum Scannen angreifbarer Elemente



Workflow zum Scannen von angreifbaren Elementen

Die zugehörigen Listen namens**Vulnerable Response** > **Angreifbares Element scannen** Der Workflow scannt ein angreifbares Element erneut.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird durch **„Schwachstelle erneut scannen“**während einer Aktion **„Schließen/Ignorieren“** ausgelöst.

Zu den Workflow-Prozessaktivitäten gehören:

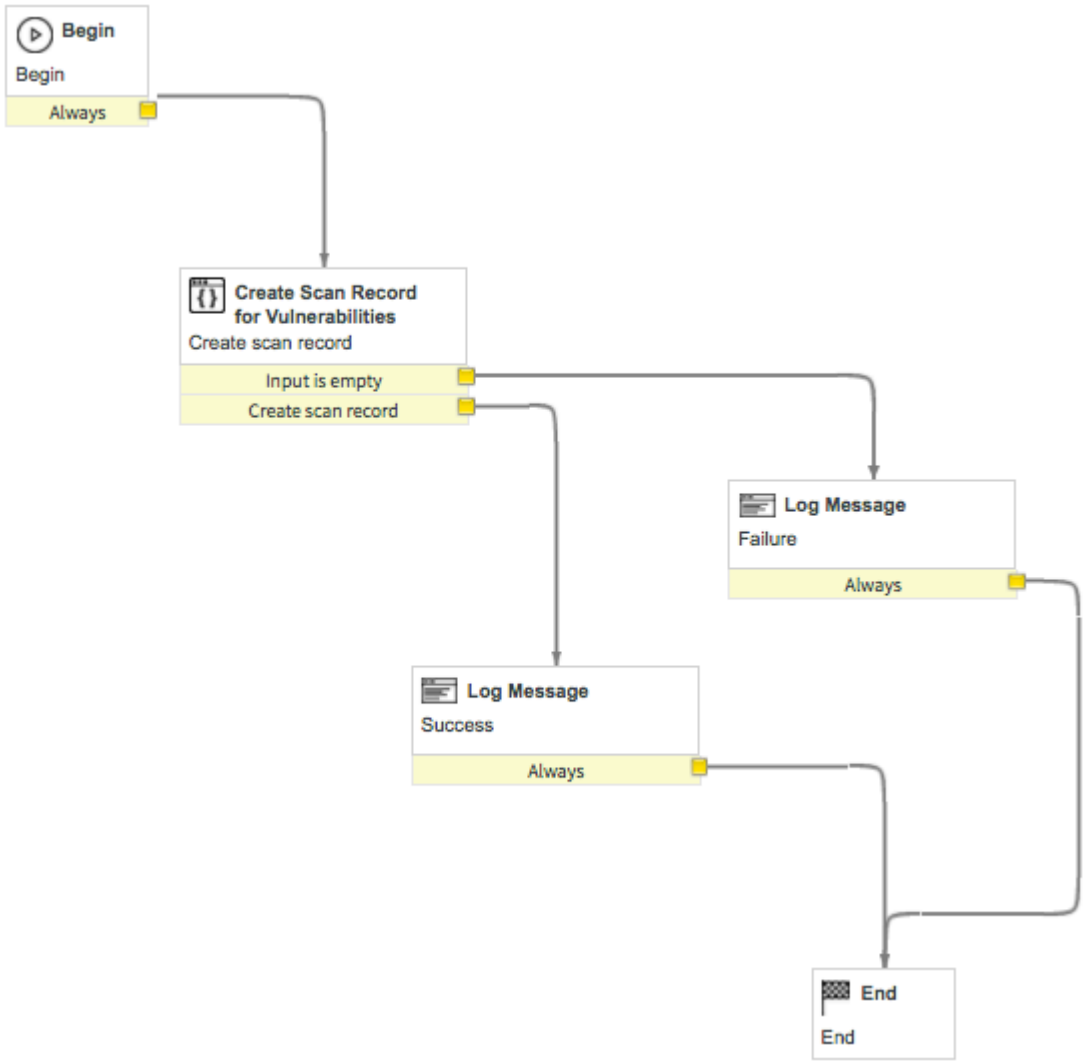
Variablen für die Aktivität Scan-Datensatz für Schwachstellen erstellen

Protokollnachricht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow zum Scannen auf Schwachstellen



Prozedur

1. Navigieren zu **Schwachstelle** > **Schwachstellen** > **Angreifbare Elemente**.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie **auf Schließen/Ignorieren**.
4. Wählen Sie **Geschlossen**für **Gewünschter Status**aus.
5. Wählen Sie **Fest** für den **Substatus**aus.
   Der **Status** der Gruppe ändert sich in **Bestätigung ausstehend**, der **Substatus** ändert sich in **Fest**und es wird ein erneuter Scan ausgeführt.

Vulnerability Response Orchestration Workflow-Aktivitäten

Vulnerability Response Orchestration Mithilfe von Workflow-Orchestration können Benutzer mithilfe von Workflow-Orchestration-Lösungen ermitteln, ob eine Schwachstelle bereits bei anderen Security Incidents oder auf anderen Systemen erkannt wurde.

Variablen für die Aktivität Scan-Datensatz für Schwachstellen erstellen

Schwachstellen-Scans für einzelne oder mehrere angreifbare Elemente können mit der Workflow-Aktivität **Scan-Datensatz für Schwachstellen erstellen** ausgeführt werden, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

im Basissystem enthalten ist. Wenn die Eingabe an die Aktivität übergeben wird, wird ein Scan-Datensatz erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Aufgaben-IDs [Zeichenfolge]	Eine Zeichenfolge von durch Kommas getrennten sysIds, die die erwarteten Eingaben definieren. Dieses Feld ist ein Pflichtfeld.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
scanResult [Boolean]	Gibt „Wahr“ zurück, wenn die Eingabe nicht leer ist. Für die Aufgaben-IDs wird ein Scan-Datensatz erstellt.

Application Vulnerability Response

Die Funktion Application Vulnerability Response (AVR) der Anwendung ServiceNow® Vulnerability Response importiert angreifbare Elemente (Application Vulnerable Items, AVITs) und ermöglicht Ihnen gemäß den Regeln die Behebung von Anwendungsschwachstellen. Vulnerability Response ist über ein separates Abonnement verfügbar.

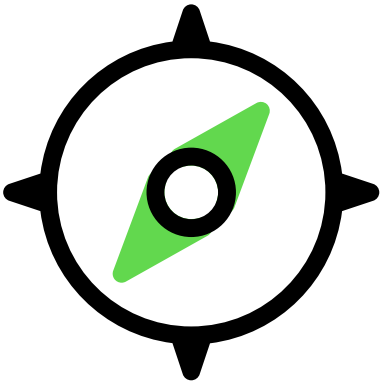
Ab AVR v19.0 wurden einige Schlüsseltabellen- und Spaltennamen aktualisiert. Daher finden Sie in der Dokumentation Verweise auf den älteren und den neueren Namen. Die vollständige Liste der aktualisierten Begriffe finden Sie unter Application Vulnerability Response-Produktübersicht.

Ab v19.0 von Vulnerability Responsekönnen Sie Schwachstellendaten für die Softwarezusammensetzungsanalyse (SCA) und die Software-Stückliste erfassen, um Schwachstellen in Ihren Softwareanwendungen zu identifizieren. Weitere Informationen finden Sie unter Application Vulnerability Response erkunden und Veracode Vulnerability Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

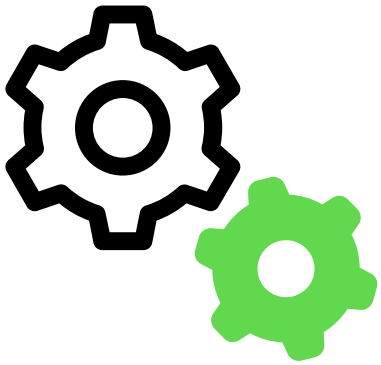
Application Vulnerability Response

Untersuchen



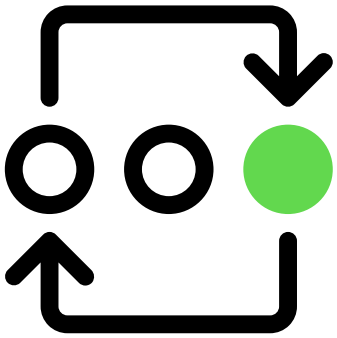
Erfahren Sie mehr über die Konzepte und Funktionen von Application Vulnerability Response.

Konfigurieren



Konfigurieren Sie Application Vulnerability Response.

integrieren

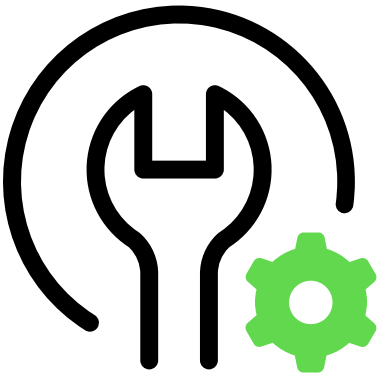


Erweitern Sie Application Vulnerability Response durch die Integration mit anderen Anwendungen.

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

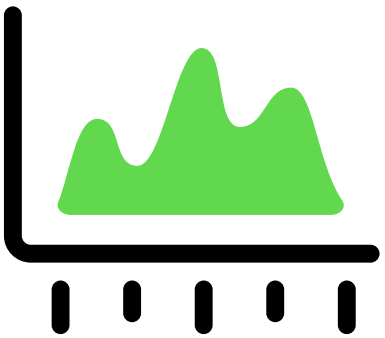
Erfahren Sie, wie Sie AVITs in den Arbeitsbereichen Vulnerability Manager, IT Remediation und Vulnerability Assessment überwachen, verwalten und beheben können.

Beheben



Erfahren Sie, wie Sie Anwendungsschwachstellen beheben können.

Analytics und Reporting

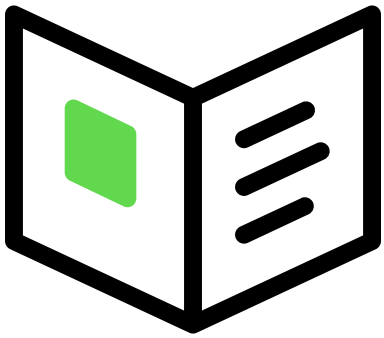


Zeigen Sie Application Vulnerability Response Analytics an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response (Fortsetzung)

	Referenz	
	 Rufen Sie Detailinformationen zu den Komponenten von Application Vulnerability Response wie Feldern, Tabellen und Eigenschaften ab.	

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Application Vulnerability Response erkunden

Anwendungsschwachstellen sind Schwachstellen in Ihren anwenderdefinierten Softwareanwendungen, die während des gesamten Entwicklungslebenszyklus der Anwendung gescannt werden.

Übersicht über Application Vulnerability Response und verfügbare Versionen

Application Vulnerability Response (AVR) ist der Teil der Anwendung Vulnerability Response, der Anwendungsschwachstellen verarbeitet.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response v23.0 Vulnerability Response v22.0 Vulnerability Response v21.0	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen (Fortsetzung)

Freigabeversion	Release-Hinweise
Vulnerability Response v20.0 Vulnerability Response v19.0 Vulnerability Response v18.2	Kompatibilitätsmatrix und Releaseschemaänderungen

Funktionsweise

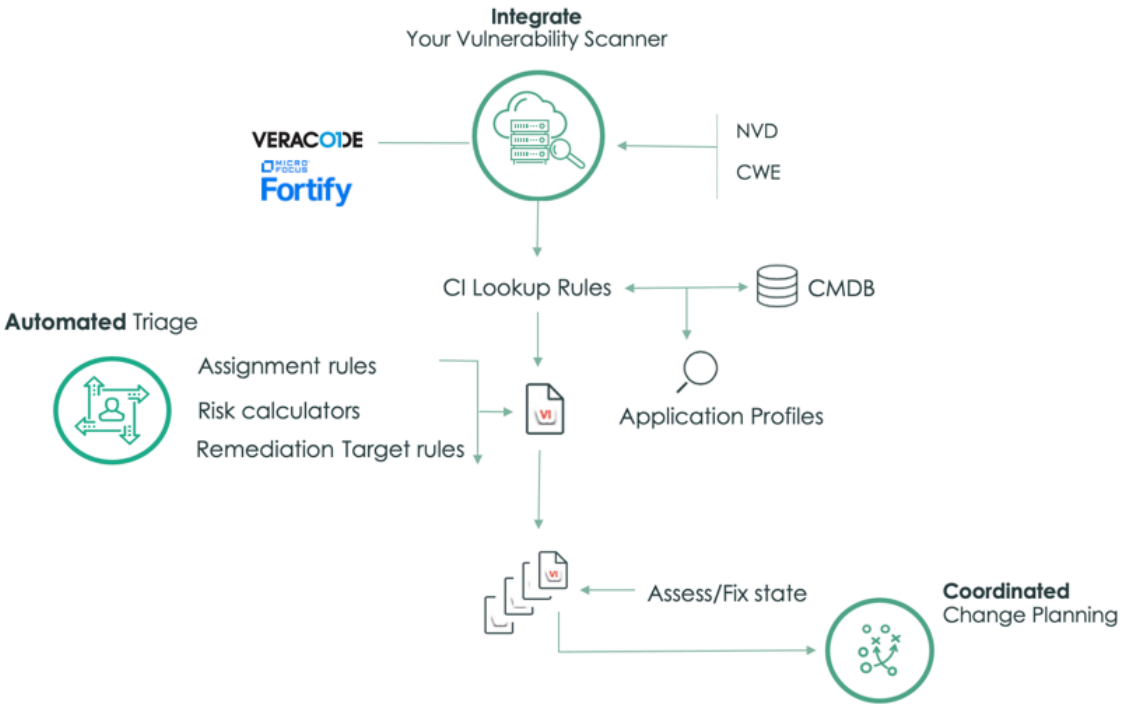
Schwachstellendaten werden aus internen und externen Quellen importiert, z. B. Common Weakness Enumeration (CWE) oder Drittanbieterintegrationen. Nach dem Import von Daten werden sie mit Anwendungsdaten in Ihrem Configuration Management Database (CMDB) verglichen und in der Anwendung Application Vulnerability Response verarbeitet. Wenn eine Übereinstimmung zwischen importierten Anwendungsschwachstellendaten und Daten in Ihrer CMDB besteht, wird ein angreifbares Element in der Anwendung (Application Vulnerable Item, AVIT) erstellt.

Application Vulnerability Response enthält die folgenden Schlüsselfunktionen:

- Integrieren Sie mit unterstützten Scannern von Drittparteien, um Schwachstellendaten zu importieren.
- Vergleichen Sie Daten im Zusammenhang mit Anwendungsschwachstellen, und ermitteln Sie, ob in einer Anwendung Anwendungsschwachstellen gefunden wurden.
- Priorisieren, korrigieren und verwalten Sie angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIT). Jede Anwendungsschwachstelle stellt einen Schwachstelleneintrag in den CWE- oder Drittparteibibliotheken dar.
- Ab Version 18.0 von Vulnerability Responsekönnen Sie AVITs in Vulnerability Manager Workspace bzw. IT Remediation Workspace überwachen und beheben. Weitere Informationen finden Sie unter Vulnerability Manager Workspace und IT Remediation Workspace.
- Korrelieren Sie Daten Application Vulnerability Response mithilfe von Rechnern und Bibliotheken, um die folgenden Aufgaben auszuführen.
  - Erstellen Sie mithilfe von **CI-Suchregeln**automatisch angreifbare Anwendungselemente. Während des Imports werden einer CWE Schwachstellen von Drittparteien zugeordnet, um eine AVIT zu erstellen.
  - Erstellen Sie Zuweisungsregeln, um die Zuweisung von angreifbaren Anwendungselementen zu automatisieren.
  - Verwenden Sie Rechnergruppen, um die Geschäftsauswirkung zu bestimmen, variierende Bedingungen mithilfe von Filtern anzugeben, einfache Berechnungen anzuwenden oder ein Skript zu verwenden.
  - Erstellen Sie Korrekturzielregeln, die den erwarteten Zeitrahmen für die Korrektur angreifbarer Anwendungselemente definieren, damit Sie bevorstehende Korrekturaktivitäten überwachen können.
- Verknüpfen Sie eine einzelne Drittanbieter-Schwachstelle mit mehreren CWE-Einträgen, und suchen Sie die primäre CWE für eine Schwachstelle, um das Risiko zu bestimmen. Weitere Informationen zur **primären CWE**finden Sie unter Anwendungsschwachstellen-Felder.
- Verwenden Sie CWE-Datensätze, die aus der CWE-Datenbank heruntergeladen oder aus Drittanbieterintegrationen importiert werden, als Referenz, um zu entscheiden, ob Sie eine Schwachstelle eskalieren müssen. Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie Application Vulnerability Response, um den Informationsfluss von der Integration über die Untersuchung bis zur Lösung zu verfolgen.



Arten der importierten Schwachstellendaten

Application Vulnerability Response unterstützt die folgenden Arten importierter Anwendungsschwachstellendaten.

Hinweis:
Vor v19.0 wurden SAST-, SCA-, IAST- und Penetrationstestdaten nicht erfasst. Dies kann Unterschiede zwischen dem, was in Veracode, Fortifyund Invicti angezeigt wird, und dem, was in Application Vulnerability Responseangezeigt wird, erklären.

Dynamische Anwendungssicherheitstests (Dynamic Application Security Testing, DAST)

DAST-Scans ermitteln Schwachstellen in Anwendungen, indem Eingaben an Ihre Anwendungen gesendet und deren Antworten während der Ausführung überwacht werden. Dieser Ansatz kann einen externen Angriff imitieren. Beim dynamischen Scannen wird ein laufender Service (URL) auf Schwachstellen gescannt. Schwachstellenergebnisse enthalten einen URL-Speicherort einer erkannten Schwachstelle.

Statische Anwendungssicherheitstests (Static Application Security Testing, SAST)

SAST-Scans überprüfen den Quellcode von Anwendungen im Ruhezustand und helfen Ihnen, Schwachstellen in der Art und Weise zu finden, wie Sie Ihren Code geschrieben haben. Der SAST-Scan erfolgt für nicht kompilierten Quellcode und ist daher unabhängig von Anwendungsservices vorhanden. Die zurückgegebenen Ergebnisse enthalten eine Datei und die Zeilennummer des Speicherorts einer erkannten Schwachstelle.

Interaktive Anwendungssicherheitstests (Interactive Application Security Testing, IAST)

IAST-Scans erkennen Softwareschwachstellen durch Interaktion mit dem Programm, während es ausgeführt wird. Beobachtung durch Menschen, automatisierte Tests und Sensoren werden in Kombination verwendet, um mit der Anwendung zu interagieren und Schwachstellen zu lokalisieren.

Softwarezusammensetzungsanalyse (SCA)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab v19.0 von Vulnerability Responsekönnen Sie SCA-Schwachstellen (Software Composition Analysis) erfassen. SCA-Schwachstellendaten helfen Ihnen, Schwachstellen in der Open Source-Software zu identifizieren, die in Ihren Softwareanwendungen verwendet wird.

Penetrationstests

Sie konfigurieren Bewertungsanforderungen für Penetrationstests in Application Vulnerability Response, um nachvollziehen zu können, wo die Schwachstellen Ihrer Anwendung liegen und was Sie tun können, um sie zu beheben.

Software-Stückliste

Laden Sie Daten Software Bill of Materials (SBOM) hoch, um Schwachstellen in Ihren Open Source-Komponenten zu identifizieren. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Anwendungsfälle

Einige der folgenden DAST-Anwendungsfälle werden unterstützt:

- Ordnen Sie jede Schwachstelle anhand der Scan-Ergebnisse einer Art von cmdb_ci (untergeordnete Klasse) zu.
- DAST-Scan-Ergebnisse mit einer vorhandenen Anwendung verknüpfen, wenn in CMDB ein Datensatz von Discovery oder einer Drittanbieterintegration vorhanden ist.
- DAST-Scan-Ergebnis mit einer neu eingefügten gescannten Anwendung verknüpfen, wenn eine neue Anwendung zuvor nicht identifiziert und/oder in der CMDB gespeichert wurde.
- Speichern Sie DAST-Scan-Ergebnisse für eine CMDB, wenn Sie Ihre Anwendungen in einem anderen -Produkt als ServiceNow®verwalten.
- Speichern Sie DAST-Scan-Ergebnisse für eine CMDB, wenn Sie sie zuvor für einen anderen Zweck angepasst haben.
- Erstellen Sie manuell eine Anwendung für das Quellcode-Repository.

Einige der unterstützten SAST-Anwendungsfälle werden unterstützt:

- Ordnen Sie jede Schwachstelle anhand der Scan-Ergebnisse einer Art von cmdb_ci (untergeordnete Klasse) zu.
- Erstellen Sie manuell ein CI für das Quellcode-Repository.
- Speichern Sie SAST-Scan-Ergebnisse ohne zugehörigen Anwendungsservice.

[store-future: BEGIN review]Einige der folgenden IAST-Anwendungsfälle werden unterstützt:[End]

[store-future: BEGIN review]Einige der unterstützten SCA-Anwendungen werden unterstützt:[End]

Integrationen von Drittparteien

Die von Application Vulnerability Response unterstützten Drittanbieterintegrationen sind als separate Anwendungen in ServiceNow Storeverfügbar. Weitere Informationen finden Sie unter Integration von Application Vulnerability Response mit anderen Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

- Eine gemeinsam genutzte API importiert DAST-, SAST-, IAST-und SCA-Daten sowie manuelle Pen-Testergebnisse. Weitere Informationen finden Sie unter Penetrationstests.
- Für den Import von SBOM-Daten wird eine separate API verwendet. Weitere Informationen finden Sie unter Software Bill of Materials erkunden und Veracode Vulnerability Integration.

CI-Suchregeln

Anwendungsdaten automatisch nach Übereinstimmungen in Configuration Management Database (CMDB)durchsuchen.

Zuweisungsregeln

Weisen Sie Anwendungsschwachstellen automatisch basierend auf Benutzergruppen, Benutzergruppenfeldern und Skripts zu.

Risikorechner

Priorisieren und bewerten Sie die Auswirkungen von AVITs mithilfe von Rechnern automatisch, basierend auf beliebigen Kriterien, indem Sie Bedingungsfilter verwenden.

Schweregradzuordnung

Anfangswerte für Felder in angreifbaren Anwendungselementen automatisch berechnen. Schwachstelleneinträge haben sowohl einen Quellschweregrad als auch einen normalisierten Schweregrad (basierend auf der Schweregradzuordnung). Der Schweregrad ist an die Common Weakness Enumeration (CWE) gebunden.

Korrekturzielregeln

Definieren Sie den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Anwendungselements.

Berichterstellung

Gewinnen Sie schnell Einblicke in Ihre Sicherheitslage, Abhilfetrends und Top-10-Anwendungen oder Geschäftsbereiche mit den wichtigsten AVITs.

Der gemeinsame Punkt für beide Arten von Scans ist das Anwendungs-Release. Ein Anwendungs-Release, das eine **Namenszeichenfolge** definiert, ist der Verbindungspunkt, um die gescannten Schwachstellenergebnisse auf der Scannerseite zu gruppieren. Auf diese Weise weiß AVR, zu welchem Anwendungs-Release die Ergebnisse gehören, wenn Scan-Ergebnisse über die Integration importiert werden.

Die untergeordnete Tabelle Configuration Item [cmdb_ci], Gescannte Anwendungen [sn_vul_app_scanned_application], wurde in der Anwendung und im Bereich Vulnerability Response erstellt. In dieser Tabelle wird die Abstraktion für das Anwendungs-Release gespeichert, und über ihre CMDB-Beziehungen werden Servicegrafiken bereitgestellt. Sie können im angezeigt werden **Alle** > **Application Vulnerability Response** > **Administration** > **Anwendungen** Modul. Die Listenansicht für gescannte Anwendungen enthält die **Abteilung** und **die Supportgruppe,** die während des Setups hinzugefügt wurden.

Angreifbare Anwendungselemente (AVITs)

Bei Anwendungsschwachstellen verknüpft AVR eine Schwachstelle mit einer Anwendung, um den AVIT-Datensatz (Application Vulnerable Item) zu erstellen. Aufgrund der Vielzahl von Definitionen dessen, was eine Anwendung in der CMDB ausmacht, beschränkt Application Vulnerability Response Anwendungen auf gescannte Anwendungen. Gescannte Anwendungen sind die in Ihrer Umgebung gescannten Anwendungen, die von AVR als **Name** und **ID**identifiziert werden. AVITs basieren auf der neuesten Scan-Zusammenfassung,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bis sie vom Scanner **behoben werden**. Wenn kein AVIT mehr gefunden wird, bleibt er an die Scan-Zusammenfassung gebunden, in der er zuletzt aufgetreten ist.

Angreifbare Anwendungselemente können über angezeigt werden **Alle** > **Application Vulnerability Response** > **Schwachstellen** > **Angreifbare Elemente** Modul.

Wenn eine Anwendung aus der CMDB entfernt wird, werden alle zugehörigen AVITs geschlossen.

Informationen zu AVIT-Formularfeldern finden Sie unter Felder für angreifbare Anwendungselemente.

Benutzergruppen und -rollen in Application Vulnerability Response

Oft arbeitet ein Team zusammen, um Anwendungsschwachstellen zu erstellen, zu verwalten und das Management von Anwendungsschwachstellen zu überwachen. Unter den Teammitgliedern gibt es strategische Rollen sowie operative Rollen. In den meisten Organisationen können Sie mehr als eine Rolle übernehmen und häufig Rollen mit anderen teilen. Application Vulnerability Response verwendet drei Anwendergruppen mit granularen Rollen: App-Sec-Manager, Anwendungssicherheits-Champion und Entwickler. Weitere Informationen zu diesen Gruppen und Rollen finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen.

Application Vulnerability Response Status

Application Vulnerability Response bietet ein Statusmodell für den Status Ihrer angreifbaren Elemente in der Anwendung (Application Vulnerable Items, AVITs) und hilft Ihnen zu bestimmen, wann und wie Sie Ihre AVITs korrigieren müssen.

Ein angreifbares Anwendungselement hat mehrere mögliche Status. Weitere Informationen finden Sie unter Status des angreifbaren Elements in der Anwendung (Application Vulnerable Item, AVI)..

Application Vulnerability Response konfigurieren

Bevor Sie Application Vulnerability Response in Ihrer Instanz Now Platform ausführen, müssen Sie es konfigurieren.

Application Vulnerability Response konfigurieren

Führen Sie vor der Konfiguration die folgenden Setup-Schritte aus, um sicherzustellen, dass Ihre Konfiguration abgeschlossen ist.

Vorbereitungen

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass Performance Analytics for Vulnerability Response installiert und aktiviert ist, um Application Vulnerability Response -Berichte anzuzeigen.	Um sicherzustellen, dass aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA]..
Vergewissern Sie sich, dass Veracode Vulnerability Integration installiert, aktiviert und konfiguriert ist. (Führen Sie die Integrationen zu diesem Zeitpunkt noch nicht aus.)	Um sicherzustellen, dass aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter ServiceNow Vulnerability Response Integration mit Veracodeinstallieren.
Version 14.0: Stellen Sie sicher, dass Fortify Vulnerability Integration installiert, aktiviert und konfiguriert ist. (Führen Sie die Integrationen zu diesem Zeitpunkt noch nicht aus.)	Um sicherzustellen, dass aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie unter ServiceNow Vulnerability Response Integration mit Fortifyinstallieren und Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integrationnach.
Stellen Sie sicher, dass die CWE 2000-Integration in Vulnerability Responseausgeführt wird.	Informationen zum Überprüfen der Integration finden Sie unter Stellen Sie sicher, dass die geplante Aufgabe zum Aktualisieren von NVD-Datensätzen ausgeführt wird.
[Optional] Stellen Sie sicher, dass die NVD-Integration in Vulnerability Responseausgeführt wird.	Informationen zur Überprüfung finden Sie unter Stellen Sie sicher, dass die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen ausgeführt wird.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen ist, installiert der Benutzer mit der Administratorrolle die Anwendung und weist Benutzer den folgenden Benutzergruppen zu: App-Sec-Manager,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Security Champion und Entwickler. Informationen zu Gruppenrollen finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen. • Die App-Sec-Managergruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. **Hinweis:** Die KonfigurationApplication Vulnerability Response ist nicht über die Funktion „Setup-Assistent“ in Vulnerability Responseverfügbar.

Erforderliche Rolle: Anwendergruppe „App-Sec-Manager“.

Prozedur

1. Navigieren zu **Security Operations** > **CMDB** > **Suchregeln**.
   Informationen zum Erstellen oder Ändern von CI-Suchregeln für Ihre Umgebung finden Sie unter Erstellen Sie eine CI-Suchregel.
2. Navigieren zu **Application Vulnerability Response** > **Administration**.
3. Wählen Sie **Zuweisungsregeln**aus.
   Informationen zum Erstellen oder Ändern von Anwendungszuweisungsregeln für Ihre Umgebung finden Sie unter Erstellen oder bearbeiten Sie Application Vulnerability Response -Zuweisungsregeln.
4. Wählen Sie **Schwachstellen-Rechner**.
   Informationen zum Erstellen oder Ändern von Anwendungsschwachstellen-Rechnern für Ihre Umgebung finden Sie unter Risiko in Application Vulnerability Response automatisch berechnen.
5. Wählen Sie **Korrekturzielregeln**aus.
   Informationen zum Erstellen oder Ändern von Anwendungskorrekturzielen für Ihre Umgebung finden Sie unter Erstellen oder bearbeiten Sie Zielregeln für die Anwendungskorrektur.
6. Wählen Sie **Normalisierte Schweregradzuordnungen**aus.
   Informationen zum Erstellen oder Ändern von Schweregradzuordnungen für Ihre Umgebung finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu.
7. Navigieren Sie zu entweder **Veracode Vulnerability Integration** > **Integrationen** oder **Fortify Vulnerability Integration** > **Integrationen**.
8. Öffnen Sie die Veracode-Anwendungslistenintegration oder die Fortify On Demand-Anwendungslistenintegration.
9. Wenn er noch nicht ausgeführt wurde, wählen Sie **Jetzt ausführen**.

   Hinweis:
   Die anderen Veracode - oder Fortify -Integrationen sind standardmäßig inaktiv.

   Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Status der Importausführung von Veracode Anwendungsschwachstellen-Integration an oder Zeigen Sie den Ausführungsstatus des Imports Fortify Vulnerability Integration an.
10. Nachdem die Ausführung der Veracode- oder Fortify-on-Demand-Anwendungslistenintegration abgeschlossen wurde, navigieren Sie zu **Application Vulnerability Response** > **Administration** > **Anwendungen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

11. Geben Sie für jede Anwendung einen Wert für **die Supportgruppe** (von Zuweisungsregeln verwendet) und für **die Abteilung** (für die Berichterstellung verwendet) ein.
Informationen zum Aktualisieren mehrerer Einträge finden Sie unter Mehrere Datensätze in einer Liste mit dem Listeneditor zur Massenausführung von Aufgaben bearbeiten.

Hinweis:
Aktualisieren Sie die Seite, um den automatisch aktualisierten **Geschäftsbereich**anzuzeigen.
Informationen zu Formularfeldern für gescannte Anwendungen finden Sie unter Gescannte Anwendungsfelder.

12. Kehren Sie zur Liste der Integrationen zurück, und aktivieren Sie die anderen Veracode - oder Fortify -Integrationen.
Informationen zum Festlegen Ihrer Delta-Datenintegrationsimporte finden Sie unter Aktivieren Sie Application Vulnerability Response Integrationen.

Die Integrationen Veracode und Fortify sind verkettet und werden nacheinander ausgeführt, wenn sie aktiviert sind.

13. **Wahlweise:** Navigieren zu **Application Vulnerability Response** > **Administration** > **Zuweisungsregeln**.

a. **Wahlweise:** Wenn Sie beim Erstellen oder Bearbeiten Ihrer Zuweisungsregeln zuvor **Konfigurationselement: Supportgruppe** für **das Feld Anwendergruppe** ausgewählt haben, können die Werte, die Sie der Listenansicht Gescannte Anwendungen hinzugefügt haben, jetzt verwendet werden.
Ihre Zuweisungsregeln werden bearbeitet.

b. Wählen Sie **Aktualisieren**.

c. Wählen Sie in der Listenansicht „Zuweisungsregeln für Schwachstellen“ **Changes anwenden**, um die Zuweisungsregeln erneut auf Ihre AVIs anzuwenden.

Ergebnisse
Die Konfiguration von Application Vulnerability Response ist jetzt abgeschlossen.

Nächste Maßnahme
Navigieren zu **Application Vulnerability Response** > **Übersicht** Informationen zu Ihrer allgemeinen Sicherheitslage finden Sie im Dashboard für Anwendungsschwachstellenmanagement [PA].

Stellen Sie sicher, dass die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen ausgeführt wird

Verwenden Sie die aus der CWE-Datenbank heruntergeladenen CWE-Datensätze (Common Weakness Enumeration) als Referenz, wenn Sie entscheiden, ob eine Schwachstelle eskaliert werden muss. Aktualisieren Sie allgemeine Schwachstellendatensätze regelmäßig aus der Common Weakness Enumeration-Datenbank. Sie können bei Bedarf auch das Standardskript aktualisieren oder eigene Skripts schreiben.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe
Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie die geplante Aufgabe **„CWE Comprehensive 2000 Integration“** aus.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.

   Hinweis:
   Die Einstellungen in diesem Formular werden von Vulnerability Response und Application Vulnerability Responsegemeinsam verwendet. Das Ändern der Integrationseinstellungen erfordert die Abstimmung mit und Fachwissen in Vulnerability Response und ServiceNow.

4. Wenn das Kontrollkästchen aktiviert ist, sind Sie fertig.

   Hinweis:
   Wenn das Kontrollkästchen nicht aktiviert ist, muss diese Integration möglicherweise in Vulnerability Responsekonfiguriert werden. Unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien finden Sie weitere Informationen, bevor Sie die Option auswählen.

Bei Bedarf rufen Sie Schwachstellenbibliotheken anzeigen auf, um die importierten Einträge anzuzeigen.

Das Feld **Primäre CWE** enthält den CWE-Eintrag. Wenn einer Schwachstelle mehrere CWEs zugeordnet sind, finden Sie unter Anwendungsschwachstellen-Felder Informationen zur Bestimmung der primären CWE.

Stellen Sie sicher, dass die geplante Aufgabe zum Aktualisieren von NVD-Datensätzen ausgeführt wird

Geben Sie die Repositorys an, die regelmäßig aktualisiert werden sollen. Sie können eine regelmäßige Aufgabe ausführen, um Datensätze aus der National Vulnerability Database (NVD) jede Nacht oder wöchentlich zu aktualisieren. Wenn er noch nicht ausgeführt wird, können Sie den Auftrag aktivieren

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Die NVD-Integration wird standardmäßig täglich montags um 00:00:00 Uhr als regelmäßige Aufgabe ausgeführt.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie die geplante Aufgabe **NIST National Vulnerability Database (National Vulnerability Database)** aus.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.

   Hinweis:
   Die Einstellungen in diesem Formular werden von Vulnerability Response und Application Vulnerability Responsegemeinsam verwendet. Das Ändern der Integrationseinstellungen erfordert die Abstimmung mit und Fachwissen in Vulnerability Response und ServiceNow.

4. Wenn das Kontrollkästchen aktiviert ist, sind Sie fertig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn das Kontrollkästchen nicht aktiviert ist, muss diese Integration möglicherweise in Vulnerability Responsekonfiguriert werden. Unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien finden Sie weitere Informationen, bevor Sie die Option auswählen.

Bei Bedarf rufen Sie Schwachstellenbibliotheken anzeigen auf, um die importierten Einträge anzuzeigen.

Aktivieren Sie Application Vulnerability Response Integrationen

Aktivieren Sie Application Vulnerability Response Integrationen, um regelmäßige Updates durchzuführen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Aktivieren Sie die Checkbox **Aktiv**.
4. Wählen Sie **Aktualisieren**.
5. Wiederholen Sie dies bei Bedarf für jede Integration.
   Nach der ersten Ausführung werden die Integrationen verkettet, um Delta-Importe für nachfolgende Ausführungen durchzuführen.

Definieren Sie E-Mail-Benachrichtigungen Application Vulnerability Response .

Richten Sie E-Mail-Benachrichtigungen ein, um nützliche Informationen über wichtige Updates und Aktivitäten wie die Genehmigung und Ablehnung von falsch positiven Anforderungen zu teilen. Beim Erstellen einer E-Mail-Benachrichtigung müssen Sie angeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **E-Mail-Vorlagen**.
2. Wählen Sie **Neu**.

Ausführliche Anweisungen zum Erstellen von E-Mail-Benachrichtigungen finden Sie unter Create an email notification .

Ergebnisse
Ab v21.0 von Vulnerability Responsewerden Empfänger, die auf die Links in einer E-Mail-Benachrichtigung klicken, je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

- Im Vulnerability Manager Workspace werden Links für Benutzer mit der Rolle sn_vul.app_sec_managergeöffnet.
- Links werden in IT Remediation Workspace für Benutzer mit den Rollen sn_vul.app_security_Champion, oder sn_vul.app_developer geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Empfänger über keine der genannten Rollen verfügt, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Erstellen oder bearbeiten Sie Benachrichtigungen für Korrekturziele in Application Vulnerability Response

Schwachstellenadministratoren können die Korrekturzielbenachrichtigung bearbeiten oder neue hinzufügen und angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**.
2. Wählen Sie den Benachrichtigungsdatensatz des Korrekturziels oder **Neu**aus.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie **Benachrichtigungsvorschau** aus, um die Nachricht anzuzeigen.

Ergebnisse
Ab v21.0 von Vulnerability Responsewerden Empfänger, die auf die Links in einer E-Mail-Benachrichtigung klicken, je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

- Im Vulnerability Manager Workspace werden Links für Benutzer mit der Rolle sn_vul.app_sec_managergeöffnet.
- Links werden in IT Remediation Workspace für Benutzer mit den Rollen sn_vul.app_security_Champion, oder sn_vul.app_developer geöffnet.

Wenn der Empfänger über keine der genannten Rollen verfügt, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Ausnahmeverwaltung in Application Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Richtlinie, einen Standard oder eine Leitlinie für das Schwachstellenmanagement oder die Sicherheit nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Element in einer Anwendung (Application Vulnerable Item, AVIT), das nicht gemäß der Richtlinie behoben werden kann.

Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen anerkennen und ihnen zustimmen, wenn die Schwachstelle nicht behoben wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Ab v21.0 von Application Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Anwendungselement in den Status „Wird überprüft“, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element der Anwendung oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Lebenszyklus einer Ausnahme

Definition einer Ausnahme

Eine Ausnahme ist eine Anforderung, die Korrektur einer AVI für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Ausnahme wird angefordert

Als Entwickler können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für eine AVI beantragen. Nachdem der Anwendungssicherheitsanalyst diese Anforderung genehmigt hat, wechselt die AVI in den Status **„Zurückgestellt** “.

Wichtig:
Sie können Ausnahmen für AVTIs und RTs im Arbeitsbereich des Schwachstellenmanagers und im Arbeitsbereich für IT-Fehlerkorrekturen anfordern. Weitere Informationen finden Sie unter Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace und Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Ausnahmeregeln

Ab v20 können Sie Ausnahmeregeln erstellen, um vorhandene und neue angreifbare Elemente in einer Anwendung (Application Vulnerable Items, AVI) automatisch für einen bestimmten Zeitraum zurückzustellen, wenn sie den Bedingungen der Regel entsprechen. Die Verwendung von Ausnahmeregeln zum automatischen Zurückstellen von AVIs minimiert das Risiko des Fehlens von Servicelevel-Vereinbarungen. Mit den Regeln können Sie mehrere Elemente verwalten, da Sie manuelle Eingriffe vermeiden. Weitere Informationen finden Sie unter Ausnahmeregel erstellen.

Verlängerung für eine Ausnahmeregel anfordern

Ab v20 können Sie eine Verlängerung des **Datums „Zurückgestellt bis** “ einer Ausnahmeregel anfordern. Sie können eine Erweiterung einer Regel anfordern, wenn Sie feststellen, dass eine große Anzahl von von der Regel erstellten Datensätzen nicht bis zum Datum „ **Zurückgestellt bis** “ aufgelöst wird. Dies ist das Datum, an dem die Korrekturaufgabe keine neuen AVIs mehr akzeptiert. Die Erweiterung aktualisiert die Ausnahmeregel, sodass das Zurückstellungsdatum der vorhandenen Regel automatisch verlängert wird. Sie können Daten bis zu einem Jahr ab dem aktuellen Datum eingeben und müssen einen Grund für die Verlängerung angeben. Eine Erweiterungsanforderung erfordert eine Genehmigung auf zwei Ebenen durch separate Genehmigungsgruppen.

Eine Ausnahmeanforderung wird genehmigt

AVITs, die nicht sofort korrigiert werden können, werden von Anwendungssicherheitsanalysten überprüft, auf Risiken bewertet und zur Zurückstellung genehmigt, bis sie korrigiert werden können. Das Genehmigen einer Ausnahmeanforderung kann ein zweistufiger Flow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger für hinzu Application Vulnerability Response.

Wichtig:
Im Arbeitsbereich des Schwachstellenmanagers können Sie Ausnahmeanforderungen genehmigen oder ablehnen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Hinweis:

Nachdem eine Ausnahmeanforderung für eine AVIT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Rufen Sie weitere Details ab

Verfolgen Sie eine Ausnahmeanforderung

Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status mithilfe der Registerkarte **Change-Genehmigungen** im AVIT nachverfolgen.

Ablauf einer Ausnahmeanforderung und Anforderung einer Verlängerung einer Ausnahmeregel

Wenn eine Ausnahmeanforderung für ein bestimmtes AVI abläuft, wird das betroffene AVI in seinen Status **„Offen“** zurückversetzt.

Ab v20 können Sie jedoch eine Anforderung zum Verlängern des Datums „Zurückgestellt **bis** “ für die Ausnahmeregel senden.

Konfigurieren Sie die Ausnahmeverwaltung für Application Vulnerability Response

Begrenzen Sie die Dauer einer angeforderten Ausnahme , und fügen Sie der Ausnahme oder falsch positiven Anforderung mithilfe des Moduls einen Fragebogen hinzu . Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Application Vulnerability Response angefordert. Sie können auch mit der -Integration GRC: Richtlinien- und Compliance-Management eine Ausnahme anfordern.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_manage_exception_configuration

Warum und wann dieser Vorgang ausgeführt wird

Wenn Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Richtlinien- und Compliance-Management installiert ist, GRC: Richtlinien- und Compliance-Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder die falsch positive Anforderung ausgelöst hat. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für das Anfordern der Ausnahme zu verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular „Ausnahmeverwaltungskonfiguration“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option in der Liste Ausnahmen verwalten mit auswählen.

   Hinweis:
   Ab Vulnerability Response Version 17.1 können Sie entweder Vulnerability Response oder GRC: Richtlinien- und Compliance-Managementauswählen. Sie müssen das Plugin GRC aktivieren, um mit GRC: Richtlinien- und Compliance-Management eine Ausnahme anzufordern. Das Ändern der Konfiguration hat keine Auswirkungen auf die vorhandenen Daten.

3. Füllen Sie die Felder im Formular basierend auf der von Ihnen ausgewählten Option aus.
   - Wenn Sie die Option Vulnerability Response ausgewählt haben, füllen Sie die Felder im Formular aus.

     Einstellungen für das Formular „VR-Ausnahmeverwaltung“.

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens zum Anfordern einer Ausnahme. Der Ausnahmefragebogen wird standardmäßig angezeigt.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung.
Fragebogen, um falsch positive Meldung zu markieren	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens als Falsch positiv markieren. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt.

   - Wenn Sie die Option GRC: Richtlinien- und Compliance-Management ausgewählt haben, füllen Sie die Felder im Formular aus.

     Einstellungen für das Formular „VR-Ausnahmeverwaltung“.

Feld	Beschreibung
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Fragebogen, um falsch positive Meldung zu markieren	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens zum Markieren als falsch positiv. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt.

4. Wählen Sie **Speichern**.

Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung

Verwenden Sie ab Application Vulnerability Response v15.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung, Ausnahmeregeln und die Verwaltung falsch positiver Ergebnisse zu genehmigen. Wenn Sie Application Vulnerability Response (AVR) zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie bereits VR-Benutzer sind, lautet die Standardoption Workflow.
Wenn Sie Application Vulnerability Response v15.0 oder höher bereitgestellt haben, ist der Wert der Systemeigenschaft *sn_vul.flow_designer_activation* auf „true“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie Application Vulnerability Response bereits vor v15.0 verwenden, ist der Wert dieser Systemeigenschaft auf „false“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in true ändern.

Hinweis:
Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Anwendungselemente
- Ausnahmeregel
- Falsch positiv für Korrekturaufgaben
- Falsch positiv für angreifbare Anwendungselemente

Hinweis:
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.
Anwendung	Der Standardwert ist Vulnerability Response.
Regeltyp	Gibt den Regeltyp an. Beispiele: Ausnahmeverwaltung, falsch positive Meldung oder Ausnahmeregel.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurze Beschreibung der Genehmigungsregeln.
Genehmigungsablaufy (Tage) Ab v21.0 von Application Vulnerability Response	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.
Genehmiger benachrichtigen (Tage) Ab v21.0 von Application Vulnerability Response	Datum, nach dem der Genehmiger benachrichtigt wird, um Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren.

Hinweis:
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die für verschiedene Konfigurationselemente gefunden wurden.

Korrektur wird zurückgestellt in Application Vulnerability Response

Ab v20.0 können Sie die Nachbesserung mit dem Status **„Warten auf Implementierung“** zurückstellen, der für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVI) und Korrekturaufgaben verfügbar ist, während sie sich durch ihren Lebenszyklus bewegen. Sie können Datensätze nur manuell in diesen Status überführen, indem Sie **„Warten auf Implementierung“** von AVI und Korrekturaufgaben-Datensätze im Status **„Wird untersucht“** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfall

Als Korrekturspezialist können Sie einen Datensatz in den Status „ **Warten auf Implementierung“** verschieben, um Ihr Team darüber zu informieren, dass Ihre Suche und die Arbeit an einer Aufgabe abgeschlossen sind. Sie können dieses Update auswählen, wenn Sie feststellen, dass ein Fix für die Implementierung bereit ist, aber noch nicht verfügbar ist. Ein Beispiel für eine nicht verfügbare Korrektur ist ein Software-Patch. Wenn das Wartungsfenster für einen Patch nach Abschluss Ihrer Recherche nicht verfügbar ist, können Sie die Aufgabe in **Warten auf Implementierung** verschieben, bis der Patch bereitgestellt werden kann.

Pflichtfelder

Es gibt zwei erforderliche, bearbeitbare Felder in den AVI- und Korrekturaufgaben-Datensätzen, die sich im Status „Warten auf Implementierung“ befinden:

Datum der Korrekturzusage

Geplantes Datum der Remediation.

Korrekturplan

Beschreibung des Korrekturplans für die Korrektur. Dieser Text wird in den Hinweisen im Datensatz angezeigt.

Felder und Systemeigenschaften

Es gibt zwei Systemeigenschaften, die für das Modal, das angezeigt wird, wenn Sie einen Datensatz in den **Status Warte auf Implementierung** überführen, standardmäßig auf `true`festgelegt sind. Wenn sie in ihren Standardeinstellungen belassen werden:

sn_vul.remediation_fields

Legt **das Datum der Korrekturzusage** und **den Korrekturplan** als Pflichtfelder fest. Bei Festlegung auf `false`sind diese Felder optional.

sn_vul.awaiting_implementation

Zeigt das Modal mit den Feldern **Korrekturzusagedatum**und **Korrekturplan** an, nachdem Sie **Warten auf Implementierung** für einen Datensatz ausgewählt haben. Wenn dies auf `false`eingestellt ist, können Sie den Status eines AVI in Warten auf Implementierung ändern, ohne dass Sie zur Eingabe eines Zusagendatums oder eines Plans aufgefordert werden.

Modul für nicht eingehaltenes Datum der Korrekturzusage

Zeigen Sie alle AVIs an, deren Datumsangaben für die Korrekturzusage im Modul **Fehlendes Datum der Korrekturzusage** versäumt wurden. Navigieren **Application Vulnerability Response** > **Angreifbare Elemente** > **Datum der Korrekturzusage vergangen** , um die Liste anzuzeigen.

Status-Rolldown von Korrekturaufgaben zu AVIs

Die UI-Aktionsschaltfläche zum Überführen eines Datensatzes in **„Warten auf Implementierung“** ist nur für Datensätze für angreifbare Anwendungselemente und Korrekturaufgaben im Status **„Wird untersucht“** sichtbar. Für den Status-Rolldown gibt es im Modal, das angezeigt wird, wenn Sie **Warten auf Implementierung** für eine Korrekturaufgabe auswählen, die Option **Vorhandene AVIs überschreiben**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Wählen Sie **Vorhandene AVIs überschreiben**aus.	Wählen Sie diese Option aus, um die Daten der Korrekturzusage und die Korrekturpläne für alle vorhandenen AVIs in der Aufgabe zu überschreiben, die sich bereits im Status „ **Warten auf Implementierung** “ befinden. Wenn diese Option ausgewählt ist, führt diese Funktion ein Rolldown für Datum und Plandaten der Korrekturaufgabe zu den AVIs durch.
„Vorhandene AVIs überschreiben“ deaktiviert lassen.	Lassen Sie die Option deaktiviert, um die Datums- und Planwerte für alle vorhandenen AVIs für die Aufgabe beizubehalten, die sich bereits im Status „ **Warten auf Implementierung“** befinden. Wenn diese Option deaktiviert ist, behalten AVIs, die sich bereits im **Status „Warten auf Implementierung“ befinden**, ihre vorhandenen Datums- und Plandaten und sind nicht vom Status-Rolldown betroffen.

Rolldown-Beispiele

Angenommen, Sie möchten eine Korrekturaufgabe von „ **Offen** “ in **„Warten auf Implementierung“** überführen, um das Datum der Zusage und die Planinformationen der Aufgabe für ein Software-Patch-Wartungsfenster zu aktualisieren. Angenommen, in dieser Aufgabe befindet sich ein AVI im Status „ **Warten auf Implementierung“**, dessen Zusagedatum und Planinformationen Sie entsprechend der Korrekturaufgabe aktualisieren möchten.

Um das Datum und die Plandaten des AVIs zu überschreiben, damit sie mit der Korrekturaufgabe übereinstimmen, aktivieren Sie das Kontrollkästchen **Vorhandene AVIs überschreiben,** wenn Sie dazu aufgefordert werden. Die Datums- und Planwerte des AVI werden zu den Plan- und Datumswerten, die Sie für die Aufgabe in der Eingabeaufforderung eingeben, wenn Sie **Warten auf Implementierung**auswählen.

Wenn Sie in diesem Fall die Überschreibungsoption nicht auswählen und in **Warten auf Implementierung**ein AVI vorhanden ist, bleiben die ursprünglichen Datums- und Plandaten im AVI erhalten. Die Plan- und Datumswerte, die Sie für die Aufgabe in der Eingabeaufforderung eingeben, wenn Sie **Warten auf Implementierung** auswählen, werden nicht für AVIs verwendet, die sich bereits im Status **Warten auf Implementierung** in der Aufgabe befinden.

Wenn sich ein AVI für eine Aufgabe im Status **„Gelöst“** oder **„Geschlossen-behoben“** befindet und Sie die Aufgabe in **„Warten auf Implementierung“**überführen, werden die AVIs durch Auswahl von **Vorhandene AVIs überschreiben** aufgrund eines höheren Statusrangs nicht von **Geschlossen-behoben** und **Gelöst** in **Warten auf Implementierung** geändert.

Wenn beim Verschieben der Aufgabe nach **„Warten auf Implementierung“** nicht „Überschreiben“ ausgewählt ist und bereits ein AVI im **Status „Warten auf Implementierung**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

“ vorhanden ist und Sie die Aufgabe zurück in den Status **„Offen“** oder **„Wird untersucht“**verschieben, verbleibt das AVI im **Status „Warten auf Implementierung“**.

Fügen Sie einen Ausnahmegenehmiger für hinzu Application Vulnerability Response

Fügen Sie den Genehmigergruppen Benutzer hinzu, um eine Ausnahme anzufordern.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_exception_approver

Warum und wann dieser Vorgang ausgeführt wird

Eine Ausnahmeanforderung für ein angreifbares Anwendungselement wird mit dem standardmäßigen zweistufigen Genehmigungs-Flow genehmigt. Die Anforderung kann von zwei Genehmigerebenen genehmigt werden. Das Hinzufügen von Anwendern zur Gruppe der ersten Ebene ist obligatorisch. Wenn es keine Benutzer auf der zweiten Ebene gibt, wird die Anforderung nach der Genehmigung auf der ersten Ebene genehmigt.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**.
2. Suchen Sie in der Spalte „Name“ nach **Ausnahme**, und klicken Sie auf **Anwendungsausnahmegenehmiger – Ebene 1**.

   Hinweis:
   Ab Application Vulnerability Response v12.8.1 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme- oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie `sn_vul.app_exception_approver_L1`, `sn_vul.app_exception_approver_L2`oder `sn_vul.app_false_positive_approver_group`, um den Eigenschaftswert zu ändern.
3. Klicken Sie im Formular „Gruppenanwendungsausnahmegenehmiger – Ebene 1“ auf die zugehörige Liste Gruppenmitglieder.
4. Klicken Sie zum Erstellen einer Liste **auf Neu**.
5. Füllen Sie die Felder des Formulars aus.

Anwenderformular

Feld	Beschreibung
Anwender-ID	Eindeutiger Bezeichner für den Benutzer
Vorname	Vorname des Anwenders.
Nachname	Nachname des Anwenders.
Titel	Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus.
Abteilung	Abteilung des Anwenders.
Passwort	Dem Anwender zugewiesenes Passwort. Dieses Passwort kann dauerhaft oder vorübergehend sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Passwort muss zurückgesetzt werden	Option, mit der der Anwender das Passwort zurücksetzen kann, um die Sicherheit zu gewährleisten.
Gesperrt	Option, den Anwender für die Instanz zu sperren und alle aktiven Sitzungen des Anwenders zu beenden. Das System verhindert, dass Benutzer mit der Rolle admin sich selbst sperren.
Aktiv	Option zum Aktivieren dieses Anwenders. Nur Sie können inaktive Anwender in den folgenden Bereichen sehen: ○ Listen von Benutzern ○ Auswahlliste für Referenzfelder (Lupensymbol) ○ AutoVervollständigen Sie die Liste, die angezeigt wird, wenn Sie etwas in ein Referenzfeld eingeben
Nur Webservice-Zugang	Option, um diesen Anwender als nicht interaktiven Anwender festzulegen.
Interner Integrationsanwender	Option, um diesen Anwender als internen Integrationsanwender festzulegen.
E-Mail	E-Mail-Adresse des Anwenders.
Sprache	Bevorzugte Sprache des Anwenders.
Kalenderintegration	Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook.
Zeitzone	Zeitzone für den Standort dieses Anwenders.
Datumsformat	Bevorzugtes Format des Anwenders für Datumsangaben.
Telefon (geschäftlich)	Geschäftstelefon des Benutzers.
Mobiltelefon	Mobiltelefon des Benutzers.
Foto	Foto, das Sie hochladen können, indem Sie auf **„Zum Hinzufügen klicken...“ klicken**.

6. Klicken Sie auf **Absenden**.
7. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 5, um einen Anwendungsausnahmegenehmiger der Ebene 2 zu erstellen.
   Der Genehmiger muss zu **Application Vulnerability Response** > **Meine Genehmigungen** navigieren und Anforderungen genehmigen.

Anfordern und Genehmigen einer Ausnahme in Application Vulnerability Response

Sie können anfordern, die Korrektur eines angreifbaren Anwendungselements und einer Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen.

Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist. Genehmiger mit Zugriffsrechten können Anforderungen anderer Benutzer genehmigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können auch Ausnahmeregeln erstellen und eine Ausnahmeerweiterung für eine Ausnahmeregel anfordern. Standardmäßig sind für Zurückstellungen, Ausnahmeregeln und Anforderungen zur Ausnahmeerweiterung zwei Genehmigungsebenen erforderlich.

Informationen zum Anfordern oder Genehmigen einer Ausnahme finden Sie unter:

- Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an
- Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Richtlinien- und Compliance-Management
- Genehmigen Sie Ausnahmeregeln und Anforderungen zur Erweiterung von Ausnahmeregeln in Application Vulnerability Response
- Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Application Vulnerability Response

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail mit dem Hinweis, dass eine Ausnahme angefordert wurde.

Ab v21.0 von Application Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Anwendungselement in den Status „Wird überprüft“, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element der Anwendung oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an

Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Wichtig:
Sie können im Vulnerability Manager Workspace und im IT Remediation Workspace Ausnahmen für ein angreifbares Anwendungselement und eine Korrekturaufgabe anfordern. Weitere Informationen finden Sie unter Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace und Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Vorbereitungen
Erforderliche Rolle: Developer Group

Prozedur

1. Navigieren zu **Application Vulnerability Response** > **Angreifbare Anwendungselemente** > **Alle** und wählen Sie das Element aus, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“ oder „Wird untersucht“ befinden.

   Hinweis:

   Ab v21.0 von Application Vulnerability Responsewird der vorherige Status eines angreifbaren Anwendungselements im Feld **„backup_state“** gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Klicken Sie im Formular „Angreifbares Anwendungselement“ **auf Ausnahme anfordern**.

Hinweis:
Je nachdem, ob Vulnerability Response oder GRC: Richtlinien- und Compliance-Management in ausgewählt ist **Application Vulnerability Response** > **Ausnahmenverwaltung** Im Bildschirm „Ausnahme anfordern“ ändert sich das Formular „Ausnahme anfordern“. Wenn GRC: Richtlinien- und Compliance-Management, siehe Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Richtlinien- und Compliance-Management

3. Wenn Vulnerability Response im Bildschirm „Ausnahmeverwaltung“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in ausgewählten Dauer liegen **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status „ **Offen“** zurück. **Hinweis:** Ab Version 18.0 von Application Vulnerability Response (AVR) kann ein zurückgestelltes angreifbares Anwendungselement von einem Scanner geschlossen und erneut geöffnet werden. Wenn das Element vor Ablauf des Ausnahmefensters erneut geöffnet wird, wird der Status der AVIT unter Berücksichtigung des aktiven Ausnahmefensters in den Status „Zurückgestellt“ zurückversetzt. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft sn_vul.auto_defer_avit_in_active_exception_window auf „wahr“ fest. Außerdem bleibt das zurückgestellte Bis-Datum auch dann erhalten, wenn die AVIT geschlossen wird oder die Ausnahme abgelaufen ist. Die erforderliche Rolle für Lese- und Schreibvorgänge lautet „sn_vul.app_manage_exception_configuration“.
Grund	Wählen Sie den **Grund**aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Informationen zum Hinzufügen neuer Gründe finden Sie unter Definieren Sie die Zuordnung von Richtliniengrund.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Besitzer der Korrektur aktualisiert werden.

4. Klicken Sie auf **Genehmigung anfordern**, um die Ausnahmeanforderung zu senden.
   Der Status der Anwendungsschwachstelle ändert sich in Wird überprüft. Verwenden Sie die Registerkarte **Change-Genehmigung**, um den Status der Ausnahmeanforderung zu verfolgen.

Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Richtlinien- und Compliance-Management

Fordern Sie mit der Funktion zur Verwaltung von Richtlinienausnahmen GRC in der Anwendung Richtlinien- und Compliance-Management innerhalb von Application Vulnerability ResponseRichtlinienausnahmen an.

Vorbereitungen

Bevor Sie die Integration für Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Richtlinien- und Compliance-Management von ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vul.remediation_Besitzer

Sie können Ausnahmen auch in der klassischen Anwenderoberfläche anfordern:

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Anwendungselemente** (oder **Korrekturaufgaben**) >**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular **auf Ausnahme anfordern**.
3. Wenn GRC: Richtlinien- und Compliance-Management im Bildschirm „Ausnahmeverwaltung“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Richtlinie	Richtlinie für Schwachstellenmanagement, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme startet. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von Zurückgestellt in Offen wechselt. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage),** die Sie für die Richtlinie in Richtlinien und Compliance festgelegt haben, nicht überschreiten. Weitere Informationen finden Sie unter Richtlinie erstellen .
Grund	Grund für das Anfordern einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Besitzer der Remediation ausgefüllt werden.

a. Klicken Sie auf **Genehmigung anfordern**, um die Ausnahmeanforderung zu senden.
Der Status der angreifbaren Elemente ändert sich in Wird überprüft, und es wird eine Richtlinienausnahme erstellt. Verwenden Sie die Registerkarte **Change-Genehmigung**, um den Status der Ausnahmeanforderung zu verfolgen.

b. Klicken Sie auf die zugehörige Liste Richtlinienausnahmen, um die Richtlinienausnahme anzuzeigen.

c. Klicken Sie auf die Nummer der Richtlinienausnahme.

d. Wählen Sie im Feld **Genehmiger** den Namen des Genehmigers aus.

e. Klicken Sie auf die Registerkarte Quelle, und wählen Sie im Feld **Kontrollziel** ein Kontrollziel aus.

f. Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie die Risikobewertung im Feld **Risikobewertung** aus.

g. Speichern Sie das Formular.

h. Klicken Sie auf die Registerkarte Betroffene Steuerungen und dann auf Hinzufügen, um Steuerungen hinzuzufügen.

i. Speichern Sie das Formular.

Hinweis:
Sie können eine Compliance-Überprüfung veranlassen, indem Sie **auf Compliance-Überprüfung anfordern**klicken.

j. Das Genehmigungsformular wird an den Genehmiger gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

k. Als Genehmiger können Sie entweder die Anforderung genehmigen, indem Sie auf **Genehmigen** klicken, oder eine zusätzliche Genehmigung anfordern, indem Sie **auf Zusätzliche Genehmigung anfordern**klicken.
Der Datensatzstatus ändert sich in Zurückgestellt. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die Registerkarte Zurückstellung enthält zusätzliche Hinweise zum Datensatz.

Hinweis:
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

4. Klicken Sie auf **Absenden**.
Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Korrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Ausnahme für eine Anwendungskorrekturaufgabe anfordern

Fordern Sie eine Ausnahme an, um eine Anwendungskorrekturaufgabe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort gelöst werden kann.

Vorbereitungen

Sie können Ausnahmen in den Arbeitsbereichen Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_Champion oder sn_vul_container.remediation_owner.

Sie können auch Ausnahmen für Anwendungskorrekturaufgaben in der klassischen Umgebung anfordern.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Alle**.

2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
Die ausgewählte Aufgabe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.

3. Wählen Sie im Datensatz der Anwendungskorrekturaufgabe **Ausnahme anfordern**.

4. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in der Konfiguration definierten Ausnahmedauer liegen.
Grund	Begründung für das Anfordern einer Ausnahme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Korrektur aktualisiert werden.

5. Klicken Sie auf **Genehmigungs-Engine**.

Genehmigen Sie Ausnahmeregeln und Anforderungen zur Erweiterung von Ausnahmeregeln in Application Vulnerability Response

Genehmigen Sie Ausnahmeanforderungen für angreifbare Anwendungselemente, die nicht sofort behoben werden können. Sie müssen diese Anforderungen auf Risiken bewerten und dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_exception_approver

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Definieren Sie die Zuordnung von Richtliniengrund

Sie können die Grundauswahlmöglichkeiten so definieren, dass sie für jeden Anwender verfügbar sind, der eine Ausnahme anfordert.

Vorbereitungen

Die Anwendung GRC: Richtlinien- und Compliance-Management muss installiert sein. Diese Anwendung ist im ServiceNow® Store mit einem separaten Abonnement verfügbar.

Weitere Informationen zu Systemanforderungen und Familienkompatibilität finden Sie in der Anwendungsliste auf der Website des ServiceNow Store .

Erforderliche Rolle: sn_vul.compliance.manager und sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**.

   Hinweis:
   Sie können entweder einen Grund aus den in der Tabelle „Grundauswahlmöglichkeiten“ verfügbaren Gründen auswählen oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Integrationsregistrierung für Ihre Anwendung, z. B. **Application Vulnerability Response**, **Vulnerability Response**usw.
3. Um eine vorhandene Grundauswahl hinzuzufügen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie in der Liste „Grund – Auswahlmöglichkeiten“ auf **Neu**.
   b. Klicken Sie auf das Lupensymbol, um einen Grund auszuwählen.
4. Um der Tabelle „Grundauswahlmöglichkeiten“ neue Gründe hinzuzufügen, gehen Sie wie folgt vor:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Liste „Grund – Auswahlmöglichkeiten“ auf **Neu**.

b. Klicken Sie auf das Lupensymbol.

c. Klicken Sie auf **Neu**.

d. Füllen Sie die Felder des Formulars aus.

Formular „Grund – Auswahlliste“.

Feld	Beschreibung
Bezeichnung	Eindeutige Bezeichnung für diese Auswahl.
Wert	Eindeutiger Wert für diese Auswahl. Dieser Wert wird in der Tabelle „Zuordnungen der Richtlinienausnahmegründe“ für die jeweiligen Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie im Filternavigator sn_vul_policy_reason_mapping.LIST ein.
Bestellung	Reihenfolge für diese Auswahl. Die Gründe werden basierend auf dieser Nummer sortiert.
Standard	Option, um anzugeben, dass diese Grundauswahl verfügbar ist, wenn eine bedarfsgesteuerte Richtlinienausnahme angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, sind alle Grundauswahlmöglichkeiten verfügbar, bei denen das Feld **„Standard“** ausgewählt ist.
Aktiv	Option zum Anzeigen der Auswahl in der Liste der Grundauswahlmöglichkeiten.

5. Klicken Sie auf **Absenden**.

Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Application Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht ist. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: App-Sec Manager sn_vul.app_sec_manager, Security Champion sn_vul.app_security_Champion.

Warum und wann dieser Vorgang ausgeführt wird

In einem Erweiterungsregel-Datensatz können Sie nur dann eine Verlängerung für das Datum **„Zurückgestellt bis** “ anfordern, wenn sich die Regel im Status **„Genehmigt“** befindet. Sie können diese Erweiterung einer Regel anfordern, wenn Sie feststellen, dass eine große Anzahl von von der Regel erstellten Datensätzen nicht **bis zum Datum „Zurückgestellt bis** “ aufgelöst wird. Dies ist das Datum, an dem die Korrekturaufgabe keine neuen AVIs mehr akzeptiert. Die Erweiterung aktualisiert die Ausnahmeregel, sodass das Zurückstellungsdatum der vorhandenen Regel automatisch verlängert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Ausnahmeregeln**.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein. Zur Auswahl stehen: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und Zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Korrekturaufgaben und angreifbaren Anwendungselemente aktualisiert. Außerdem wird bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers eine E-Mail ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Ausnahmeregel erneut verlängert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe in an Application Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor das Datum für „Zurückgestellt bis“ erreicht wird. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur
1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status „Zurückstellen“ abläuft und die Korrekturaufgabe erneut aktiviert wird.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Nach der Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Anwendungselemente übertragen, die Teil der Korrekturaufgabe sind. Die angreifbaren Anwendungselemente müssen sich jedoch im Status „Zurückgestellt“ befinden, und ihre aktuellen Bis-Daten müssen vor dem „Aktualisiert bis“-Datum liegen. Außerdem wird bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers eine E-Mail ausgelöst.

Hinweis:
- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Korrekturaufgabe erneut verlängert wird, erhöht sich die Anzahl der Zurückstellungen verlängern im Back-End.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Anwendungselement in an Application Vulnerability Response

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Anwendungselement an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht wird. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**.
2. Öffnen Sie ein zurückgestelltes angreifbares Anwendungselement.
3. Wählen Sie **Verlängerung anfordern**aus.

   Hinweis:
   Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Anwendungselements Zurückgestellt ist.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten angreifbaren Anwendungselements verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Wenn eine zurückgestellte Ausnahmeregel erneut verlängert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden die Hinweise Bis, Grund und Zurückstellung aktualisiert.

Erstellen, löschen und stornieren Sie eine Ausnahmeregel für Application Vulnerability Response

Erstellen Sie eine Regel, um automatisch eine Ausnahme für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVI) anzufordern, die bestimmte Bedingungen erfüllen.

Vorbereitungen

Sie können beispielsweise eine Regel mit einer Bedingung erstellen, die auf einer bestimmten bekannten oder kritischen Schwachstelle basiert, von der Sie wissen, dass Sie sie nicht sofort beheben können. Mit dieser Regel können Sie neue und vorhandene AVIs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

- Die Ausnahmeregel wird ab dem Datum **Gültig von** bis **Gültig bis** angewendet, das Sie im Regeldatensatz eingeben.
- Die Korrekturaufgabe (AVUL) wird erstellt, nachdem die Regel für **übereinstimmende** AVIs im Status Zurückgestellt genehmigt wurde.
- Die Gruppierungsmethode für diese AVUL wird als Ausnahmeregel bezeichnet.
- Sie können diese AVUL nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete AVIs werden zurückgestellt und dieser AVUL ab dem Datum **„Gültig von** “ hinzugefügt, bis die Gruppe am Datum „ **Gültig bis** “ abläuft.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmeregel-Workflows gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung übermittelt wurde.

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung einreichen.

Erforderliche Rolle: App SEC Manager sn_vul.app_sec_manager und Security Champion sn_vul.app_security_Champion.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Wählen Sie auf der neuen Datensatzseite „Ausnahmeregel“ **Neu**.
3. Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Ausnahmeregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Schreibgeschützt: Entwurf
Gültig ab	Datum, ab dem diese Regel aktiv ist, um AVIs zurückzustellen.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel. Ein niedrigerer Wert hat Vorrang vor einem höheren.
Gültig bis	Datum, an dem die Korrekturaufgabe die Annahme neuer AVIs beendet.
Zurückgestellt bis	Datum, bis zu dem die Korrekturaufgaben und AVIs zurückgestellt werden. An diesem Datum werden die AVULs geschlossen, und alle AVIs werden aus den Aufgaben entfernt und erneut geöffnet. Gruppenregeln werden erneut auf diese AVIs angewendet.
Grund	Grund für die Erstellung dieser Ausnahmeregel.
Zuweisungsgruppe	Gruppe, der die Korrekturaufgabe zur Nachverfolgung der zurückgestellten AVIs zugewiesen ist.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen.
Bedingung	Filterbedingungen, um anzugeben, welche AVIs mit dieser Regel übereinstimmen.
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für bereits vorhandene Daten ausführen können. Wenn Sie diese Option deaktiviert lassen, wird Ihre Regel täglich von der geplanten Aufgabe *Associate existing AVIs with Auto Exception Rule* ausgeführt, beginnend mit neuen Daten. Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wird am **Gültig ab-** Datum einmalig eine geplante Aufgabe für die vorhandenen Daten ausgeführt.

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Wählen Sie eine aus.

Nachdem die Regel genehmigt wurde, wechselt sie in den Status **Genehmigt**. Ihre Regel wertet AVIs mit dem Auftrag *Associate existing AVIs with Auto Exception Rule scheduled* aus. Wenn Sie **Für vorhandene Daten ausführen**ausgewählt haben, werden vorhandene AVIs ausgewertet. Für die Regel wird automatisch eine Korrekturaufgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellt, und alle übereinstimmenden AVIs, die die Bedingungen erfüllen, werden der Aufgabe zugeordnet.

Die geplante Aufgabe führt die Ausnahmeregel einmal für vorhandene Daten aus. Die Regel wird für vorhandene Daten nicht erneut ausgeführt, auch wenn keine AVIs gefunden werden. Es werden nur neue Daten ausgewertet, da die vorhandenen AVIs, die der Regel entsprechen, bereits zurückgestellt wurden.

6. Um eine Regel zu löschen, wählen Sie im Datensatz der Ausnahmeregel **die Option Löschen aus**. Die folgende Meldung wird angezeigt: Wenn Sie die Regel löschen, wird die zugehörige Korrekturaufgabe gelöscht, und die zugehörigen angreifbaren Elemente werden erneut geöffnet. Die Regeln für Korrekturaufgaben werden dann auf die einzelnen AVIs angewendet, und die Ausnahmeregel wird gelöscht.
7. Wählen Sie**Regel beibehalten**, um anzuhalten oder **Regel löschen,** um fortzufahren.
8. Um eine Regel zu deaktivieren, sie aber in der Liste der Ausnahmeregeln zu belassen, wählen Sie **Abbrechen aus**.
   Die folgende Meldung wird angezeigt: Wenn Sie diese Regel abbrechen, wird die zugehörige Korrekturaufgabe gelöscht, und die zugehörigen angreifbaren Elemente werden erneut geöffnet. Die Regeln für Korrekturaufgaben werden dann auf die einzelnen angreifbaren Elemente angewendet, und die Ausnahmeregel wird in den Entwurfsstatus versetzt.
9. Wählen Sie**Regel zum Anhalten beibehalten** oder **Abbrechen**, um die Regel in **den Entwurfsstatus** zu verschieben und zu deaktivieren.

Application Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln

Konfigurieren Sie Korrekturaufgaben (AVULs), damit Analysten und Korrekturspezialisten angreifbare Elemente in der Anwendung organisieren und massenweise analysieren können. Die Kriterien, nach denen Korrekturaufgaben erstellt werden, sind so konfiguriert, dass AVIs automatisch Korrekturaufgaben zugewiesen werden. Mit Korrekturaufgaben können Sie den Fortschritt überwachen und den Nachbesserungsprozess effizienter gestalten.

Nachverfolgung der Anzahl der Zurückstellungen für angreifbare Anwendungselemente und Korrekturaufgaben

Verfolgen Sie, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Die geplante Aufgabe `set deferral counts` wird täglich ausgeführt, um die Anzahl der Datensätze zu erfassen, die in der Spalte Anzahl der Zurückstellungen mehr als einmal zurückgestellt wurden. Datensätze werden in den Modulen „Mehrere Zurückstellungen“ für VR, AVR und CVR angezeigt.

Die Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Anwendungselemente automatisch gruppiert und zugewiesen werden. Das Basissystem enthält eine Standardregel **für Schwachstellen**, die AVIs basierend auf ihren Schwachstellen sammelt. Sie können jedoch nach jedem anderen Satz von Werten in Spalten gruppieren, auf die über das AVI zugegriffen werden kann. Diese Werte können Configuration Item (CI), Schwachstelleneintrag und Ähnliches umfassen.

Es gibt Aufgabenregeln für Application Vulnerability Response, die in der Anwendung Vulnerability Response enthalten sind. Sie ist verfügbar, wenn Sie sie aktivieren.

Mit dem Bedingungsgenerator können Sie mehrere Bedingungen erstellen. Nachdem Sie im Abschnitt „Gruppieren nach“ ein Feldpaar festgelegt haben, wird eine weitere Zeile

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angezeigt. Sie können bis zu sechs **„Gruppieren nach** “-Auswahlen auswählen. Sie können auch die Gruppenzuweisung automatisieren. Siehe Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

Beispielsweise können Sie Ihre angreifbaren Anwendungselemente nach Configuration Item oder nach Produktmodell gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit niedrigem Schweregrad oder für CIs mit geringem Risiko festlegen. Sie können eine andere Aufgabenregel für kritische Server und Schwachstellen festlegen, die das Unternehmen einem höheren Risiko aussetzen. Unter Erstellen, bearbeiten und löschen Sie Application Vulnerability Response Regeln für Korrekturaufgaben finden Sie weitere Informationen zu den Optionen, die Ihnen zur Verfügung stehen.

Für angreifbare Elemente in der Anwendung, die das Unternehmen einem höheren Risiko aussetzen, kann ein anderer Satz von Regeln verwendet werden. Der Name der Korrekturaufgabe wird an die Korrekturaufgabenregel „ **Gruppieren nach** “-Werte angehängt, um die Kurzbeschreibung des neuen Datensatzes zu erstellen.

Wenn ein neues angreifbares Anwendungselement erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Regeln entsprechend ausgewertet. Eine AVI wird nur einmal automatisch ausgewertet, es sei denn, sie wird nach dem Schließen erneut geöffnet oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete AVI verwendet:

- Für jede Regel für Korrekturaufgaben wird die AVI mit dem Regelfilter für Korrekturaufgaben verglichen.
- Für jede Regel, mit der die Regelbedingung für Korrekturaufgaben übereinstimmt, ruft die Regel die Daten aus der **Auswahl Gruppe nach** Auswahl im AVI ab. Es erstellt einen Gruppennamen und ein Feld. In diesem Fall, **Hohes Risiko: QID-32342:***Zusammenfassung von QID-3242* (Name: Schwachstellen-ID: Schwachstellenzusammenfassung).

  Hinweis:
  Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

  Die Regel prüft, ob eine übereinstimmende **offene** Korrekturaufgabe vorhanden ist, die der gleichen Zuweisungsgruppe wie die AVI zugewiesen ist.
  - Wenn die Aufgabe gefunden wird, wird die AVI der vorhandenen Aufgabe im Status „ **Offen“** hinzugefügt.
  - Wenn keine Aufgabe im Status „ **Offen“** gefunden wird, erstellt die Regel eine Aufgabe **mit hohem Risiko: QID-32342**, weist sie derselben Zuweisungsgruppe wie die AVI zu und platziert die AVI in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Bedingungen der Korrekturaufgabenregel verglichen wird, bevor sie in eine Korrekturaufgabe aufgenommen wird, können zu viele Regeln die Leistung beeinträchtigen. Richten Sie Ihre Aufgabenregeln so ein, dass die Bedingungen Ihnen helfen, die Erstellung von doppelten Korrekturaufgaben zu vermeiden.

Standardmäßig verwenden Regeln für Korrekturaufgaben beim Gruppieren der Elemente die von den **Zuweisungsregeln** im AVI festgelegte Zuweisungsgruppe und weisen die Korrekturaufgabe entsprechend den AVIs zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln im Modul **„Zuweisungsregeln“** gesteuert. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn eine Aufgabenregel aus dem Formular oder der Listenansicht gelöscht wird, können Sie alle von dieser Regel erstellten **offenen** Aufgaben löschen. Aufgaben, die sich nicht im Status „ **Offen“** befinden, werden ausgeschlossen.

Die Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Regel für Korrekturaufgaben ändern möchten, klicken Sie auf der Seite für die Regel für **Korrekturaufgaben** auf die Schaltfläche Erneut anwenden, um die geänderte Regel für alle aktiven **offenen** Korrekturaufgaben erneut auszuführen, die von dieser Regel erstellt wurden. Es löscht Korrekturaufgaben basierend auf der geänderten Regel automatisch und erstellt sie neu.

Beim erneuten Anwenden werden nur vorhandene Korrekturaufgaben überprüft.

Nachdem Sie **Erneut**anwenden ausgewählt haben, wird die folgende Meldung angezeigt: Durch das erneute Anwenden dieser Regel für Korrekturaufgaben werden die Korrekturaufgaben für diese Regel gelöscht und neu erstellt. Korrekturaufgaben, die sich nicht im Status „Offen“ befinden, werden nicht gelöscht.

Korrekturaufgaben erstellen und AVIs manuell hinzufügen

Sie erstellen eine Anwendungskorrekturaufgabe (AVUL) aus einem anderen Datensatz für eine Anwendungskorrekturaufgabe und fügen manuell Anwendungsangreifbare Elemente (Application Vulnerable Items, AVITs) hinzu. Weitere Informationen finden Sie unter Erstellen Sie eine Anwendungskorrekturaufgabe manuell in Application Vulnerability Response.

Regeln für Korrekturaufgaben und AVI erstellen und aktualisieren

Wenn ein CI oder Produktmodell aus einem Scan mit einer bekannten Schwachstelle verknüpft ist, wird ein AVI erstellt. Nach der Erstellung wird die AVI anhand der Bedingungen der Regeln für Korrekturaufgaben auf Übereinstimmung ausgewertet. Wenn es eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe gibt, wird die AVI hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für die AVI erstellt.

Wenn eine Eigenschaft, die in den Filterbedingungen für Korrekturaufgaben erfasst wird, in einem AVI aktualisiert oder geändert wird, wird die aktualisierte AVI auch anhand der Regeln für Korrekturaufgaben auf Übereinstimmung ausgewertet. Wenn es eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe gibt, wird die AVI hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für die AVI erstellt.

Status-Rollup und -Rolldown

Wenn Sie eine Korrekturaufgabe auf „Offen“ oder von „Offen“ auf „Wird untersucht“ ändern, wird der neue Status auf alle zugeordneten AVIs übertragen. Das Status-Rolldown erfolgt unmittelbar nach dem Ändern des Status.

Ein Status-Rollup von AVIs zur Korrekturaufgabe findet nur statt, wenn sich alle AVIs für die Aufgabe im Status **„Zurückgestellt“** oder **„Geschlossen – Fest“** befinden. Rollup erfolgt mit der regelmäßigen Aufgabe `Rollup application vulnerable item values to vulnerability and group`, die alle 15 Minuten ausgeführt wird. Für den Status wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erst ein Rollup durchgeführt, wenn der Auftrag ausgeführt wird. Damit ein Rollup von den AVIs zur Korrekturaufgabe erfolgt, müssen sich alle AVIs im gleichen Status befinden.

Erstellen, bearbeiten und löschen Sie Application Vulnerability Response Regeln für Korrekturaufgaben

Sie können Regeln erstellen, um angreifbare Elemente in Anwendungen (Application Vulnerable Items, AVI) basierend auf Filterbedingungen automatisch in Korrekturaufgaben (AVUL) zu gruppieren. Diese Regeln gruppieren automatisch AVIs, wenn sie importiert oder manuell erstellt werden.

Vorbereitungen

Wenn Sie eine neue Regel erstellen, gilt sie nicht für vorhandene Daten. Nachdem Sie es übermittelt haben, wird es für neue Importe ausgeführt.

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben**.
2. Öffnen Sie die Regel, oder wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie.

Regel für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Aufgabenregel.
Aktiv	Gibt an, ob die Aufgabe aktiv ist.
Beschreibung	Eine Beschreibung der Regel.
Groß-/ Kleinschreibung beachten	Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht. **Hinweis:** Beim Standardwert wird zwischen Groß- und Kleinschreibung unterschieden.
Bedingung	Optionale Filterbedingungen für die Regel. Standardmäßig (Kontrollkästchen**„Groß-/Kleinschreibung beachten** “ nicht aktiviert) berücksichtigt der Suchtext, den Sie im Bedingungsgenerator für Aufgabenregeldatensätze und -formulare eingeben, Groß-/Kleinschreibung. Sie können die Suche nach Groß-/ Kleinschreibung für Aufgabendatensätze und Formulare aktivieren. Eine Beispielbedingung ist **Schwachstelle** > **ist** > **VULNENT123451** (eine bekannte importierte Schwachstelle). Alle AVIs, die diese Schwachstelle aufweisen, erfüllen diese Bedingung.
Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)	
Angreifbare Anwendungselemente gruppieren aus	Die Tabelle, die von der Regel zum Gruppieren von AVIs verwendet wird. Wählen Sie die Elemente aus der Struktur aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Angreifbares Anwendungselement [sn_vuln_vulnerable_item] ◦ Angreifbares Anwendungselement – Konfigurationselement [cmdb_ci] ◦ Angreifbares Anwendungselement Anwendungsschwachstelle [sn_vul_ third_party_entry] ◦ Produktmodell für angreifbare Anwendungselemente **Hinweis:** Wenn Sie eine erweiterte Tabelle wählen, wird das **Feld Verwendet** nur für angreifbare Anwendungselemente angewendet, die diese erweiterte Tabelle verwenden.
Mit Feld	Feld in der Tabelle, das von der Regel zum Gruppieren von AVIs verwendet wird. Wählen Sie in der Struktur Bedingungen aus. **Hinweis:** Sie können „Gruppieren nach“-Bedingungen erstellen, sodass nicht alle AVIs, die Daten freigeben, der gleichen Korrekturaufgabe zugewiesen werden. Wenn Sie beispielsweise Zuweisungsgruppe und IP-Adresse als Felder Verwenden von auswählen und mehrere AVIs die anfängliche Filterbedingung **Schwachstelle**erfüllen, können diese AVIs mithilfe der vielen im Abschnitt Gruppieren nach verfügbaren Optionen zur Korrektur verschiedenen Zuweisungsgruppen zugewiesen werden. Die Bedingungen für Gruppieren nach geben Ihnen die Flexibilität, eindeutige Korrekturaufgaben zu erstellen, die anderen Gruppen zugewiesen werden können, selbst wenn sie einige Daten gemeinsam nutzen.
Zuweisung	
Korrekturaufgaben zuweisen nach	Bei der automatischen Zuweisung von Korrekturaufgaben wird die Option Zuweisung zusätzlich zu den Auswahlmöglichkeiten **für Gruppieren nach** verwendet, um die angreifbaren Elemente zu gruppieren. Neue Aufgaben werden nach Bedarf erstellt, sodass jedes AVI in einer Aufgabe mit einer übereinstimmenden Zuweisungsgruppe platziert wird. Um die Zuweisung von auf der Grundlage dieser Regel erstellten Aufgaben zu automatisieren, wählen Sie eine der verfügbaren Optionen aus. ◦ Feld Gruppieren nach: Wenn Sie ein Benutzergruppenfeld aus Feldwerte **werden verwendet** im Abschnitt **Gruppieren nach**ausgewählt haben, werden diese im Dropdown-Menü angezeigt. ◦ Benutzergruppe: Verwenden Sie die Suchliste, um eine statische Benutzergruppe auszuwählen.

Wenn Sie eine Regel aus dem Formular oder der Listenansicht löschen, können Sie alle **offenen** Korrekturaufgaben löschen, die von dieser Regel erstellt wurden. Gruppen, die sich nicht im Status **„Offen“** befinden, werden ausgeschlossen.

4. Wählen Sie **Absenden** für neue Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie **Absenden**gewählt haben, wird Ihre Regel in der Liste Regeln für Korrekturaufgaben [sn_vul_grouping_rule] angezeigt. Die folgenden Situationen initiieren Ihre Regel.

- Wenn neue AVIs erstellt werden
- Wenn Sie **Erneut anwenden**wählen. Sie wählen **Erneut anwenden,** um Aufgabenregeln nur für vorhandene Korrekturaufgaben auszuwerten.
- Wenn AVIs aktualisiert werden, entweder von Ihnen oder vom System.

  Wenn ein AVI aktualisiert wird, werden Aufgabenregeln auf Übereinstimmungen mit vorhandenen Korrekturaufgaben ausgewertet. Einige häufige Updates, die eine Regelprüfung auslösen, sind:

  - Wenn der Status von „Geschlossen“ zu „Offen“ oder von „Geschlossen“ zu „Wird untersucht“ wechselt.
  - Das Configuration Item (CI) wird geändert.
  - Die Schwachstelle wird geändert.

Das System überprüft alle Aufgabenregeln auf Übereinstimmungen mit dem aktualisierten AVI. Wenn die Bedingungen einer Regel mit den Bedingungen einer Korrekturaufgabe übereinstimmen, werden ihr entsprechende AVIs zugewiesen.

Wenn keine Übereinstimmung gefunden wird, wird eine neue Korrekturaufgabe erstellt.

Weitere Informationen zum Status-Rollup von AVIs zu Korrekturaufgaben und zum Status-Rolldown von Korrekturaufgaben zu AVIs finden Sie unter Application Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln.

Ein Beispiel für eine Regel für Korrekturaufgaben finden Sie unter Application Vulnerability Response Beispiele für Regeln für Korrekturaufgaben.

5. Um eine Aufgabenregel zu löschen, wählen Sie die Regel in der Liste „Regeln für Korrekturaufgaben“ aus, und wählen Sie **Löschen aus**.
   Die folgende Meldung wird angezeigt: Die ausgewählte Regel für Korrekturaufgaben hat n Korrekturaufgaben erstellt. Von den Korrekturaufgaben haben n den Status „Offen“..

Option	Beschreibung
Kontrollkästchen deaktiviert (Standard).	Löschen Sie nur die Regel. Aufgaben, die sich nicht im Status „ **Offen“** befinden, werden ausgeschlossen.
Checkbox aktiviert.	Schließen Sie die Korrekturaufgaben in den Status „ **Offen** “ ein, wenn Sie die Regel für Korrekturaufgaben löschen. Löschen Sie die Regel und alle Korrekturaufgaben im Status „ **Offen** “.

6. Wählen Sie eine Option und anschließend **Löschen**aus.

Erstellen Sie eine Anwendungskorrekturaufgabe manuell in Application Vulnerability Response

Erstellen Sie eine Anwendungskorrekturaufgabe (AVUL) aus einem anderen Datensatz für eine Anwendungskorrekturaufgabe, und fügen Sie manuell Anwendungsangreifbare Elemente (Application Vulnerable Items, AVITs) hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_sec_manager

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Alle**.
2. Wählen Sie oben rechts auf der Seite **Neu**aus.
3. Wählen Sie auf der Registerkarte Gruppenkonfiguration für Gruppierungsmethode **Manuell**aus.
4. Wählen Sie **Absenden**.
5. Suchen Sie Ihren neuen Aufgabendatensatz (AVUL) in der Tabelle „Anwendungskorrekturaufgaben“ [sn_vul_app_vulnerability].
   Der Datensatz wird im Status **Offen** erstellt.
6. Öffnen Sie den Datensatz, und fügen Sie dieser Gruppe mithilfe der zugehörigen Liste „Angreifbare Anwendungselemente“ (**Bearbeiten** oder **Hinzufügen**) neue oder vorhandene angreifbare Anwendungselemente hinzu.
7. Wählen Sie **Aktualisieren**, um den Datensatz zu speichern, oder andere UI-Aktionen, um den Datensatz in einen anderen Status zu überführen.

Erstellen Sie Regeln für das automatische Schließen

Verwenden Sie Regeln zum automatischen Schließen, um ältere AVITs basierend auf den von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_manage_auto_close_rules

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Regeln zum automatischen Schließen**.
   Das -Basissystem stellt die folgenden Regeln für das automatische Schließen bereit:

   Zuletzt gescannte Anwendungsschwachstellen Schwachstellen, die in den letzten 90 Tagen nicht gemeldet wurden, werden in den Status **„Veraltet“** versetzt.
2. Wählen Sie **Neu** aus, um eine neue Regel für das automatische Schließen zu erstellen.
3. Füllen Sie die Felder des Formulars aus.

Feld	Wert
Name	Name der Regel zum automatischen Schließen.
Aktiv	Option zum Aktivieren der Regel. Wenn aktiviert, werden Erkennungen automatisch geschlossen, die den Filterkriterien entsprechen.
Ausführungsreihenfolge	Eindeutiger Wert für die Ausführung der Regel zum automatischen Schließen. Dieser Wert bestimmt die Reihenfolge der Ausführung. Der Standardwert ist 100.
Integrationstyp	Anwendungsschwachstellenintegration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Beschreibung	Beschreibung der Regel zum automatischen Schließen.
Bedingung	Filterbedingungen, die zum Identifizieren von Erkennungen verwendet werden, die geschlossen werden sollten.

4. Wählen Sie **Absenden**.

Die regelmäßige Aufgabe **„Regeln für automatisches Schließen“** wird jede Nacht ausgeführt. Identifiziert AVITs basierend auf den angegebenen Bedingungen und versetzt die übereinstimmenden in den Status **Veraltet**. In Fällen, in denen AVITs mit den Status „Geschlossen“ und „Veraltet“ vorhanden sind, wird das AVIT mit dem Substatus „ **Fest“**geschlossen.

Konfigurieren Sie Penetrationstests

Sie können die Sprint-Dauer und den geschätzten Aufwand für Bewertungstypen für Penetrationstests konfigurieren. Dies stellt Anwendungsbesitzern Zeitplanungsfunktionen bereit, mit denen sie einen vorläufigen Zeitrahmen für ihre Anforderungen für die Bewertung von Penetrationstests bestimmen können.

Vorbereitungen
Erforderliche Rolle: Ethical Hacker

Warum und wann dieser Vorgang ausgeführt wird
Durch die Konfiguration der Bewertungseinstellungen für Penetrationstests für das Team für ethisches Hacken können Sie auch die Gruppe und den Ansprechpartner festlegen, die die Bewertungsanforderung für Penetrationstests erhalten.

Ab v19.0 von Vulnerability Responsesind, wenn Sie Veracode Vulnerability Integrationverwenden, die Penetrationsbewertungstests in Veracode Vulnerability Integration manuelle Ergebnisse von Veracode. Sie sind nicht mit Bewertungsanforderungen für Penetrationstests verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstestbewertungen von Veracodefinden Sie unter Veracode Vulnerability Integration.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**.
2. Verwenden Sie den ersten Abschnitt, um die Zuweisungsgruppe zu konfigurieren.
3. Füllen Sie die Felder des Formulars aus.

Formular „Konfigurationen für Penetrationstests“.

Feld	Beschreibung
Anwendergruppe des Penetrationstestteams	Gruppe, der die Penetrationstest-Bewertungsanforderung zugewiesen ist.
Standard-Beauftragter für Bewertungsanforderungen für Penetrationstests	Ansprechpartner für die Anforderung für die Penetrationstestbewertung.

4. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Verwenden Sie den zweiten Abschnitt, um Sprints zu konfigurieren.
   Details finden Sie unter Sprints für Penetrationstests konfigurieren.
6. Verwenden Sie den dritten Abschnitt zum Konfigurieren von Bewertungstypen.
   Details finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests.

Sprints für Penetrationstests konfigurieren

Konfigurieren Sie die Sprint-Dauer und -Kapazität für das Team für ethisches Hacken, damit es die Sprint-Kapazität für Penetrationstest-Bewertungen verwalten kann.

Vorbereitungen

Erforderliche Rolle: Ethical Hacking

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**.
2. Wählen Sie die Option **Konfigurieren** für Sprints konfigurieren aus.
3. Füllen Sie die Felder des Formulars aus.

Formular „Sprint-Konfiguration“.

Feld	Beschreibung
Sprint-Dauer (Tage)	Anzahl der Tage in einem Sprint.
Startdatum	Startdatum für die Sprint-Dauer.
Anzahl der Sprints	Anzahl der Sprints, die basierend auf dem Start- und Enddatum für den Sprint-Bereich generiert werden können.
Enddatum	Enddatum für die Sprint-Dauer.
Sprint-Kapazität	
Sprint-Kapazität (Stunden)	Kapazität eines Sprints in Stunden.

4. Wählen Sie **Sprints generieren aus**.
   Um die erstellten Sprints anzuzeigen, wählen Sie **Sprints anzeigen**aus.

Hinweis:
Nachdem die Sprints generiert wurden und in Bearbeitung sind und Sie **Sprints generieren** für die gleiche Dauer auswählen, wird der aktuelle Sprint wie gewohnt abgeschlossen. Die verbleibenden Sprints werden basierend auf der aktualisierten Sprint-Konfiguration neu berechnet.

Konfigurieren Sie Bewertungstypen für Penetrationstests

Konfigurieren Sie den geschätzten Aufwand für jede Art von Penetrationstestbewertung. Auf diese Weise können Sie die Kapazität jedes Sprints verwalten, indem Sie den erforderlichen Aufwand für jeden Bewertungstyp schätzen.

Vorbereitungen

Erforderliche Rolle: Ethical Hacking

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Jeder Sprint ist einer Penetrationstestanforderung zugewiesen. Basierend auf dem geschätzten Aufwand für den Bewertungstyp werden die Stunden angepasst, um die Stundensaldo für den Sprint widerzuspiegeln.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**.
2. Ab v19.0 von Vulnerability Responsewählen Sie **Konfigurieren**, um Bewertungstypen, Anwendungsgröße und Geschätzter Aufwand anzuzeigen.
3. **Wahlweise:** Wählen Sie einen Bewertungstyp-Datensatz aus, um die Felder nach Bedarf zu aktualisieren, oder erstellen Sie neue Datensätze.

   (Optional) Die Werte für die Anwendungsgröße bieten Ihnen weitere Optionen, um die Testzeit und den Aufwand für Tests genauer einzuschätzen. Sie können die Stunden für diese Datensätze bearbeiten oder **„Neu“** auswählen, um eigene Kombinationen zu erstellen.

   Sie können den Bewertungstyp und die Anwendungsgröße der Werte in vorhandenen Anforderungsdatensätzen für Penetrationstests ändern, um Tests entsprechend der Sprint-Kapazität zu planen. Wenn Sie beispielsweise eine Testanforderung ausfüllen, wird die Anzahl der konfigurierten Sprints möglicherweise nicht angezeigt, da einige Sprints bereits getestet wurden. Wenn der geschätzte Aufwand in Stunden eines Sprints mit der für den Typ und die Größe eines Tests erforderlichen Kombination übereinstimmt, sind sie nicht für neue Anforderungen verfügbar.

   Sie können die Sprints, die Testanforderungen für Datensätze in der Liste der Penetrationstest-Sprints zugewiesen sind, unter einsehen **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration** > **Sprints konfigurieren**. Weitere Informationen zum Konfigurieren von Sprints finden Sie unter Sprints für Penetrationstests konfigurieren.

   Die Basiswerte für Bewertungstyp, Anwendungsgröße und Geschätzter Aufwand sind:

Formular für die Konfiguration des Bewertungstyps für Penetrationstests

Bewertungstyp	Anwendungsgröße	Geschätzter Aufwand (Stunden)
Fokussierter Test	Klein	20
Fokussierter Test	Mittel	30
Fokussierter Test	Groß	40
Fokussierter Test	Standard	40
Erneut testen	Klein	10
Erneut testen	Mittel	15
Erneut testen	Groß	20
Erneut testen	Standard	20
Vollständiger Penetrationstest	Klein	60
Vollständiger Penetrationstest	Mittel	70
Vollständiger Penetrationstest	Groß	80

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertungstyp	Anwendungsgröße	Geschätzter Aufwand (Stunden)
Vollständiger Penetrationstest	Standard	80

4. Wählen Sie Aktualisieren, um Ihre Änderungen zu speichern, oder Absenden für einen neuen Datensatz.
5. Wählen Sie vor v19.0 die Option **Konfigurieren** für Bewertungstypen konfigurieren aus.
6. Aktualisieren Sie die Werte für die Bewertungstypen nach Bedarf.
   Basiswerte sind:

Formular für die Konfiguration des Bewertungstyps für Penetrationstests

Bewertungstyp	Geschätzter Aufwand (Stunden)
Fokussierter Test	40
Erneut testen	20
Vollständiger Penetrationstest	80

7. Speichern Sie die Änderungen.

Integration von Application Vulnerability Response mit anderen Anwendungen

Vulnerability Response beinhaltet Unterstützung für Drittanbieterintegrationen.

Integrationen von Drittparteien

Anwendungsschwachstellen-Integrationen ergänzen die Anwendungsschwachstellendaten in Ihrer Instanz durch Abrufen von Daten aus externen Systemen und Lieferanten.Weitere Informationen zu unterstützten Integrationen finden Sie in den folgenden Übersichtsthemen:

- Fortify Vulnerability Integration
- GitHub-Anwendungsschwachstellen-Integration
- Invicti-Schwachstellen-Integration
- Veracode Vulnerability Integration
- Integration von Atlassian Jira

Wichtig:
Im Arbeitsbereich des Schwachstellenmanagers können Sie ein Agile-Problem manuell mit der Listen- und Formularaktion erstellen, um die Nachbesserung von AVITs und RTs nachzuverfolgen.

Hinweis:

Integrationen mit mehreren Quellen werden in Application Vulnerability Responsenicht unterstützt. Drittanbieterintegrationen werden separat behandelt. Wenn in Ihrer Umgebung mehr als eine Integrationsanwendung von Drittparteien verwendet wird, gibt es keine integrationsübergreifende Deduplizierung von angreifbaren Elementen (Application Vulnerable Item, AVI).

Zusätzliche Hinweise zu Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Application Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Schwachstellen-Integrationen für Application Vulnerability Response sind so konfiguriert, dass sie auf Zeitplanbasis ausgeführt werden. Sie können sie jedoch bei Bedarf manuell ausführen.

Erforderliche Rolle: sn_vul.app_read_integrations

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Öffnen Sie den Datensatz für die Integration, die Sie ausführen möchten.
3. Klicken Sie auf **Jetzt ausführen**.

Vulnerability Response-Integration mit Black Duck

Die Integration Vulnerability Response von mit Vulnerability Response-Integration mit Black Duck verwendet die Daten, die aus dem Tool Black Duck Software Composition Analysis (SCA) importiert werden, um Ihnen zu helfen, die Auswirkung und Priorität der Fehler in Ihrem Code zu bestimmen.

Integrationsübersicht

Mit Vulnerability Response-Integration mit Black Duckkönnen Sie SCA sammeln und diese Daten für Now Platformverfügbar machen. Ab v22.0.5 von Vulnerability Responsekönnen Sie die SCA-Schwachstellendaten in Ihre Instanz importieren, um die Schwachstellen in Ihren Softwareanwendungen zu identifizieren. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Eine gemeinsam genutzte API erfasst die SCA-Daten.

Hinweis:
Für jeden Integrationsdatensatz ist die Ausführung als Benutzer konfiguriert. Der Standardwert für diesen Anwender ist VR-System. Ändern Sie diesen Wert nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeden Tag rufen geplante Aufgaben die Integrationen automatisch in der Reihenfolge auf, in der sie aufgeführt sind. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Verfügbare Versionen

Verfügbare Versionen von Black Duck-Integration

Freigabeversion	Release-Hinweise
Vulnerability Response-Integration mit Black Duck 1.0.5	Application Vulnerability Response release notes

Benutzergruppe und -rollen

Vulnerability Response-Integration mit Black Duck wird von einem Benutzer mit der Administratorrolle installiert und von einem Mitglied der App-Sec-Manager-Gruppe konfiguriert. Weitere Informationen finden Sie im Abschnitt Application Vulnerability Response Benutzergruppen und -rollen.

Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus des Imports Vulnerability Response-Integration mit Black Duck an

Informationen zum Anzeigen von Daten in den Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

Bereiten Sie Vorintegrationsaufgaben für vor Vulnerability Response-Integration mit Black Duck

Planen und führen Sie die Vorintegrationsaufgaben für Vulnerability Response-Integration mit Black Duck aus, damit die Integration erfolgreich ist. Vulnerability Response-Integration mit Black Duck setzt voraus, dass Sie mit der Anwendung Black Duck Software Composition Analysis (SCA) und den APIs vertraut sind.

Vorbereitungen

Bevor Sie Vulnerability Response-Integration mit Black Duckinstallieren und konfigurieren, sollten Sie die Common Weakness Enumeration-Integration (CWE) ausführen und installieren, die auch von Application Vulnerability Responseverwendet wird. Die CWE-Integration wird standardmäßig mit Vulnerability Response installiert.

Hinweis:
Die Daten der NIST Vulnerability Database (NVD) sind zwar nicht erforderlich, um die Black Duck Application Vulnerability Integration zu installieren, es wäre jedoch nützlich, sie zu besitzen. Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

Für jeden Integrationsdatensatz ist die Ausführung als Benutzer konfiguriert. Der Standardwert für diesen Anwender ist VR.System. Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen vor, die auf Ihren Anforderungen basieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Validiert die Größe Ihrer Instanz anhand der Anzahl der angreifbaren Anwendungselemente, die importiert werden sollen. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer -Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Vulnerability Response-Integration mit Black Duck erfordert eine API-URL und ein API-Token.

Prozedur

Erstellen Sie das API-Token und die Key-Anmeldeinformationen.

a. Melden Sie sich bei der Black Duck-Plattform an.

b. Wechseln Sie zum Menü „Benutzeraccount“, und wählen Sie **API-Anmeldeinformationen**aus.

c. Wählen Sie **API-Anmeldeinformationen generieren aus**.

d. Notieren Sie Ihre Anmeldeinformationen zur späteren Verwendung.

Installieren Sie ServiceNow Vulnerability Response-Integration mit Black Duck

Bevor Sie die Integration in Ihrer -Instanz ausführen, müssen Sie die Installations- und Konfigurationsschritte abschließen, damit das Tool Black Duck Software Composition Analysis (SCA) ordnungsgemäß in Application Vulnerability Responseintegriert werden kann.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Sie müssen diese Setupaufgaben ausführen, damit das Tool Black Duck Software Composition Analysis (SCA) ordnungsgemäß in Application Vulnerability Responseintegriert werden kann.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben (Fortsetzung)

Setupaufgaben	Beschreibung
	• Wenn sie noch nicht zugewiesen sind, installiert der Benutzer mit der Administratorrolle die Anwendung und weist der App-Sec-Manager-Gruppe Benutzer zu. Informationen zu Gruppenrollen finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen. • Die App-Sec-Manager-Gruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Dieses SCA-Tool ist als separates Abonnement verfügbar.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie Vulnerability Response-Integration mit Black Duck installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie im Feld ServiceNow Storenach Vulnerability Response Integration with the Black Ente.
4. Wählen Sie die Anwendungskachel aus.
   Die Details zu der Anwendung, die Sie installieren, werden angezeigt.

   Hinweis:
   Lesen Sie ggf. die Abschnitte über weitere Anforderungen und Abhängigkeiten.

5. Wählen Sie **App anfordern** aus, und geben Sie Ihre Now Support -Anmeldeinformationen ein.
6. Wählen Sie **Abrufen aus**.
7. Geben Sie den Instanznamen und den Grund für die Instanz ein, und wählen Sie **Validate Instance (Instanz validieren)**aus.
8. Wählen Sie **Anforderung**aus.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie **Installieren**aus.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Nächste Maßnahme

Konfigurieren Sie Vulnerability Response-Integration mit Black Duck für Ihre Umgebung. Siehe Konfigurieren Sie die Eigenschaften Vulnerability Response-Integration mit Black Duck

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Eigenschaften Vulnerability Response-Integration mit Black Duck

Bevor Sie Vulnerability Response-Integration mit Black Duck in Ihrer Instanz von ausführen, müssen Sie die Installations- und Konfigurationsschritte durchführen, damit das Tool Black Duck Software Composition Analysis (SCA) ordnungsgemäß in die Anwendung Application Vulnerability Response integriert werden kann.

Vorbereitungen

Erforderliche Rolle: Anwendergruppe „App-Sec-Manager“.

Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response-Integration mit Black Duck ist als separates Abonnement verfügbar.

Prozedur

1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Konfiguration**.
2. Wählen Sie den Standardauthentifizierungstyp aus.
   Die Standardauthentifizierung erfordert MID-Server für lokale Instanzen. Sie können das API-Token, das für die Standardauthentifizierung erforderlich ist, von Ihrem Black Duck-Konto generieren.
3. Füllen Sie die Felder des Formulars aus.
   Basic Authentication

Feld	Beschreibung
API-URL	Black-Duck-API-URL für Enterprise-Instanzen oder lokale Instanzen. Die lokale Instanz ist Ihre Black-Duck-Endpunkt-URL.
API-Token	Token, das Sie über Ihre Black Duck-Konsole generiert haben.
MID-Server	MID-Server , das für lokale Instanzen für die Standardauthentifizierung erforderlich ist.
SCA einbeziehen	Schwachstellen aus Software Composition Analysis-Scans (SCA), die standardmäßig enthalten sind. SCA-Scans identifizieren die Schwachstellen in Open Source-Komponenten.
Wählen Sie die Option zum Verwalten von Falschmeldungen in ServiceNow	ServiceNow Option zum Verwalten von Falschmeldungen. Lassen Sie diese Option aktiviert, wenn Sie die importierten angreifbaren Elemente der Anwendung (Application Vulnerable Items, AVIs) mit **Quellstatus**, die als **Falsch positiv** oder **Potenziell falsch positiv**markiert sind, selektieren möchten. AVIs mit diesen **Quellstatus**, die in Ihrer Instanz normalerweise einem Status **„Geschlossen“** zugeordnet sind, werden **Offen**zugeordnet. Sie können ein **Falsch positives Ergebnis** aus dem AVI-Datensatz anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Deaktivieren Sie eine oder beide Optionen, wenn Sie die **Quellstatus** beibehalten möchten, die von Ihrem Scanner importiert wurden. ○ Wenn diese Option deaktiviert ist, sind die Aktionen **„Ausnahme anfordern“** und **„Falsch positiv“** in den AVIs nicht sichtbar.
Integrationsinstanz	Instanz, die Sie zum Importieren der Daten verwenden.

4. Wählen Sie **Anmeldeinformationen speichern und testen aus**.
5. Führen Sie die **Black-Duck-Projektlistenintegration** aus, bevor Sie andere Integrationen ausführen. Die anderen Black-Duck-Integrationen, z. B. die Black-Duck-Applikationslisten-Integration und die Black-Duck-Integration für angreifbare Elemente der Anwendung, hängen von den aktuellen Projekt- und Anwendungsdaten ab, die Sie aus der Projektlisten-Integration importiert haben.

Zeigen Sie den Ausführungsstatus des Imports Vulnerability Response-Integration mit Black Duck an

Überprüfen Sie den Erfolg Ihrer Integrationsausführungen, lokalisieren Sie Probleme, und bestätigen Sie Ihre Entscheidungen zur Problembehebung, indem Sie sich die zugehörige Liste „Integrationsausführungen für Schwachstellen“ ansehen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Wählen Sie die zugehörige Liste Integrationsausführungen für Schwachstellen aus.
4. Stellen Sie sicher, dass alle Importe erfolgreich waren.
   Problembehandlung:

   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

   ○ Netzwerkunterbrechung.

   ○ Ein Problem bei der Datenübertragung, das während einer Transformation zu beschädigten Daten führt.

   Wenn eine dieser Bedingungen bei Ihnen auftritt, wählen Sie **Jetzt ausführen aus**, und führen Sie die Integration erneut aus.
5. Zeigen Sie die importierten Repositorys an, indem Sie zur Integrationsliste navigieren und den Black-Duck-Integrationsdatensatz auswählen.
6. Wählen Sie die zugehörige Liste „Ausführungen der Schwachstellenintegration“ aus, und öffnen Sie einen Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datentransformation für die Vulnerability Response-Integration mit Black Duck

Nachdem Sie die zu importierenden Daten identifiziert haben, werden die Daten von Vulnerability Response-Integration mit Black Duckabgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz transformiert.

Vulnerability Response-Integration mit Black Duck

Die Daten aus der API werden zuerst in die Tabelle „Black Duck AppVul-Elementimport“ [sn_vul_blackduck_appvul_item_import] geladen. Anschließend wird die Black Duck AppVul-Elementtransformation zur Transformation der importierten Informationen verwendet.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach **Black Ente AppVul Item Transformieren**. In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

Black Duck – AppVul Item – Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
app_id	source_app_id	Anwendungs-ID.
Ausgabe-ID	source_avit_id	AVIT-ID
app_name	app_name	Anwendungsname.
version	app_version	Anwendungsversion.
build_id	source_scan_id	Build-ID der Anwendung.
account_id	account_id	Account-ID.
Sandbox-ID	Sandbox-ID	Sandbox-ID.
last_update_time	last_scan_date	Uhrzeit der letzten Aktualisierung.
app_name + last_scan_date	scan_summary_name	Scan-Zusammenfassung.
life_cycle_stage	source_sdlc_status	SDLC-Status der Quelle.
level	source_severity	Quellenschweregrad.
kategoriename	Kategorie	Kategorie.
source_severity	source_severity	Quellenschweregrad.
category_id + „CWE-“ + cweId	source_entry_id	Quelleintrags-ID.
source_vulnerability_summary	source_vulnerability_summary	Zusammenfassung der Quellschwachstelle.
source_recommendation	source_recommendation	Quellempfehlung.
description	description	Beschreibung aus der Quelle.
description	source_vulnerability_explanation	Erklärung der Quellschwachstelle.
mitigation_status_desc	source_mitigation_status	Quellverringerungsstatus.
remediation_status	source_remediation_status	Korrekturstatus der Quelle.
Zeile	zeilennummer	Position, in der der Fehler gefunden wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Black Duck – AppVul Item – Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
Modul	application_module	Anwendungsmodul
Quelldatei	source_notes	Quellhinweise.
impacts_policy_compliance	Compliance_mit_Richtlinie	Die Werte können „Ja“ oder „Nein“ sein, je nachdem, ob die Quellinformationen „wahr“ oder „falsch“ sind.
Quelldateipfad und Quelldatei	location	Standortzuordnung eines statischen Fehlers.
URL	location	Standortzuordnung für einen dynamischen Fehler.
Umfang, Typ, ExploitLevel	source_additional_info	Namenswertfeld, das mit den Werten aus der Quelle für statische Fehler gefüllt wird.

In der folgenden Tabelle sind die Transformationsskripts aufgeführt, die während des Transformationsprozesses ausgeführt werden.

Timing und Zweck des Skripts für die Black-Duck-Transformationszuordnung

Black-Duck-Transformationszuordnungsskript

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zur Verarbeitung des Datensatzes und zum Aktualisieren der Anzahl der erstellten, aktualisierten oder unveränderten Entitäten sowie der als Teil dieser Integration importierten Entitäten verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Skript, mit dem das Verhalten für Datensätze definiert wird, die ungültig sind und ignoriert werden müssen. Wird auch verwendet, um das globale Objekt für die Datensatzverarbeitung zu definieren. Dieses Skript dient zur internen Verwendung und darf nicht geändert oder gelöscht werden.

Black-Duck-Integration – Statuszuordnung

Die folgende Tabelle zeigt die Quellstatus aus der Black Duck-Schwachstellenintegration und ihre Zielstatus in Ihrer Instanz.

Black-Duck-Quellstatus und die entsprechenden Now Platform -Status

Black-Duck-Quellstatus	Beschreibung der Quellstatus	Zielstatus in der Now Platform
Neu	Die Schwachstelle betrifft diese Komponentenversion.	Öffnen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Black-Duck-Quellstatus und die entsprechenden Now Platform -Status (Fortsetzung)

Black-Duck-Quellstatus	Beschreibung der Quellstatus	Zielstatus in der Now Platform
Benötigt Überprüfung	Es kann nicht bestimmt werden, ob eine Schwachstelle diese Komponentenversion betrifft.	Öffnen
Korrektur erforderlich	Für diese Version ist eine Korrektur erforderlich.	Öffnen
Korrektur abgeschlossen	Die Korrektur für diese Schwachstelle ist abgeschlossen.	Abgeschlossen
Verringert	Schwachstelle wurde gemindert.	Abgeschlossen
Gepatcht	Schwachstelle wurde gepatcht.	Abgeschlossen
Ignoriert	Schwachstelle wurde ignoriert.	Abgeschlossen

Importieren Sie die Projektinformationen aus der Black-Duck-Integrationsinstanz

Importieren Sie die Projektinformationen aus der Black Duck-Integrationsinstanz, um sicherzustellen, dass die Schwachstellen-Integrationen nacheinander ausgeführt werden. Eine erfolgreiche Integration hilft Ihnen, die angreifbaren Elemente der Anwendung (Application Vulnerable Items, AVIs) zu identifizieren und zu erfassen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Sie können alle Projektinformationen aus Vulnerability Response-Integration mit Black Duck in der Black-Duck-Projekttabelle [sn_vul_blackduck_project] importieren. Alle erforderlichen Attribute (z. B. Projekt-GUID), die für die Abfrage verschiedener Versionen des Projekts erforderlich sind, werden in der Black-Duck-Projekttabelle [sn_vul_blackduck_project] erfasst.

Prozedur

1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
   Sie können beispielsweise die **Black-Duck-Projektlistenintegration auswählen.**
3. Wählen Sie **Jetzt ausführen**.

   Hinweis:
   Vulnerability Response-Integration mit Black Duck soll einen möglichst vollständigen Datenabruf bieten. Das Ausführen dieser Integrationen in falscher Reihenfolge kann zu unvollständigen Daten führen und erfordert Fachwissen über ServiceNow und Application Vulnerability Response.

   Nachdem der Import abgeschlossen ist, können Sie die Projektdetails in der Black-Duck-Projekttabelle [sn_vul_blackduck_project] anzeigen.
4. Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus des Imports Vulnerability Response-Integration mit Black Duck an.
5. **Wahlweise:** Wenn Sie andere Integrationsparameter ändern möchten, müssen Sie zur Integrationsinstanz navigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie Vulnerability Response-Integration mit Black Duck Projektversionen in die Tabelle „Erkannte Anwendungen“.

Importieren Sie die Vulnerability Response-Integration mit Black Duck-Projektversionen in die Tabelle „Erkannte Anwendungen“ [sn_vul_release], damit die Black Duck-Schwachstellen-Integrationen nacheinander ausgeführt werden. Eine erfolgreiche Integration hilft Ihnen, die angreifbaren Elemente der Anwendung (Application Vulnerable Items, AVIs) zu identifizieren und zu erfassen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Sie können alle verschiedenen Versionen der -Projekte hinzufügen und anzeigen (siehe die Details in der Black-Duck-Projekttabelle), die aus Vulnerability Response-Integration mit Black Duck in der Tabelle „Erkannte Anwendungen“ [sn_vul_release] importiert wurden.

Prozedur

1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Integrationen** .
2. Wählen Sie eine Integration aus.
   Sie können beispielsweise **Black Duck-Anwendungslistenintegration**auswählen.
3. Wählen Sie **Jetzt ausführen**.

   Hinweis:
   Jede Projektversion der Integrationen soll einen möglichst vollständigen Datenabruf ermöglichen. Das Ausführen dieser Integrationen in falscher Reihenfolge kann zu unvollständigen Daten führen und erfordert Fachwissen über ServiceNow und Application Vulnerability Response.

   Nachdem der Import abgeschlossen ist, können Sie die verschiedenen Versionen eines Projekts in der Tabelle „Erkannte Anwendungen“ [sn_vul_release] anzeigen. Wenn Sie CI-Suchregeln verwenden, sind diese erkannten Anwendungen mit der Tabelle „Configuration Item“ [cmdb_ci] verknüpft.
4. Zeigen Sie den Status Ihrer Integrationsausführungen an.
   Weitere Informationen finden Sie unter Zeigen Sie den Ausführungsstatus des Imports Vulnerability Response-Integration mit Black Duck an.

Importieren Sie die angreifbaren Anwendungselemente aus dem Vulnerability Response-Integration mit Black Duck

Importieren Sie die angreifbaren Elemente der Anwendung (Application Vulnerability Items, AVIs) aus der Vulnerability Response-Integration mit Black Ente, damit die Integration sequenziell ausgeführt wird. Eine erfolgreiche Integration hilft Ihnen, die AVIs zu identifizieren und zu erfassen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Scan-Ergebnisse aus Vulnerability Response-Integration mit Black Duckanzeigen, AVIs in Ihre Instanz einfügen und Ihre Drittpartei-Schwachstellendaten ergänzen. Standardmäßig werden keine AVIs erstellt, wenn sich der Scanner-Datensatz im Status „Geschlossen“ befindet. Sie können vorhandene AVIs mithilfe der Eigenschaft „sn_vul_create_closed“ steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Black Duck-Schwachstellen-Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
   Sie können beispielsweise **Black Duck Application Vulnerable Item Integration**auswählen.
3. Wählen Sie **Jetzt ausführen**.

Hinweis:
Vulnerability Response-Integration mit Black Duck soll Ihnen den vollständigsten Datenabruf ermöglichen. Das Ausführen dieser Integrationen in falscher Reihenfolge kann zu unvollständigen Daten führen und erfordert das Fachwissen von ServiceNow und Application Vulnerability Response.

Nachdem Sie alle SCA-Schwachstellen aus Vulnerability Response-Integration mit Black Duckimportiert haben, können Sie die AVIs und die Schwachstellendaten von Drittparteien anzeigen.

Legen Sie die Importzeiten für fest Vulnerability Response-Integration mit Black Duck

Legen Sie die Startzeit für die Vulnerability Response-Integration mit Black Duck -Importe fest. Sie können die Integrationen vorab festlegen, um eine bessere Leistung und schnellere Importausführungen zu erzielen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import führen die Black Duck-Schwachstellen-Integrationen bei jeder Ausführung einen vollständigen Import durch.

Prozedur

1. Navigieren zu **Alle** > **Black Duck-Schwachstellen-Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Legen Sie die neue **Startzeit**fest.
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für Importe der Black Duck-Anwendungslistenintegration ist 00:00:00. Die anderen Integrationen sind **bei Bedarf verfügbar** und verkettet. Dies bedeutet, dass sie einer bestimmten Reihenfolge folgen, um nach der Black-Duck-Anwendungslisten-Integration ausgeführt zu werden. Das Ändern der **Startzeit** erfordert fortgeschrittene Kenntnisse über ServiceNow und Application Vulnerability Management.
4. Wählen Sie **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

Schließt angreifbare Elemente der Black-Duck-Anwendung ein

Schließen Sie geschlossene angreifbare Elemente in der Anwendung (Application Vulnerable Items, geschlossene Anwendungselemente) bei Importen der Black Duck-Integration für angreifbare Elemente ein, da sie standardmäßig nicht während der Integrationsimporte erstellt werden. Wenn Sie sie erstellen möchten, müssen Sie die Systemeigenschaft ändern.

Vorbereitungen
Stellen Sie sicher, dass Vulnerability Response-Integration mit Black Duck installiert ist und ausgeführt wird.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein.
2. Geben Sie im Feld **Name** für die Liste sn_vul.create_closedein.
3. Doppelklicken Sie auf das Feld **Wert**, und setzen Sie es auf **true**
4. Speichern Sie, indem Sie das grüne Häkchen-Symbol .
   Die Datensätze im Status „Geschlossen“ im nächsten Black-Duck-Import werden als AVIs in Application Vulnerability Responseerstellt.

Fortify Vulnerability Integration

Fortify Vulnerability Integration verwendet Daten, die aus dem Produkt Fortify importiert wurden, um Ihnen zu helfen, die Auswirkungen und Priorität von Fehlern in Ihrem Code zu bestimmen.

Fortify Vulnerability Integration

Das Produkt Fortify sammelt Scannerdaten und stellt diese Daten dem Now Platform®zur Verfügung. Es lässt sich problemlos in die Funktion ServiceNow® Application Vulnerability Response von Vulnerability Response integrieren, um Schwachstellen von Drittparteien abzubilden, die die Daten in Ihrer -Instanz ergänzen.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Geplante Aufgaben rufen die Integrationen jeden Tag automatisch auf. Sobald alle Integrationen aktiviert sind, werden sie so verkettet, dass sie der Reihe nach ausgeführt werden. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Integration von Vulnerability Response mit Fortify v2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Fortify Vulnerability Integration

Um Fortify Vulnerability Integrationanzuzeigen, navigieren Sie zu **Fortify-Schwachstellenintegration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig nicht alle aktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um die Integrationen automatisch der Reihe nach auszuführen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Fortify Integrationen für Schwachstellen

Integration	Beschreibung
Fortify Integration der Anwendungsliste bei Bedarf	Ruft Fortify Anwendungsscannerdaten (Schwachstellen, Metadaten) ab und erweitert Ihre Drittanbieteranwendungsdaten. Diese Integration wird täglich um 00:00:00 Uhr ausgeführt. Sie ist standardmäßig aktiviert.
Fortify Integration der Zusammenfassungsscans bei Bedarf	Ruft Scan-Datensätze von Fortifyab. Diese Integration ist so verkettet, dass sie nach Fortify bei der Integration der bedarfsgesteuerten Anwendungsliste ausgeführt wird, wenn sie aktiviert ist. Standardmäßig ist es inaktiv.
Fortify Integration von angreifbaren Elementen einer Anwendung bei Bedarf	Ruft Scan-Ergebnisse von Fortifyab, fügt AVITs ein und erweitert Ihre Drittpartei-Schwachstellendaten. Wenn sich der Scanner-Datensatz im Status **„Geschlossen“** befindet, werden keine AVITs erstellt. Vorhandene AVITs werden weiterhin aktualisiert. Ab v2.3 können Sie Detailinformationen wie Gesamtverarbeitungszeiten, Durchschnittszeiten für Prozesse vor und nach der Integration und Berichte zu den Integrationsausführungsdatensätzen für die Integration von angreifbaren Anwendungselementen anzeigen. Diese Integration ist so verkettet, dass sie nach der Fortify on Demand Scan Summary Integration ausgeführt wird, wenn sie aktiviert ist. Standardmäßig ist es inaktiv.

Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus des Imports Fortify Vulnerability Integration an.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

Vorbereitung auf das Fortify Vulnerability Integration

Ein erfolgreiches Fortify Vulnerability Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Bei Fortify Vulnerability Integration wird davon ausgegangen, dass Sie mit dem Produkt und der API Fortify vertraut sind.

Vorbereitungen

Die Integration mit der Common Weakness Enumeration (CWE) wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration von Fortify Vulnerability Integrationausgeführt werden.

Hinweis:
Daten der NIST Vulnerability Database (NVD) sind für die Installation von Fortify Vulnerability Integrationnicht erforderlich. Sie stellen jedoch eine Ergänzung dar und wären nützlich.

Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validiert die Dimensionierung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die importiert werden sollen. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Für Fortify Vulnerability Integration sind ein API-Schlüssel, ein API-Geheimnis und eine API-Stamm-URL erforderlich, die in Ihrem Konto Fortify bei Bedarf verfügbar sind.

Prozedur

So erstellen Sie einen geheimen API-Schlüssel:

a. Melden Sie sich bei Ihrem Fortify on Demand-Portal an.

b. Navigieren zu **Alle** > **Administration** > **Einstellung** > **API**.

c. Fügen Sie ServiceNow als Anwendung hinzu.

d. Klicken Sie auf **Neues Geheimnis**, um ein API-Geheimnis zu generieren.

e. Notieren Sie Ihr API-Geheimnis zur späteren Verwendung.

ServiceNow® Vulnerability Response Integration mit Fortifyinstallieren

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Fortify ordnungsgemäß in Application Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen sind, installiert der Systemadministrator [admin] die Anwendung und weist der App-Sec-Manager-Gruppe Benutzer zu. Informationen zu Gruppenrollen finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen. • Die App-Sec-Managergruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie Fortify Vulnerability Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Vulnerability Response Integration with Fortify.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Nächste Maßnahme

Konfigurieren Sie Fortify Vulnerability Integration für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration.

Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit das Produkt Fortify ordnungsgemäß

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in die Funktion Application Vulnerability Response von Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Stellen Sie sicher, dass die Anwendung Vulnerability Response Integration with Fortify installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie ServiceNow Vulnerability Response Integration mit Fortifyinstallieren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen sind, installiert der Systemadministrator [admin] die App und weist der App-Sec-Manager-Gruppe Benutzer zu. • Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
Halten Sie für Fortify Vulnerability Integrationlhre **API-ID** und **Ihren API-Schlüssel** bereit.	Wenden Sie sich an Fortify, um die **API-ID** und **den API-Schlüssel**zu erhalten.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie die Anwendungsschwachstellen-Integrationen Fortify installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Vulnerability Response integration with Fortify.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.
11. Navigieren Sie nach Abschluss der Installation zu **Fortify-Schwachstellenintegration** > **FoD-Konfiguration**.
12. Füllen Sie die Felder des Formulars aus.

Fortify on Demand-Konfigurationsformular

Feld	Beschreibung
API-Stamm-URL	Fortify-Instanz-URL des Anwenders.
API Key	Eindeutiger Bezeichner, der an die Fortify -API gesendet wird.
Geheimer API-Schlüssel	Von Fortifybereitgestellter geheimer Clientschlüssel.
DAST einbeziehen	Option zum Einbeziehen von Schwachstellen aus DAST-Scans. DAST-Scans identifizieren Schwachstellen im Verhalten der gesamten Anwendung.
SAST einbeziehen	Option zum Einbeziehen von Schwachstellen aus SAST-Scans. SAST-Scans identifizieren Schwachstellen im Code.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Selektierung von Ausnahmen und falsch positiven Meldungen in ServiceNow (ab v20.0 von Vulnerability Response)	Wählen Sie Optionen aus, um die Workflows „Ausnahmeverwaltung“ und „Falsch positiv“ für AVIs mit ServiceNow beim Import automatisch zu verwalten. Diese Optionen sind standardmäßig aktiviert. Ein Beispiel für einen Anwendungsfall finden Sie unter Verwalten der Statuszuordnung für Zurückstellungen und falsch positive Meldungen in Application Vulnerability Response. **Verwalten Sie Ausnahmen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte AVIs, die für den Status „ **Zurückgestellt“** markiert sind, selektieren möchten. AVIs mit **Quellstatus**, die in Ihrer Instanz normalerweise einem Status **„Zurückgestellt“** zugeordnet sind, werden stattdessen „ **Offen“**zugeordnet. Sie **fordern eine Ausnahme aus dem AVI-Datensatz an**. **Verwalten Sie falsch positive Meldungen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte AVIs mit **Quellstatus**, die als **Falsch positiv** oder **Potenziell falsch positiv**markiert sind, selektieren möchten. AVIs mit diesen **Quellstatus**, die in Ihrer Instanz normalerweise einem Status **„Geschlossen“** zugeordnet sind, werden **Offen**zugeordnet. Sie fordern ein **Falsch positives Ergebnis** aus dem AVI-Datensatz an. ○ Deaktivieren Sie eines oder beide Kontrollkästchen, wenn Sie die von Ihrem Scanner importierten **Quellstatus** beibehalten möchten. ○ Diese AVIs werden beim Import den Zielstatus und Zielgrundstatus zugeordnet, werden jedoch nicht von den Ausnahme- und falsch positiven Workflows selektiert. Die Aktionen **„Ausnahme anfordern“** und **„Falsch positiv“** sind in AVIs nicht sichtbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Selektierung in ServiceNow (vor v20.0 von Vulnerability Response)	Verwalten Sie die Selektierung von Anwendungsschwachstellen in Instanz ServiceNow : ○ Aktivieren Sie das Kontrollkästchen, um die AVIs in ServiceNowzu selektieren. Wenn diese Option ausgewählt ist, werden AVIs im Status „Offen“ importiert. Sie können dann eine Ausnahme anfordern oder die AVI als falsch positiv markieren. ○ Um den Quellstatus beizubehalten, also den vom Scanner importierten Status, stellen Sie sicher, dass das Kontrollkästchen nicht aktiviert ist. **Hinweis:** Die Optionen **„Als falsch positiv markieren“** und **„Ausnahme anfordern“** sind nur für AVIs verfügbar, die innerhalb von ServiceNowselektiert werden.

13. Wählen Sie **Anmeldeinformationen speichern und testen aus**.

Nächste Maßnahme

Wenn Ihre Umgebung domänengetrennte Importe erfordert, lesen Sie unter Erstellen Sie domänengetrennte Importe für eine Integrationnach.

Weitere Anweisungen zur Erstinstallation finden Sie unter Application Vulnerability Response konfigurieren.

Änderungen nach der Erstinstallation finden Sie unter Fortify Vulnerability Integration Änderung und Aktivitäten.

Zeigen Sie den Ausführungsstatus des Imports Fortify Vulnerability Integration an

Verwenden Sie die zugehörige Liste **„Integrationsausführungen für Schwachstellen“,** um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Nachbesserungsentscheidungen zu treffen.

Vorbereitungen

So zeigen Sie den Ausführungsstatus des Imports Fortify an:

- Die Anwendungen Vulnerability Response und Fortify Vulnerability Integration müssen installiert und konfiguriert sein.
- Die Fortify Vulnerability Integration -Importe müssen geplant sein und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Application Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf die zugehörige Liste **Integrationsausführungen für Schwachstellen**.
4. Stellen Sie sicher, dass alle Importe erfolgreich waren.
5. Ab v2.3 können Sie Detailinformationen wie Gesamtverarbeitungszeiten, Durchschnittszeiten für Prozesse vor und nach der Integration und Berichte zu Integrationsausführungsdatensätzen für Integrationen von angreifbaren Anwendungselementen anzeigen.

Fortify Vulnerability Integration Änderung und Aktivitäten

Konfigurieren Sie optionale Änderungen speziell für Fortify Vulnerability Integration.

Hinweis:
Das Ändern anderer Fortify Vulnerability Integration -Einstellungen, die nicht die hier aufgeführten sind, erfordert fortgeschrittene Kenntnisse ServiceNow von und Application Vulnerability Response und liegt außerhalb des Umfangs der Produktdokumentation.

Führen Sie einen manuellen Fortify Import von Anwendungsschwachstellen durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie unabhängig von der täglichen geplanten Aufgabe einen vollständigen Datenimport durchführen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus, z. B. Fortify Application List Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Jetzt ausführen**.

> **Hinweis:**
> Um einen vollständigen Datenabruf zu erhalten, führen Sie die Fortify-Anwendungsschwachstellen-Integrationen nacheinander aus.

Importieren Sie Daten mit Fortify Vulnerability Integration

Importieren Sie Daten aus dem Fortify-Scanner, um angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIs) zuzuordnen und dadurch die Daten in Ihrer Instanz zu ergänzen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import führen Fortify Schwachstellen-Integrationen bei jeder Ausführung einen Delta-Import durch und rufen die aktuellen Daten ab. Weitere Informationen zu vollständigen Importen finden Sie unter Führen Sie einen manuellen Fortify Import von Anwendungsschwachstellen durch.

Prozedur

1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Name der Integrationsausführung.
Aktiv	Option zum Aktivieren einer Integration.
Ausführen	Häufigkeit der Integrationsausführung.
Zeit	
Anwendung	Anwendung, die diesen Datensatz enthält.
Quellenintegration	Quellintegration für diese Integration.
Quellinstanz	Quellinstanz für diese Integration.
Nächste Integration	Integration in nächster Reihenfolge, die nach der aktuellen Integration ausgeführt werden soll.
Startzeit	Startdatum und -uhrzeit der letzten erfolgreichen Integrationsausführung. Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für die erste Ausführung ist 00:00:00.
Integrationsdetails	
Integrationsskript	Skripteinbindung, die `VulnerabilityIntegrationBase` für die Ausführung erweitert, wenn die Integration ausgeführt wird. Dieses Skript definiert, wie Daten aus einem Drittparteisystem abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Integrationswerksskript	Skript, das definiert, wie die für das Integrationsskript ausgewählte Skripteinbindung erstellt wird.
Berichtsprozessorstrategie	Strategie, die Sie für die Verarbeitung der vom Integrationsskript zurückgegebenen Daten verwenden möchten, wenn die Integration ausgeführt wird.

4. Wählen Sie **Jetzt ausführen aus**, um die Integration auszuführen.

Schließt angreifbare Elemente der Anwendung „Fortify on Demand“ in der geschlossenen Anwendung ein

Standardmäßig werden **geschlossene** angreifbare Anwendungselemente (Application Vulnerable Items, AVITs) nicht während Importen der Integration von Fortify angreifbare Elemente erstellt. Wenn Sie sie erstellen möchten, müssen Sie eine Systemeigenschaft ändern.

Vorbereitungen

Fortify Vulnerability Integration muss installiert sein und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Geben Sie im Textfeld **des Filternavigators** für die Navigation auf der linken Seite sys_properties.listein.
2. Geben Sie im **Namenssuchfeld** für die Liste sn_vul.create_closedein.
3. Doppelklicken Sie auf das Feld **Wert**, und setzen Sie es auf **Wahr**
4. Klicken Sie auf das grüne Häkchen-Symbol um zu speichern.
   Datensätze im Status **„Geschlossen“** im nächsten Import Fortify werden als AVITs in Application Vulnerability Responseerstellt.

GitHub-Anwendungsschwachstellen-Integration

GitHub-Anwendungsschwachstellen-Integration importiert SAST-Daten (Static Application Security Testing) und SCA-Daten (Software Composition Analysis), um Sie bei der Anzeige von Schwachstellenwarnungen in den Repositorys in Ihrer GitHub -Umgebung zu unterstützen.

GitHub-Anwendungsschwachstellen-Integration

GitHub-Anwendungsschwachstellen-Integration sammelt Scannerdaten und stellt diese Daten dem Now Platform®zur Verfügung. Es lässt sich problemlos in die Funktion ServiceNow® Application Vulnerability Response von Vulnerability Response integrieren, um Schwachstellen von Drittparteien und Warnungen GitHub von in Ihrer -Instanz zuzuordnen.

Die Umgebung GitHub unterstützt mehrere Organisationen. Diese Organisationen, sowohl lokale als auch Enterprise-Organisationen, können verschiedene Abteilungen enthalten, z. B. Engineering, Qualität, Dokumentation usw. Jede Organisation kann wiederum mehrere Repositorys unterstützen. Nachdem Sie Ihre Anwendungsdaten mit der Repository-Integration GitHub importiert haben, können Sie Schwachstellen- und Warnungsdaten aus diesen Repositorys importieren. Importierte Daten werden wie eine -Anwendung in der Anwendung Application Vulnerability

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Response verarbeitet. Wenn Scanner Schwachstellen erkennen und Warnungen für die Repositorys generieren, werden in Application Vulnerability ResponseSchwachstellen erstellt.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
GitHub-Anwendungsschwachstellen-Integration v1.2, v1.1, 1.0	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

GitHub-Integrationen

Integration	Beschreibung
GitHubOrganisationsintegration	Diese Integration importiert die Organisationen, die zu einem bestimmten Unternehmen gehören, das bei der Konfiguration von GitHub aufgeführt wurde. Alle Organisationen werden in die mit diesem Release eingeführte Tabelle „sn_vul_discovered_org“ (Erkannte Organisationen) eingetragen. Diese Integration unterstützt die APIs der Enterprise-Ebene.
GitHub Repository-Integration	Importieren Sie ab v1.1 alle Anwendungsdaten für Ihre GitHub lokalen und Cloud (Enterprise)-Accounts. Die Integration importiert Anwendungen aus den Repositorys, die Sie für eine Organisation (lokal) oder aus Ihrer Enterprise-Umgebung (Cloud) konfiguriert haben. Führen Sie diese Integration aus, bevor Sie die anderen GitHub Integrationen ausführen, da sie von den aktuellen Anwendungsdaten abhängen, die aus der Repository-Integration importiert wurden.
GitHub CodeScan-Integration	Ruft Schwachstellenwarnungen für Code-Scans aus Repositorys GitHub für Sicherheitsschwachstellen und Codierungsfehler ab. Importierte Daten werden SAST-Ergebnissen in Ihrer Instanz zugeordnet.
GitHub Dependabot-Integration	Ruft Dependabot-Warnungen für Abhängigkeiten mit bekannten Schwachstellen aus Repositorys ab. Importierte Daten werden in Ihrer Instanz den SCA-Ergebnissen zugeordnet.
GitHub Geheimes Scannen	Ruft Geheimnisse aus dem Code Ihrer Organisation zusammen mit den Ergebnissen der Anwendungssicherheitstests ab. Die Daten werden den SCA-Ergebnissen in Ihrer -Instanz zugeordnet.
GitHub Geheimer Scan-Speicherort	Ruft den Speicherort und die Zeilennummern für die gescannten Geheimnisse im Code Ihrer Organisation ab, um Ihre Entwickler bei der Korrektur zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SBOM -Dateien werden aus Ihren GitHub -Repositorys in Now Platform® hochgeladen

Stellen Sie fest, ob die in Ihren CI/CD-Pipelines (kontinuierliche Integration und kontinuierliche Bereitstellung/Bereitstellung) generierten Dateien SBOM erfolgreich in der Instanz Now Platform® in die Warteschlange gestellt wurden.

- Schützen Sie Ihre Umgebungen während Software-Entwicklungszyklen mit GitHub -Aktionen, die Sie in Ihrer GitHub -Umgebung initiieren, vor potenziell schädlichen Komponenten.
- Rufen Sie alle erforderlichen GitHub -Aktionen für den Upload von SBOM im GitHub-Marketplace ab.

Die SBOM -Anwendungen sind erforderlich, um SBOM -Dateien hochzuladen. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Importierte Daten werden angezeigt

Importierte Anwendungsdaten aus der Repository-Integration GitHub werden in der Tabelle „Erkannte Anwendungen“ [sn_vul_app_release] angezeigt. Führen Sie diese Integration zuerst aus.

Die Repository-Integration importiert Tags und Themen, die Sie für ein Repository in Ihrem Konto GitHub aus dem Menü „Einstellungen“ konfiguriert haben. Anwenderdefinierte Eigenschaften befinden sich im Menü unter Ihrem Repository. Die von Ihnen für die Eigenschaften festgelegten Werte werden als Schlüssel-Wert-Paare importiert. Weitere Informationen dazu, wo Sie diese Informationen in Ihrer Instanz anzeigen können, finden Sie unter Zeigen Sie den Ausführungsstatus des Imports GitHub-Anwendungsschwachstellen-Integration und die importierten Repository-Daten an.

Importierte Daten (Ergebnisse) aus der Dependabot-Integration GitHub werden in den folgenden Tabellen angezeigt.

- Erkannte Anwendungen [sn_vul_app_release].
- Zusammenfassungen von Anwendungsschwachstellen-Scans [sn_vul_app_vul_scan_summary].
- Angreifbare Anwendungselemente [sn_vul_app_vulnerable_item]
- Pakete [sn_vul_app_package]

Importierte Daten aus der GitHub CodeScan Integration werden in den folgenden Tabellen angezeigt.

- Erkannte Anwendungen [sn_vul_app_release].
- Zusammenfassungen von Anwendungsschwachstellen-Scans [sn_vul_app_vul_scan_summary].
- Anwendungsschwachstelleneinträge [sn_vul_app_vul_entry]
- Angreifbare Anwendungselemente [sn_vul_app_vulnerable_item]

Vorbereitung auf das GitHub-Anwendungsschwachstellen-Integration

Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. GitHub-Anwendungsschwachstellen-Integration setzt voraus, dass Sie mit dem Produkt und der API GitHub vertraut sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Erforderliche Rollen:

- -Administrator zum Herunterladen, Installieren und Aktivieren von Anwendungen und Zuweisen von Rollen.
- GitHub-Administrator, der in der GitHub-Konsole Anmeldeinformationen abruft und Token generiert.
- -Administrator zum Einrichten von Verbindungen und Aliasdatensätzen in Ihrer Instanz.

Setupaufgaben

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass GitHub-Anwendungsschwachstellen-Integration installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Installieren Sie ServiceNow GitHub-Anwendungsschwachstellen-Integration.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen sind, installiert der Systemadministrator [admin] die App und weist Benutzer der Benutzergruppe „App-Sec Manager“ zu. • Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. • „sn_vul_github_config_integration“ wird von der Benutzergruppe „App-Sec-Manager“ geerbt. Diese Rolle enthält die Rollen connection_admin und oauth_admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben (Fortsetzung)

Setupaufgaben	Beschreibung
Rufen Sie Ihre GitHub-Anmeldeinformationen und -Kontoinformationen ab.	In Datensätzen, die Sie für die Authentifizierung erstellen, sind Accountinformationen erforderlich. Unter Erstellen von OAuth 2.0-Anmeldeinformationen für GitHub Apps – JWT für GitHub-Anwendungsschwachstellen-Integration finden Sie weitere Informationen zu den von Ihnen benötigten Details und zum Einrichten der erforderlichen Datensätze für die OAuth-Authentifizierung.
Vergewissern Sie sich, dass Sie Daten der Common Weakness Enumeration (CWE) importieren.	Die Common Weakness Enumeration (CWE)-Integration wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration der GitHub-Schwachstellenintegration ausgeführt werden. Es wird standardmäßig mit Vulnerability Responseinstalliert. **Hinweis:** Daten der NIST Vulnerability Database (NVD) sind für die Installation der GitHub Vulnerability-Integration nicht erforderlich, bieten jedoch Ergänzungen und wären nützlich. Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

Erstellen von OAuth 2.0-Anmeldeinformationen für GitHub Apps – JWT für GitHub-Anwendungsschwachstellen-Integration

Führen Sie die folgenden Schritte aus, um Ihre GitHub -Apps mit dem JWT-Bearer-Token für GitHub-Anwendungsschwachstellen-Integrationzu integrieren.

Erforderliche Rollen:

- sn_vul.app_sec_manager und admin für Datensätze in Ihrem Now Platform.
- Für Aufgaben in Ihrem Account GitHub ist keine Instanzrolle erforderlich.
- Weitere Informationen zum Kontext der Schritte für dieses Setup finden Sie unter OAuth 2.0-Protokoll .

App GitHub für GitHub-Anwendungsschwachstellen-Integrationerstellen und konfigurieren

Erstellen Sie eine anwenderdefinierte GitHub App von Ihrem Konto GitHub, um die OAuth 2.0-Authentifizierung mit Ihrem GitHub-Anwendungsschwachstellen-Integration in Ihrer -Instanz zu aktivieren.

Vorbereitungen
Erforderliche Rolle: Keine Instanzrolle erforderlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie diese Schritte in Ihrem Konto GitHub aus. Siehe Gebäude GitHub Apps Auf der Developer Site GitHub finden Sie Anweisungen zum Erstellen und Konfigurieren benutzerdefinierter Anwendungen.

Prozedur

1. Erstellen Sie in Ihrem Konto GitHub Ihre App GitHub, indem Sie zu navigieren **Entwicklereinstellungen** > **GitHub-Apps**.
2. Geben Sie im Feld **Homepage-URL**den Wert https://ein.<instance-name> .service-now.com .
3. Geben Sie im Feld **Rückruf-URL für Anwenderautorisierung**den Wert https://ein.<instance-name> .service-now.com/oauth_redirect.do
4. Deaktivieren Sie im Abschnitt **„Identifizieren und Autorisieren von Anwendern“** das Feld **Anwenderautorisierungstoken ablaufen lassen**.
5. Wählen Sie im Abschnitt **„Webhook“** das Feld **Aktiv** aus.
6. Geben Sie im Feld **Webhook-URL**https://instanzname>.service-now.com/ein.
7. Lassen Sie die verbleibenden Felder leer (Standard).
8. Konfigurieren Sie im Abschnitt **Repository-Berechtigungen** die folgenden Einstellungen.

Scannen von Code	Schreibgeschützt
Inhalt	Schreibgeschützt
Anwenderdefinierte Eigenschaften	Schreibgeschützt
Dependabot-Warnungen	Schreibgeschützt
Metadaten	Schreibgeschützt
Geheime Scan-Warnungen	Schreibgeschützt

Hinweis:
Wenn Sie bereits eine GitHub-App verwenden und Berechtigungen aktualisieren, müssen Sie diese Berechtigungen für Ihre GitHub-App überprüfen und akzeptieren. Sie können zu Ihrer App navigieren und **„Konfigurieren > Anforderung überprüfen > Neue Berechtigungen akzeptieren“**auswählen.

9. Belassen Sie die verbleibenden Berechtigungen als Kein Zugriff (Standard).
10. Wählen Sie im Abschnitt **„Ereignisse abonnieren“** die Option **Bereitstellungsschutzregel** aus.
11. Klicken Sie mit der rechten Maustaste in den Header, um die Änderungen zu speichern.
12. Installieren Sie die neu erstellte App GitHub auf den Konten Ihrer Wahl.
    a. Wählen Sie auf der Einstellungsseite für GitHub-Apps Ihre App aus.
    b. Wählen Sie in der linken Sidebar **App installieren**aus.
    c. Wählen Sie **Installieren** neben der Organisation oder dem persönlichen Account, die das richtige Repository enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Installieren Sie die App in allen Repositorys oder wählen Sie Repositorys aus.
Weitere Informationen finden Sie unter GitHub-Apps installieren .

13. Wählen Sie nach der Installation die Einstellungen (Zahnradsymbol) für Ihre App aus, und notieren Sie die folgenden Informationen.

Diese Details sind erforderlich, wenn Sie die Anwendungsregistrierung in Ihrer Instanz Now Platform erstellen.

- App-ID
- Client-ID
- Geheimer Clientschlüssel.
- Beachten Sie das Token in der URL. Dies ist die Token-ID, die Sie in der Token-URL in Ihrer Instanz eingeben.

14. Scrollen Sie auf der Seite nach unten, generieren Sie einen neuen privaten Schlüssel, und speichern Sie ihn auf Ihrem Computer.

Generieren Sie das JKS-Zertifikat für das GitHub-Anwendungsschwachstellen-Integration

Generieren Sie ein JKS-Zertifikat für die JWT-Authentifizierung für GitHub-Anwendungsschwachstellen-Integration.

Vorbereitungen

Sie müssen sich das Passwort merken, das Sie zum Generieren der .jks-Datei (KeyStore-Passwort) verwenden.

Erforderliche Rolle: sn_vul.app_sec_manager

Prozedur

1. Erstellen Sie ein CA-signiertes Zertifikat mit dem privaten Schlüssel der App GitHub :

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem -days 1095
```

2. Geben Sie die erforderlichen Details ein.
3. Erstellen Sie die PKCS 12-Datei mit dem privaten App-Schlüssel GitHub und dem CA-signierten Zertifikat:

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey <file-name>.pem -certfile
 <certificate-name>.pem -out <PKCS-12-file-name>.p12
```

4. Geben Sie das Exportpasswort an.
5. Erstellen Sie die JKS-Datei:

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12 -srcstoretype pkcs12
 -destkeystore <JKS-certificate-filename>.jks -deststoretype JKS
```

6. Geben Sie die Passwörter für Ziel- und Quell-Schlüsselspeicher an.

Fügen Sie Ihrer Instanz das Java-Schlüsselspeicher-Zertifikat GitHub für GitHub-Anwendungsschwachstellen-Integrationhinzu.

Aktivieren Sie die JWT-Bearer-Grant-Token-Authentifizierung, indem Sie das gültige GitHub Java KeyStore-Zertifikat (JKS) an Ihre -Instanz anhängen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Ein gültiges Java KeyStore-Zertifikat

Erforderliche Rolle: sn_vul.app_sec_manager

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formularfelder „X.509-Zertifikat“.

Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des Datensatzes. Beispiel: My GitHub App Certificate for AVR (Mein GitHub-App-Zertifikat für AVR).
Benachrichtigung bei Ablauf	Option zum Festlegen der Benutzer, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage zum Senden einer Benachrichtigung, bevor das Zertifikat abläuft.
Aktiv	Option zum Aktivieren des -Zertifikats.
Typ	Option zum Auswählen des Zertifikattyps. Wählen Sie **Java Key Store**aus.
Läuft in Tagen ab	Anzahl der Tage, bis das Zertifikat abläuft.
Schlüsselspeicher-Passwort	Dem Zertifikat zugeordnetes Passwort (Hinweis: das zuvor erstellte Ziel-KeyStore-Passwort).
Kurzbeschreibung	Zusammenfassung des Zertifikats.

4. Wählen Sie das Anhangsymbol, und hängen Sie ein JKS-Zertifikat an.
5. Wählen Sie **Speicher/Zertifikate validieren aus**.
   Für gültige Zertifikatdateien wird die Meldung Valid key_store (Gültiger Schlüsselspeicher) angezeigt.

Einen JWT-Signaturschlüssel für das JKS-Zertifikat GitHub für das GitHub-Anwendungsschwachstellen-Integrationerstellen

Erstellen Sie einen JSON-Web-Token-Signaturschlüssel (JWT), um ihn Ihrem GitHub Java KeyStore-Zertifikat zuzuweisen.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.app_sec_manager

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Schlüssel**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder „JWT-Schlüssel“.

Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des JWT-Signaturschlüssels. Beispiel: Mein GitHub-App-JWT-Schlüssel für AVR.
Signatur-Schlüsselspeicher	Wählen Sie das Gültige JKS-Zertifikat aus, das Sie in der vorherigen Aufgabe angehängt haben.
Schlüssel-ID	Lassen Sie dieses Feld leer.
Signaturalgorithmus	Behalten Sie diesen Wert als RSA 256 bei.
Signaturschlüssel-Passwort	Passwort, das dem Signaturschlüssel zugeordnet ist. Dies ist das Passwort, das Sie zum Generieren der JKS-Datei verwendet haben.
Aktiv	Option zum Aktivieren des Schlüssels.

4. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im grauen Header der Seite, und wählen Sie **Speichern**aus.

Einen JWT-Provider für Ihren GitHub -Signaturschlüssel für GitHub-Anwendungsschwachstellen-Integrationerstellen

Fügen Sie Ihrer -Instanz ServiceNow für GitHubeinen JSON-Web-Token-Provider (JWT) hinzu.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.app_sec_manager

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Anbieter**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formularfelder des JWT-Providers

Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des JWT-Anbieters. Beispiel: Mein GitHub-App-JWT-Provider für AVR.
Ablaufintervall (Sek.)	Anzahl in Sekunden zum Festlegen der Lebensdauer von JWT-Anbieter-Token. Sie können diese Einstellung auf Standard belassen.
Signierkonfiguration	Wählen Sie den JWT-Schlüssel aus, den Sie in den vorherigen Schritten erstellt haben.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und wählen Sie **Speichern**aus.
5. Geben Sie Ihre GitHub App- **App-ID** für den Wert des **iss** -Anspruchs in der zugehörigen Liste „Standardansprüche“ ein.
   Dies ist die App-ID der App GitHub in Ihrer GitHub -Konsole, die Sie in den vorherigen Schritten erstellt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. **Aud-** und **Sub-** Werte leer lassen (Standard).
7. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und wählen Sie **Speichern**aus.

Registrieren Sie GitHub als OAuth-Provider (JWT) für den GitHub-Anwendungsschwachstellen-Integration

Verwenden Sie die Informationen, die während der Konfiguration des App-Accounts GitHub von generiert wurden, um GitHub als OAuth-Anbieter zu registrieren und der Instanz die Anforderung von OAuth 2.0-Token zu gestatten.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.app_sec_manager

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**.
2. Wählen Sie **Neu**.
   Die Frage **Welche Art von OAuth-Anwendung?** Meldung wird angezeigt.
3. Wählen Sie **Verbindung zu einem fremden OAuth-Provider herstellen** aus.
4. Füllen Sie die Felder des Formulars aus.

Formularfelder „Anwendungsregistrierung“.

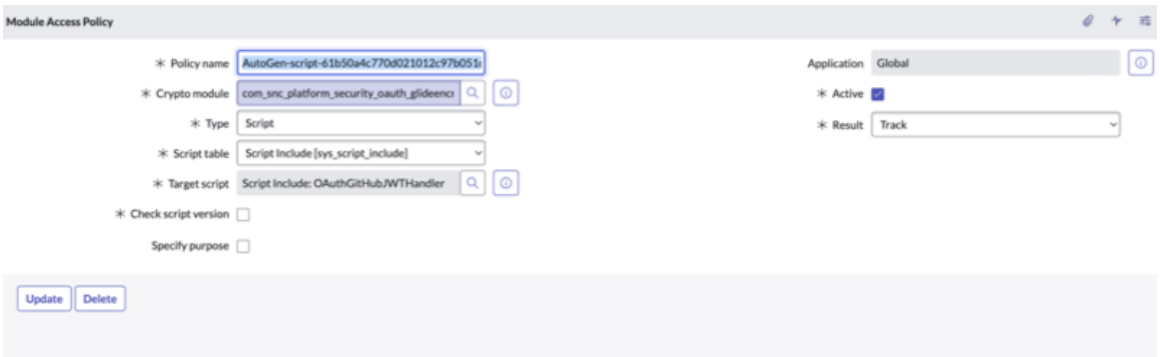
Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des Datensatzes. Geben Sie beispielsweise My GitHub App Provider for AVRein.
Client-ID	Client-ID Ihrer GitHub -App. Die Client-ID stammt aus der Anwendung GitHub in Ihrer Konsole GitHub, die Sie in den vorherigen Schritten erstellt haben. Diese ID ist im Abschnitt **„Info“** Ihrer GitHub App-Konfiguration in GitHubverfügbar.
Zugänglich	Behalten Sie den aktuellen Wert für diese Einstellung bei.
Geheimer Clientschlüssel	Geheimer Clientschlüssel Ihrer App GitHub. Der geheime Clientschlüssel stammt aus der Anwendung GitHub in Ihrer GitHub -Konsole, die Sie in den vorherigen Schritten erstellt haben. Diese ID ist im Abschnitt **„Info“** Ihrer GitHub App-Konfiguration in GitHubverfügbar.
Aktiv	Option zum Aktivieren des Schlüssels. Lassen Sie dies ausgewählt.
Autorisierungs-URL	Diese URL wird automatisch generiert.
Token-URL	Die Position des Tokenendpunkts, den die Instanz zum Abrufen und Aktualisieren von Token verwendet. Geben Sie das Token aus der URL in Ihrer App GitHub ein. Dies ist das Token, das in der URL angezeigt wird, nachdem Ihre App in GitHubinstalliert wurde. Wählen Sie im Abschnitt „App installieren“ in Ihrer GitHub-App-Konfiguration in GitHubdas Zahnrad aus. Das Token wird in der Webseiten-URL angezeigt. ○ Für Cloud: https://api.github.com/app/installations/49374672/access_tokens . Installations-ID: 9374672 ○ Für lokale: https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

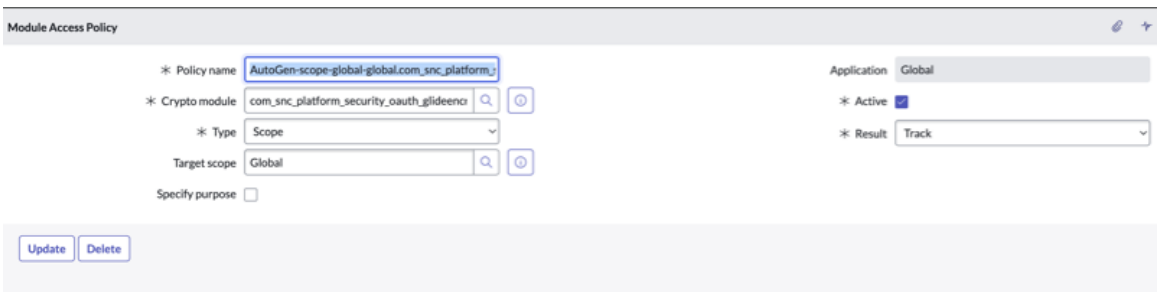
Feld	Beschreibung
OAuth-API-Skript	Option, mit der Sie auf eine geänderte OAuthUtil-Skripteinbindung verweisen können. Wählen Sie **OAuthGitHubJWTHandler**aus.
Standardgewährungstyp	Typ der Erteilung, die der Anwendungsregistrierung zugeordnet ist. Wählen Sie **JWT Bearer**aus.

5. Behalten Sie für die restlichen Formularfelder den Standardwert bei.
6. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und wählen Sie **Speichern**aus.
7. Scrollen Sie zur zugehörigen Liste **OAuth-Entitätsprofile**, wählen Sie sie aus, und öffnen Sie das Standardprofil, das in der Liste erstellt wurde.
8. Füllen Sie das Feld **JWT-Provider** mit dem zuvor erstellten JWT-Provider aus, und speichern Sie das Formular.
9. Kehren Sie zur Anwendungsregistrierungsdatei zurück, und speichern Sie sie.
10. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**.
11. Wählen Sie die Richtlinie so aus, dass „com_snc_platform_security_oauth_glideencrypter“ als **Modulfeldwert Krypto** und „OAuthGitHubJWTHandler“ als Skripteinbindung im Skriptfeld **„Ziel“** angezeigt wird.

    In der folgenden Abbildung wird com_snc_platform_security_oauth_glideencrypter als Wert für das Feld **Krypto-Modul** ausgewählt. Das Feld **Skripttabelle** zeigt die Tabelle „Skripteinbindung“ [sys_script_include] an, und der Wert des Skriptfelds **„Ziel“** ist OAuthGitHubJWTHandler.



12. Wählen Sie **Aktualisieren**.



    Wie in der vorherigen Abbildung gezeigt, ändert sich der Wert im Feld **Richtlinienname**, und die Felder **Skripttabelle** und **Zielskript** werden nicht mehr angezeigt.

13. Stellen Sie sicher, dass das Feld **Ergebnis** auf Nachverfolgen festgelegt ist, und speichern Sie Ihre Änderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Anmeldeinformationen und Verbindungen für die GitHub-Anwendungsschwachstellen-Integration

Erstellen Sie einen Anmeldeinformationsdatensatz für den zuvor erstellten App-Anbieter GitHub, um Aktionen zu autorisieren.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.app_sec_manager

Prozedur

1. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Anmeldeinformationen**.
2. Wählen Sie **Neu**.
3. Wählen Sie **OAuth 2.0-Anmeldeinformationen** aus.
4. Wählen Sie **Neu** und füllen Sie die Felder aus.
5. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im Header der Seite, und wählen Sie **Speichern**aus.
   Die Liste der Anmeldeinformationen wird angezeigt.
6. Öffnen Sie den soeben erstellten Datensatz, und wählen Sie den zugehörigen Link **OAuth-Token** abrufen aus.
   Es wird eine Meldung angezeigt, dass das OAuth-Token erfolgreich importiert wurde.
7. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**.
8. Wählen Sie **Neu**.
9. Wählen Sie **HTTP(s)-Verbindung**aus.
10. Wählen Sie **Neu** und füllen Sie die Felder aus.
11. Wählen Sie **Absenden**.
    Die Liste der Aliasse für Verbindungen und Anmeldeinformationen wird angezeigt.
12. Öffnen Sie Ihren Datensatz, und wählen Sie auf der Registerkarte der zugehörigen Liste „Verbindungen“ **Neu,** und füllen Sie die Felder im Datensatz HTTP-Verbindung aus.
13. Wählen Sie **Absenden**.
    Die Liste der Aliasse für Verbindungen und Anmeldeinformationen wird angezeigt. Sie können jetzt die Schritte für Konfigurieren Sie die Eigenschaften GitHub-Anwendungsschwachstellen-Integrationausführen. Im Feld Verbindung geben Sie die Anmeldeinformationen ein, die Sie in den vorherigen Schritten erstellt haben.

Installieren Sie ServiceNow® GitHub-Anwendungsschwachstellen-Integration

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit GitHub-Anwendungsschwachstellen-Integration ordnungsgemäß in Application Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie GitHub-Anwendungsschwachstellen-Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in der Anwendung ServiceNow Storenach der Anwendung GitHub-Anwendungsschwachstellen-Integration.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Wählen Sie **App anfordern** aus, und geben Sie Ihre Now Support -Anmeldeinformationen ein.
6. Wählen Sie **Abrufen aus**.
7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance (Instanz validieren)**.
8. Wählen Sie **Anforderung**aus.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie **Installieren**aus.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Konfigurieren Sie die Eigenschaften GitHub-Anwendungsschwachstellen-Integration

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit das GitHub-Produkt ordnungsgemäß in Application Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen
Erforderliche Rollen:

- App-Sec-Manager-Benutzergruppe
- sn_vul.app_sec_manager für OAuth-Einrichtung erforderlich

Prozedur

1. Navigieren zu **Alle** > **GitHub-Schwachstellenintegration** > **Konfiguration**.
2. Wählen Sie **Standardauthentifizierung** oder **OAuth** als Authentifizierungstyp aus.
   - Die Standardauthentifizierung erfordert einen MID-Server für lokale Instanzen. Generieren Sie das für die Standardauthentifizierung erforderliche API-Token in Ihrem GitHub -Konto.
   - OAuth erfordert die in Erstellen von OAuth 2.0-Anmeldeinformationen für GitHub Apps – JWT für GitHub-Anwendungsschwachstellen-Integrationbeschriebene Einrichtung von OAuth-App, -Anmeldeinformationen und -Verbindung.
3. Füllen Sie die Felder je nach ausgewähltem Typ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basic Authentication

Feld	Beschreibung
API-URL	Die entsprechende GitHub API-URL für Enterprise oder lokal. Die Standard-URL lautet https://api.github.com . Lokal ist Ihre Endpunkt-URL GitHub.
API-Token	Token, das Sie über Ihre GitHub -Konsole generiert haben.
API-Typ	Wählen Sie eines aus: **Organisation** Wählen Sie diese Option, wenn Sie Daten für eine bestimmte Organisation nach Name importieren möchten. Die Umgebung GitHub unterstützt mehrere Organisationen. Jede Organisation kann mehrere Repositorys unterstützen. Wenn Sie eine Organisation eingeben, werden nur Daten von dieser Organisation importiert. **Enterprise** Die Enterprise-Umgebung unterstützt mehrere Organisationen. Wählen Sie diese Option aus, wenn Sie Schwachstellendaten aus allen Organisationen in Ihrer Enterprise (Cloud)-Umgebung importieren möchten.
Organisationsname	Name Ihres GitHub -Repositorys. Nur Daten aus der von Ihnen eingegebenen Organisation werden importiert.
MID-Server	Für lokale Instanzen ist für die Standardauthentifizierung ein MID Server erforderlich.
Wählen Sie Optionen aus, um Ausnahmeverwaltung und falsch positive Meldungen zu verwalten.	Wählen Sie Optionen aus, um Workflows für Ausnahmeverwaltung und falsch positive Elemente für angreifbare Elemente in Anwendungen mit ServiceNow beim Import automatisch zu verwalten. **Verwalten Sie Ausnahmen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte AVIs, die für den Status „ **Zurückgestellt“** markiert sind, selektieren möchten. AVIs mit **Quellstatus**, die in Ihrer Instanz normalerweise einem Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	„Zurückgestellt“ zugeordnet sind, werden stattdessen „ **Offen“**zugeordnet. Sie **fordern eine Ausnahme aus dem AVI-Datensatz an**. **Verwalten Sie falsch positive Meldungen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte AVIs mit **Quellstatus**, die als **Falsch positiv** oder **Potenziell falsch positiv**markiert sind, selektieren möchten. AVIs mit diesen **Quellstatus**, die in Ihrer Instanz normalerweise einem Status **„Geschlossen“** zugeordnet sind, werden **Offen**zugeordnet. Sie fordern ein **Falsch positives Ergebnis** aus dem AVI-Datensatz an. ○ Deaktivieren Sie eines oder beide Kontrollkästchen, wenn Sie die von Ihrem Scanner importierten **Quellstatus** beibehalten möchten. ○ Wenn diese Option deaktiviert ist, sind die Aktionen **„Ausnahme anfordern“** und **„Falsch positiv“** in AVIs nicht sichtbar.
Integrationsinstanz	Instanz, in die Sie Daten importieren.

OAuth

Feld	Beschreibung
API-URL	Die entsprechende GitHub API-URL für Enterprise oder lokal. Die Standard-URL lautet https://api.github.com . Lokal ist Ihre Endpunkt-URL GitHub.
Verbindung	Die von Ihnen erstellte Verbindung, beschrieben in Erstellen von OAuth 2.0-Anmeldeinformationen für GitHub Apps – JWT für GitHub-Anwendungsschwachstellen-Integration.
API-Typ	Wählen Sie eines aus: **Organisation** Wählen Sie diese Option, wenn Sie Daten für eine bestimmte Organisation nach Name importieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	möchten. Die Umgebung GitHub unterstützt mehrere Organisationen. Jede Organisation kann mehrere Repositorys unterstützen. Wenn Sie eine Organisation eingeben, werden nur Daten von dieser Organisation importiert. **Enterprise** Die Enterprise-Umgebung unterstützt mehrere Organisationen. Wählen Sie diese Option aus, wenn Sie Schwachstellendaten aus allen Organisationen in Ihrer Enterprise (Cloud)-Umgebung importieren möchten. **Hinweis:** GitHub Apps unterstützen keine APIs der Enterprise-Ebene.
Organisationsname	Organisationsname für Ihre GitHub -Repositorys. Nur Daten aus den Repositorys in der von Ihnen eingegebenen Organisation werden importiert.
Wählen Sie Optionen aus, um Ausnahmeverwaltung und falsch positive Meldungen zu verwalten.	Wählen Sie Optionen aus, um Workflows für Ausnahmeverwaltung und falsch positive Elemente für angreifbare Elemente in Anwendungen mit ServiceNow beim Import automatisch zu verwalten. **Verwalten Sie Ausnahmen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte AVIs, die für den Status „ **Zurückgestellt“** markiert sind, selektieren möchten. AVIs mit **Quellstatus**, die in Ihrer Instanz normalerweise einem Status **„Zurückgestellt“** zugeordnet sind, werden stattdessen „ **Offen“**zugeordnet. Sie **fordern eine Ausnahme aus dem AVI-Datensatz an**. **Verwalten Sie falsch positive Meldungen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte AVIs mit **Quellstatus**, die als **Falsch positiv** oder **Potenziell falsch**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	positivmarkiert sind, selektieren möchten. AVIs mit diesen **Quellstatus**, die in Ihrer Instanz normalerweise einem Status **„Geschlossen“** zugeordnet sind, werden **Offen**zugeordnet. Sie fordern ein **Falsch positives Ergebnis** aus dem AVI-Datensatz an. ○ Deaktivieren Sie eines oder beide Kontrollkästchen, wenn Sie die von Ihrem Scanner importierten **Quellstatus** beibehalten möchten. ○ Wenn diese Option deaktiviert ist, sind die Aktionen **„Ausnahme anfordern“** und **„Falsch positiv“** in AVIs nicht sichtbar.

4. Wählen Sie **Anmeldeinformationen speichern und testen aus**.
5. Führen Sie die GitHub Repository-Integration aus, bevor Sie die anderen Integrationen ausführen. Die anderen GitHub -Integrationen hängen von aktuellen Anwendungsdaten ab, die aus der Repository-Integration importiert werden. Daten aus der Repository-Integration werden in der Tabelle „Erkannte Anwendungen“ [sn_vul_app_release] gespeichert. Weitere Informationen finden Sie unter Zeigen Sie den Ausführungsstatus des Imports GitHub-Anwendungsschwachstellen-Integration und die importierten Repository-Daten an.

Zeigen Sie den Ausführungsstatus des Imports GitHub-Anwendungsschwachstellen-Integration und die importierten Repository-Daten an

Verwenden Sie die zugehörige Liste **„Integrationsausführungen für Schwachstellen“,** um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Nachbesserungsentscheidungen zu treffen.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_sec_manager

Prozedur

1. Navigieren zu **Alle** > **GitHub – Schwachstellen-Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Wählen Sie die zugehörige Liste **Integrationsausführungen für Schwachstellen** aus.
4. Stellen Sie sicher, dass alle Importe erfolgreich waren.

Trouble?

Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

- Netzwerkunterbrechung.
- Ein Problem bei der Datenübertragung, das während der Transformation zu beschädigten Daten führt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine dieser Bedingungen bei Ihnen auftritt, wählen Sie **Jetzt ausführen aus**, und führen Sie die Integration erneut aus.

5. Um importierte Repositorys anzuzeigen, navigieren Sie zurück zur Liste der Integrationen, und wählen Sie den Datensatz GitHub Repository Integration [] aus.
6. Wählen Sie die zugehörige Liste **„Ausführungen der Schwachstellenintegration“** aus, und öffnen Sie einen Datensatz.
   Die Anzahl der Repositorys, die Sie mit einer Integrationsausführung importiert haben, wird in der Spalte Importierte Elemente angezeigt.

   Alle Tags und Themen, die Sie für ein Repository in Ihrem Account GitHub im Menü Einstellungen konfiguriert haben, werden importiert. Alle importierten anwenderdefinierten Eigenschaften befinden sich im Menü unter Ihrem Repository.

   Tags, Themen und anwenderdefinierte Eigenschaften werden nur dann in Ihre -Instanz importiert, wenn sie in Ihrem -Account GitHub konfiguriert sind.

   Bei Import werden diese GitHub -Informationen in Ihrer Instanz in der Spalte „Zusätzliche Informationen zur Quelle“ in der Tabelle „Erkannte Anwendungen“ [sn_vul_app_release] und zu den zusätzlichen Informationen zur Quelle angezeigt. Abschnitt für einen erkannten Anwendungsdatensatz. Anwenderdefinierte Eigenschaften werden als Schlüssel-Wert-Paare angezeigt, und Tags und Themen werden in Arrays angezeigt.

Importsätze für GitHub-Anwendungsschwachstellen-Integration anzeigen

Zeigen Sie Details für Importinformationen für GitHub-Anwendungsschwachstellen-Integrationan.

Vorbereitungen
Erforderliche Rolle: sn_vul.app_sec_manager

Prozedur

1. Navigieren Sie zu **GitHub – Schwachstellen-Integration** > **Importsatztabellen**.
2. Wählen Sie einen Datensatz für eine Integration aus.
3. Wählen Sie einen zugehörigen Link, um die folgenden Informationen anzuzeigen:
   - Importsätze
   - Transformationszuordnungen
   - Verlauf umwandeln

Invicti-Schwachstellen-Integration

Invicti-Schwachstellen-Integration verwendet Anwendungsdaten, die aus dem Invicti-Produkt importiert wurden, um Ihnen zu helfen, die Auswirkungen und Priorität von Fehlern in Ihrem Code zu bestimmen.

Invicti-Schwachstellen-Integration

Invicti-Schwachstellen-Integration sammelt Scannerdaten und stellt diese Daten dem Now Platform®zur Verfügung. Es lässt sich problemlos in die Funktion ServiceNow® Application Vulnerability Response von Vulnerability Response integrieren, um importierte Informationen zu Anwendungsschwachstellen von Drittparteien Ihrer -Instanz zuzuordnen.

Die Integration importiert die folgenden Arten gescannter Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Dynamische Anwendungssicherheitstests (Dynamic Application Security Testing, DAST)
- Interaktive Anwendungssicherheitstests (Interactive Application Security Testing, IAST)

Weitere Informationen zu DAST und IAST finden Sie unter Application Vulnerability Response erkunden.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Invicti-Schwachstellen-Integration v1.1 Invicti-Schwachstellen-Integration 1.0	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Integrationen

Die folgenden Integrationen sind im Basissystem enthalten. Die Integrationen sind verkettet, sodass die nächste Integration initiiert wird, nachdem eine Integration erfolgreich abgeschlossen wurde. Die Integrationen werden in der in der folgenden Tabelle aufgeführten Reihenfolge ausgeführt.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um diese Integrationen automatisch der Reihe nach auszuführen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Invicti-Anwendungsschwachstellen-Integrationen

Integration	Beschreibung
Invicti-Anwendungslistenanwendung	Importiert von Invicti gescannte Anwendungen in die Tabelle „Erkannte Anwendungen“ [sn_vul_app_release] oder „Gescannte Anwendung“ [sn_vul_app_scanned_application], je nachdem, wie die Systemeigenschaft *sn_vul.use_product_model* für die CI-Suchregeldatensätze festgelegt ist. • Wenn die Produktmodelleigenschaft auf true festgelegt ist, wird eine Anwendung in die Releasetabelle „Erkannte Anwendungen“ eingefügt. • Wenn die Produktmodelleigenschaft auf „false“ festgelegt ist, wird eine Anwendung in die Tabelle „Gescannte Anwendung“ eingefügt. Sie können Suchregeln mit Configuration Items (CIs) als Suchziele aktivieren,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Invicti-Anwendungsschwachstellen-Integrationen (Fortsetzung)

Integration	Beschreibung
	indem Sie die Systemeigenschaft ändern. Wenn Sie sie ändern, sollten Sie auch CI-Suchregeln aktivieren, um sie an das Suchziel anzupassen. Weitere Informationen finden Sie unter: • Konfigurieren Sie die Eigenschaften Invicti-Schwachstellen-Integration • Erstellen Sie eine CI-Suchregel • CI-Suchregeln werden in erneut angewendet Application Vulnerability Response
Invicti-Scan-Listenintegration	Diese Integration wird initiiert, nachdem die Integration der Anwendungsliste erfolgreich abgeschlossen wurde. Diese Integration importiert Daten über das Datum und die Uhrzeit der Ausführung eines Scans.
Integration von angreifbaren Elementen in der Invicti-Anwendung	Diese Integration wird initiiert, nachdem die Scan-Listenintegration erfolgreich abgeschlossen wurde. Ab v1.1 können Sie Details wie Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integration und Berichte zu den Integrationsausführungsdatensätzen für die Integration von angreifbaren Anwendungselementen anzeigen. Jede Schwachstelle in Invicti hat einen Typ, z. B.**DirectoryListing**. Dieser Typ wird als eindeutige ID in Ihrer -Instanz zugeordnet und als Teil des Werts im Feld „Schwachstelle“ im Datensatz des angreifbaren Elements (AVI) der Anwendung angezeigt: **Invicti-DirectoryListing**. Weitere Informationen zur Zuordnung finden Sie unter Invicti-Schwachstellen-Integration Statuszuordnung.

Die Obergrenze für Elemente pro Seite für alle drei Integrationen beträgt 200.

Bereiten Sie sich auf die vor Invicti-Schwachstellen-Integration

Eine erfolgreiche Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Invicti-Schwachstellen-Integration setzt voraus, dass Sie mit dem Invicti-Produkt und der API vertraut sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Common Weakness Enumeration (CWE)-Integration wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration der Invicti-Schwachstellenintegration ausgeführt werden.

Hinweis:
Daten der NIST Vulnerability Database (NVD) sind für die Installation der Integration nicht erforderlich, bieten jedoch Ergänzungen zu Schwachstellen und sind nützlich.

Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validiert die Dimensionierung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die importiert werden sollen. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support. Die Administratorrolle ist erforderlich, um -Anwendungen in Ihrer Now Platform-Instanz zu installieren und zu konfigurieren.

Rufen Sie Ihre API-Anmeldeinformationen und das API-Token in Ihrer Invicti-Konsole ab. Überprüfen Sie die Informationen, die auf der Invicti-Produktwebsite unter API-Übersicht verfügbar sind.

Installieren Sie ServiceNow® Vulnerability Response Integration with Invicti

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit die Anwendung Invicti-Schwachstellen-Integration ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie Invicti-Schwachstellen-Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Invicti-Schwachstellen-Integration.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Wählen Sie **App anfordern** aus, und geben Sie Ihre Now Support -Anmeldeinformationen ein.
6. Wählen Sie **Abrufen aus**.
7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance (Instanz validieren)**.
8. Wählen Sie **Anforderung**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.

9. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie **Installieren**, um sie zu aktivieren. Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Konfigurieren Sie die Eigenschaften Invicti-Schwachstellen-Integration

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit Invicti-Schwachstellen-Integration ordnungsgemäß mit der Funktion Application Vulnerability Response von Vulnerability Responsefunktioniert.

Vorbereitungen
Erforderliche Rollen:

- -Administrator zum Installieren und Aktivieren von Anwendungen
- App-Sec-Manager-Benutzergruppe zur Konfiguration der Integration

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass Invicti-Schwachstellen-Integration installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Installieren Sie ServiceNow Vulnerability Response Integration with Invicti.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	• Wenn sie noch nicht zugewiesen sind, installiert der Systemadministrator [admin] die App und weist der App-Sec-Manager-Gruppe Benutzer zu. • Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.
Halten Sie für die Inviciti Vulnerability Integration Ihre **Anwender-ID** und **das API-Token** bereit.	Wenden Sie sich an Ihren Invicti-Administrator, um die **Anwender-ID** und **das API-Token** zu erhalten, wenn Sie diese nicht kennen. Weitere Informationen finden Sie auf der Invicti-Produktwebsite unter API-Übersicht .

Prozedur

1. Navigieren zu **Alle** > **Invicti** > **Invicti-Konfiguration**.
2. Füllen Sie die Felder aus.

Feld	Beschreibung
API-URL	URL der Invicti-Instanz des Anwenders. Dies sind die Informationen, die Sie von Bereiten Sie sich auf die vor Invicti-Schwachstellen-Integrationerhalten haben.
Anwender-ID	Eindeutige Anwender-ID.
API-Token	API-Token, das Sie über Ihre Invicti-Konsole generiert haben. Dies sind die Informationen, die Sie von Bereiten Sie sich auf die vor Invicti-Schwachstellen-Integrationerhalten haben.
Wählen Sie den Scantyp aus. Sie müssen mindestens einen auswählen.	
DAST importieren	Option zum Einbeziehen von Schwachstellen aus DAST-Scans. DAST-Scans ermitteln dynamisch Schwachstellen für eine Anwendung, während sie ausgeführt wird. Dieser Ansatz kann einen externen Angriff imitieren.
IAST importieren	Option zum Einbeziehen von Schwachstellen aus IAST-Scans. IAST-Scans erkennen Softwareschwachstellen durch Interaktion mit dem Programm, während es ausgeführt wird. Beobachtung durch Menschen, automatisierte Tests und Sensoren werden in Kombination verwendet, um mit der Anwendung zu interagieren und Schwachstellen zu lokalisieren.
Datumsformat	Parameter, der die Startzeit in das Format konvertiert, das von der Invicti-API unterstützt wird, die von der Invicti-Anwendungsintegration für angreifbare Elemente verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieser Parameter muss mit dem Format übereinstimmen, das Sie in Ihrem Invicti-Konto definiert oder ausgewählt haben, z. B. **tt/MM/jjjj**. Stellen Sie sicher, dass die Formate für Datum und Uhrzeit in der Invicti-Konsole mit den Formaten übereinstimmen, die Sie für das Datumsformat in Ihrer Instanz Now Platform eingegeben haben. So ändern Sie dieses Format in der Invicti-Konsole: **a.** Melden Sie sich bei Invicti-Anmeldung an . **b.** Wählen Sie oben rechts **Anwendername** aus. **c.** Navigieren zu **Benutzereinstellungen** > **Datums-/Uhrzeitformat**. **Hinweis:** Fehlgeschlagene Importe können auftreten, wenn Sie in Ihrer Instanz Now Platform ein ungültiges Datumsformat eingeben. Wenn Sie in Ihrer Instanz ein gültiges Format eingeben, das sich vom Datumsformat in Ihrer Invicti-Konsole unterscheidet, gibt Invicti eine leere Nutzlast zurück.
Ausnahmen in ServiceNow verwalten	Wählen Sie eines aus: **Aktiviert (ausgewählt)** Angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIT) von Invicti mit Status wie **„Present“** und **„AcceptedRisk“**, die in Ihrer Instanz möglicherweise zurückgestellt werden, werden stattdessen „ **Offen** “ automatisch zugeordnet. **Deaktiviert (nicht ausgewählt)** Quellstatus für aus Invicti importierte angreifbare Elemente der Anwendung (Application Vulnerable Items, AVITs) werden beibehalten. Sie müssen Ausnahmen für diese AVITs über AVIT-Datensätze verwalten (und zurückstellen). Weitere Informationen zu Invicti-Quellstatus und -Zielfeldern finden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie unter Invicti-Schwachstellen-Integration Statuszuordnung.
Falsch positive Ergebnisse in ServiceNow verwalten	Wählen Sie eines aus: **Aktiviert (ausgewählt)** AVITs mit Status aus Invicti wie **„Vorhanden“** und **„Falsch positiv“**, die in Ihrer Instanz zu **„Geschlossen“** übergehen können, werden stattdessen automatisch „ **Offen** “ zugeordnet. **Deaktiviert (nicht ausgewählt)** Aus Invicti importierte AVIT-Status werden beibehalten. Sie müssen falsch positive oder potenziell falsch positive Werte für diese AVITs aus AVIT-Datensätzen verwalten.

3. Wählen Sie **Anmeldeinformationen speichern und testen aus**.
4. **Wahlweise:** Ändern Sie Ihre Suchregeln so, dass sie auf Konfigurationselementen basieren.

   (Optional) Standardmäßig ist die Systemeigenschaft **sn_vul.use_product_model** für Ihre Suchregeln, die in der Tabelle [sn_sec_cmn_ci_lookup_rule] aufgeführt sind, basierend auf dem Produktmodell aktiviert (auf truefestgelegt). Wenn diese Regel aktiviert ist:

   - Diese Regel identifiziert Übereinstimmungen zwischen importierten Daten und den Daten in Ihrem Configuration Management Database (CMDB) basierend auf dem Produktmodell.
   - Datensätze werden in der Tabelle „Erkannte Anwendungen“ [sn_vul_app_release] erstellt oder aktualisiert.
   - Wenn Sie Ihre Suchregeln für Invicti erstellen oder bearbeiten, wird **das Produktmodell** im Feld **Suchziel** im Regelformular angezeigt.

   Um Ihre Regeln so zu ändern, dass sie auf Konfigurationselementen basieren, müssen Sie die Systemeigenschaft **sn_vul.use_product_model**manuell deaktivieren (auf false setzen).

   a. Navigieren zu **Alle** > **Systemeigenschaften** Suchen Sie den Datensatz **sn_vul.use_product_model**, und legen Sie den Wert auf falsefest.

   b. Wählen Sie **Aktualisieren**.

   c. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Suchregeln**.

   d. Suchen Sie die Regeln für Anwendungsname und Quellanwendungs-ID, die das Suchziel als **Configuration Item**festlegen.

   e. Aktivieren Sie für diese Regeln das Kontrollkästchen Aktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie **Aktualisieren**.
Wenn Sie Ihre Suchregeln für Invicti erstellen oder bearbeiten, beachten Sie, dass **Configuration Item** im Feld **Suchziel** im Regelformular angezeigt wird. Datensätze werden in der Tabelle „Gescannte Anwendungen“ [sn_vul_app_scanned_application] erstellt oder aktualisiert.

Status der Importausführung von Invicti-Schwachstellen-Integration und Datensätze werden angezeigt

Verwenden Sie die zugehörige Liste **„Integrationsausführungen für Schwachstellen“,** um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Nachbesserungsentscheidungen zu treffen.

Importstatus, Importsätze und Datensätze werden angezeigt

Um den Status Ihrer Importe anzuzeigen, navigieren Sie als Benutzer in der Benutzergruppe „App-Sec-Manager“ zu **Alle** > **Invicti-Schwachstellenintegration** > **Integrationen** und wählen Sie einen Integrationsdatensatz aus. Wählen Sie die zugehörige Liste **Integrationsausführungen für Schwachstellen** aus.

Ab v1.1 können Sie Details wie Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integration und Berichte zu den Integrationsausführungsdatensätzen für die Integration von angreifbaren Anwendungselementen anzeigen.

Um die Importsätze anzuzeigen, navigieren Sie zu **Alle** > **Invicti-Schwachstellenintegration** > **Integrationen** > **Importsatztabellen** und wählen Sie eine Integration aus.

Die Application List Integration erstellt oder aktualisiert Datensätze basierend auf dem Suchziel:

- Produktmodell: Tabelle „Erkannte Anwendungen“ [sn_vul_app_release].
- Configuration Item: Tabelle der gescannten Anwendungen [sn_vul_app_scanned_application].

Die Scan List-Integration erstellt oder aktualisiert Datensätze in der Tabelle „Gescannte Anwendungen“ [sn_vul_app_scan_summary].

Die Integration für angreifbare Elemente in der Anwendung erstellt oder aktualisiert Datensätze in der Tabelle „Angreifbare Elemente in der Anwendung“ [sn_vul_app_vulnerable_item] und „CWEs“ [sn_vul_cwe].

Hinweis:
Jede Schwachstelle in Invicti hat einen „Typ“, z. B. ProductDirectoryListing. Dieser Typ wird importiert, als eindeutige ID in Ihre Instanz zugeordnet und als Teil des Werts im Feld „Schwachstelle“ im AVIT-Datensatz (Application Vulnerability Item) angezeigt. In diesem Beispiel lautet der Wert Invicti-ProductDirectoryListing, und dieser Wert wird auch als eindeutige ID im Datensatz „Anwendungsschwachstelleneintrag“ angezeigt. Invicti-AVITs unterstützen mehrere Common Weakness Enumeration-Einträge (CWE), sodass CWEs nicht als eindeutige IDs verwendet werden. CWEs werden auch im AVIT-Datensatz angezeigt.

Wenn bei Invicti-AVITs in Invicti doppelte Typen für eine Schwachstelle vorhanden sind, wird das Wort „custom“ in den Wert eingefügt, z. B. Invicti-custom-ProductDirectoryListing. Wenn Sie einen Typ „Anwenderdefiniert“ für Schwachstellen erstellen, lautet die Schwachstellen-ID möglicherweise Invicti-Custom-<title of vulnerability>.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Felder: Für scan type=Invictienthalten die Felder Betroffene Parameter und Anwenderdefiniert möglicherweise Daten, die Ihnen helfen, die Schwachstelle zu verstehen und sie zu beheben. Wenn keine Daten vorhanden sind, werden diese Felder im AVIT nicht angezeigt.

Invicti-Schwachstellen-Integration Statuszuordnung

Die folgenden Quellstatus aus Invicti-Schwachstellen-Integration und ihre Zielstatus in Ihrer Instanz sind in der folgenden Tabelle aufgeführt.

Invicti-Quellstatus und ihre entsprechenden Now Platform-Status

Invicti-Quellstatus	Beschreibung der Quellstatus	Zielstatus in der Now Platform
Anwesend	Das Problem wurde identifiziert.	Öffnen
Vorhanden, Akzeptiertes Risiko, Wiederbelebend	Das Problem wurde berücksichtigt und als Schwachstelle mit geringem Risiko gekennzeichnet.	Zurückgestellt
Vorhanden, Falsch positiv	Das Problem wurde berücksichtigt und als keine echte Schwachstelle markiert.	Abgeschlossen
„FixedUnbestätigt“: „Fixiert – Unbestätigt“.	Das Problem wurde behoben, aber von Invicti Enterprise nicht bestätigt.	Gelöst
Befestigt (Bestätigt), BefestigtBestätigt, BefestigtBestätigt, AkzeptiertesRisiko, BefestigtBestätigt, Falsch positiv	Das Problem wurde von Invicti Enterprise behoben und bestätigt, und es sind keine weiteren Maßnahmen erforderlich.	Abgeschlossen
Repariert (kann nicht erneut getestet werden)	Das Problem wurde identifiziert, aber Invicti kann nicht erneut testen, um zu bestätigen, ob das Problem behoben wurde oder nicht.	Gelöst
Wiederbeleben	Das Problem wurde in vorherigen Scans behoben, wurde jedoch erneut gefunden.	Öffnen
Zurückgestellt, ignoriert	Das Problem wurde vom Anwender ignoriert. Um ein Problem zu ignorieren, aktualisiert ein Benutzer in Invicti Enterprise den Status in „Akzeptiertes Risiko“.	Risiko akzeptiert

Zuordnung des Anwendungs-Release

Quellfeld	Zielfeld in Now Platform
ID	source_app_id
CreatedAt	app_creation_date
UpdatedAt	app_updation_date

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	app_name
Stamm-URL	Source_additional_info
Beschreibung	description
Tags	Tags

Schwachstellenzuordnung

Quellfeld	Zielfeld in Now Platform
Typ	Kategoriename
Schwachstellendetail	Zusammenfassung
Auswirkung	Bedrohung
Quellreferenzen	Webreferenzen
Quellempfehlung	Lösung
Typ	source_entry_id/ID
Schweregrad	source_severity
Klassifizierung[„Cwe“]	CWE-Liste
CvssVectorString	CVVS v3-Felder

Scan-Zusammenfassungszuordnung

Quellenfeld	Zielfeld
Quelle	Quelle
Schwachstellenanzahl insgesamt	erkennung_fehler_anzahl
Datum der Initiierung	Dynamisches Scandatum
id	source_scan_id

Zuordnung von angreifbaren Elementen in der Anwendung (Application Vulnerable Item, AVIT).

Quellfeld	Zielfeld in Now Platform
Typ	Überprüfungstyp
Website-ID	Quell-App-ID
ID	AVIT-ID der Quelle
Zuletzt gesehen am	Zuletzt gefunden
Datum der ersten Sichtung	Zuerst gefunden
Datum der letzten Aktualisierung	Datum des letzten Scans
parameters	Betroffener Parameter
URL	Betroffene URL
Schweregrad	Quellenschweregrad

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

URL	Quell-Link
Schwachstellendetail	Zusammenfassung der Quellschwachstelle
Externe Referenzen	Quellreferenzen
Abhilfe + Abhilfereferenzen	Quellempfehlung
Status	Quellenkorrekturstatus
Auswirkung	Erklärung der Quellschwachstelle

Veracode Vulnerability Integration

Die Anwendung Vulnerability Response Integration with Veracode verwendet Daten, die aus dem Produkt Veracode importiert wurden, um Ihnen zu helfen, die Auswirkungen und Priorität von Fehlern in Ihrem Code zu bestimmen.

Veracode Vulnerability Integration

Das Produkt Veracode erfasst Daten zu dynamischen Anwendungssicherheitstests (Dynamic Application Security Testing, DAST), statische Anwendungssicherheitstests (SAST) sowie manuelle Scannerdaten und stellt diese Daten für Now Platform® zur Verfügung. Es lässt sich problemlos in die Funktion Application Vulnerability Response von Vulnerability Response integrieren, um Schwachstellen von Drittparteien abzubilden, die die Daten in Ihrer -Instanz ergänzen.

Ab v19.0 von Vulnerability Responsekönnen Sie SCA-Schwachstellen (Software Composition Analysis) und Schwachstellendaten Software Bill of Materials vom Typ (SBOM) importieren, um Schwachstellen in Ihren Softwareanwendungen zu identifizieren. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Eine gemeinsam genutzte API erfasst DAST-, SAST- und SCA-Daten sowie die Ergebnisse manueller Penetrationstests.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Jeden Tag rufen geplante Aufgaben die Integrationen automatisch in der Reihenfolge auf, in der sie aufgelistet sind. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem sie die Instanz mit anderen Schwachstellenmanagementsystemen synchronisieren.

Weitere Details erhalten Sie von Veracode

Wählen Sie ab v4.2 in der Tabelle „Angreifbares Element der Anwendung“ [sn_vul_app_vulnerable_item] oder in den Listenansichten in den Vulnerability Response-Arbeitsbereichen für angreifbare Elemente der Anwendung (Application Vulnerable Items, AVITs) mit Veracode als Quelle, um die folgenden Daten Veracode anzuzeigen .

- Details zu HTTP-Quellanforderungen und Quellantworten für DAST-Scans (Dynamische Anwendungssicherheitstests) werden in der zugehörigen Liste „HTTP-Anforderung/-Antwort“ angezeigt.
- Lösungsempfehlungen von Veracode werden in der zugehörigen Liste „Ergebnisse“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die HTTP-Quellanforderung, die Quellantwort und die Empfehlungen werden auf der Registerkarte „Details“ in den Vulnerability Response-Arbeitsbereichen Vulnerability Response angezeigt.
- Die Spalte „Beschreibung“ wird in der Tabelle für angreifbare Elemente der Anwendung [sn_vul_app_vulnerable_item] unterstützt.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Veracode v4.3 Veracode v4.2 Veracode v4.1	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Benutzergruppe und -rollen

Veracode Vulnerability Integration wird von einem Systemadministrator [admin] installiert und von einem Mitglied der App-Sec-Manager-Gruppe konfiguriert. Weitere Informationen finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen.

Veracode Vulnerability Integration

Um die Veracode Schwachstellen-Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

Veracode Vulnerability Integration

Integration	Beschreibung
Ab v4.1: Veracode Integration von Linkprojekten	Diese Integration ist standardmäßig aktiviert. Ruft alle zugeordneten Projekte für jede Anwendung von Veracodeab. Anwendungen können mehrere Projekte in der Anwendung Veracode haben. Aus dieser Integration importierte Daten werden in den folgenden Datensätzen angezeigt: • **Das Datum des letzten SCA-Scans**, **das Erstellungsdatum der App**und **das Datum der App-Aktualisierung** sind in Datensätzen unter **Erkannte Anwendungen**aufgeführt. • In den Datensätzen „Zusammenfassung des Anwendungsschwachstellen-Scans“ und „Application Vulnerable Items“ (AVITs) wird der **Quell-SDLC-Status** (Software Development Life Cycle) angezeigt. • **Die Ausnutzbarkeit der Quelle** wird für Datensätze von angreifbaren Elementen in der Anwendung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode Vulnerability Integration (Fortsetzung)

Integration	Beschreibung
Veracode Integration der Anwendungsliste (JSON)	Diese Integration ist standardmäßig inaktiv. Ruft Veracode Anwendungsscannerdaten (Schwachstellen, Metadaten) ab und erweitert Ihre Anwendungsdaten. Ruft Scan-Datensätze von Veracode über eine JSON-basierte API ab.
Veracode Integration der Anwendungsliste (XML)	Diese Integration ist standardmäßig inaktiv. Die XML-basierte Version dieser Integration wurde deaktiviert (veraltet). Ruft Veracode Anwendungsscannerdaten (Schwachstellen, Metadaten) ab und erweitert Ihre Anwendungsdaten. Diese Integration wird täglich um 00:00:00 Uhr ausgeführt. **Hinweis:** Zum Abrufen der Liste der Anwendungen wird eine JSON-basierte API von Veracode verwendet. Diese API importiert für diese Anwendungen das Datum der letzten Prüfung der Richtlinien-Compliance, das angibt, wann diese Anwendungen zuletzt von Veracodegescannt wurden.
Veracode Software Bill of Materials (SBOM) Integration	Version 4.3 von Veracode Vulnerability Integration enthält die folgenden Erweiterungen für Veracode SBOM -Dateien: • Wenn Sie SBOM Response installiert haben, können Sie von Veracode gefundene Schwachstellen für die von Ihnen hochgeladenen SBOM-Dateien einbeziehen. • Veracode wird dem Feld **Quelle** für Datensätze in der Stücklistentabelle [sn_sbom_doc] für die SBOM-Dateien Veracode zugeordnet. Diese Integration ist standardmäßig aktiviert. Ab v4.2 importiert von [Veracode generierte Software Bill of Materials -Dateien in den Formaten Epic (CycloneDX) und SPX und stellt sie zur Analyse in Ihrer -Instanz in die Warteschlange. Sie müssen die Anwendungen Software-Stückliste installiert haben, um diese Daten importieren und anzeigen zu können.
Veracode Integration der Scan-Zusammenfassung (JSON)	Diese Integration ist standardmäßig inaktiv. Ruft Scan-Datensätze von Veracode über eine JSON-basierte API ab. Diese Integration ersetzt die XML-basierte API-Integration. Sie ist verkettet und folgt der Veracode Application List Integration, wenn sie aktiviert ist.
Veracode Scan-Zusammenfassung (XML)	Diese Integration ist standardmäßig inaktiv. Die XML-basierte Version dieser Integration wurde deaktiviert (veraltet). Ruft Scan-Datensätze von Veracodeab. Diese Integration ist verkettet und folgt der Veracode Application List Integration, wenn sie aktiviert ist. **Hinweis:** Verfolgt automatisch die Integration der Veracode Anwendungsliste, wenn sie aktiviert ist. Mit „Letzte Prüfung der Richtlinien-Compliance“ für die Anwendungen von Veracoderuft diese Integration nur Daten für die Anwendungen ab, die nach der „delta_start_time“ dieser Integration gescannt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode Vulnerability Integration (Fortsetzung)

Integration	Beschreibung
Veracode Integration von angreifbarem Anwendungselement in JSON	Ab v4.2 können Sie Details wie Gesamtverarbeitungszeiten, Durchschnittszeiten für Prozesse vor und nach der Integration und Berichte zu Integrationsausführungsdatensätzen für Integrationen von angreifbaren Anwendungselementen anzeigen. Diese Integration ist standardmäßig inaktiv. Ruft Scan-Ergebnisse mit mehr Schwachstellendaten als die XML-basierte Integration von Veracodeab. Es fügt AVIs ein und ergänzt Ihre Drittpartei-Schwachstellendaten.
Veracode Integration angreifbarer Elemente in der Anwendung (XML)	Ab v4.2 können Sie Details wie Gesamtverarbeitungszeiten, Durchschnittszeiten für Prozesse vor und nach der Integration und Berichte zu Integrationsausführungsdatensätzen für Integrationen von angreifbaren Anwendungselementen anzeigen. Diese Integration ist standardmäßig inaktiv. Ruft Scan-Ergebnisse von Veracodeab, fügt angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs) ein und erweitert Ihre Schwachstellendaten von Drittparteien. Standardmäßig werden keine AVITs erstellt, wenn sich der Scanner-Datensatz im Status **Geschlossen** befindet. Vorhandene AVITs werden weiterhin aktualisiert. Diese Integration ist verkettet und folgt der Veracode Scan Summary-Integration, wenn sie aktiviert ist. Die XML-basierte API ist für die Veracode Integration mit der Scan-Zusammenfassung JSON veraltet. **Hinweis:** Entspricht automatisch der Veracode Integration der Scan-Zusammenfassung. Mit „Letzte Prüfung der Richtlinien-Compliance“ für die Anwendungen von Veracoderuft diese Integration nur Daten für die Anwendungen ab, die nach der „delta_start_time“ dieser Integration gescannt wurden.
Veracode Integration von Kategorien	Diese Integration ist standardmäßig inaktiv. Ruft erweiterte Kategoriedaten von Veracodeab.
Veracode CWE-Integration	Diese Integration ist standardmäßig aktiviert. Ruft Veracode spezifische Common Weakness Enumeration-Daten (CWE) für Bedrohungsinformationen und Korrekturempfehlungen ab. Diese Daten werden in den Anwendungsschwachstelleneintrags-Datensätzen eingetragen und aktualisiert. Diese CWE-Integration funktioniert unabhängig von der geplanten Aufgabe für die Integration von CWE Comprehensive 2000, die Sie für die Anwendung Vulnerability Response aktivieren. Ihre Daten werden nicht dupliziert, wenn Sie die Veracode CWE-Integration und die CWE Comprehensive 2000-Integration aktiviert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode Vulnerability Integration (Fortsetzung)

Integration	Beschreibung
Veracode DevOps-Integration	Diese Integration ist standardmäßig inaktiv. Die Integration kann in der Liste Anwendungsschwachstellen-Integrationen in Application Vulnerability Responseangezeigt werden. Wenn Sie über eine DevOps Change Velocity-Lizenz verfügen, ist diese Funktion so strukturiert, dass DevOps-Benutzer keine SecOps-Lizenz benötigen, um Zusammenfassungsdetails für Schwachstellen-Scans von Drittparteien anzuzeigen. Es gibt keine Auswirkungen oder Changes für Application Vulnerability Response.

Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Status der Importausführung von Veracode Anwendungsschwachstellen-Integration an.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

Vorbereitung auf das Veracode Vulnerability Integration

Ein erfolgreiches Veracode Vulnerability Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie die Integration vor, indem Sie diese Aufgaben ausführen. Bei Veracode Vulnerability Integration wird davon ausgegangen, dass Sie mit dem Produkt und der API Veracode vertraut sind.

Vorbereitungen

Die Integration mit der Common Weakness Enumeration (CWE) wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration von Veracode Vulnerability Integrationausgeführt werden. Es wird standardmäßig mit Vulnerability Responseinstalliert.

Hinweis:
Daten der NIST Vulnerability Database (NVD) sind für die Installation der Integration für Anwendungsschwachstellen Veracode nicht erforderlich. Sie ergänzen jedoch die Daten und sind daher nützlich. Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer. Der Standardwert für diesen Anwender ist **VR.System**. Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen vor, die auf Ihren Anforderungen basieren.

Validiert die Dimensionierung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die importiert werden sollen. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Veracode Vulnerability Integration erfordert eine API-ID und einen API-Schlüssel.

Prozedur

So erstellen Sie die API-ID und die Schlüsselanmeldeinformationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Melden Sie sich bei der Veracode -Plattform an.

b. Wechseln Sie zum Menü „Benutzeraccount“, und wählen Sie **API-Anmeldeinformationen**aus.

c. Klicken Sie auf **API-Anmeldeinformationen generieren**.

d. Notieren Sie Ihre Anmeldeinformationen zur späteren Verwendung.

ServiceNow® Vulnerability Response Integration mit Veracodeinstallieren

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Veracode ordnungsgemäß in Application Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen sind, installiert der Systemadministrator [admin] die Anwendung und weist der App-Sec-Manager-Gruppe Benutzer zu. Informationen zu Gruppenrollen finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen. • Die App-Sec-Managergruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie Veracode Vulnerability Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Vulnerability Response Integration with Veracode.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie gegebenenfalls auch die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Nächste Maßnahme

Konfigurieren Sie Veracode Vulnerability Integration für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integration.

Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integration

Bevor Sie die Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Veracode ordnungsgemäß in Application Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Stellen Sie sicher, dass die Anwendung Vulnerability Response Integration with Veracode installiert und aktiviert ist.	Um sicherzustellen, dass diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie ServiceNow Vulnerability Response Integration mit Veracodeinstallieren.
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen sind, installiert der Systemadministrator [admin] die App und weist Benutzer der Benutzergruppe „App-Sec Manager“ zu. • Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.
Halten Sie für die Integration der Anwendungsschwachstelle Veracode Ihre **API-ID** und **Ihren API-Schlüssel** bereit.	Wenden Sie sich an Veracode, um die**API-ID** und **den API-Schlüssel**zu erhalten. Weitere Informationen finden Sie unter Vorbereitung auf das Veracode Vulnerability Integration. Wenn Sie Veracode Vulnerability Integrationverwenden, sind die Penetrationsbewertungstests in Veracode Vulnerability Integration ab Version 4.0 manuelle Ergebnisse von Veracode. Diese Ergebnisse sind nicht mit Bewertungsanforderungen für Penetrationstests verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstest-Anforderungen in Application Vulnerability Responsefinden Sie unter Konfigurieren Sie Penetrationstests.

Erforderliche Rolle: Anwendergruppe „App-Sec-Manager“.

Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Konfiguration**.
2. Füllen Sie die Felder **API-ID** und **API-Schlüssel** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie Ihre Testergebnisse aus.

Option	Bezeichnung
Version 4.0:	**a.** Wählen Sie die Datentypen **DAST** oder **SAST** aus, die in den Import aufgenommen werden sollen. **Hinweis:** Sie können das eine oder das andere oder beides auswählen, Sie müssen jedoch mindestens eins auswählen. **b.** Wählen Sie **SCA** aus, um SCA-Schwachstellen (Software Composition Analysis) zu importieren. **c.** Wählen Sie **Manuelle einbeziehen aus**, um die Ergebnisse für manuelle Penetrationstests aus Veracodezu importieren. Für diese Ergebnisse werden AVITs erstellt.
Version 3.0	Wählen Sie die Datentypen **DAST** oder **SAST** aus, die in den Import aufgenommen werden sollen. **Hinweis:** Sie können das eine oder das andere oder beides auswählen, Sie müssen jedoch mindestens eins auswählen.
Version 1.0:	Standardmäßig werden die Testergebnisse für die dynamische Anwendungssicherheit ausgewählt.

4. Fügen Sie die Veracode **Schweregradstufe** hinzu, um Ihre importierten Daten zu filtern.
Dieser Wert wird aus Veracodeimportiert. Sie können dem Feld mehrere Werte hinzufügen. Wenn ausgefüllt, sammelt der Import nur Daten, die den von Ihnen hinzugefügten Schweregradstufen entsprechen.

5. Speichern und validieren Sie Ihre Auswahl.

Option	Bezeichnung
Version 3.0:	Klicken Sie **auf Anmeldeinformationen speichern und testen**. **Hinweis:** Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, es wird eine Fehlermeldung angezeigt. Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein.
Version 1.0:	Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken. **Hinweis:** Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, es wird eine Fehlermeldung angezeigt. Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein.

6. Wählen Sie aus, wie Sie Ausnahmen und falsch positive Meldungen für AVITs beim Import verwalten möchten.
   Optionen zur Verwaltung von AVITs beim Import mit den Workflows ServiceNow Ausnahmeverwaltung und Falsch positiv sind standardmäßig aktiviert. Die Workflows werden basierend darauf ausgelöst, wie die **Quellstatus** für die AVITs in Ihrer Instanz zugeordnet sind. Ein Beispiel für einen Anwendungsfall finden Sie unter Verwalten der Statuszuordnung für Zurückstellungen und falsch positive Meldungen in Application Vulnerability Response.

7. Ab v4.3 können Sie Einstellungen für die folgenden Parameter auswählen oder überprüfen.

8. Wählen Sie **Anmeldeinformationen speichern und testen aus**.

Nächste Maßnahme
Wenn Ihre Umgebung domänengetrennte Importe erfordert, lesen Sie unter Erstellen Sie domänengetrennte Importe für eine Integrationnach.

Weitere Anweisungen zur Erstinstallation finden Sie unter Application Vulnerability Response konfigurieren.

Änderungen nach der Erstinstallation finden Sie unter Veracode Vulnerability Integration Änderungen und Aktivitäten.

Zeigen Sie den Status der Importausführung von Veracode Anwendungsschwachstellen-Integration an

Verwenden Sie die zugehörige Liste **„Integrationsausführungen für Schwachstellen“,** um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Nachbesserungsentscheidungen zu treffen.

Vorbereitungen
So zeigen Sie den Ausführungsstatus des Imports Veracode Vulnerability Integration an:

- Application Vulnerability Response und Veracode Vulnerability Integration müssen installiert und konfiguriert sein.
- Die Veracode Vulnerability Integration -Importe müssen geplant sein und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager-Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Application Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. [store-future: BEGIN review]Wenn Sie das Statusdiagramm für die Integrationsausführung Veracode nicht verwenden, benötigen [End] Navigieren Sie zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf die zugehörige Liste **Integrationsausführungen für Schwachstellen**.
4. Stellen Sie sicher, dass alle Importe erfolgreich waren.

   Trouble?

   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

   - Netzwerkunterbrechung.
   - Ein Problem bei der Datenübertragung, das während der Transformation zu beschädigten Daten führt.

   Wenn eine dieser Bedingungen auftritt, klicken Sie auf **Execute Now (Jetzt ausführen)**, und führen Sie die Integration erneut aus.
5. Ab v4.2 können Sie Details wie Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integration und Berichte zu den Integrationsausführungsdatensätzen für die Integrationen von angreifbaren Anwendungselementen anzeigen.
   Weitere Informationen zum Anzeigen zusätzlicher, von Veracodeimportierter Details finden Sie unter Weitere Details in Veracode Vulnerability Integrationabrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Veracode Scan-Zusammenfassungen an

Zeigen Sie Details für Scan-Zusammenfassungsinformationen für Veracode Vulnerability Integration an.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Prozedur

1. Navigieren Sie zur Tabelle Zusammenfassungen von Anwendungsschwachstellen-Scans [sn_vul_app_vul_scan_summary_list].
2. Wählen Sie einen Datensatz für einen Veracode -Scan aus.
3. Ab v19.0 von Vulnerability Response und v4.0 der Veracode-Schwachstellenintegration verwenden Sie das Symbol „Liste personalisieren“ (Zahnradsymbol), um die folgenden Spalten anzuzeigen.
   - Größe des statischen Scans
   - Anzahl Bibliotheken von Drittparteien
   - Anzahl anfälliger Drittparteibibliotheken
   - Gesamtanzahl der Drittanbieterfehler nach Schweregrad
   - Anzahl Probleme von Drittparteibibliotheken
   - Anzahl Probleme von Drittparteilizenzen
   - Anzahl gemischter Fehler
   - Anzahl verringerter Fehler
   - Anzahl nicht verringerter Fehler
   - Anzahl statischer Fehler nach Schweregrad
   - Anzahl neuer Fehler nach Schweregrad
   - Anzahl nicht verringerter Fehler nach Schweregrad
   - Gesamtanzahl der Fehler nach Schweregrad
   - Bewertung des letzten SCA-Scans
   - Datum des letzten SCA-Scans
   - Veröffentlichungsdatum des Scans
   - Tags

Datentransformation für die Veracode Vulnerability-Integration

Nachdem Sie die zu importierenden Daten identifiziert haben, werden die Daten aus der Anwendung Veracode abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer -Instanz transformiert.

Veracode Integration angreifbarer Anwendungselemente

Die Daten aus der API werden zuerst in die Tabelle Veracode AppVul Item Import [sn_vul_veracode_appvul_item_import] geladen. Die importierten Informationen werden dann mit der Veracode AppVul Item Transform transformiert.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu *System Import Sets > Transform Maps*, und suchen Sie nach Veracode AppVul Item Transform. In der folgenden Tabelle sind die Transformationszuordnungsfelder nach Integration geordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode AppVul Item-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
app_id	source_app_id	Anwendungs-ID.
Ausgabe-ID	source_avit_id	AVIT-ID
app_name	app_name	Anwendungsname.
version	app_version	Anwendungsversion.
build_id	source_scan_id	Build-ID der Anwendung.
account_id	account_id	Account-ID.
Sandbox-ID	Sandbox-ID	Sandbox-ID.
last_update_time	last_scan_date	Uhrzeit der letzten Aktualisierung.
app_name + last_scan_date	scan_summary_name	Scan-Zusammenfassung.
life_cycle_stage	source_sdlc_status	SDLC-Status der Quelle.
level	source_severity	Quellenschweregrad.
kategoriename	Kategorie	Kategorie.
source_severity	source_severity	Quellenschweregrad.
category_id + „CWE-“ + cweId	source_entry_id	Quelleintrags-ID.
source_vulnerability_summary	source_vulnerability_summary	Zusammenfassung der Quellschwachstelle.
source_recommendation	source_recommendation	Quellempfehlung.
description	description	Beschreibung aus der Quelle.
description	source_vulnerability_explanation	Erklärung der Quellschwachstelle.
mitigation_status_desc	source_mitigation_status	Quellverringerungsstatus.
remediation_status	source_remediation_status	Korrekturstatus der Quelle.
Zeile	zeilennummer	Position, in der der Fehler gefunden wurde.
Modul	application_module	Anwendungsmodul
Quelldatei	source_notes	Quellhinweise.
impacts_policy_compliance	Compliance_mit_Richtlinie	Die Werte können „Ja“ oder „Nein“ sein, je nachdem, ob die Quellinformationen „wahr“ oder „falsch“ sind.
Quelldateipfad und Quelldatei	location	Standortzuordnung im Falle eines `static` -Fehlers.
URL	location	Standortzuordnung im Falle eines `dynamic` -Fehlers.
Umfang, Typ, ExploitLevel	source_additional_info	Namenswertfeld, das bei statischen Fehlern mit den Werten aus der Quelle gefüllt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Veracode Zeitpunkt und Zweck des Skripts für die Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Skript, das verwendet wird, um die Datenquelle zu verarbeiten und die Anzahl der erstellten, aktualisierten oder unveränderten AVITs sowie der als Teil dieser Integration von Veracodeimportierten AVITs zu aktualisieren. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Veracode Vulnerability Integration Änderungen und Aktivitäten

Konfigurieren Sie optionale Änderungen speziell für Veracode Vulnerability Integration.

Von werden zusätzliche Daten angezeigt, die von importiert wurden Veracode Vulnerability Integration

Hinweis:
Das Ändern anderer Veracode Vulnerability Integration -Einstellungen, die nicht die hier aufgeführten sind, erfordert fortgeschrittene Kenntnisse ServiceNow von und Application Vulnerability Response und liegt außerhalb des Umfangs der Produktdokumentation.

Weitere Details erhalten Sie von Veracode

Wählen Sie ab v4.2 in der Tabelle „Angreifbares Element der Anwendung“ [sn_vul_app_vulnerable_item] oder in den Listenansichten in den Vulnerability Response-Arbeitsbereichen für angreifbare Elemente der Anwendung (Application Vulnerable Items, AVITs) mit Veracode als Quelle, um die folgenden Daten Veracode anzuzeigen .

- Details zu HTTP-Quellanforderungen und Quellantworten für DAST-Scans (Dynamische Anwendungssicherheitstests) werden in der zugehörigen Liste „HTTP-Anforderung/-Antwort“ angezeigt.
- Lösungsempfehlungen von Veracode werden in der zugehörigen Liste „Ergebnisse“ angezeigt.
- Die HTTP-Quellanforderung, die Quellantwort und die Empfehlungen werden auf der Registerkarte „Details“ in den Vulnerability Response-Arbeitsbereichen Vulnerability Response angezeigt.
- Die Spalte „Beschreibung“ wird in der Tabelle für angreifbare Elemente der Anwendung [sn_vul_app_vulnerable_item] unterstützt.

Ändern Sie die Parameter der Integrationsinstanz Veracode .

Nach der Erstinstallation können Sie Parameter für die Veracode -Integrationen in der Instanz der Veracode -Integration ändern.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Parameter für eine Integration von ihrer Instanz aus ändern, um zu bestimmen, welche Art von Daten Sie erfassen. Für einige dieser Einstellungen können Sie diese Parameter auch auf der Konfigurationsseite der Integration ändern.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie **Veracode-Anwendungsschwachstelle** in der Spalte Quellinstanz für die Integration Veracode aus, die Sie ändern möchten.
3. Wählen Sie die Registerkarte **Integrationsinstanzparameter** aus, und doppelklicken Sie auf ein Feld in der Spalte Wert, um die Werte zu ändern.

   Ab v19.0 von Vulnerability Response und v4.0 von Veracode Vulnerability Integrationkönnen Sie die folgenden Parameter für die Integrationen Veracode von konfigurieren.

   Import manuell

   Geben Sie „true“ ein, um die Ergebnisse für manuelle Penetrationstests aus Veracodezu importieren. Sie können diesen Wert auch auf der Konfigurationsseite der Integration ändern.

   Die Penetrationsbewertungstests in Veracode Vulnerability Integration sind manuelle Ergebnisse von Veracode. Diese Ergebnisse sind nicht mit Bewertungsanforderungen für Penetrationstests verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstest-Anforderungen in Application Vulnerability Responsefinden Sie unter Konfigurieren Sie Penetrationstests.

   import_sca

   Geben Sie „true“ ein, um SCA-Schwachstellen (Software Composition Analysis) zu importieren. Sie können diesen Wert auch auf der Konfigurationsseite der Integration ändern.

   status

   Geben Sie Offen oder Geschlossen ein, um Ergebnisse für die gewünschten Status zu importieren. Wenn Sie dieses Feld leer lassen, importieren die Integrationsergebnisse sowohl für den Status „Offen“ als auch für den Status „Geschlossen“.

   policy_sandbox

   Geben Sie eine Richtlinie oder eine Sandbox ein, um Datensätze zu importieren, die einer Richtlinie oder einer Sandbox entsprechen. Diese Datensätze können sich darauf beziehen, wie Anwendungen in Ihrer Umgebung getestet werden.

   policy_rule_passed

   Geben Sie wahr oder falsch ein, um Datensätze zu importieren, die eine Richtlinienregel übergeben haben. Diese Datensätze können sich darauf beziehen, wie Anwendungen in Ihrer Umgebung getestet werden.

4. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

Führen Sie einen manuellen Veracode Import von Anwendungsschwachstellen durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie unabhängig von der täglichen geplanten Aufgabe einen vollständigen Datenimport durchführen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.
2. Wählen Sie und Integration, z. B. Veracode Application List Integration.
3. Klicken Sie auf **Jetzt ausführen**.

> **Hinweis:**
> Jede der Veracode Anwendungsschwachstellen-Integrationen soll einen möglichst vollständigen Datenabruf ermöglichen. Wenn Sie sie in Unordnung bringen, sind die Fachkenntnisse ServiceNow und Application Vulnerability Response erforderlich und können zu unvollständigen Daten führen.

Sobald der Import abgeschlossen ist, werden die geplanten Importe fortgesetzt.

4. Informationen zu den Status der Integrationsausführung finden Sie unter Zeigen Sie den Status der Importausführung von Veracode Anwendungsschwachstellen-Integration an.
5. Wenn Sie andere Integrationsparameter ändern möchten, müssen Sie zur Integrationsinstanz navigieren.

Legen Sie die Importzeiten Veracode Vulnerability Integration fest

Zur Vereinfachung können Sie die Startzeit für Veracode Vulnerability Integrationzurücksetzen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Nach dem ersten Import führen die Veracode Schwachstellen-Integrationen bei jeder Ausführung einen vollständigen Import durch. Weitere Informationen zur Durchführung von Importen finden Sie unter Führen Sie einen manuellen Veracode Import von Anwendungsschwachstellen durch.

Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Legen Sie die neue **Startzeit**fest.
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für Importe von Veracode Application List Integration ist 00:00:00. Die anderen Integrationen sind **bei Bedarf** und sind so verkettet, dass sie nach der Veracode Application List Integration ausgeführt werden. Das Ändern der **Startzeit** für eine dieser Optionen erfordert fortgeschrittene Kenntnisse über ServiceNow und Application Vulnerability Management.
4. Klicken Sie auf **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

Schließt angreifbare Elemente der Veracode-Anwendung ein

Standardmäßig werden **geschlossene** angreifbare Anwendungselemente (Application Vulnerable Items, AVIs) nicht während Importen der Integration von Veracode angreifbare Elemente erstellt. Wenn Sie sie erstellen möchten, müssen Sie eine Systemeigenschaft ändern.

Vorbereitungen

Veracode Vulnerability Integration muss installiert sein und ausgeführt werden.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Textfeld **des Filternavigators** für die Navigation auf der linken Seite sys_properties.listein.
2. Geben Sie im **Namenssuchfeld** für die Liste sn_vul.create_closedein.
3. Doppelklicken Sie auf das Feld **Wert**, und setzen Sie es auf **Wahr**
4. Klicken Sie auf das grüne Häkchen-Symbol um zu speichern.
   Datensätze im Status **„Geschlossen“** im nächsten Import Veracode werden als AVIs in Application Vulnerability Responseerstellt.

Application Vulnerability Response Schwachstellen werden behoben

Die Überwachung der Remediation ist ein Prozess, der mit der Überprüfung des Status beginnt und mit dem Schließen von angreifbaren Elementen in der Anwendung (Application Vulnerable Items, AVITs) endet. Application Vulnerability Response bietet Tools und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

Application Vulnerability Response Nachbesserungsprozess

Die Korrektur angreifbarer Anwendungselemente erfolgt manuell.

Übersicht über den -Prozess:

- Melden Sie sich bei der Application Vulnerability Response-Instanz an.
- Überprüft, ob Ihre Regeln (CI-Suche, Zuweisung) für angreifbare Anwendungselemente wie erwartet funktionieren. Informationen zum Überarbeiten von CI-Suchregeln finden Sie unter Identifizieren Sie -Anwendungen in Application Vulnerability Response automatisch. Informationen zu Zuweisungsregeln finden Sie unter Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu.
- Überprüfen Sie, ob Ihre Korrekturziele korrekt sind. Informationen dazu, wie Korrekturzielregeln funktionieren und wie sie überarbeitet werden können, finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response. Zeigen Sie den Nachbesserungszielstatus eines angreifbaren Anwendungselements an.

  Hinweis:
  Korrekturzielregeln gehören zu AVITs. Diese Regeln werden ausgeführt, wenn die AVIT importiert wird.

- Überprüfen Sie die Dashboards oder Berichte. Zeigen Sie beispielsweise Dashboards an, die das Altern von AVITs nach Status anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn die Anwendung Performance Analytics for Vulnerability Response (com.snc.vulnerability.analytics) aktiviert ist, können Benutzer mit bestimmten Rollen Daten anzeigen, die für Mitglieder der Gruppen „App-Sec-Manager“ und „Security Champion“ von Interesse sind.

Für App-Sec-Manager enthält Performance Analytics for Vulnerability Response die Übersicht Application Vulnerability Response, mit der Sie Problembereiche überwachen können. Weitere Informationen finden Sie unter Analyse- und Berichterstellungslösungen fürdas Dashboard „Application Vulnerability Response“ und „Application Vulnerability Management“ [PA].

Ab Version 13.0 der Anwendung Vulnerability Response : Für Security Champions enthält Performance Analytics for Vulnerability Response das Dashboard Meine Anwendungsschwachstellen, mit dem Sie die Problembereiche überwachen können. Weitere Informationen finden Sie unter Dashboard Meine Anwendungsschwachstellen.

Ab Version 13.0 der Anwendung Vulnerability Response : Informationen zum Beschränken der für Berichte oder zugehörigen Listen gesammelten Datenmenge finden Sie unter Definieren Sie Serviceklassifizierungen für die Berichterstellung Vulnerability Response und zugehörige Listen.

- Überprüfen Sie den Status von AVITs in der Reihenfolge der Priorität, indem Sie nach Änderungen suchen.
- Überarbeiten Sie das Risiko für die AVITs nach Bedarf. Weitere Informationen finden Sie unter Erstellen Sie einen Anwendungsschwachstellen-Rechner.
- Weisen Sie die AVIT bei Bedarf zur Korrektur einer Zuweisungsgruppe zu.
- Erneute Scans werden automatisch durch den Importzeitplan der Drittpartei ausgelöst.
- Wenn der Status nach dem erneuten Scannen **Fest**ist, werden AVITs während des Imports automatisch geschlossen.
- Wenn der Status nach dem Scan nicht **Fest**ist, wird der AVIT erneut geöffnet.

Weitere Details erhalten Sie von Veracode

Wählen Sie in der Tabelle für angreifbare Elemente der Anwendung [sn_vul_app_vulnerable_item] oder in den Listenansichten in Vulnerability Response-Arbeitsbereichen für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs), bei denen Veracode als Quelle vorliegt, die **Option Weitere Details abrufen aus**, um die folgenden Veracode -Daten anzuzeigen.

- Details zu HTTP-Quellanforderungen und Quellantworten für DAST-Scans (Dynamische Anwendungssicherheitstests) werden in der zugehörigen Liste „HTTP-Anforderung/-Antwort“ angezeigt.
- Lösungsempfehlungen von Veracode werden in der zugehörigen Liste „Ergebnisse“ angezeigt.
- Die HTTP-Quellanforderung, die Quellantwort und die Empfehlungen werden auf der Registerkarte „Details“ in den Vulnerability Response-Arbeitsbereichen Vulnerability Response angezeigt.
- Die Spalte „Beschreibung“ wird in der Tabelle für angreifbare Elemente der Anwendung [sn_vul_app_vulnerable_item] unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellenbibliotheken anzeigen

Sie können Schwachstellendaten anzeigen, die aus der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder von Drittanbietern importiert wurden, um zu entscheiden, ob eine Korrekturaufgabe eskaliert werden soll.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Prozedur

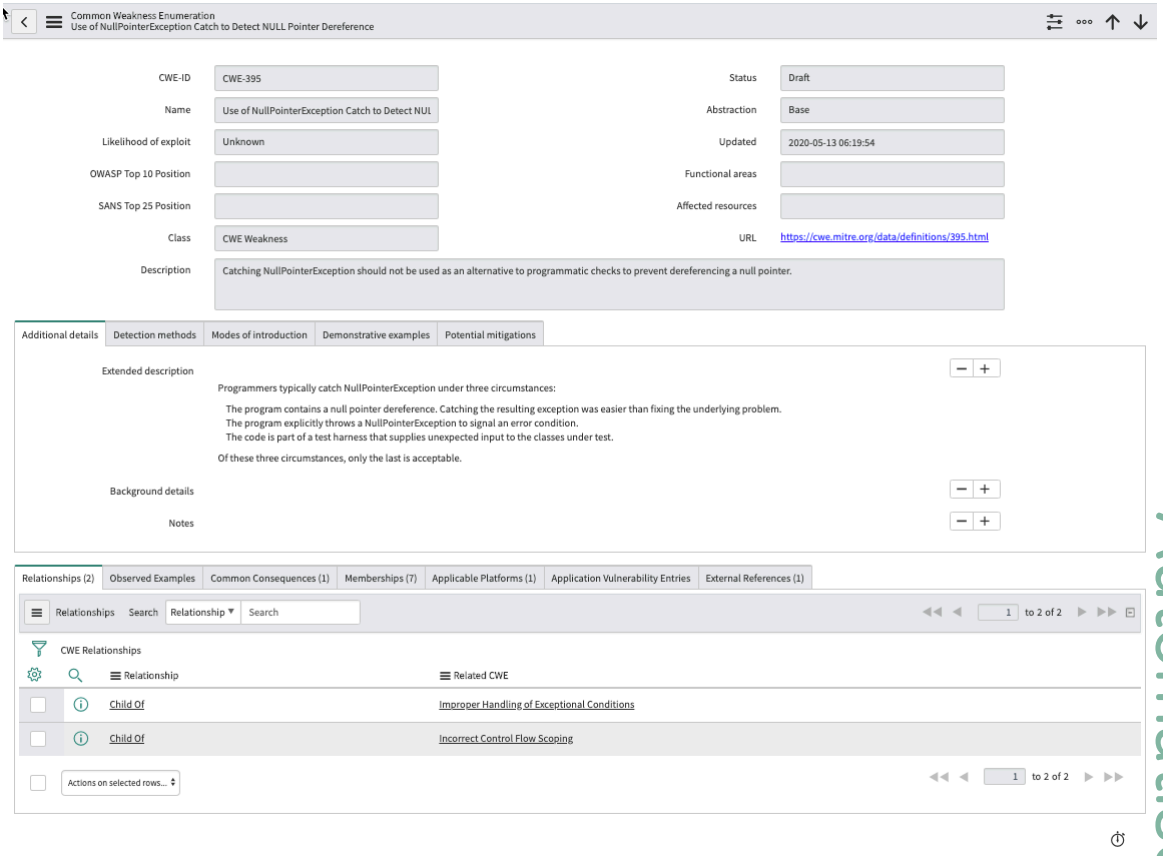
1. Navigieren zu **Alle** > **Application Vulnerability Response** > für **Bibliotheken**.

   Die folgenden Bibliotheken sind verfügbar:

Bibliotheken	Beschreibung
NVD	Liste der von NVD gefundenen Schwachstellen, einschließlich Sicherheitsprüflisten, sicherheitsbezogener Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits.
CWE	Liste der von der Community entwickelten Software-Schwachstellentypen. Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Common Weakness Enumerations“ eskalieren, er dient nur zur Referenz.
Drittpartei	Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits, CWEs und CVEs.

2. Wählen Sie eine Bibliothek, um Schwachstellen anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Informationen zu bestimmten Feldern finden Sie unter Anwendungsschwachstellen-Felder.

Anwendungsschwachstellen-Felder

Schwachstellen werden automatisch erstellt, wenn Datensätze aus der National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) oder Drittanbieterintegrationen heruntergeladen werden. NVD und CWE werden unter **Bibliotheken** in Vulnerability Response oder unter **Schwachstellen** in Application Vulnerability Responsegespeichert.

Eingabefelder für CWE-Schwachstellen

Die Felder in dieser Tabelle sind schreibgeschützt.

Feld	Beschreibung
CWE-ID	Bezeichner für diesen Schwachstelleneintrag. Dieser Bezeichner wird für Kategorien und Schwachstellen verwendet und ist für die beiden Datensätze eindeutig.
Name	Beschreibender Name, der dieser CWE-ID zugewiesen ist.
Wahrscheinlichkeit der Ausnutzung	Wie wahrscheinlich ist, dass die Schwachstelle ausgenutzt wird, auf einer qualitativen Skala. Einer der folgenden: • Niedrig • Mittel • Hoch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Position in OWASP Top 10	Die numerische Position dieser Schwachstelle in der OWASP-Top-10-Liste.
SANS bis Position 25	Numerische Position dieser Schwachstelle in der SAN-Top-25-Liste.
Klasse	Typ der Schwachstelle
Status	Einer der folgenden: • Unvollständig • Entwurf • Stabil • Überholt • Veraltet • Unstabil
Zusammenfassung	Einer der folgenden: • Variante • Klasse • Basis • Verbindung
Aktualisiert	Zeitpunkt der letzten Aktualisierung des Datensatzes in der Instanz.
Funktionsbereiche	Liste der betroffenen Funktionsbereiche. Beispiel: **Dateiverarbeitung**. Wird nur für 24/862-Schwächen ausgefüllt.
Betroffene Ressourcen	Liste der betroffenen Ressourcen. Zum Beispiel **Datei** oder **Verzeichnis**. Wird nur für 51/863-Schwächen ausgefüllt.
URL	Knowledge Base-Artikel, der dieser Schwachstelle zugeordnet ist.
Beschreibung	Beschreibung der Schwachstelle.
Integrationsausführung	Die Integrationsausführung, in die diese CWE importiert wurde.
Abschnitte	
Zusätzliche Details	Beschreibungen des Softwarekonzepts, die die Schwachstelle weiter erläutern. Beinhaltet: • Erweiterte Beschreibung • Hintergrunddetails • Notizen
Erkennungsmethoden	Details dazu, wie Sie diese Schwachstelle in einer Anwendung erkennen können.
Einführungsmodi	Die Phasen, in denen die Schwachstelle eingeführt wird, z. B. **Implementierung**, **Architektur und Design**usw.
Demo-Beispiele	Codebeispiele der Schwachstelle mit zugehörigen Beschreibungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Potenzielle Minderungen	Details dazu, wie die Schwachstelle verhindert werden kann, einschließlich Angabe, in welcher Phase des Anwendungslebenszyklus sie auftritt, und zur Effektivität der Minderung.
Zugehörige Listen	
Beziehungen	CWEs, die dieser Schwachstelle zugeordnet sind. Listet Beziehungen zwischen dieser CWE und anderen auf. Kann übergeordnetes/untergeordnetes Element, folgt/Vorrang, erforderlich von/erfordert (für zusammengesetzte Schwachstellen), CanAlsoBe, PeerOf, MemberOf einschließen.
Beispiele für Beobachtung	Einige CVEs, die für diese Schwachstelle repräsentativ sind
Häufige Konsequenzen	Konsequenzen eines erfolgreichen Exploits in Bezug auf Umfang und Auswirkung. Zum Beispiel: Geltungsbereich: Vertraulichkeit Auswirkung: Anwendungsdaten werden gelesen
Mitgliedschaften	CWE-Mitgliedschaften mit dieser Schwachstelle.
Anwendbare Plattformen	Plattformen, die dieser Schwachstelle zugeordnet sind.
Anwendungsschwachstelleneinträge	Andere Anwendungsschwachstelleneinträge, die mit einer verknüpft sind.
Externe Referenzen	Informationen zur Schwachstelle aus externen Quellen.

Eingabefelder für Anwendungsschwachstellen

Die Felder in dieser Tabelle sind schreibgeschützt.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Quelle	Ursprung der Schwachstelle – ob Scanner oder physischer Test.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle Schweregradzuordnungen werden für NVD und mit ServiceNow -Drittparteiintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu.
Version 13.0: Primäre CWE Version 12.1: CWE-Eintrag	Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt. Wenn der Schwachstelle mehrere CWEs zugeordnet sind, wird die primäre CWE wie folgt bestimmt: • Ist die CWE den OWASP Top 10 zugeordnet? Wenn ja, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort. • Wird die CWE den Top 25 SANs zugeordnet? Wenn ja, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Hat die CWE den höchsten Schweregrad? Wenn ja, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort. • Wählen Sie die neueste aller CWEs aus. Die neueste CWE ist die mit dem neuesten **aktualisierten** Feldwert im CWE-Datensatz.
Kategoriename	Von der Drittanbieterintegration bereitgestellte Klassifizierung. Hilft bei der Zuweisung.
Schwachstellendetails	
Bedrohung	Beschreibung der Bedrohung, die von dieser Schwachstelle ausgeht.
Beschreibung der Verringerung	Beschreibung der Schritte, die zum Mindern der Schwachstelle ausgeführt werden können.
Zugehörige Liste	
Version 13.0: CWEs	Liste der CWEs, die dieser Schwachstelle zugeordnet sind. Gilt nicht für Veracode Vulnerability Integration.

NVD-Eintragsfelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

Hinweis:

NVD-Daten werden in Application Vulnerability Response nicht verwendet, und Einträge repräsentieren nur Vulnerability Response -Daten.

CWEs, die in Application Vulnerability Responseverwendet werden, können auf NVD-Einträge als Beispiele für eine Schwachstelle verweisen und werden hier nur zu Informationszwecken bereitgestellt.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Risikobewertung	(Ausgeblendet, wenn der Schwachstelle keine Vulnerability Response angreifbaren Elemente zugeordnet sind) Quantifizierte **Risikopunktzahl,** die VIs in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt.
Risikopunktzahl	(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle in Vulnerability Response. Schweregradzuordnungen werden für NVD und mit ServiceNow -Drittparteiintegrationen bereitgestellt. Application Vulnerability Response **Der Schweregrad** wird vom importierten **Quellschweregrad** und nicht von NVD abgeleitet. Informationen zur Schweregradzuordnung Application Vulnerability

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Response finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu.
Exploit vorhanden	Ja, wenn dieser Schwachstelle mindestens ein Exploit zugeordnet ist.
Exploit-Kompetenzniveau	Niedrigste Kompetenzstufe, die zum Ausnutzen dieser Schwachstelle erforderlich ist.
Exploit-Angriffsvektor	Angreifbarster Angriffsvektor der Exploits für diese Schwachstelle.
Aktive AEs	(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) Anzahl der angreifbaren Elemente, die dieser Schwachstelle zugeordnet sind und sich nicht im Status „Geschlossen“ befinden. Wenn für diese Schwachstelle keine aktiven AVIs vorhanden sind, werden **Risikobewertung** und **Risikopunktzahl** nicht angezeigt.
CWE-Eintrag	Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle gemäß NVD am besten passt.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Zusammenfassung	Beschreibung der Schwachstelle.
Schwachstellendetails	
CVSS v2	CVSS v2-Daten importiert
CVSS v3	Importierte CVSS v3-Daten, vor 2015 nicht verfügbar.
Bevorzugte Lösung	(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) Höchste Ersatzlösung in der Kette, abgeleitet von den Lösungen, auf die in der Schwachstelle verwiesen wird. Wenn in der Kette mehr als eine höchste Ersatzlösung vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen.
Nachbesserungsstatus (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Anwendungselemente für diese Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
AEs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
AEs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle.
%VIs behoben	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle.
Zugehörige Links	
Vor v13.0: Import von Software-Schwachstellen erzwingen **Hinweis:** In v13.0 entfernt	(Veraltet) Berechnet die Produktzuordnung mit ITSM Software Asset Management basierend auf Informationen von NVD neu. Aktualisiert die Bibliothek für angreifbare Software.
Zustand aktualisieren	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Aktualisiert Folgendes: • Status der Korrekturaufgabe • Risikopunktzahl und Bewertung • Metriken wie Aktive AEs, AEs insgesamt aus dem Abschnitt „Korrekturstatus“.
Zugehörige Listen	
Angreifbare Elemente	(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind.
Verwundbarkeitsreferenzen	Informationen zur Schwachstelle aus externen Quellen, angegeben von NVD.
Exploits	Exploits, die dieser Schwachstelle zugeordnet sind.
Lösungen	(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) Alle Vulnerability Solution Management -Integrationslösungen, die dieser Schwachstelle zugeordnet sind.
Version 13.0: Schwachstellen	Importierte CWE-Schwachstellendaten, die Common Vulnerabilities and Exposures (CVE) zugeordnet sind.
Version 13.0: Software mit Schwachstellen	(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) Importierte CPE-Daten (Common Platform Enumeration), die der Schwachstelle zugeordnet sind.

Identifizieren Sie -Anwendungen in Application Vulnerability Response automatisch

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Application Vulnerability Response automatisch Anwendungsdaten, um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. Dies geschieht mithilfe von **CI-Suchregeln**. Diese Regeln identifizieren Anwendungen für den Datensatz des angreifbaren Elements in der Anwendung (Application Vulnerable Item, AVI), um bei der Behebung zu helfen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beim Importieren von Anwendungen wird mithilfe von source_app_id und app_name eine Suche für die gescannte Anwendung [sn_vul_app_scanned _application] durchgeführt, um Übereinstimmungen mit Anwendungen aus vorherigen Importen zu finden. Wenn eine Übereinstimmung mit der Anwendungs-ID gefunden wird, werden ihre Werte in den Feldern **„Anwendung“** und **„App-Release“** im Datensatz des angreifbaren Anwendungselements verwendet.

Wenn keine Übereinstimmung gefunden wird oder das Feld „Anwendungs-ID“ leer ist, versuchen die Regeln anhand der anderen Anwendungsinformationen, die Anwendung korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein als Platzhalter gescannter Anwendungsdatensatz nur mit den Feldern **Anwendungsname** und **Anwendungs-ID** erstellt.

Die Suchregeln **für Quellanwendungs-ID** und **Anwendungsname** sind standardmäßig im Lieferumfang von Veracode Vulnerability Integrationenthalten.

Hinweis:
Standardmäßige CI-Suchregeln für Application Vulnerability Response sind nur für die Schwachstellenintegration Veracode verfügbar.

Beim Versuch einer Übereinstimmung werden die Suchregeln zuerst anhand des niedrigsten **Reihenfolgewerts** ausgewertet. Sie werden beendet, wenn eine Regel ein einzelnes CI als Übereinstimmung zurückgibt.

Hinweis:
Wenn eine Regel so erstellt wird, dass mehr als ein CI zurückgegeben wird, wird nur die erste Übereinstimmung verwendet.

Um das Auffinden von Übereinstimmungsproblemen zu erleichtern, wird bei einer Übereinstimmung die verwendete CI-Suchregel zum Feld **„CI-Übereinstimmungsregel“** für Gescannte Anwendungen hinzugefügt. Klicken Sie oben in der Listenansicht der gescannten Anwendung auf das Personalisierte Liste aktualisieren, um sie der Ansicht hinzuzufügen.

Hinweis:
Einmal entfernte Regeln können nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

CI-Suchregeln können domänengetrennt sein und sind quellenspezifisch. Bei Unterstützung kann jede Quelle über mehrere Bereitstellungen verfügen. Beispielsweise kann Veracode Vulnerability Integration mehrere Bereitstellungen der Veracode Vulnerability Integration aufweisen. Jede Bereitstellung verfügt über einen eigenen Satz von CI-Suchregeln.

Hinweis:
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellen-Integration gemeinsam verwendet. Wenn eine Regel gelöscht oder geändert wird, wirken sich die Löschung oder Änderungen auf alle Bereitstellungen der Schwachstellenintegration aus.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Abgleichen von CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie alle anwenderdefinierten CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln**. Unter Verhindern Sie doppelte oder verwaiste Datensätze nach dem Ausführen von CI-Suchregeln für Application Vulnerability Response finden Sie weitere Informationen zum Verhindern des Duplikats von verwaisten Elementen, zum Löschen von Daten und zum Bereinigen von Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurationsverwaltung und die CMDB

Erstellen Sie eine CI-Suchregel

Das Modul **CI-Suchregeln** enthält Regeln, die definieren, welche Felder übereinstimmende Daten in Configuration Management Database (CMDB)enthalten. Diese Regeln werden verwendet, um Anwendungen und Anwendungs-Releases zu identifizieren und dem AVI-Datensatz (Application Vulnerable Item) hinzuzufügen, um die Nachbesserung zu unterstützen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Das Erstellen von CI-Suchregeln erfordert fortgeschrittene Kenntnisse ServiceNow von und Application Vulnerability Management. Anstatt eine der vorhandenen Suchregeln zu ändern, sollten Sie sie kopieren und die Kopie ändern. Wenn Sie zufrieden sind, dass die neue Regel das bewirkt, was Sie möchten, deaktivieren Sie die ursprüngliche.

Hinweis:
Einmal entfernte Regeln können nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **CI-Suchregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „CI-Suchregel“.

Feld	Beschreibung
Name	Name der Regel.
Suchmethode	Für die Übereinstimmung verwendete Methode. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Skript**: Vorgefertigtes oder anwenderdefiniertes Skript. ○ **Feldabstimmung**: Suchen Sie in der Tabelle oder dem Feld in der CMDB.
Typ	Typ, der mit der **Skriptsuchmethode**verwendet wird.
Bestellung	Rangfolge für die Regel. Übereinstimmungen mit der niedrigsten Reihenfolge werden zuerst ausgewertet.
Aktiv	Checkbox, um festzulegen, ob die Regel aktiv oder deaktiviert ist.
Quelle	Quelle, die als Eingabe für diese Regel verwendet wird. Nach der Auswahl werden Bedingungsfilter angezeigt.
Quellenfeld	Quellfeld, das als Eingabe für diese Regel verwendet wird. Felder müssen eine Zeichenfolge oder Zahl sein.
Beschreibung	Text, der die Regel beschreibt.
V19.0: Suchziel	Suchansatz, dem Sie folgen möchten. Wählen Sie aus:

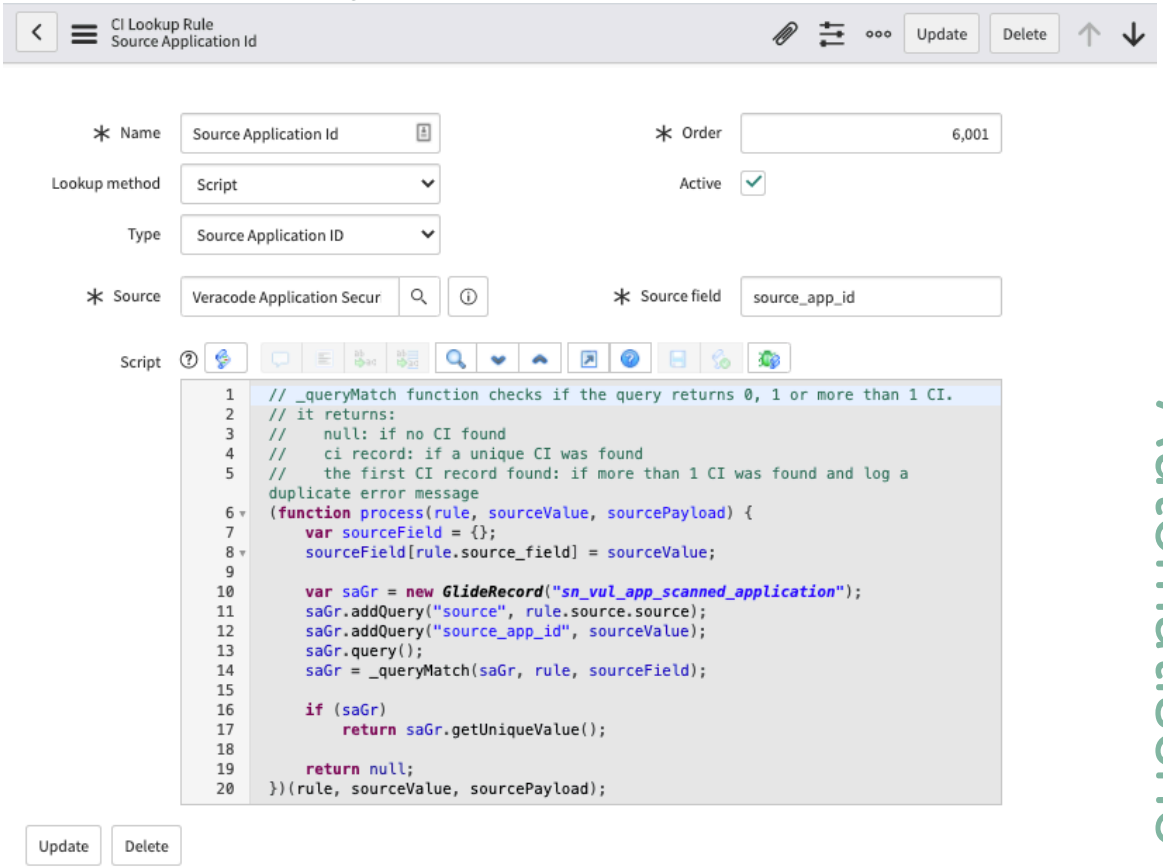
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Konfigurationselement ○ Produktmodell
Skript	Bearbeitbares Beispielskript, basierend auf dem **Typ**, wird angezeigt. Implementieren Sie das anwenderdefinierte Skript nach den Kommentaren, die in der Vorlage der Standardfunktion enthalten sind. **Hinweis:** Die Funktion process besitzt drei Parameter: `rule`, `sourceValue`und `sourcePayload`
Suchen Sie in der CI-Tabelle .	Tabelle für die Suche in der CMDB. Wird mit **der Suchmethode**für die Feldübereinstimmung verwendet.
V19.0: Produkttabelle durchsuchen	Wenn Sie das Produktmodell- **Suchziel**auswählen, lautet der Standardwert Anwendungsmodell.
Suchen Sie in CI Feld	Feld, das Informationen enthält, die zum Suchen eines CI verwendet werden können. Wird mit der **Suchmethode**für übereinstimmende Felder verwendet. Dieses Feld kann sich im CI-Datensatz oder in einem zugehörigen Datensatz wie einem Netzwerkadapter befinden.
V19.0: Suche im Produktmodellfeld	Wenn Sie das Produktmodell- **Suchziel**auswählen, lautet der Standardwert Name.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

Beispiel für eine CI-Suchregel mit einem Skript



Zugehörige Informationen

Felder für angreifbare Anwendungselemente

CI-Suchregeln werden in erneut angewendet Application Vulnerability Response

Sie können Ihre Suchregeln für Configuration Item (CI) erneut anwenden, um vorhandene CIs (gescannte Anwendungen und Produktmodelle) für erkannte Anwendungsdatensätze zu aktualisieren.

Eine Suchregel wird erneut angewendet

Wenn Sie die CI-Suchregeln erneut anwenden, werden alle aktivierten Regeln auf vorhandene erkannte Anwendungen angewendet. Das Aktualisieren der erkannten Anwendungsdatensätze kann einige Zeit in Anspruch nehmen.

Um die Regeln erneut auf vorhandene erkannte Anwendungen anzuwenden, navigieren Sie zu **Alle** > **Security Operations** > **CMDB** > **Suchregeln** und wählen Sie **Änderungen übernehmen aus**.

Hinweis:
Ab v25.0.3 von Application Vulnerability Responsewird die neue Regel für das automatische Schließen des Typs „CI außer Betrieb genommen“ eingeführt, um die angreifbaren Elemente und Erkennungen im Zusammenhang mit außer Betrieb genommenen CIs zu schließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchziel festlegen

Standardmäßig ist die Systemeigenschaft *sn_vul.use_product_model* aktiviert (auf **true**festgelegt). Abhängig davon, wie die Systemeigenschaft für die Datensätze der CI-Suchregel festgelegt ist, werden erkannte Anwendungsdatensätze wie folgt aktualisiert:

- Wenn das Feld Wert auf **true**festgelegt ist, ist das Produktmodell das Suchziel für CI-Suchregeln, und erkannte Anwendungen werden mit den Produktmodellen aktualisiert.
- Wenn das Feld Wert auf **false**festgelegt ist, ist Configuration Item (gescannte Apps) das Suchziel, und erkannte Anwendungen werden mit den Configuration Items (gescannte Anwendungen) aktualisiert.

So ändern Sie die Systemeigenschaft *sn_vul.use_product_model* so, dass Konfigurationselemente als Ziel verwendet werden:

1. Navigieren Sie als Benutzer mit der Rolle sn_vul.app_sec_manager zu **Alle** > **Systemeigenschaften** > **Alle**
2. Suchen Sie *sn_vul.use_product_model*.
3. Öffnen Sie den Datensatz.
4. Legen Sie das Feld Typ auf **den Wert false**fest.
5. Wählen Sie **Aktualisieren**.

Wenn Sie diese Systemeigenschaft zurücksetzen, müssen Sie Ihre Regeln ändern, damit die Suchziele mit der Einstellung der Systemeigenschaft übereinstimmen. Wenn Sie beispielsweise die Systemeigenschaft zurücksetzen, sodass Sie das Configuration Item als Ziel verwenden, suchen Sie die Regeln, die das Suchziel als Configuration Item festlegen.

1. Aktivieren Sie für diese Regeln das Kontrollkästchen Aktiv, und wählen Sie **Aktualisieren**aus.
2. Suchen Sie die Regeln, die das Produktmodell als Ziel verwenden, und deaktivieren Sie sie, indem Sie das Kontrollkästchen Aktiv deaktivieren und **Aktualisieren**wählen.

Wenn Sie eine neue Suchregel erstellen, legen Sie das Suchziel für die Regel im Regelformular fest. Weitere Informationen finden Sie unter Erstellen Sie eine CI-Suchregel.

Verhindern Sie doppelte oder verwaiste Datensätze nach dem Ausführen von CI-Suchregeln für Application Vulnerability Response

Ergreifen Sie Maßnahmen, um zu verhindern, dass doppelte oder verwaiste Datensätze durch den Abgleich von (Configuration Items (CI)) in CMDBentstehen.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die zum Iterieren und Abgleichen in der CMDB verwendete Logik kann zu langen Verarbeitungszeiten führen. Gründliches Testen und Debuggen von Verarbeitungsskripts in den Regeln trägt dazu bei, das Risiko von Problemen später im Prozess zu minimieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Doppelte oder verwaiste Datensätze verhindern

- Verwenden Sie kleine Teilmengen von Daten, die für die getestete CI-Suchregel spezifisch sind.
  - Legen Sie alle anderen **CI-Suchregeln**als die, die gerade getestet werden, auf **Inaktiv fest**.
  - Analysieren Sie die importierten Anwendungen und Configuration Items (CIs), um sicherzustellen, dass Sie das erwartete Verhalten beobachten und die Übereinstimmung ordnungsgemäß erfolgt.
- Überprüfen Sie CI-Status wie **Deaktiviert**.
- Entfernen Sie Testdaten. Sobald Sie beginnen, das richtige oder erwartete Verhalten beim CI-Abgleich zu beobachten, beginnen Sie von vorne. Sie können dies wie folgt tun:
  - Die zum Testen verwendeten Daten werden gelöscht: (siehe Abschnitt „ **Daten aus Tabellen löschen** “)
    - Gescannte Anwendungen
    - Angreifbare Anwendungselemente (AVIs)
  - Führen Sie die Integrationen manuell erneut aus.

.

Daten werden aus Tabellen gelöscht

Manchmal haben Sie Daten importiert und stellen fest, dass etwas nicht stimmt. Wenn dies in einer Entwicklungs- oder Leistungsumgebung passiert, können Sie aus einer besseren Umgebung erneut klonen. Das ist jedoch nicht immer eine Option.

Hinweis:
Das Ausführen dieser Aktionen erfordert fortgeschrittene Kenntnisse über ServiceNow.

Es gibt vier Optionen zum Löschen von Daten aus Tabellen:

- **Alle Datensätze löschen** in **der Tabellenkonfiguration**verwendet.
- Konfigurieren Sie die **Tabellenbereinigung**, indem Sie zu **Automatisch Leerungen** (sys_auto_flush.list) navigieren und einen neuen Datensatz **für die automatische Leerung** erstellen.
- Kürzen Sie gs.truncateTable mit einem Hintergrundskript.

  Hinweis:
  Verwenden Sie `truncateTable` niemals in einer Produktionsumgebung. Wenden Sie sich an Ihren Support-Mitarbeiter, bevor Sie große Löschungen in Produktionsumgebungen oder gemeinsam genutzten Umgebungen ausführen.

- Erstellen Sie in HI einen Antrag, um die Daten löschen zu lassen.

Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu

Weisen Sie Anwendungsschwachstellen automatisch basierend auf Anwendungs-Tags oder einer der Zuweisungsgruppen im Konfigurationselement [cmdb_ci] oder Plattform-Zuweisungsgruppen zu, um die durchschnittliche Zeit bis zur Zuweisung zu verkürzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbare Anwendungselemente werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, AVIs mit **Zuweisen mit zuzuweisen**:

Hinweis:
Die Funktion für Zuweisungsempfehlungen in Vulnerability Response ist für Application Vulnerability Responsenicht verfügbar.

- Anwendergruppe: Mit dieser Option können Sie eine der vorhandenen Now Platform® -Anwendergruppen auswählen.
- Anwendergruppenfeld: Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle cmdb_ci verfügbar ist. Standardmäßig werden im Listenmenü unter **Benutzergruppenfeld**die folgenden drei Gruppenfelder angezeigt.
  - Keine: Gibt an, dass für dieses Pflichtfeld kein Standardwert vorhanden ist
  - Konfigurationselement: Genehmigungsgruppe
  - Konfigurationselement: Zuweisungsgruppe
  - Konfigurationselement: Supportgruppe
- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Kenntnisse in der Codierung oder fortgeschrittenen ServiceNow.

Führen Sie zuerst Regeln mit hoher Priorität aus (Elemente, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist oder bei denen ein AVI von der Compliance-Abteilung behandelt werden sollte). Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist und Sie wissen, wer dafür verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um der Gruppe AVIs zuzuweisen, die bestimmt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt.

Bewertungsprozess für Zuweisungsregeln

Wenn ein neues AVI erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Zuweisungsregeln dafür ausgewertet. Ein AVI wird nur einmal ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet. Sie können Regeln nach Änderungen manuell erneut anwenden.

Der folgende Prozess wird für jedes neue, aktualisierte oder erneut geöffnete AVI verwendet:

- Für jede Zuweisungsregel für Schwachstellen wird die AVI mit dem Zuweisungsfilter verglichen, wobei zuerst die Regel niedrigster Ordnung verwendet wird.
- Wenn die Bedingung erfüllt ist, wird die AVI einer Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung mit allen anderen Regeln finden, wird die AVI der Standardzuweisungsgruppe zugewiesen, sofern eine Standardregel vorhanden ist.

Hinweis:
Wenn keine Standardregel vorhanden ist, bleibt die AVI nicht zugewiesen.

Zuweisungstyp: **Manuell** oder **Regel**. **Die Zuweisungsregel** ist im Slushbucket für das Formularlayout im Formular für angreifbare Elemente der Anwendung verfügbar. Jedes AVI,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das ursprünglich von einer Regel zugewiesen wurde, später aber manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel. Verwenden Sie **Zuweisungsregel-** und **Zuweisungstypinformationen,** um Fälle zu identifizieren, in denen die Zuweisungsregeln keine richtige Übereinstimmung für den beabsichtigten Empfänger gefunden haben. Oder welche Regeln die meisten Neuzuweisungen hatten.

Hinweis:
Manuell erstellte Zuweisungen werden durch die Zuweisungsregeln nicht neu bewertet.

Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie die Schaltfläche **Changes übernehmen** in der Listenansicht Zuweisungsregeln, um alle geänderten Regeln für alle aktiven offenen AVIs erneut auszuführen (mit Ausnahme der manuell zugewiesenen).

Hinweis:

Wenn die geplante Aufgabe *`Reapply all vulnerability assignment rules`* vor der ersten Verwendung **von Änderungen anwenden**nicht ausgeführt wurde, werden alle Zuweisungsregeln für alle offenen AVIs mit Ausnahme der manuell zugewiesenen AVIs ausgeführt. Danach werden bei allen nachfolgenden Verwendungen von **Changes übernehmen** nur die geänderten Regeln und alle abhängigen Regeln erneut ausgeführt. Änderungen an einer Regel können dazu führen, dass ein AVI mit einer anderen unveränderten Regel übereinstimmt. [store-future: BEGIN review]Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.[End]

Die geplante Aufgabe [*`Reapply all assignment rules`*] ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle Regeln auf alle offenen AVIs angewendet, mit Ausnahme der manuell zugewiesenen. Sie kann **Täglich**, **Wöchentlich**, **Monatlich**, **Regelmäßig**, **Einmal**oder **Bei Bedarf**ausgeführt werden. Je nachdem, wie viele aktive AVIs Sie in Ihrer Umgebung haben, denken Sie daran, das Feld **Ausführen** nach der ersten Ausführung entsprechend zu setzen, um Auswirkungen auf die Leistung zu vermeiden.

Erstellen oder bearbeiten Sie Application Vulnerability Response -Zuweisungsregeln

Sie können Regeln für die automatische Zuweisung von angreifbaren Elementen in Anwendungen (Application Vulnerable Items, AVIs) basierend auf Filterbedingungen erstellen. Diese Regeln weisen AVIs zu, wenn sie importiert oder manuell erstellt werden.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Mit Zuweisungsregeln definieren Sie die Zuweisungsbedingungen und die Reihenfolge der Ausführung. Sobald ein AVI mit einer Regelbedingung übereinstimmt, wird die Zuweisungssuche beendet. Weitere Informationen finden Sie unter Filtern in Application Vulnerability Management.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Klicken Sie auf **Neu**.
3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisungsregel für Anwendungsschwachstellen

Feld	Beschreibung
Name	Name der Gruppenregel.
Aktiv	Gibt an, ob die Zuweisungsregel aktiv ist.
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Regeln mit hoher Priorität, Elemente, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist, oder eine AVI, die von der Compliance mit Vorschriften und Gesetzen behandelt werden sollten, um zuerst ausgeführt zu werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist, und Sie wissen , wer dafürverantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um der Gruppe AVIs zuzuweisen, die bestimmt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt.
Beschreibung	Beschreibung der Zuweisungsregel.
Bedingung	
Bedingungsfelder	Bedingungen, die erfüllt werden müssen.
Neues Kriterium	Fügt weitere Bedingungsfilterfelder zur Auswahl hinzu.
Zuweisen mit	Um die Zuweisung von anhand dieser Regel erstellten Gruppen zu automatisieren, wählen Sie eine der verfügbaren Optionen aus. ○ Anwendergruppe: Wählen Sie eine Anwendergruppe aus der Suchtabelle aus. ○ Anwendergruppenfeld: Wählen Sie ein Anwendergruppenfeld aus dem Listenmenü aus. ○ Skript: Erstellen oder bearbeiten Sie ein Skript. **Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert das Fachwissen ServiceNow.

4. Klicken Sie auf **Absenden**.
   Neue oder aktualisierte Regeln werden beim nächsten Import bewertet.

Risiko in Application Vulnerability Response automatisch berechnen

Anwendungsschwachstellen-Rechner automatisieren die Berechnung der anfänglichen Risikowerte für die Felder in angreifbaren Elementen der Anwendung (Application Vulnerable Items, AVIs). Risikoberechnungen bieten Einblicke in die Priorisierung der Problembehebung. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste passende Rechner wird verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsschwachstellen-Rechner

Das -Basissystem Application Vulnerability Response enthält zwei Schwachstellen-Rechner, die die Basis- **Risikopunktzahl** für das angreifbare Anwendungselement festlegen.

- **Basisrisiko-Rechner**
- **Rechner für erweitertes Risikomanagement**

Anwendungsschwachstellen-Rechner können so erstellt werden, dass sie mithilfe von Bedingungsfiltern die Auswirkungen von AVIs anhand beliebiger Kriterien priorisieren und bewerten. Unabhängig davon, ob es sich um die geschäftlichen Auswirkungen der Schwachstelle, die Klasse des Konfigurationselements (Configuration Item, CI) oder das Alter des AVI handelt, können Sie zusätzliche Schwachstellen-Rechner erstellen, um andere Felder in AVIs festzulegen. Oder Sie können die vorhandenen Schwachstellen-Rechner anpassen. Ein Rechner kann so geschrieben werden, dass er jeden Satz von Prioritäten widerspiegelt. Weitere Informationen finden Sie unter Filtern in Application Vulnerability Management.

AVIs enthalten den von den Risikorechnern abgeleiteten **Risikopunktzahlwert**.

Hinweis:
Eine AVI zeigt **den Quellenschweregrad**, aber nicht den normalisierten Schweregrad an. Der normalisierte Schweregrad wird von den Rechnern verwendet, um den Wert **der Risikopunktzahl** zu erhalten, wird jedoch nicht in AVIs angezeigt.

Jeder Rechner enthält eine Liste von Rechnerregeln, wobei eine Bedingung bestimmt, wann sie angewendet wird. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel der Reihe nach ausgewertet, und die erste passende Rechnerregel wird verwendet.

Alle aktivierten Schwachstellen-Rechner legen die ausgewählten Felder jedes Mal fest, wenn ein AVI erstellt wird, wenn sich ein zugehöriges CI oder eine zugehörige Schwachstelle ändert.

Der Rechner **für das Basisrisiko** berechnet **die Risikopunktzahl** für AVIs anhand des normalisierten Schwachstellenschweregrads.

Hinweis:
Pro Zielfeld (**Risikopunktzahl**) kann jeweils nur ein Rechner aktiv sein.

Das **Basisrisiko** ist standardmäßig aktiviert. Der **Rechner für erweitertes Risikomanagement** ist standardmäßig inaktiv.

Regeln des Anwendungsschwachstellen-Rechners

Der **Basisrisiko-** Rechner des Basissystems enthält Rechnerregeln, die jedem Schweregrad (Keine bis Kritisch) einen Wert (0–100) für **die Risikopunktzahl** basierend auf dem Schweregrad zuweisen. **Dem Schweregrad „Unbekannt“** wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden, und wie **beim erweiterten Risikorechner**können neue Rechnerregeln oder neue Risikoregeln erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v23.0 von Application Vulnerability Responsewird bei jeder Aktualisierung der Risikopunktzahl für eine AVIT der Abschnitt **„Hinweise“** mit den folgenden Details aktualisiert:

- Name der Rechnergruppe
- Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, werden dem Namen die Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und aktivieren Sie das Kontrollkästchen **Erweiterte Ansicht**. Wählen Sie im Dropdown-Feld **Werttyp** die gewünschte Option aus. Wenn **Vorlage** ausgewählt ist, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** ausgewählt ist, können Sie entweder das vorhandene Skript hinzufügen oder aktualisieren. Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes` hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v25.0.3 von Application Vulnerability Responseist die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes` standardmäßig deaktiviert. Wenn Sie die Option aktivieren, können Sie nur dann im Abschnitt „Arbeitsnotizen“ alle Änderungen anzeigen, die sich auf die Risikopunktzahl eines angreifbaren Anwendungselements beziehen. Darüber hinaus werden die Arbeitsnotizen nur aktualisiert, wenn sich die Risikopunktzahl ändert.

Der Rechner **für das erweiterte Risikomanagement** des Basissystems enthält eine spezielle Regel für den Schwachstellen-Rechner namens **Standardrisikoregel**. Es berechnet **die Risikopunktzahl** basierend auf mehreren Werten:

- Schwachstellenschweregrad
- OWASP Top 10
- SANS Top 25

Sie können die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel.

Sie können die Werte anpassen, die in der **Standardrisikoregel** verwendet werden sollen, und festlegen, wie viel Gewichtung jeder dieser Werte erhalten soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der **Risikopunktzahl**zählt.

Jede Regel hat eine Einstellung **für Reihenfolge.** Die erste Regel, die den Bedingungen entspricht, aktualisiert jedoch das Feld **Risikopunktzahl** in der AVI. Rechnerregeln ohne Skript haben in der Regel weniger Auswirkungen auf die Leistung als Rechnerregeln mit Skript.

Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen wird basierend auf Faktoren wie Schweregrad, Kritikalität, Exploit-Informationen usw. eine Risikopunktzahl und Bewertung zugewiesen. Die Geschäftsregel `Update Risk Rating from Risk Score` in der Tabelle der angreifbaren Elemente ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert waren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Ab Version 18.0 von Vulnerability Response,

- Die Risikoeinstufungstypen werden in der Basistabelle als avr_risk_rating geliefert. Diese Typen werden als Teil der Geschäftsregel in jeder Tabelle übergeben, in der die Risikoeinstufung berechnet wird.
- Das Skript wird so geändert, dass Sie die Einträge in der Tabelle „Risikopunktzahlgewichtungen“ für die Berechnung der Risikoeinstufung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, müssen Sie die Bezeichnungen für die neue Risikoeinstufung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Risikopunktzahlgewichtungen“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn ein Configuration Item (CI) von ohne Internetzugriff in mit Internetzugriff geändert wird.
- Wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittparteieinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer Known Exploit Vulnerability (KEV) verknüpft sind.

Definieren Sie Felder und Gewichtungen für die Risikoregel

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, um Risikopunktzahlen zu generieren, die die für Ihre Organisation eindeutigen Schwachstellen- und Asset-Daten verwenden. Durch Auswahl der Felder, die in der Risikoregel enthalten sind, können Sie ein effektives Framework für die Risikobewertung definieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_manage_risk_score_configuration

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**.
2. Klicken Sie auf der Seite „Schwachstellen-Rechner **“ auf Erweiterter Risikorechner**.
3. Navigieren zu **Seite „Schwachstellen-Rechner“.** > **Registerkarte Regeln des Schwachstellen-Rechners** > **Standardrisikoregel**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. **Wahlweise:** Legen Sie im Abschnitt „Kriterien des Risikorechners“ der Seite „Regel für Schwachstellenrisiko“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung in der Berechnung der Gesamtrisikopunktzahl fest.
5. Um die Regel zu deaktivieren, müssen Sie das Kontrollkästchen **Aktiv** deaktivieren.
6. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien hinzufügen**.
7. Füllen Sie die Felder des Formulars aus.

Formular „Risikoregelfeld“.

Feld	Beschreibung
Referenztabelle auswählen	Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Sie können eine dieser Optionen auswählen: ○ **Angreifbares Anwendungselement**: Fügen Sie Felder hinzu, die direkt vom angreifbaren Element (VI) aus punktweise durchlaufbar sind. ○ **Angreifbares Anwendungselement – Konfigurationselement**: Fügen Sie Dot-Walking-Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. die Hardwaretabelle. Diese Felder sind nicht Teil der Basistabelle (cmdb_ci). ○ **Angreifbares Anwendungselement – Schwachstelle**: Fügen Sie Dot-Walking-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. Drittpartei-Eintrag. Diese Felder sind nicht Teil der Basistabelle des Schwachstelleneintrags. ○ **Referenztabelle für angreifbare Anwendungselemente**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) oder Tabellen sind, die einen Verweis auf das angreifbare Element enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar. ○ **Referenztabelle für Konfigurationselement**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar. ○ **Referenztabelle für Schwachstellen**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von „sn_vul_entry“ sind, oder Tabellen, die einen Verweis auf „sn_vul_entry“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar. ○ **Anwenderdefinierte Bedingungen**: Verwenden Sie diese Option, um der Regel durch Auswertung der Bedingung Gewichtungen zuzuweisen. Beispielsweise bestimmt der Filter mit Internetverbindung, ob ein Configuration Item (CI) extern oder intern ist.
Tabelle	Feld, das nur angezeigt wird, wenn in der Referenzauswahltabelle eine der folgenden Optionen ausgewählt wird: ○ **Angreifbares Anwendungselement -> Konfigurationselement** ○ **Angreifbares Anwendungselement -> Schwachstelle** ○ **Referenztabelle für angreifbare Anwendungselemente** ○ **Referenztabelle für Konfigurationselemente** ○ **Referenztabelle für Schwachstellen**
Feld	Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet werden soll.
Aggregation	Feld, das nur angezeigt wird, wenn eine Referenztabelle aus der Referenztabelle auswählen ausgewählt wird. Wählen Sie den Mindest- oder Höchstwert aus, der für Berechnungen berücksichtigt werden soll, wenn das Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird.
Gewichtung	Gewichtung dieses Feldes innerhalb der Risikoregel. Der Wert muss eine ganze Zahl von 0 bis 100 sein.
Definieren Sie die Wertgewichtung	Komponente zum Zuweisen von Gewichtungen zu jedem Feldwert. Für numerische Felder können Feldwerte als Bereich definiert werden (z. B. 1–5). Die Gewichtungen müssen Ganzzahlen zwischen 0 und 100 sein. **Hinweis:** Dieses Feld wird nicht angezeigt, wenn in der Referenzauswahltabelle die Option Anwenderdefinierte Bedingungen ausgewählt ist.
Bedingungstabelle	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenzauswahltabelle ausgewählt werden. Wählen Sie eine Bedingung aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Feldname	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenzauswahltabelle ausgewählt werden. Geben Sie einen Namen für die Risikokriterien ein.
Bedingung	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenzauswahltabelle ausgewählt werden. Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen.

8. Klicken Sie auf **Absenden**.
9. Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für die aktiven angreifbaren Elemente neu zu bewerten.

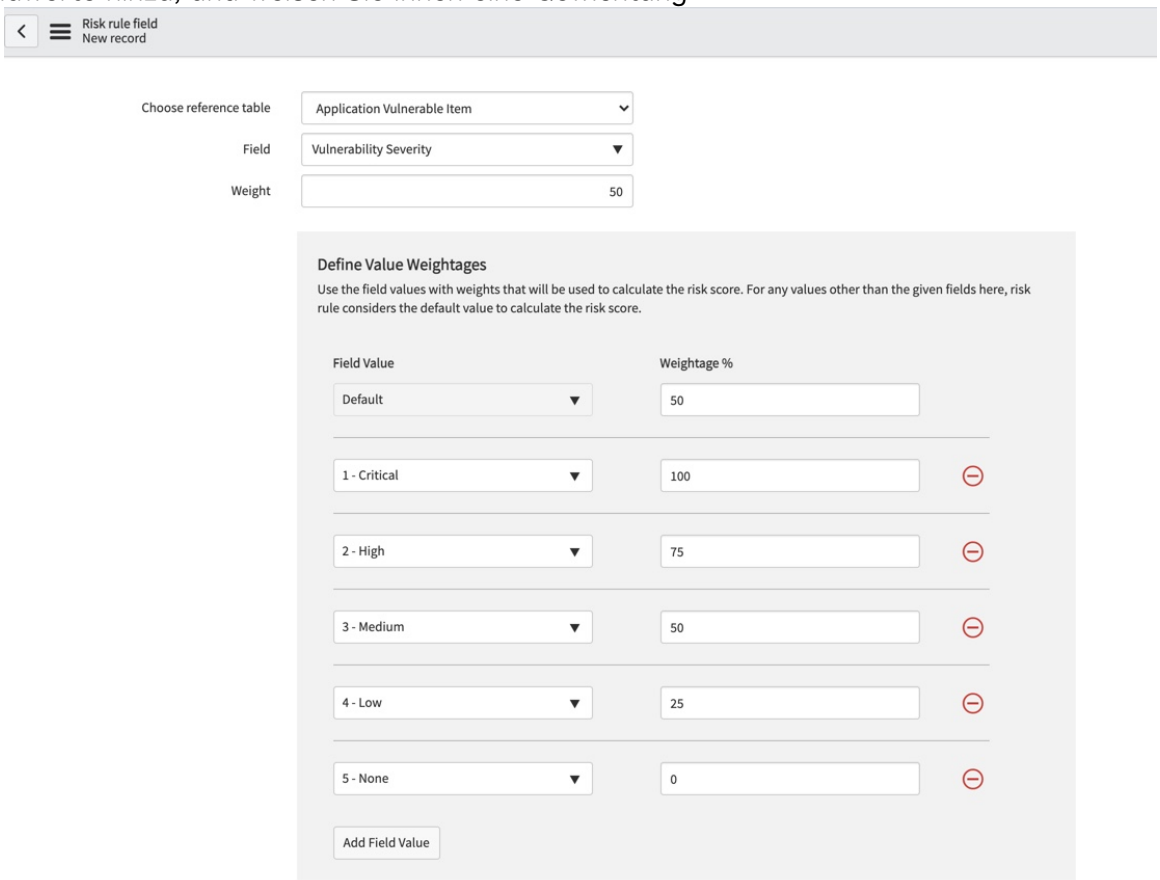
Example:
Fügen Sie den Schweregrad der Quelle als Kriterium für eine Risikoregel hinzu.

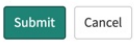
Anwendungsfall: Drittanbieter wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden im Feld **Quellenschweregrad** in der Tabelle sn_vul_entry eingetragen. Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl. Um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

1. Navigieren Sie zur Seite Risikoregel.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien hinzufügen**.
4. Wählen Sie in der Liste Referenztabelle auswählen **die Option Angreifbares Anwendungselement**aus.
5. Wählen Sie in der Liste Feld die Option **Vulnerability.Severity**aus.
6. Geben Sie im Feld **Gewicht** die relative Bedeutung des Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl von 0 bis 100 sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Fügen Sie im Abschnitt „Wertgewichtung definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung



zu. 

8. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Vulnerability Response-Rechner und Regeln des Schwachstellen-Rechners

Erstellen Sie einen Anwendungsschwachstellen-Rechner

Ein Anwendungsschwachstellen-Rechner enthält eine vordefinierte Formel zur Berechnung eines Zielfelds, wenn bestimmte Kriterien erfüllt sind. Rechner, die die **Risikopunktzahl**des angreifbaren Elements (AVI) der Anwendung berechnen, können **Risikoregeln**enthalten. Risikoberechnungen bieten Einblicke in die Priorisierung der Problembehebung.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Hinweis:

Beim Ausführen von Anwendungsschwachstellen-Rechnern, die Skripts enthalten, kann es zu einer Verschlechterung der Leistung kommen.

Ordnen Sie Ihre Regeln so an, dass die einfachsten Regeln zuerst ausgeführt werden. Führen Sie Skripts nur für die Elemente aus, die nicht mit einer Bedingung und einem Vorlagenwert oder einer Risikoregel behandelt werden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Formular „Schwachstellen-Rechner“.

Feld	Beschreibung
Name	Der Name des Anwendungsschwachstellen-Rechners.
Tabelle	Automatisch mit dem Namen der AVI-Tabelle ausgefüllt.
Anwendung	Automatisch ausgefüllt mit Vulnerability Response.
Zielfeld	Zu berechnendes Feld.
Beschreibung	Textbeschreibung des Rechners.
Aktiv	Rechner ein- oder ausschalten.

4. Klicken Sie mit der rechten Maustaste in den Header, um **Speichern**zu wählen.
   Der Abschnitt **Regeln des Schwachstellen-Rechners** wird angezeigt.
5. Erstellen Sie eine Regel für den Rechner, indem Sie auf **Neu**klicken.

Hinweis:
Das Formular **„Neue Risikoregeln“** (nur verfügbar, wenn das **Feld Zielauf Risikopunktzahl**festgelegt ist) finden Sie in Schritt 10.

6. Füllen Sie die Felder entsprechend aus.

Formular „Regel des Schwachstellen-Rechners“.

Feld	Beschreibung
Name	Name der Rechnerregel.
Bestellung	Reihenfolge, in der der Schwachstellen-Rechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeneintrag von 100 wird vor einem Rechner mit einem Reihenfolgeneintrag von 200 ausgeführt.
Rechner	Automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist das Kontrollkästchen **Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden.
Erweiterte Ansicht	Wenn diese Option ausgewählt ist, können geskriptete Bedingungen und geskriptete Werte unter **Bedingungstyp** und **Werttyp**ausgewählt werden.

7. Füllen Sie die Felder auf der Registerkarte **Wenn diese Bedingung erfüllt ist** entsprechend aus.

Registerkarte, wenn diese Bedingung erfüllt ist

Feld	Beschreibung
Bedingungstyp	Verfügbar, wenn Sie die **Ansicht „Erweitert“**auswählen. Zur Auswahl stehen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Filter: Verwendet Filterbedingungen. ○ Filtergruppe: Siehe Filtergruppen erstellen und definieren, um die Rechnerkriterien zu definieren. ○ Skript: Skriptbedingung, anhand derer bestimmt wird, wann dieser Rechner angewendet werden soll. **Hinweis:** Bevor Sie Skripts schreiben, um zu bestimmen, wann die Rechner angewendet werden sollen, kehren Sie zur Liste **der Rechner für Anwendungsschwachstellen** zurück. Machen Sie sich mit den Datensätzen des Schwachstellen-Rechners vertraut, die im Lieferumfang des Basissystems enthalten sind.
Bedingung	Definiert grundlegende Filterbedingungen, um zu bestimmen, ob der Rechner verwendet werden soll oder nicht. Wenn Sie entweder den Bedingungstyp **„Filtergruppe“** oder **„Skript“** auswählen, wird dieses Feld ausgeblendet.

8. Klicken Sie auf die Registerkarte **Diese Werte festlegen**, und füllen Sie die Felder im Formular entsprechend aus.

Legen Sie die Registerkarte für diese Felder fest

Feld	Beschreibung
Werttyp	Verfügbar, wenn Sie die **Ansicht „Erweitert“**auswählen. Zur Auswahl stehen: ○ Vorlage: Definieren Sie die Werte, die für jedes Feld festgelegt werden sollen. ○ Skript: Wird verwendet, um die Werte für jedes Feld festzulegen.
Skriptwerte	Verfügbar, wenn Sie den Werttyp **„Skript“** ausgewählt haben. Definiert, auf welche Werte die Berechnungen angewendet werden sollen.
Vorlage	Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten. Wenn Sie den Werttyp **„Skript“** auswählen, wird dieses Feld ausgeblendet.

9. Wenn Sie alle Eingaben abgeschlossen haben, klicken Sie auf **Absenden**.

Hinweis:
Wenn Sie einen vorhandenen Rechner bearbeiten und alle vorhandenen Punktzahlen aktualisieren möchten, können Sie die Schaltfläche **Rechner erneut** anwenden verwenden. Er durchläuft alle aktiven AVIs, und wenn dieser Rechner zum Festlegen des Werts verwendet wird, berechnet er den Wert für diese AVIs neu. Da das erneute Anwenden eines Rechners sehr lange dauern kann, wird dies von einer regelmäßigen Aufgabe verarbeitet.

10. Füllen Sie im Formular **„Neue Risikoregeln“** die entsprechenden Felder aus.

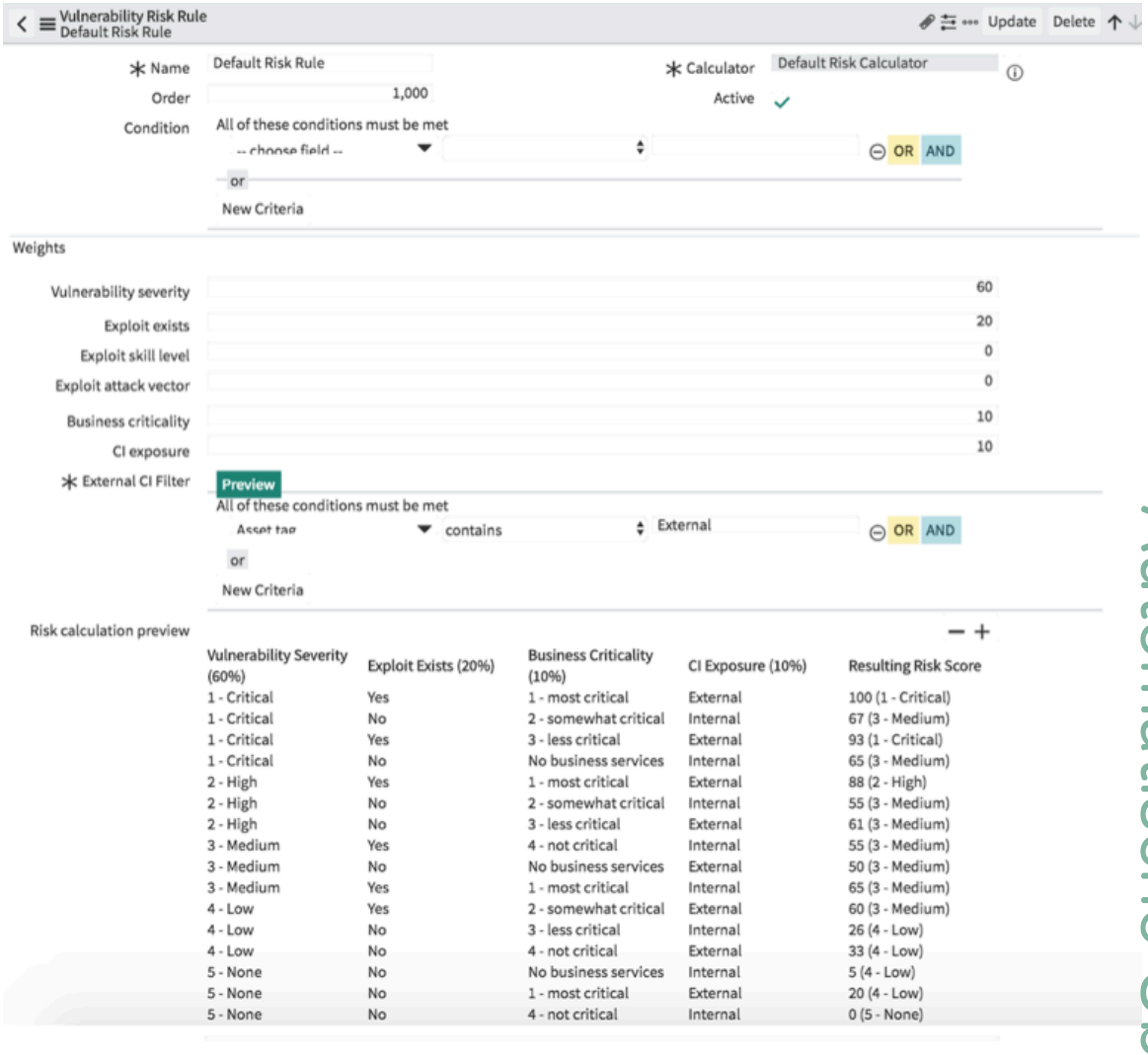
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie jede Gewichtung entsprechend dem Prozentsatz des Ergebnisses fest, der von diesem Wert stammen soll. Legen Sie für alle Daten, die Ihr Scanner nicht bereitstellt, oder für Daten, die nicht Teil der Risikopunktzahl sein sollen, die Gewichtung auf Null fest.

Wenn Sie die Gewichtungen aktualisieren, zeigen die Szenarien die verbleibenden Gewichtungen sowie die erwarteten **Risikopunktzahlergebnisse** an.

Feld	Beschreibung
Name	Name der Rechnerregel.
Bestellung	Die Reihenfolge, in der der Rechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeneintrag von 100 wird vor einem Rechner mit einem Reihenfolgeneintrag von 200 ausgeführt.
Rechner	Automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist das Kontrollkästchen **Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden.
Bedingung	Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll. Wenn Sie entweder den Bedingungstyp **„Filtergruppe“** oder **„Skript“** auswählen, wird dieses Feld ausgeblendet.
Gewichtungen	
Schwachstellenschweregrad	Prozentsatz des Ergebnisses, der sich aus dem Schweregrad ergibt.
OWASP Top 10	Prozentsatz des Ergebnisses, der sich aus dem Vorhandensein der Schwachstelle in der OWASP-Top-10-Liste ergibt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0.
SANS Top 25	Prozentsatz des Ergebnisses, der sich aus dem Vorhandensein der Schwachstelle in der SANS-Top-25-Liste ergibt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0.
Laufende Summe	Automatisch berechnete Prozentsätze insgesamt. Wenn dieser Wert 100 erreicht, zeigt die Szenariovorschau Beispiel-Risikopunktzahlen in verschiedenen Szenarien an.
Beispielszenarien	Wenn alle Gewichtungen insgesamt 100 % ergeben, werden Risikopunktzahl-Szenarien angezeigt, die eine Vorschau der Risikopunktzahl in einigen der möglichen Szenarien bieten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Klicken Sie auf **Absenden**.

Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu

Die SchweregradzuordnungApplication Vulnerability Response wandelt Quellschweregradfelder von Drittparteien in erkennbare Felder innerhalb von Vulnerability Responseum.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Application Vulnerability Response Drittanbieterintegrationen wie Veracode Vulnerability Integration bieten Schweregradzuordnungen bei der Installation. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.

Das Erstellen oder Bearbeiten einer Schweregradzuordnung ist nur für anwenderdefinierte oder nicht standardmäßige Drittparteizuordnungen in Ihrer Umgebung vorgesehen und erfordert das Fachwissen Application Vulnerability Response und ServiceNow.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Normalisierte Schweregradzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldzuordnung

Feld	Beschreibung
Quelle	Der Name der Quelle für die Schweregradzuordnung.
Quellwert	Der Wert des Quellschweregrads.
Zielwert	Der Zielschweregradwert. Die Auswahlmöglichkeiten lauten wie folgt: ○ 1 – Kritisch ○ 2 – Hoch ○ 3 – Mittel ○ 4 – Niedrig ○ 5 – Keine

4. Wiederholen Sie Schritt 3 für jeden Quellschweregrad.
5. Klicken Sie auf **Absenden**.

Filtern in Application Vulnerability Management

Rechner und Zuweisungsregeln verwenden während des Imports Bedingungen, die mit dem **Bedingungsgenerator**erstellt wurden. Änderungen an den Kriterien können sich auf die Leistung auswirken, da jeder Datensatz mit diesen Filtern ausgewertet wird.

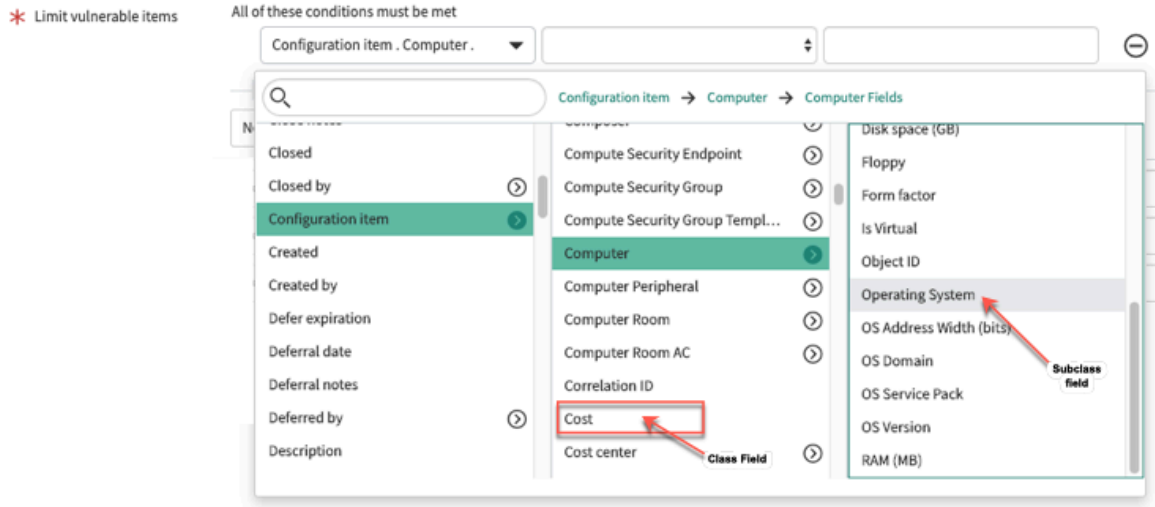
Die im Lieferumfang des Basissystems enthaltenen Regeln und Rechner sind auf Leistung optimiert. Das Bearbeiten oder Erstellen von Regeln oder Rechnern erfordert Sorgfalt und erfordert möglicherweise sowohl ServiceNow - als auch Application Vulnerability Response -Kenntnisse. Allerdings sind einige Anleitungen verfügbar.

Vermeiden Sie die Filterung auf Grundlage von Unterklassenfeldern

Einige Tabellen unterstützen Erweiterungen. Ein Beispiel hierfür ist die CMDB-CI-Tabelle [cmdb_ci]. Tabellen wie „cmdb_ci_hardware“ und „cmdb_ci_computer“ erweitern diese Tabelle. Wenn Sie basierend auf einem Feld filtern, das sich nicht in der übergeordneten Tabelle befindet, kann die Erstellung und Auswertung dieses Filters teuer sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dropdown-Menü für Bedingungsfilter



Filtern Sie beispielsweise nach **Konfigurationselement** > **Kosten** würde die Leistung nicht beeinträchtigen, da **Kosten** ein Klassenfeld und kein Unterklassenfeld von **Configuration Item**ist.

Konfigurationselement > **Computer**ist jedoch eine Unterklasse, die einen Dot-Walk zu einem anderen Feld erfordert, in diesem Fall **Betriebssystem**. Dieser Prozess kann viele Millisekunden dauern, was sich schnell summiert, wenn Millionen von angreifbaren Elementen importiert werden, und die Leistung beeinträchtigen.

Hinweis:
Die Verwendung der Bedingung [enthält] ist wie eine Platzhaltersuche und kann die Leistung beeinträchtigen. Wo immer möglich, ist die Verwendung von [is] effizienter.

Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response

Zielregeln für Anwendungskorrekturen definieren den erwarteten Zeitrahmen für die Korrektur von angreifbaren Elementen in einer Anwendung (Application Vulnerable Items, AVIs) und bieten einen Zeitrahmen für die Korrektur der Schwachstelle selbst. Wenn beispielsweise ein angreifbares Anwendungselement eine kritische Risikobewertung enthält, muss die Schwachstelle für dieses Element innerhalb von 15 Tagen behoben werden.

App-Sec-Manager können Zielregeln für Anwendungskorrekturen erstellen, indem sie Folgendes definieren:

- Das Korrekturziel.
- Das Erinnerungsziel.
- [store-future: BEGIN review]Die Empfänger der Erinnerung und der Benachrichtigung – Wer benachrichtigt werden soll, wenn die AVIs das Zieldatum für Erinnerung oder Korrektur überschritten haben und nicht korrigiert wurden.[End]

App-Sec-Manager können das Zieldatum der Korrektur im AVI-Formular und in den Listenansichten anzeigen. Für AVIs im Status **„Zurückgestellt“**, **„Gelöst“**oder **„Geschlossen“** werden keine Daten aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das **Zieldatum der Korrektur** ist in der AVI-Listenansicht als Punkte wie folgt farbcodiert:

- AVIs, deren Benachrichtigungsdatum noch nicht erreicht ist, werden grün angezeigt.
- AVIs, deren Zieldatum für die Korrektur bevorsteht, werden orange angezeigt.
- AVIs, die nach dem Korrekturzieldatum liegen, werden rot angezeigt.

[store-future: BEGIN review]Pro Anwendungskorrektur-Zielregel wird eine Zusammenfassungs-E-Mail gesendet, wenn mindestens ein AVI entweder auf das Korrekturzieldatum zusteuert oder das Korrekturzieldatum verstrichen ist.[End]

Standardregeln

Application Vulnerability Response enthält drei Standardregeln, die standardmäßig inaktiv sind:

- Regel für die Einstufung kritischer Risiken: Ein Korrekturziel mit einer Risikobewertung **„1 – Kritisch“**, ein Korrekturziel von 15 Tagen und eine Erinnerung von **7** Tagen vor dem Zieldatum.
- Regel für die Einstufung mittelhoher Risiken: Ein Korrekturziel mit einer Risikobewertung **von 2 – Hoch** oder **3 – Mittel**, ein Korrekturziel von 30 Tagen und eine Erinnerung von **7** Tagen vor dem Zieldatum.
- Regel für die Einstufung weniger kritischer Risiken: Ein Korrekturziel mit einer Risikobewertung **von 4 – Niedriges** Risiko, einem Korrekturziel von 45 Tagen und einer Erinnerung von **7** Tagen vor dem Zieldatum.

Korrekturzielregeln können deaktiviert oder gelöscht werden

Wenn eine Regel deaktiviert ist, werden die aktuellen Korrekturzieldaten für die AVIs gelöscht, auf die sie angewendet wurde. Wenn eine AVI eine aktive Regel erfüllt, wird diese Regel angewendet. Andernfalls hat die AVI keine Regel oder kein Zieldatum, und ihr Status ist **Kein Ziel**.

Wenn Regeln gelöscht werden, werden das **Zieldatum der Korrektur** und zugehörige Felder in geschlossenen AVIs beibehalten. Das **Zieldatum der Korrektur** und zugehörige Felder in nicht geschlossenen AVIs werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

Korrekturregel-Szenario

Wenn mehrere Korrekturzielregeln auf dasselbe AVI angewendet werden, wird die restriktivste Regel angewendet.

Beispiel: Wenn ein AVI die Bedingung für zwei Anwendungskorrektur-Zielregeln erfüllt:

Szenario: AVI zuletzt geöffnet am 01.03.2018 um 10:00:00.

- Anwendungskorrektur-Zielregel 1: Zuletzt geöffnet am 07.03.2018; Korrekturziel ist 15 Tage seit dem letzten Öffnen; Das berechnete Zieldatum der Korrektur ist der 16.03.2018 10:00:00.
- Anwendungskorrektur-Zielregel 2: Zuletzt geöffnet am 10.03.2018; Korrekturziel ist 10 Tage seit dem letzten Öffnen; Das berechnete Zieldatum der Korrektur ist der 11.03.2018 10:00:00.

In diesem Szenario gilt die Zielregel für die Anwendungskorrektur 2 für die AVI, da sie das restriktivere Datum hat. 10 Tage seit der ersten Identifizierung des AVI gegenüber 15 Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Anwendungskorrekturziele werden aus dem Datum **von „Zuletzt geöffnet“** plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. Sie können dieses Feld dem AVI-Formular aus dem Slushbucket „Formularlayout“ hinzufügen. Dies ist das Datum, an dem das AVI zuletzt in Ihrer Instanz geöffnet wurde.

Ab V17.1 werden Korrekturziele anhand des **Ziels ab (Datum)**berechnet. Der Standardwert ist weiterhin **das Datum von „Zuletzt geöffnet“**.

Hinweis:

Sobald die Zielregel für die Anwendungskorrektur definiert ist, werden die Zieldaten für die Korrektur anhand der geplanten Aufgabe *`Evaluate remediation targets`* oder anhand der Schaltfläche **Changes übernehmen** in der Listenansicht für Korrekturzielregeln berechnet.

Über die geplante Aufgabe „Korrekturziele auswerten“

`Evaluate remediation targets` wird einmal täglich um 4:00:00 ausgeführt.

`Evaluate remediation targets` iteriert alle aktiven Schwachstellenregeln, beginnend mit den Regeln mit dem frühesten Korrekturzieldatum. Es werden alle AVIs untersucht, die:

- befinden sich nicht im Status **Geschlossen**, **Zurückgestellt**oder **Gelöst**.
- Hat kein Korrekturzieldatum.
- Ein Korrekturzieldatum aufweisen, das nach dem Datum in der Anwendungskorrektur-Zielregel liegt.

`Evaluate remediation targets` fügt ein Korrekturzieldatum hinzu. Wenn keines vorhanden ist oder wenn diese Regel ein früheres Datum als das im Datensatz enthaltene enthält, wird das vorhandene Zieldatum aktualisiert. Abschließend werden die Felder **„Zieldatum der Korrektur“** und **„Status der Korrektur“** im AVI-Formular aktualisiert. Bei inaktiven Regeln **werden durch Korrekturziele auswerten** die Korrekturfelder im AVI gelöscht.

Korrekturzielregeln werden erneut angewendet

Wenn Sie eine Korrekturzielregel ändern, verwenden Sie die Schaltfläche **Changes übernehmen** auf der Listenseite für Korrekturzielregeln, um alle geänderten Regeln für alle aktiven offenen AVIs mit Ausnahme der Status **Geschlossen**, **Zurückgestellt** oder **Gelöst erneut** auszuführen.

Hinweis:

Wenn die geplante Aufgabe *`Evaluate remediation targets`* ausgeführt wird, können Sie keinen Prozess zum erneuten Anwenden initiieren. Wenn jedoch bereits ein Prozess zum erneuten Anwenden ausgeführt wird und die geplante Aufgabe ausgelöst wird, werden sie parallel ausgeführt.

Die Prozesse zum erneuten Anwenden in Vulnerability Response und Application Vulnerability Response sind unabhängig und können parallel ausgeführt werden.

Erstellen oder bearbeiten Sie Zielregeln für die Anwendungskorrektur

Fördern Sie die rechtzeitige Korrektur von Schwachstellen mit hohem Risiko, indem Sie eine Korrekturzielregel auf Ebene des angreifbaren Elements der Anwendung (Application Vulnerable Item, AVI) einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Hinweis:
Im Lieferumfang des Basissystems sind drei Korrekturzielregeln enthalten.

- Regel für die Einstufung kritischer Risiken
- Weniger kritische Risikoeinstufungsregel
- Regel für die Einstufung mittelhoher Risiken

Standardmäßig sind diese Regeln deaktiviert. Wenn Sie eines bearbeiten, anstatt ein neues Element zu erstellen, denken Sie daran, vor dem Speichern das Kontrollkästchen**Aktiv** zu aktivieren.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Korrekturzielregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Name der Regel.
Ziel (Tage)	Geben Sie die Anzahl der Tage an, in denen die AVIs seit dem letzten Öffnen korrigiert werden sollen.
V17.1: Ziel ab (Datum)	Datum, ab dem die Ziel-SLAs berechnet werden. Sie können nur das Datum oder die Felder für den Datums- und Uhrzeittyp angeben. Der Standardwert ist Datum der letzten Öffnung. Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1642413 .
Aktiv	Standardmäßig ist das Kontrollkästchen **Aktiv** aktiviert, was bedeutet, dass die Korrekturzielregel aktiv ist. Wenn dieses Kontrollkästchen deaktiviert ist, gilt diese Regel nicht für neue AVIs, die im System erstellt werden.
Benachrichtigen (Tage vor dem Fälligkeitsdatum)	Anzahl der Tage vor der angestrebten Korrekturzeit, bis eine Erinnerung festgelegt werden kann. Das mit diesem Wert berechnete Benachrichtigungsdatum wird verwendet, um den Korrekturstatus und die Farbcodierung anzuzeigen. Wenn das Datum vor dem Benachrichtigungsdatum liegt, lautet der Korrekturstatus „In Bearbeitung“. Wenn es nach dem Benachrichtigungsdatum und vor dem Korrekturzieldatum liegt, wird der Status als „Ziel erreicht“ angezeigt. **Hinweis:** Wenn dieses Feld auf 0 festgelegt ist, wird nur die Benachrichtigung **„Ziel verfehlt“** festgelegt.
Regel gilt für	Wählen Sie mithilfe des Bedingungsfilters die Kriterien für die Anwendung der Regel auf die AVIs aus. Um eine Beeinträchtigung der Leistung zu vermeiden, testen Sie Ihre Bedingungen im vollen Produktionsmaßstab. Durch Tests können Sie bestimmen, wie lange die Ausführung des Auftrags **„Korrekturziele auswerten“** unter Berücksichtigung der Bedingungen und der Größe von Configuration Management Database (CMDB)dauert.
Aktualisierungsverlauf	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktivitäten	Wird für die erstmalige Erstellung einer Regel nicht verwendet. Anschließend werden hier Systemarbeitsnotizen protokolliert.

4. Klicken Sie auf **Absenden**.
   Diese Regel tritt während der nächsten Ausführung der geplanten Aufgabe `Evaluate remediation targets`in Kraft. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird oder wenn Sie die Schaltfläche **Changes anwenden** in der Listenansicht für Korrekturzielregeln verwenden. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird. Weitere Informationen zur geplanten Aufgabe und **zum Anwenden von Changes** finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response.

Zeigen Sie den Nachbesserungszielstatus eines angreifbaren Anwendungselements an

Wenn ein angreifbares Element in einer Anwendung (Application Vulnerable Item, AVI) sein durch eine Korrekturzielregel definiertes Korrekturzieldatum fast erreicht (oder überschritten) hat, wird der AVI-Datensatz mit einem Status aktualisiert. Diese Informationen können Ihnen helfen, bevorstehende Korrekturaktivitäten proaktiv zu überwachen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Die **regelmäßige Aufgabe „Korrekturziele auswerten“** wird einmal pro Tag ausgeführt, um das aktuelle Datum mit dem Korrekturdatum für angreifbare Elemente zu vergleichen, das in der zugehörigen Korrekturzielregel angegeben ist. Wenn das aktuelle Datum innerhalb der Anzahl der Tage liegt, bevor die Remediation überfällig ist, wird dem Datensatz des angreifbaren Elements ein Remediationsstatus hinzugefügt.

Prozedur

Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**.
Wenn das Korrekturdatum für die AVI im Bereich der in der Korrekturzielregel festgelegten Bedingungen liegt, überprüfen Sie die Spalten Korrekturzielstatus, die in der Listenansicht der angreifbaren Elemente sichtbar sind. Wenn das Zieldatum der Korrektur für ein AVI verstrichen ist, wird im AVI-Formular eine Anmerkung angezeigt.

Hinweis:
Informationen zur Anzahl der AVIs mit **den Status „Nächstes Ziel“**, **„In Ausführung“**und**„Vergangenes Ziel**“ finden Sie unter Dashboard für Anwendungsschwachstellenmanagement [PA].

Zugehörige Informationen

Erstellen oder bearbeiten Sie Zielregeln für die Anwendungskorrektur

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das einer Anwendungskorrekturaufgabe zugeordnete Problem ohne weitere Analyse sofort geschlossen werden kann, können Sie die Funktion **Schließen** verwenden. Ab v23.0 von Vulnerability Responsewurde die Schaltfläche **Schließen** für eine Anwendungskorrekturaufgabe entfernt.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

In den Vulnerability Response -Arbeitsbereichen durchläuft eine Korrekturaufgabe dieselben Status wie eine Korrekturaufgabe in früheren Versionen von Vulnerability Response. Wenn alle angreifbaren Elemente (VITs) in einer Korrekturaufgabe geschlossen wurden, geht die Korrekturaufgabe in den Status „Inaktiv“ über.

Wichtig:
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder aus einer Korrekturaufgabe entfernen kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben Korrekturaufgaben jedoch nicht automatisch aus den Status „Geschlossen “ oder „Zurückgestellt“.

Prozedur

1. Öffnen Sie den Datensatz, für den Sie eine Überprüfung anfordern möchten.
2. Wählen Sie die Schaltfläche **Schließen** aus.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Status	Wählen Sie als Status Geschlossen aus.
Grund	Geben Sie den Grund für das Schließen des Problems ein.
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

4. Wählen Sie **Absenden**.
   Die Korrekturaufgabe wird als **Geschlossen**markiert.

Change Management für Application Vulnerability Response

Erstellen Sie Change-Anforderungen aus Korrekturaufgaben in der Anwendung Application Vulnerability Response, um Ihre Untersuchung von Anwendungsschwachstellen (AVIT), die manuelles Eingreifen erfordern, zu beschleunigen.

Erstellen Sie Change-Anforderungen mit vorab ausgefüllten Informationen für gescannte Anwendungen, die als Configuration Items (CI) klassifiziert sind, um Ihre Untersuchung von Anwendungsschwachstellen (AVITs), die manuelles Eingreifen erfordern, zu beschleunigen.

- Der Workflow für Change-Anforderungen in Application Vulnerability Response ähnelt dem in Vulnerability Responseunterstützten Workflow.
- Weitere Informationen zum Workflow für Change-Anforderungen Vulnerability Response finden Sie unter Change Management für Vulnerability Response.

Erstellen Sie eine Change-Anforderung für die Aufgabe zur Anwendungskorrektur

Als App-Sec-Manager oder Security Champion können Sie in der Anwendung Application Vulnerability Response Change-Anforderungen aus Korrekturaufgaben erstellen.

Vorbereitungen

Erforderliche Rollen:

In Manager-Arbeitsbereich des Schwachstellenmanagers: sn_vul.app_sec_manager.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aus dem Arbeitsbereich des ITRem-Besitzers: sn_vul.app_sec_Champion oder sn_vul.app_developer und die Rolle itil.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die unten aufgeführten Schritte aus, um eine Change-Anforderung in der klassischen Umgebung zu erstellen.

Sie können Change-Anforderungen direkt von einer Korrekturaufgabe aus erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

- Standard Ein zuvor autorisierter Change, der als risikoarm und relativ gängig gilt und anhand eines festgelegten Verfahrens oder einer festgelegten Arbeitsanweisung implementiert wird.
- Normal Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsebenen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall Ein Change zur Lösung eines schwerwiegenden Incident.

Hinweis:
Change-Anforderungen werden für Application Vulnerability Response nur unterstützt, wenn die erkannte Anwendung einem Configuration Item (CI) zugeordnet ist. Dies geschieht nur, wenn Sie „Produktmodell“ in der Systemeigenschaft „Produktmodell verwenden“ [sn_vul.use_product_model] auf „Falsch“ setzen.

Prozedur

1. Um eine vollständige Change-Anforderung aus einem vorhandenen Korrekturaufgaben-Datensatz zu erstellen, navigieren Sie zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.
   Die Liste der Korrekturaufgaben, die Ihrer Zuweisungsgruppe zugewiesen sind, wird angezeigt.
2. **Wahlweise:** Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturübersicht** um das Dashboard „Remediationsübersicht“ anzuzeigen und eine VUL zu suchen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen ist.
3. Alternativ können Sie in der Spalte Nummer auf eine Korrekturaufgabe klicken, um den Datensatz zu öffnen und die Details anzuzeigen.
   Der Datensatz wird angezeigt.
4. Klicken Sie bei angezeigtem APP-VUL-Datensatz, für den Sie die Change-Anforderung erstellen möchten, oben rechts im Datensatz **auf Change erstellen**.
   Das Formular „Change-Anforderung erstellen“ wird angezeigt.
5. Füllen Sie die Felder aus.

   a. Wählen Sie in der Auswahlliste des Felds Gilt für eines aus, um fortzufahren.

Option	Beschreibung
Alle aktiven angreifbaren Anwendungselemente in dieser Gruppe	Wenn diese Option ausgewählt ist, werden alle aktiven angreifbaren Anwendungselemente aus dieser Korrekturaufgabe mit einem anderen Status als „Geschlossen“ automatisch der Change-Anforderung hinzugefügt, nachdem Sie **auf Change erstellen**klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Alle angreifbaren Anwendungselemente in dieser Gruppe, die eine Reihe von Bedingungen erfüllen	Wenn diese Option ausgewählt ist, wird der Bedingungsgenerator wie in der zweiten Abbildung unten angezeigt. Geben Sie Filterkriterien ein, um die angreifbaren Elemente zu identifizieren, die Sie für die neue Change-Anforderung verwenden möchten. Ein Beispiel für einen Filter könnte nur angreifbare Elemente enthalten, die bestimmten Suchkriterien entsprechen: **Status ist „Offen“** und **Risikopunktzahl größer als 75**. Nachdem Sie Ihre Bedingungen eingegeben haben, wird eine Nachricht mit der Anzahl der AVITs angezeigt, die Ihren Kriterien entsprechen (10). Es wird ein Link (**Vorschau passende Elemente anzeigen**) zur Vorschau der übereinstimmenden Elemente angezeigt. Wenn keine Elemente Ihren Filterbedingungen entsprechen, wird unter dem Bedingungsgenerator eine Meldung angezeigt, in der Sie aufgefordert werden, den Filter anzupassen. Nachdem Sie auf **Change erstellen**geklickt haben, werden alle angreifbaren Anwendungselemente, die diesem Bedingungsfilter entsprechen, in eine neue Korrekturaufgabe verschoben. Diese Change-Anforderung ist mit der neuen Korrekturaufgabe verknüpft.

Erstellen Sie eine Change-Anforderung für angreifbare Anwendungselemente in einer Aufgabe, die eine Reihe von Bedingungen erfüllen

b. **Wahlweise:** Wenn sie im Formular angezeigt wird, klicken Sie auf den Link **Vorschau passende Elemente anzeigen,** um eine Liste der AVITs anzuzeigen, die Ihren Filterkriterien entsprechen. Die Vorschau der Korrekturaufgabenliste wird angezeigt. Sie können Elemente in dieser Vorschauliste auswählen und UI-Aktionen dafür ausführen. Diese Aktionen werden jedoch auch für die APP-VUL ausgeführt. Wenn Sie beispielsweise ein VI aus der Vorschauliste löschen, wird dieses AVIT auch aus der APP-VUL gelöscht.

c. Schließen Sie nach Abschluss der Vorschau das Browserfenster, um zum Formular „Change-Anforderung“ zurückzukehren.

d. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Das Kontrollkästchen CIs zu CR hinzufügen ist aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle Configuration Items (CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, zu dieser Change-Anforderung hinzugefügt. Die APP-VUL wechselt automatisch in den Status Warten auf Implementierung.
Das Kontrollkästchen „CIs zu CR hinzufügen“ ist deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass die CIs aus den aktiven angreifbaren Anwendungselementen dieser Korrekturaufgabe dem neuen Change Request hinzugefügt werden. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit der APP-VUL synchronisiert, und die APP-VUL verbleibt in ihrem aktuellen Status.

e. Wählen Sie aus der Auswahlliste für das Feld Change-Typ einen aus, um fortzufahren.

Änderungstyp	Beschreibung
Notfall	Ein Change zur Lösung eines schwerwiegenden Incident.
Normal	Ein Change-Typ, mit dem Changes an einem Service implementiert werden, bei denen es sich nicht um Standard- oder Notfall-Changes handelt.
Standard	Eine vorab autorisierte Change-Anforderung mit geringem Risiko, die häufig implementiert wird. Genehmigte Standard-Change-Anforderungen können in einem Vorlagenkatalog vordefiniert werden, um den Zugriff auf und die Anfrage eines Standard-Changes effizienter zu gestalten. Wenn diese Option ausgewählt ist, werden zwei Felder angezeigt. Wählen Sie in jeder Auswahlliste eines aus, um diese Felder auszufüllen: ▪ Change-Kategorie: Wählen Sie eine Kategorie für den Change aus Ihrem vorhandenen Katalog aus, z. B. Hardware, Server-Standard-Changes, Software. In diesem Beispiel ist Patchen von Standard-Changes ausgewählt. ▪ Change-Vorlage: Wählen Sie eine verfügbare Vorlage für Change-Anforderungen mit vordefinierten unterstützenden Aufgaben aus Ihrem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Änderungstyp	Beschreibung
	Katalog aus. In diesem Beispiel wird die Vorlage „Microsoft Monatlicher Patchzyklus“ ausgewählt. Weitere Informationen zu Kategorien, Vorlagen und Change-Typen von ITSM-Change-Anforderungen finden Sie unter Change-Typen .

Die Funktion liest automatisch die Typen von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change Management eingerichtet haben. Wenn Sie beispielsweise den Namen für Ihre Standard-Change-Anforderungen in ITSM von Standard in Vorgenehmigtändern, wird Ihr neuer Name automatisch in der Auswahlliste Change type (Change-Typ) unter Change Request erstellen (Change-Anforderung erstellen) angezeigt (siehe folgende Abbildung).

Die Felder im Abschnitt „Vorschau auf Change-Anforderung“ des Formulars sind bereits mit Informationen aus der APP-VUL ausgefüllt. Bei Bedarf können diese Feldwerte bearbeitet werden. Überprüfen Sie beispielsweise die Werte in den Feldern in der folgenden Abbildung:

Geplantes Enddatum

Dieses Datum (10.10.2019) ist derselbe Wert, der im Feld Korrekturzieldatum der APP-VUL angezeigt wird. Dieser Wert wird vom frühesten Nachbesserungszieldatum aus den angreifbaren Anwendungselementen abgeleitet, die zur APP-VUL gehören. Wenn Sie eine Change-Anforderung für ein kritisches Problem erstellen, das ein früheres Korrekturdatum erfordert, können Sie diesen Wert und den Wert im Feld Priorität bearbeiten.

Begründung

Dieses Feld zeigt die Anzahl der CIs an, die dem CHG hinzugefügt wurden. Wenn Sie zusätzliche Informationen hinzufügen möchten, können Sie diesen Text bearbeiten. Beispielsweise können Sie in diesem Feld eine Notiz zu dem Filter hinzufügen, den Sie zum Erstellen der neuen APP-VUL verwendet haben, z. B. Risikopunktzahl höher als 75. Dieser Text kann Ihnen helfen, Ihre neue Change-Anforderung und Korrekturaufgabe zu finden.

Implementierungsplan

In diesem Feld wird die bevorzugte Lösung für die Schwachstelle angezeigt.

Zuweisungsgruppe und Zugewiesen an

Bearbeiten Sie diese Felder, um die Zuweisungsgruppe zu ändern, oder weisen Sie diese Change-Anforderung einem Anwender in einer Ihrer Zuweisungsgruppen neu zu.

6. Zeigen Sie eine Vorschau an, und bearbeiten Sie die Felder nach Bedarf.
7. Um Ihre Änderungen zu speichern und auf dieser Seite zu bleiben, klicken Sie im grauen Banner oben im Formular mit der rechten Maustaste, und wählen Sie **Einfügen und bleiben aus**.
8. Nachdem Sie Ihre Änderungen abgeschlossen haben, wählen Sie eine aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Überwachen Sie die Change-Anforderung und die Change-Aufgaben, um sicherzustellen, dass sie abgeschlossen und die Change-Anforderung implementiert wird. Nachdem dieses CHG implementiert und in den Status Überprüfen versetzt wurde und die Statussynchronisierung aktiviert ist, wird die APP-VUL automatisch in den Status Gelöstverschoben.

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Wenn Sie Appsec-Manager oder Security Champion sind, sollten Sie vermeiden, dass bei der Lösung Ihrer Korrekturaufgaben doppelte Change-Anforderungen (CHG) erstellen, indem Sie einer bereits in Ihrer Instanz verfügbaren Change-Anforderung eine Korrekturaufgabe (APP-VUL) zuordnen.

Vorbereitungen

Erforderliche Rollen:

In Manager-Arbeitsbereich des Schwachstellenmanagers: sn_vul.app_sec_manager.

Aus dem Arbeitsbereich des ITRem-Besitzers: sn_vul.app_sec_Champion oder sn_vul.app_developer und die Rolle itil.

Warum und wann dieser Vorgang ausgeführt wird

Als Korrekturbesitzer können Sie Korrekturaufgaben, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, vorhandenen Change-Anforderungen direkt aus den Korrekturaufgaben-Datensätzen zuordnen. Die folgende Abbildung zeigt den Basis-Flow für die Zuordnung einer Change-Anforderung zu einer vorhandenen APP-VUL (VG).

Hinweis:
Sie können einer APP-VUL in jedem Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „Geschlossen“ und „Zurückgestellt“) eine vorhandene Change-Anforderung zuordnen. Wenn Sie einer vorhandenen VUL einen Change Request zuordnen, werden dem Change Request nur die aktiven AEs hinzugefügt.

Bevor Sie beginnen, sollten Sie, um die Erstellung doppelter Change-Anforderungen zu vermeiden, alle vorhandenen Change-Anforderungen anzeigen, die bereits einer APP-VUL zugeordnet sind. Um die Anzahl der Change-Anforderungen, die sich auf eine bestimmte APP-VUL beziehen, einfach nachzuverfolgen, konsultieren Sie die Spalte CR-Anzahl in der Liste der Korrekturaufgaben. Falls nicht angezeigt, klicken Sie auf das Einstellungssymbol () oben rechts. Verschieben Sie die Spalte CR-Anzahl von Verfügbar in Ausgewählt, und klicken Sie auf **OK**.

Um die neue Spalte automatisch auszufüllen, führen Sie für Kunden mit vorhandenen Daten in dieser Tabelle die geplante Aufgabe aus: Neue CR-Anzahlspalte ausfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um einer vorhandenen Change-Anforderung eine Korrekturaufgabe zuzuordnen, navigieren Sie zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben**.
2. Suchen Sie die Korrekturaufgabe, mit der Sie arbeiten.
3. **Wahlweise:** Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturübersicht** um das Dashboard „Remediationsübersicht“ anzuzeigen und eine APP-VUL zu suchen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen ist.
4. Klicken Sie in der Spalte Nummer auf einen APP-VUL-Datensatz, um ihn zu öffnen.
   Der APP-VUL-Datensatz wird angezeigt.
5. Scrollen Sie bei angezeigtem geöffneten Datensatz zur zugehörigen Liste Change-Anforderungen, und wählen Sie sie aus.
   Alle Change-Anforderungen, die der APP-VUL zugeordnet sind, werden zusammen mit der Schaltfläche **Hinzufügen** angezeigt. In der folgenden Abbildung sind dieser APP-VUL bereits Change-Anforderungen zugeordnet.
6. Um die APP-VUL einem vorhandenen CHG zuzuordnen, klicken Sie auf **Hinzufügen**.
   Das Formular „Vorhandene Change-Anforderung zu Korrekturaufgabe hinzufügen“ wird angezeigt.
7. Klicken Sie im Formular auf das Suchsymbol.
   In einem neuen Fenster wird eine Listenansicht der vorhandenen Change-Anforderungen angezeigt (siehe folgende Abbildung).
8. Wählen Sie ein Element aus der angezeigten Liste aus, oder klicken Sie alternativ auf den Filter (), und geben Sie Bedingungen ein, um Ihre Suchergebnisse einzuschränken.
9. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen aus, um fortzufahren.

Hinweis:
Diese Checkbox wird nur für vorhandene Change-Anforderungen im Status Neu angezeigt.

Option	Beschreibung
Das Kontrollkästchen CIs zu CR hinzufügen ist aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle Configuration Items (CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, zu dieser Change-Anforderung hinzugefügt. Wenn diese Option ausgewählt ist, wird der Status der Change-Anforderung mit der APP-VUL synchronisiert. Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.
Das Kontrollkästchen „CIs zu CR hinzufügen“ ist deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass die CIs aus den aktiven angreifbaren Elementen aus dieser Korrekturaufgabe dem neuen Change Request hinzugefügt werden. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit der APP-VUL synchronisiert, und die APP-VUL verbleibt in ihrem aktuellen Status.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie im Feld Search for Change Request (Nach Change-Anforderung suchen) auf **Absenden**. Die APP-VUL wird angezeigt. Oben im Datensatz wird eine blaue Bestätigungsmeldung angezeigt, die anzeigt, dass die von Ihnen ausgewählte Change-Anforderung erfolgreich der APP-VUL zugeordnet wurde.

Hinweis:
Bei einer APP-VUL im Status Offen mit nicht zugewiesenen Feldern Zuweisungsgruppe und Zugewiesen an (leer) wird der aktuell angemeldete Benutzer automatisch der APP-VUL zugewiesen, nachdem Sie auf **Hinzufügen**geklickt haben. Außerdem muss das Kontrollkästchen CIs zu CR hinzufügen aktiviert sein. Oben in APP-VUL wird eine blaue Bestätigungsmeldung angezeigt, die angibt, dass der aktuelle Benutzer zugewiesen ist.

Nächste Maßnahme
Überprüfen Sie den APP-VUL-Datensatz. Klicken Sie in der Spalte „Change-Anforderung“ in der zugehörigen Liste „Change-Anforderungen“ auf den Link für das neue CHG, um den CR-Datensatz anzuzeigen. Im geöffneten CHG-Datensatz können Sie den Status des Change Request überwachen. Die betroffenen Configuration Items (CI) und die Korrekturaufgaben werden in den zugehörigen Listen Betroffene CIs und Korrekturaufgaben angezeigt.

Penetrationstests

Penetrationstests in Application Vulnerability Response ermöglichen Anwendungsbesitzern, den Sicherheitsstatus ihrer Anwendung zu bewerten. Es handelt sich um das manuelle Testen einer Anwendung durch das Team für ethisches Hacken.

Erforderliche Rollen

Penetrationstests erfordern die folgenden Rollen:

App-Sec-Manager: Enthält Sicherheitsmanager und Anwendungsbesitzer, die die Bewertungsanforderungen für Penetrationstests verwalten. Sie enthält die folgenden granularen Rollen:

- sn_vul.app_manage_pen_test_request
- sn_vul.app_read_all
- cmdb_read

Ethischer Hacker: Enthält Mitglieder des Teams für ethisches Hacken, die Penetrationstests für Anwendungen durchführen. Sie enthält die folgenden granularen Rollen:

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- ITIL
- sn_vul.app_read_all
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

Weitere Informationen zu diesen Rollen finden Sie unter Application Vulnerability Response Benutzergruppen und -rollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab v19.0 von Vulnerability Responsesind, wenn Sie Veracode Vulnerability Integrationverwenden, die Penetrationsbewertungstests in Veracode Vulnerability Integration manuelle Ergebnisse von Veracode. Sie sind nicht mit Bewertungsanforderungen für Penetrationstests verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstestbewertungen von Veracodefinden Sie unter Veracode Vulnerability Integration.

Lebenszyklus von Penetrationstests

Als Besitzer der Anwendung können Sie das Team für ethisches Hacken um einen Penetrationstest Ihrer Anwendung bitten. Das Team für ethisches Hacken bearbeitet diese Anforderung und erstellt Ergebnisse für Penetrationstests. Bei diesen Ergebnissen handelt es sich um manuell erstellte angreifbare Anwendungselemente (Application Vulnerable Items, AVIs).

Der Penetrationstest-Workflow deckt den Lebenszyklus für Penetrationstests ab, von der Erstellung der Testanforderung bis zur Lösung der Ergebnisse des Teams für ethisches Hacken.

Penetrationstestbewertung wird angefordert

Ab v19.0 können Sie unter neue Anforderungen erstellen oder vorhandene Anforderungen kopieren **Alle** > **Anforderungen für Penetrationstestbewertung** > **Alle**.

Vor v19.0 können Sie als Anwendungsbesitzer mithilfe des ITSM-Servicekatalogs eine Penetrationstestbewertung für Ihre Anwendung anfordern.

Die Bewertungsanforderung für den Penetrationstest wird überprüft

Das Team für ethisches Hacken überprüft und bewertet die Anwendung und den Umfang der Penetrationstest-Bewertungsanforderung und fügt sie dem vorhandenen Backlog hinzu.

Vorbereiten einer -Umgebung

Das Team für ethisches Hacken sendet dann eine Anforderung an den Anwendungsbesitzer, eine Umgebung bereitzustellen, in der er mit dem Testen beginnen kann. Sobald die Umgebung bereit ist, informiert der Besitzer der Anwendung das Team für ethisches Hacken.

Weitere Informationen zum Konfigurieren von Testanforderungen finden Sie unter Konfigurieren Sie Penetrationstests.

Testen und Melden der Penetrationstestergebnisse

Das Team für ethisches Hacken testet die Anwendung und meldet die Ergebnisse dem Besitzer der Anwendung. Das Team für ethisches Hacken definiert auch die Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) für die Penetrationstestergebnisse anhand des Korrekturzieldatums. Diese Ergebnisse sind die manuell erstellten AVIs. Der Besitzer der Anwendung überprüft wiederum die vom Team für ethisches Hacken erstellten AVIs. Sie planen die Korrekturen und weisen sie dem Anwendungsteam zu.

Hinweis:
Korrekturzielregeln gelten nicht für die Penetrationstestergebnisse.

Das Team für ethisches Hacken kann eine Bibliothek mit Einträgen zu Anwendungsschwachstellen erstellen und diese beim Melden der AVIs wiederverwenden. Sie können auch den Status der Penetrationstestergebnisse verfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

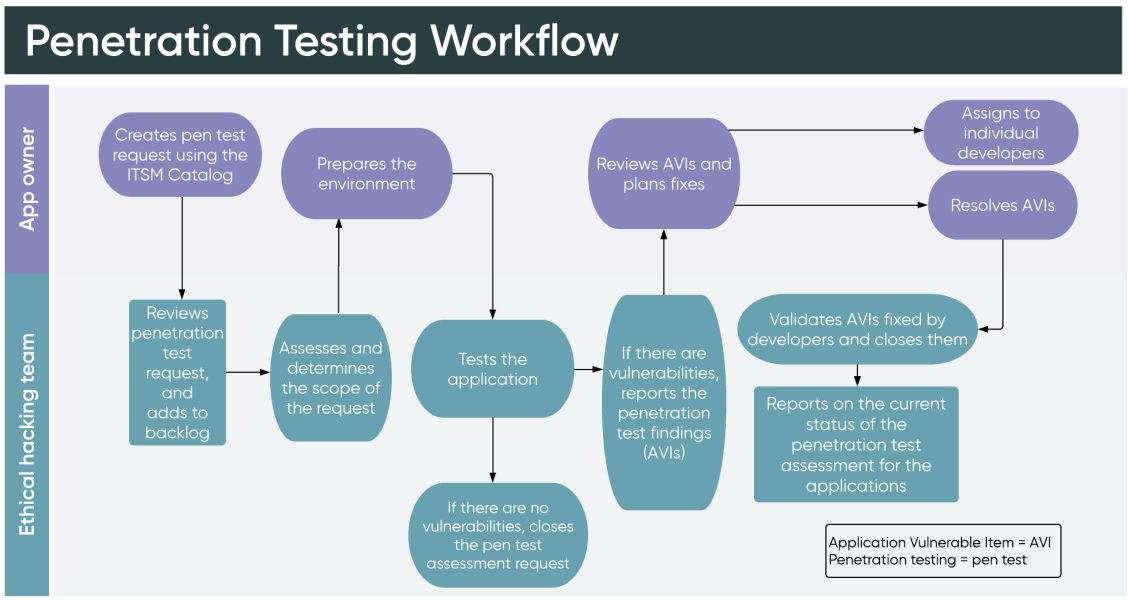
Penetrationstestergebnisse korrigieren und validieren

Nachdem die Penetrationstestergebnisse vom Anwendungsteam korrigiert und gelöst wurden, werden die Korrekturen manuell validiert und vom Team für ethisches Hacken geschlossen.

Application Vulnerability Management-Berichte

Verwenden Sie die im PA-Dashboard Application Vulnerability Management verfügbaren Berichte, um die Ergebnisse von Penetrationstests nachzuverfolgen.

Lebenszyklus von Penetrationstests



Bewertungsanforderung für Penetrationstest aus vorhandenen Anforderungen erstellen (v19.0)

Ab v19.0 erstellen Sie Bewertungsanforderungen für Penetrationstests direkt aus der Liste der vorhandenen Anforderungen. Sie können auch vorhandene Anforderungen im Status „Geschlossen“ in diese Liste kopieren, um Anforderungen zu erstellen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird

Ab v19.0 von Vulnerability Responsesind, wenn Sie Veracode Vulnerability Integrationverwenden, die Penetrationsbewertungstests in Veracode Vulnerability Integration manuelle Ergebnisse von Veracode. Sie sind nicht mit Bewertungsanforderungen für Penetrationstests verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstestbewertungen von Veracodefinden Sie unter Veracode Vulnerability Integration.

Prozedur

1. Navigieren zu **Alle** > **Anforderungen für Penetrationstestbewertung** > **Alle**.
2. **Wahlweise:** Alternativ können Sie eine Anforderung erstellen, indem Sie geschlossene Anforderungen replizieren.
   Alle Werte aus der ursprünglichen Anforderung werden im neuen Formular beibehalten. Aktive angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIs) werden automatisch in die neue

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderung kopiert. Wählen Sie **Kopieren und Anforderung erstellen** aus Datensätzen im Status „Geschlossen“ aus.

3. Wählen Sie Neu und füllen Sie die Felder aus.

Formular „Bewertungsanforderung für Penetrationstests“.

Feld	Beschreibung
Nummer	Eindeutiger Bezeichner, der für die Penetrationstest-Bewertungsanforderung generiert wurde.
Status	Wählen Sie einen Wert basierend auf dem Status der Anforderung aus.
Angefordert von	Person, die die Bewertung der Anwendung anfordert.
Zuweisungsgruppe	Gruppe, die für die Bearbeitung der Penetrationstestergebnisse ausgewählt wurde. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. Informationen zum Konfigurieren von Gruppen finden Sie unter Konfigurieren Sie Penetrationstests.
Anwendung	Wählen Sie mithilfe der Suchoption eine Anwendung aus.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an den Ergebnissen des Penetrationstests arbeitet. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Anwendungstyp	Wählen Sie eine Option aus: ○ Webservice (vor v16.1 als API bezeichnet) ○ Web-Anwendung ○ Thick Client ○ Mobil (Wenn Sie **Mobil**auswählen, wird die Registerkarte Mobil am unteren Rand des Formulars mit zusätzlichen Feldern angezeigt.)
Sprint	Zeigt die Sprints mit verfügbarer Bandbreite für die Bewertungsanforderung basierend auf dem ausgewählten Bewertungstypfeld an. Weitere Informationen zum Ändern der Sprint-Kapazität und des Testumfangs finden Sie unter Sprints für Penetrationstests konfigurieren und Konfigurieren Sie Bewertungstypen für Penetrationstests.
v19.0: Anwendungsgröße	Wählen Sie die Größe der Anwendung aus, die Sie testen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Klein ○ Mittel ○ Groß ○ Standard (wählen Sie diese Option, wenn Sie sich bezüglich der Größe nicht sicher sind) Weitere Informationen finden Sie unter Konfigurieren Sie Penetrationstests zum Ändern der Sprint-Kapazität und zum Testen des Umfangs mit Anwendungsgröße und Sprint-Kapazität.
Erstellt	Datum und Uhrzeit der Erstellung der Anforderung.
Bewertungstyp	Wählen Sie den Typ der Bewertung aus: ○ Vollständiger Penetrationstest ○ Fokussierter Test ○ Erneut testen Weitere Informationen zu Testkombinationen und Testumfang finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Anforderung.
Demo-Datum	Datum, an dem diese Anwendung vorgeführt werden kann.
Produktbereitstellung geplant am	Geplantes Datum für die Bereitstellung dieser Anwendung in der Produktion.
Anwendungsversion/-release für die Bereitstellung geplant	Version der Anwendung, die für die Produktionsbereitstellung geplant ist.
v19.0: Anwendung im Besitz eines Drittanbieters oder einer Joint-Venture-Registerkarte Wenn Sie für dieses Feld „Ja“ auswählen, wird die Registerkarte Lieferanten-/Joint-Venture-Informationen angezeigt. Füllen Sie die zusätzlichen Felder aus.	
Gibt es eine Klausel, die es uns ermöglicht, Pen-Tests durchzuführen?	Der Begriff „Klausel“ kann sich auf Standards für Tests beziehen, die Vereinbarungen enthalten, die zwischen zwei oder mehr Parteien bestehen, die Sie hinzufügen möchten. Wenn Sie **Ja**auswählen, fügen Sie die Klausel hinzu.
Die Klausel, die die Erlaubnis zur Durchführung von Pen-Tests enthält	
Vollständiger offizieller Name und Adresse des Lieferanten	
Angriffserkennungssystem	
Technischer Kontakt des Lieferanten	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wurden die protokollierten Informationen auf schädliche Aktivitäten geprüft?	
Wird die Anwendung von einem anderen Drittanbieter gehostet?	
Kontakt des Lieferanten, der den Pen-Test abzeichnet	
Registerkarte „Anwendungsdetails“.	
Zweck der Anwendung	Beschreibung der Funktionalität der Anwendung.
Details des Technologiestapels	Vollständiger Technologiestapel vom Front-End bis zum Back-End, Datenbanken und andere Schlüsseltechnologien.
Ist Drittparteianwendung?	Bestätigt, ob diese Anwendung im Besitz eines Drittanbieters ist.
Listet die Arten sensibler Daten auf, auf die über die Anwendung zugegriffen werden kann.	Arten vertraulicher Daten, auf die über die Anwendung zugegriffen werden kann. Zum Beispiel PII-Daten, PHI-Daten und Finanzdaten wie Kreditkartennummern.
Authentifizierungstyp	Gibt an, ob diese Anwendung die LDAP-Authentifizierung, ihre eigene native Authentifizierung oder andere Formen der Authentifizierung verwendet.
Fällt die Anwendung unter ein Compliance-Programm?	Gibt an, ob sich diese Anwendung auf Compliance-Programme wie PCI auswirkt.
Kontakte im Anwendungsteam	Mitglieder des Anwendungsteams, die vom Team für ethisches Hacken bei Fragen kontaktiert werden sollen.
Liste der Compliance-Programme	
Zugehörige Schnittstellen oder Anwendungen von Drittparteien	
IP-Adresse	
Ungefähre Anzahl der Anwender in der Produktion?	
Automatisiertes Skript vorhanden?	
Ist die Produktionsversion dieser App extern ausgerichtet?	
v 19.0: Geschäftsauswirkung	
Finanzieller Schaden	Wählen Sie eine aus der Liste aus.
Nichteinhaltung	Wählen Sie eine aus der Liste aus.
Reputationsschaden	Wählen Sie eine aus der Liste aus.
Datenschutzverletzung	Wählen Sie eine aus der Liste aus.
Registerkarte „Testdetails“.	
Zu testende URLs	URLs, die in Penetrationstests einbezogen werden müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Auszuschließende URLs	URLs, die von Penetrationstests ausgeschlossen werden müssen.
Wurde diese Anwendung zuvor getestet?	Gibt an, ob diese Anwendung bereits einem Penetrationstest unterzogen wurde.
Grund für erneuten Test	Grund für die Anforderung eines erneuten Penetrationstests, wenn die Anwendung zuvor getestet wurde.
Wann wurde die Anwendung getestet?	Zeitrahmen, in dem die Anwendung auf Penetration getestet wurde.
Details des Test-Accounts	Details des Test-Accounts, die vom Team für ethisches Hacken für Penetrationstests verwendet werden können.
Anwendungsrollen	Rollen, die von der Anwendung für ihre Benutzer unterstützt werden.
Meistverwendete Rollen	Die am häufigsten verwendeten Rollen in der Anwendung.
Registerkarte „Zusätzliche Kommentare“.	
Arbeitsnotizen	

4. Wählen Sie **Speichern,** um Ihre Änderungen zu speichern, oder **Absenden,** um die Anforderung zu initiieren.

Bewertungsanforderung für Penetrationstest erstellen (vor v19.0)

Initiieren Sie eine Penetrationstest-Bewertungsanforderung für Ihre Webanwendungen oder APIs. Diese Anforderungen werden an das Team für ethisches Hacken übermittelt, das dann diese Anwendungen testet und die Ergebnisse der Penetrationstests manuell meldet.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird

Der Anwendungsbesitzer stellt eine Bewertungsanforderung für einen Penetrationstest, um seine Anwendung oder APIs manuell zu scannen. Das Team für ethisches Hacken testet die Anwendung und erstellt manuell die Ergebnisse der Penetrationstests. Bei diesen Ergebnissen handelt es sich um manuell erstellte angreifbare Elemente in Anwendungen (Application Vulnerable Items, AVIs).

Die Standardzuweisungsgruppe für das Penetrationstestergebnis ist die Gruppe, die im Feld „Anwendungsteam“ der zugehörigen Penetrationstestbewertungsanforderung konfiguriert ist. Der Zuweisungstyp des Penetrationstestergebnisses ist Manuell. Die Zuweisungsregeln können die Zuweisung dieser Penetrationstestergebnisse nicht überschreiben.

Ab v19.0 können Sie Bewertungsanforderungen für Penetrationstests direkt in der Tabelle „Bewertungsanforderungen für Penetrationstests“ [sn_vul_pen_test_assessment_request_list] erstellen. Weitere Informationen finden Sie unter Bewertungsanforderung für Penetrationstest aus vorhandenen Anforderungen erstellen (v19.0).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Vor v19.0 navigieren Sie mit zu **Alle** > **Selfservice** > **Servicekatalog** > **Services** > **Anforderung für Penetrationstestbewertung**.
2. **Wahlweise:** Alternativ können Sie eine Anforderung erstellen, indem Sie geschlossene Anforderungen replizieren.
   Alle Werte aus der ursprünglichen Anforderung werden beibehalten. Aktive angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIs) werden automatisch in die neue Anforderung kopiert.
3. Füllen Sie die Felder des Formulars aus.

Formular „Bewertungsanforderung für Penetrationstests“.

Feld	Beschreibung
Nummer	Eindeutiger Bezeichner, der für die Penetrationstest-Bewertungsanforderung generiert wurde.
Angefordert von	Person, die die Bewertung der Anwendung anfordert.
Übergeordnete Bewertungsanforderung	Ursprüngliche Bewertungsanforderung für Penetrationstests, die zum Erstellen der untergeordneten Anforderung verwendet wurde. Sie wird mithilfe einer geschlossenen Bewertungsanforderung erstellt. Nur im Formular zum Anfordern der untergeordneten Bewertung sichtbar.
Anwendung	Wählen Sie mithilfe der Suchoption eine Anwendung aus.
Anwendungstyp	Wählen Sie eine Option aus: ○ Webservice (vor v16.1 als API bezeichnet) ○ Web-Anwendung ○ Thick Client ○ Mobil (Wenn Sie Mobil auswählen, wird die Registerkarte Mobil mit zusätzlichen Feldern unten im Formular angezeigt.)
v19.0: Anwendungsgröße	Wählen Sie die Größe der Anwendung aus, die Sie testen möchten. ○ Klein ○ Mittel ○ Groß ○ Standard (wählen Sie diese Option, wenn Sie sich bezüglich der Größe nicht sicher sind)
Bewertungstyp	Wählen Sie den Typ der Bewertung aus: ○ Vollständiger Penetrationstest ○ Fokussierter Test ○ Erneut testen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Details finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests.
Zweck der Anwendung	Beschreibung der Funktionalität der Anwendung.
Details des Technologiestapels	Vollständiger Technologiestapel vom Front-End bis zum Back-End, Datenbanken und andere Schlüsseltechnologien.
Ist Drittparteianwendung?	Bestätigt, ob diese Anwendung im Besitz eines Drittanbieters ist.
Listet die Arten sensibler Daten auf, auf die über die Anwendung zugegriffen werden kann.	Arten vertraulicher Daten, auf die über die Anwendung zugegriffen werden kann. Zum Beispiel PII-Daten, PHI-Daten und Finanzdaten wie Kreditkartennummern.
Authentifizierungstyp	Gibt an, ob diese Anwendung die LDAP-Authentifizierung, ihre eigene native Authentifizierung oder andere Formen der Authentifizierung verwendet.
Fällt die Anwendung unter ein Compliance-Programm?	Gibt an, ob sich diese Anwendung auf Compliance-Programme wie PCI auswirkt.
Kontakte im Anwendungsteam	Mitglieder des Anwendungsteams, die vom Team für ethisches Hacken bei Fragen kontaktiert werden sollen.
Demo-Datum	Datum, an dem diese Anwendung vorgeführt werden kann.
Produktbereitstellung geplant am	Geplantes Datum für die Bereitstellung dieser Anwendung in der Produktion.
Anwendungsversion/-release für die Bereitstellung geplant	Version der Anwendung, die für die Produktionsbereitstellung geplant ist.
v19.0: Anwendung im Besitz eines Drittanbieters oder Joint-Venture-Unternehmens	Wenn Sie „Ja“ für dieses Feld auswählen, wird die Registerkarte Lieferanten-/Joint-Venture-Informationen mit zusätzlichen Feldern angezeigt. Der Begriff „Klausel“ kann sich auf Standards für Tests beziehen, die Vereinbarungen enthalten, die zwischen zwei oder mehr Parteien bestehen.
Status	Wählen Sie einen Wert basierend auf dem Status der Anforderung aus.
Zuweisungsgruppe	Gruppe, die für die Bearbeitung der Penetrationstestergebnisse ausgewählt wurde. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an den Ergebnissen des Penetrationstests arbeitet. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sprint	Zeigt die Sprints mit verfügbarer Bandbreite für die Bewertungsanforderung basierend auf dem ausgewählten Bewertungstypfeld an.
Erstellt	Datum und Uhrzeit der Erstellung der Anforderung.
Teststartdatum	Datum und Uhrzeit des Beginns der Prüfung
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Anforderung.
Testdetails	
Zu testende URLs	URLs, die in Penetrationstests einbezogen werden müssen.
Auszuschließende URLs	URLs, die von Penetrationstests ausgeschlossen werden müssen.
Wurde diese Anwendung zuvor getestet?	Gibt an, ob diese Anwendung bereits einem Penetrationstest unterzogen wurde.
Grund für erneuten Test	Grund für die Anforderung eines erneuten Penetrationstests, wenn die Anwendung zuvor getestet wurde.
Wann wurde die Anwendung getestet?	Zeitrahmen, in dem die Anwendung auf Penetration getestet wurde.
Details des Test-Accounts	Details des Test-Accounts, die vom Team für ethisches Hacken für Penetrationstests verwendet werden können.
Anwendungsrollen	Rollen, die von der Anwendung für ihre Benutzer unterstützt werden.
Meistverwendete Rollen	Die am häufigsten verwendeten Rollen in der Anwendung.

4. Wählen Sie **Absenden**.
   Eine E-Mail-Benachrichtigung wird an das Team für ethisches Hacken gesendet, dass die Anforderung für die entsprechende Anwendung erstellt wurde.

Replizieren Sie eine Penetrationstest-Anforderung im Status „Geschlossen“.

Erstellen Sie eine Bewertungsanforderung für einen Penetrationstest, indem Sie eine Anforderung im Status „Geschlossen“ replizieren. Aktive angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIs) werden in die neue Anforderung kopiert.

Vorbereitungen

Erforderliche Rolle: Anwendungsteam

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Anforderungen für Penetrationstestbewertung** > **Alle**.
2. Wählen Sie eine Anforderung im Status Geschlossen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Kopieren und Anforderung erstellen aus**.
   Eine neue Anforderung wird erstellt, und die aktiven AVIs werden mit aktualisierten Daten in diese Anforderung kopiert. Um den ursprünglichen Status der AVIs aus der übergeordneten Anforderung anzuzeigen, navigieren Sie zur Registerkarte **Snapshot der Penetrationstest-Ergebnisse**.

Penetrationstestergebnisse basierend auf Bewertungsanforderungen erstellen (vor v19.0)

Erstellen Sie Penetrationstestergebnisse basierend auf der Penetrationstest-Bewertungsanforderung. Diese Ergebnisse sind manuell erstellte Anwendungsschwachstellenelemente (Application Vulnerability Items, AVIs).

Vorbereitungen

Erforderliche Rolle: Ethical Hacker

Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Servicekatalog** > **Services** > **Anforderungen für Penetrationstestbewertung**.
2. Um ein AVI für eine Penetrationstest-Bewertungsanforderung zu erstellen, wählen Sie die entsprechende Anforderung aus.
3. Wählen Sie im Abschnitt „Angreifbare Anwendungselemente“ **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Angreifbares Anwendungselement“ (Penetrationstest-Ansicht)

Feld	Beschreibung
Nummer	Automatisch generierter AVI-Bezeichner für diesen Datensatz.
Bewertungsanforderung	Penetrationstest-Bewertungsanforderung, der dieses AVI zugeordnet ist.
Schwachstelle	Schwachstelle, die mit der Suchoption aus der Tabelle „Schwachstelleneinträge“ ausgewählt wurde.
Risikobewertung	Quantifizierte **Risikopunktzahl,** die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikoeinstufungen finden Sie unter Risiko in Application Vulnerability Response automatisch berechnen. Ab V16.1 entspricht der Wert standardmäßig dem Schweregrad der Schwachstelle.
Auswirkungen auf Compliance-Programme?	Überprüft, ob Auswirkungen auf ein Compliance-Programm vorliegen. Auswahlmöglichkeiten sind Ja und Nein.
Liste der betroffenen Compliance-Programme	Dieses Feld wird angezeigt, wenn der Wert des Felds „Wirkt sich auf jedes Compliance-Programm aus“ auf *Yes* festgelegt ist. Listet die betroffenen Compliance-Programme auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geplante(s) Release/Korrekturversion	Geben Sie bis zu dem Zeitpunkt frei, zu dem die Penetrationstestergebnisse gelöst werden müssen.
Status	Der Standardwert ist **„Offen“**, wenn das AVI erstellt wird. Weitere Informationen zur Zuordnung von Status finden Sie unter Status des angreifbaren Elements in der Anwendung (Application Vulnerable Item, AVI)..
Zuweisungsgruppe	Gruppe für die Arbeit an diesem AVI ausgewählt. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an diesem AVI arbeitet. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Korrekturziel	Datum, bis zu dem die AVIs korrigiert werden müssen, ab der ersten Identifizierung. Dieses Feld wird nur angezeigt, wenn zutreffend. Weitere Informationen zu Korrekturzielen finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response.
Erstellt	Zeitstempel, der angibt, wann das angreifbare Element in der Anwendung erstellt wurde.
Aktualisiert	Zeitstempel, der angibt, wann das angreifbare Element in der Anwendung (Application Vulnerable Item, AVI) aktualisiert wurde.
Geöffnet von	Benutzer, der dieses Penetrationstest-Ergebnis erstellt hat.
Sicherheitsteamkontakt	Ansprechpartner im Team für ethisches Hacken.
Kurzbeschreibung	Kurze Erläuterung des Penetrationstest-Ergebnisses.
Details	
Technische Details	Technische Details des Penetrationstestergebnisses.
Auswirkung	Bewertung der Auswirkungen des Penetrationstestergebnisses.
Schritte zum Reproduzieren	Dokumentieren Sie die Schritte zum Reproduzieren und Überprüfen des Penetrationstestergebnisses.
Empfehlung	Erfassen Sie die empfohlenen Aktionen in diesem Feld.
Notizen	
Arbeitsnotizen	Fügen Sie Notizen hinzu, um Informationen über Statusübergänge und andere Feldaktualisierungen zu übermitteln.
V16.1: Betroffene URLs	Weitere Informationen im Zusammenhang mit den betroffenen URLs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
V16.1: Betroffene Parameter	Weitere Informationen zu den betroffenen Parametern.
V16.1: Betroffene Funktionalitäten	Weitere Informationen zu den betroffenen Funktionalitäten.

5. Um das Formular zu speichern, wählen Sie **Absenden**.

Erstellen Sie einen Anwendungsschwachstelleneintrag

Erstellen Sie einen Anwendungsschwachstelleneintrag für die Schwachstelle, die für das Penetrationstestergebnis angegeben ist. Anwendungsschwachstellen sind Schwachstellen in anwenderdefinierten Softwareanwendungen.

Vorbereitungen

Erforderliche Rolle: Ethical Hacker

Warum und wann dieser Vorgang ausgeführt wird

Application Vulnerability Response stellt eine Schwachstelle mit einer Anwendung in Zusammenhang, um das Penetrationstestergebnis zu erstellen. Bei diesen Ergebnissen handelt es sich um manuell erstellte angreifbare Elemente in Anwendungen (Application Vulnerable Items, AVIs). Sie können einen vorhandenen Eintrag wiederverwenden oder während Penetrationstests für jede Schwachstelle manuell einen erstellen.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Bibliotheken** > **Drittpartei**.
2. Wählen Sie auf der Seite „Anwendungsschwachstelleneinträge“ **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Anwendungsschwachstelle – Eintrag“ (Penetrationstest-Ansicht)

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle Schweregradzuordnungen werden für NVD und mit ServiceNow-Drittparteiintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu.
Primäres CVE	Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt.
Kategoriename	Von der Drittanbieterintegration bereitgestellte Klassifizierung. Hilft bei der Zuweisung.
Schwachstellendetails	
Angriffsvektor	Verwundbarster Angriffsvektor für diese Schwachstelle.
Angriffskomplexität	Metrik, die die Bedingungen beschreibt, die außerhalb der Kontrolle des Angreifers liegen und zum Ausnutzen der Schwachstelle vorliegen müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Umfang	Metrik zur Messung der Fähigkeit einer Softwareschwachstelle, Ressourcen über ihre Grenzen hinaus zu beeinträchtigen.
Integrität	Metrik zur Messung der Auswirkungen auf die Integrität einer erfolgreich ausgenutzten Schwachstelle.
CVSS-Vektor	Offenes Framework zur Erfassung der Merkmale und des Schweregrads von Softwareschwachstellen.
Erforderliche Berechtigungen	Berechtigungsebene, die ein Angreifer besitzen muss, damit er die Schwachstelle erfolgreich ausnutzen kann.
Anwenderinteraktion	Anforderung für menschliche Interaktion, um eine Schwachstelle erfolgreich auszunutzen.
Vertraulichkeit	Auswirkung auf die Vertraulichkeit der Informationsressourcen aufgrund einer erfolgreich ausgenutzten Schwachstelle. Diese Ressourcen werden von einer Softwarekomponente verwaltet.
Verfügbarkeit	Auswirkung auf die Verfügbarkeit der betroffenen Komponente, die sich aus einer erfolgreich ausgenutzten Schwachstelle ergibt.
CVSS-Basispunktzahl	Numerische Darstellung (0–10) des Schweregrads eines Anwendungsschwachstelleneintrags.
Bedrohung	Beschreibung der Bedrohung, die von dieser Schwachstelle ausgeht.
Beschreibung der Verringerung	Beschreibung der Schritte zum Minimieren der Schwachstelle.

4. Um das Formular zu speichern, wählen Sie **Absenden**.

Hinweis:
AVEs werden in der Tabelle „Anwendungsschwachstelleneintrag“ (sn_vul_app_vul_entry) erstellt. Die Tabelle „Anwendungsschwachstelleneintrag“ ist ein untergeordnetes Element der Tabelle „Schwachstelleneintrag“ (`sn_vul_entry`). Daher werden die erstellten AVEs auch der Tabelle „Schwachstelleneintrag“ hinzugefügt.

Arbeitsbereich für Penetrationstests

Der Arbeitsbereich für Penetrationstests in Application Vulnerability Response hilft Kunden, die Bewertung von Penetrationstests anzufordern und mithilfe des Workflows nachzuverfolgen. Damit können Anwendungsbesitzer die Sicherheitslage ihrer Anwendung bewerten. Es handelt sich um das manuelle Testen einer Anwendung durch das Team für ethisches Hacken.

Erforderliche Rollen

Penetrationstests erfordern die folgenden Rollen:

sn_vul.app_pen_tester: Stellt einen Pen-Tester dar, der für die Erstellung von Pen-Test-Ergebnissen als Teil der Anwendungspenetrationstests verantwortlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_vul.app_pen_test_requester: Datensatz für Aktion auswählen: sn_vul.app_pen_test_requester.

Lebenszyklus von Penetrationstests

Als Besitzer der Anwendung können Sie das Team für ethisches Hacken um einen Penetrationstest Ihrer Anwendung bitten. Das Team für ethisches Hacken bearbeitet diese Anforderung und erstellt Ergebnisse für Penetrationstests. Bei diesen Ergebnissen handelt es sich um manuell erstellte angreifbare Anwendungselemente (Application Vulnerable Items, AVIs).

Der Penetrationstest-Workflow deckt den Lebenszyklus für Penetrationstests ab, von der Erstellung der Testanforderung bis zur Lösung der Ergebnisse des Teams für ethisches Hacken.

Neue Anforderung für Penetrationstestbewertung erstellen

Initiieren Sie eine Penetrationstest-Bewertungsanforderung für Ihre Webanwendungen, mobilen Anwendungen oder APIs. Diese Anforderungen werden an das Team für ethisches Hacken übermittelt, das dann diese Anwendungen testet und die Ergebnisse der Penetrationstests manuell meldet.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Penetrationstest-Arbeitsbereich**.
2. Füllen Sie im Formular **„Anforderung für Penetrationstestbewertung“** die Felder aus.
3. Wählen Sie **Absenden**.
   Eine E-Mail-Benachrichtigung wird an das Team für ethisches Hacken gesendet, dass die Anforderung für die entsprechende Anwendung erstellt wurde.
4. Sobald das Formular übermittelt wurde, kann das Team für ethisches Hacken **mit der Umfangsdefinition beginnen**.
5. Nach der Umfangsdefinition vorbereitet der Besitzer der Anwendung die Testumgebung, und das Team für ethisches Hacken kann **mit dem Testen beginnen**.
6. Falls Sie die Details in der Anforderung von verifizieren müssen, können Sie die Testphase als angehalten markieren, indem Sie auf die Schaltfläche **In Warteschleife setzen** klicken.
7. Sobald die Tests abgeschlossen sind, können Sie die AVITs auf der Registerkarte Penetrationstest-Testergebnisse anzeigen.

Hinweis:
Sie können eine Anforderung aus einer vorhandenen Anforderung duplizieren. Nach dem Duplizieren werden die an die übergeordnete Anforderung angehängten AVITs in die duplizierte Anforderung verschoben (nicht kopiert).

Erstellen Sie Penetrationstestergebnisse basierend auf einem Bewertungsfragebogen

Erstellen Sie Penetrationstestergebnisse, die die Tests an den anerkannten Standards des LASVS-Fragebogens in den Penetrationstest-Workflow ausrichten. Bei diesen Ergebnissen handelt es sich um manuell erstellte Anwendungsschwachstellen (Application Vulnerability Items, AVIs).

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Penetrationstest-Ergebnisse** Registerkarte
2. Wählen Sie den veröffentlichten Fragebogen basierend auf Ihrer Anwendung aus.
3. Überprüfen Sie Tests, und markieren Sie die Testphase als abgeschlossen.
4. Schließen Sie die Anforderung nach Abschluss des obigen Schritts.

Hinweis:
Die vorhergehenden Schritte können von einem Mitglied des Teams für ethisches Hacken ausgeführt werden.

Veröffentlichen Sie den Bewertungsfragebogen

Für das Testen einer mobilen Anwendung hat die OAS-Community bestimmte Standards entwickelt, um Tester bei der Identifizierung von Fehlern in ihren Produkten zu unterstützen. Navigieren Sie zum Bewertungsarbeitsbereich, um den Fragebogen Ihrer Wahl zu erstellen. Veröffentlichen Sie sie, um sie im Formular für die Anforderung von Bewertungen anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_pen_test_requester

Erforderliche Rolle für anfordernde Person und Tester für Penetrationstests:

sn_vul.app_manage_pen_test_request:

enthält: sn_mart_asmt.assessment_reader sn_mart_asmt:assessment_admin sn_mart_asmt.actor.

sn_vul.app_pen_tester

enthält: sn_mart_asmt.assessment_reader sn_mart_asmt:actor.

Hinweis:
Als Teil der Funktion „Intelligente Bewertungs-Engine“ haben wir die oben genannten Rollen hinzugefügt. Diese Rollen sind wichtig, damit die anfordernde Person und der Tester für Penetrationstests die Fragebogen anzeigen und übermitteln können.

Prozedur

1. Navigieren zu **Bewertungsarbeitsbereich**.
2. In jedem Fragebogen befinden sich Richtlinien. Überprüfen Sie die Fragebögen, und ändern Sie sie bei Bedarf, um die Testanforderungen Ihrer Organisation zu erfüllen. Anschließend können Sie die Tests abschließen.
   Der Fragebogen entspricht standardmäßig den LASVS-Standards. Weitere Informationen finden Sie unter:
3. Veröffentlichen Sie die Fragebogen, und wählen Sie den veröffentlichten Fragebogen aus der Liste im Abschnitt „Testdetails“ des Formulars „Anforderung für Penetrationstestbewertung“ aus.

Hinweis:
Veröffentlichen Sie den Fragebogen, um ihn im Formular zum Anfordern einer Bewertung für Penetrationstests anzeigen zu können.

4. Die Persona, die die Tests durchführt, kann die Tests dann auf der Registerkarte Bewertung des Anforderungsformulars für Penetrationstests als „Bestanden“, „Nicht bestanden“ oder „Nicht zutreffend“ markieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie einen Bewertungsfragebogen

Nach der Erstellung des Bewertungsfragebogens können Sie diese Fragebogen zu Testzwecken verwenden.

Vorbereitungen

Erforderliche Rolle: sn_vul.app_pen_tester

Prozedur

1. Navigieren zu **Anforderung für Penetrationstests** Formular.
2. Befolgen Sie die im Formular genannten Richtlinien.
3. Wählen Sie eine **Penetrationstest-Anforderung**aus.
4. Navigieren Sie zur **Registerkarte Bewertung**.
5. Öffnen Sie die Registerkarte, beantworten Sie den Fragebogen, und **wählen Sie Absenden aus**.

Hinweis:
Die Persona, die der Penetrationstestanforderung zugewiesen ist, kann sie übermitteln.

Penetrationstest-Dashboard

Verschaffen Sie sich in Ihrem persönlichen Penetrationstest-Dashboard einen Überblick über Ihre Anforderungen für Penetrationstests und die manuellen Ergebnisse. Sie können den Fortschritt Ihres Teams mit im Penetrationstest-Arbeitsbereich anzeigen. Das Dashboard bietet Ihnen einen Überblick über die Ergebnisse von Penetrationstests. Sie können Tests, die Ihre Aufmerksamkeit erfordern, anzeigen und priorisieren, Testergebnisse nachverfolgen und Zuweisungen anzeigen.

Der Pen-Test-Manager /Leiter des Teams für ethisches Hacken kann die wichtigsten Metriken identifizieren und analysieren, z. B. die Überwachung der Penetrationstest-Anforderungen, und den Gesamtfortschritt seines Teams im Penetrationstest-Arbeitsbereich anzeigen. Der Pen-Test-Manager /Leiter des Teams für ethisches Hacken kann auch die folgenden Einblicke anzeigen:

- Übersicht über manuelle Ergebnisse, kategorisiert nach Status und Bewertungstyp, als Grundlage für strategische Entscheidungen.
- Verteilung der zugewiesenen Penetrationstests auf Personen zwecks besserer Kapazitätsplanung
- Priorisieren Sie überfällige Ergebnisse basierend auf ihrem Fortschritt, um die Lösungseffizienz zu verbessern.
- Landschaft der Pen-Test-Ergebnisse basierend auf kritischer Verteilung nachvollziehen.

Komponenten des Penetrations-Dashboards

Analysieren Sie den Fortschritt und die Daten Ihres Teams visuell, und verbessern Sie Ihre Geschäftsergebnisse mithilfe der Komponenten in Ihrem persönlichen Dashboard.

Indikatoren für wichtige Elemente

Zeigen Sie den nicht zugewiesenen Notfall-Release, Tests mit vergangenem Übersichtsdatum, nicht zugewiesene Tests und alle ausstehenden kritischen Validierungen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Nicht zugewiesene Notfall-Release**: Gibt die Gesamtanzahl der nicht zugewiesenen Penetrationstest-Anforderungen für den Bewertungstyp „Notfall-Release“ an.
- **Überfällige Tests**: Gibt die Gesamtanzahl der Tests mit überschrittenem Fälligkeitsdatum an.
- **Nicht zugewiesene Tests**: Gibt die Gesamtanzahl der dem Team nicht zugewiesenen Tests an.
- **Kritische Validierung ausstehend**: Gibt die Gesamtanzahl der AVITs für alle Anforderungen im Status „Validierung ausstehend“ an.

Hinweis:
Wählen Sie jede Kachel aus, um die Liste der Elemente anzuzeigen und die erforderlichen Aufgaben auszuführen.

Penetrationstest-Anforderungen

Zeigen Sie die Testanforderungen nach Status, überfällige Tests und Tests nach Release-Genehmigungen an.

- **Testanforderungen nach Status**: Gibt die Anzahl der Testanforderungen in diesen verschiedenen Status des Penetrationstest-Zyklus an. Sie können die Liste der Testanforderungen in verschiedenen Status anzeigen und zu ihnen navigieren, indem Sie auf die jeweilige farbige Kachel klicken. Sie können den Status dieser Tests auch für die folgenden sechs Monate anzeigen, indem Sie den Monat aus der Filter-Dropdown-Liste oben rechts auf der Registerkarte auswählen. Im Folgenden sind die verschiedenen Testanforderungsstatus aufgeführt:
  - Offen: Anzahl der offenen Testanforderungen.
  - Umfangsdefinition in Bearbeitung:
  - Umfangsdefinition abgeschlossen:
  - Vorbereitung der Umgebung:
  - Umgebung bereit zum Testen:
  - Test läuft:
  - Vollständiger Penetrationstest:
  - Fehlerprämienprogramme: Anreize für ethische Hacker mit Vergütungen, um Sicherheitsschwachstellen zu finden und zu melden.
  - Fokussierter Test:
  - Führungskompetenz: Bericht über Engagement und Unterstützung der Geschäftsleitung für kritische Projekte innerhalb der Organisation.
  - Einmalige Überprüfungen: Bewerten Sie bestimmte Projekte außerhalb der regulären Entwicklungs- und Releasezyklen, um die Leistung zu bewerten und Verbesserungen zu implementieren.
  - Notfall-Release: Unterstützt Notfall-Releases, die für schnelle Software-Updates erforderlich sind, um kritische Probleme wie Sicherheitsschwachstellen zu beheben.
- **Überfällige Tests:**: Gibt den Test an, der ab einem bestimmten Zeitraum aussteht. Sie können die Zeitleiste auswählen, für die Sie die fälligen Tests anzeigen möchten. Die Dropdown-Optionen lauten: **Gestern fällig**,**Diese Woche fällig**,**Letzte Woche fällig**,**Letzten Monat fällig**und **Vor dem letzten Monat fällig**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Tests nach Release-Genehmigungen**: Gibt Genehmigungsstatus für abgeschlossene Tests an, die zur Veröffentlichung bereit sind. Außerdem wird verifiziert, ob alle erforderlichen Prüfungen abgeschlossen sind, bevor neue Software bereitgestellt wird. Sie können den Status dieser Tests auch für die folgenden sechs Monate anzeigen, indem Sie den Monat aus der Filter-Dropdown-Liste oben rechts auf der Registerkarte auswählen.

Ergebnisse

Gibt die Anzahl der gemeldeten offenen Penetrationstestergebnisse (AVITs) zusammen mit der Anzahl der AVITs mit ausstehender Validierung an. Sie können die Liste der Ergebnisse in verschiedenen Status anzeigen und zu ihnen navigieren, indem Sie die jeweilige farbige Kachel auswählen. Die folgenden Daten können Sie in diesem Abschnitt anzeigen:

- **Offene Ergebnisse (AVITs) nach Risikobewertung**
- **Validierung für Ergebnisse ausstehend (AVITs)**

Teamübersicht

Gibt die Tests an, die den Teammitgliedern für die folgenden sechs Monate zugewiesen wurden. Im Folgenden finden Sie die verschiedenen Status:

- **Umfangsdefinition wird ausgeführt**
- **Offen**
- **Umfangsdefinition abgeschlossen**
- **Umgebung bereit zum Testen**
- **Test läuft**
- **Vorbereitung der Umgebung**

Platform Analytics-Lösungen für Application Vulnerability Response

Platform Analytics-Lösungen enthalten vorgefertigte Platform Analytics Inhalte zur Verwendung mit anderen Now Platform -Produkten. Dieser Platform Analytics-Lösung enthält wichtige Metriken zur Analyse des Prozesses für das Management von Anwendungsschwachstellen.

Übersicht

Das Inhaltspaket „Performance Analytics for Vulnerability Response“ ist unter ServiceNow® Store als separates Abonnement verfügbar. Die Anwendung wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Das Application Vulnerability Response-Inhaltspaket ist ein Teil des Performance Analytics for Vulnerability Response-Inhaltspakets.

Weitere Informationen zum Einrichten, Installieren und Konfigurieren Ihrer Anwendung Performance Analytics for Vulnerability Response finden Sie unter Anwendung Performance Analytics for Vulnerability Response [PA] installieren und konfigurieren.

Wichtige Begriffe

Performance Analytics (PA)

Lösung, die Managementdashboards und Berichte zu KPIs und Metriken erstellt und wichtige geschäftliche Fragen beantwortet, um die Qualität zu erhöhen und Kosten zu senken.

Angreifbares Anwendungselement (AVI)

Eine Anwendungsschwachstelle, die von einem Schwachstellenscanner einer Drittpartei gemeldet wurde und für ein Configuration Item (CI) vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PA-Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen einer Aktivität oder eines Organisationsverhaltens durchgeführt wird, z. B. Top-10-Anwendungen mit den kritischsten angreifbaren Anwendungselementen.

PA-Indikatorquelle

Datensätze, die Datensätze aus einer Tabellen- oder Datenbankansicht filtern, z. B. AVI Active.

- Das Dashboard „Meine Anwendungsschwachstellen“ verfolgt das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse/Erkennung bis zur Eindämmung oder Behebung.
- Zeigen Sie die Erreichungsraten der Korrekturziele an, und bestimmen Sie auf effiziente Weise, welche angreifbaren Elemente in einer Anwendung (Application Vulnerable Items, AVIs) das meiste Risiko für Ihre Organisation darstellen.

Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Die folgenden Dashboards bieten eine grafische Ansicht der AVI-Aktivität, um Korrekturpläne und Statusfortschritt zu bestimmen. Sie können sich auf die KPIs konzentrieren, die den kritisch betroffenen Anwendungen und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind.

- Das PA-Dashboard (Application Vulnerability Management) kommuniziert KPIs für Schwachstellenrisiko und -verbreitung, betroffene Anwendungen, Korrekturtrends und Korrekturfortschritt. Der Standardwert für Trends ist drei Monate, kann jedoch in „7 Tage“, „1 Monat“, „3 Monate“, „6 Monate“, „seit Jahresbeginn“, „1 Jahr“ oder „Alle“ geändert werden.
- Das Dashboard „Meine Anwendungsschwachstellen“ verfolgt das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse/Erkennung bis zur Eindämmung oder Behebung.

Hinweis:
Das Dashboard „Meine Anwendungsschwachstellen“ ist eine Teilmenge des Dashboards „Übersicht“ und nur verfügbar, wenn sich ein Mitglied der Benutzergruppe „Security Champion“ bei einer Instanz anmeldet. Weitere Informationen zum Dashboard „Meine Anwendungsschwachstellen“ finden Sie unter Dashboard „Meine Anwendungsschwachstellen“.

Application Vulnerability Management (PA)-Dashboard

Verfolgen Sie Volumen, Leistung und Fortschritt von Anwendungsschwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Behebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

Anwender	Dashboard-Verwendung
Schwachstellenmanager	Mit dem Dashboard Application Vulnerability Management kann das Schwachstellenmanagement bestimmen, welche angreifbaren Elemente in einer Anwendung (Application Vulnerable Items, AVIs) das meiste Risiko für ihre Organisationen darstellen. Diese Dashboards bieten eine grafische Ansicht der AVI-Aktivität, um Korrekturpläne und Statusfortschritt zu bestimmen. Konzentrieren Sie sich auf die KPIs, die kritischen betroffenen Anwendungen und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind.

Erforderliche Now Platform Rollen, Setup und die Dashboard-Registerkarten

Das Dashboard „Application Vulnerability Management“ (PA) ist als Teil des Inhaltspakets „Performance Analytics for Vulnerability Response“ enthalten. Das Performance Analytics for Vulnerability Response-Inhaltspaket wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Es ist unter ServiceNow® Store als separates Abonnement verfügbar.

Weitere Informationen zum Einrichten, Installieren und Konfigurieren Ihrer Anwendung Performance Analytics for Vulnerability Response finden Sie unter Anwendung Performance Analytics for Vulnerability Response [PA] installieren und konfigurieren.

Um das Dashboard anzuzeigen, navigieren Sie als Benutzer, der den Benutzergruppen Security Champion, App-Sec-Manager oder Entwickler zugewiesen ist, zu **Application Vulnerability Response** > **Übersicht**.

Hinweis:
Das Dashboard „Meine Anwendungsschwachstellen“ ist eine Teilmenge des Dashboards „Übersicht“ und nur verfügbar, wenn sich ein Mitglied der Benutzergruppe „Security Champion“ bei einer Instanz anmeldet. Informationen zum Dashboard „My Application Vulnerabilities“ (Meine Anwendungsschwachstellen) finden Sie unter Dashboard „Meine Anwendungsschwachstellen“..

Ab Version 19.0 von Application Vulnerability Responsekann dieses Dashboard auch in der New Experience UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard** -Symbol. Je nach Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdownliste neben dem Namen des Dashboards. Weitere Informationen finden Sie unter Seite „Dashboards“ im Vulnerability Manager Workspace und Seite „Dashboards“ im IT Remediation Workspace.

Das Dashboard „Übersicht“ kommuniziert KPIs für Schwachstellenrisiko und -verbreitung, betroffene Anwendungen, Korrekturtrends und Korrekturfortschritt. Der Standardwert für Trends ist drei Monate, kann jedoch in „7 Tage“, „1 Monat“, „3 Monate“, „6 Monate“, „seit Jahresbeginn“, „1 Jahr“ oder „Alle“ geändert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederung der Daten im Dashboard Application Vulnerability Management nach **Scantyp**, **Anwendung** oder **Geschäftsbereich**. Jede dieser Auswahlmöglichkeiten verfügt über einen zusätzlichen Filter: **Elemente auswählen**, um Ihre Auswahl einzugrenzen. Ab Application Vulnerability Response v15.0 wurden den Auswahlmöglichkeiten für den **Anwendungsfilter** Geschäfts- und CI-Anwendungen hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

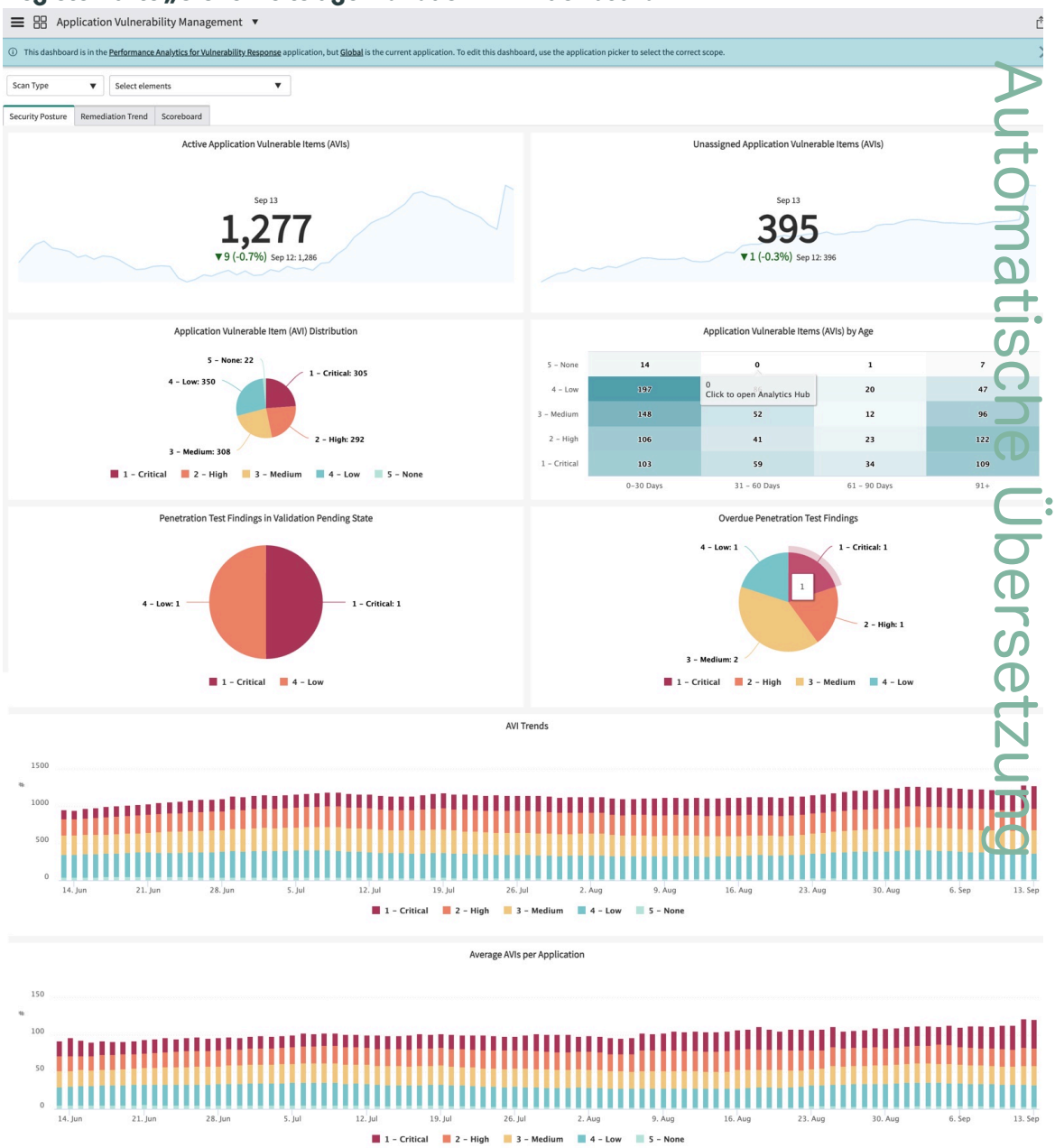
Registerkarte „Sicherheitslage“.

Die Registerkarte Sicherheitslage hilft Ihnen, Ihre Sicherheitslage und den Fortschritt Ihrer Korrekturmaßnahmen zu verstehen.

Ab Application Vulnerability Response v15.0 können Sie die Ergebnisseberichte zu Penetrationstests anzeigen. Penetrationstestergebnisse sind angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIs), die manuell basierend auf den Penetrationstest-Bewertungsanforderungen erstellt werden.

Hinweis:
Der Scantyp für diese Widgets ist Manuell.

Registerkarte „Sicherheitslage“ für das AVM-Dashboard



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

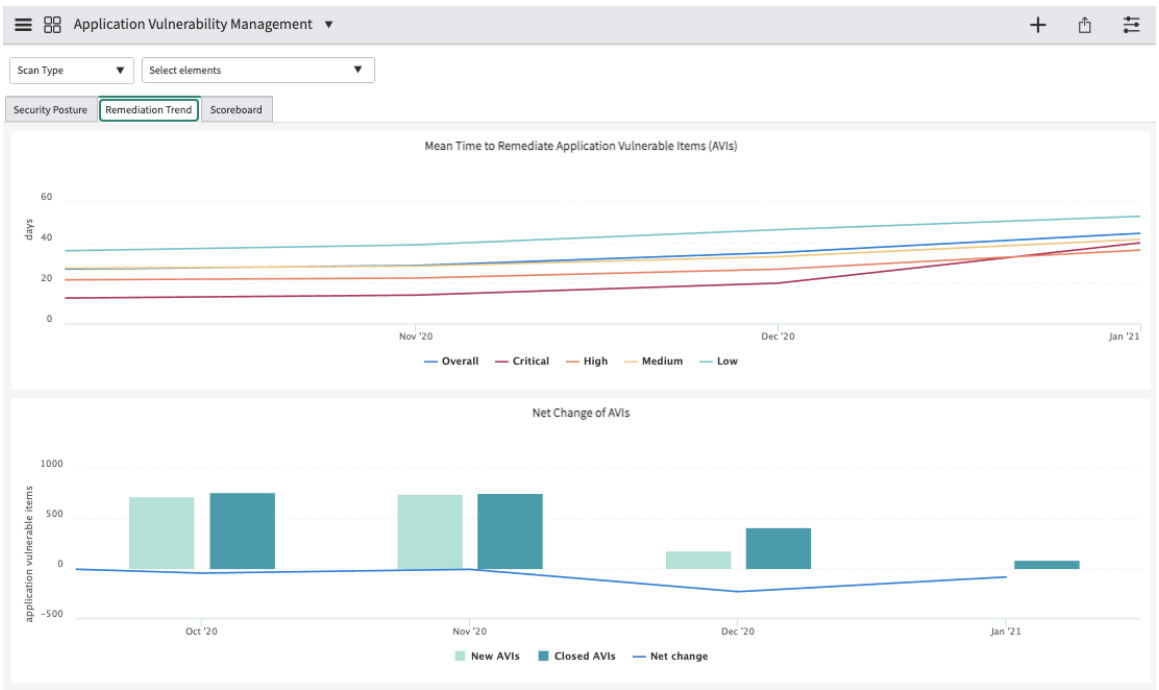
Registerkarte Ausnahmen

Dieses Dashboard hilft Ihnen zu verstehen, wo Ihre Organisation aufgrund potenziell übermäßiger Zurückstellungen Risiken eingeht, und hilft Ihnen, Abhilfemaßnahmen zu überdenken.

Sie können zurückgestellte angreifbare Anwendungselemente nach Grund, ablaufende Zurückstellungsanforderungen für AVIs, Ausnahmen für kritische angreifbare Anwendungselemente nach Zuweisungsgruppe und AVI-Ausnahmeanforderungen nach anfordernder Person anzeigen.

Registerkarte „Nachbesserungstrend“.

Auf der Registerkarte Korrekturtrend können Sie den Fortschritt Ihrer Korrekturaktionen nachvollziehen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

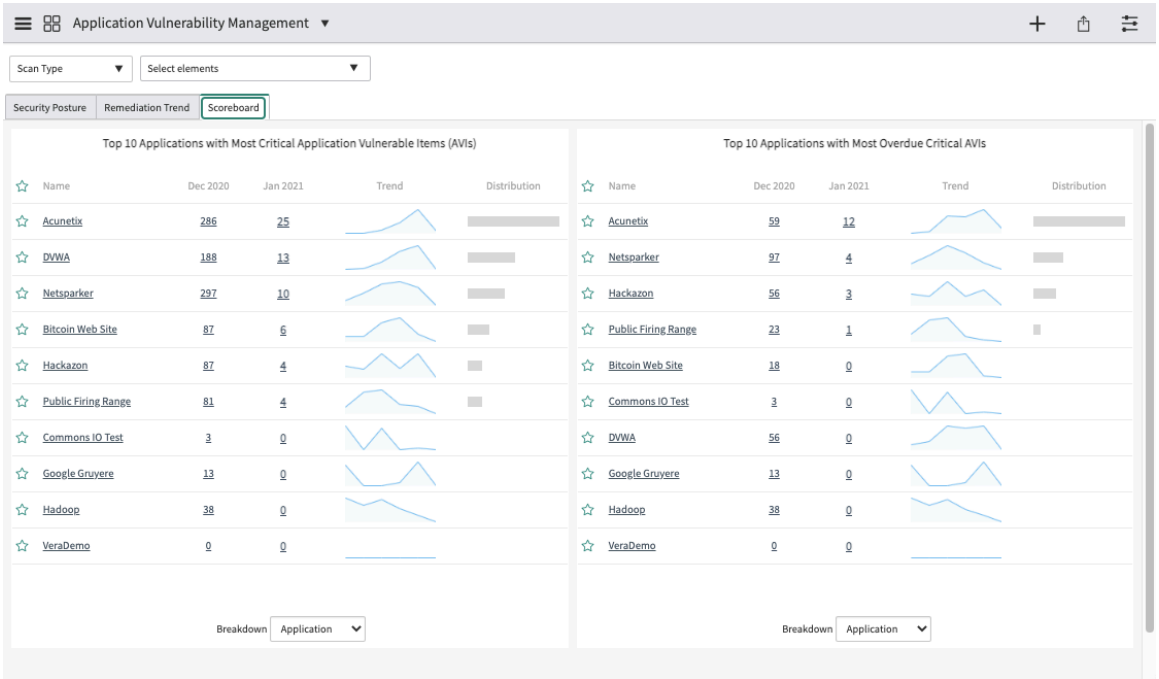
Registerkarte Anzeigetafel

Auf der Registerkarte „Bewertungsliste“ können Sie den Fortschritt Ihrer Korrekturmaßnahmen nachvollziehen und erfahren, welche AVIs bei deren Abschluss am meisten Unterstützung benötigen.

Scan-Typelemente:

- Dynamisch: Verwenden Sie nur Metriken aus dem dynamischen Datenimport
- Statisch: Verwenden Sie nur Metriken aus dem statischen Datenimport

Sie können eine oder beide Optionen auswählen.



Indikatoren

Mittlere Zeit bis zur Fehlerkorrektur niedriger AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 4 – Niedrig]]/[[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 4 – Niedrig]]. Ziel ist die Minimierung.

Anwendungsreleases

Dies ist die Anzahl eindeutiger Werte in Anwendungen von AVI.Active, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Angreifbare Anwendungselemente

Dies ist die Anzahl der angreifbaren Elemente in der App „AVI.Active“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Durchschnittliche AVIs pro Anwendung

[Aktive angreifbare Anwendungselemente]] / [[Anwendungsreleases]]. Ziel ist die Minimierung.

Nicht zugewiesene AEs

Dies ist die Anzahl der Indikatorquelle AVI.Active, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur von AVIs

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente]]/ [[Geschlossene angreifbare Anwendungselemente]] Ziel ist die Minimierung.

Mittlere Zeit bis zur Korrektur hoher AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 2 – Hoch]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 2 – Hoch]]. Ziel ist die Minimierung.

Geschlossene angreifbare Anwendungselemente

Dies ist die Anzahl der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Maximierung.

Mittlere Zeit bis zur Fehlerkorrektur kritischer AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 1 – Kritisch]]/[[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 1 – Kritisch]]. Ziel ist die Minimierung.

Neue angreifbare Anwendungselemente

Dies ist die Anzahl der Indikatorquelle „AVI.New“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur mittlerer AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 3 – Mittel]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 3 – Mittel]]. Ziel ist die Minimierung.

Nettoänderung in AEs

[[Neue angreifbare Anwendungselemente]] – [[Geschlossene angreifbare Anwendungselemente]] Ziel ist die Minimierung.

Summierte Dauer der geschlossenen angreifbaren Anwendungselemente

Dies ist die Anzahl der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Kritische überfällige angreifbare Anwendungselemente

Dies ist die Anzahl der Datenquelle „AVI.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Kritische angreifbare Anwendungselemente

Dies ist die Anzahl der Indikatorquellanwendungen mit aktiven AVIs, die die folgende Tabelle verwenden: sn_vul_analytics_app_ci_dept_bu. Ziel ist die Minimierung.

Aufgliederungen

- Alter
- Geschlossen mit Alter
- Anwendung
- Geschäftsbereich
- Risikobewertung
- Scantyp

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Anpassen von Alter und Alter der Berechnung von angreifbaren Elementen in Anwendungen kann zu einem starken Anstieg oder Rückgang der PA-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von „Alter“ und „Alter geschlossen für AVIs“ finden Sie im KB-Artikel KB1703270 .

Datenvisualisierungen

Sicherheitslage

Name	Typ	Beschreibung
V15.0: Penetrationstest-Ergebnisse im Status „Validierung ausstehend“.	Kreisdiagramm	Penetrationstest-Ergebnisse im Status „Gelöst“, aber mit ausstehender Validierung, gruppiert nach Risikobewertung
V15.0: Überfällige Penetrationstestergebnisse	Kreisdiagramm	Kritische Penetrationstestergebnisse, bei denen ihr Nachbesserungszieldatum verfehlt wurde, gruppiert nach Risikobewertung.
Aktive angreifbare Anwendungselemente (AVIs)	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) angreifbaren Anwendungselemente (AVIs).
Nicht zugewiesene angreifbare Anwendungselemente (AVIs)	Einzelne Punktzahl	Anzahl der aktiven angreifbaren Anwendungselemente (AVIs) ohne eine Zuweisungsgruppe.
Verteilung des angreifbaren Anwendungselements (AVI)	Kreisdiagramm	Distribution aller aktiven angreifbaren Anwendungselemente (AVIs) sortiert nach Risikobewertung.
Angreifbare Anwendungselemente (AVIs) nach Alter	Heatmap	Anzahl der aktiven angreifbaren Elemente in Anwendungen (Application Vulnerable Items, AVIs), gruppiert nach Risikobewertung und Alter (in Tagen). **Hinweis:** Das Anpassen von Alter und Alter der Berechnung von angreifbaren Elementen in Anwendungen kann zu einem starken Anstieg oder Rückgang der PA-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von „Alter“ und „Alter geschlossen für AVIs“ finden Sie im KB-Artikel KB1703270 .
AVI-Trends	Trendleisten-	Trend der aktiven angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.
Durchschnittliche AVIs pro Anwendung	Trendleisten-	Trend der durchschnittlichen angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trend bei Korrekturen

Name	Typ	Beschreibung
Durchschnittliche Zeit bis zur Korrektur von angreifbaren Elementen in der Anwendung (Application Vulnerable Items, AVIs)	Linie	Trend der durchschnittlichen Nachbesserungszeit für angreifbare Elemente in einer Anwendung (AVIs) nach Risikobewertung.
Nettoänderung von AVIs		Trend der erkannten neuen angreifbaren Anwendungselemente (Application Vulnerable Items, AVIs) im Vergleich zu den Schließungen pro Monat.

Anzeigetafel

Name	Typ	Beschreibung
Top-10-Anwendungen mit den kritischsten angreifbaren Anwendungselementen (AVIs)	Bewertungskarte und Verteilungsleiste	Anwendungen mit der höchsten Anzah an kritischen angreifbaren Elementen in einer Anwendung (AVIs).
Top-10 Anwendungen mit den meisten überfälligen kritischen angreifbaren Anwendungselementen (AVIs)	Bewertungskarte und Verteilungsleiste	Anwendungen mit der höchsten Anzahl aktiver angreifbarer Elemente in der Anwendung, deren Korrekturzieldaten verstrichen sind.

Dashboard „Meine Anwendungsschwachstellen“.

Dieses Dashboard enthält wichtige Metriken für die Analyse Ihres Prozesses für das Management von Anwendungsschwachstellen, z. B. die Anzeige der erreichten Raten für Korrekturziele.

Erforderliche Now Platform Rollen beim Anzeigen des Dashboards

Hinweis:

- Dieses Dashboard ist Teil des Inhaltspakets für Application Vulnerability Response. Das Application Vulnerability Response-Inhaltspaket ist Teil des Performance Analytics for Vulnerability Response-Inhaltspakets.
- Das Inhaltspaket „Performance Analytics for Vulnerability Response“ ist unter ServiceNow® Store als separates Abonnement verfügbar.
- Das Performance Analytics for Vulnerability Response-Inhaltspaket wird nicht automatisch mit der Anwendung Vulnerability Response installiert.

Das Dashboard „My Application Vulnerabilities“ (Meine Anwendungsschwachstellen) ist nur verfügbar, wenn sich ein Mitglied der Benutzergruppe „Security Champion“ bei einer Instanz anmeldet. Informationen zum Dashboard „Übersicht“ finden Sie unter Dashboard für das Anwendungs-Schwachstellenmanagement [PA].

Um das Dashboard anzuzeigen, navigieren Sie zu **Application Vulnerability Response** > **Meine Anwendungsschwachstellen**.

Ab Version 19.0 von Application Vulnerability Responsekann dieses Dashboard auch in der New Experience UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard** -Symbol. Je nach Rolle wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdownliste neben dem Namen des Dashboards. Weitere Informationen finden Sie unter Seite „Dashboards“ im Vulnerability Manager Workspace und Seite „Dashboards“ im IT Remediation Workspace.

Zeigen Sie Berichte an, die Trenddaten im Zeitverlauf zeigen. Zeigen Sie regelmäßig Trends wichtiger Metriken an, um Ihre allgemeinen Geschäftsprozesse zu analysieren und Verbesserungsbereiche zu identifizieren.

Das Dashboard „Meine Anwendungsschwachstellen“ ist im Inhaltspaket „Performance Analytics for Vulnerability Response“ enthalten. Das Performance Analytics for Vulnerability Response-Inhaltspaket wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Es ist unter ServiceNow® Store als separates Abonnement verfügbar.

Anwendungsfälle

Anwender	Dashboard-Verwendung
IT-Spezialisten, Korrekturbesitzer oder Analysten, die Schwachstellen beheben, die ihnen oder einer Gruppe, der sie angehören, zugewiesen sind.	Ein Security Champion verwendet das Dashboard „My Application Vulnerabilities“ (Meine Anwendungsschwachstellen), um Volumen, Leistung und Fortschritt der Nachbesserung von Anwendungsschwachstellen nachzuverfolgen. Ermitteln Sie effizient, welche angreifbaren Elemente in einer Anwendung (Application Vulnerable Items, AVIs) das meiste Risiko für Ihre Organisation darstellen. Diese Dashboards bieten eine grafische Ansicht der AVI-Aktivität, um Korrekturpläne und Statusfortschritt zu bestimmen. Sie können sich auf die KPIs konzentrieren, die den kritisch betroffenen Anwendungen und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind. Gewinnen Sie schnell Einblicke in das Gefahrenpotenzial von Schwachstellen und die Sicherheitslage. Nachverfolgung von der ersten Analyse und Erkennung bis zur Eindämmung oder Nachbesserung.

Registerkarten des Dashboards „My Application Vulnerabilities“ [PA]

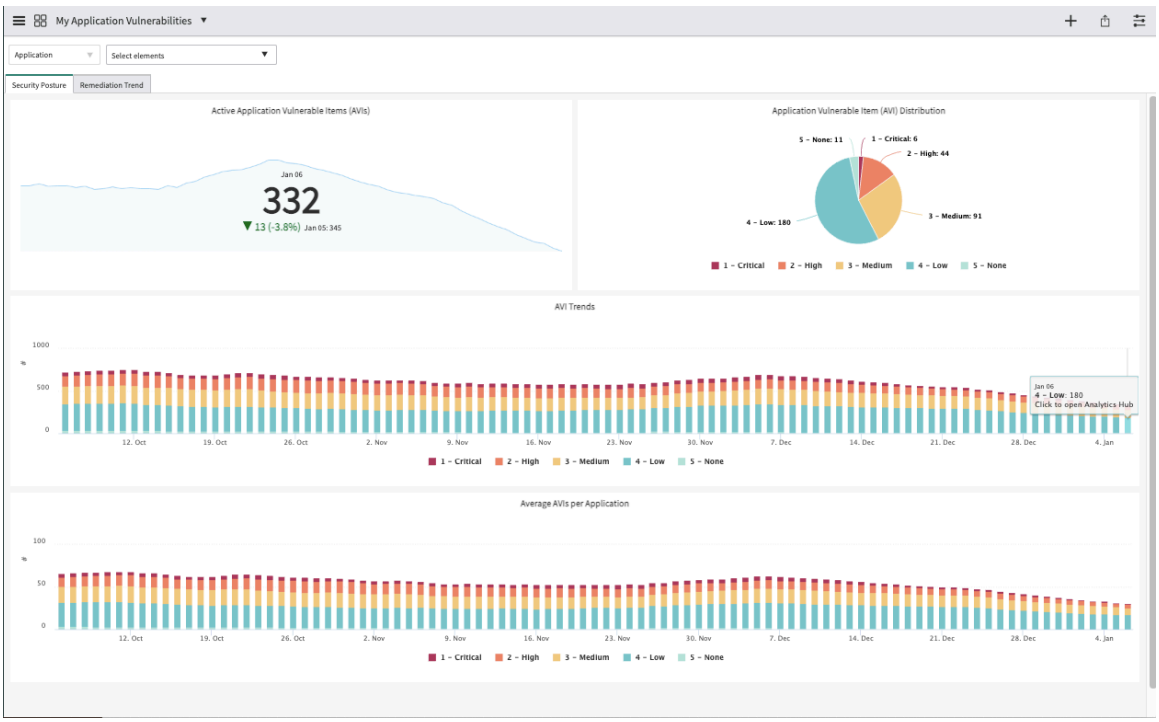
Das Dashboard „My Application Vulnerabilities“ (Meine Anwendungsschwachstellen) kommuniziert KPIs für Schwachstellenrisiko und -verbreitung, betroffene Anwendungen, Korrekturtrends und Korrekturfortschritt. Der Standardwert für Trends ist drei Monate, kann jedoch in „7 Tage“, „1 Monat“, „3 Monate“, „6 Monate“, „seit Jahresbeginn“, „1 Jahr“ oder „Alle“ geändert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Daten im Dashboard werden nach **Anwendung**aufgeschlüsselt. Verwenden Sie die Liste **Elemente auswählen**, um Ihre Auswahl zu verfeinern.

Registerkarte „Sicherheitslage“.

Die Registerkarte Sicherheitslage hilft Ihnen, Ihre Sicherheitslage und den Fortschritt Ihrer Korrekturmaßnahmen zu verstehen. Daten im Dashboard für Anwendungsschwachstellenmanagement nach **Scan-Typ, Anwendung** oder **Geschäftsbereich**aufschlüsseln. Jede dieser Auswahlmöglichkeiten verfügt über einen zusätzlichen Filter: **Elemente auswählen**, um Ihre Auswahl einzugrenzen.

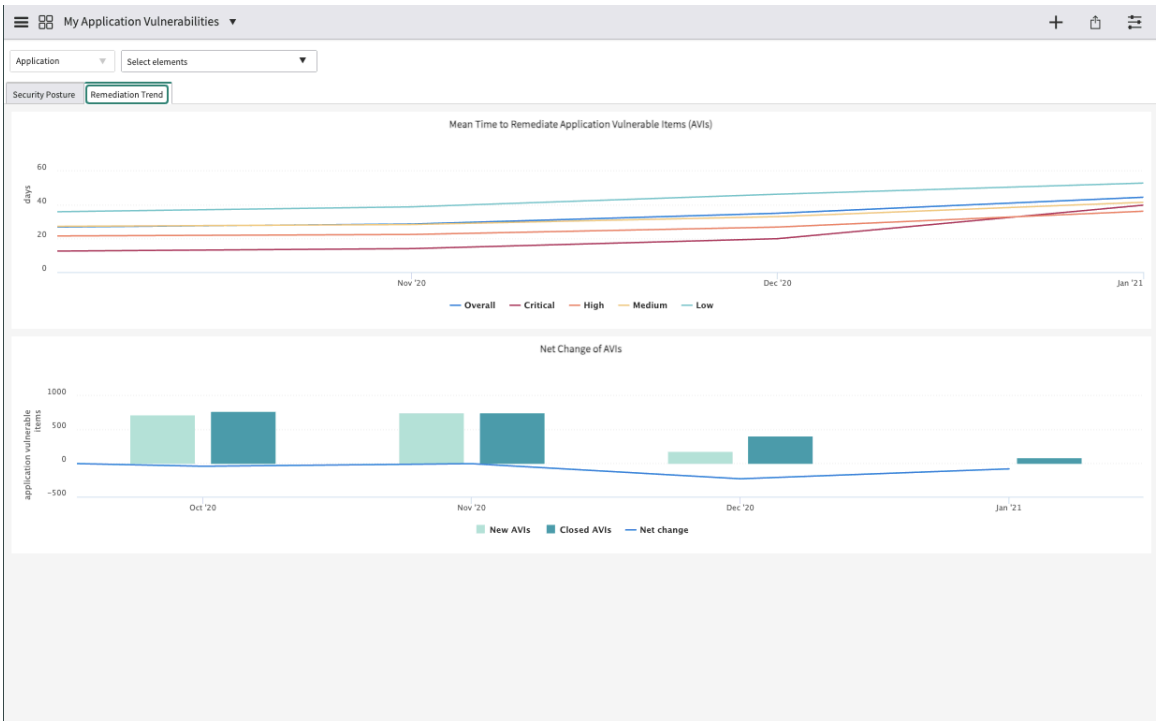


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Nachbesserungstrend“.

Auf der Registerkarte Korrekturtrend können Sie den Fortschritt Ihrer Korrekturaktionen nachvollziehen.



Indikatoren

Mittlere Zeit bis zur Fehlerkorrektur niedriger AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 4 – Niedrig]]/[[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 4 – Niedrig]]. Ziel ist die Minimierung.

Anwendungsreleases

Dies ist die Anzahl eindeutiger Werte in Anwendungen von AVI.Active, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Angreifbare Anwendungselemente

Dies ist die Anzahl der angreifbaren Elemente in der App „AVI.Active“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Durchschnittliche AVIs pro Anwendung

[Aktive angreifbare Anwendungselemente]] / [[Anwendungsreleases]]. Ziel ist die Minimierung.

Nicht zugewiesene AEs

Dies ist die Anzahl der Indikatorquelle AVI.Active, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur von AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente]]/ [[Geschlossene angreifbare Anwendungselemente]] Ziel ist die Minimierung.

Mittlere Zeit bis zur Korrektur hoher AVIs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 2 – Hoch]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 2 – Hoch]]. Ziel ist die Minimierung.

Geschlossene angreifbare Anwendungselemente

Dies ist die Anzahl der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Maximierung.

Mittlere Zeit bis zur Fehlerkorrektur kritischer AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 1 – Kritisch]]/[[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 1 – Kritisch]]. Ziel ist die Minimierung.

Neue angreifbare Anwendungselemente

Dies ist die Anzahl der Indikatorquelle „AVI.New“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur mittlerer AVIs

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 3 – Mittel]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 3 – Mittel]]. Ziel ist die Minimierung.

Nettoänderung in AEs

[[Neue angreifbare Anwendungselemente]] – [[Geschlossene angreifbare Anwendungselemente]] Ziel ist die Minimierung.

Summierte Dauer der geschlossenen angreifbaren Anwendungselemente

Dies ist die Anzahl der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Kritische überfällige angreifbare Anwendungselemente

Dies ist die Anzahl der Datenquelle „AVI.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

Kritische angreifbare Anwendungselemente

Dies ist die Anzahl der Indikatorquellanwendungen mit aktiven AVIs, die die folgende Tabelle verwenden: sn_vul_analytics_app_ci_dept_bu. Ziel ist die Minimierung.

Aufgliederungen

- Alter
- Geschlossen mit Alter
- Anwendung
- Geschäftsbereich
- Risikobewertung
- Scantyp

Hinweis:
Das Anpassen von Alter und Alter der Berechnung von angreifbaren Elementen in Anwendungen kann zu einem starken Anstieg oder Rückgang der PA-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von „Alter“ und „Alter geschlossen für AVIs“ finden Sie im KB-Artikel KB1703270 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen

Sicherheitslage

Name	Typ	Beschreibung
Aktive angreifbare Anwendungselemente (AVIs)	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) angreifbaren Anwendungselemente (AVIs).
Verteilung des angreifbaren Anwendungselements (AVI)	Kreisdiagramm	Distribution aller aktiven angreifbaren Anwendungselemente (AVIs) sortiert nach Risikobewertung.
AVI-Trends	Trendleisten-	Trend der aktiven angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.
Durchschnittliche AVIs pro Anwendung	Trendleisten-	Trend der durchschnittlichen angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.

Trend bei Korrekturen

Name	Typ	Beschreibung
Durchschnittliche Zeit bis zur Korrektur von angreifbaren Elementen in der Anwendung (Application Vulnerable Items, AVIs)	Linie	Trend der durchschnittlichen Nachbesserungszeit für angreifbare Elemente in einer Anwendung (AVIs) nach Risikobewertung.
Nettoänderung von AVIs		Trend der erkannten neuen angreifbaren Anwendungselemente (Application Vulnerable Items, AVIs) im Vergleich zu den Schließungen pro Monat.

Framework für zusammengefasste Berichte für Application Vulnerability Response

Mit dem Framework für aggregierte Berichte können Sie Berichte für die Daten erstellen, die komplexe und zeitaufwändige On-the-fly-Abfragen beinhalten, um eine bessere Leistung zu erzielen.

Das Framework für aggregierte Berichte verbessert die Leistung durch:

- Ressourcenverbrauch und Berichte werden schneller erstellt,
- die Daten zusammenzufassen und Zusammenfassungen und Aufgliederungen wiederzuverwenden (Gruppieren nach) und
- Dadurch werden weniger Abfragen an die Datenbank durchgeführt

Wenn Sie mehr als eine Million angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs) haben, verwenden Sie zusätzlich zu den Standardberichten das Framework für aggregierte Berichte.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- Now Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics -Administrator (pa_admin): Zusammenfassungen, Widgets und Dashboards überprüfen Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- VR-Lesevorgang (sn_vul_cmn.read): Überprüfen Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- Schwachstellenanalyst (sn_vul.vulnerability_analyst): Aggregierte Ergebnisse überprüfen.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Application Vulnerability Response Referenzen

Referenzthemen, die Informationen zu Tabellen, Rollen und Eigenschaften enthalten, die mit der Anwendung Application Vulnerability Response installiert werden.

Details finden Sie unter:

- Application Vulnerability Response Benutzergruppen und -rollen
- Mit Application Vulnerability Response installierte Komponenten
- Status des angreifbaren Elements in der Anwendung (Application Vulnerable Item, AVI).
- Gescannte Anwendungsfelder
- Felder für angreifbare Anwendungselemente
- Anwendungsschwachstellen-Felder
- Status der Penetrationstests

Application Vulnerability Response Benutzergruppen und -rollen

Bevor Sie Schwachstellen mit Application Vulnerability Response (AVR) erfolgreich beheben können, müssen Sie Benutzer Benutzergruppen zuweisen.

Rollen definieren, was Sie und Ihre Gruppen in Application Vulnerability Response, Performance Analytics for Vulnerability Responseund Drittanbieterintegrationen mit Application Vulnerability Responsesehen und tun können.

Anwendergruppen

Im Folgenden sind die Standardanwendergruppen aufgeführt, die Application Vulnerability Responseunterstützen:

- App-Sec-Manager: Enthält Sicherheitsmanager. Ab Application Vulnerability Response v15.0 enthält sie auch Anwendungsbesitzer, die die Bewertungsanforderungen für Penetrationstests verwalten.
- Security Champion: Enthält Verbindungspersonen zwischen der Entwicklungsgruppe und Sicherheitsmanagern.
- Entwickler: Enthält einzelne Beitragende.
- V15.0: Ethischer Hacker: Enthält Mitglieder des Teams für ethisches Hacken, die Penetrationstests für Anwendungen durchführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Systemadministratorrolle [admin] ist erforderlich, um Benutzer den Standardbenutzergruppen Application Vulnerability Response mithilfe des Moduls Benutzerverwaltung zuzuweisen.

Hinweis:

Das Zuweisen von AVR-Anwendern zu den Anwendergruppen Application Vulnerability Response für Application Vulnerability Response ist im Setup-Assistenten Vulnerability Response von nicht verfügbar. Dort sind nur Vulnerability Response Rollen zugewiesen.

In der folgenden Tabelle sind die verfügbaren -Anwendergruppen Application Vulnerability Response und die ihnen zugeordneten Rollen aufgeführt. Verwenden Sie diese Tabelle, um zu bestimmen, welche Anwender welchen Gruppen zugewiesen werden sollen.

Anwendergruppe	Rollen in dieser Gruppe
Security Champion Mitglieder dieser Gruppe können: • Ihnen zugewiesene angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVIs) lesen und schreiben. • Weisen Sie ein Ihnen zugewiesenes AVI einer anderen Person oder Gruppe zu. • V20.0: Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren)	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
App-Sec-Manager Mitglieder dieser Gruppe können: • V20.0: Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren) • Lese-, Schreib-, Lösch- und alle Vorgänge für Regeln für Anwendungskorrekturaufgaben. • Alle AVIs lesen und schreiben. • Konfigurieren Sie AVR, indem Sie Regeln, Rechner und Schweregradzuordnungen erstellen und verwalten. • Konfigurieren Sie Integrationen. • Löschen Sie AVIs. • Weisen Sie AVI Einzelpersonen oder Gruppen zu. • Verwalten Sie -Anwendungen. • Ermöglicht den Zugriff auf das Anwendungsmodul.	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_read_all • sn_vul.app_write_all • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations **Hinweis:** Standardmäßig enthält diese Rolle granulare Rollen für die Konfiguration der Drittanbieterintegration. Informationen zum Definieren oder Bearbeiten einer App-Sec-Manager-Benutzergruppe nach einzelnen oder spezifischen Integrationen finden Sie unter Vulnerability Response Personae und granulare Rollen. • sn_vul.app_manage_assignment_rules • sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendergruppe	Rollen in dieser Gruppe
• Integration planen, konfigurieren und ausführen. • Integrationen lesen und ausführen. • Zeigen Sie AVR-Dashboards Performance Analytics und Berichte an. • V15.0: Verwaltung von Bewertungsanforderungen für Penetrationstests.	• sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • Version 13.0: sn_vul.app_manage_app_sc • Nur Version 12.0: sn_vul.app_read_application_release [Entfernt in v12.1. Nicht verwenden] • sn_sec_int.admin • Version 13.0: pa_power_user • pa_viewer **Hinweis:** Ab Vulnerability Response v13.0 ist „pa_viewer“ in „pa_power_user“ enthalten und wird nicht mehr selbst benötigt. • V15.0: sn_vul.app_manage_pen_test_request • V15.0: sn_vul.app_update_state • V15.0: cmdb_read
Entwickler Mitglieder dieser Gruppe können: • Ihnen zugewiesene AVR-Datensätze für Lese- und Schreibvorgänge ausführen. • Weisen Sie ein Ihnen zugewiesenes AVI einer anderen Person oder Gruppe zu.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view
V15.0: Ethischer Hacker Mitglieder dieser Gruppe können: • Konfigurieren Sie die Standardzuweisungsgruppe und den Beauftragten für Bewertungsanforderungen für Penetrationstests. • Verwalten Sie die Ergebnisse von Penetrationstests.	• V15.0: sn_vul.app_update_state • V15.0: sn_vul.app_manage_pen_test_request • V15.0: itil • V15.0: sn_vul.app_read_all • V15.0: sn_vul.app_manage_pen_test_request_config • V15.0: sn_vul.app_manage_manual_avits

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendergruppe	Rollen in dieser Gruppe
• Verwalten Sie Bewertungsanforderungen für Penetrationstests. • Zeigen Sie angreifbare Anwendungselemente an. • Aktualisieren Sie die Zuweisung für angreifbare Anwendungselemente.	• V15.0: sn_vul.app_update_assigned_to • V15.0: sn_vul.app_update_assignment_group

Weisen Sie Anwender zu Anwendergruppen in zu Application Vulnerability Response

Weisen Sie Benutzer mithilfe des Moduls Benutzeradministration in Ihrer -Instanz Gruppen zu.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

So weisen Sie einen Anwender einer Gruppe zu oder entfernen ihn:

a. Navigieren zu **Administration** > **Gruppen**.

b. Suchen und öffnen Sie die entsprechende Gruppe, z. B. **App-Sec Manager**.
Der Gruppendatensatz wird angezeigt.

c. Wählen Sie die Registerkarte **Gruppenmitglieder** aus.
Die aktuellen Mitglieder der Gruppe werden angezeigt.

d. Klicken Sie auf **Bearbeiten**.
Das Formular „Mitglieder bearbeiten“ wird angezeigt.

e. Wählen Sie in der Liste **Sammlung** Anwender aus, die Sie der Gruppe hinzufügen oder aus ihr entfernen möchten.

f. Wenn alle Benutzer der **Liste Gruppenmitglieder** hinzugefügt oder entfernt wurden, klicken Sie auf **Speichern**.
Sie kehren zur Registerkarte **Gruppenmitglieder** zurück.

g. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Gruppenliste zurückzukehren.

Zugehörige Informationen

Mit Application Vulnerability Response installierte Komponenten

Mit Application Vulnerability Response installierte Komponenten

Mit der Aktivierung der Funktion Application Vulnerability Response werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen, Anwenderrollen und geplanten Aufgaben.

Ab v24.0.6 von Application Vulnerability Responsesind die am häufigsten verwendeten Systemeigenschaften jetzt in der Anwendung Application Vulnerability Response zugänglich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Application Vulnerability Response**Eigenschaften**.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Installierte Rollen

Granulare Rollen in Application Vulnerability Response werden standardmäßig bestimmten Anwendergruppen zugewiesen.

Hinweis:
Die Verwendung granularer Rollen außerhalb dieser Benutzergruppen erfordert Programmierkenntnisse und fortgeschrittene Application Vulnerability Response - oder ServiceNow -Kenntnisse.

Rollentitel [Name]	Beschreibung	Enthält Rollen
V20.0: sn_vul.app_manage_auto_exception_rule	Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren)	sn_vul.app_read_auto_exception_rule
sn_vul.app_manage_group_rules	Lese-, Schreib-, Lösch- und alle Vorgänge für Regeln für Anwendungskorrekturaufgaben.	• sn_vul.app_read_all • sn_vul.app_read_group_rules
V20.0: sn_vul.app_exception_approver	Genehmigt Ausnahmeregeln und Anforderungen zur Erweiterung von Ausnahmeregeln. Ab v20.0 wird die granulare Rolle sn_vul.app_read_all für diese Rolle entfernt, sodass Sie auf die Ihnen und Ihrer Gruppe zugewiesenen angreifbaren Anwendungselemente und Korrekturaufgaben zugreifen können, anstatt auf alle angreifbaren Anwendungselemente und Korrekturaufgaben.	• sn_vul.app_read_auto_exception • sn_vul.view_manager_workspace
sn_vul.app_false_positive_approver	Genehmigt falsch positive Anforderungen oder lehnt sie ab.	sn_vul.view_manager_workspace
sn_vul.app_read_assigned	Zeigen Sie Ihnen zugewiesene angreifbare Anwendungselemente (Application Vulnerable Items, AVIs) sowohl in der klassischen Anwenderoberfläche als auch in IT Remediation Workspacean.	sn_vul.view_rem_workspace

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Wichtig: Ab v24.0 von Vulnerability Responsehat die Rolle sn_vul.app_read_assigned die Berechtigung zum Zugriff auf IT Remediation Workspace.	
sn_vul.app_read_all	Zeigen Sie alle AVIs und zugehörige Informationen entweder in der klassischen Anwenderoberfläche oder in Vulnerability Manager Workspacean. **Wichtig:** Ab v24.0 von Vulnerability Responsehat die Rolle sn_vul.app_read_all die Berechtigung zum Zugriff auf Vulnerability Manager Workspace.	sn_vul.view_manager_workspace
sn_vul.app_write_assigned	Ihnen zugewiesene AVIs aktualisieren.	
sn_vul.app_write_all	Alle AVIs und zugehörigen Informationen aktualisieren.	
sn_vul.app_update_assignment_group	Aktualisieren Sie die AVI-Zuweisungsgruppe.	**Hinweis:** Bei Verwendung außerhalb der Standardbenutzergruppe ist sn_vul.ap oder sn_vul.app_write_assigned erfo
sn_vul.app_update_assigned_to	Aktualisieren Sie den AVI-Beauftragten.	**Hinweis:** Bei Verwendung außerhalb der Standardbenutzergruppe ist sn_vul.ap oder sn_vul.app_write_assigned erfo
sn_vul.app_configure_integrations	Konfigurieren Sie Drittanbieterintegrationen.	sn_vul.app_read_all sn_vul.app_read_integrations sn_sec_int.admin sn_vul_veracode.configure_integra sn_vul.configure_nvd_administratio [store-future: BEGIN review]sn_vul_fortify.configure_int

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
		Hinweis: Informationen zum Definieren oder einer App-Sec-Manager-Benutzergru einzelnen oder spezifischen Integrati Sie unter Vulnerability Response Per granulare Rollen.
sn_vul.app_read_integrations	Zeigen Sie alle Integrationen von Drittparteien an.	
sn_vul_veracode.configure_integration	Definieren, aktualisieren und löschen Sie Veracode-Integrationen.	
sn_vul.app_manage_assignment_rules	Definieren, aktualisieren und löschen Sie AVI-Zuweisungsregeln.	sn_vul.app_read_all sn_vul.app_read_assignment_rules
sn_vul.app_read_assignment_rules	Zeigen Sie Zuweisungsregeln an.	
sn_vul.app_manage_remediation_target_rules	Definieren, aktualisieren und löschen Sie AVI-Korrekturzielregeln.	sn_vul.app_read_all sn_vul.app_read_remediation_targ
sn_vul.app_manage_risk_score_configurations	Definieren, aktualisieren und löschen Sie AVR-Rechner und Risikoregeln.	sn_vul.app_read_all sn_vul.app_read_risk_score_config sn_sec_cmn.calc.write
sn_vul.app_read_risk_score_configuration	Zeigen Sie AVR-Rechner und Risikoregeln an.	
sn_vul.app_manage_applications	Anwendungsdatensätze anzeigen, aktualisieren und löschen.	
sn_vul.app_manage_app_sc	Gibt einem Security Champion die Möglichkeit, sich selbst zur zugehörigen Liste „Gescannte Anwendung“ hinzuzufügen oder daraus zu entfernen.	
sn_vul.app_pa_sc_view	Bietet relevante Ansicht für einen bestimmten Security Champion.	
sn_vul.app_manage_app_vul_permissions	[internal] Verwendet von sn_vul.app_manage_applications.	
sn_vul.app_manage_normalized_severity	Aktualisieren Sie die Zuordnung auf den Schweregrad „Normalisiert“.	sn_vul.app_read_normalized_severity
sn_vul.app_read_normalized_severity [Entfernt in v12.1. Nicht verwenden.]	Zeigen Sie Datensätze mit normalisiertem Schweregrad an.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul.app_read_application_release	Zeigen Sie Anwendungs-Release-Datensätze an.	
sn_sec_int.admin	Bietet Zugriff auf Integrationen.	
pa_power_user	Bietet Zugriff auf Berichte	pa_viewer
sn_vul.app_sec_manager	Priorisiert und verwaltet angreifbare Anwendungselemente.	
sn_vul.app_developer	Entwickler, der für die Behebung der Anwendungsschwachstellen verantwortlich ist.	
sn_vul.app_create_watch_topic	Erstellen Sie Überwachungsthemen für Anwendungsschwachstellen.	
sn_vul.app_read_watch_topic	Lesen Sie Überwachungsthemen für Anwendungsschwachstellen.	
sn_vul.app_edit_watch_topic	Bearbeiten Sie Überwachungsthemen für Anwendungsschwachstellen.	
sn_vul_blackduck.configure_integration	Konfigurieren Sie Drittanbieterintegrationen.	sn_vul_blackduck.configure_integration

Installierte geplante Aufgaben

Informationen zu gemeinsam genutzten geplanten Aufgaben für Vulnerability Response finden Sie unter Mit Vulnerability Response installierte Komponenten.

Geplante Aufgabe	Beschreibung
Ordnen Sie der automatischen Ausnahmeregel vorhandene AVIs zu	Wertet angreifbare Anwendungselemente im Hinblick auf Übereinstimmungen mit Ausnahmeregeln aus.
Eintrag und CVE M2M ausfüllen	Stellt vorhandene Datensätze mit mehreren CWE-Datensätzen in Einklang. Einmal nach dem Upgrade ausführen, um auszufüllen und dann zu deaktivieren.
Synchronisieren Sie die primäre CWE erneut	Für anwenderdefinierte primäre CWE-Berechnungen. Einmal nach dem Upgrade ausführen, um erneut zu synchronisieren und dann zu deaktivieren.
Rollup der Werte von angreifbaren	Berechnet Schwachstellen und Gruppen-Rollups für angreifbare Anwendungselemente.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
Anwendungselementen zu Schwachstelle und Gruppe	**Hinweis:** Ab v23.0 von Application Vulnerability Responsewird die regelmäßige Aufgabe erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade beinhaltet die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.
Black-Duck-Projektlisten-Integration	Ruft Daten in die Black-Duck-Projekttabelle ab und erfasst sie.
Black Duck-Anwendungslistenintegration	Importiert Anwendungen in die Tabelle der erkannten Anwendungen für alle Projektversionen, die mit der Black-Duck-Integration in der Projekttabelle verfügbar sind.
Integration von angreifbaren Elementen in der Black Duck-Anwendung	Nimmt angreifbare Elemente basierend auf den Schwachstellen, die von Scannern für jede erkannte Anwendung im System erkannt wurden, in eine ServiceNow-Anwendung auf.

Installierte Tabellen

Tabelle	Beschreibung
Anwendungs-Release sn_vul_app_release	Enthält Informationen zur Anwendungsversion.
Version 13.0: Anwendungssicherheits-Champions sn_vul_app_m2m_app_sc]	Enthält die Datensätze der Security Champion-Gruppe Application Vulnerability Response.
Anwendungsschwachstelleneintrag [sn_vul_app_vul_entry]	Enthält Anwendungsschwachstelleneinträge.
Anwendungsschwachstellenintegration sn_vul_app_integration	Enthält Application Vulnerability Response Integrationsdatensätze.
Ort für Anwendungsschwachstellen-Scan sn_vul_app_vul_scan_location	Enthält Informationen zum Scan-Standort von Drittparteien.
Zusammenfassung von Anwendungsschwachstellen-Scan sn_vul_app_vul_scan_summary	Enthält Zusammenfassungsinformationen zu Drittpartei-Scans.
Angreifbares Anwendungselement	Enthält AVI-Datensätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vul_app_vulnerable_item	Ab v19.0 werden für Software-Stücklisten folgende Spalten hinzugefügt: • sn_sbm_config_rule • sn_sbom_component • vex_berichtigung • vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
Gescannte Anwendung [sn_vul_app_scanned_application]	Enthält Anwendungsinformationen.
Statuszuordnung sn_vul_app_state_map]	Enthält die Statuszuordnung von Drittanbieterintegrationen zu AVI-Status (Application Vulner Item).
Schwachstellen-CWEs [sn_vul_m2m_entry_cwe]	Verknüpft CVE-Daten mit angreifbaren Anwendungseinträgen.
Anwendungskorrekturaufgabe – Manifest sn_vul_app_rt_manifest	Alle Aktualisierungen der Korrekturaufgabe werden mithilfe dieser Manifesttabelle von geplanten Aufgaben durchgeführt.
Anwendungskorrekturaufgabe sn_vul_app_vulnerability	Enthält Anwendungskorrekturaufgaben.
Element der Anwendungskorrekturaufgabe sn_vul_app_m2m_vul_group_item	M2M-Tabelle zwischen AVI und Anwendungskorrekturaufgaben.
Version 21.0: Angreifbare Anwendungselemente sn_vul_app_vulnerable_item	Enthält AVI-Datensätze.
Version 21.0: Paket sn_vul_app_package	Enthält Details zum Anwendungspaket.
Version 21.0: Lizenzen sn_vul_app_license	Enthält Anwendungslizenzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Version 21.0: Anwendungskorrekturaufgaben sn_vul_app_vulnerability	Enthält Anwendungskorrekturaufgaben.
sn_vul_blackduck_config	Enthält Konfigurationsdetails für die Black-Duck-Integration.
sn_vul_blackduck_project	Enthält Details der Projekte, die von Black Ente stammen.
sn_vul_blackduck_project_import	Importsatztabelle für die Black-Duck-Projekterfassung.
sn_vul_blackduck_app_import	Importsatztabelle für die Black Duck-Anwendungserfassung.
sn_vul_blackduck_avit_import	Importsatztabelle für die Black Duck-AVIT-Erfassung.

Status des angreifbaren Elements in der Anwendung (Application Vulnerable Item, AVI).

Application Vulnerability Response bietet ein Statusmodell für den Status Ihrer angreifbaren Elemente in der Anwendung (Application Vulnerable Items, AVIs) zu jedem Zeitpunkt. Wenn Sie wissen, wie die einzelnen Status miteinander zusammenhängen und sich gegenseitig beeinflussen, können Sie bestimmen, wann und wie Sie Ihre AVIs korrigieren müssen.

Status des angreifbaren Anwendungselements

Wenn Sie wissen, wie Status funktionieren, können Sie beim Erstellen oder Bearbeiten von Regeln für angreifbare Elemente in einer Anwendung helfen. AVIs haben mehrere mögliche Status, die vom importierten Korrekturstatus aus der Drittanbieterintegration zugeordnet werden. In einer AVI ist das Feld **„Status“** schreibgeschützt.

Application Vulnerability Response Status-Flow-Diagramm

Status	Beschreibung
Öffnen	Status beim Erstellen. In diesem Status können Sie: **V16: Weitere Details abrufen** Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen • Anforderung • Antwort **V16: Als falsch positiv markieren** Markieren Sie ein Element als falsch positiv, wenn der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, in Tatsächlich jedoch keine Schwachstelle vorliegt. **V16: Ausnahme anfordern**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (Bis) und einen Grund an, und geben Sie optional zusätzliche Informationen an. Verschiebt die Korrektur des Elements bis zu dem Datum, bis zu dem eine Ausnahme angefordert wird. **V15: Schließen** Wählen Sie den Status Geschlossen, einen Grund aus dem Dialogfeld „Angreifbares Element schließen“ aus, und geben Sie zusätzliche Informationen an. Schließt das AVI. **V15: Lösen** Markieren Sie ein geöffnetes AVI als gelöst, um es in den Status „Gelöst“ zu versetzen. Sie müssen im Dialogfeld „Angreifbares Anwendungselement beheben“ Lösungshinweise hinzufügen.
Zurückgestellt	**V15:** Dies wird durch die Option **„Ausnahme anfordern“** ausgelöst. Als Teil des Genehmigungs-Workflows lautet der Status „Zurückgestellt“ „Wird überprüft“ und kann erst geschlossen werden, wenn er genehmigt wurde. In diesem Status können Sie: **V16: Weitere Details abrufen** Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen • Anforderung • Antwort **Erneut öffnen** Überführt eine geschlossene oder gelöste AVI zurück in den Status „Offen“. **Schließen** Wählen Sie den Status Geschlossen, einen Grund aus, und geben Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	zusätzliche Informationen an. Schließt das AVI.
Wird untersucht	Wählen Sie diese Option aus der Liste **Status** aus. In diesem Status können Sie: **V20.0** Überführen Sie eine Korrekturaufgabe oder einen AVI-Datensatz manuell in den **Status „Warten auf Implementierung“**. **V16: Weitere Details abrufen** Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen • Anforderung • Antwort **V16: Als falsch positiv markieren** Markieren Sie ein Element als falsch positiv, wenn der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, in Tatsächlich jedoch keine Schwachstelle vorliegt. **V16: Ausnahme anfordern** Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (Bis) und einen Grund an, und geben Sie optional zusätzliche Informationen an. Verschiebt die Korrektur des Elements bis zu dem Datum, bis zu dem eine Ausnahme angefordert wird. **V15: Schließen** Wählen Sie den Status Geschlossen, einen Grund aus dem Dialogfeld „Angreifbares Element schließen“ aus, und geben Sie zusätzliche Informationen an. Schließt das AVI. **V15: Lösen** Markieren Sie ein geöffnetes AVI als gelöst, um es in den Status „Gelöst“ zu versetzen. Sie müssen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	im Dialogfeld „Angreifbares Anwendungselement beheben“ Lösungshinweise hinzufügen.
Warten auf Implementierung	Sie können Datensätze nur manuell in diesen Status überführen, indem Sie „Warten auf Implementierung“ von AVI und Korrekturaufgaben-Datensätze im Status „Wird untersucht“ auswählen. In diesem Status können Sie: **Öffnen** Überführt AVI zurück in den Status „Offen“. **Wird untersucht** Rufen Sie weitere Informationen zur Lösung ab. Wechselt zu „Wird untersucht“ **Lösen** Markieren Sie ein geöffnetes AVI als gelöst, um es in den Status „Gelöst“ zu versetzen. Sie müssen im Dialogfeld „Angreifbares Anwendungselement beheben“ Lösungshinweise hinzufügen. **Schließen** Wählen Sie den Status Geschlossen, einen Grund aus dem Dialogfeld „Angreifbares Element schließen“ aus, und geben Sie zusätzliche Informationen an. Schließt das AVI. Überführen Sie in diesem Status einen Datensatz in „Warten auf Implementierung“, wenn Ihre Recherche und Arbeit an einer Aufgabe abgeschlossen sind und zwar ein Fix für die Implementierung bereit ist, aber noch nicht verfügbar ist. Legen Sie das **Datum der Korrekturzusage** und **den Korrekturplan** fest. Nach der Implementierung lösen oder schließen Sie die -Datensätze.
Gelöst	Wird über die Schaltfläche „Lösen“ ausgelöst. In diesem Status können Sie: **V16: Weitere Details abrufen**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen • Anforderung • Antwort **Erneut öffnen** Wechselt zurück in den Status **„Offen“**. **Schließen** Wählen Sie den Status **Geschlossen**, einen Grund aus, und geben Sie zusätzliche Informationen an. Schließt die Gruppe. Notizen und Lösungsinformationen werden unter der Registerkarte **Notizen** angezeigt.
Abgeschlossen	Wird über die Schaltfläche „Schließen“ ausgelöst. In diesem Status können Sie: Erneut öffnen: Wechselt zurück in den Status „Offen“.

Hinweis:
Informationen zu den verschiedenen Integrationen, aus denen die AVI stammt, finden Sie unter Application Vulnerability Response mit anderen Anwendungen integrieren.

Status der Anwendungskorrekturaufgabe

Von der Erstellung bis zum Abschluss einer Anwendungskorrekturaufgabe durchläuft die Anwendungskorrekturaufgabe während des gesamten Nachbesserungsprozesses verschiedene Status.

Der Statusvorrang lautet wie folgt:

Zurückgestellt > **Gelöst** > **Warten auf Implementierung** > **Wird untersucht** > **Offen**

Der Statusübergang erfolgt, wenn Sie verschiedene Aktionen ausführen, z. B. Zurückstellen, Öffnen, Schließen usw.

Die Aktionen, die Sie für eine Anwendungskorrekturaufgabe in einem bestimmten Status ausführen können, ähneln denen einer Host-Korrekturaufgabe. Weitere Informationen finden Sie unter Vulnerability Response Status der Korrekturaufgaben in der Dokumentation Vulnerability Response.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v23.0 von Vulnerability Responsewurde die Schaltfläche **Schließen** entfernt, um sicherzustellen, dass das Schließen der Korrekturaufgabe vom Scanner gesteuert wird.

Application Vulnerability Response Beispiele für Regeln für Korrekturaufgaben

Beispiel für eine Korrekturaufgabenregel mit dem Bedingungsgenerator.

Eine Regel für Korrekturaufgaben anhand von Schwachstelle, Produktmodell, IP-Adresse und Zuweisungsgruppe

1. Legen Sie im Bedingungsgenerator für einen neuen Datensatz die Bedingung auf fest **Schwachstelle** > **ist** und geben Sie eine bekannte Schwachstelle ein.

   Schwachstellen werden aus den Integrationen „Nation Vulnerability Database“ (NVD) und „Common Weakness Enumeration“ (CWE) importiert (siehe Application Vulnerability Response konfigurieren) .

2. Wählen Sie im Abschnitt Gruppieren nach für das Feld Angreifbare **Anwendungselementegruppieren von die Option Angreifbares Anwendungselement aus**.
3. Wählen Sie im Feld Verwenden von **die Option Zuweisungsgruppe**aus.

   Verwenden Sie Zuweisungsregeln, um das Feld **Zuweisungsgruppe** automatisch für die Verwendung in Ihrer Regel für Korrekturaufgaben festzulegen. Sie können eine mit der Anwendung bereitgestellte Regel verwenden oder eigene Zuweisungsregeln einrichten. Weitere Informationen finden Sie unter Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu.

4. Wählen Sie eine andere Bedingung aus, z. B. Konfigurationselement für angreifbares Anwendungselement im Feld **Angreifbares Anwendungselement gruppieren von** und IP-Adresse oder Produktmodell im Feld **Verwenden von**.
5. Wählen Sie im Abschnitt Zuweisung für Korrekturaufgabenfeld nach Feld zuweisen **die Option Nach Feld gruppieren aus**.
6. Wählen Sie im Feld Gruppieren nach die **Option Zuweisungsgruppe**aus.

   Wie in diesem Abschnitt beschrieben, weist diese Auswahl angreifbare Elemente verschiedenen Gruppen basierend auf den Bedingungen zu, die Sie im Abschnitt „Gruppieren nach“ festgelegt haben. Obwohl die AVIs die Schwachstelle teilen, werden sie je nach CI-Produktmodell oder nach IP-Adresse verschiedenen Gruppen zugewiesen.

7. Wählen Sie **Absenden aus**, um Ihre Regel zu speichern.

Gescannte Anwendungsfelder

Anwendungen werden während des Imports unter gespeichert **Administration** > **Erkannte Anwendungen** in Application Vulnerability Response.

Gescannte Anwendungsfelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt, sofern nicht anders angegeben. **Abteilungs-** und **Supportgruppeneinträge** können von einem App-Sec-Manager manuell hinzugefügt oder bearbeitet werden.

Feld	Beschreibung
Name	Importierter Name der Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Version	Importierte Version der Anwendung, falls zutreffend.
Betriebsstatus	Importierter Betriebsstatus der Anwendung.
Abteilung	Importierte Abteilung, zu der die Anwendung gehört. Wenn leer, kann manuell hinzugefügt werden.
Geschäftsbereich	Importierter Geschäftsbereich, zu dem die Abteilung gehört. Wenn das Feld **Abteilung** ausgefüllt wird, wird dieses Feld automatisch mit dem Geschäftsbereich gefüllt, zu dem die Abteilung gehört. Andernfalls bleibt es leer und schreibgeschützt.
Support-Gruppe	Importierte Supportgruppe, zu der die Anwendung gehört. Wenn leer, kann manuell hinzugefügt werden.
Beschreibung	Importierte Beschreibung der Anwendung.
Letzte Complianceprüfung der Richtlinie am	Datum, an dem die Anwendung zuletzt von Veracode auf Richtlinien-Compliance gescannt wurde. Es wird in den verketteten Integrationen der Anwendungslistenintegration verwendet, in denen Unterstützung für die Delta-Erfassung für Anwendungen verfügbar ist, indem dieses Datum mit der Delta-Startzeit der jeweiligen Integrationen verglichen wird. **Hinweis:** Daten werden für Anwendungen abgerufen, die aus Veracode abgerufen werden, deren Wert für „Letzte Prüfung der Richtlinien-Compliance“ größer als oder gleich der „Startzeit“ (delta_start_time) der verketteten Integrationen ist.
Zugehörige Liste (nur für einen App-Sec-Manager oder Security Champion sichtbar)	
Security Champion	Listet die Anwendungen auf, die einem Security Champion zugeordnet sind. App-Sec-Manager können Mitglieder zur Liste hinzufügen oder daraus entfernen.

Felder für angreifbare Anwendungselemente

Angreifbare Elemente in der Anwendung (Application Vulnerability Items, AVITs) werden während des Imports von Drittpartei-Schwachstellenintegrationen automatisch erstellt.

Felder für angreifbare Anwendungselemente

Mit Ausnahme der Felder **Zuweisungsgruppe**, **Zugewiesen an** und **Notizen**sind alle anderen Felder in der AVIT schreibgeschützt.

Feld	Beschreibung
Nummer	Automatisch generierter AVIT-Bezeichner für diesen Datensatz.
Überprüfungstyp	Typ des Scanners, der diese AVIT gefunden hat. Die Auswahlmöglichkeiten lauten wie folgt: • Dynamisch • Statisches Objekt • SCA
Risikobewertung	Quantifizierte **Risikopunktzahl,** die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Risikoeinstufungen finden Sie unter Risiko in Application Vulnerability Response automatisch berechnen.
Risikopunktzahl	Berechnetes Risiko, das die AVI für Ihre Umgebung darstellt. Weitere Informationen finden Sie unter Risiko in Application Vulnerability Response automatisch berechnen.
Datum der Korrekturzusage	Das Datum, an dem AVITs korrigiert werden sollten, nachdem sie in **„Wird untersucht“**verschoben wurden. Dieses Feld wird nur angezeigt, wenn sich die AVIT im **Status „Wird untersucht“**befindet.
Korrekturziel	Datum, bis zu dem die AVITs korrigiert werden sollten, ab der ersten Identifizierung. Wird nur angezeigt, wenn zutreffend. Weitere Informationen zu Korrekturzielen finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response.
Korrekturstatus	Status der Korrektur für AVIT. Sie wird von der AVIT mit dem nächsten Fälligkeitsdatum bestimmt, falls zutreffend. Status umfassen: • In Ausführung • Ziel rückt näher • Vergangenes Ziel
Kategoriename	Name der Kategorie der Schwachstelle.
Schwachstelle	ID der Schwachstelle, die diesem angreifbaren Anwendungselement zugeordnet ist.
Anwendungs-Release	Version der Anwendung.
Anwendungsmodul	Betroffene Anwendung im DAST-Scan. Für SAST-Scans ausgeblendet.
Standort Version 14.0: SAST	DAST: URL-Speicherort der Schwachstelle in der Anwendung. SAST: Dateipfad und Zeilennummer der Schwachstelle in der Anwendung.
Status	Dieses Feld wird bei der Erstellung standardmäßig auf **Öffnen** gesetzt. Weitere Informationen zur Zuordnung von Status finden Sie unter Status des angreifbaren Elements in der Anwendung (Application Vulnerable Item, AVI)..
Grund	[Nur sichtbar, wenn sich das AIV im Status **„Geschlossen** “ befindet.] Erklärung des Status.
Zuweisungsgruppe	Gruppe für die Bearbeitung dieses AVIT ausgewählt. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an diesem AVI arbeitet. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden
Zuerst gefunden	Datum, an dem die Drittanbieterquelle das angreifbare Anwendungselement zum ersten Mal gefunden hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuletzt gefunden	Datum, an dem die Drittanbieterquelle das angreifbare Anwendungselement zuletzt gefunden hat.
Abgeschlossen	[Nur sichtbar, wenn sich die AVIT im Status „ **Geschlossen“** befindet.] Datum, an dem die AVI geschlossen wurde.
Geschlossen von	[Nur sichtbar, wenn sich die AVIT im Status „ **Geschlossen** “ befindet.] Entität, die die AVIT geschlossen hat.
Zusammenfassung	Importierte Beschreibung der Schwachstelle.
Ergebnisse Schreibgeschützte Daten, die aus einer Drittanbieterintegration importiert werden.	
AVIT-ID der Quelle	Importierter Identifier für die AVIT-Quelle.
Quellenschweregrad	Aus der Quellanwendung importierter Schweregrad.
Zieldatum für Quellenkorrektur	Importdatum, bis zu dem die Quelle eine Korrektur der AVIT erwartet.
Quellenminderungsstatus	Importierter Risikominderungsstatus aus der Quellanwendung.
Quellenkorrekturstatus	Korrekturstatus aus der Quellanwendung importiert.
Quellermittlungsstatus	[Nur sichtbar, wenn ausgefüllt] Importierter Problemstatus aus der Quellanwendung.
SDLC-Status	Importierter Status des Software-Entwicklungs-Lebenszyklus.
Entspricht der Richtlinie	Importierter Compliance-Status. Wenn kein Status angegeben wird, wird dieses Feld auf **„Nicht zutreffend“**festgelegt.
Quell-Link	URL zur AVIT-Quelle.
Quellhinweise	Notizen aus der Quelle importiert.
Schwachstellenzusammenfassung	Zusammenfassung aus der Quelle importiert.
Erklärung der Schwachstelle	Erklärung aus der Quelle importiert.
Empfehlung	Empfehlung aus der Quelle importiert.
Referenzen	Referenzen aus der Quelle importiert.
HTTP-Anforderung/-Antwort (nur bei DAST-Scans sichtbar)	
Quellenanforderung	HTTP-Anforderung
Quellenantwort	HTTP-Antwort
Notizen	
Korrekturplan	Details dazu, wie die AVITs korrigiert werden. Der Plan sollte bis zum **Datum der Korrekturzusage**implementiert werden. Dieses Feld wird nur angezeigt, wenn sich die AVIT im **Status „Wird untersucht“**befindet.
Zusätzliche Kommentare/ Arbeitsnotizen	Alle relevanten Informationen. Wählen Sie das Textfeld für Arbeitsnotizen aus, um Informationen hinzuzufügen. Ab Vulnerability Response v20.0 können Sie im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Anwendungselement Arbeitsnotizen hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Altersberechnungen für eine AVIT:

- Die Spalte „Alter“ in der AVIT-Liste zeigt an, wie lange (Format: Tage HH:MM:SS) ein AVIT aktiv ist. Der Alterswert für eine geschlossene AVIT ist 0.
- Die Spalte „Alter geschlossener“ in der AVIT-Liste zeigt die Dauer (Format: Tage HH:MM:SS) an, für die ein AVI aktiv ist, bevor es geschlossen wird. Für AVITs, die sich nicht im Status „Geschlossen“ befinden, ist der Wert „Alter geschlossen“ 0.

Weitere Informationen zum Anpassen der Berechnung des Alters und der Schließdauern finden Sie im Artikel KB1703270 .

Status der Penetrationstests

Anwendungsbesitzer können die Bewertung von Penetrationstests für ihre Anwendungen anfordern und den Fortschritt des Teams für ethisches Hacken überwachen, bis die Anforderung gelöst ist.

Die Bewertungsanforderung für einen Penetrationstest durchläuft die folgenden Übergangsstatus, bis sie gelöst wird.

Phasen der Bewertungsanforderung für Penetrationstests

Feld	Beschreibung
Status der Penetrationstests	
Öffnen	Status, wenn die Bewertungsanforderung vom Anwendungsbesitzer erstellt wird.
Umfangsdefinition	Das Team für ethisches Hacken bewertet die Anforderung und den Umfang der Anwendung.
Vorbereitung der Umgebung	Der Anwendungsbesitzer erstellt eine Umgebung mit Rollen und anderen Informationen und stellt sie dem Team für ethisches Hacken zu Testzwecken zur Verfügung.
Tests	Das Team für ethisches Hacken testet die Anwendung manuell, um die Ergebnisse des Penetrationstests zu identifizieren.
V16.1: Test läuft	Das Team für ethisches Hacken gibt an, dass derzeit Tests ausgeführt werden. Wenn dieser Status ausgewählt ist, wird die Option **Tests angehalten** im Formular verfügbar.
V16.1: Tests in der Warteschleife	Dieses Feld wird nur angezeigt, wenn der Status Test in Bearbeitung ausgewählt ist. Das Team für ethisches Hacken steuert die Servicelevel-Vereinbarungen (SLAs) der Penetrationstest-Bewertungsanforderungen, indem es bei Bedarf diesen Status auswählt. Dadurch wird sichergestellt, dass genaue SLAs gemeldet werden.
V16.1: Tests werden überprüft	Das Team für ethisches Hacken gibt an, dass die Tests abgeschlossen sind und von einem Fachexperten überprüft werden.
Abgeschlossen	Das Team für ethisches Hacken schließt die Bewertungsanforderungen für Penetrationstests,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Phasen der Bewertungsanforderung für Penetrationstests (Fortsetzung)

Feld	Beschreibung
	nachdem die Ergebnisse des Penetrationstests gemeldet wurden. **Hinweis:** Ab V16.1 können Sie die Option **„Anforderung kopieren und erstellen“** im Formular verwenden, um die Anforderung im Status „Geschlossen“ zu replizieren und eine neue Anforderung zu erstellen. Details finden Sie unter Replizieren Sie eine Penetrationstest-Anforderung im Status „Geschlossen“..
V16.1: Abgebrochen	Der Anwendungsbesitzer bricht die Bewertungsanforderung für den Penetrationstest ab.
V16.1: Entwurf	Der Anwendungsbesitzer erstellt eine Anforderung und speichert sie als Entwurf, bevor er die Anforderung übermittelt.
Status des angreifbaren Anwendungselements	
Öffnen	Wenn das Team für ethisches Hacken die Penetrationstestergebnisse identifiziert und erstellt, lautet sein Status „Offen“.
Gelöst	Wenn die Anwendungsteams die Ergebnisse des Penetrationstests auflösen, ändert sich ihr Status in Gelöst. **Hinweis:** Wenn das Ergebnis des Penetrationstests gelöst wurde, aber noch vom Team für ethisches Hacken validiert werden muss, lautet der Substatus `Validation Pending`.
Abgeschlossen	Das Team für ethisches Hacken überprüft, ob die Ergebnisse des Penetrationstests gelöst wurden, und ändert den Status in „Geschlossen“.

Verwalten der Statuszuordnung für Zurückstellungen und falsch positive Meldungen in Application Vulnerability Response

Sie können verwalten, wie die **Quellstatus** für angreifbare Elemente (Application Vulnerable Items, AVIs), die von Veracode Vulnerability Integration und Fortify Vulnerability Integration importiert werden, nach dem Import in Ihrer Instanz zugeordnet werden.

Ab v20.0 von Vulnerability Responsehaben Sie mehr Optionen für das Selektieren Ihrer importierten AVIs mit ServiceNow -Workflows.

Wenn Sie Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration oder Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integrationverwenden, bieten Ihnen die Konfigurationsseiten für die Integration zwei Optionen zur Verwaltung von Ausnahmen und falsch positiven Meldungen in Ihrer Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwalten Sie Ausnahmen in ServiceNow
- Verwalten Sie falsch positive Meldungen in ServiceNow

Erforderliche Rolle: App-Sec-Manager.

Anwendungsfall für Ausnahmeverwaltung

AVIs werden aus diesen Integrationen mit **Quellstatus** importiert. Beim Import werden diese Status den Status für **den Zielgrund** und **den Zielgrund** in Ihrer Instanz zugeordnet, da in einigen Fällen keine genauen Übereinstimmungen zwischen den Quellstatus Ihres Scanners und den von Ihrer Instanz verwendeten Status bestehen.

Beispielsweise werden Quellstatus wie **Keine Korrektur**, **Korrektur Zurückgestellt**, **Risiko akzeptiert**und **Risiko gemindert** aus Fortify Vulnerability Integration dem Status **Zurückgestellt** mit dem Substatus **Risiko akzeptiert** oder **Minderungssteuerung vorhanden** in Ihrer Instanz zugeordnet.

Auf den Konfigurationsseiten für diese Integrationen haben Sie die folgenden Optionen:

Option	Checkbox aktiviert	Beschreibung
Verwalten Sie Ausnahmen in ServiceNow	Y (standardmäßig)	Wenn Sie diese Option ausgewählt lassen, müssen Sie Ausnahmen aus AVI-Datensätzen anfordern. Importierte AVIs, die für den Status **„Zurückgestellt“** markiert sind, werden mit dem Ausnahmeverwaltungs-Workflow ServiceNow selektiert. AVIs mit **Quellstatus**, die normalerweise einem Status **„Zurückgestellt“** zugeordnet sind, werden dem **Zielstatus für die Selektierung** im Status „ **Offen** “ zugeordnet.
	N	Wenn Sie das Kontrollkästchen deaktivieren, bleiben die von Ihrem Scanner importierten **Quellstatus** erhalten. Diese AVIs werden dem **Zielstatus** als **Zurückgestellt**und einem **Zielgrundstatus** in Ihrer -Instanz zugeordnet. Sie werden nicht vom Ausnahme-Workflow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Checkbox aktiviert	Beschreibung
		selektiert, da sie nicht den Status für den **Zielselektierungsstatus** und **den Zielstatus für den Selektierungsgrund** zugeordnet sind. Die UI-Aktion „ **Ausnahme anfordern“** ist für den AVI-Datensatz nicht verfügbar, da sich der Datensatz bereits im Status „ **Zurückgestelltes** Ziel“ befindet.

Anwendungsfall für Falsch positiv

Für falsch positive Ergebnisse aus Veracode Vulnerability Integration werden Quellstatus wie **„Falsch positiv“** oder **„Potenziell falsch positiv“** dem Status „ **Geschlossenes Ziel“** mit dem Substatus „ **Falsch positiv“**zugeordnet.

Option	Checkbox aktiviert	Beschreibung
Verwalten Sie falsch positive Meldungen in ServiceNow	Y (standardmäßig)	Wenn Sie diese Option ausgewählt lassen, müssen Sie ein **Falsch-Positiv** aus AVI-Datensätzen anfordern. Importierte AVIs, die für den Status **„Falsch positiv“** oder **„Potenziell falsch positiv“** markiert sind, werden mit dem Ausnahmeverwaltungs-Workflow ServiceNow selektiert. AVIs mit **Quellstatus**, die normalerweise einem **geschlossenen Zielstatus** zugeordnet sind, werden in **Open** einem **Ziel-**Selektierungsstatus zugeordnet. Die UI-Aktion **„Falsch positiv“** ist für den AVI-Datensatz verfügbar.
	N	Wenn Sie das Kontrollkästchen deaktivieren, bleiben die von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Checkbox aktiviert	Beschreibung
		Ihrem Scanner importierten **Quellstatus** erhalten. Diese AVIs werden in Ihrer Instanz dem **ZielstatusGeschlossen** und dem **Zielgrund** Status **Falsch positiv** zugeordnet. Sie werden nicht vom falsch positiven Workflow selektiert. Die UI-Aktion **„Falsch positiv“** ist für den AVI-Datensatz nicht verfügbar, da sich der Datensatz bereits im Status „ **Geschlossenes** Ziel“ befindet.

Application Vulnerability Response Referenzen

Die folgenden Begriffe werden in Application Vulnerability Responseverwendet.

Angreifbare Anwendungselemente (AVIs)

Paarungen von Schwachstelleneinträgen und potenziell angreifbaren Anwendungen in Ihrer Unternehmensumgebung.

Zuweisungsregeln

Regeln für die Zuweisung von AVIs basierend auf Ihren definierten Kriterien.

Common Platform Enumeration (CPE)

Ein strukturiertes NIST NVD-Benennungsschema für IT-Systeme, Software und Pakete.

Common Vulnerabilities and Exposures (CVE)

Wörterbuch der öffentlich bekannten Informationssicherheitsschwachstellen und -risiken.

Common Weakness Enumeration (CWE)

Liste der von der Community entwickelten Software-Schwachstellentypen.

Integrationen

Geplante Aufgaben, die Berichtsdaten aus CWE oder einem Drittanbietersystem wie Veracodeabrufen, um Schwachstellendaten abzurufen.

Hinweis:
Wenn die Integration der US-Schwachstellendatenbank (National Vulnerability Database) des NIST in Vulnerability Response aktiviert und konfiguriert ist, ist die CVE-Ergänzung für CWEs verfügbar, aber nicht erforderlich. Informationen zur Integration der US-Schwachstellendatenbank (National Vulnerability Database) des NIST finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.

National Vulnerability Database (NVD)

Repository der US-Regierung für standardbasierte Schwachstellenmanagementdaten, dargestellt unter Verwendung des Security Content Automation Protocol (SCAP).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachbesserungszielregeln

Regeln, die zum Zuweisen von AVIs-Zieldaten für die Korrektur basierend auf Ihren definierten Kriterien verwendet werden.

Schwachstellen-Rechner

Rechner, die zur Priorisierung und Kategorisierung von Anwendungsschwachstellen auf Grundlage Ihrer definierten Kriterien verwendet werden.

Beispiel für eine Ausnahmeregel für Application Vulnerability Response

Beispielregel basierend auf einer bekannten Schwachstelle für eine Ausnahmeregel.

Feld	Beschreibung
Name	Ein eindeutiger Name, mit dem Sie den Zweck identifizieren und die Regel leicht finden können, z. B. Veracode-1 cwe-22exception.
Status	Schreibgeschützt: Entwurf
Gültig ab	Datum, ab dem diese Regel aktiv ist, um AVIs zurückzustellen.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel. Ein niedrigerer Wert hat Vorrang vor einem höheren.
Gültig bis	Datum, an dem die Korrekturaufgabe die Annahme neuer AEs beendet.
Zurückgestellt bis	Datum, bis zu dem die Korrekturaufgaben und AVIs zurückgestellt werden. An diesem Datum wird die AVUL geschlossen, alle AVIs werden aus der Aufgabe verschoben und werden erneut geöffnet. Gruppenregeln werden erneut auf diese AVIs angewendet.
Grund	Grund für die Erstellung dieser Ausnahmeregel. Wählen Sie eines aus der Liste aus, z. B. **Korrektur nicht verfügbar**.
Zuweisungsgruppe	Gruppe, die für die Nachverfolgung der zurückgestellten VIs zugewiesen ist, z. B. APP-Sicherheitsmanager.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen. In diesem Beispiel „AVIs zurückstellen“ mit der Schwachstelle – Veracode-1-22.
Bedingung	Filterbedingungen, um anzugeben, welche AVIs mit dieser Regel übereinstimmen. In diesem Beispiel lautet die Schwachstelle Veracode-1-22.
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für bereits vorhandene Daten ausführen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Sie diese Option deaktiviert lassen, wird Ihre Regel täglich von der geplanten Aufgabe *`Associate existing AVIs with Auto Exception Rule`* ausgeführt, beginnend mit neuen Daten. Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wird am **Gültig ab-**Datum einmalig eine geplante Aufgabe für die vorhandenen Daten ausgeführt.

Application Vulnerability Response-Produktübersicht

Application Vulnerability Response (AVR) erfasst die von Ihren Tools zum Testen der Anwendungssicherheit erkannten Schwachstellen und Schwachstellen und bietet einen zentralen Einblick, um die Sicherheitslage aller Anwendungen in Ihrer Umgebung zu verstehen.

Mit AVR können Sie die Risiken mit Nachbesserungs-Workflows reduzieren. Diese Produktansicht soll Ihnen helfen zu verstehen, wie AVR-Schlüsselentitäten mit dem Core-CSDM-Framework funktionieren.

Aktualisierte Terminologie

Ab AVR v19.0 wurden die folgenden Schlüsseltabellen- und Spaltennamen aktualisiert. Daher finden Sie in der Dokumentation Verweise auf den älteren und den neueren Namen.

Aktualisierte Liste von Begriffen, Tabellen und Feldnamen für AVR

Vor AVR v19.0	Ab AVR v19.0
CI-Suchregeln	Suchregeln
Formular „CI-Suchregel“.	Formular „Suchregel“.
CI-Übereinstimmungsregel	Übereinstimmungsregel
Tabelle durchsuchen	CI-Tabelle durchsuchen
Feld durchsuchen	CI-Feld durchsuchen
Anwendungs-Release	Erkannte Anwendungen
Anwendungs-Release-Tabelle	Tabelle der erkannten Anwendungen
Business-Relevanz	Geschäftsrelevanz – Quelle

Voraussetzungen

Installieren Sie die neuesten Versionen der folgenden Anwendungen:

- Security Support Common
- Vulnerability Response
- Security Integration Framework
- Security Support Orchestration
- Scanner-Integrationen wie Veracode und Fortify

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AVR und CSDM 4.0

Wenn Anwendungsschwachstellen vor AVR v19.0 erfasst wurden, wurde die Anwendung, für die die Schwachstellen erfasst wurden, mithilfe der CI-Suchregeln für die gescannten Anwendungen (sn_vul_app_scanned_application) gesucht. Wenn der Anwendungsnamen-Datensatz nicht vorhanden wäre, würde ein Eintrag vorgenommen.

Ab AVR v19.0 werden zur Ausrichtung an das CSDM 4.0-Framework die Produktmodelltabellen anstelle der Tabelle „Gescannte Anwendungen“ verwendet. Wenn die Anwendung über die -Version verfügt, erfolgt die Suche anhand der Tabelle „Softwaremodell“. Wenn keine Version vorhanden ist, erfolgt die Suche anhand der Tabelle „Anwendungsmodell“. Sowohl das Anwendungsmodell als auch das Softwaremodell sind untergeordnete Tabellen der Produktmodelltabelle, der Grundlagentabelle in CMDB. Im folgenden Screenshot wird das Produktmodell erläutert.

Systemeigenschaft

Um den auf dem CSDM 4.0-Produktmodell basierenden Suchprozess zu verwenden, legen Sie die Systemeigenschaft *sn_vul.use_product_model* auf *true*fest.

Überlegungen zu Systemeigenschaften

Name der Systemeigenschaft	Systemeigenschaftswert	Suchzielwert	Überlegungen
sn_vul.use_product_model	wahr	Wählen Sie den Wert **Produktmodell**aus	Neue Benutzer sollten den Wert **Produktmodell** auswählen, um die Produktmodell-Suchregeln des CSDM 4.0-Frameworks zu verwenden.
	falsch	Wählen Sie den Wert **Configuration item (Konfigurationselement)**aus	Bestehende Benutzer können weiterhin den CI-Suchprozess und die vorhandenen **CI-Suchregeln**verwenden.

Hinweis:
Um den Suchzielwert festzulegen, navigieren Sie zur Seite **„Suchregel“** > **[Suchregel für AVR-Integration]** > Feld **„Suchziel“**.

Suchregeln in AVR

Im CSDM 4.0-Framework werden anstelle von CI-Suchregeln produktmodellbasierte Suchregeln verwendet, um Einträge in den entsprechenden Produktmodellklassen zu erstellen. Ähnlich können Sie für Skripts die Suchregeln im Framework des CSDM 4.0-Modells definieren.

Ab AVR v19.0 müssen Sie beim Erstellen einer Suchregel im Feld **Suchziel** definieren, ob Sie den Konfigurationselement- oder den Produktmodell-Ansatz verwenden möchten. Weitere Informationen finden Sie unter Erstellen Sie eine CI-Suchregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkannte Anwendungen

Navigieren zu **Alle** > **Erkannte Anwendungen**. In der Tabelle Erkannte Anwendungen werden die von den Scannern erfassten Anwendungen angezeigt. Wenn die Systemeigenschaft `sn_vul.use_product_model` auf `true`festgelegt ist, können Sie die entsprechenden Produktmodelle für die Anwendungen anzeigen.

Überlegungen zu AVR

Vorhandensein von doppelten CI- oder Produktmodelldatensätzen

Stellen Sie sicher, dass die Systemeigenschaft `sn_vul.use_product_model` für den Suchprozess richtig konfiguriert wurde. Stellen Sie sicher, dass Sie entweder **Configuration Item** oder **Produktmodell** als Suchziel auswählen, wenn Sie das Suchregelformular konfigurieren.

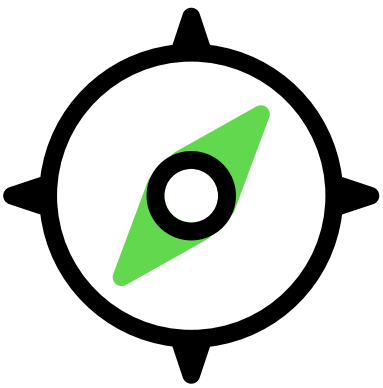
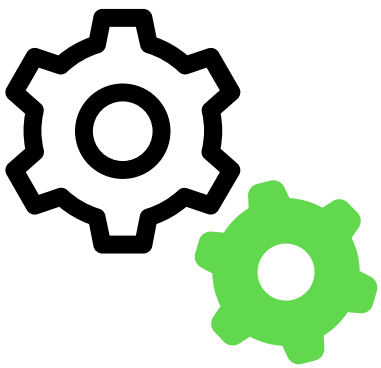
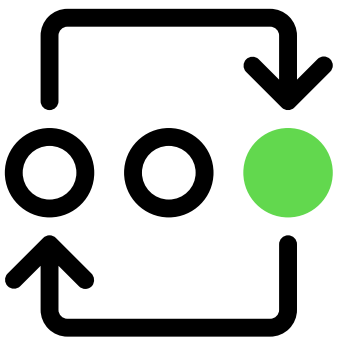
Container Vulnerability Response

Die Anwendung ServiceNow® Container Vulnerability Response importiert angreifbare Container-Elemente (CVITs) und ermöglicht Ihnen gemäß den Regeln, Container-Schwachstellen zu beheben. Schwachstellendaten werden aus internen und externen Quellen abgerufen, z. B. aus der National Vulnerability Database (NVD) oder aus Drittanbieterintegrationen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Container Vulnerability Response

Untersuchen	Konfigurieren	integrieren
		
Erfahren Sie mehr über die Konzepte und Funktionen von Container Vulnerability Response.	Konfigurieren Sie Container Vulnerability Response.	Erweitern Sie Container Vulnerability Response durch die Integration mit anderen Anwendungen.

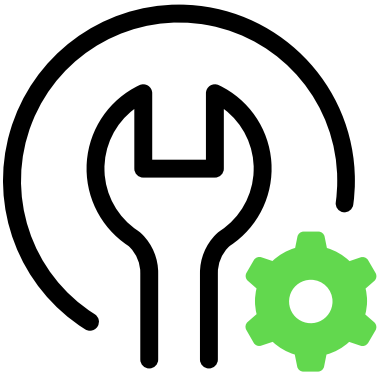
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Container Vulnerability Response (Fortsetzung)

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

Erfahren Sie, wie Sie CVITs in den Arbeitsbereichen Vulnerability Manager, IT Remediation und Vulnerability Assessment überwachen, verwalten und beheben können.

Beheben

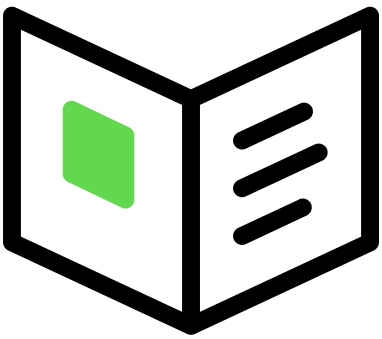


Erfahren Sie, wie Sie Container-Schwachstellen beheben können.

Analytics und Reporting

Zeigen Sie Container Vulnerability Response Analytics an

Referenz



Rufen Sie Details zu Container Vulnerability Response-Komponenten wie Felder, Tabellen und Eigenschaften ab.

Vorteile

Die Anwendung Container Vulnerability Response bietet die folgenden Vorteile:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Integration von Containersicherheitsprodukten von Drittparteien wie Prisma Cloud Compute von Palo Alto Networks.
- Importiert Schwachstellendaten für die Images, die zur Laufzeit bereitgestellt werden, und ergänzt die Schwachstellendaten mit kontextbezogenen Informationen zur Laufzeit (Hosts, Kubernetes-Cluster, Services und Namespaces).
- Stellt eine Liste der Referenzen bereit, die aus Schwachstellen für die relevanten Kubernetes-Entitäten in Configuration Management Database (CMDB) mithilfe von ServiceNow Kubernetes-Discovery erstellt wurden.
- Bietet ein umfassendes Reporting-Dashboard, das Einblicke in Schwachstellen- und Korrekturtrends gewährt.

Schlüsselfunktionen

Die Anwendung Container Vulnerability Response verwaltet in den -Containern erkannte Schwachstellen. Sie bietet die folgenden Funktionen:

- Zeigen Sie, um ein Docker-Image aus CVITs zu beziehen, anstatt Container auszuführen.
- Konfigurieren Sie die Granularität von CVITs, um sie auf Image-, Kubernetes-Cluster-, Namespace- oder Serviceebene nachzuverfolgen.
- Verfolgen Sie neue Image-Versionen, um behobene Schwachstellen zu identifizieren. Alle in älteren Versionen gemeldeten Schwachstellen werden in ServiceNow automatisch behoben, wenn neue Image-Versionen zur Laufzeit bereitgestellt werden.
- Verfolgen Sie CVITs in Basis-Images getrennt von Anwendungs-Images, um eine unabhängige Korrektur zu ermöglichen.
- Lösen Sie Ausnahmeanforderungen oder falsch positive Anforderungen aus, die durch einen mehrstufigen Genehmigerprozess überprüft werden können.
- Definieren Sie Ausnahmeregeln, um CVITs automatisch zurückzustellen.

Anwendungsfälle

Container sind eine großartige Möglichkeit, Anwendungen in mehreren Umgebungen mit weniger Overhead und erhöhter Portabilität bereitzustellen und zu skalieren. Schwachstellen in Container-Images können jedoch ein Risiko für den zugrunde liegenden Host und letztendlich für die Infrastruktur darstellen, in der Container von diesen Images gestartet wurden. Obwohl es viele Containersicherheitsprodukte gibt, die Containerbilder auf Schwachstellen scannen, gibt es bei der Nachbesserung von Schwachstellen einige Überlegungen und Probleme. Container Vulnerability Response kann zur Lösung verschiedener Probleme oder Anwendungsfälle im Zusammenhang mit der Behebung von Container-Image-Schwachstellen beitragen. Erfahren Sie, wie Sie das Modul Container Vulnerability Response nutzen können:

Laufzeitkontext

Schwachstellen in Container-Images können erkannt werden, indem das Image in den folgenden Phasen des Anwendungslebenszyklus gescannt wird.

- Phase 1: Wenn Bilder in der CI/CD-Pipeline erstellt werden.
- Phase 2: Wenn Bilder in der Registry veröffentlicht werden
- Phase 3: Wenn Bilder zur Laufzeit bereitgestellt werden.

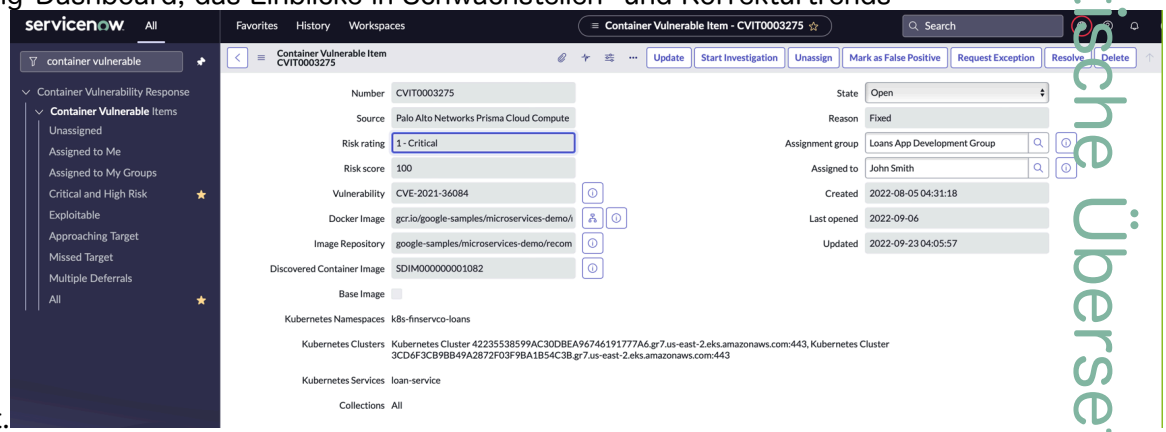
Während es wichtig ist, Schwachstellen in Phase 1 und Phase 2 so früh wie möglich zu identifizieren, ist es ebenso wichtig, einen Scan der Images

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

durchzuführen, die in einer Laufzeitumgebung bereitgestellt werden. Sie bietet folgende Vorteile:

- Identifizieren neuer allgemeiner Schwachstellen und Gefährdungen (CVE), die veröffentlicht wurden.
- Bietet genauen Einblick in die Risikosituation der bereitgestellten Anwendungen.
- Priorisierung von Schwachstellen, die behoben werden müssen. Der Laufzeitkontext in Bezug auf die Anwendungsservices oder Business Services, die von einer Schwachstelle betroffen sind, kann bei der Priorisierung helfen.

Container Vulnerability Response lässt sich in Containersicherheitsprodukte wie Prisma Cloud Compute von Palo Alto Networks integrieren, um die Schwachstellendaten für die Images abzurufen, die zur Laufzeit bereitgestellt werden, und erweitert die Schwachstellendaten mit den kontextbezogenen Laufzeitinformationen wie Hosts, Kubernetes-Cluster, Services und Namespaces, in denen diese Container-Images werden bereitgestellt. Kunden, die die Kubernetes-Discovery ServiceNow verwenden, können die aus Schwachstellen erstellten Verweise auf die relevanten Kubernetes-Entitäten in ihrer Configuration Management Database (CMDB)sehen. Zusätzlich zur Anreicherung von Metadaten bietet ServiceNow auch ein umfassendes Reporting-Dashboard, das Einblicke in Schwachstellen- und Korrekturtrends gewährt.



Identifizieren Sie den Besitz

Voraussetzungen

- **Kubernetes-Metadaten und -Referenzen**: Damit Container Vulnerability Response Kubernetes-Metadaten (Namespace, Cluster usw.) und Verweise auf Configuration Management Database (CMDB) -Einträge ausfüllen kann, müssen Sie die Kubernetes-Discovery von Information Technology Operations Management (ITOM) implementieren. Die Kubernetes-Discovery füllt das Docker-Image, die ausgeführten Docker-Container, Pods, Kubernetes-Cluster usw. im CMDBaus. Container Vulnerability Response identifiziert das Docker-Image in CMDB basierend auf der Image-ID, identifiziert dann die zugehörigen Kubernetes-Entitäten und füllt die Verweise auf diese Entitäten aus angreifbaren Elementen.
- **Cloud-Metadaten und Docker-Image-Bezeichnungen**: Container Vulnerability Response füllt auch Docker-Image-Bezeichnungen, Cloud-Account-IDs und Regionen aus, in denen ein Image bereitgestellt wird. Diese Daten werden im Datensatz „Erkanntes Containerimage“ verwaltet, das dem angreifbaren Element zugeordnet ist. Es gibt keine Voraussetzungen, damit

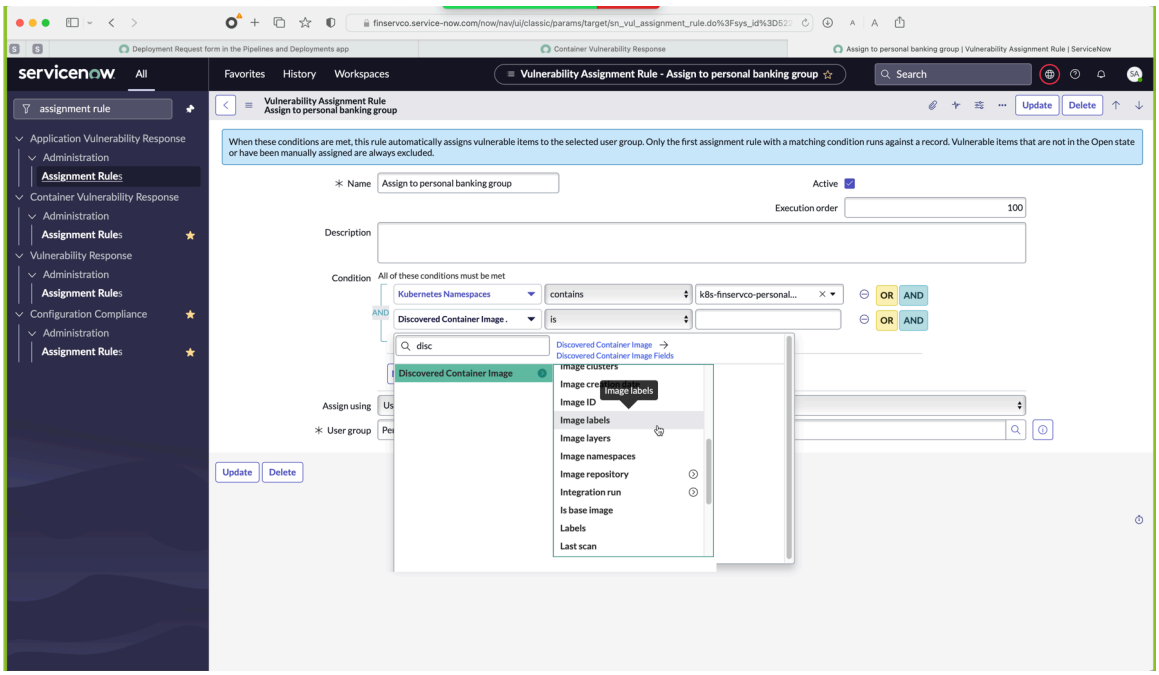
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Daten ausgefüllt werden. Container Vulnerability Response verwendet die von Containersicherheitsprodukten (z. B. Palo Alto Prisma Cloud Compute) zurückgegebenen Daten, um diese Einträge zu füllen.

Die Zuständigkeit für das Patchen einer Schwachstelle in einem Containerimage kann von Organisation zu Organisation unterschiedlich sein. Diese Informationen können an verschiedenen Orten erfasst werden. Einige Organisationen verwenden Docker-Image-Bezeichnungen, um die Anwendungsteams zu identifizieren, die Besitzer eines bestimmten Containerimages sind, während andere Organisationen den Kubernetes-Namespace oder den Cloud-Account, in dem ein Containerimage bereitgestellt wird, verwenden können, um den richtigen Besitzer zu identifizieren.

Container Vulnerability Response stellt die erforderlichen Datenmodellelemente bereit, um Docker-Image-Bezeichnungen, Kubernetes-Cluster-/Service-/Namespace-Metadaten oder Cloud-Account-Metadaten (Cloud-Account-ID, Region, Provider usw.) unter „Zuweisungsregeln“ erfassen und verwenden zu können. Modul und weisen Schwachstellen automatisch dem richtigen Anwendungsteam basierend auf den Metadaten des Images oder der Laufzeitumgebung zu.



Verfolgen Sie Schwachstellen in Basis-Images nach

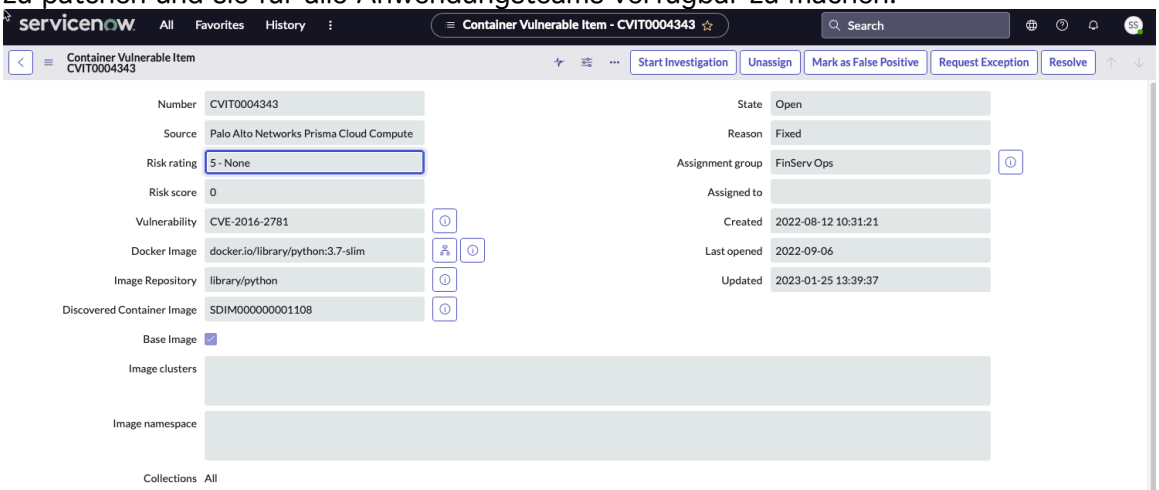
Voraussetzungen

Damit die Eigenschaft „Basisimage“ in Container Vulnerability Responseausgefüllt wird, müssen Basisimages explizit in der Konsole Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute konfiguriert werden. Weitere Informationen zur Konfiguration von Basis-Images in Prisma Cloud finden Sie unter https://docs.palalatonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/base_images.

Container Vulnerability Response ermöglicht die Erstellung separater Schwachstellen-Datensätze für eine Basisebene, sodass sie einem anderen Team zugewiesen werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

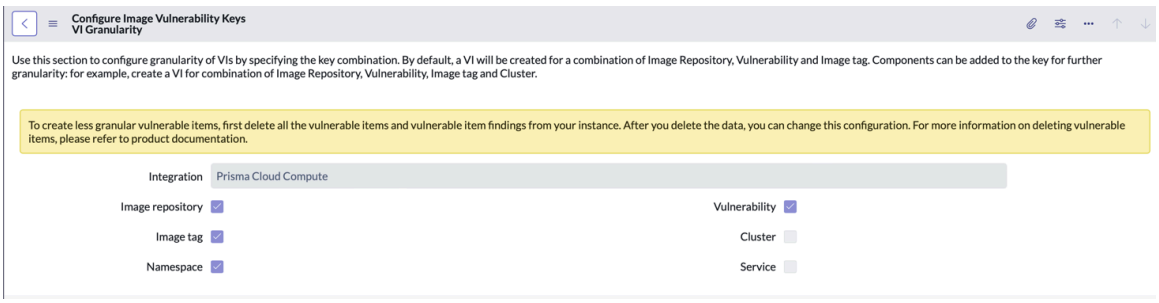
Verfolgen Sie Schwachstellen, die in einem Basis-BS-Image (z. B. Country) identifiziert wurden, anhand der in anderen Ebenen des Container-Images erkannten Schwachstellen. Viele Organisationen haben dedizierte Teams, die dafür verantwortlich sind, Basisbetriebssysteme zu patchen und sie für alle Anwendungsteams verfügbar zu machen.



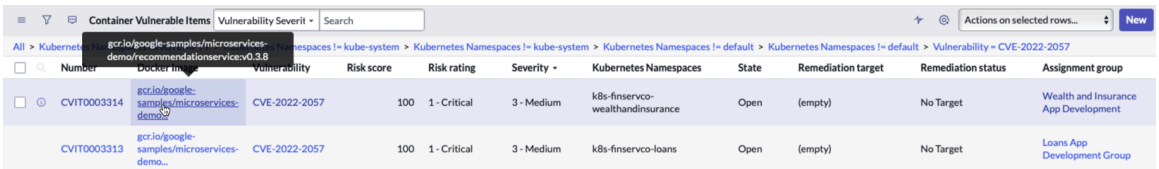
Definieren Sie Granularität für angreifbare Elemente

Voraussetzungen

Konfigurieren Sie die Granularität von CVITs, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.



Standardmäßig wird für jede eindeutige Kombination aus CVE und Docker-Image-Version (Referenz + Tag) ein angreifbares Element erstellt. Einige Docker-Images können jedoch in mehr als einem Kubernetes-Namespace bereitgestellt werden, und jeder Namespace kann im Besitz anderer Geschäftsbereiche oder Teams sein. Jedes Team kann seinem eigenen Zeitplan für die Einführung neuer Versionen von Container-Images folgen, um Schwachstellen zu beheben. Um diesem Szenario Rechnung zu tragen, können Sie Container Vulnerability Response mit die Granularität für angreifbare Elemente definieren: Gibt an, ob für jeden Kubernetes-Namespace/-Cluster/-Service ein eigenes angreifbares Element erstellt werden soll, auch für jede eindeutige Kombination aus Docker-Image-Version und Schwachstelle.



Im Beispiel sehen Sie zwei angreifbare Elemente, die für dieselbe Kombination aus Docker-Image und CVE erstellt wurden. Einer für den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kubernetes-Namespace „k8s-finservco-loans“ und einer für „k8s-finservco-wealthandinsurance“.

Identifizieren Sie betroffene Services mithilfe der Tag-basierten Serviceidentifizierung

Voraussetzungen

- Identifizieren Sie verschiedene Services in Ihrer Anwendung, und definieren Sie die Tags/Schlüssel-Wert-Paare, die diese Services darstellen.
- Stellen Sie Docker-Images und Kubernetes-Pods mit diesen Tags oder Bezeichnungen bereit.
- ITOM Kubernetes Discovery bereitstellen Definieren Sie „Tag-basierte Services“ mit den richtigen Tags oder Bezeichnungen.
- Stellen Sie ITOM Kubernetes Discovery bereit
- Definieren Sie „Tag-basierte Services“ mit den richtigen Tags oder Schlüssel-Wert-Paaren.
- Schwachstellendaten mit ServiceNow in Container Vulnerability Responseimportieren

Die Berechnung des Risikos für angreifbare Elemente kann anhand des CI (Docker-Image) und der Relevanz der zugehörigen Services in CMDBerfolgen. Um jedoch die Identifizierung betroffener Services zu erleichtern, bietet Container Vulnerability Response eine tagbasierte Serviceidentifizierung an.

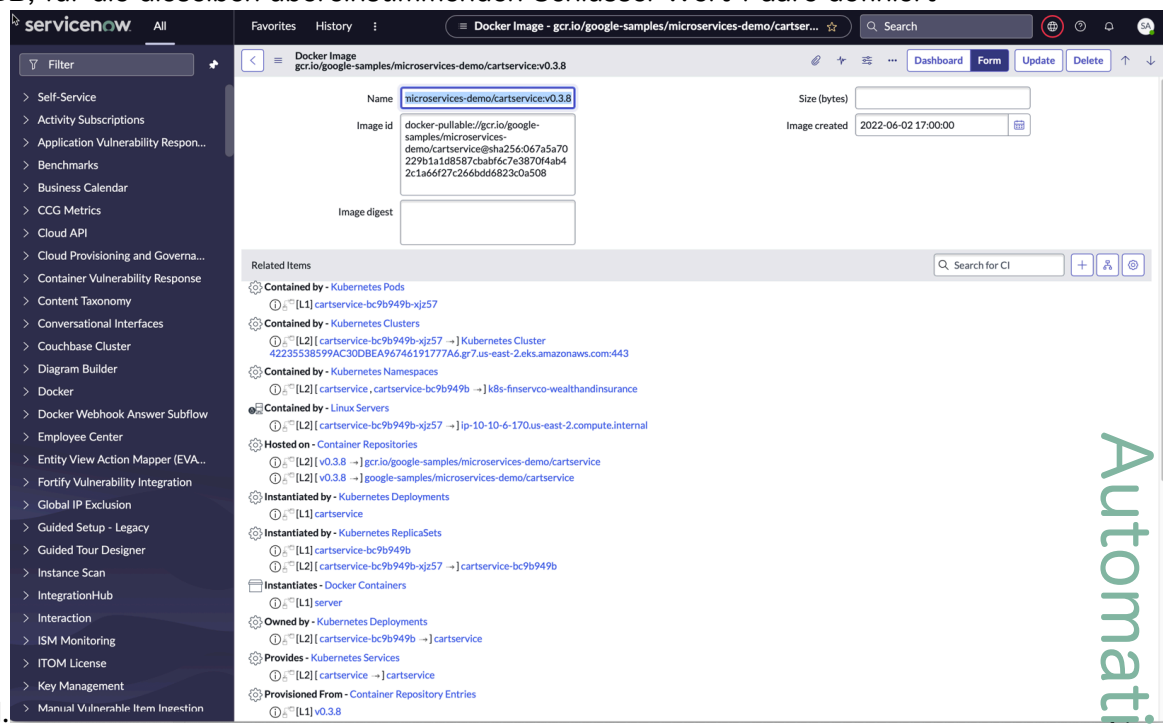
Wenn Kubernetes-Pods oder -Entitäten mit Schlüsselwerten oder Bezeichnungen veröffentlicht werden, die den Schlüsselwerten entsprechen, die in einem „Tag-basierten Service“ in ServiceNowdefiniert sind, stellt Container Vulnerability Response automatisch die Beziehung zwischen einem Docker-Image und dem betroffenen Anwendungsservice her und verwendet den Relevanz dieses Anwendungsservice bei der Risikoberechnung.

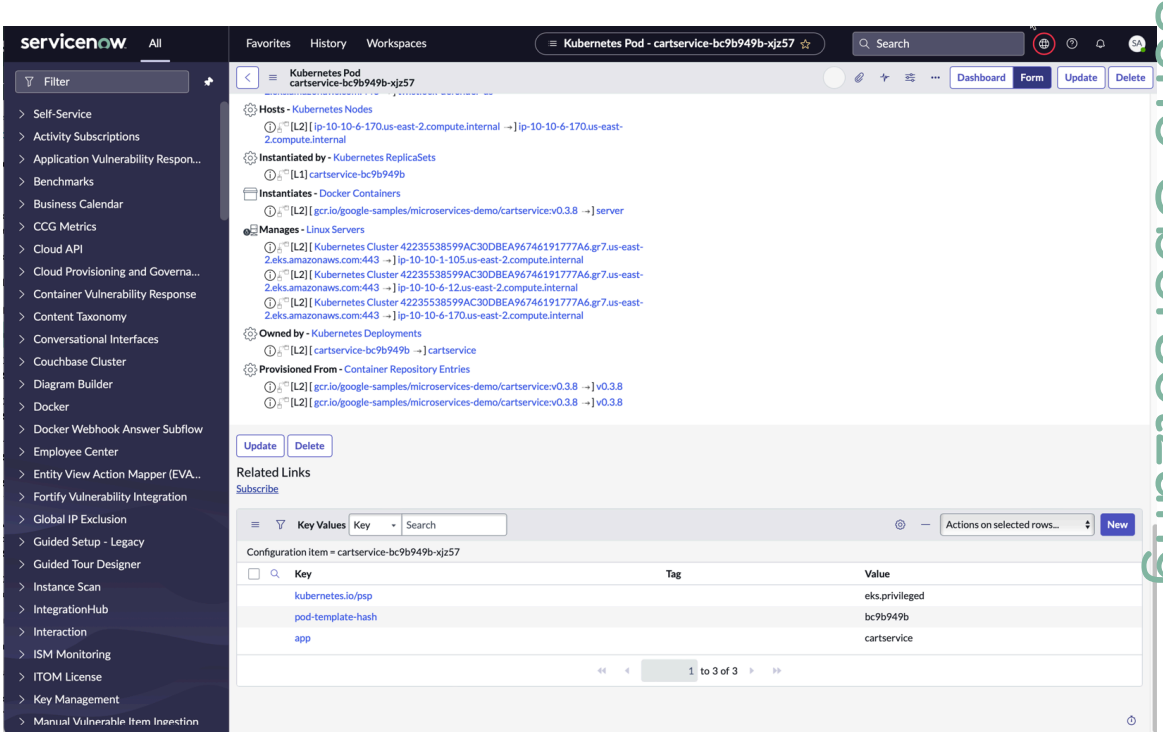
Der Flow sieht wie folgt aus:

1. Container Vulnerability Response importiert Schwachstellendaten aus dem Containersicherheitsprodukt.
2. Für jedes angreifbare Container-Element füllt Container Vulnerability Response das Docker-Image aus CMDB, das die Schwachstelle aufweist.
3. Container Vulnerability Response prüft dann die Docker-Image-Bezeichnungen oder die Bezeichnungen/Schlüssel-Werte, die mit Kubernetes-Pods veröffentlicht wurden, in denen dieses Image bereitgestellt wird. Dieses Image ist in CMDB verfügbar, wenn die Kubernetes-Discovery ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Container Vulnerability Response sucht dann nach „Tag-basierten Services“ in CMDB, für die dieselben übereinstimmenden Schlüssel-Wert-Paare definiert sind.

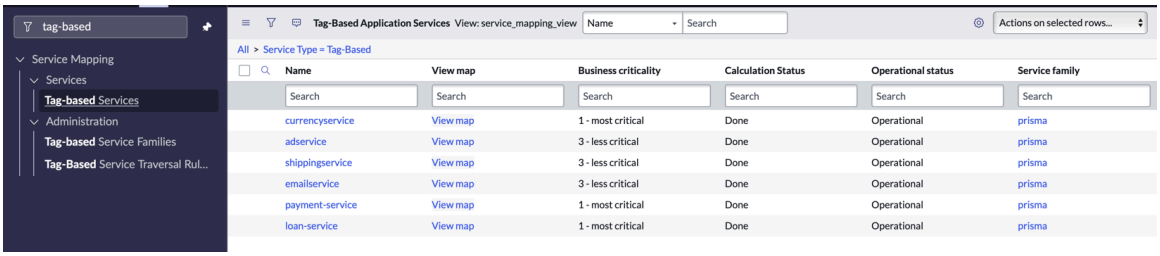


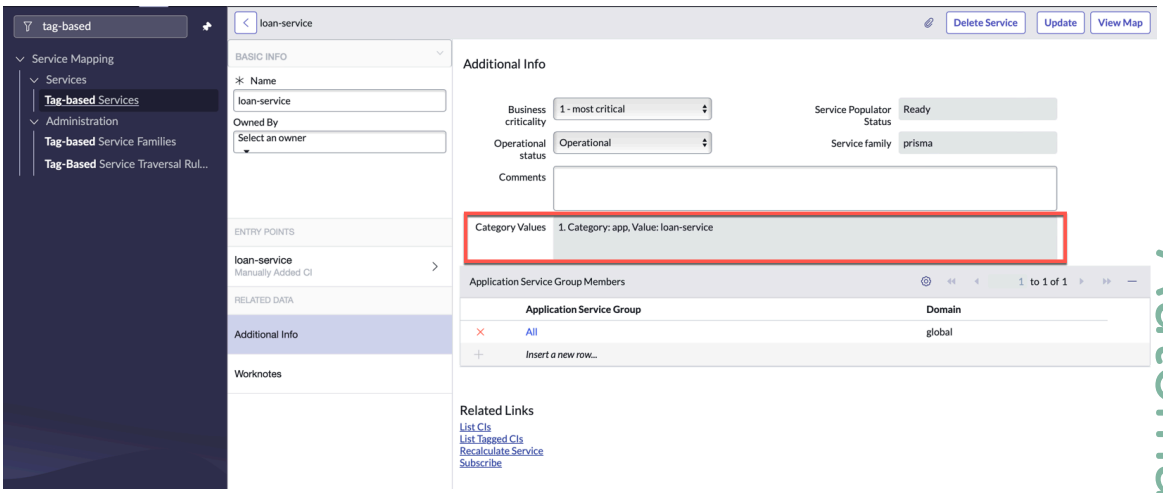


5. Container Vulnerability Response verwendet die „Geschäftskritikalität“ des übereinstimmenden „Tag-basierten Service“ (falls vorhanden), um das Risiko eines angreifbaren Containerelements zu berechnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

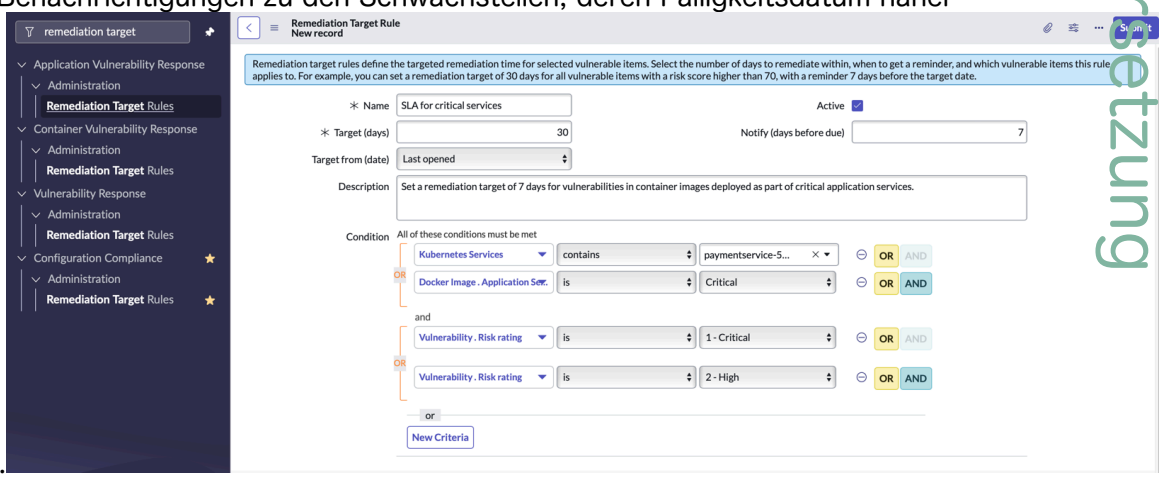




Nachverfolgung von Schwachstellen

Korrekturziele festlegen

ServiceNow ermöglicht es Schwachstellenmanagern, „Korrekturzielregeln“ zu definieren, um Servicelevel-Vereinbarungen (SLAs) zur Behebung von in Container-Images gefundenen Schwachstellen definieren zu können. Das Zieldatum für die Korrektur kann basierend auf einer Bedingung/einem Kriterium für Image-Metadaten oder Schwachstelleninformationen definiert werden. Korrekturbesitzer erhalten E-Mail-Benachrichtigungen zu den Schwachstellen, deren Fälligkeitsdatum näher rückt.



Identifizieren behobener Schwachstellen

Im Gegensatz zu Host-Schwachstellen, die durch Anwenden eines Patches auf einem Host behoben werden können, können Container-Schwachstellen nicht gepatcht werden. Neue Versionen von Container-Images müssen erstellt und bereitgestellt werden, um die älteren Versionen zu ersetzen. Die neuen Versionen haben im Vergleich zu den vorherigen Versionen einen anderen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichner (Image-ID), wodurch es schwierig ist, nachzuverfolgen, welche Schwachstellen bereits behoben wurden.

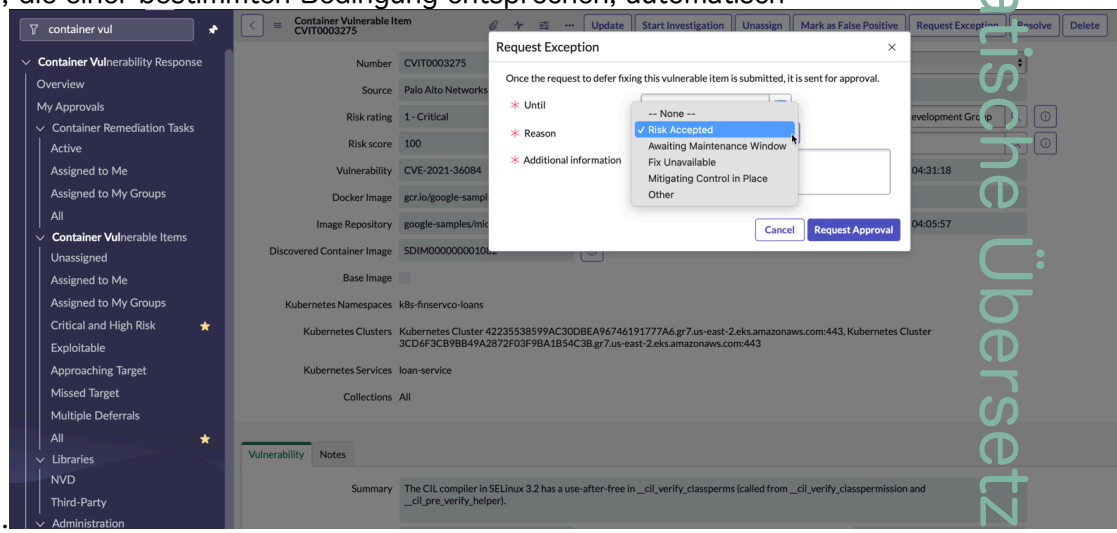
ServiceNow identifiziert Schwachstellen, die in früheren Versionen der Container-Images gemeldet, aber in der aktuellen Version des Images behoben wurden, und versetzt diese Schwachstellen automatisch in den Status „Geschlossen/Behoben“, sodass Sicherheitsteams immer einen genauen Einblick in die aktuelle Risikosituation haben.

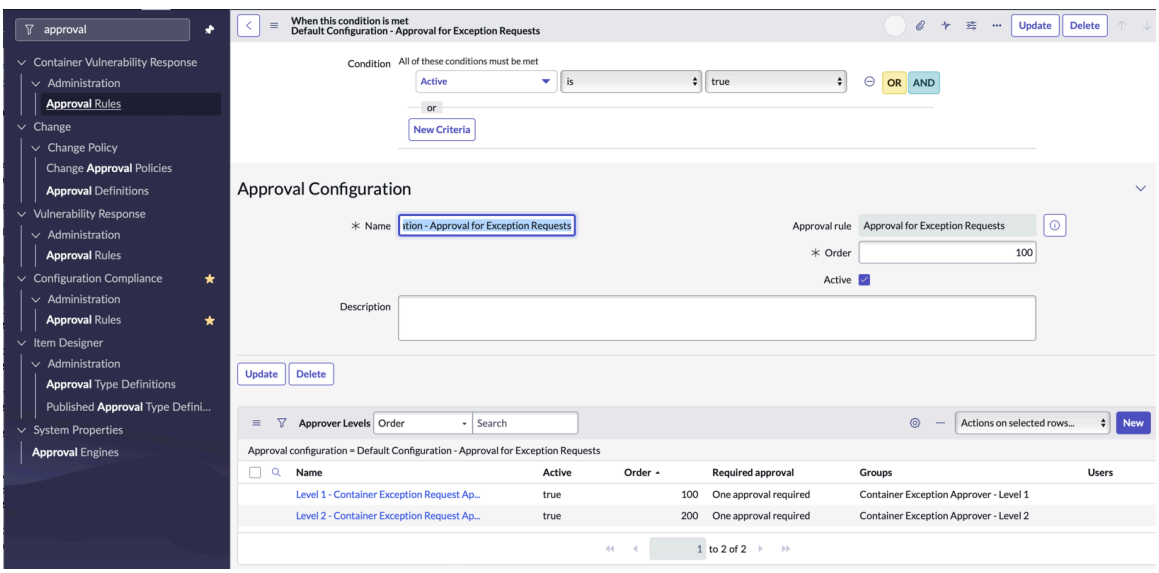
Ausnahmen verwalten

Anwendungsteams oder für die Nachbesserung verantwortliche Personen müssen möglicherweise aus den folgenden Gründen eine Ausnahme anfordern.

- Eine Ausgleichssteuerung ist bereits vorhanden
- Risiko akzeptiert
- Warten auf Wartungsfenster, um Korrektur zu veröffentlichen.

ServiceNow Mit können Sicherheitsadministratoren mehrere Ebenen von Genehmigern für Ausnahmeanforderungen definieren. Sie können auch automatische Ausnahmeregeln definieren, die verwendet werden können, um Schwachstellen, die einer bestimmten Bedingung entsprechen, automatisch zurückzustellen.





Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neuigkeiten

Weitere Informationen zu den Neuerungen und Änderungen in Yokohamafinden Sie in den Versionshinweisen zu Yokohama.

Erste Schritte

- Eine Übersicht über Security Operations in Ihrer Instanz Now Platform finden Sie unter Security Operations verstehen.
- Informationen zu allen Security Operations -Anwendungen, die von ServiceNow Storeheruntergeladen werden können, finden Sie unter Security Operations und ServiceNow Store.

Container Vulnerability Response erkunden

Die Anwendung Container Vulnerability Response importiert angreifbare Container-Elemente (CVITs). Gemäß den Regeln können Sie mit dieser Funktion die Container-Schwachstellen beheben. Container Vulnerability Response ist über ein separates Abonnement verfügbar.

Im Gegensatz zu herkömmlichen Anwendungen packen Container den gesamten Anwendungsquellcode zusammen mit ihren Abhängigkeiten in eine Binärdatei, die als Containerimage bezeichnet wird. Das Image wird in einer Registrierung veröffentlicht, um eine Option zum Ausführen des Image als Anwendung oder Containerinstanz auf einer beliebigen Plattform bereitzustellen. Ein Container-Lebenszyklus vor der Bereitstellung wird in folgenden Phasen unterteilt:

1. Containerimage zusammenstellen: Das Containerimage wird erstellt, und es wird auf einen Quellcode oder eine abhängige Bibliothek verwiesen.
2. Containerimage erstellen
3. Containerimage veröffentlichen: Die Container-Image-Datei wird in einer Registrierung veröffentlicht. Jedes Bild hat eine eigene eindeutige ID, die auf dem Inhalt des Bilds basiert. Diese Bilder werden im Modus nach der Bereitstellung aus der Registrierung in die Laufzeitumgebung abgerufen. Die Bilder werden dann als Containerinstanzen auf dem Host in der Produktionsumgebung ausgeführt.

Containerbilder werden gescannt

Ein Containerimage kann vor oder nach der Bereitstellung auf Schwachstellen gescannt werden. Wenn Containerbilder während der Phase vor der Bereitstellung gescannt werden, erhalten Sie möglicherweise viele Schwachstellenwarnungen, die möglicherweise nicht Ihre sofortige Aufmerksamkeit erfordern. Das Scannen auf Schwachstellen während der Phase nach der Bereitstellung bietet jedoch noch größere Vorteile, z. B.:

- Transparenz der mit den bereitgestellten Anwendungen verbundenen Risiken.
- Bereitstellung einer fokussierten Ansicht nur für die Bilder in der Produktionsumgebung.
- Identifiziert und priorisiert die Schwachstellen, auf die sofort reagiert werden muss.
- Gruppierung und Zuweisung von Schwachstellen basierend auf den Metadaten des Image. Beispielsweise können ein Image-Repository, eine Image-Bezeichnung und andere Attribute, die sich auf das Containerimage beziehen, für Gruppierungs- und Zuweisungsregeln verwendet werden.

Jedes Containerimage weist die folgenden Schlüsselkomponenten auf:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Container- oder Image-Repository: Stellt das Docker-Image mit einem bestimmten Repository oder Namen dar. Hostet alle Versionen des -Images.
- Docker-Image: Stellt eine bestimmte Version des Build-Docker-Image dar.
- Docker-Container: Stellt eine laufende Instanz des Docker-Image dar. Jede Version hat eine eindeutige ID, und in der Produktionsumgebung werden mehrere Instanzen der Container ausgeführt.

Container Vulnerability Response Module

Das Modul Container Vulnerability Response enthält Details zu folgenden Themen:

Angreifbare Container-Elemente

Die angreifbaren Elemente in Containern (Container Vulnerable Items, CVITs) werden gruppiert und basierend auf Zuweisung, Relevanz, Ausnutzbarkeit und Nachbesserungsstatus aufgelistet.

Bibliotheken

Erhalten Sie Zugriff auf die National Vulnerability Database (NVD) und Bibliotheken von Drittparteien. Während die NVD-Bibliothek Informationen bietet, die auf die ID des angreifbaren Elements beschränkt sind, bietet die Drittanbieterbibliothek die meisten Details zu einem angreifbaren Element. Der NVD-Bildschirm wird nur gefüllt, wenn die NVD-Integration ausgelöst wird.

Administration

Das -Modul „Administration“ enthält Informationen zu Zuweisungsregeln für angreifbare Elemente, zu Korrekturzielregeln und zu Container-Schwachstellen-Integrationen. Darüber hinaus können Sie auch die Dauer konfigurieren, nach der ein angreifbares Element automatisch geschlossen werden soll. Im Abschnitt VI-Granularität konfigurieren können Sie die Granularität von CVITs konfigurieren, indem Sie die Tastenkombinationen angeben. Standardmäßig wird eine CVIT für eine Kombination aus einem Image-Repository, einem Image-Tag und einer Schwachstelle erstellt. Sie können dem Schlüssel zusätzliche Komponenten hinzufügen, um die Granularität zu erhöhen. Sie können beispielsweise eine CVIT für eine Kombination aus Image-Repository, Image-Tag, Schwachstelle und Cluster erstellen.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Container Vulnerability Response v2.1 Container Vulnerability Response v2.06 Container Vulnerability Response v2.0.4	Versionshinweise zu Container Vulnerability Response Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen .

Container Vulnerability Response Status von Korrekturaufgaben und angreifbaren Containerelementen

Mit der Anwendung Container Vulnerability Response können Sie das Statusmodell verwenden, um den Status einer Korrekturaufgabe jederzeit anzuzeigen. Wenn Sie wissen, wie die einzelnen Status miteinander in Beziehung stehen und sich gegenseitig beeinflussen, können Sie bestimmen, wann und wie Ihre angreifbaren Elemente in Containern (CVITs) korrigiert werden müssen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Korrekturaufgaben

Komplexe Anwendungsfälle können manchmal dazu führen, dass ein angreifbares Container-Element einen anderen Status aufweist als seine Korrekturaufgabe. Wenn Sie wissen, wie Status funktionieren, können Sie dieses Verhalten erklären und können bei der Erstellung von Korrekturaufgaben und beim Erstellen oder Bearbeiten von Regeln für Korrekturaufgaben helfen.

Korrekturaufgaben haben viele mögliche Status, wie im folgenden Diagramm dargestellt.

Status-Flow von Container Vulnerability Response

Hinweis:

- Angreifbare Container-Elemente können nicht manuell geschlossen werden.
- Jedes Aufgabenformular enthält die Schaltflächen **Verfolgen** und **Aktualisieren**, die bei ServiceNow -Aufgaben standardmäßig verwendet werden.

Container Vulnerability Response konfigurieren

Bevor Sie Container Vulnerability Response in Ihrer Instanz Now Platform ausführen, müssen Sie es konfigurieren.

Vulnerability Response und Configuration Compliance für Container installieren

Bevor Sie die Anwendung Vulnerability Response und Configuration Compliance für Container in Ihrer Instanz Now Platform ausführen, müssen Sie sich die -Berechtigung besorgen und die Anwendung von ServiceNow Storeherunterladen. Installieren Sie die Anwendung in Ihrer Instanz Now Platform, und führen Sie im Setup-Assistenten einige Installationsschritte aus.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:

Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Setupaufgaben	Beschreibung
Vergewissern Sie sich, dass die Anwendung installiert und aktiviert ist.	Um sicherzustellen, dass aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren.
Vergewissern Sie sich, dass Ihrer Instanz die erforderlichen Rollen ServiceNow zugewiesen sind.	Für die Installation von ist die Administratorrolle erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Wenn dies noch nicht geschehen ist, weist der Systemadministrator [admin] auch die Rollen „Schwachstellen-Administrator“, „sn_vul.vulnerability_admin“ oder „sn_vul.admin“ (veraltet)] zu.

Erforderliche Rolle: Administrator

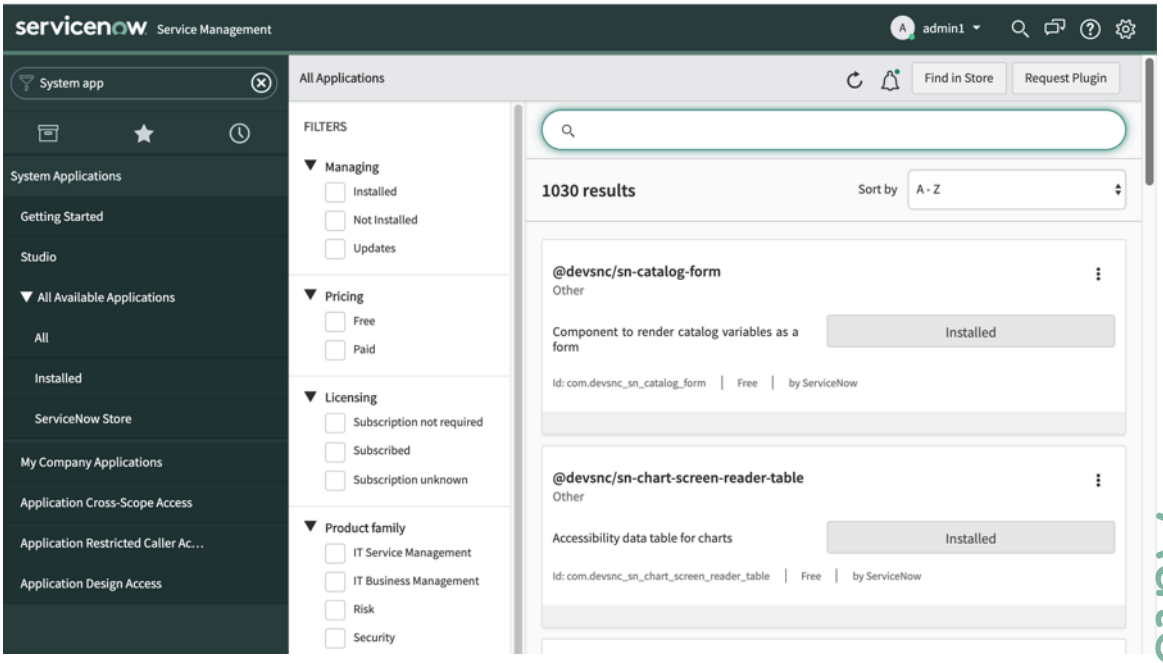
Prozedur

1. Um die Berechtigung zu erhalten und die Anwendung Vulnerability Response und Configuration Compliance für Container herunterzuladen, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite **auf Anmelden**.
3. Geben Sie in der Suchleiste Vulnerability Response und Configuration Compliance für Containerein.
4. Klicken Sie unter Apps and Lösungen auf die Kachel Vulnerability Response und Configuration Compliance für Container.

5. Klicken Sie auf **Installation anfordern**.
6. Melden Sie sich bei der Now Platform-Instanz an, auf der Sie die Anwendung Vulnerability Response und Configuration Compliance für Container installieren möchten.
7. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Vulnerability Response und Configuration Compliance für Container, wählen Sie eine Version aus der Liste aus, und klicken Sie auf **Installieren**.
   Das Dialogfeld „Anwendungsinstallation“ wird angezeigt. Alle installierten Abhängigkeiten werden angezeigt.
9. Klicken Sie auf **Schließen**.

Definieren Sie E-Mail-Benachrichtigungen Container Vulnerability Response .

Richten Sie E-Mail-Benachrichtigungen ein, um nützliche Informationen über wichtige Updates und Aktivitäten wie die Genehmigung und Ablehnung von falsch positiven Anforderungen zu teilen. Beim Erstellen einer E-Mail-Benachrichtigung müssen Sie angeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **E-Mail-Vorlagen**.
2. Wählen Sie **Neu**.

   Ausführliche Anweisungen zum Erstellen von E-Mail-Benachrichtigungen finden Sie unter Create an email notification .

Ergebnisse

Ab v21.0 von Vulnerability Responsewerden Empfänger, die auf die Links in einer E-Mail-Benachrichtigung klicken, je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

- Links werden in Vulnerability Manager Workspace für Benutzer mit den Rollen sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admingeöffnet.
- Links werden in IT Remediation Workspace für Benutzer mit den Rollen sn_vul_container.remediation_ownergeöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Empfänger über keine der genannten Rollen verfügt, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Erstellen oder bearbeiten Sie Benachrichtigungen für Korrekturziele

Schwachstellenadministratoren können die Korrekturzielbenachrichtigung bearbeiten oder neue hinzufügen und angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**.
2. Wählen Sie den Benachrichtigungsdatensatz des Korrekturziels oder **Neu**aus.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie **Benachrichtigungsvorschau** aus, um die Nachricht anzuzeigen.

Ergebnisse
Ab v21.0 von Vulnerability Responsewerden Empfänger, die auf die Links in einer E-Mail-Benachrichtigung klicken, je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

- Im Vulnerability Manager Workspace werden Links für Benutzer mit den Rollen sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admingeöffnet.
- Links werden in IT Remediation Workspace für Benutzer mit den Rollen sn_vul_container.remediation_ownergeöffnet.

Wenn der Empfänger über keine der genannten Rollen verfügt, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Konfigurieren Sie die Ausnahmeverwaltung für Container Vulnerability Response

Begrenzen Sie die Dauer einer angeforderten Ausnahme, und fügen Sie der Ausnahme oder der falsch positiven Anforderung mithilfe des Moduls Container Vulnerability Responseeinen Fragebogen hinzu . Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Container Vulnerability Response angefordert. Sie können auch mit der -Integration GRC: Richtlinien- und Compliance-Management eine Ausnahme anfordern.

Vorbereitungen
Erforderliche Rolle: sn_vul_container.manage_exception_configuration

Warum und wann dieser Vorgang ausgeführt wird
Wenn Container Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Richtlinien- und Compliance-Management installiert ist, GRC: Richtlinien- und Compliance-Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder falsch positive Anforderung ausgelöst hat. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen. .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für das Anfordern der Ausnahme zu verstehen.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular **„Ausnahmeverwaltungskonfiguration“** aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option in der Liste **Ausnahmen verwalten mit** auswählen. Sie können entweder Vulnerability Response oder GRC: Richtlinien- und Compliance-Managementauswählen.
3. Wenn Sie die Option Vulnerability Response ausgewählt haben, geben Sie die folgenden Informationen ein:

Vulnerability Response Felder

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Zeigt den von Ihnen ausgewählten Fragebogen zum Anfordern einer Ausnahme an. Der Ausnahmefragebogen wird standardmäßig angezeigt.

Hinweis:
Wenn Sie GRC: Richtlinien- und Compliance-Managementauswählen, werden die Felder Dauer und Einheit ausgeblendet, da Governance, Risk und Compliance diesen Flow verarbeitet.

4. Wählen Sie **Speichern**.

Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung

Verwenden Sie ab Vulnerability Response v15.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung, Ausnahmeregeln und die Verwaltung falsch positiver Ergebnisse zu genehmigen. Wenn Sie Vulnerability Response (VR) zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Container-Elemente
- Ausnahmeregel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Falsch positiv für Korrekturaufgaben
- Falsch positiv für angreifbare Container-Elemente

Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.
Anwendung	Der Standardwert ist Vulnerability Response.
Regeltyp	Gibt den Regeltyp an. Beispiele: Ausnahmeverwaltung, falsch positive Meldung oder Ausnahmeregel.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurze Beschreibung der Genehmigungsregeln.
Genehmigungsablaufy (Tage) Ab v2.5 von Container Vulnerability Response	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.
Genehmiger benachrichtigen (Tage) Ab v2.5 von Container Vulnerability Response	Datum, nach dem der Genehmiger benachrichtigt wird, um Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel.

Hinweis:
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für die Ausnahmeverwaltung.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die für verschiedene Konfigurationselemente gefunden wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schnellstarttests für Container Vulnerability Response

Überprüfen Sie, ob Container Vulnerability Response immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwickeln einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demo-Accounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird. Unter Führen Sie die Automated Test Framework-Test-Suite (ATF) für aus Vulnerability Response finden Sie weitere Informationen zum Einrichten und Ausführen der Test-Suite für Container Vulnerability Response.

Container Vulnerability Response-Schnellstarttests erfordern die Aktivierung der Anwendung Container Vulnerability Response (sn_vul_container).

Container Vulnerability Response-Tests

Test	Beschreibung	Release-Version
CVR: Zuweisungsregeln	Ermittelt, ob angreifbare Elemente in Containern mit einem Mustersatz von Zuweisungsregeln zur Korrektur erfolgreich automatisch einer Zuweisungsgruppe zugewiesen werden können.	Vancouver
CVR: Ausnahmeregel	Testet Ausnahmeregeln.	Vancouver
CVR: Flow „Als falsch positiv markieren“	Testet, ob der Flow „Als falsch positiv markieren“ für das angreifbare Container-Element funktioniert.	Vancouver
CVR: Korrekturzielregeln	Erstellt eine Fehlerkorrektur-Zielregel.	Vancouver
CVR: Flow „Ausnahmeanforderung“	Testet, ob der Flow „Ausnahmeanforderung“ wie erwartet funktioniert.	Vancouver
CVR: Schwachstellen-Rechner	Testen Sie die Schwachstellen-Rechner des Containers.	Vancouver

Zugehörige Informationen

Schnellstarttests

Führen Sie die Automated Test Framework-Test-Suite (ATF) für aus Container Vulnerability Response

Führen Sie die Automated Test Framework-Test-Suite (ATF) aus, nachdem Sie die Anwendung Container Vulnerability Response installiert oder aktualisiert haben.

Vorbereitungen

Bestätigen Sie eine erfolgreiche Installation und dass Ihre Instanz ordnungsgemäß funktioniert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demo-Accounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird.

- Um den Test zu aktivieren, gehen Sie wie folgt vor:
  1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Administration** > **Eigenschaften**.
  2. Wenn die Option nicht ausgewählt ist, aktivieren Sie das Kontrollkästchen **Ausführung von Test-/Test-Suites aktivieren**.
  3. Klicken Sie auf **Speichern**.
  4. Wenn der Bereich im Header nicht auf **Container Vulnerability Response** festgelegt oder der Bereich nicht im Header angezeigt wird, klicken Sie auf das Einstellungssymbol.
  5. Klicken Sie im Fenster „Systemeinstellungen“ auf **Entwickler**.
  6. Wenn die Option nicht ausgewählt ist, klicken Sie auf **Anwendungsauswahl in Header anzeigen**, und schließen Sie das Fenster.
  7. Klicken Sie in der Liste, die neben Systemadministratorangezeigt wird, für das Feld **Container Vulnerability Response**.

Erforderliche Rolle: admin oder atf_test_admin

Prozedur

1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Tests**.
2. Suchen Sie in der Paketliste nach **Vulnerability Response und Configuration Compliance für Container**.
3. Wählen Sie einen Test aus, um den Datensatz zu öffnen.
4. Aktivieren Sie im geöffneten Datensatz das Kontrollkästchen **Aktiv**.
5. Wählen Sie in der zugehörigen Liste „Testschritte“ in der Spalte Aktiv die Option true aus.
6. Klicken Sie auf **Aktualisieren**.
7. Öffnen Sie den Test erneut, und klicken Sie **auf Ausführung von Tests und Test-Suite hier aktivieren**.
8. Aktivieren Sie Test-/Test-Suite-Eigenschaften und Test-Debugging-Eigenschaften.
9. Klicken Sie auf **Speichern**.
10. Wenn die Schaltfläche **Test ausführen** nicht angezeigt wird, aktualisieren Sie den Bildschirm, öffnen Sie den Datensatz erneut, und klicken Sie auf **Test ausführen**, um den Test zu starten.
    Nach einigen Minuten zeigt das Dialogfeld Run Test (Test ausführen) an, dass der Test erfolgreich war.
    Klicken Sie **auf Zu Ergebnis wechseln,** um weitere Informationen zu erhalten.

Nächste Maßnahme

Herzlichen Glückwunsch! Sie können mit der Konfiguration von Container Vulnerability Responsefortfahren.

Weitere Informationen zu automatisierten Tests für Container Vulnerability Response sowie zu automatisierten Tests, Test-Suites und zum Erstellen automatisierter Tests finden Sie unter Automated Test Framework (ATF) .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration von Container Vulnerability Response mit anderen Anwendungen

Erweitern Sie die Fähigkeiten von Container Vulnerability Response durch die Integration mit anderen -Anwendungen.

Container Vulnerability Response ist in Containersicherheitsprodukte integriert, um Schwachstellendaten für die Images abzurufen, die zur Laufzeit bereitgestellt werden. Anschließend werden die Schwachstellendaten mit kontextbezogenen Laufzeitinformationen wie Hosts, Kubernetes-Clustern, Services und Namespaces angereichert, in denen diese Containerbilder bereitgestellt werden. Mit der Kubernetes-Discovery von ServiceNow können Sie die aus Schwachstellen erstellten Verweise auf die relevanten Kubernetes-Entitäten in Ihrem Configuration Management Database (CMDB)anzeigen. Zusätzlich zur Anreicherung von Metadaten bietet ServiceNow ein umfassendes Dashboard zur Berichterstellung, das Einblicke in Schwachstellen- und Korrekturtrends gewährt.

Container Vulnerability Response bietet Integrationen für die folgenden Anwendungen:

- Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Integration
- Integration von Atlassian Jira mit Vulnerability Response

Wichtig:
Im Arbeitsbereich des Schwachstellenmanagers können Sie ein Agile-Problem manuell mit der Listen- und Formularaktion erstellen, um die Nachbesserung von CVITs und RTs nachzuverfolgen.

Zusätzliche Hinweise zu Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 2.1.2 von Container Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Integration

Mit der Prisma-Cloud-Computing-Integration können Sie Container-Images scannen, um Schwachstellen zu erkennen.

Ab Version 23.0 von Vulnerability Responsekönnen Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in der Anwendung Container Vulnerability Response verwenden, um Schwachstellen auf den laufenden Hosts zu importieren. Die Prisma-Host-APIs ermöglichen das Abrufen umfassender Schwachstelleninformationen für einen bestimmten Host und liefern außerdem einen Snapshot der Host-Schwachstellen zu einem bestimmten Zeitpunkt. Diese API ermöglicht die regelmäßige Synchronisierung zwischen Prisma- und ServiceNow-Instanz. Da Prisma sowohl als Software-as-a-Service-Lösung (SaaS) als auch als lokale Lösung angeboten wird, ist die Verwendung eines MID Servers erforderlich, um Prisma-APIs aus der ServiceNow-Instanz aufzurufen.

Ab Version 16.1 von Vulnerability Responsekönnen Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in der Anwendung Container Vulnerability Response verwenden, um Container-Image-Schwachstellendaten für bereitgestellte Container zu importieren. Anschließend können Sie in den Dashboards Vulnerability Response Berichte zu Schwachstellen und angreifbaren Elementen anzeigen. Diese Schwachstellen können dann priorisiert und behoben werden.

Wenn sich das Produkt Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID-Server verwenden. Weitere Informationen finden Sie unter Systemanforderungen für MID-Server .

Integrationen anzeigen

Sie können die Integrationen anzeigen, die Teil von Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Computesind. Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Integrationen**.

Die folgenden Integrationen sind verfügbar.

Ausführungssequenz	Zeitplan	Integration	Beschreibung
1	Täglich	Prisma-Cloud-Computing – Basis-Image-Integration	Ruft die Schwachstellen für Basis-Images von der Prisma-API ab und meldet die Schwachstellen der Basis-Images separat. Außerdem werden Image-Ergebnisse und angreifbare Elemente erstellt, die auf die Basis-Images verweisen.
2	Täglich	Prisma-Cloud-Computing-Schwachstellenintegration	Ruft Container-Schwachstellen ab. Erstellt Ergebnisse, angreifbare Container-Elemente (CVITs) und erkannte Container-Images.
3	Bei Bedarf	Prisma-Cloud-Computing – Containeranzahl-Integration	Ruft die Containeranzahl für jedes Nicht-Basis-Image ab.
4	Täglich	Prisma-Cloud-Computing-Registrierungsintegration	Ruft statische Bildergebnisse ab, die beim Prisma-Registrierungsscan erhalten wurden, und erfasst sie in Container Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

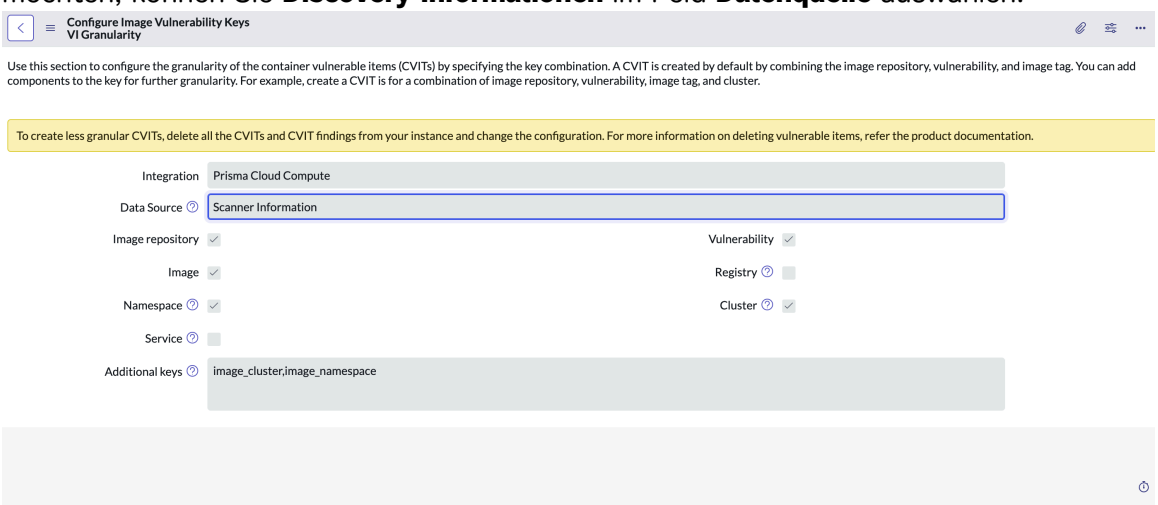
Basis-Image-Konfiguration in Prisma

In der Prisma-Konsole können Sie die Registrierung und dann die Basis-Images aus diesen Registrierungen konfigurieren. Wenn im Basisimage eine Schwachstelle vorhanden ist und Sie die Prisma-Cloud-Computing-Basisimage-Integration ausführen, wird das Kontrollkästchen **Basisimage** aktiviert, um anzuzeigen, dass die Schwachstellen im Basisimage vorhanden sind.

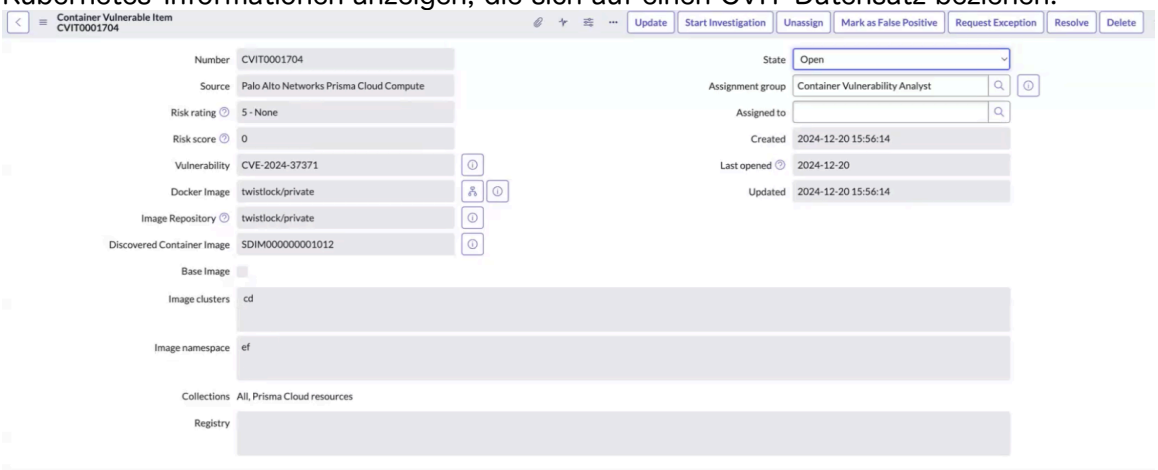
Konfigurieren Sie die CVR-basierte VI-Granularität

Um die Granularität von CVITs zu konfigurieren, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **CVS-basierte-VI-Granularität konfigurieren** und geben Sie die Tastenkombinationen an. Standardmäßig wird eine CVIT für eine Kombination aus Image-Repository, Image und Schwachstelle erstellt. Sie können dem Schlüssel zusätzliche Komponenten hinzufügen, um die Granularität zu erhöhen. Sie können beispielsweise eine CVIT für eine Kombination aus Image-Repository, Image, Schwachstelle und Cluster erstellen.

Ab v2.12.1 von Container Vulnerability Responsekönnen Sie die Granularität von angreifbaren Elementen in Containern (Container Vulnerable Items, CVITs) auch mithilfe von Registrierungsinformationen und Datenquellen konfigurieren. Der Namespace und die Clusterinformationen werden sowohl vom Scanner als auch von Discoveryempfangen. Wenn Sie diese Informationen nur von Discoveryerhalten möchten, können Sie **Discovery-Informationen** im Feld **Datenquelle** auswählen.



Abhängig von der ausgewählten Datenquelle können Sie entweder Bild- oder Kubernetes-Informationen anzeigen, die sich auf einen CVIT-Datensatz beziehen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn **Scannerinformationen** ausgewählt sind, zeigt der CVIT-Datensatz die Felder **Image-Cluster** und **Image-Namespace** an.

Wenn **Discovery-Informationen** ausgewählt sind, zeigt der CVIT-Datensatz **Kubernetes-Cluster-** und **Kubernetes-Namespace-** Felder an.

Prisma-Integrations Prozess

Wenn Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ausgeführt wird, wird geprüft, ob in der Tabelle der National Vulnerability Database (NVD) ein Common Vulnerability and Exposure (CVE) vorhanden ist. Wenn sie bereits vorhanden ist, werden die vorhandenen Informationen verwendet. Wenn das CVE jedoch nicht gefunden wird, werden in der NVD-Tabelle Platzhalterdatensätze generiert. Beim Erstellen dieser Platzhalter-NVD-Datensätze werden zunächst nur das CVE und sein Name ausgefüllt. Andere Details werden nicht mit der Annahme ausgefüllt, dass die NVD-Integration diese Details später ausfüllt. Wenn der Parameter der Integrationsinstanz *update_nvd* auf true festgelegt ist, werden die Platzhalter-NVD-Datensätze aktualisiert. Standardmäßig ist der Instanzparameter auf „falsch“ festgelegt. Zumindest bis die NVD-Integration ausgeführt wird und diese Details ausfüllt, ist jedoch ein gewisses Verständnis des CVE erforderlich, z. B. sein Schweregrad oder andere Details zum Problem. Um diese Anforderung zu erfüllen, werden die Felder **Exploit vorhanden** und **Korrekturhinweise** mit den aus Prisma erhaltenen Details ausgefüllt. Darüber hinaus ist diese Konfiguration anpassbar, sodass Sie beliebige andere Felder angeben können, die Sie im NVD-Eintrag basierend auf den von Prisma bereitgestellten Informationen ausfüllen möchten.

Vorbereitung auf das Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Sie können sich auf den Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute vorbereiten, indem Sie Setupaufgaben ausführen.

Bevor Sie beginnen

Zur Installation und Konfiguration der Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute können Sie die folgende Prüfliste drucken. Stellen Sie sicher, dass die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und die Schwachstellendaten in Ihre Instanz Now Platform® importieren.

Prüfliste für die Vorbereitung der Integration

Aufgabe	Beschreibung
☐	Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen: • API-Basis-URL • Anwendername und Passwort. Diese Anmeldeinformationen werden verwendet, um die Schwachstellen aus der Prisma-Cloud-Computing-Integration abzurufen. Weitere Informationen finden Sie unter https://pan.dev/compute/api/ **Hinweis:** MID-Server ist optional.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
	Die für die Prisma-Cloud-Computing-Integration verwendeten Anwenderanmeldeinformationen benötigen die Berechtigung zum Überwachen der Images. Siehe folgenden Code: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Wenn die Anwendung Vulnerability Response [] noch nicht installiert und aktiviert ist, installieren Sie die Anwendung , bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher.
☐	Rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in Ihrer Instanz Now Platform® herunter.
☐	Schätzen Sie die Anzahl der zu importierenden angreifbaren Elemente. Vergewissern Sie sich, dass Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie voraussichtlich importieren werden. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support ServiceNow von .
☐	Stellen Sie sicher, dass Sie über die folgenden Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und die angreifbaren Elemente zu korrigieren: **Administrator** Installieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Wenn dies nicht zugewiesen ist, weist der Administrator den Container-Schwachstellen-Administrator (sn_vul_container.vulnerability_admin) und andere Rollen zu. **sn_vul_container.vulnerability_admin** Schließt die Konfiguration der Prisma-Cloud-Computing-Integration ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Container Vulnerability Response (CVR) und ihre Datensätze. Dieser Administrator konfiguriert Integrationen und Regeln in Container Vulnerability Response. **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben sn_vul.read_all und sn_vul_container.read_all. **Besitzergruppe für Container-Korrektur**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
	Standardmäßig ist die Gruppe „Besitzer der Container-Korrektur“ verfügbar. Anwender, die dieser Gruppe zugewiesen sind, erben sn_vul_container.remediation_owner. Der Container-Korrekturbesitzer behebt Container-Schwachstellen, die ihm oder einer Gruppe, der er angehört, zugewiesen sind. **Schwachstellenanalyst** Benutzer, die der Gruppe der Container-Schwachstellenanalysten zugewiesen sind, erben die Eigenschaft „sn_vul.vulnerability_analyst“. Der Schwachstellenanalyst überwacht die Behebung aller angreifbaren Elemente. Wenn dies noch nicht geschehen ist, können Sie zusätzliche Gruppen erstellen und Benutzer mit dem -Benutzerverwaltungsmodul in Ihrer -Instanz hinzufügen. Weitere Informationen finden Sie unter Benutzergruppen erstellen .
☐	Installieren Sie die Integration Vulnerability Response mit NVD, und führen Sie die Integration der US-Schwachstellendatenbank (National Vulnerability Database Integration) des NIST API – API (nur CVE) aus.

Sie sind bereit für Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ..

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren

Bevor Sie die Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit das Produkt Prisma Cloud Compute ordnungsgemäß in Vulnerability Response und Container Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in der Anwendung ServiceNow Storenach der Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie bei Bedarf die Abschnitte **Weitere Anforderungen** und **Abhängigkeiten**.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Aktualisieren Sie die Felder **Instanzname** und **Grund für die Instanz**, und klicken Sie auf **Instanz validieren**.
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.

Ergebnisse
Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Nächste Maßnahme
Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ..

Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute .

Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Importieren Sie Daten aus Prisma Cloud Compute. Sie können die importierten Daten verwenden, um Schwachstellen für Ihre Docker-Images und Docker-Hosts zu priorisieren und zu beheben.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die E-Mail von ServiceNow, die Sie zur Integration erhalten haben.
2. Melden Sie sich bei Ihrer -Instanz als Administrator an.
3. Befolgen Sie die Anweisungen in der E-Mail, um Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Computeabzurufen.
4. Navigieren zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**.
   Füllen Sie die Felder im Formular „Prisma-Cloud-Computing-Konfiguration“ aus. Weitere Informationen finden Sie unter Formular „Prisma-Cloud-Computing-Konfiguration“.
5. Wählen Sie in der Projektliste entweder **Alle Projekte** oder **Bestimmte Projekte** aus, um entweder alle Projekte oder ausgewählte Projekte zu konfigurieren.
   Wenn Sie **Bestimmte Projekte**auswählen, können Sie die Projekte aus der Liste Verfügbar auswählen.
6. Schließen Sie die Konfiguration ab, indem Sie entweder **Fertigstellen** oder **Anmeldeinformationen speichern und testen**wählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie ein Projekt konfiguriert haben, wählen Sie **Fertig stellen**aus.
- Wenn Sie kein Projekt konfiguriert haben, wählen Sie **Anmeldeinformationen speichern und testen aus**

7. Zeigen Sie die neu erstellte Instanz an, indem Sie zu navigieren **Prisma-Cloud-Computing-Integration** > **Administration** > **Integrationsinstanzen**.
8. Zeigen Sie die Projekte an, die Sie zuvor konfiguriert haben, indem Sie **Integration Instance Parameters**ausgewählt haben.
9. Führen Sie die neu erstellte Integrationsinstanz aus, um die folgenden Daten zu importieren:
   - Docker-Images: Listet die Docker-Images auf, die mit einer Engine für Identifizierung und Abgleich (Identification and Reconciliation Engine, IRE) erstellt werden. Jedes Docker-Image enthält auch Informationen über die Beziehung zwischen den Repositorys und den installierten Versionen.
   - Erkannte Container-Images: Das Modul „Erkannte Container-Images“ enthält Informationen zur Image-ID, zum Docker-Image und zum Image-Repository. Außerdem werden die Ebeneninformationen gespeichert und dem erkannten Image zugeordnet. Sie können die Projekte und die Containeranzahl auch hier anzeigen. Für ein erkanntes Containerimage können Sie Cloud-Metadaten wie Cloud-Anbieter, Cloud-Region, Cloud-Account-ID und Cloud-Ressourcen-IDs anzeigen.
   - Container-Image-Pakete: Stellt Informationen zu den Paketen bereit, in denen die Schwachstellen vorhanden sind. Die Details des Binärpakets werden auch als kommagetrennter Wert angegeben.
   - Container-Image-Ebenen: In diesem Bildschirm wird der Datensatz für jede Image-Ebene angezeigt.
   - Container-Image-Ergebnisse: In diesem Bildschirm wird die Liste der Ergebnisse zusammen mit Informationen zu den zugehörigen Schwachstellen, der Image-Ebene, dem Docker-Image, dem Image-Repository und dem erkannten Image angezeigt. Derzeit sind die Schwachstelleninformationen auf die ID beschränkt. Zusätzliche Informationen werden ausgefüllt, wenn die Integration der National Vulnerability Database (**NVD**) ausgelöst wird.
   - Angreifbare Container-Elemente: Jedes Ergebnis weist eine entsprechende Schwachstelle auf. Die CVITs werden basierend auf der Granularität weiter erstellt.
10. Konfigurieren Sie die Granularität eines angreifbaren Elements.

    a. Navigieren zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Image-Schwachstellenschlüssel konfigurieren**

    b. Konfigurieren Sie die Granularität der CVITs, indem Sie die erforderlichen Kontrollkästchen aktivieren. Die angreifbaren Elemente werden basierend auf den ausgewählten Schlüsseln während des nächsten Imports erstellt.

    Hinweis:
    Standardmäßig wird eine CVIT für eine Kombination aus Image-Repository, Schwachstelle und Image-Tag erstellt. Sie können dem Schlüssel Komponenten hinzufügen, um die Granularität zu erhöhen. Sie können beispielsweise ein CVIT für eine Kombination aus Image-Repository, Schwachstelle, Image-Tag und Cluster erstellen. Sobald die angreifbaren Elemente oder die Ergebnisse zu angreifbaren Elementen erstellt wurden, können die Kontrollkästchen nicht mehr bearbeitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Container-Schwachstellen beheben

Die Überwachung der Remediation ist ein Prozess, der mit der Überprüfung des Status beginnt und mit dem Schließen von angreifbaren Container-Elementen (Container Vulnerable Items, CVITs) endet. Container Vulnerability Response bietet Tools und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

Container Vulnerability Response Rechnerregeln

Schwachstellen-Rechner automatisieren die Berechnung der Anfangswerte für die Felder in angreifbaren Container-Elementen. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste passende Rechner wird verwendet.

Um Schwachstellen-Rechner anzuzeigen und zu erstellen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**.

Das -Basissystem Container Vulnerability Response enthält zwei Schwachstellen-Rechner, die die Basis-Risikopunktzahl für das angreifbare Container-Element festlegen. Die folgenden Rechnergruppen sind im Basissystem verfügbar:

- Schwachstellenschweregrad: Berechnet die Risikopunktzahl für angreifbare Elemente anhand des normalisierten Schwachstellenschweregrads.
- Standardrisiko-Rechner: Basiert auf der Risikoregel.

Hinweis:
Ab Version 2.10 von Container Vulnerability Response, im Fall von:

- Regel**des Standardrisiko-Rechners** : Wenn sich die Risikopunktzahl für ein angreifbares Element in einem Container ändert, werden die folgenden Details im Abschnitt „Hinweise“ des CVIT dokumentiert:
  - Name der Rechnergruppe
  - Name des Rechners
  - Feldwerte, die eine Gewichtung von mehr als 1 haben, und ihr Beitrag zur Risikopunktzahl.
  - Endgültige Risikopunktzahl
- Risikoregel**für Schwachstellenschweregrad** : Bei jeder Aktualisierung der Risikopunktzahl für einen CVIT wird der Abschnitt **„Hinweise“** mit den folgenden Details aktualisiert:
  - Name der Rechnergruppe
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, werden dem Namen die Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und aktivieren Sie das Kontrollkästchen **Erweiterte Ansicht**. Wählen Sie im Dropdown-Feld **Werttyp** die gewünschte Option aus. Wenn **Vorlage** ausgewählt ist, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** ausgewählt ist, können Sie entweder das vorhandene Skript hinzufügen oder aktualisieren. Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes` hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v2.12.2 von Container Vulnerability Responseist die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes` standardmäßig inaktiv. Wenn Sie die Option aktivieren, können Sie nur dann alle Änderungen im Zusammenhang mit der Risikopunktzahl eines angreifbaren Containerelements im Abschnitt „Arbeitsnotizen“ anzeigen. Darüber hinaus werden die Arbeitsnotizen nur aktualisiert, wenn sich die Risikopunktzahl ändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen wird basierend auf Faktoren wie Schweregrad, Kritikalität, Exploit-Informationen usw. eine Risikopunktzahl und Bewertung zugewiesen. Die Geschäftsregel *`Update Risk Rating from Risk Score`* in der Tabelle der angreifbaren Containerelemente ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Container-Elemente eingetragen. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert waren.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Ab Version 18.0 von Vulnerability Response,

- Die Risikoeinstufungstypen werden in der Basistabelle „Gewichtungen der Risikopunktzahl“ [sn_sec_cmn_risk_scorew_weights] als cvr_risk_rating geliefert. Diese Typen werden als Teil der Business-Regeln oder Skripteinbindungen in jeder Tabelle übergeben, in der die Risikoeinstufung berechnet wird.
- Das Skript wird so geändert, dass Sie die Einträge in der Tabelle „Risikopunktzahlgewichtungen“ für die Berechnung der Risikoeinstufung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, müssen Sie die Bezeichnungen für die neue Risikoeinstufung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Risikopunktzahlgewichtungen“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn ein Configuration Item (CI) von ohne Internetzugriff in mit Internetzugriff geändert wird.
- Wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittparteieinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer Known Exploit Vulnerability (KEV) verknüpft sind.

Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.

Container Vulnerability Response Zuweisungsregeln

Definieren Sie die Kriterien, nach denen angreifbare Elemente in Containern (CVITs) automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Erstellen und Anzeigen von Zuweisungsregeln für angreifbare Container-Elemente. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Zuweisungsregeln**. Wenn Sie eine Zuweisungsregel erstellen, können Sie die Bedingungen festlegen. Wenn diese Bedingungen erfüllt sind, weist die Regel der ausgewählten Benutzergruppe automatisch angreifbare Elemente im Container zu. Nur die erste Zuweisungsregel mit einer übereinstimmenden Bedingung wird für einen Datensatz ausgeführt.

Hinweis:
Angreifbare Container-Elemente, die sich nicht im Status „Offen“ befinden oder manuell zugewiesen wurden, werden immer ausgeschlossen.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Wichtig:
Als Schwachstellenadministrator und -analyst können Sie die aktuellen Zuweisungen für ausgewählte CVITs unter Vulnerability Manager Workspaceabrufen. Diese Methode ist effizienter als das erneute Anwenden der Zuweisungsregeln für alle CVITs in der UI klassisch, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Container Vulnerability Response Korrekturzielregeln

Korrekturzielregeln definieren den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Elements in einem Container (CVIT). Diese Regeln ähneln der Art und Weise, wie SLAs einen Zeitrahmen für die Behebung der Schwachstelle selbst bereitstellen.

Um Korrekturzielregeln für Container-Schwachstellen zu erstellen und anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Korrekturzielregeln**.

Die Korrekturzielregeln definieren die Zielkorrekturzeit für ausgewählte angreifbare Containerelemente (CVITs). Legen Sie eine Frist für die Korrektur der Schwachstelle fest, indem Sie die Anzahl der Tage für die Korrektur auswählen. Legen Sie eine Erinnerung für die Korrektur fest, und legen Sie die angreifbaren Container-Elemente fest, für die die Regel gilt. Sie können ein Korrekturziel für die Tage festlegen, in denen eine Korrektur erforderlich ist, und eine Erinnerung festlegen, bevor das Zieldatum erreicht wird. Weitere Informationen finden Sie unter Vulnerability Response Korrekturzielregeln.

Wichtig:
Als Schwachstellenadministrator und -analyst können Sie das späteste Nachbesserungszieldatum für ausgewählte CVITs unter Vulnerability Manager Workspaceabrufen. Diese Methode ist effizienter als das Ausführen der Korrekturzielregeln für alle CVITs in der UI klassisch, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Ausnahmeverwaltung in Container Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Richtlinie, einen Standard oder eine Leitlinie für das Schwachstellenmanagement oder die Sicherheit nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Containerelement (Container Vulnerable Item, CVIT), das nicht gemäß der Richtlinie behoben werden kann.

Für einige Container-Schwachstellen (CVIT) ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen anerkennen und ihnen zustimmen, wenn die Schwachstelle nicht behoben wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lebenszyklus einer Ausnahme

Definition einer Ausnahme

Eine Ausnahme ist eine Anforderung, die Korrektur einer CVIT oder RT für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Ausnahme wird angefordert

Als Besitzer der Korrektur können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für eine CVIT oder RT beantragen. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wird CVIT oder RT in den Status **„Zurückgestellt“** versetzt.

Eine Ausnahmeanforderung wird genehmigt

CVIT oder RTs, die nicht sofort behoben werden können, werden von Schwachstellenanalysten überprüft, auf Risiken geprüft und zur Zurückstellung genehmigt, bis sie behoben werden können. Das Genehmigen einer Ausnahmeanforderung kann ein zweistufiger Workflow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger hinzu.

Hinweis:

Ab Vulnerability Response v15.0 wird der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert, wenn Sie die VR-Anwendung zum ersten Mal bereitstellen. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Sobald eine Ausnahmeanforderung für eine CVIT oder RT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Löschen
- Aktualisieren Sie das Feld **Zuweisung an** oder **Zuweisungsgruppen**

Verfolgen Sie eine Ausnahmeanforderung

Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status mithilfe der Registerkarte **Change-Genehmigungen** im CVIT oder RT nachverfolgen. Wenn eine Aktion für eine RT ausgeführt wird, können Sie den Status der einzelnen CVITs in dieser RT nicht nachverfolgen.

Ablauf einer Ausnahmeanforderung

Wenn eine Ausnahmeanforderung für eine bestimmte CVIT oder RT abläuft, wird die betroffene CVIT oder RT in den Status **„Offen“** versetzt.

Wenn ein einzelner CVIT oder alle CVITs in einem RT beim nächsten Scan bestanden werden, ändern sich die CVITs und gegebenenfalls das Feld RT- **Status** in **Geschlossen** mit dem Substatus **Fest**.

Konfigurieren Sie Genehmigungsregeln

Sie können Genehmigungsregeln anzeigen und konfigurieren, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Administration** > **Genehmigungsregeln**. Fordern Sie eine Ausnahme für CVITs an, die nicht sofort behoben oder zurückgestellt werden können, indem Sie die betroffenen Schwachstellen, Konfigurationselemente (CIs) oder CVITs identifizieren. Automatisieren Sie den CVIT-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zurückstellungsprozess. Übereinstimmende CVITs basierend auf diesen Regeln zurückstellen, wenn das System diese CVITs identifiziert.

Die folgenden Genehmigungsregeln werden standardmäßig bereitgestellt:

- Genehmigung für Ausnahmeanforderungen: Im Basissystem wird eine Standardkonfiguration mit zwei Genehmigungsebenen bereitgestellt. Immer wenn für ein angreifbares Element eine Ausnahmeanforderung angefordert wird, wird die Genehmigungsanforderung an die Benutzer oder Gruppen in Ebene 1 gesendet. Nach der Genehmigung durch die Genehmiger der Ebene 1 wird sie an die Genehmiger der Ebene 2 gesendet.

  Hinweis:
  Sie können die Standardebenen ändern und nach Bedarf bearbeiten. Ab Container Vulnerability Response v2.0.6 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme- oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie *sn_vul_container.container_exception_approver_L1*, *sn_vul_container.container_exception_approver_L2*oder *sn_vul_container.container_false_positive_approver_group*, um den Eigenschaftswert zu ändern.

- Genehmigung für Ausnahmeregeln: Hat keine Konfiguration, aber zwei Genehmigungsebenen.
- Genehmigung für falsch positive Ergebnisse: Verfügt über eine Konfiguration mit einer Genehmigungsebene.

Hinweis:
Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status Wird überprüft, und es wird ein Datensatz für die Statusänderung erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element des Containers oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Anfordern und Genehmigen einer Ausnahme in Container Vulnerability Response

Sie können anfordern, die Korrektur eines angreifbaren Elements in einem Container (CVIT) für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist. Genehmiger mit Zugriffsrechten können Anforderungen anderer Benutzer genehmigen.

Informationen zum Anfordern oder Genehmigen einer Ausnahme finden Sie unter:

- Fordern Sie eine Ausnahme für ein angreifbares Container-Element an
- Fordern Sie mit eine Ausnahme für Container-Schwachstellen an GRC: Richtlinien- und Compliance-Management

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail mit dem Hinweis, dass eine Ausnahme angefordert wurde. Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status Wird überprüft, und es wird ein Datensatz für die Statusänderung erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element des Containers oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Fordern Sie eine Ausnahme für ein angreifbares Container-Element an

Fordern Sie eine Ausnahme für ein angreifbares Container-Element (CVIT) an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Vorbereitungen

Erforderliche Rolle: Developer Group

Warum und wann dieser Vorgang ausgeführt wird

Mit der Funktion Massenbearbeitung in Vulnerability Manager Workspacekönnen Sie eine Ausnahme für mehrere CVITs gleichzeitig anfordern. Weitere Informationen finden Sie unter Massenausnahme im Arbeitsbereich des Schwachstellenmanagers anfordern.

Prozedur

1. Navigieren zu **Container Vulnerability Response** > **Angreifbare Container-Elemente** > **Alle**.
2. Wählen Sie den Artikel aus, für den Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“ oder „Wird untersucht“ befinden.
3. Klicken Sie im Formular „Angreifbares Container-Element“ **auf Ausnahme anfordern**.
   [store-future: BEGIN review]

   Hinweis:

   Je nachdem, ob Vulnerability Response oder GRC: Richtlinien- und Compliance-Management in ausgewählt ist **Container Vulnerability Response** > **Ausnahmenverwaltung** Im Bildschirm „Ausnahme anfordern“ ändert sich das Formular „Ausnahme anfordern“.

   [End]
4. [store-future: BEGIN review]Wenn Vulnerability Response im Bildschirm „Ausnahmeverwaltung“ ausgewählt ist, gehen Sie wie folgt vor.[End]

   a. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ausgewählten Dauer liegen **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status „Offen“ zurück. **Hinweis:** Ab Version 1.2 von Container Vulnerability Responsegilt: Wenn ein angreifbares Element mithilfe der Ausnahmeverwaltungsfunktion zur Korrektur zurückgestellt wurde und es vom Scanner erneut geöffnet wird, bleibt das für die Schwachstelle festgelegte Zurückstellungsdatum erhalten. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft `sn_vul.container.auto_defer_cvit_in_active_e` auf „true“ fest. Außerdem wird das Datum für „Zurückgestellt bis“ beibehalten, auch nachdem die CVIT geschlossen wurde oder die Ausnahme abgelaufen ist. Die erforderliche Rolle „sn_vul_container.manage_exception_configuration“ für Lese- und Schreibzugriff ist erforderlich.
Grund	Grund für die Ausnahme. Die Auswahlmöglichkeiten lauten wie folgt: ▪ Risiko akzeptiert ▪ Warten auf Wartungsfenster ▪ Behebung nicht verfügbar ▪ Ausgleichende Steuerung vorhanden ▪ Sonstige Informationen zum Hinzufügen neuer Gründe finden Sie unter Definieren Sie eine Richtliniengrundzuordnung.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Korrektur aktualisiert werden.

b. Senden Sie die Ausnahmeanforderung, indem Sie **auf Genehmigung anfordern**klicken.
Der Status des angreifbaren Container-Elements ändert sich in Wird überprüft. Verwenden Sie die Registerkarte **Change-Genehmigung**, um den Status der Ausnahmeanforderung zu verfolgen.

Ausnahme für eine Container-Korrekturaufgabe anfordern

Fordern Sie eine Ausnahme an, um eine Container-Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort gelöst werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Sie können Ausnahmen in den Arbeitsbereichen Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Erforderliche Rolle:

sn_vul.remediation_owner, sn_vul.app_security_Champion oder sn_vul_container.remediation_owner.

Sie können auch Ausnahmen für Container-Korrekturaufgaben in der klassischen Umgebung anfordern.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Korrekturaufgaben** > **Alle**.
2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Wählen Sie im Datensatz der Container-Korrekturaufgabe **die Option Ausnahme anfordern**aus.
4. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in der Konfiguration definierten Ausnahmedauer liegen.
Grund	Begründung für das Anfordern einer Ausnahme.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Korrektur aktualisiert werden.

5. Klicken Sie auf **Genehmigungs-Engine**.

Fordern Sie mit eine Ausnahme für Container-Schwachstellen an GRC: Richtlinien- und Compliance-Management

Fordern Sie mit der Funktion zur Verwaltung von Richtlinienausnahmen GRC in der Anwendung Richtlinien- und Compliance-Management innerhalb von Container Vulnerability ResponseRichtlinienausnahmen an.

Vorbereitungen

Bevor Sie die Integration für Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Richtlinien- und Compliance-Management von ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können Ausnahmen auch in der klassischen Anwenderoberfläche anfordern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** (oder **Korrekturaufgaben**) >**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular **auf Ausnahme anfordern**.

   Hinweis:
   Wenn GRC: Richtlinien- und Compliance-Management im Bildschirm „Ausnahmeverwaltung“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus. Weitere Informationen zu den Formularfeldern finden Sie unter Formular „Ausnahme anfordern“..

   a. Senden Sie die Ausnahmeanforderung, indem Sie **auf Genehmigung anfordern**klicken.
   Der Status der angreifbaren Elemente ändert sich in Wird überprüft, und es wird eine Richtlinienausnahme erstellt. Verwenden Sie die Registerkarte **Change-Genehmigung**, um den Status der Ausnahmeanforderung zu verfolgen.

   b. Zeigen Sie die Richtlinienausnahme an, indem Sie auf die zugehörige Liste Richtlinienausnahmen klicken.

   c. Klicken Sie auf die Nummer der Richtlinienausnahme.

   d. Wählen Sie im Feld **Genehmiger** den Namen des Genehmigers aus.

   e. Klicken Sie auf die Registerkarte Quelle, und wählen Sie im Feld **Kontrollziel** ein Kontrollziel aus.

   f. Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie die Risikobewertung im Feld **Risikobewertung** aus.

   g. Speichern Sie das Formular.

   h. Klicken Sie auf die Registerkarte **Betroffene Steuerungen**.

   i. Fügen Sie die Steuerungen hinzu, indem Sie auf **Hinzufügen**klicken.

   j. Speichern Sie das Formular.

   Hinweis:
   Sie können eine Compliance-Überprüfung veranlassen, indem Sie **auf Compliance-Überprüfung anfordern**klicken.

   Das Genehmigungsformular wird an den Genehmiger gesendet.

   Der Genehmiger kann entweder die Anforderung genehmigen, indem er auf **Genehmigen** klickt, oder eine zusätzliche Genehmigung anfordern, indem er **auf Zusätzliche Genehmigung anfordern**klickt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Datensatzstatus ändert sich in Zurückgestellt. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die Registerkarte **Zurückstellung** enthält zusätzliche Hinweise zum Datensatz.

Hinweis:
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

3. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Korrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Definieren Sie eine Richtliniengrundzuordnung

Definieren Sie Grundauswahlmöglichkeiten, die jedem Anwender zur Verfügung stehen, der eine Ausnahme anfordert.

Vorbereitungen
Erforderliche Rolle: sn_vul.compliance.manager und sn_vul_container.manage_exception_configuration

Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**.

   Hinweis:
   Sie können entweder einen Grund aus den in der Tabelle „Grundauswahlmöglichkeiten“ verfügbaren Gründen auswählen oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Registrierung Container Vulnerability Response – CVIT-Integration.
3. Klicken Sie in der Liste „Grund – Auswahlmöglichkeiten“ auf **Neu**.
4. Klicken Sie auf das Lupensymbol.
5. Fügen Sie eine vorhandene Grundauswahl hinzu, um eine neue zu erstellen.
   - Wenn Sie eine vorhandene Grundauswahl hinzufügen möchten, wählen Sie einen Grund aus.
   - Wenn Sie der Tabelle „Grundauswahlmöglichkeiten“ eine neue Begründung hinzufügen möchten, klicken Sie auf **Neu**, und füllen Sie die Felder im Formular aus.

Formular „Grund – Auswahlliste“.

Feld	Beschreibung
Bezeichnung	Eindeutige Bezeichnung für diese Auswahl.
Wert	Eindeutiger Wert für diese Auswahl. Dieser Wert wird in der Tabelle „Richtliniengrundzuordnung“ für die jeweiligen Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie im Filternavigator sn_vul_policy_reason_mapping.LIST ein.
Bestellung	Reihenfolge für diese Auswahl. Die Gründe werden basierend auf dieser Nummer sortiert.
Standard	Option, um anzugeben, dass diese Grundauswahl verfügbar ist, wenn eine bedarfsgesteuerte Richtlinienausnahme angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	sind alle Grundauswahlmöglichkeiten verfügbar, bei denen das Feld **„Standard“** ausgewählt ist.
Aktiv	Option zum Anzeigen der Auswahl in der Liste der Grundauswahlmöglichkeiten.

6. Klicken Sie auf **Absenden**.

Ergebnisse
Die Grundauswahl wird hinzugefügt. Die Auswahl des Grunds ist im Feld **Grund** des Formulars zum Anfordern einer Richtlinienausnahme für die ausgewählte Anwendung verfügbar.

Genehmigen Sie eine Ausnahmeanforderung in Container Vulnerability Response

Genehmigen Sie Ausnahmeanforderungen für angreifbare Container-Elemente oder Korrekturaufgaben, die nicht sofort korrigiert werden können. Sie müssen diese Anforderungen auf Risiken bewerten und dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Vorbereitungen
Erforderliche Rolle: sn_vul.exception_approver

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Ausnahme- und falsch-positiven Anforderungen in Vulnerability Manager Workspacegenehmigen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Sie können Ausnahmeanforderungen auch in der klassischen Umgebung genehmigen:

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Stellen Sie ein angreifbares Container-Element in zurück Container Vulnerability Response

Wenn Sie feststellen, dass das mit einem angreifbaren Element im Container (CVIT) verbundene Problem ein geringes Risiko aufweist und ohne weitere Analyse sofort zurückgestellt werden kann, können Sie die Funktion **Zurückstellen** verwenden.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
Täglich wird eine geplante Aufgabe ausgeführt, um nach zurückgestellten angreifbaren Elementen zu suchen, deren Wiedereröffnungsdatum erreicht ist. An dem Tag, an dem die Zurückstellung der CVIT abläuft, wird der Datensatz erneut geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie auf **Ausnahme anfordern**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Bis	Wählen Sie das Datum aus, an dem der Status „Zurückgestellt“ abläuft und die Korrekturaufgabe erneut aktiviert wird. **Hinweis:** Ab Version 18.0 von Container Vulnerability Responsewird der Status des CVIT unter Berücksichtigung des aktiven Ausnahmefensters in den Status „Zurückgestellt“ geändert, wenn ein zurückgestelltes angreifbares Element in einem Container (CVIT) von einem Scanner geschlossen und erneut geöffnet wird, bevor das Ausnahmefenster abläuft. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft *sn_vul.container.auto_defer_cvit_in_active_ex* auf „true“ fest. Darüber hinaus bleibt das zurückgestellte Bis-Datum auch dann erhalten, wenn das angreifbare Element geschlossen wird oder die Ausnahme abgelaufen ist. Die erforderliche Rolle „sn_vul_container.manage_exception_configuration“ für Lese- und Schreibzugriff ist erforderlich. Nachdem der Datensatz übermittelt wurde und E-Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Container Vulnerability Response eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird das angreifbare Element auf „Offen“ zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Falsch positiv ○ Fix nicht verfügbar ○ Risiko akzeptiert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Klicken Sie auf **Absenden**.
   Die Gruppe wird **als In Überprüfung**markiert. Der zugehörige Link **Erneut öffnen** wird angezeigt. Das Datum und der Grund der Wiedereröffnung werden in den Arbeitsnotizen unter der Registerkarte **Change-Genehmigungen** anzeigen angezeigt.

   Ab Container Vulnerability Response v2.3 können Sie für ein zurückgestelltes angreifbares Container-Element im Feld „Arbeitsnotizen“ im Abschnitt „Notizen“ relevante Informationen hinzufügen.

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Container-Element an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Container-Element an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht wird. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**.
2. Öffnen Sie ein zurückgestelltes angreifbares Container-Element.
3. Wählen Sie **Verlängerung anfordern**aus.

   Hinweis:
   Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Containerelements Zurückgestellt ist.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten angreifbaren Container-Elements verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

   Hinweis:
   - Die Anforderung durchläuft zwei Genehmigungsebenen.
   - Wenn ein zurückgestelltes angreifbares Container-Element erneut erweitert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden die Hinweise Bis, Grund und Zurückstellung aktualisiert.

Arbeiten mit einer Ausnahmeregel in Container Vulnerability Response

Sie können eine Ausnahme für angreifbare Elemente in Containern (CVITs) anfordern, die nicht sofort behoben oder zurückgestellt werden können. Durch die Automatisierung des VI-Zurückstellungsprozesses können Sie die übereinstimmenden CVITs basierend auf der Regel zurückstellen, wenn sie vom System identifiziert werden.

Sie können die folgenden Aufgaben für eine Ausnahmeregel ausführen:

- Erstellen Sie eine Ausnahmeregel in Container Vulnerability Response
- Genehmigen Sie die Anforderung einer Ausnahmeregel in Container Vulnerability Response
- Ausnahmeregel wird in aktiviert Container Vulnerability Response
- Öffnen Sie eine Ausnahmeregel in erneut Container Vulnerability Response
- Aktualisiert eine genehmigte Ausnahmeregel in Container Vulnerability Response
- Löschen Sie eine Ausnahmeregel in Container Vulnerability Response
- Stellen Sie ein angreifbares Container-Element in zurück Container Vulnerability Response

Hinweis:
Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status Wird überprüft, und es wird ein Datensatz für die Statusänderung erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element des Containers oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Ausnahmeregel in Container Vulnerability Response

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe von angreifbaren Elementen in Containern (CVITs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser CVITs basiert. Mit dieser Regel können Sie neue und vorhandene CVITs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Regel wird vom „Gültig ab“-Datum bis zum „Gültig bis“-Datum angewendet.
Die Korrekturaufgabe (VUL) wird erstellt, wenn die Regel genehmigt wird. Die Gruppierungsmethode für diese VUL wird als Ausnahmeregel bezeichnet. Die VUL wird im Status „Zurückgestellt“ erstellt. Sie können diese VUL nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete CVITs werden zurückgestellt und dieser VUL vom „Gültig ab“-Datum hinzugefügt, bis die Gruppe am „Gültig bis“-Datum abläuft.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmeregel-Workflows gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung übermittelt wurde.

Hinweis:

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung einreichen.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Klicken Sie auf der neuen Datensatzseite „Ausnahmeregel“ auf **Neu**, um eine Regel zu erstellen.
3. Füllen Sie die Felder im Formular „Ausnahmeregel“ aus.

   Hinweis:

   Weitere Informationen zu den Formularfeldern finden Sie unter Formular „Ausnahmeregel“..
4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Senden Sie das Formular zur Genehmigung.
   Der Status der Anforderung ändert sich in Überprüfung. Bis Sie die Ausnahmeregel nicht absenden, verbleibt sie im Status Entwurf.
6. So zeigen Sie eine Gruppe zum Verwalten von Ausnahmeregeln an und erstellen diese:

   a. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**.

   b. Klicken Sie in einer Ausnahmeregel auf die Registerkarte **Angeforderte Genehmigungen**, um den Status der Anforderung anzuzeigen.
   Täglich wird eine geplante Aufgabe ausgeführt, die die Ausnahmeregeln für vorhandene Daten ausführt. Alle angreifbaren Elemente, die der Bedingung entsprechen, werden in den Status „Zurückgestellt“ versetzt. Wenn eine genehmigte Ausnahmeregel gelöscht wird, werden alle zurückgestellten angreifbaren Elemente in ihren vorherigen Status zurückversetzt. Weitere Informationen finden Sie unter Arbeiten mit einer Ausnahmeregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigen Sie die Anforderung einer Ausnahmeregel in Container Vulnerability Response

Bewerten Sie Anforderungen für Ausnahmeregeln von Anwendern, um diese Anforderungen genehmigen oder ablehnen zu können.

Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

Warum und wann dieser Vorgang ausgeführt wird

Mitglieder der Benutzergruppe „Ausnahmegenehmiger Ebene 1“ können die Anforderungen der Ausnahmeregel der Ebene 1 genehmigen. In ähnlicher Weise können Mitglieder der Benutzergruppe, die Ausnahmegenehmiger der Ebene 2 sind, die Anforderungen einer Ausnahmeregel der Ebene 2 genehmigen. Beide Benutzergruppen erben standardmäßig die Rolle des Ausnahmegenehmigers.

Hinweis:

Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern. Informationen zur Konfiguration von Genehmigungsregeln für die Ausnahmeverwaltung und für falsch positive Meldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit ab, und erläutern Sie, warum Sie die Anforderung genehmigt oder abgelehnt haben.
   Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe (RT) im Status „Zurückgestellt“ erstellt. Ab dem Datum „Gültig ab“ wird diese Regel für alle CVITs ausgeführt, die erstellt werden, sowie für diejenigen, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden. CVITs, die den definierten Bedingungen entsprechen, werden der RT hinzugefügt und für den angegebenen Zeitraum zurückgestellt.

   Hinweis:
   Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung einreichen.

Ausnahmeregel wird in aktiviert Container Vulnerability Response

Eine Regel wird an ihrem „Gültig ab“-Datum aktiviert. Nach der Aktivierung wird der Ausnahmeprozess für angreifbare Elemente in Containern (CVITs) automatisiert.

Die Ausnahmeregel folgt diesem Lebenszyklus:

1. Die neuen CVITs, die Sie erstellen oder erneut öffnen und die die angegebene Bedingung erfüllen, werden zurückgestellt. Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wenn Sie die Ausnahmeregel zum ersten Mal ausführen, werden alle aktiven und nicht zurückgestellten CVITs, die der Ausnahmeregelbedingung entsprechen, in die neu erstellte Korrekturaufgabe (RT) verschoben, und ihr Status wird geändert auf „Zurückgestellt“
2. Wenn eine neu erstellte CVIT mit der Ausnahmeregelbedingung übereinstimmt, wird sie in die zurückgestellte RT verschoben, die der Regel zugeordnet ist, und die Gruppenregel wird nicht dafür ausgeführt.
3. Am Datum „Gültig ab“ werden vorhandene CVITs hinzugefügt, wenn Sie die Option Für vorhandene Daten ausführen aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Die RT akzeptiert keine neuen CVITs mehr, wenn die Regel am „Gültig bis“-Datum abläuft. Die RT bleibt bis zum Datum „Zurückgestellt bis“ bestehen.
5. Die Ausnahmeregel läuft am „Gültig bis“-Datum ab.

Öffnen Sie eine Ausnahmeregel in erneut Container Vulnerability Response

Öffnen Sie eine Ausnahmeregel erneut, die abgelehnt wurde, Sie möchten jedoch erneut übermitteln. Durch erneutes Öffnen wird die Regel in den Status Entwurf versetzt.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Regel dann aktualisieren und erneut zur Genehmigung einreichen.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Suchen Sie die Regel, die Sie erneut öffnen möchten, und klicken Sie auf **Erneut öffnen**.
3. Aktualisieren Sie das Formular, und senden Sie es erneut zur Genehmigung.

Aktualisiert eine genehmigte Ausnahmeregel in Container Vulnerability Response

Brechen Sie eine genehmigte Regel ab, um sie aktualisieren zu können. Bevor Sie beispielsweise Datumsangaben ändern oder einer genehmigten Regel eine Bedingung hinzufügen können, müssen Sie sie abbrechen, damit die Korrekturaufgabe (VUL) gelöscht wird und die angreifbaren Elemente des Containers (CVITs) in den Status Offen versetzt werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Gruppenregeln werden erneut auf diese CVITs angewendet. Senden Sie die Regel, nachdem Sie die Änderungen vorgenommen haben, damit sie den Genehmigungsprozess erneut durchläuft.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie abbrechen möchten, und klicken Sie auf **Abbrechen**.
3. Klicken Sie im Dialogfeld „Regel abbrechen“ auf **Regel abbrechen**.
   Die Regel wird zurück in den Status Entwurf verschoben, und die zugehörige VUL wird gelöscht.
   Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

Löschen Sie eine Ausnahmeregel in Container Vulnerability Response

Löschen Sie eine Ausnahmeregel, die nicht mehr erforderlich ist. Sie können beispielsweise eine Regel löschen, wenn Sie ein angreifbares Container-Element (CVIT) während der Erfassung nicht zurückstellen möchten.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Durch das Löschen einer Regel wird die zugehörige Korrekturaufgabe (VUL) abgebrochen. Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Klicken Sie im Dialogfeld „Regel löschen **" auf Regel löschen**, um die ausgewählte Regel zu löschen. Die zugehörige Korrekturaufgabe wird ebenfalls gelöscht. Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe in an Container Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor das Datum für „Zurückgestellt bis" erreicht wird. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status „Zurückstellen" abläuft und das angreifbare Container-Element erneut aktiviert wird.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Container-Elemente übertragen, die Teil der Korrekturaufgabe sind. Die angreifbaren Container-Elemente müssen sich jedoch im Status „Zurückgestellt“ befinden, und ihre aktuellen Bis-Daten müssen vor dem „Aktualisiert bis“-Datum liegen. Außerdem wird bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers eine E-Mail ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Korrekturaufgabe erneut verlängert wird, erhöht sich die Anzahl der Zurückstellungen verlängern im Back-End.

Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Container Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht ist. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.exception_approver

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Ausnahmeregeln**.
2. Wählen Sie eine zurückgestellte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein. Zur Auswahl stehen: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Fix nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und Zusätzliche Informationen für die Ausnahmeregel und die angreifbaren Container-Elemente aktualisiert. Außerdem wird bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers eine E-Mail ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Ausnahmeregel erneut verlängert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.

Markieren und Genehmigen eines falsch positiven angreifbaren Container-Elements

Angreifbare Container-Elemente (CVITs) und Korrekturaufgaben (VULs) können als falsch positive Meldungen markiert werden. Genehmiger mit Schreibzugriff können solche Anforderungen von anderen Benutzern genehmigen.

- Markieren Sie als falsch positiv in Container Vulnerability Response
- Genehmigen Sie ein falsch positives Ergebnis

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des falsch positiven Workflows gesendet und enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine CVIT- oder Korrekturaufgabe als falsch positiv markiert wird, erhält die anfordernde Person eine Bestätigungs-E-Mail. Gleichzeitig erhält der Genehmiger eine E-Mail, in der angegeben wird, dass ein CVIT oder eine Korrekturaufgabe als falsch positiv markiert wurde. Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status Wird überprüft, und es wird ein Datensatz für die Statusänderung erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element des Containers oder die Korrekturaufgabe in den Status „Offen“ zurückversetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Wichtig:
Als Schwachstellenanalyst und Nachbesserungsbesitzer können Sie im Vulnerability Manager Workspace bzw. IT Remediation Workspace Falschmeldungen anfordern und genehmigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Markieren Sie als falsch positiv in Container Vulnerability Response

Markieren Sie ein angreifbares Containerelement (CVIT) oder eine Korrekturaufgabe als falsch positiv, wenn die vom Scanner ausgegebene Warnung kein tatsächliches Problem darstellt. Wenn beispielsweise ein CVIT außer Betrieb genommen wurde, der Scanner jedoch immer noch ein damit zusammenhängendes Problem auslöst, markieren Sie es als falsch positiv.

Wichtig:
Als Schwachstellenanalyst und Nachbesserungsbesitzer können Sie im Vulnerability Manager Workspace bzw. im IT Remediation Workspace Falschmeldungen anfordern.

Vorbereitungen
Erforderliche Rolle: Korrekturbesitzer

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response (oder Korrekturaufgaben)** > **Alle**.
2. Öffnen Sie das CVIT, das Sie als falsch positiv markieren möchten, und klicken Sie auf **Als falsch positiv markieren**.
   CVIT muss sich im Status **„Offen"** befinden.
3. Geben Sie im Formular „Falsch positiv" unter **Zusätzliche Informationen** Details ein, und klicken Sie auf **Genehmigung anfordern**.
   Die Anforderung wird zur Genehmigung gesendet, und der Status des CVIT ändert sich in **Wird überprüft**. Sowohl die anfordernde Person als auch der Genehmiger werden per E-Mail benachrichtigt.

Genehmigen Sie ein falsch positives Ergebnis

Als falsch positiver Genehmiger können Sie falsch positive Anforderungen von anderen Benutzern genehmigen.

Wichtig:
Im Vulnerability Manager Workspacekönnen Sie falsch positive Anforderungen genehmigen oder ablehnen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Vorbereitungen
Erforderliche Rolle: false_positive_approver
Sie können Ausnahmen und falsch positive Anforderungen auch in der klassischen Umgebung genehmigen:

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Hinweis:
Ein falsch positives Ergebnis kann zeitgebunden sein. Nur der Genehmiger kann das Enddatum festlegen.

Übersicht über Korrekturaufgaben und Aufgabenregeln in Container Vulnerability Response

Konfigurieren Sie Korrekturaufgaben (CVULs), damit Analysten und Korrekturspezialisten angreifbare Container-Elemente (CVIT) organisieren und massenweise analysieren können. Die Kriterien, nach denen Korrekturaufgaben entstehen, sind so konfiguriert, dass CVITs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

automatisch Korrekturaufgaben zugewiesen werden. Mit Korrekturaufgaben können Sie den Fortschritt überwachen und den Nachbesserungsprozess effizienter gestalten.

Nachverfolgung der Anzahl der Zurückstellungen für angreifbare Container-Elemente und Korrekturaufgaben

Verfolgen Sie, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Die regelmäßige Aufgabe zum Festlegen der Anzahl der Zurückstellungen wird täglich ausgeführt, um die Anzahl der Datensätze zu erfassen, die in der Spalte Anzahl der Zurückstellungen mehr als einmal zurückgestellt wurden. Datensätze werden in den Modulen „Mehrere Zurückstellungen“ für VR, AVR und CVR angezeigt.

Die Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Container-Elemente automatisch gruppiert und zugewiesen werden. Das Basissystem enthält eine Standardregel **für Schwachstellen**, die CVITs basierend auf ihren Schwachstellen sammelt. Sie können jedoch nach jedem anderen Satz von Werten in Spalten gruppieren, auf die über CVIT zugegriffen werden kann. Diese Werte können Configuration Item (CI), Schwachstelleneintrag und Ähnliches umfassen.

Es gibt Aufgabenregeln für Container Vulnerability Response, die in der Anwendung Vulnerability Response enthalten sind. Sie ist verfügbar, wenn Sie sie aktivieren.

Mit dem Bedingungsgenerator können Sie mehrere Bedingungen erstellen. Nachdem Sie im Abschnitt „Gruppieren nach“ ein Feldpaar festgelegt haben, wird eine weitere Zeile angezeigt. Sie können bis zu sechs **„Gruppieren nach** “-Auswahlen auswählen. Sie können auch die Gruppenzuweisung automatisieren.

Beispielsweise können Sie Ihre angreifbaren Container-Elemente nach Configuration Item oder nach dem Produktmodell gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit niedrigem Schweregrad oder für CIs mit geringem Risiko festlegen. Sie können eine andere Aufgabenregel für kritische Server und Schwachstellen festlegen, die das Unternehmen einem höheren Risiko aussetzen. Unter Erstellen, bearbeiten und löschen Sie Regeln für Korrekturaufgaben in Container Vulnerability Response finden Sie weitere Informationen zu den Optionen, die Ihnen zur Verfügung stehen.

Für angreifbare Container-Elemente, die das Unternehmen einem höheren Risiko aussetzen, kann ein anderer Regelsatz verwendet werden. Der Name der Korrekturaufgabe wird an die Korrekturaufgabenregel „ **Gruppieren nach** “-Werte angehängt, um die Kurzbeschreibung des neuen Datensatzes zu erstellen.

Wenn ein neues angreifbares Container-Element erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Regeln entsprechend ausgewertet. Ein CVIT wird nur einmal automatisch ausgewertet, es sei denn, er wird nach dem Schließen erneut geöffnet oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jede neue oder erneut geöffnete CVIT verwendet:

- Für jede Regel für Korrekturaufgaben wird die CVIT mit dem Filter für die Regel für Korrekturaufgaben verglichen.
- Für jede Regel, mit der die Regelbedingung für Korrekturaufgaben übereinstimmt, ruft die Regel die Daten aus der **Auswahl Gruppe nach** Auswahl im CVIT ab. Es erstellt einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppennamen und ein Feld. In diesem Fall, **Hohes Risiko: QID-32342:Zusammenfassung von QID-3242** (Name: Schwachstellen-ID: Schwachstellenzusammenfassung).

Hinweis:
Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

Die Regel prüft, ob eine übereinstimmende **offene** Korrekturaufgabe vorhanden ist, die der gleichen Zuweisungsgruppe wie CVIT zugewiesen ist.

- Wenn die Aufgabe gefunden wird, wird die CVIT der vorhandenen Aufgabe im Status „ **Offen** “ hinzugefügt.
- Wenn keine Aufgabe im Status „ **Offen“** gefunden wird, erstellt die Regel eine Aufgabe **mit hohem Risiko: QID-32342**, weist sie derselben Zuweisungsgruppe wie das CVIT zu und platziert das CVIT in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Bedingungen der Korrekturaufgabenregel verglichen wird, bevor sie in eine Korrekturaufgabe aufgenommen wird, können zu viele Regeln die Leistung beeinträchtigen. Richten Sie Ihre Aufgabenregeln so ein, dass die Bedingungen Ihnen helfen, die Erstellung von doppelten Korrekturaufgaben zu vermeiden.

Standardmäßig verwenden die Regeln für Korrekturaufgaben beim Gruppieren der Elemente die von den **Zuweisungsregeln** im CVIT festgelegte Zuweisungsgruppe und weisen die Korrekturaufgabe entsprechend den CVITs zu.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln im Modul **„Zuweisungsregeln“** gesteuert. Weitere Informationen zu Zuweisungsregeln finden Sie unter Übersicht über Zuweisungsregeln für Vulnerability Response.

Wenn eine Aufgabenregel aus dem Formular oder der Listenansicht gelöscht wird, können Sie alle von dieser Regel erstellten offenen Aufgaben löschen. Aufgaben, die sich nicht im Status **„Offen“** befinden, werden ausgeschlossen.

Die Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Regel für Korrekturaufgaben ändern möchten, klicken Sie auf der Seite für die Regel für **Korrekturaufgaben** auf die Schaltfläche Erneut anwenden, um die geänderte Regel für alle aktiven **offenen** Korrekturaufgaben erneut auszuführen, die von dieser Regel erstellt wurden. Es löscht Korrekturaufgaben basierend auf der geänderten Regel automatisch und erstellt sie neu.

Beim erneuten Anwenden werden nur vorhandene Korrekturaufgaben überprüft.

Nachdem Sie **Erneut**anwenden ausgewählt haben, wird die folgende Meldung angezeigt: Durch das erneute Anwenden dieser Regel für Korrekturaufgaben werden die Korrekturaufgaben für diese Regel gelöscht und neu erstellt. Korrekturaufgaben, die sich nicht im Status „Offen“ befinden, werden nicht gelöscht.

Wichtig:
Als Schwachstellenadministrator und -analyst können Sie die Regeln für Korrekturaufgaben für ausgewählte angreifbare Elemente im Vulnerability Manager Workspacebewerten. Diese Methode ist effizienter als die erneute Anwendung der Regeln für Korrekturaufgaben in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln für Korrekturaufgaben und CVIT-Erstellung und -Aktualisierung

Wenn ein CI aus einem Scan einer bekannten Schwachstelle zugeordnet ist, wird eine CVIT erstellt. Nach der Erstellung wird die CVIT anhand der Bedingungen der Regeln für Korrekturaufgaben für eine Übereinstimmung ausgewertet. Wenn es eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe gibt, wird die CVIT hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für CVIT erstellt.

Wenn eine Eigenschaft, die in den Filterbedingungen für Korrekturaufgaben erfasst wird, in einem CVIT aktualisiert oder geändert wird, wird die aktualisierte AVI auch anhand der Regeln für Korrekturaufgaben auf Übereinstimmung ausgewertet. Wenn es eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe gibt, wird die CVIT hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für CVIT erstellt.

Status-Rollup und -Rolldown

Wenn Sie eine Korrekturaufgabe auf „Offen“ oder von „Offen“ auf „Wird untersucht“ ändern, wird der neue Status auf alle zugehörigen CVITs übertragen. Das Status-Rolldown erfolgt unmittelbar nach dem Ändern des Status.

Ein Status-Rollup von CVITs zur Korrekturaufgabe findet nur statt, wenn sich alle CVITs für die Aufgabe im Status **„Zurückgestellt“** oder **„Geschlossen – Fest“** befinden. Das Rollup erfolgt mit den Werten der angreifbaren Elemente des Rollup-Containers für die Schwachstelle und einer geplanten Gruppenaufgabe, die alle 15 Minuten ausgeführt wird. Für den Status wird erst ein Rollup durchgeführt, wenn der Auftrag ausgeführt wird. Damit ein Status für ein Rollup von den CVITs zur Korrekturaufgabe erfolgt, müssen sich alle CVITs im selben Status befinden.

Erstellen, bearbeiten und löschen Sie Regeln für Korrekturaufgaben in Container Vulnerability Response

Sie können Regeln erstellen, um angreifbare Elemente in Containern (CVIT) basierend auf Filterbedingungen automatisch in Korrekturaufgaben (CVUL) zu gruppieren. Diese Regeln gruppieren CVITs automatisch, wenn sie importiert oder manuell erstellt werden.

Vorbereitungen

Wenn Sie eine neue Regel erstellen, gilt sie nicht für vorhandene Daten. Nachdem Sie es übermittelt haben, wird es für neue Importe ausgeführt.

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben.**.
2. Öffnen Sie die Regel, oder wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie.

Regel für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Aufgabenregel.
Aktiv	Gibt an, ob die Aufgabe aktiv ist.
Beschreibung	Eine Beschreibung der Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Groß-/Kleinschreibung beachten	Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht. **Hinweis:** Beim Standardwert wird zwischen Groß- und Kleinschreibung unterschieden.
Bedingung	Optionale Filterbedingungen für die Regel. Standardmäßig (Kontrollkästchen**„Groß-/Kleinschreibung beachten** “ nicht aktiviert) berücksichtigt der Suchtext, den Sie im Bedingungsgenerator für Aufgabenregeldatensätze und -formulare eingeben, Groß-/Kleinschreibung. Sie können die Suche nach Groß-/Kleinschreibung für Aufgabendatensätze und Formulare aktivieren. Eine Beispielbedingung ist **Schwachstelle** > **ist** > **VULNENT123451** (eine bekannte importierte Schwachstelle). Alle CVITs, die diese Schwachstelle aufweisen, erfüllen diese Bedingung.
Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)	
Gruppieren Sie angreifbare Container-Elemente aus	Die Tabelle, die von der Regel zum Gruppieren von CVITs verwendet wird. Wählen Sie die Elemente aus der Struktur aus: ○ Angreifbares Container-Element [sn_vuln_vulnerable_item] ○ Angreifbares Container-Element: Docker-Image ○ Angreifbares Container-Element: Container-Schwachstelle **Hinweis:** Wenn Sie eine erweiterte Tabelle wählen, wird das **Feld Verwendet** nur für angreifbare Anwendungselemente angewendet, die diese erweiterte Tabelle verwenden.
Mit Feld	Feld in der Tabelle, das die Regel zum Gruppieren von CVITs verwendet. Wählen Sie in der Struktur Bedingungen aus.
Zuweisung	
Korrekturaufgaben zuweisen nach	Bei der automatischen Zuweisung von Korrekturaufgaben wird die Option Zuweisung zusätzlich zu den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Auswahlmöglichkeiten **für Gruppieren nach** verwendet, um die angreifbaren Elemente zu gruppieren. Neue Aufgaben werden nach Bedarf erstellt, sodass jedes CVIT in einer Aufgabe mit einer übereinstimmenden Zuweisungsgruppe platziert wird. Um die Zuweisung von auf der Grundlage dieser Regel erstellten Aufgaben zu automatisieren, wählen Sie eine der verfügbaren Optionen aus. ○ Feld Gruppieren nach: Wenn Sie ein Benutzergruppenfeld aus Feldwerte **werden verwendet** im Abschnitt **Gruppieren nach** ausgewählt haben, werden diese im Dropdown-Menü angezeigt. ○ Benutzergruppe: Verwenden Sie die Suchliste, um eine statische Benutzergruppe auszuwählen.

Hinweis:
Wenn Sie eine Regel aus dem Formular oder der Listenansicht löschen, können Sie alle offenen Korrekturaufgaben löschen, die von dieser Regel erstellt wurden. Gruppen, die sich nicht im Status „Offen“ befinden, werden ausgeschlossen.

4. Wählen Sie **Absenden** für neue Regeln.
Nachdem Sie **Absenden**gewählt haben, wird Ihre Regel in der Liste Regeln für Korrekturaufgaben [sn_vul_grouping_rule] angezeigt. Die folgenden Situationen initiieren Ihre Regel.
   - Wenn neue CVITs erstellt werden
   - Wenn Sie **Erneut anwenden**wählen. Sie wählen **Erneut anwenden,** um Aufgabenregeln nur für vorhandene Korrekturaufgaben auszuwerten.
   - Wenn CVITs aktualisiert werden, entweder von Ihnen oder vom System.

     Wenn eine CVIT aktualisiert wird, werden Aufgabenregeln auf Übereinstimmungen mit vorhandenen Korrekturaufgaben ausgewertet. Einige häufige Updates, die eine Regelprüfung auslösen, sind:
     - Wenn der Status von „Geschlossen“ zu „Offen“ oder von „Geschlossen“ zu „Wird untersucht“ wechselt.
     - Das Configuration Item (CI) wird geändert.
     - Die Schwachstelle wird geändert.

   Das System prüft alle Aufgabenregeln auf Übereinstimmungen mit der aktualisierten CVIT. Wenn die Bedingungen einer Regel mit den Bedingungen einer Korrekturaufgabe übereinstimmen, werden ihr entsprechende CVITs zugewiesen.

   Wenn keine Übereinstimmung gefunden wird, wird eine neue Korrekturaufgabe erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Status-Rollup von CVITs zu Korrekturaufgaben und zum Status-Rolldown von Korrekturaufgaben zu CVITs finden Sie unter Container Vulnerability Response – Übersicht über Korrekturaufgaben und Aufgabenregeln.

Ein Beispiel für eine Regel für Korrekturaufgaben finden Sie unter Beispiele für Regel für Korrekturaufgaben in Application Vulnerability Response.

5. Um eine Aufgabenregel zu löschen, wählen Sie die Regel in der Liste „Regeln für Korrekturaufgaben“ aus, und wählen Sie Löschen aus.
   Die folgende Meldung wird angezeigt: Die ausgewählte Regel für Korrekturaufgaben hat n Korrekturaufgaben erstellt. Von den Korrekturaufgaben haben n den Status „Offen“.

Option	Beschreibung
Kontrollkästchen deaktiviert (Standard).	Löschen Sie nur die Regel. Aufgaben, die sich nicht im Status „Offen“ befinden, werden ausgeschlossen.
Checkbox aktiviert.	Schließen Sie die Korrekturaufgaben in den Status „Offen“ ein, wenn Sie die Regel für Korrekturaufgaben löschen. Löschen Sie die Regel und alle Korrekturaufgaben im Status „Offen“.

6. Wählen Sie eine Option und anschließend **Löschen**aus.

Erstellen Sie Regeln für das automatische Schließen für Container Vulnerability Response

Verwenden Sie Regeln zum automatischen Schließen, um ältere angreifbare Elemente in Containern (CVITs) automatisch basierend auf den von Ihnen festgelegten Filterbedingungen zu schließen.

Vorbereitungen
Erforderliche Rolle: sn_vul.container_manage_auto_close_stale_vi

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** > **Regeln für automatisches Schließen**.

   Das Basissystem stellt die folgenden Regeln für das automatische Schließen bereit: **Container-Schwachstellen zuletzt gescannt**: Schwachstellen, die in den letzten 90 Tagen nicht gemeldet wurden, werden in den Status „Veraltet“ versetzt.

2. Wählen Sie **Neu** aus, um eine Regel für das automatische Schließen zu erstellen.
3. Füllen Sie die Felder des Formulars aus.

Feld	Wert
Name	Name der Regel zum automatischen Schließen.
Aktiv	Option zum Aktivieren der Regel. Wenn aktiviert, werden Erkennungen automatisch geschlossen, die den Filterkriterien entsprechen.
Ausführungsreihenfolge	Eindeutiger Wert für die Ausführung der Regel zum automatischen Schließen. Dieser Wert bestimmt die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Reihenfolge der Ausführung. Der Standardwert ist 100.
Integrationstyp	Integration von Container-Schwachstellen **Hinweis:** Um Host-Schwachstellen mit der Prisma-Cloud-Computing-Integration zu scannen, wählen Sie **Integration des Schwachstellenscanners**aus.
Beschreibung	Beschreibung der Regel zum automatischen Schließen.
Bedingung	Filterbedingungen, die zum Identifizieren von Erkennungen verwendet werden, die geschlossen werden sollten.

4. Wählen Sie **Absenden**.
   Die geplanten Aufgaben für Regeln **zum automatischen Schließen** werden täglich ausgeführt. Identifiziert CVITs basierend auf den angegebenen Bedingungen und versetzt die übereinstimmenden in den Status **Veraltet**. In Fällen, in denen CVITs mit den Status „Geschlossen“ und „Veraltet“ vorhanden sind, wird die CVIT mit dem Substatus „Fest“ geschlossen.

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das einer Anwendungskorrekturaufgabe zugeordnete Problem ohne weitere Analyse sofort geschlossen werden kann, können Sie die Funktion **Schließen** verwenden. Ab v2.10 von Container Vulnerability Responsewurde die Schaltfläche **Schließen** für eine Container-Korrekturaufgabe entfernt.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
In den Vulnerability Response -Arbeitsbereichen durchläuft eine Korrekturaufgabe dieselben Status wie eine Korrekturaufgabe in früheren Versionen von Vulnerability Response. Wenn alle angreifbaren Elemente (VITs) in einer Korrekturaufgabe geschlossen wurden, geht die Korrekturaufgabe in den Status „Inaktiv“ über.

Wichtig:
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder aus einer Korrekturaufgabe entfernen kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben Korrekturaufgaben jedoch nicht automatisch aus den Status „Geschlossen “ oder „Zurückgestellt“.

Prozedur

1. Öffnen Sie den Datensatz, für den Sie eine Überprüfung anfordern möchten.
2. Wählen Sie die Schaltfläche **Schließen** aus.
3. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Wählen Sie als Status *Geschlossen*aus.
Grund	Geben Sie den Grund für das Schließen des Problems ein.
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

4. Wählen Sie **Absenden**.
   Die Korrekturaufgabe wird als **Geschlossen**markiert.

IT Operations Management und Muster-Discovery

Wenn Discovery aktiviert ist, werden Informationen vom Information Technology Operations Management (ITOM)-Team empfangen. Wenn die Discovery ITOM aktiviert ist, können Sie Kubernetes-Namespaces, Kubernetes-Cluster und Kubernetes-Services anzeigen, wenn Sie ein angreifbares Containerelement (CVIT) öffnen. Andernfalls können Sie Informationen zur Prisma-Nutzlast anzeigen.

Die Bildbezeichnungen aus den Prisma-Nutzlasten werden als Schlüssel-Wert-Paare unter dem Docker-Bild gespeichert. Die Bezeichnungen in einer Prisma-Nutzlast werden in der Tabelle „cmdb_key_value“ gespeichert. Um diese Funktion zu aktivieren, wird vom ITOM-Team eine Identifizierungsregel für cmdb_ci_docker_image bereitgestellt. Öffnen Sie das Docker-Image, um die Liste der zugehörigen Elemente anzuzeigen. Die meisten Elemente werden vom Team ITOM ausgefüllt. Der Identifizierungseintrag für ein Docker-Image wird so geliefert, dass die Werte als Schlüssel-Wert-Paare angezeigt werden.

Die Geschäftskritikalität wird basierend auf den Informationen zur Servicekritikalität bestimmt, die vom Team ITOM erhalten wurden. Eine regelmäßige Aufgabe wird ausgeführt, um Daten aus allen Services abzurufen, die einem Image zugeordnet sind. Es berechnet die Geschäftskritikalität basierend auf dem Service-Mapping. Da die Risikopunktzahl von der Geschäftskritikalität abhängen kann, wird die Risikopunktzahl auch auf dieser Grundlage berechnet.

Analyse- und Berichterstellungslösungen für Container Vulnerability Response

Platform Analytics-Lösung enthält vorgefertigte Platform Analytics Inhalte zur Verwendung mit anderen Now Platform -Produkten. Platform Analytics-Lösung bietet Einblicke in das Management von Schwachstellen in den verschiedenen Diagrammen.

Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Platform Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Zugehörige Informationen

Analytics- und Reporting-Lösungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Container Vulnerability Response-Dashboard

Analytics- und Reporting-Lösungen enthalten vorpaketierte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten. Mit Platform Analytics-Lösung können Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Behebung nachverfolgen. Sie können Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern.

Erforderliche Now Platform-Rollen

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Zugriff auf das Dashboard von Container Vulnerability Response

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Container Vulnerability Response** > **Übersicht**.

Wichtig:

Ab Version 2.2 von Container Vulnerability Responsekann dieses Dashboard auch in der Anwenderoberfläche Next Experience von angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und wählen Sie das **Dashboardsymbol**. Je nach Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, wählen Sie die Dropdownliste neben dem Namen des Dashboards. Weitere Informationen finden Sie unter Seite „Dashboards“ im Vulnerability Manager Workspace und Seite „Dashboards“ im IT Remediation Workspace.

Hinweis:

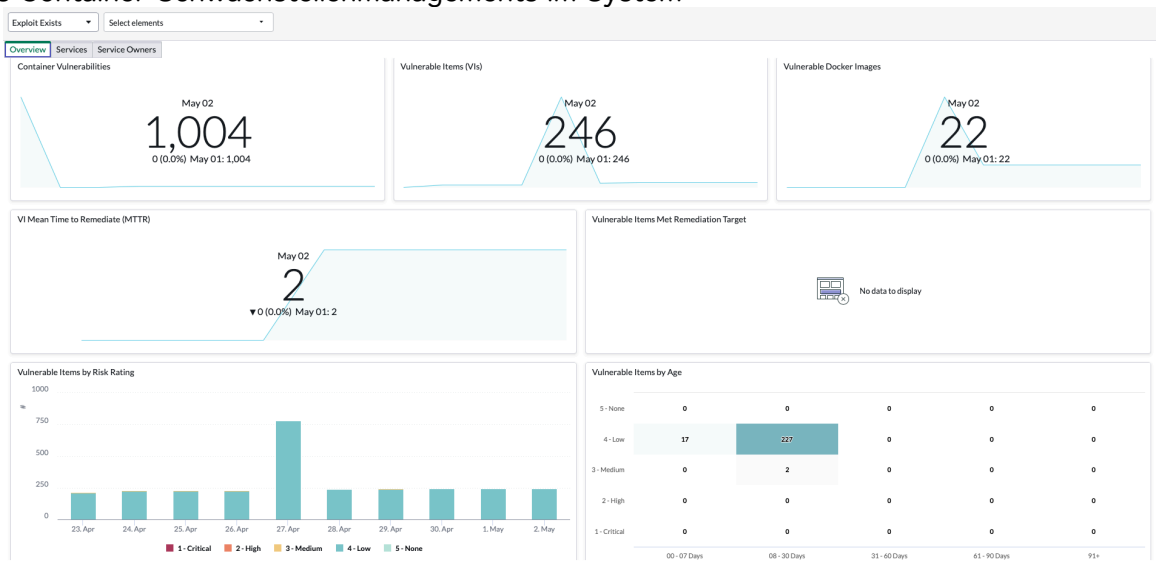
- Wenn Sie ein neuer Benutzer sind, können Sie die Dashboards nur in den -Arbeitsbereichen anzeigen.
- Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Registerkarten für Container-Schwachstellenmanagement

Mit diesem Dashboard können Sie die Schwachstellen anzeigen, die in Containern vorhanden sind. Sie können die Schwachstellen und die zugehörigen Daten nach Region, Alter, Services und anderen Aufgliederungen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

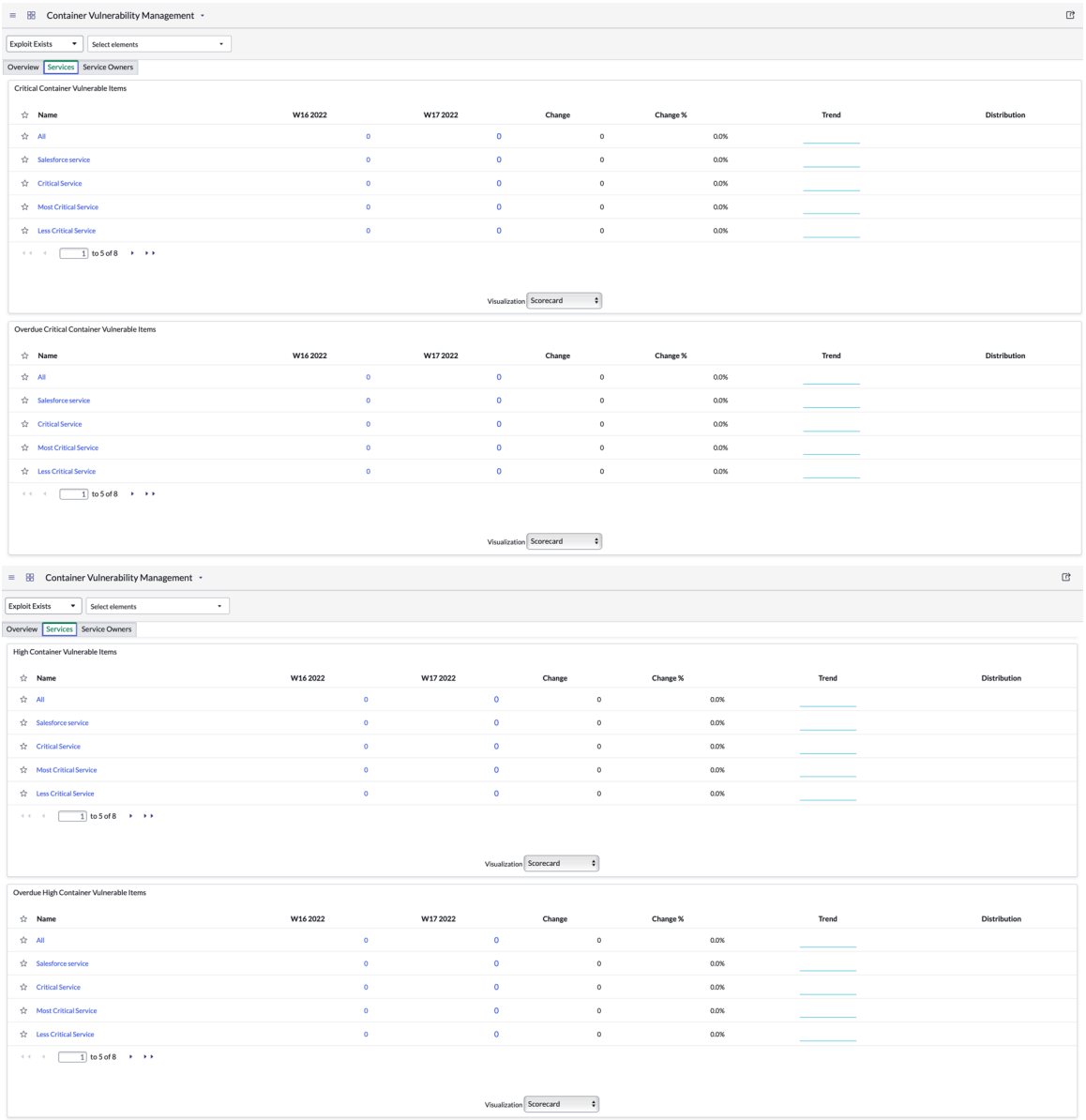
Die Registerkarte **„Übersicht“** zeigt den Gesamtstatus des Container-Schwachstellenmanagements im System an.



Auf der Registerkarte **„Services“** werden angreifbare Container-Elemente angezeigt, die sich auf Anwendungsservices auswirken.

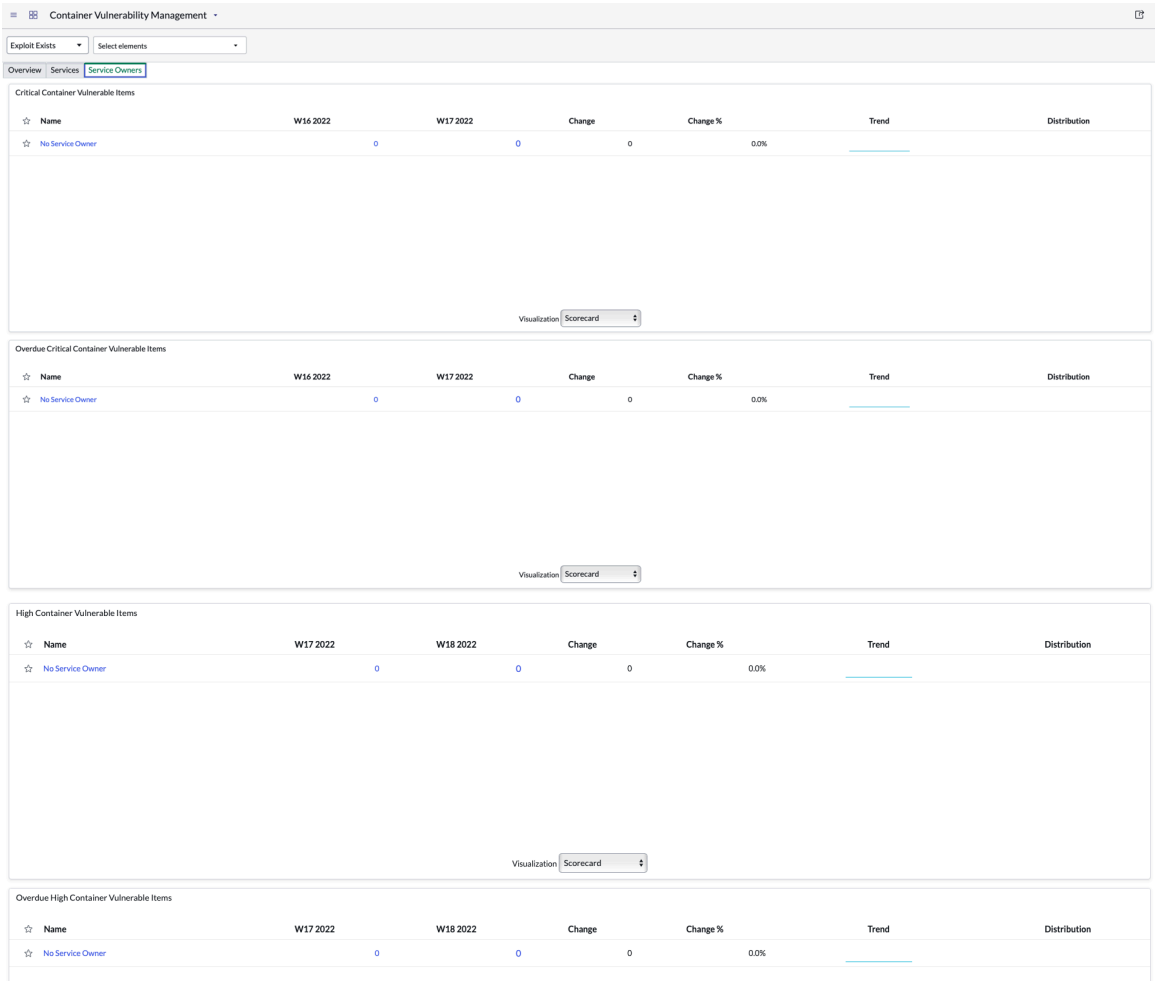
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Registerkarte **„Serviceverantwortliche“** werden angreifbare Container-Elemente angezeigt, die sich auf Serviceverantwortliche auswirken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aufgliederungen

- Exploit vorhanden
- Exploit-Angriffsvektor
- Exploit-Kompetenzniveau
- Nachbesserungszielstatus
- Risikobewertung
- Status
- Zuweisungsgruppe

Automatische Übersetzung

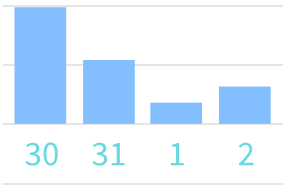
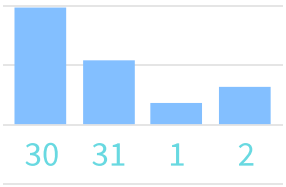
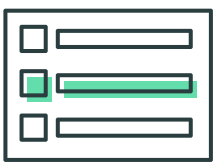
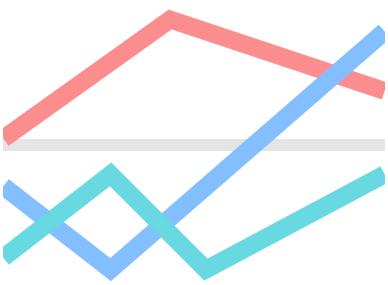
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen

Name	Typ	Beschreibung
Container-Schwachstellen	Einzelwert	Anzahl der Container-Schwachstellen, die mit einem oder mehreren aktiven angreifbaren Container-Elementen verknüpft sind.
Angreifbare Elemente (AEs)	Einzelwert	Anzahl der aktiven (nicht geschlossener) angreifbaren Containerelemente.
Angreifbare Docker-Images	Einzelwert	Anzahl der Docker-Images, die mit aktiven angreifbaren Container-Elementen verknüpft sind.
Durchschnittliche Zeit bis zur Korrektur (MTTR) für AEs	Einzelwert	Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements, angezeigt als laufender 30-Tage-Durchschnitt.
Angreifbare Elemente mit erfülltem Korrekturziel	Einzelwert	Prozentsatz der geschlossenen angreifbaren Container-Elemente, deren Nachbesserungszieldaten im aktuellen und vorherigen Quartal eingehalten wurden. Korrekturziele werden aus dem Datum von „Zuletzt geöffnet“ plus der Anzahl der Tage berechnet.

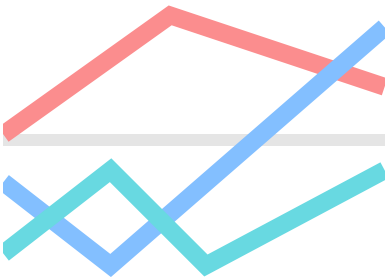
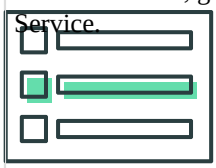
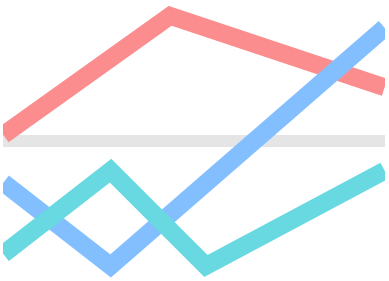
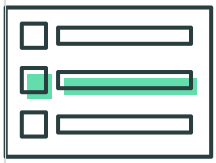
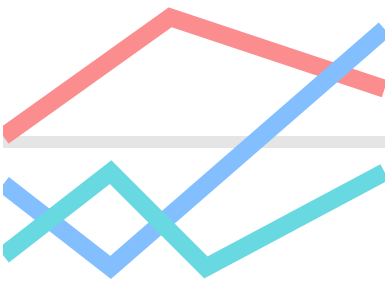
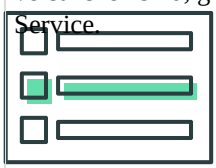
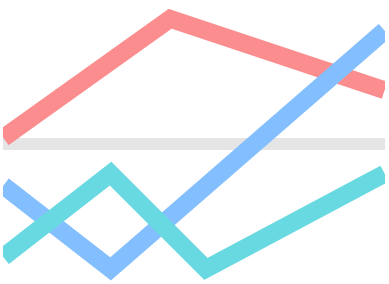
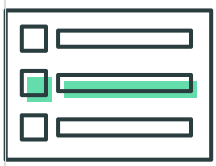
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Angreifbare Elemente nach Risikobewertung	 Leiste	Anzahl der aktiven angreifbaren Container-Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne.
Angreifbare Elemente nach Alter	 L	Anzahl der aktiven angreifbaren Container-Elemente, gruppiert nach Risikobewertung und Alter (in Tagen). **Hinweis:** Das Anpassen des Alters und der Berechnung des Alters der angreifbaren Elemente in Containern kann zu einem starken Anstieg oder Rückgang der PA-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von „Alter“ und „Alter geschlossen für CVIs“ finden Sie im KB-Artikel KB1703270 .
Kritische angreifbare Container-Elemente	Listen- und  	Anzahl der aktiven angreifbaren Container-Elemente mit kritischer Risikobewertung, gruppiert nach Service.

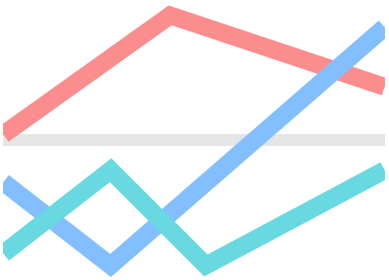
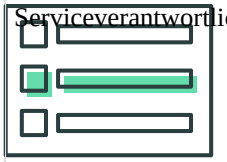
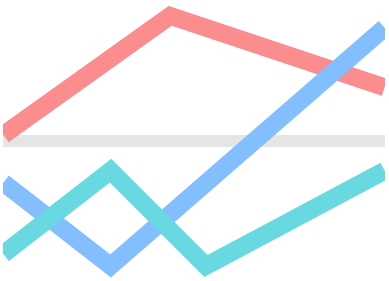
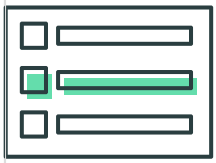
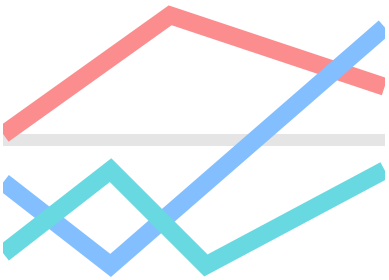
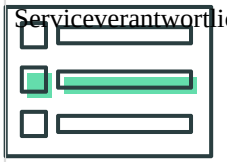
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Überfällige kritische angreifbare Container-Elemente	Liste und  	Anzahl der aktiven angreifbaren Container-Elemente mit kritischer Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Service.
Hoch angreifbare Container-Elemente	Liste und  	Anzahl der aktiven angreifbaren Container-Elemente mit hoher Risikobewertung, gruppiert nach Service.
Überfällige, hoch angreifbare Container-Elemente	Liste und  	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Service.
Kritische angreifbare Container-Elemente	Liste und  	Anzahl der aktiven angreifbaren Container-Elemente mit kritischer Risikobewertung, gruppiert nach Serviceverantwortlichem.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Überfällige kritische angreifbare Container-Elemente	Liste und 	Anzahl der aktiven angreifbaren Container-Elemente mit kritischer Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Serviceverantwortlichem. 
Hoch angreifbare Container-Elemente	Liste und 	Anzahl der aktiven angreifbaren Container-Elemente mit hoher Risikobewertung, gruppiert nach Serviceverantwortlichem. 
Überfällige, hoch angreifbare Container-Elemente	Liste und 	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, deren Nachbesserungszieldaten verstrichen sind, gruppiert nach Serviceverantwortlichem. 

Automatische Übersetzung

Framework für zusammengefasste Berichte für Container Vulnerability Response

Mit dem Framework für aggregierte Berichte können Sie Berichte für die Daten erstellen, die komplexe und zeitaufwändige On-the-fly-Abfragen beinhalten, um eine bessere Leistung zu erzielen.

Das Framework für aggregierte Berichte verbessert die Leistung durch:

- Ressourcenverbrauch und Berichte werden schneller erstellt,
- die Daten zusammenzufassen und Zusammenfassungen und Aufgliederungen wiederzuverwenden (Gruppieren nach) und
- Dadurch werden weniger Abfragen an die Datenbank durchgeführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie mehr als eine Million angreifbare Container-Elemente (Container Vulnerable Items, CVITs) haben, verwenden Sie zusätzlich zu den Standardberichten das Framework für aggregierte Berichte.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- Now Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics -Administrator (pa_admin): Zusammenfassungen, Widgets und Dashboards überprüfen Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- VR-Lesevorgang (sn_vul_cmn.read): Überprüfen Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- Schwachstellenanalyst (sn_vul.vulnerability_analyst): Aggregierte Ergebnisse überprüfen.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Container Vulnerability Response – Referenz

Referenzthemen, die Informationen zu Tabellen, Rollen und Eigenschaften enthalten, die mit Container Vulnerability Responseinstalliert werden.

Mit Container Vulnerability Response installierte Komponenten

Bei der Aktivierung der Anwendung Container Vulnerability Response werden mehrere Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und regelmäßige Aufgaben.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Ab v2.11 von Container Vulnerability Responsesind die am häufigsten verwendeten Systemeigenschaften jetzt in der Anwendung Container Vulnerability Response zugänglich. Um diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Container Vulnerability Response**Eigenschaften**.

Mit Container Vulnerability Response installierte Rollen

Rollen werden bei der Aktivierung von Container Vulnerability Response hinzugefügt.

Es sind Persona-Rollen und granulare Rollen verfügbar, mit denen Sie verwalten können, was Benutzer und Gruppen in der Anwendung Vulnerability Response sehen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Hinweis:

Wenn Sie ein Upgrade-Kunde sind, hat sich der Zugriff für die Benutzer und Gruppen, die Sie mit den Berechtigungen sn_vul.vulnerability_read und sn_vul.vulnerability_write vor v10.3 zugewiesen haben, nicht geändert. Anwendern und Gruppen bleiben diese Rollen zugewiesen, bis Sie sie ändern. Ab v10.3 können Sie jedoch granulare Rollen zuweisen, um mehr Kontrolle darüber zu haben, was Benutzer und Gruppen in der Anwendung Vulnerability Response tun und sehen können. Eine Übersicht und weitere Informationen über die Verwaltung dieser Rollen finden Sie unter Vulnerability Response Personae und granulare Rollen und Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Rollentitel [Name]	Beschreibung
V2.10: sn_vul_container.delete	Löscht Quelldatensätze. Enthält die Rollen sn_vul_cmn.delete und sn_vul_container.delete_vi.
sn_vul_container.ci_manager	Verwaltet die erneute Klassifizierung abgeglichenen Configuration Items
sn_vul_container.configure_integrations	Konfiguriert Container-Integrationen
sn_vul_container.configure_vi_granularity	Konfiguriert die Granularität angreifbarer Container-Elemente
sn_vul_container.create_vi	Kann angreifbare Elemente in Containern manuell erstellen.
sn_vul_container.delete_vi	Kann angreifbare Container-Elemente löschen, die manuell erstellt wurden.
sn_vul_container.exception_approver	Genehmigt Ausnahmen, Zurückstellungen und Schließungen von angreifbaren Containerelementen. Enthält die Rolle „sn_vul.view_manager_work Ab v2.3 wurde die granular sn_vul_container.read_all fü Rolle entfernt, sodass Sie a Ihnen und Ihrer Gruppe zug angreifbaren Container-Ele Korrekturaufgaben zugreife anstatt auf alle angreifbare Elemente und Korrekturauf
sn_vul_container.false_positive_approver	Genehmigt oder lehnt das Schließ angreifbaren Container-Elemente positiv ab. Enthält die Rolle sn_vul.view_manager_works

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
sn_vul_container.manage_assignment_rules	Definiert und aktualisiert Zuweis angreifbare Container-Elemente.
sn_vul_container.manage_auto_close_stale_vi	Konfigurieren Sie, dass veraltete Container-Elemente automatisch werden
sn_vul_container.manage_auto_exception_rule	Ausnahmeregeln verwalten (erste aktualisieren/löschen).
sn_vul_container.manage_normalized_severity	Kann die Zuordnung aktualisiere Schweregrad zu normalisieren.
sn_vul_container.manage_permissions	Kann Anwendern Container-Vuln Response-Rollen zuweisen.
sn_vul_container.manage_remediation_targ…	Definiert und aktualisiert Contain Korrekturzielregeln.
sn_vul_container.manage_risk_score_configur...	Definiert und aktualisiert Risikop Rechner, Risikoregeln und Schw Rollup-Rechner für angreifbare C Elemente.
sn_vul_container.read_all	Kann alle angreifbaren Container zugehörigen Informationen anzei Enthält die Rolle sn_vul.view_manager_works
sn_vul_container.read_assigned	Kann angreifbare Container-Elem oder Ihren Gruppen zugewiesen s der klassischen Anwenderoberflä Remediation Workspace anzeigen Enthält die Rolle sn_vul.view_rem_workspace **Wichtig:** Ab v24.0 von Vulnerability die Rolle sn_vul_container.r die Berechtigung zum Zugri Remediation Workspace.
sn_vul_container.read_assignment_rules	Kann Zuweisungsregeln für angr Container-Elemente anzeigen.
sn_vul_container.read_auto_exception_rule	Ausnahmeregeln für das Lesen
sn_vul_container.read_discovered_image	Kann erkannte Elemente anzeige
sn_vul_container.read_integrations	Kann Ergebnisse von Integration anzeigen.
sn_vul_container.read_normalized_severity	Kann die normalisierte Schwereg anzeigen.
sn_vul_container.read_remediation_target...	Kann Korrekturzielregeln anzeig

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
sn_vul_container.read_risk_score_configu...	Kann Risikopunktzahl-Rechner, und Schwachstellen-Rollup-Rech angreifbare Container-Elemente
sn_vul_container.remediation_owner	Liest und schreibt angreifbare Co Elemente, die ihnen zugewiesen Schwachstellen-Datensätze könn einem Benutzer mit dieser Rolle
sn_vul_container.update_assigned_to	Kann die Zuweisung von ar Container-Elementen aktua Erfordert sn_vul_container. sn_vul_container.write_assi
sn_vul_container.update_assignment_group	Kann Zuweisungsgruppe fü Container-Elemente aktualis Erfordert sn_vul_container. sn_vul_container.write_assi
sn_vul_container.update_state	Kann Status von angreifbar Elementen aktualisieren. Erfordert sn_vul_container. sn_vul_container.write_assi
sn_vul_container.vulnerability_admin	Konfiguriert alle Regeln, integrat das Produkt Container Vulnerabi
sn_vul_container.vulnerability_analyst	Überwacht die Korrektur aller an Container-Elemente.
sn_vul_container.write_all	Kann alle angreifbaren Container Korrekturaufgaben aktualisieren.
sn_vul_container.write_assigned	Kann angreifbare Container-Elem Korrekturaufgaben aktualisieren, meinen Gruppen zugewiesen sind
sn_vul_container.read_watch_topic	Kann Überwachungsthemen für Schwachstellen lesen.
sn_vul_container.create_watch_topic	Kann Überwachungsthemen für Schwachstellen erstellen.
sn_vul_container.edit_watch_topic	Kann Überwachungsthemen für Schwachstellen bearbeiten.
sn_vul_container.manage_exception_configuration	Kann Konfigurationen für die Ausnahmeverwaltung verwalten.

Mit Container Vulnerability Response installierte Tabellen

Tabellen werden bei der Aktivierung von Container Vulnerability Response (CVR) hinzugefügt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Container-Image-Ergebnis sn_vul_container_image_findings	Speichert Informationen zu den zugeordneten Schwachstellen, der Image-Ebene, dem Docker-Image, dem Image-Repository und dem erkannten Image. Ab v2.11.3 von Container Vulnerability Responsekönnen Sie auch den Pfad anzeigen, in dem das Ergebnis angezeigt wird.
Container-Image-Ebene sn_vul_container_image_layer	Enthält die Informationen jeder Bildebene. Ein Image ist eine statische Datei mit ausführbarem Code, die einen Container auf einem Computersystem erstellen kann.
Container-Image-Paket sn_vul_container_image_package	Stellt Informationen zu den Paketen bereit, in denen die Schwachstellen vorhanden sind. Die Details des Binärpakets werden auch als kommagetrennter Wert angegeben. Ab v2.11.3 von Container Vulnerability Responsekönnen Sie auch die Paket-URL (PURL) anzeigen.
Angreifbares Container-Element sn_vul_container_image_vulnerable_item	Enthält Details zu jedem Ergebnis und zur entsprechenden Schwachstelle. Ab v2.11.3 von Container Vulnerability Responsekönnen Sie auch Informationen zum Datum des letzten Scans eines Image anzeigen, das als Container ausgeführt wird.
Schwachstelleneintrag (v2.11.3) sn_vul_entry	Stellt Informationen über den Schweregrad eines CVE und alle zusätzlichen Informationen bereit, die von Prisma gesendet werden.
Erkanntes Containerimage sn_vul_container_image	Stellt Informationen zur Image-ID, zum Docker-Image und zum Image-Repository bereit. Außerdem werden die Ebeneninformationen gespeichert und dem erkannten Image zugeordnet. Ab v2.11.3 von Container Vulnerability Responsebietet sie auch Informationen zum Image-Digest eines Docker-Images und zum Datum des letzten Scans eines Image, das als Container und als Registry ausgeführt wird.
Ergebniszuordnungen sn_vul_container_finding_m2m_vul_item	M2M-Beziehung der Container-Image-Ergebnisse und der angreifbaren Container-Elemente (CVITs).
Angreifbare Elemente automatisch schließen sn_vul_container_image_auto_close_config	Enthält Informationen zum Schließen der veralteten Container-Image-Ergebnisse und zum Rollup des Status für die CVITs.
Container-Image-Schwachstellenschlüssel sn_vul_container_image_vulnerability_keys	Enthält die Granularitätskonfiguration für die Erstellung von CVITs aus den Container-Image-Ergebnissen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Docker-bezogene Services sn_vul_container_m2m_ci_services	Enthält alle Business-Services, die sich auf ein Containerimage beziehen.
Anzahlen der VR-Container sn_vul_container_vr_container_counts	Enthält den gleitenden Durchschnitt der Containerinstanzen, die in den letzten 90 Tagen aus einem Containerimage hervorgegangen sind.
Element der Container-Korrekturaufgabe sn_vul_container_m2m_vul_group_item	M2M-Tabelle zwischen CVIT und Container-Korrekturaufgaben.
Container-Korrekturaufgabe sn_vul_container_vulnerability	Enthält Container-Korrekturaufgaben.
Container-Korrekturaufgabe – Manifest sn_vul_container_rt_manifest	Alle Aktualisierungen der Korrekturaufgabe werden mithilfe dieser Manifesttabelle durch geplante Aufgaben durchgeführt.

Mit Container Vulnerability Response installierte regelmäßige Aufgaben

Regelmäßige Aufgaben werden bei der Aktivierung von Container Vulnerability Response hinzugefügt.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Geplante Aufgabe	Beschreibung
Ordnen Sie vorhandene Container-VIs der automatischen Ausnahmeregel zu	Ordnet die automatische Ausnahmeregel automatisch vorhandenen angreifbaren Container-Elementen (CVITs) zu.
Überprüfen Sie den Ablauf der Zurückstellung des angreifbaren Container-Elements	Sendet Benachrichtigungen, wenn angreifbare Container-Elemente oder Container-Schwachstellen abgelaufen sind (und wenn sie in einer Woche ablaufen).
Anzahl der Vulnerability Response-Container (Anwendung – Vulnerability Response und Configuration Compliance für Container)	Wird täglich ausgeführt, um die Tabelle sn_vul_container_vr_container_counts zu füllen, die den gleitenden 90-Tage-Durchschnitt für Container berechnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
CVITs automatisch schließen	Schließt automatisch angreifbare Container-Elemente, die der in der Konfiguration für das automatische Schließen definierten Bedingung entsprechen. Ihr Status wird in „behoben“ geändert.
Geschäftsrelevanz für CVIT berechnen	Verarbeitet alle aktiven CVITs und aktualisiert das Feld Business-Relevanz basierend auf den betroffenen Services des Docker-Images des CVIT.
Abbrechen von CVITs schließen, denen kein Docker-Image zugeordnet ist	CVITs, denen kein CI zugeordnet ist, lassen automatisch ablaufen. Ihr Status wird auf „Geschlossen“ und ihr Substatus auf „Abgebrochen“ festgelegt.
Berechnen Sie die zugehörigen VI-Anzahlen für die Container-Korrekturaufgabe	Berechnet die Anzahl der Datensätze für Container-Korrekturaufgaben.
Rollup der Werte von angreifbaren Container-Elementen zu Schwachstelle und Gruppe	Berechnet Schwachstellen und Gruppen-Rollups für angreifbare Container-Elemente. **Hinweis:** Ab v2.10 von Container Vulnerability Responsewird die geplante Aufgabe erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade beinhaltet die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.

Container Vulnerability Response -Glossar

Erfahren Sie mehr über Begriffe und Konzepte, die für Container Vulnerability Responseeindeutig sind.

Wichtige Begriffe

Behälter

Eine Softwareeinheit, die den Code und alle zugehörigen Abhängigkeiten so paketiert, dass die Anwendung nahtlos und zuverlässig von einer Computerumgebung in eine andere ausgeführt wird.

Containerimage

Eine statische Datei mit ausführbarem Code, die einen Container auf einem Computersystem erstellen kann. Ein Containerimage kann nicht geändert und daher in jeder Umgebung konsistent bereitgestellt werden.

Cluster

Eine Reihe von Worker-Computern, die als Knoten bezeichnet werden und containerisierte Anwendungen ausführen.

Docker

Software zum Erstellen, Bereitstellen und Verwalten von Anwendungscontainern auf Servern und in der Cloud.

Docker-Bild

Eine Vorlagendatei, die Code, erforderliche Bibliotheken, Konfigurationen usw. enthält. Die Datei wird zum Starten von Containerinstanzen verwendet. Es besteht aus einer Vereinigung von geschichteten Dateisystemen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Docker-Datei

Eine Textdatei mit Anweisungen zum Erstellen von Containerbildern durch Hinzufügen mehrerer Ebenen. Zum Beispiel die Schichtung von Basiscode für Ubuntu, Nginx und App.

Docker Compose

Ein Tool zum Definieren und Ausführen komplexer Anwendungen mit Docker. Mit Compose können Sie eine Anwendung mit mehreren Containern in einer einzigen Datei definieren.

Docker-Container

Ein Docker-Container ist eine Laufzeitinstanz, die von einem Docker-Image gestartet wird.

Image-Ebene

Eine Ebene ist eine Änderung an einem Bild. Sie wird durch eine Anweisung in der Docker-Datei dargestellt. Ebenen werden nacheinander auf das Basisimage angewendet, um das endgültige Image zu erstellen.

Image-Repository

Eine Sammlung von Docker-Images mit unterschiedlichen Tags oder Versionen.

Bildbezeichnungen

Ein Satz von Schlüssel-Wert-Paaren, die mit dem Bild als Metadaten gespeichert werden.

Namespace

Eine von Kubernetes verwendete Abstraktion zur Unterstützung der Isolierung von Ressourcengruppen innerhalb eines einzelnen Clusters.

Pod

Eine Reihe von ausgeführten Containern (eine andere Abstraktion über einem Container).

Registrierung

Ein gehosteter Service, der Repositorys mit Images enthält.

Service

Eine abstrakte Methode, um eine Anwendung, die auf einer Reihe von Pods ausgeführt wird, als Netzwerkdienst verfügbar zu machen.

Tag

Ein Tag ist eine Bezeichnung, die auf ein Docker-Image in einem bestimmten Image-Repository angewendet wird. Tags sind die Art und Weise, wie verschiedene Images in einem Repository voneinander unterschieden werden.

Formularfelder „Angreifbares Container-Element“.

Angreifbare Container-Elemente (Container Vulnerability Items, CVITs) werden während des Imports von Drittpartei-Schwachstellenintegrationen automatisch erstellt.

Formularfelder „Angreifbares Container-Element“.

Mit Ausnahme der Felder **Zuweisungsgruppe**, **Zugewiesen an** und **Notizen**sind alle anderen Felder in CVIT schreibgeschützt.

Feld	Beschreibung
Nummer	Automatisch generierter CVIT-Bezeichner für diesen Datensatz.
Quelle	Scanner, der die Schwachstelle identifiziert hat.
Risikobewertung	Quantifizierte **Risikopunktzahl,** die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Risikopunktzahl	Berechnetes Risiko, das CVIT für Ihre Umgebung darstellt.
Korrekturzielregel	Korrekturzielregel, nach der das Korrekturzieldatum berechnet wird.
Korrekturziel	Datum, bis zu dem die CVITs nachgebessert werden sollen, ab der ersten Identifizierung. Wird nur angezeigt, wenn zutreffend.
Korrekturstatus	Status der Korrektur für CVIT.
Schwachstelle	ID der Schwachstelle, die diesem angreifbaren Anwendungselement zugeordnet ist.
Docker-Bild	Vorlagendatei, die Code, erforderliche Bibliotheken, Konfigurationen usw. enthält. Die Datei wird zum Starten von Containerinstanzen verwendet. Es besteht aus einer Vereinigung von geschichteten Dateisystemen.
Erkanntes Container-Image	Eindeutiger Datensatz für jede Image-ID.
Basis-Image	Ein grundlegendes Image zum Erstellen von containerisierten Anwendungen, das das wichtige Betriebssystem und die wichtigsten Bibliotheken enthält. Sie dient als Ausgangspunkt zum Erstellen und Anpassen von Anwendungen in Umgebungen wie Docker.
Image-Cluster	Gruppen zusammengehöriger Images, die in verschiedenen Kontexten verwendet werden, z. B. zur Gruppierung ähnlicher Images in maschinellem Lernen oder von Container-Images in einem Repository.
Image-Namespace	Wird zum Organisieren und Isolieren von Containerbildern in einer Registrierung verwendet, sodass verschiedene Teams oder Projekte separate Sammlungen verwalten können.
Status	Dieses Feld wird bei der Erstellung standardmäßig auf **Öffnen** festgelegt. Weitere Informationen zur Zuordnung von Status finden Sie unter Status des angreifbaren Elements in der Anwendung (Application Vulnerable Item, AVI)..
Zuweisungsgruppe	Gruppe für die Bearbeitung dieses CVIT ausgewählt.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an diesem CVIT arbeitet. Können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Erstellt	Datum und Uhrzeit der Erstellung einer CVIT.
Zuletzt geöffnet	Spätestes Datum und Uhrzeit für die erneute Öffnung der CVIT.
Aktualisiert	Datum und Uhrzeit der letzten Änderung der CVIT.
Zuerst gefunden (v2.12.1)	Datum, an dem die Schwachstelle zuerst gefunden wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit der ersten Erkennung anzeigen, um für Übersichtlichkeit zu sorgen und verschiedene Zeitzonen zu berücksichtigen. Um die ersten gefundenen Datums- und Uhrzeitdetails auszufüllen, muss die Integration erneut ausgeführt werden.
Zuletzt gefunden (v2.12.1)	Datum, an dem die Schwachstelle zuletzt gefunden wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit des letzten Funds anzeigen, um für Übersichtlichkeit zu sorgen und verschiedene Zeitzonen zu berücksichtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Um die Details zu zuletzt gefundenem Datum und Uhrzeit auszufüllen, muss die Integration erneut ausgeführt werden.
Datum der Lösung (v2.12.1)	Datum, an dem die Schwachstelle gelöst wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit der Lösung des Problems anzeigen, um für Übersichtlichkeit zu sorgen und verschiedene Zeitzonen zu berücksichtigen. Das Lösungsdatum wird gefüllt, wenn die CVIT als Teil des Workflows gelöst wird.
Zuletzt geöffnet (v2.12.1)	Datum, an dem die Schwachstelle zuletzt geöffnet wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit der letzten Öffnung anzeigen, um für Übersichtlichkeit zu sorgen und verschiedene Zeitzonen zu berücksichtigen. Die geplante Aufgabe *`Add default values for last_opened_dt_tm from last _opened`* füllt die Daten in diesem Feld aus. Er darf nur einmal bei Bedarf ausgeführt werden.
Schwachstelle	
Zusammenfassung	Beschreibung der Schwachstelle.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle Schweregradzuordnungen werden für die National Vulnerability Database (NVD) und für ServiceNow-Drittparteiintegrationen bereitgestellt.
Schwachstellenpunktzahl (v3)	Punktzahl des Common Vulnerability Bewertungssystems (CVSS) v3.
Schwachstellenpunktzahl (v2)	CVSS v2-Punktzahl.
Exploit vorhanden	Ja, wenn mindestens ein Exploit den Schwachstellen zugeordnet ist, die diesem angreifbaren Element zugeordnet sind.
Exploit-Angriffsvektor	Angreifbarster Angriffsvektor der Exploits für die Schwachstellen, die diesem angreifbaren Element zugeordnet sind.
Exploit-Kompetenzniveau	Niedrigste Kompetenzebene, die zum Ausnutzen der mit diesem angreifbaren Element verbundenen Schwachstellen erforderlich ist.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Bedrohung	Relevante Informationen zur Bedrohung. Aus dem angreifbaren Eintragsdatensatz abgerufen. **Hinweis:** Alle hier vorgenommenen Änderungen aktualisieren den Datensatz des angreifbaren Eintrags.
Korrekturhinweise	Relevante Lösung für die Bedrohung, abgerufen aus dem Datensatz des angreifbaren Eintrags.
Notizen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Arbeitsnotizen	Alle relevanten Informationen. Wählen Sie das Textfeld für Arbeitsnotizen aus, um Informationen hinzuzufügen.
Bildergebnisse	Ergebnisse der Überprüfung von Container-Images auf Schwachstellen.
Angeforderte Genehmigungen	Genehmigungsanforderung für CVIT ausgelöst.
Genehmigungen der Statusänderung	Anforderung von Statusänderungsgenehmigungen für CVIT ausgelöst.

Berechnungen des Alters einer CVIT:

- Die Spalte „Alter“ in der Liste der CVITs zeigt an, wie lange (Format: Tage HH:MM:SS) eine CVIT aktiv ist. Der Wert für das Alter ist für eine geschlossene CVIT 0.
- Die Spalte Alter geschlossen in der Liste CVITs zeigt an, wie lange (Format: Tage HH:MM:SS) ein CVIT aktiv ist, bevor er geschlossen wird. Für CVITs, die sich nicht im Status „Geschlossen“ befinden, ist der Wert „Alter geschlossen“ 0.

Weitere Informationen zum Anpassen der Berechnung des Alters und der Schließdauern finden Sie im Artikel KB1703270 .

Formular „Prisma-Cloud-Computing-Konfiguration“

Auf das Formular „Prisma-Cloud-Computing-Konfiguration“ kann innerhalb des Moduls „Prisma-Cloud-Computing-Integration“ zugegriffen werden.

Um das Formular „Prisma-Cloud-Computing-Konfiguration“ anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**.

Konfiguration des Prisma-Cloud-Computings

Feld	Beschreibung
Integrationsinstanz	Name der neuen Integrationsinstanz. Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen.
API-Basis-URL	URL für die Integration mit Prisma Cloud Compute.
Anwendername	Anwendername für den Zugriff auf Prisma Cloud Compute.
Passwort	Passwort für den Zugriff auf Prisma Cloud Compute.
MID-Server	Eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. Der MID-Server ermöglicht die Kommunikation und die Bewegung von Daten zwischen einer Instanz ServiceNow und externen Anwendungen, Datenquellen und Services.
Projekte verwenden	Option zum Konfigurieren der -Projekte. Wenn Sie das Kontrollkästchen aktivieren, können Sie Projekte auf der Konfigurationsseite auswählen und die Integrationen basierend auf den konfigurierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration des Prisma-Cloud-Computings (Fortsetzung)

Feld	Beschreibung
	Projekten ausführen, um projektspezifische Details auszufüllen. **Hinweis:** Wenn dieses Kontrollkästchen aktiviert ist, wird die Registerkarte **Projekte konfigurieren** aktiviert. Klicken Sie **auf Weiter**, um mit der Konfiguration der Projekte fortzufahren.

Formular „Ausnahme anfordern“.

Fordern Sie mit der Funktion zur Verwaltung von Richtlinienausnahmen GRC in der Anwendung Richtlinien- und Compliance-Management innerhalb von Container Vulnerability ResponseRichtlinienausnahmen an.

Um das Formular „Prisma-Cloud-Computing-Konfiguration“ anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** (oder **Korrekturaufgaben**) >**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Richtlinie	Richtlinie für Schwachstellenmanagement, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und wann der Status des angreifbaren Elements oder der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ wechselt. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)**, die Sie für die Richtlinie in Richtlinien und Compliance festgelegt haben, nicht überschreiten. Weitere Informationen finden Sie unter Richtlinie erstellen .
Grund	Grund für das Anfordern einer Ausnahme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahme anfordern“. (Fortsetzung)

Feld	Beschreibung
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Remediation ausgefüllt werden.

Formular „Ausnahmeregel“.

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe von angreifbaren Elementen in Containern (CVITs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser CVITs basiert. Mit dieser Regel können Sie neue und vorhandene CVITs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

Um das Formular „Ausnahmeregel“ anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.

Formular „Ausnahmeregel“.

Feld	Beschreibung
Name	Name der Ausnahmeregel.
Gültig ab	Datum, ab dem diese Regel aktiv ist, um die CVITs zurückzustellen.
Gültig bis	Datum, ab dem die Korrekturaufgabe keine neuen CVITs mehr akzeptiert.
Grund	Grund für die Erstellung dieser Ausnahmeregel.
Zuweisungsgruppe	Gruppe, der die Korrekturaufgabe zugewiesen ist, die für die Nachverfolgung der zurückgestellten CVITs erstellt wurde.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen.
Bedingung	Filterbedingung für die CVITs, die während der Verarbeitung der CVITs definiert werden kann.
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für bereits vorhandene Daten ausführen können.
Workflow-Phase	Aktueller Genehmigungsstatus der Ausnahmeregel.
Status	Status der Ausnahmeregel.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel.
Zurückgestellt bis	Datum, bis zu dem die VULs und CVITs zurückgestellt werden. An diesem Datum wird die erstellte VUL geschlossen, alle CVITs werden aus der Gruppe entfernt, und Gruppenregeln werden erneut angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

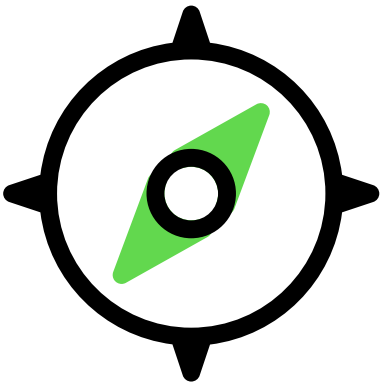
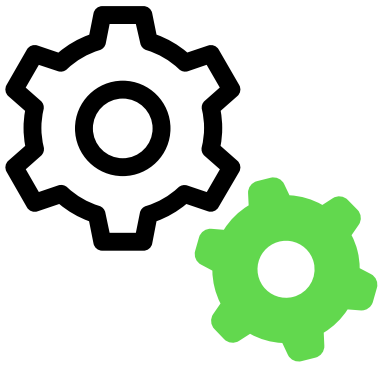
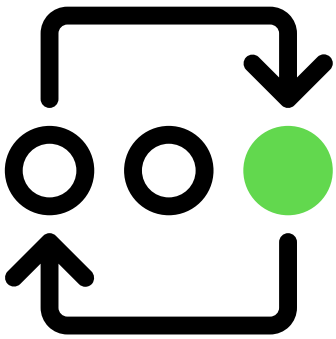
Konfigurations-Compliance

Die Anwendung ServiceNow® Konfigurations-Compliance ist eine Secure Configuration Assessment-Anwendung (SCA), die Scan-Ergebnisse aus Integrationen mit Konfigurations-Scan-Anwendungen von Drittanbietern aggregiert. Sie können Konfigurations-Compliance-Probleme mit Configuration Management Database (CMDB)priorisieren. Konfigurations-Compliance ist eng in den IT-Change-Management-Prozess integriert, um Ihre nicht konformen Konfigurationen zu korrigieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Konfigurations-Compliance

Untersuchen	Einrichtung, Installation und Konfiguration	integrieren
		
Erfahren Sie mehr über die Konzepte und Funktionen von Configuration Compliance	Konfigurations-Compliance konfigurieren	Erweitern Sie die Konfigurations-Compliance durch die Integration mit anderen -Anwendungen

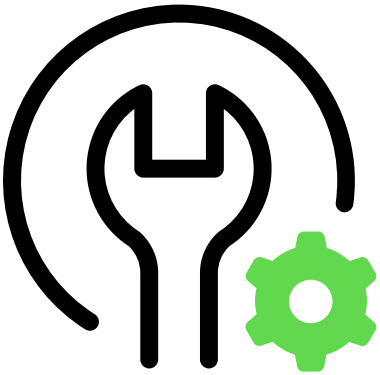
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance (Fortsetzung)

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

Erfahren Sie, wie Konfigurationsprobleme in den Arbeitsbereichen Vulnerability Manager, IT Remediation und Vulnerability Assessment überwacht, verwaltet und behoben werden.

Beheben

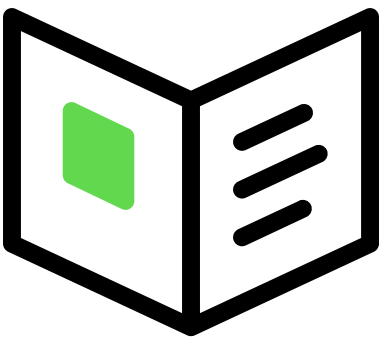


Erfahren Sie, wie Sie Ihre nicht konformen Assets mit Configuration Compliance korrigieren können

Analysen und Berichte

Zeigen Sie Berichte und Dashboards in Configuration Compliance an

Referenz



Rufen Sie Details zu Configuration Compliance-Komponenten wie Feldern, Tabellen und Eigenschaften ab

Automatische Übersetzung

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Konfigurations-Compliance erkunden

Verwenden Sie Testergebnisse aus SCA-Integrationen (Secure Configuration Assessment), um die Compliance mit Sicherheits- oder Unternehmensrichtlinien zu überprüfen. Identifizieren, priorisieren und korrigieren Sie nicht konforme Konfigurationselemente.

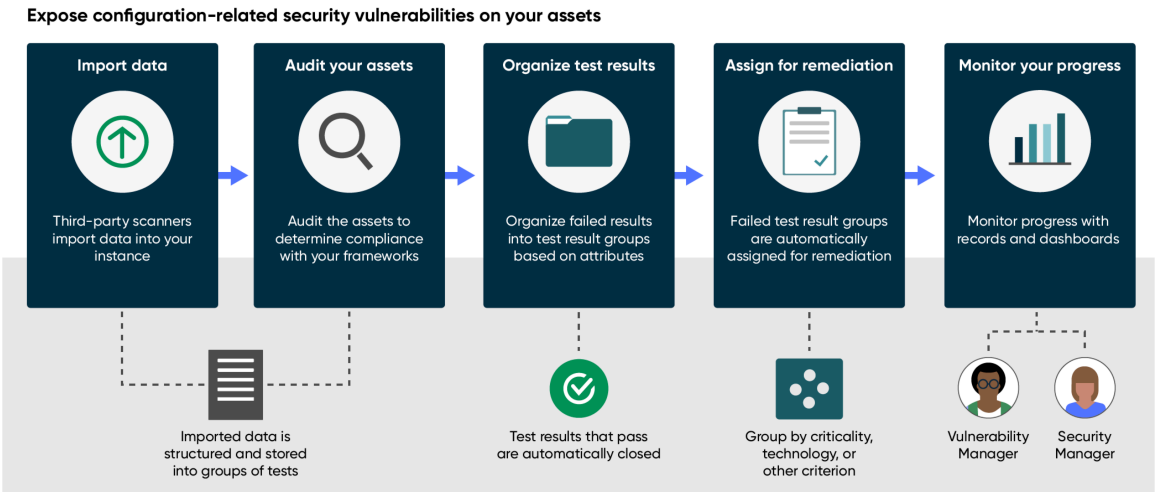
Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Konfigurations-Compliance – Beschreibung

Mit der Anwendung ServiceNow® Konfigurations-Compliance können Sie die kritischsten konfigurationsbezogenen Schwachstellen in Ihrer Umgebung schnell und effizient priorisieren und beheben. Konfigurations-Compliance ist per Abonnement im ServiceNow® Storeverfügbar.



Schlüsselfunktionen von Konfigurations-Compliance

Verwenden Sie Configuration Management Database (CMDB) in Ihrem Now Platform®, um Ihre kritischsten konfigurationsbezogenen Sicherheitsschwachstellen aufzudecken und zu beheben. Konzentrieren Sie Ihre Nachbesserungsressourcen auf Aktivitäten mit der größten Risikoreduzierung. Optimieren Sie den Nachbesserungsprozess für Sicherheits-, IT- und Geschäftsprozess-Stakeholder. Die Anwendung Konfigurations-Compliance enthält die folgenden Schlüsselfunktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit unterstützten Drittanbieterintegrationen werden Richtlinien, Tests, autoritative Quellen und Technologien automatisch importiert. Weitere Informationen zu unterstützten Integrationen finden Sie unter Konfigurations-Compliance-Integrationen.
- Korrelieren Sie Richtlinien und Tests mit Konfigurationselementen (Assets), um konfigurationsbezogene Schwachstellen zu identifizieren und um sicherzustellen, dass Ihre Assets Ihren Richtlinien und Steuerungen entsprechen.
- Vereinheitlichen Sie die Bewertung, Zuweisung und Korrektur der Konfiguration für alle Ihre Assets.
- Inhalte von Konfigurationsscans können aus führenden Secure Configuration Assessment (SCA)-Ökosystemintegrationsanwendungen importiert werden.
- Konfigurationsergebnisse und Testfehler können gruppiert und automatisch basierend auf den Kompetenzen von Korrekturspezialisten und den Verantwortungsbereichen weitergeleitet werden. Intelligente Workflows und die nahtlose Integration mit dem Change-Management sorgen für eine reibungslose Aufgabenübergabe zwischen Gruppen.
- Bei Verwendung mit der Anwendung ServiceNow Governance, Risk und Compliance (GRC) können Konfigurationstests in Konfigurations-Compliance per Rollup zu den entsprechenden GRC-Steuerungen zusammengefasst werden.
- Mit dem erweiterten Change-Management können Sie vorab ausgefüllte Change-Anforderungen für die IT direkt aus Konfigurations-Compliance erstellen, um Sie bei Ihren Korrekturaufgaben zu unterstützen, die zusätzliche Ressourcen erfordern.
- Mit Dashboards können Sie den Korrekturstatusmetriken für Korrekturaufgaben, Compliance-Tests und Richtliniendatensätze anzeigen.

Konfigurations-Compliance – Benutzer

Konfigurations-Compliance An Aktivitäten können viele Managementebenen beteiligt sein.

- Systemadministratoren
- Schwachstellenadministratoren
- Schwachstellenmanager
- Schwachstellenanalysten
- Compliance-Administratoren

Konfigurations-Compliance -Aufgaben betreffen die folgenden Rollen.

- sn_vulc.admin – kann lesen, schreiben, löschen
- sn_vulc.write – kann lesen und schreiben
- sn_vulc.remediation_owner – Kann zugewiesene Datensätze lesen und aktualisieren

Hinweis:
Die Rolle sn_vulc.remediation_owner wird auch automatisch zugewiesen, wenn einem Benutzer die Rolle itil zugewiesen wird.

- sn_vulc.read – kann lesen

Konfigurations-Compliance und Security Operations

Wenn Qualys Vulnerability Integration und Tenable Vulnerability Integration installiert sind, wird der Zugriff auf Vulnerability Response verfügbar. Sie können mehrere Bereitstellungen dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen haben. Daten, die aus den einzelnen Bereitstellungen stammen, werden identifiziert und sind in einer einzigen Instanz von GRCverfügbar.

Verfügbare Versionen für Yokohama

Freigabeversion	Release-Hinweise
Konfigurations-Compliance v15.2	Konfigurations-Compliance – Versionshinweise Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen Weitere Informationen zum Aktivieren der Anwendung finden Sie unter Anwendung Konfigurations-Compliance einrichten, installieren und konfigurieren.

Konfigurations-Compliance importierte Daten

Die Anwendung Konfigurations-Compliance importiert Richtlinien, Tests, autoritative Quellen und Testergebnisse aus Drittanbieterintegrationen und speichert sie in -Modulen zur Ansicht.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Unterstützte Integrationen

Integrationen von Drittparteien importieren Konfigurationsbewertungsergebnisse, Testgruppen, Tests, Technologien, autoritative Quellen und Testergebnisse in die Anwendung Konfigurations-Compliance. Schwachstellenmanager oder Schwachstellenanalysten können diese Daten verwenden, um die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren.

Weitere Informationen zu unterstützten Integrationen finden Sie unter Konfigurations-Compliance-Integrationen.

Testgruppen

Testgruppen beziehen sich auf autoritative Dokumente und Testdatensätze. Eine Gruppe von Konfigurationstests definiert Testgruppen. Testgruppen sind in der Regel an einer Technologieklasse ausgerichtet, z. B. Windows, Oracle Databases, Cisco IOS, und werden häufig vom primären Branchenstandard abgeleitet. Testgruppen können so geändert werden, dass sie den Anforderungen der Organisation entsprechen. Ein einzelner Konfigurationstest kann mehreren Testgruppen angehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
Qualys Vulnerability Integration	Testgruppen werden abgerufen und Kontroll-IDs werden um 1:00 Uhr von der geplanten Aufgabe **„Qualys PC-Richtlinien“** ausgefüllt. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys PC-Richtlinien**. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie zuerst **Qualys PC-Richtlinien** aus.
Tenable Vulnerability Integration	Die regelmäßige Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert Richtlinien. Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Assets Integration • Tenable.io Integration von Compliance-Ergebnissen • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen • Tenable.io Assets Integration • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen Um den Richtliniendatensatz anzuzeigen, navigieren Sie zu **Alle** > **Konfigurations-Compliance** > **Testgruppen**. Um die Datensätze der Testgruppen korrekt zu identifizieren und zu erstellen, werden Audit-Informationen für Testgruppen importiert und im Feld **Kurzbeschreibung** angezeigt.

Tests

Tests sind Bibliotheken mit Datensätzen, die Scans von Computing-Assets organisieren. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets verwaltet werden soll.

Ein Konfigurations-Compliance -Test ist der Mechanismus, den Integrationsanwendungen von Drittanbietern verwenden, um Assets nach Schwachstellentyp zu gruppieren. Einige VA-Scanlösungen von Drittparteien wie Qualys verfügen über sehr große Testbibliotheken (bis zu 8.000), die Richtlinien und „Frameworks“ maßgeblicher Quellen zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Test kann viele Werte haben, Eins-zu-Viele, erwartete vs. tatsächliche Werte usw. Ein Test ist alles, was verwendet werden kann, um eine Klasse von Software- oder Hardware-Assets zu identifizieren, die nicht konform ist. Zum Beispiel eine Release- oder Hardwarenummer.

Integration	Beschreibung
Qualys Vulnerability Integration	Die geplante Aufgabe **Qualys PC-Steuerungen**ruft die Tests ab. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys PC-Steuerungen**. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie **Qualys PC-Steuerungen** nach **Qualys PC-Richtlinien**aus.
Tenable Vulnerability Integration	Die regelmäßige Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert Konfigurationstests (Tests). Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Assets Integration • Tenable.io Integration von Compliance-Ergebnissen • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen • Tenable.io Assets Integration • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen Um den Konfigurationstestdatensatz anzuzeigen, navigieren Sie zu **Konfigurations-Compliance** > **Tests**. Im Datensatz werden importierte Daten im Feld **Kurzbeschreibung** sowie auf den Registerkarten Korrekturstatus, Beschreibung und Korrektur angezeigt. Daten werden auch in den zugehörigen Links **Zitate**, **Richtlinien**und **Testergebnisse** angezeigt.

Technologien

Eine der Techniken, mit denen die Schwachstellenscanner von Drittparteien Testgruppen von Software- und Hardwarekonfigurationselementen zur Analyse erstellen, besteht darin,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sie nach Technologie zu organisieren. Technologien sind eine importierte Bibliothek von Betriebssystemen, Netzwerkgeräten, Datenbanken und Apps, die Richtlinien zugeordnet sind. Tests haben mehrere Implementierungen für verschiedene Technologien. Die Remediation ist auch technologiespezifisch.

Sie können die anwendbaren Technologien für einen Test anzeigen, um besser zu verstehen, auf welche Arten von Software- oder Hardware-Assets die Steuerung angewendet werden kann. Beispiele für Technologien, die auf Steuerelemente angewendet werden können, sind CentOS 7.x, Windows 8.1, Windows 2016 Server usw. Die Liste der Technologien ist schreibgeschützt und entspricht den in der Anwendung Qualys Cloud Platform definierten Technologien.

Technologien werden nur für datenbankbezogene Konfigurationsbewertungen importiert. Das *db_type* (falls nicht leer) im Import wird zum Erstellen einer Technologie verwendet. Zeigen Sie die im Abschnitt „Technologien“ für Konfigurationstestdatensätze, Testergebnisdatensätze, Richtliniendatensätze und unter aufgeführten Technologien an **Konfigurations-Compliance** > **Unterstützungsdaten** > **Technologien**.

Autorisierende Quellen

Konfigurations-Compliance Bei der Generierung von Schwachstellenwarnungen für Tests werden autoritative Quellen und Zitate verwendet. Autoritative Quellen sind normalerweise Abschnitten veröffentlichter Branchenstandards zugeordnet, z. B. „NIST 800-53 Version 3 (2009) 3: 2009, SA-4“.

Hinweis:
In Qualys Vulnerability Integrationwird diese Kombination als Framework bezeichnet.

Autoritative Quellen und Zitate (auch bekannt als Mandate) werden aus den Schwachstellenscannern von Drittparteien importiert.

Datensätze aus autoritativen Quellen enthalten Verweise auf Informationen zu bekannten Software- und Hardware-Konfigurationsproblemen von Experten auf dem Gebiet der Computersicherheit. Sie definieren Anforderungen für Sicherheitsrichtlinien und -verfahren. Konfigurationstests können durch Zitate auf mehrere autorisierende Quellen verweisen. Autoritative Quellen können zur Vorbereitung eines Audits Berichte über die Compliance für einen bestimmten Standard erstellen.

Integration	Beschreibung
Qualys Vulnerability Integration	Die geplante Aufgabe **Qualys PC-Richtliniendetail**ruft die autorisierenden Quellen und Zitate ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys PC-Richtliniendetail**. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie nach **Qualys PC-Richtlinien Detail** für **Qualys-PC-Richtlinien**aus.
Tenable Vulnerability Integration	Die regelmäßige Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert autoritative Quellen als Teil von Zitatdaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
	Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Assets Integration • Tenable.io Integration von Compliance-Ergebnissen • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen • Tenable.io Assets Integration • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen Daten werden unter dem zugehörigen Link **„Zitate“** in Konfigurationstestdatensätzen angezeigt.

Testergebnisse

Konfigurations-Compliance berechnet die Testergebnisse nicht, importiert sie jedoch als Teil einer Drittanbieterintegration. Sobald sie in Konfigurations-Compliancesichtbar sind, werden sie mit **Korrekturaufgaben**korrigiert. Weitere Informationen finden Sie unter Konfigurations-Compliance Korrelation.

Integration	Beschreibung
Qualys Vulnerability Integration	Sie können die Testergebnisse auf eine der folgenden Arten abrufen: Die regelmäßige Aufgabe **Qualys PC-Ergebnisse**ruft die Testergebnisse ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys PC-Ergebnisse**. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie **Qualys PC-Ergebnisse** nach **Qualys PC-Richtlinien** und **Qualys PC-Richtliniendetails**aus. Der Import der **Qualys PC-Ergebnisse** verwendet den Parameter `Start Time` auf der Registerkarte **Integrationsdetails**. Alle anderen Konfigurations-Compliance -Importe übernehmen alle verfügbaren Daten unabhängig von `Start Time`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
	Wenn der Import der **Qualys PC-Ergebnisse** abgeschlossen ist, wird ein Ereignis ausgelöst, um Berechnungen für das Importende auszulösen. Weitere Informationen finden Sie unter Konfigurations-Compliance Status. Alternativ können Sie ab V14.5 auch die folgenden Integrationen ausführen, um die Testergebnisse abzurufen: • Qualys PCRS-Richtlinien-Host-Integration: Ruft die Host-IDs für jede Richtlinie ab. Um diese geplante Aufgabe anzuzeigen, navigieren Sie zu: Qualys Vulnerability-Integration > Primäre Integrationen > Integration des Qualys-PCRS-Richtlinien-Hosts. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie die Qualys PCRS-Richtlinien-Hostintegration nach Qualys PC-Richtlinien und Qualys PC-Richtliniendetail aus. Nach Abschluss dieser geplanten Aufgabe wird automatisch die Integration der Qualys-PCRS-Testergebnisse ausgelöst. • Qualys Integration der PCRS-Testergebnisse: Ruft die Testergebnisse für jede Host-ID ab. Um diese geplante Aufgabe anzuzeigen, navigieren Sie zu Qualys Schwachstellenintegration > Primäre Integrationen > Qualys PCRS-Testergebnisintegration. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie die Qualys PCRS-Testergebnisintegration nach Qualys PC-Richtlinien, Qualys PC-Richtliniendetail und Qualys PCRS-Richtlinien-Host-Integration aus. Diese Integration verwendet den Parameter „Startzeit“ auf der Registerkarte „Integrationsdetails“.
Tenable Vulnerability Integration	Die regelmäßige Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert Testergebnisse. Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
	aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Assets Integration • Tenable.io Integration von Compliance-Ergebnissen • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen • Tenable.io Assets Integration • Tenable.io Integration der Auffüllung von Compliance-Ergebnissen Um den Konfigurationstestdatensatz anzuzeigen, navigieren Sie zu **Konfigurations-Compliance** > **Testergebnisse**. Im Datensatz werden importierte Daten in den Feldern**Test**und **Configuration Item** angezeigt. Daten werden auch auf den Registerkarten **Erwartete Werte**, **Ist-Werte**und **Fehlerkorrektur** angezeigt. Die zugehörigen Links **Korrekturaufgaben** und **Testergebnisverlauf** sind ausgefüllt.

Erkennung von Konfigurations-Compliance

Konfigurations-Compliance werden aus SCA-Scanneranwendungen von Drittparteien importiert. Sie strukturieren Gruppen von Software- und Hardwaretests in Datensätzen, um die Durchführung von Bewertungen zu beschleunigen.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Wenn ein Import abgeschlossen ist, wird ein Ereignis gesendet, um Aktionen für das Importende anzuzeigen. Für jede aktive Korrekturaufgabe werden die folgenden Aktionen durchgeführt:

- Gelöste Korrekturaufgaben mit fehlgeschlagenen Ergebnissen kehren in den Status **Warten auf Implementierung** zurück.
- Korrekturaufgaben, bei denen alle Ergebnisse bestanden haben, werden **als Geschlossen eingestuft**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Status von Testergebnissen in aktiven Korrekturaufgaben wird aktualisiert.
- Die Kennzeichnung, die angibt, ob ein Ergebnis Teil einer aktiven Korrekturaufgabe ist, wird aktualisiert.

Konfigurations-Compliance Korrelation

Konfigurations-Compliance bietet Priorisierung und Gruppierung von Testergebnissen (in Korrekturaufgabe), um die Behebung von Compliance-Problemen zu unterstützen.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Assetorientierte Priorisierung

Konfigurationsscans können eine große Anzahl von Ergebnissen bringen. Priorisieren Sie Ergebnisse, um das Risiko so gering wie möglich zu halten. Die Priorität umfasst sowohl die Kritikalität des Konfigurationstests als auch die Kritikalität des Assets. Die Priorität des Konfigurationstestergebnisses wird als Risikopunktzahl von 0 bis 100 ausgedrückt. Rechnergruppen berechnen die Risikopunktzahl und können angepasst werden.

Wenn der Import der Drittpartei abgeschlossen ist, sendet Konfigurations-Compliance ein Ereignis, um Aktionen für das Importende anzuzeigen. Für jede aktive Ergebnisgruppe werden die folgenden Aktionen ausgeführt:

- Gelöste Korrekturaufgaben mit fehlgeschlagenen Ergebnissen kehren in den Status **Warten auf Implementierung** zurück.
- Korrekturaufgaben, bei denen alle übergebenen Ergebnisse **Geschlossen**sind.
- Der Status von Testergebnissen in aktiven Korrekturaufgaben wird aktualisiert.
- Die Kennzeichnung, die angibt, ob ein Ergebnis Teil einer aktiven Korrekturaufgabe ist, wird aktualisiert.

Rangfolge für Korrekturaufgaben

Wenn Testergebnisse zu mehr als einer Gruppe gehören, wird der **Status** eines Testergebnisses anhand einer Rangfolge abgeleitet.

Die Felder **„Status“** und **„Lösung“** im Formular **„Konfigurationstest“** sowie das Feld **„Ergebnis“** im Formular **„Testergebnis“** werden anhand dieser Rangfolge berechnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Der Vorrang für die Gruppenmitgliedschaft gilt nur für Elemente, bei denen das Element den Konfigurationstest nicht bestanden hat. **Übergebene** Elemente haben immer den Status **Geschlossen – Repariert**.

Der **Ergebniswert** bestimmt den Status. Korrekturaufgaben im Status **„Geschlossen – Behoben“** und **„Geschlossen – Abgebrochen“** werden ignoriert. Der Artikelstatus wird aus den Status aller anderen Korrekturaufgaben berechnet, zu denen er gehört oder auf die er **gesetzt**wird, wenn keine andere Gruppe für den Artikel vorhanden ist.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Erstellung von Korrekturaufgaben

Konfigurations-Compliance Korrekturaufgaben werden manuell erstellt.

Es gibt zwei Möglichkeiten, **Korrekturaufgaben**zu erstellen und auszufüllen.

- Über das Modul **„Korrekturaufgaben“** und mithilfe von Filtern, die die Registerkarte **„Testergebnisse“** automatisch ausfüllen.

  Diese Methode eignet sich, wenn Sie wissen, welche Filter Sie verwenden möchten. Beispielsweise können alle Ergebnisse fehlgeschlagener Tests erfasst werden, die eine moderate und höhere Relevanz haben, sich auf die Windows-basierte Infrastruktur auswirken und nur für die SAP-Lieferkettenanwendung gelten.

- Durch Auswahl von Testergebnissen in der Liste **Testergebnisse** und Erstellung einer Korrekturaufgabe aus dem Menü **Aktionen für ausgewählte Zeilen...**

  Diese Methode eignet sich für Ergebnisse, die sich nicht leicht filtern lassen, oder für Situationen, in denen Sie Testergebnisse zur Korrektur angeben möchten. Zum Beispiel Ausreißer, die nichts gemeinsam haben.

Hinweis:

Wenn Sie eine Korrekturaufgabe aus der Liste **„Testergebnisse“** erstellen und später entscheiden, einen Filter für diese Korrekturaufgabe zu verwenden, werden Ihre ursprünglichen Einträge entfernt und durch die Filterergebnisse ersetzt.

Nicht gruppierte Testergebnisse

Nicht gruppierte Testergebnisse enthalten alle nicht bestandenen Testergebnisse, die nicht Mitglieder einer aktiven (nicht**geschlossenen**) Korrekturaufgabe sind. Dieses Modul wird nach jedem Import und immer dann aktualisiert, wenn Testergebnisse zu einer Korrekturaufgabe hinzugefügt oder daraus entfernt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkannte Elemente für Konfigurations-Compliance

Assets werden mithilfe von CI-Suchregeln automatisch mit Configuration Items (CIs) abgeglichen, wenn sie mit den -Host- und Testergebnisintegrationen importiert werden. Erkannte Elemente geben Ihnen Einblick in die Zuordnung der Asset-Identifizierung zu CIs in CMDB.

Erkannte Elemente werden **als abgeglichen**, **nicht abgeglichen**oder **neu klassifiziert**betrachtet. Identifizierte CIs befinden sich im Status **Abgeglichen**.

Um das Auffinden potenzieller Übereinstimmungsprobleme zu erleichtern, wird im Feld „CI-**Übereinstimmungsregel" die CI-Suchregel angezeigt, die dem CI** entspricht.

Hinweis:
Unterstützung**für CI-Übereinstimmungsregelfelder** ist nur für die Qualys -Integration verfügbar.

Wenn keine Übereinstimmung gefunden wurde, wird ein CI in der *CI-Klasse Nicht abgeglichen*[sn_sec_cmn_unmatched_ci], [cmdb_ci_unclassed_hardware]oder [cmdb_ci_incomplete_ip] von CMDBerstellt. Wenn das ursprüngliche nicht abgeglichene CI neu klassifiziert wurde, werden die Datensätze für erkannte Elemente aktualisiert, um diesen Status widerzuspiegeln. Weitere Informationen finden Sie unter Nicht abgeglichene CIs und Nicht abgeglichene Configuration Items anzeigen und neu klassifizieren.

Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Das Modul listet nicht abgeglichene Konfigurationselemente auf. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Eine Beschreibung der Felder in Erkannte Elemente finden Sie unter Formularfelder für erkannte Elemente.

CI-Änderungen für erkannte Elemente für Konfigurations-Compliance

Der Standardwert der Eigenschaft sn_sec_cmn.update_on_ci_change ist true. Wenn also das Configuration Item (CI) für ein erkanntes Element aktualisiert wird, werden auch die Testergebnisse aktualisiert.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die externe ID für das Testergebnis wird aktualisiert, und Risikopunktzahl, Zuweisungsregeln, Regeln für Korrekturaufgaben und Korrekturzielregel werden neu ausgewertet. Wenn ein Testergebnis mit demselben Test und CI vorhanden ist, werden die Testergebnisse mit dem vorhandenen Testergebnis aktualisiert, und das aktuelle Testergebnis wird mit dem Substatus ungültiges CIgeschlossen. Arbeitsnotizen werden entsprechend hinzugefügt.

Wenn Sie das CI für das vorhandene Testergebnis nicht aktualisieren möchten, legen Sie die Eigenschaft auf „falsch" fest. In diesem Fall wird bei einer CI-Änderung ein neues Testergebnis erstellt und das vorhandene als ungültigesCI geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gleichen Sie nicht übereinstimmende erkannte Elemente für ab Konfigurations-Compliance

Erstellen Sie eine geplante Aufgabe, um nicht abgeglichene erkannte Elemente abzugleichen. Wenn ein Testergebnis erstellt wird, ist das Configuration Item (CI), das ihm zum Zeitpunkt der Erstellung hinzugefügt wurde, möglicherweise veraltet.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn sich die Informationen in der CMDB ändern, werden nicht abgeglichene CI-Informationen nicht abgeglichen. Wenden Sie zum Abgleichen CI-Suchregeln auf die Testergebnisse an, die sich in einem nicht abgeglichenen Status befinden, wenn die CMDB mit den neuesten CIs aktualisiert wird.

Bei Bedarf wird eine geplante Aufgabe ausgeführt, um die CI-Übereinstimmungsregel für die erkannten Elemente in einem nicht abgeglichenen Status erneut anzuwenden. Wenn sich das CI nach dem erneuten Anwenden der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Betroffene Testergebnisse werden ebenfalls aktualisiert. Details finden Sie unter CI-Änderungen für erkannte Elemente für Konfigurations-Compliance.

Hinweis:

Ab Konfigurations-Compliance v24 können Sie die erneute Anwendung von CI-Suchregeln auf erkannte Elemente mit dem Substatus „CI außer Betrieb genommen“ überspringen, indem Sie die Systemeigenschaft `sn_sec_cmn.skipItemsWithCIDecommissioned` aktivieren.

Prozedur

1. Navigieren zu **Alle** > **Security Operations > Nicht übereinstimmende erkannte Elemente abgleichen**.
2. Klicken Sie auf der Seite „Hintergrundaufträge“ **auf Abgleichsauftrag erstellen**.
3. Füllen Sie die Felder des Formulars aus.

Hinweis:

Sie können nur das Feld „Parameter“ bearbeiten.

Hintergrundauftrag

Feld	Beschreibung
Nummer	Eindeutige Auftragsnummer.
Erstellt von	Benutzer, der den Auftrag erstellt hat.
Parameter	Parameter zum Abgleichen der nicht abgeglichenen erkannten Elemente: ○ limit: Maximale Anzahl erkannter Elemente, die abgeglichen werden sollen. Wenn Sie keinen Wert eingeben, werden 10.000 erkannte Elemente abgeglichen. ○ firstDiscovereditem: Erstes erkanntes Element, das abgeglichen werden muss. Wenn Sie keinen Wert eingeben, beginnt der Abgleichsprozess mit dem ersten erkannten Element.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Aktueller Status des Hintergrundauftrags.
Statusbeschreibung	Beschreibung des aktuellen Status des Hintergrundauftrags.
Auftragstyp	Typ des Auftrags. Der Wert lautet **Abgleich nicht übereinstimmender erkannter Elemente**.
Gestartet um	Zeit, zu der der Auftrag gestartet wurde.
Endete um	Zeitpunkt, zu dem der Auftrag abgeschlossen wurde.
Auftragsdauer	Gesamtzeit, die für den Abschluss des Auftrags benötigt wurde.
Substatus	Substatus für den ausgewählten Status.
Notizen	Anzahl der verarbeiteten Datensätze.

4. Klicken Sie auf **Absenden**.

Hinweis:

- Um die Ausführung des Auftrags zu beenden, klicken Sie auf **Abbrechen**.
- Sie können nicht übereinstimmende CIs nicht abgleichen oder CI-Suchregeln erneut anwenden, während Sie Hosts oder Testergebnisse importieren.

Wenden Sie die CI-Suchregeln erneut auf ausgewählte erkannte Elemente für an Konfigurations-Compliance

Wenden Sie die Suchregeln für Configuration Item (CI) erneut auf ausgewählte erkannte Elemente aus den Auswahlaktionen der Listenansicht für erkannte Elemente an. Der Administrator muss möglicherweise eine Suchregel aus mehreren Gründen bearbeiten oder aktualisieren. Wenn sich die Suchregel ändert, kann sie erneut auf die erkannten Elemente angewendet werden.

Vorbereitungen

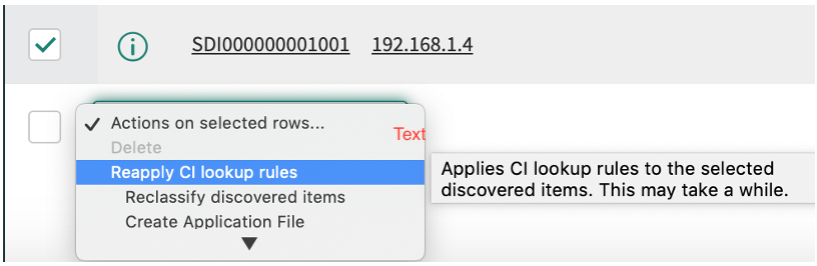
Erforderliche Rollen:

Warum und wann dieser Vorgang ausgeführt wird

Wenn sich das CI nach dem erneuten Anwenden der CI-Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI und den Testergebnissen aktualisiert. Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente für Konfigurations-Compliance.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Erkannte Elemente**.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und klicken Sie auf **Aktion für ausgewählte Zeilen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **CI-Suchregeln erneut anwenden** aus der Liste aus.

   Die Regeln werden erneut auf diese erkannten Elemente angewendet.

   Hinweis:

   Ab Konfigurations-Compliance v15.1.5 können Sie die erneute Anwendung von CI-Suchregeln auf erkannte Elemente mit dem Substatus „CI außer Betrieb genommen“ überspringen, indem Sie die Systemeigenschaft *sn_sec_cmn.skipItemsWithCIDecommissioned*aktivieren.

Tenable Vulnerability Integration mit Konfigurations-Compliance

Das Produkt Tenable.io von Tenable Vulnerability Integration importiert Richtlinien, Steuerungen (Testergebnisse) und Konfigurationstests für die Verarbeitung in der Anwendung Konfigurations-Compliance.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Tenable.io

Tenable Vulnerability Integration wird unterstützt.

Importierte Daten können für folgende Aufgaben verwendet werden:

- Identifizieren Sie konfigurationsbezogene Schwachstellen für Ihre in aufgeführten Assets Configuration Management Database (CMDB)
- Vergewissern Sie sich, dass Ihre Assets Ihren Richtlinien und Kontrollen entsprechen.

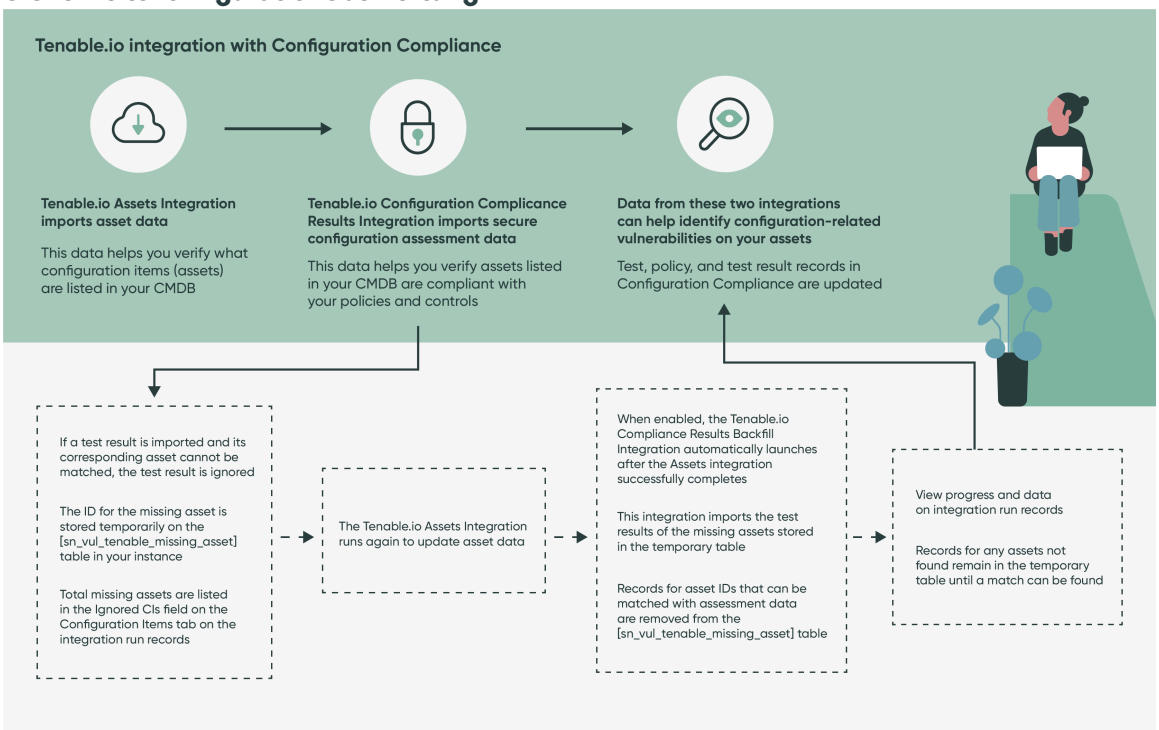
Asset-Daten, Richtlinien, Steuerungen (Testergebnisse) und Konfigurationstests werden mit den folgenden Integrationen importiert:

- Tenable.io Assets Integration
- Tenable.io Integration von Compliance-Ergebnissen
- Tenable.io Integration der Auffüllung von Compliance-Ergebnissen

Die folgende Abbildung zeigt, wie die Integrationen zusammenarbeiten, um Asset- und Konfigurationsbewertungsdaten zu importieren und alle ignorierten CIs abzugleichen, die während eines Imports übersehen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie den Flow für die Ergebnisse der Sicherheitskonfigurationsbewertung



Daten werden importiert, aktualisiert und in den Testergebnis-, Richtlinien- und Konfigurationstestdatensätzen in der Anwendung Konfigurations-Compliance angezeigt.

In einigen Fällen unterscheidet sich die Anzahl der importierten Configuration Items (CIs) für die Tenable.io Assets-Integration und die Tenable.io Compliance-Ergebnisintegration. In diesem Fall werden temporäre Datensätze für die ignorierten Asset-IDs erstellt und gespeichert. Diese Datensätze können später durch Importe aus der Compliance-Ergebnisauffüllungsintegration mit importierten Bewertungsdaten abgeglichen werden.

Angenommen, die Assets-Integration importiert 80 Assets in einer Integrationsausführung, die Compliance-Ergebnisintegration jedoch 100.

Hinweis:
Sie können die Anzahl der ignorierten CIs bei Integrationsausführungen überprüfen, indem Sie zu navigieren **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**. Klicken Sie auf den Namen einer Integration, um den Datensatz zu öffnen. Öffnen Sie im zugehörigen Link **„Integrationsausführungen für Schwachstellen“** einen Integrationsausführungsdatensatz, und wählen Sie die Registerkarte **Elemente**, um den Wert im Feld **Ignorierte CIs** anzuzeigen. Dieses Feld verfolgt die Gesamtzahl der ignorierten (fehlenden) Assets aus dem Import.

Beim Vergleich der Werte in den Feldern **Ignorierte CIs** für jeden Datensatz der Integrationsausführung ergibt sich ein Unterschied von 20 ignorierten CIs. Daher wird die Auffüllungsintegration automatisch ausgeführt (siehe Abbildung). Diese Integration importiert die Konfigurationsbewertungsinformationen für die zusätzlichen 20 Assets, die von der Compliance-Ergebnisintegration gefunden wurden, aber von der Assets-Integration übersehen wurden. Da Bewertungsdaten für fehlende Assets nicht importiert werden, importiert die Tenable.io Integration zum Auffüllen von Compliance-Ergebnissen bis zu 200 Asset-IDs pro Integrationsausführung, um die fehlenden Assets mit den entsprechenden Bewertungsdaten abzugleichen. Alle Datensätze, die für fehlende oder ignorierte Assets erstellt wurden und in der temporären Tabelle aufgeführt sind, werden gelöscht, nachdem diese Assets und ihre Daten abgeglichen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Es kann mehrere Ausführungen dieser Integrationen erfordern, um alle ignorierten Assets zu importieren.

Weitere Informationen zum Aktivieren und Konfigurieren der Tenable.io Asset Integration finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten. Weitere Informationen zur Integration finden Sie unter Die Tenable-Schwachstellenintegration verstehen.

Die Tenable.io Integration für Compliance-Ergebnisse und die Tenable.io Integration für die Auffüllung von Compliance-Ergebnissen sind standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
2. Klicken Sie in der Liste „Tenable Integrations“ (Tenable-Integrationen) auf einen Integrationsnamen, um den Datensatz zu öffnen, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen auf ihren Standardwerten belassen, damit diese Integrationen gestartet werden können.

CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Konfigurations-Compliance Schwachstellenintegrationen von Drittparteien

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Konfigurations-Compliance automatisch Hostdaten, um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. Dies geschieht mithilfe von **CI-Suchregeln**. Diese Regeln werden verwendet, um Configuration Items (CIs) zu identifizieren und dem Testergebnisdatensatz hinzuzufügen, um die Behebung zu erleichtern.

Beim Importieren von Assets wird zuerst eine Suche in der Liste **„Erkannte Elemente“** anhand von Drittpartei-IDs durchgeführt, um Übereinstimmungen mit Configuration Items (CIs) aus vorherigen Importen zu finden. Wenn eine Übereinstimmung mit der Host-ID gefunden wird, wird sie als Feld **Configuration item (Konfigurationselement)** im Testergebnis-Datensatz verwendet.

Sie können sehen, wie importierte Assets mithilfe der Liste **Erkannte Elemente** CIs zugeordnet werden. Wenn keine Übereinstimmung gefunden wird oder das Feld cmdb_ci leer ist, verwenden die Regeln die Informationen des anderen Hosts, um zu versuchen, das CI korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein Platzhalter-CI erstellt und als **nicht abgeglichenes CI**gekennzeichnet. Unter Nicht abgeglichene CIs finden Sie weitere Informationen zur Behandlung dieser CIs.

Ein neues erkanntes Element wird erstellt und diesem CI zugeordnet.

Hinweis:
CI-Suchregeln sind nur für die Qualys Integration for Security Operations verfügbar.

CI-Suchregeln können domänengetrennt sein und sind quellenspezifisch. Jede Quelle kann mehrere Bereitstellungen haben. Qualys kann mehrere Bereitstellungen der Qualys-Integration aufweisen. Jede Bereitstellung verfügt über einen eigenen Satz von CI-Suchregeln.

Hinweis:
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellen-Integration gemeinsam verwendet. Wenn eine Regel gelöscht oder geändert wird, wirken sich die Löschung oder Änderungen auf alle Bereitstellungen der Schwachstellenintegration aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn versucht wird, eine Übereinstimmung zu finden, besteht der erste Schritt in der Lieferanten-ID-Suche nach einer genauen Übereinstimmung zwischen Quelle, Quellinstanz und Lieferanten-ID. Dann werden Suchregeln der Reihe nach von der niedrigsten zur höchsten ausgeführt und angehalten, wenn eine Regel nur ein einziges CI als Übereinstimmung zurückgibt. Wenn eine Regel so erstellt wird, dass mehr als ein CI zurückgegeben wird, wird nur die erste Übereinstimmung verwendet.

Hinweis:
Um einen Abgleich mit Netzwerkelementen auf niedriger Ebene zu vermeiden, wenn es sich bei einem übereinstimmenden CI um eines der folgenden Elemente handelt: `dscy_Switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic`oder `cmdb_ci_ip_address`, wird das übergeordnete CI zurückgegeben.

Eine Systemeigenschaft zum Ausschließen von CI-Klassen ist verfügbar. Diese Eigenschaft ist mit einem Upgrade nicht verfügbar. Upgrade-Informationen und Anweisungen zum Festlegen der Eigenschaft finden Sie unter CI-Klassen ignorieren.

Um das Auffinden von Übereinstimmungsproblemen zu erleichtern, wird bei einer Übereinstimmung die CI-Suchregel, mit der sie gefunden wird, dem Datensatz „Erkanntes Element“ im Feld **„CI-Übereinstimmungsregel“** hinzugefügt. Suchregeln werden zuerst anhand des niedrigsten **Reihenfolgewerts** ausgewertet.

Einige der Qualys CI-Suchregeln, die im Lieferumfang des Basissystems enthalten sind, sind:

- QUALYS-HOST-ID
- FQDN
- NetBIOS
- DNS
- IP

Einige der im Basissystem enthaltenen Microsoft Defender CI-Suchregeln sind:

- S3-Bucket
- Name
- Ressourcen-ID

Einige der im Basissystem enthaltenen Palo Alto Prisma Cloud-CI-Suchregeln sind:

- S3-Bucket
- Name
- Ressourcen-ID

Das Importieren von Testergebnisdaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn die Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Abgleichen von CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie alle anwenderdefinierten CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln**. Unter Schritte zum Verhindern von doppelten oder verwaisten Datensätzen nach dem Ausführen von Vulnerability Response CI-Suchregeln finden Sie weitere Informationen zum Verhindern des Duplikats von verwaisten Elementen, zum Löschen von Daten und zum Bereinigen von Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisierte CI-Suchregeln werden erneut angewendet

Wenn Sie eine CI-Suchregel ändern, klicken Sie auf der Listenseite „CI-Suchregeln“ **auf Änderungen anwenden,** um alle Regeln für die erkannten Elemente erneut auszuführen, die:

- Wurden mit den aktualisierten Regeln abgeglichen
- Werden von keiner Regel abgeglichen

Wenn sich das Configuration Item (CI) nach dem erneuten Anwenden der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Die Testergebnisse werden ebenfalls aktualisiert. Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente für Konfigurations-Compliance.

Deduplizieren vorhandener Konfigurationselemente für Konfigurations-Compliance

Die Nachbesserung von CI-Duplikaten für Deduplizierungsaufgaben wird mit der Eigenschaft „sn_sec_cmn_src_ci.cmdb_ci“ aktualisiert.

Wann immer eine Deduplizierungsaufgabe zum Aktualisieren der Konfigurationselemente (CIs) verwendet wird, aktualisiert sie auch die erkannten Elemente, die sich auf diese CIs beziehen. Daher werden die Testergebnisse mit dem CI aktualisiert. Details finden Sie unter CI-Änderungen für erkannte Elemente für Konfigurations-Compliance.

CIs für Konfigurations-Compliance werden mit der Engine Identification and Reconciliation erstellt

Ab Konfigurations-Compliance 11.1 können Sie Configuration Items (CIs) in Configuration Management Database (CMDB) mithilfe der Identification and Reconciliation Engine (IRE)-API erstellen. Durch die Verwendung der IRE-API zum Erstellen von CIs können Sie verhindern, dass doppelte CIs erstellt werden, und Sie können CI-Attribute abgleichen, indem Sie zulassen, dass nur autorisierende Datenquellen in CMDBschreiben.

Eine CI-Klasse (Tabelle) ist der ursprüngliche Tabellenname in der Instanzdatenbank. CMDB enthält Basissystemklassen, in denen Daten zu CIs gespeichert werden.

IRE für CI-Erstellung verwenden

Wenn vor Version 11.1 weder in der Liste „Erkannte Elemente“ noch in CMDBein übereinstimmendes CI gefunden wurde, wurde ein CI in der Klasse der nicht abgeglichenen CIs (sn_sec_cmn_unmatched_ci) erstellt.

Weitere Informationen finden Sie unter Nicht abgeglichene CIs.

Ab Version 11.1 können Sie die IRE-API zum Erstellen von CIs in CMDBverwenden. Anstatt die CI-Klasse Nicht abgeglichen zu verwenden, wird ein CI in der Klasse Nicht klassifizierte Hardware oder Unvollständige IP-Identifizierung erstellt.

CMDB CI-Klassen

Hinweis:
Um die neuen Klassen zu verwenden, aktivieren Sie das Plugin CMDB CI Class Models. Andernfalls werden CIs in der nicht abgeglichenen CI-Klasse erstellt.

Ab Version 11.1: Wenn der Host, den Sie von einem Drittanbieterscanner importiert haben, nicht in der Liste „Erkannte Elemente“ oder in CMDBzu finden ist, wird er in einer der folgenden neuen CMDB CI-Klassen gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CMDB CI-Klassen

CMDB CI-Klasse	Beschreibung
Unvollständige IP-Identifizierung des Geräts (cmdb_ci_incomplete_ip)	In dieser Tabelle wird ein CI erstellt, wenn nur die IP-Adresse in den vom Scanner empfangenen Hostinformationen verfügbar ist.
Nicht klassifizierte Hardware (cmdb_unclassed_hardware_ci)	Das CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen eine der folgenden Informationen verfügbar ist: • Hostname • IP-Adresse • DNS • NETBIOS • MAC-Adresse **Hinweis:** Wenn die MAC-Adresse verfügbar ist, wird der Netzwerkadaptereintrag erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft. Wenn sowohl die IP-Adresse als auch die MAC-Adresse verfügbar sind, wird auch das IP-Adressen-CI erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft.

In folgenden Fällen verwendet das System automatisch eine nicht abgeglichene CI-Klasse:

- Das CMDB CI-Klassen-Plugin ist nicht aktiviert.
- IRE löst beim Erstellen eines neuen CI eine Ausnahme aus.

Zugehörige Informationen

Store-App „CMDB CI Class Models“

Identification and Reconciliation Engine (IRE)

Konfigurations-Compliance Übersicht über Zuweisungsregeln

Definieren Sie die Kriterien, nach denen Testergebnisse automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die standardmäßige Zuweisungsregel **An CI-Supportgruppe zuweisen**ist im Basissystem enthalten, das der **CI-Supportgruppe**Testergebnisse zuweist. Standardmäßig inaktiv.

Die von den Zuweisungsregeln festgelegten Zuweisungsgruppen werden von **den Korrekturaufgabenregeln** verwendet, um Besitzer zu Korrekturaufgaben (RTs) zuzuweisen.

Testergebnisse werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, Testergebnisse mit **Zuweisen mit zuzuweisen**:

- Zuweisungsgruppe: Mit dieser Option können Sie eine der vorhandenen Now Platform® -Anwendergruppen auswählen.
- Zuweisungsgruppenfeld: Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle cmdb_ci verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder angezeigt:
  - Keine: Gibt an, dass für dieses Pflichtfeld kein Standardwert vorhanden ist
  - Konfigurationselement: Genehmigungsgruppe
  - Konfigurationselement: Zuweisungsgruppe
  - Konfigurationselement: Supportgruppe
- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Kenntnisse in der Codierung oder fortgeschrittenen ServiceNow®.

Weitere Informationen zum Erstellen von Zuweisungsregeln finden Sie unter Erstellen oder bearbeiten Sie Konfigurations-Compliance -Zuweisungsregeln.

Mit der Rolle sn_vulc.remediation_owner können Sie Testergebnisse und Korrekturaufgaben anzeigen und aktualisieren, die ihnen oder ihren Zuweisungsgruppen zugewiesen sind. Um die Module anzuzeigen, navigieren Sie zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse** > **Meine offenen Testergebnisse**, oder **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**.

Die Rolle sn_vulc.remediation_owner kann direkt einem Benutzer zugewiesen werden oder wird automatisch zugewiesen, wenn Sie einem Benutzer die Rolle itil zuweisen.

Bewertungsprozess für Zuweisungsregeln

Wenn ein neues Testergebnis importiert oder nach dem Schließen erneut geöffnet wird, werden die Zuweisungsregeln dafür ausgewertet. Die Zuweisungsregeln werden nach dem CI-Abgleich und der Berechnung der Risikopunktzahl ausgewertet. Ein Testergebnis wird nur beim ersten Import und wenn eine Regel geändert wird, automatisch ausgewertet, es sei denn, sie wird nach dem Schließen erneut geöffnet. Sie können Regeln nach Änderungen manuell erneut anwenden.

Der folgende Prozess wird für jedes neue oder erneut geöffnete Testergebnis verwendet:

- Für jede Zuweisungsregel für Testergebnisse wird das Testergebnis mit dem Zuweisungsfilter verglichen, wobei die Regel niedrigster Ordnung zuerst ist.
- Wenn die Bedingung erfüllt ist, wird das Testergebnis einer Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung unter allen Regeln finden, bleibt das Testergebnis nicht zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, klicken Sie auf die Schaltfläche **Changes anwenden** auf der Listenseite für Zuweisungsregeln, um alle geänderten Regeln für alle aktiven offenen Testergebnisse mit Ausnahme der manuell zugewiesenen Regeln erneut auszuführen.

Hinweis:
Manuell erstellte Zuweisungen werden durch die Zuweisungsregeln nicht neu bewertet.

Die geplante Aufgabe [*Reapply all assignment rules*] ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle offenen Testergebnisse für alle aktiven Regeln mit Ausnahme der manuell zugewiesenen ausgewertet. Sie kann täglich, wöchentlich, monatlich, regelmäßig, einmal oder bei Bedarf ausgeführt werden.

Wichtig:
Als Administrator und Analyst können Sie die neuesten Zuweisungen für ausgewählte Testergebnisse unter Vulnerability Manager Workspaceabrufen. Diese Methode ist effizienter als das erneute Anwenden der Zuweisungsregeln für alle Testergebnisse in der UI klassisch, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Zuweisungsregeln und Korrekturaufgabenzuweisung

Normalerweise weisen Sie Ihre Korrekturaufgabe (RT) derselben Zuweisungsgruppe zu wie die darin enthaltenen Testergebnisse. Das ist es, was die Regeln für Korrekturaufgaben standardmäßig tun.

Wenn Ihre RT-Gruppierungen beispielsweise nach Configuration Item-Klasse erfolgen, kann die erstellte Korrekturaufgabe nach den verschiedenen Zuweisungsgruppen aufgeschlüsselt werden. Eine Oracle Database-TRG kann der Gruppe 1 und eine Oracle Database-TRG der Gruppe 2 zugewiesen werden.

Wenn die Zuweisungsgruppe auf der Ebene der Korrekturaufgabe geändert wird, werden alle Testergebnisse in dieser Korrekturaufgabe, die dieselbe Zuweisungsgruppe aufweisen, auf die neue Zuweisungsgruppe aktualisiert. Die Testergebnisse werden als manuell zugewiesen markiert und können nicht für weitere Regelauswertungen geeignet sein.

Zuweisungen werden aus Korrekturaufgaben Konfigurations-Compliance entfernt

Sie können die Felder **Zugewiesen an** und **Zuweisungsgruppe** in Korrekturaufgaben (RT) und den zugehörigen Testergebnissen direkt aus den TRG-Datensätzen löschen, von denen Sie feststellen, dass sie Ihnen oder Ihren Gruppen möglicherweise nicht korrekt zugewiesen sind.

Übersicht

Ab v14.3 der Anwendung Konfigurations-Compliance können Korrekturbesitzer Datensätze für die Neuzuweisung mit der Schaltfläche **Zuweisung** aufheben aktualisieren.

Anwendungsfall für sn_vulc.remediation_owner

Wenn Sie feststellen, dass RTs und die zugehörigen Testergebnisse nicht in Ihrem Korrekturbereich liegen, oder wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen nicht korrekt zugewiesen wurden, sollten Sie sich oder Ihre Gruppen aus **Zugewiesen an** und entfernen **Zuweisungsgruppenfelder** für diese Korrekturaufgabendatensätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Heben Sie die Zuweisung des Moduls auf

Die Schaltfläche **„Zuweisung aufheben“** wird für die RT-Datensätze in jedem anderen Status als dem Status „Geschlossen“ oder „Gelöst“ angezeigt.

Wenn Sie **Zuweisung aufheben**auswählen, werden Sie aufgefordert, dass alle mit der Korrekturaufgabe verknüpften Testergebnisse neu zugewiesen werden und in den Zuweisungstyp **Nicht zugewiesen** übergehen.

Alle Datensätze, die Sie entweder mit der UI-Schaltfläche oder manuell aktualisieren, werden im Modul Nicht zugewiesen unter Konfigurations-Complianceangezeigt.

Informationen zum erneuten Zuweisen von Datensätzen mithilfe der UI-Aktion *Unassigned*] finden Sie unter Entfernen Sie Zuweisungen aus Korrekturaufgaben für Sie oder Ihre Gruppen.

Systemeigenschaft und Benachrichtigungen

Wenn Sie ein Administrator mit der Rolle sn_vulc.vulnerability_admin sind und für einen Datensatz **die Option Aufheben** der Zuweisung auswählen, löst die Systemeigenschaft *sn_vulc.unassign_test_result_group.approval_required* standardmäßig den Datensatz „Genehmigung der Statusänderung“ und den Datensatz „Genehmigung angefordert“ aus. Außerdem wird die Anforderung in der Liste Meine Genehmigungen des Genehmigers angezeigt.

Hinweis:
Als Schwachstellenadministrator können Sie die Systemeigenschaft *sn_vulc.unassign_test_result_group.approval_required* auf **„false“** festlegen, um den Genehmigungsprozess zu deaktivieren.

- Wenn der Genehmiger Ihre Anforderung genehmigt, leert die Systemeigenschaft *sn_vulc.default_assignment_group*standardmäßig die Felder Zugewiesen an und Zuweisungsgruppe und füllt das Feld Zuweisungstyp mit **Nicht zugewiesen**aus.
  Als Schwachstellenadministrator können Sie den Wert in der Systemeigenschaft *sn_vulc.default_assignment_group* ändern, sodass die Zuweisungsfelder gelöscht werden und dann eine bestimmte Gruppe zugewiesen wird. Wenn ein Benutzer beispielsweise für einen Datensatz **die Option Zuweisung aufheben** auswählt und Sie ihn zur Überprüfung an eine bestimmte Gruppe umleiten möchten, können Sie im Wertfeld der Systemeigenschaft eine System-ID für die Gruppe Ihrer Wahl hinzufügen.
- Wenn der Genehmiger Ihre Anforderung ablehnt, wird der Grund für die Ablehnung auf der Registerkarte **Notizen** angezeigt.

Wenn alternativ *sn_vulc.default_assignment_group* nicht für eine bestimmte Gruppe konfiguriert ist, werden Benutzer, die Sie der Benutzergruppe „Benachrichtigung für die Zuweisung aufheben“ hinzufügen, benachrichtigt, wenn die Zuweisung von Datensätzen aufgehoben wird. Die Systemeigenschaft *sn_vulc.default_notification_group* bestimmt die Benachrichtigungen an diese Gruppe.

Der Zuweisungstyp – **Manuell**, **Regel**oder **Nicht zugewiesen**– ist in den RT-Datensätzen und in der Listenansicht verfügbar. Der Zuweisungstyp **Nicht zugewiesen** wird angezeigt, nachdem die Felder **Zugewiesen an** und **Zuweisungsgruppe** durch die Systemeigenschaft der Funktion gelöscht wurden.

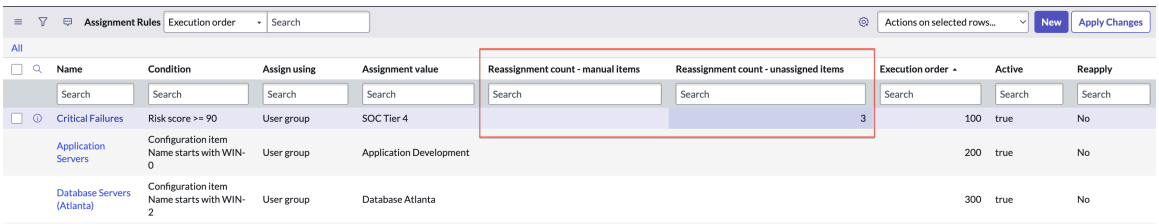
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen Sie Ihre Zuweisungsregeln mit der geplanten Aufgabe für diese Funktion

Eine tägliche regelmäßige Aufgabe zählt die Datensätze beim Übergang in den Zuweisungstyp **„Nicht zugewiesen“**. Mit dieser Anzahl können Schwachstellenanalysten Zuweisungsregeln überwachen und anpassen, die basierend auf Zuweisungsregeln mit einer höheren Anzahl nicht zugewiesener RTs möglicherweise nicht gut funktionieren.

Die geplante Aufgabe *`Reassignment count for assignment rules`* wird täglich ausgeführt und gibt die Gesamtzahl der RTs an, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen wurden.

Die Aufgabe zählt auch alle Datensätze, deren Zuweisung manuell aufgehoben wurde. Sowohl die manuellen Anzahlen als auch die Anzahlen, die von dieser Funktion gesammelt werden, werden in der Liste „Regeln für die Zuweisung von Schwachstellen“ in zwei Spalten veröffentlicht: *`Reassignment count - manual items`* und *`Reassignment count - unassigned items`*.



1. Als Schwachstellenadministrator können Sie diese Anzahlen anzeigen, indem Sie zu navigieren **Konfigurations-Compliance** > **Administration** > **Zuweisungsregeln**.
2. Wählen Sie das Zahnradsymbol oben rechts in der Liste und anschließend **Anzahl der Neuzuweisungen – manuelle Elemente**und **anschließend Anzahl der Neuzuweisungen – nicht zugewiesene Elemente** aus.
3. Jedes RT, das ursprünglich von einer Regel zugewiesen wurde, später jedoch automatisch oder manuell neu zugewiesen wurde, enthält in der Listenansicht einen Verweis auf die ursprüngliche Regel.

Konfigurations-Compliance Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben

Erstellen Sie automatisch Korrekturaufgaben (RTs), um die Ergebnisse mithilfe von Korrekturaufgabenregeln massenweise zu analysieren. Die Kriterien, nach denen Aufgaben entstehen, sind so konfiguriert, dass Sie Testergebnisse nicht manuell Korrekturaufgaben zuweisen müssen.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgaben verstehen

Korrekturaufgaben stellen einen Satz von zu korrigierenden Testergebnissen dar. Das Gruppieren von Testergebnissen hat viele Vorteile. Durch die Verwendung von Gruppen können Sie Testergebnisse massenweise durch die Korrekturstatus befördern, mit „Wird untersucht“ markieren, zurückstellen und als gelöst markieren. Sie können Bedingungen erstellen, um alle Ergebnisse automatisch mit den angegebenen Ergebnissen, Technologien, Risikopunktzahlen und anderen Daten im Zusammenhang mit den Testergebnissen zu gruppieren. Testergebnisse können zu mehr als einer Korrekturaufgabe gehören, sodass Sie die Flexibilität haben, aktiv an einer Korrekturaufgabe zu arbeiten und eine andere zu überwachen. Es hängt alles von Ihren organisatorischen Anforderungen ab. Sie können beispielsweise nach Zuweisung gruppieren und auch eine Gruppe mit Technologien erstellen.

Korrekturaufgaben werden wie folgt erstellt.

- Manuell mit einer von zwei Optionen, um der Gruppe Testergebnisse hinzuzufügen.
  - **Manuell**: Erstellt eine Korrekturaufgabe ohne Einträge. Testergebnisse müssen manuell hinzugefügt werden.
  - **Filter**: erstellt eine Korrekturaufgabe und verwendet Bedingungen, um dieser Korrekturaufgabe automatisch Testergebnisse hinzuzufügen.

  Hinweis:
  Manuell hinzugefügte Testergebnisse werden durch Regeln für Korrekturaufgaben oder Bedingungen für Korrekturaufgaben nicht automatisch aus Korrekturaufgaben entfernt.

- Automatisch, mithilfe von Regeln für Korrekturaufgaben. Dies ist die einfachste Option. Nach der Konfiguration erstellen die Regeln für Korrekturaufgaben alle gewünschten Korrekturaufgaben.

Von einer Korrekturaufgabe aus kann die Gruppe der Testergebnisse einem Benutzer zugewiesen, auf einen späteren Zeitpunkt zurückgestellt, zum Erstellen einer **Change-Anforderung**verwendet usw. werden.

Hinweis:

Mit der Rolle sn_vulc.remediation_owner können Sie Testergebnisse und Korrekturaufgaben anzeigen und aktualisieren, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind. Um die Module anzuzeigen, navigieren Sie zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse** > **Meine offenen Testergebnisse**, oder **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**.

Wenn festgestellt wird, dass einer Korrekturaufgabe ein neues Testergebnis hinzugefügt werden kann, wird das Testergebnis in die zugehörige Liste **„Testergebnisse“** der Korrekturaufgabe aufgenommen.

Beim Aktualisieren des Status einer Korrekturaufgabe kann der Status der zugehörigen Testergebnisse so aktualisiert werden, dass er mit dieser Korrekturaufgabe übereinstimmt. Weitere Informationen zu Statusänderungen finden Sie unter Konfigurations-Compliance Status.

Die Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie Testergebnisse automatisch gruppiert und zugewiesen werden. Die Standardregel **Zuweisungsgruppe Test**ist im Basissystem enthalten, das Testergebnisse basierend auf einem Testergebnis **Zuweisungsgruppe** und dem Feld **Test** gruppiert. Diese Regel ist standardmäßig deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach jedem anderen Satz von Werten in Spalten gruppieren, auf die über das Testergebnis zugegriffen werden kann. Sie können bis zu sechs Schlüssel und eine beliebige Anzahl von Bedingungen verwenden. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Sie Konfigurations-Compliance Regeln für Korrekturaufgaben.

Wichtig:
Als Administrator und Analyst können Sie im Arbeitsbereich des Schwachstellen-Managers die Regeln für Korrekturaufgaben für ausgewählte Testergebnisse auswerten. Diese Methode ist effizienter als die erneute Anwendung der Korrekturaufgabenregeln in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Sie können Ihre Testergebnisse beispielsweise nach Zuweisungsgruppe oder Technologie und Configuration Item (CI) gruppieren. Für Testergebnisse, die das Unternehmen einem höheren Risiko aussetzen, können andere Regeln verwendet werden. Sie können eine Regel für Korrekturaufgaben für CIs mit niedrigem Schweregrad oder geringem Risiko haben. Weitere Informationen zu verfügbaren Feldern finden Sie unter Zeigen Sie Konfigurations-Compliance Testergebnisse an.

Wenn ein neues Testergebnis importiert oder nach dem Schließen erneut geöffnet wird, werden die Regeln für Korrekturaufgaben dafür ausgewertet. Ein Testergebnis wird nur einmal ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet.

Die Regeln für Korrekturaufgaben werden nach dem CI-Abgleich, der Berechnung der Risikopunktzahl und den Zuweisungsregeln ausgewertet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete Testergebnis verwendet:

- Für jede Regel für Korrekturaufgaben wird das Testergebnis mit dem Bedingungsfilter verglichen.
- Für jede Regel, bei der die Regelbedingung erfüllt ist, werden die Daten aus den Gruppenschlüsselspalten des Testergebnisses abgerufen. Die Regel prüft, ob eine übereinstimmende **offene** Korrekturaufgabe vorhanden ist, die der gleichen Zuweisungsgruppe wie das Testergebnis zugewiesen ist.

  Wenn die Korrekturaufgabe gefunden wird, wird das Testergebnis der vorhandenen Korrekturaufgabe im Status **Offen** hinzugefügt.

- Wenn keine Korrekturaufgabe im Status „ **Offen** “ gefunden wird, erstellt die Regel eine Korrekturaufgabe, weist sie basierend auf der **Benutzergruppe** oder **dem Schlüsselwert** in der Regel zu und platziert das Testergebnis darin.

Es kann mehr als eine Testergebnisregel definiert werden, um verschiedene Arten von Ergebnissen zu gruppieren. Da jedes Ergebnis mit den Regelbedingungen verglichen wird, bevor es in eine Korrekturaufgabe aufgenommen wird, können sich zu viele Regeln auf die Leistung auswirken.

Wenn eine Regel für Korrekturaufgaben gelöscht wird, können Sie alle offenen Aufgaben löschen, die von der Regel erstellt wurden. Dies gilt sowohl für die Regelformularansicht als auch für die Listenansicht.

Wenn eine Korrekturaufgabenzuweisung vorgenommen oder geändert wird, werden die Felder **Zuweisungsgruppe** und **Zugewiesen** an auf alle Testergebnisse heruntergesetzt, mit Ausnahme derer, bei denen das Testergebnis eine andere Zuweisungsgruppe als das RT hat. Weitere Informationen zu Zuweisungsregeln finden Sie unter Konfigurations-Compliance Übersicht über Zuweisungsregeln. Diese Zuweisungen werden für diese Gruppe beim nächsten Import automatisch verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl der Zurückstellungen von Testergebnissen und Korrekturaufgaben nachverfolgen

Verfolgen Sie ab v14.3 im Modul „Mehrere Zurückstellungen“, wie oft ein Testergebnis oder eine Korrekturaufgabe zurückgestellt wird. Eine regelmäßige Aufgabe, **Anzahl der Zurückstellungen festlegen**, wird täglich ausgeführt, um die Anzahl der Datensätze zu erfassen, die mehr als einmal in der Spalte „Zurückstellungsanzahl“ in den Datensätzen zurückgestellt werden, die im Modul Mehrere Zurückstellungen aufgeführt sind.

Rechnergruppen und Rechner für konfigurieren Konfigurations-Compliance

Konfigurations-Compliance-Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner sind nach den Kriterien gruppiert, mit denen bestimmt wird, wie die Datensätze aktualisiert werden.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Konfigurations-Compliance-Rechner

Die Anwendung Configuration Compliance enthält zwei Arten von Rechnern: Risiko-Rechner und Rollup-Rechner für Risikopunktzahlen. Diese Rechnergruppen sind standardmäßig aktiviert.

Die Rechnergruppe für die Risikopunktzahl wurde in Risikorechner umbenannt.

Die Rollup-Rechner für Risikopunktzahlen enthalten Rollup-Rechner für Konfigurationstests und Korrekturaufgaben.

Das Konfigurieren von Risiko- und Rollup-Rechnern für die Korrektur von Testergebnissen und Korrekturaufgaben umfasst folgende Aufgaben:

- Erstellen Sie einen Risikorechner
- Erstellen Sie einen Rollup-Rechner für die Risikopunktzahl

Nachdem Sie einen Risikorechner erstellt haben, ist er für Berechnungen mit der nächsten Datenerfassung verfügbar. Nachdem Sie sie erstellt haben, möchten Sie sie möglicherweise auch bei Bedarf anwenden.

Weitere Informationen zu Rechnern und Rechnergruppen finden Sie unter Konfigurations-Compliance Rechnergruppen.

Konfigurations-Compliance Übersicht über Ausnahmeverwaltung

Wenn Ihre Organisation eine veröffentlichte Richtlinie, einen Standard oder eine Leitlinie für das Schwachstellenmanagement oder die Sicherheit nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für eine Korrekturaufgabe, die nicht gemäß der Richtlinie behoben werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Die Ausnahmeverwaltung wird im Arbeitsbereich des Schwachstellenmanagers und im Arbeitsbereich für IT-Korrekturenunterstützt.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen anerkennen und ihnen zustimmen, wenn die konfigurationsbezogene Schwachstelle nicht behoben wird.

Lebenszyklus einer Ausnahme

Eine Ausnahme ist eine Anforderung, die Korrektur einer Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen.

Der Lebenszyklus einer Ausnahme ist wie folgt:

- Ausnahme wird angefordert
- Eine Ausnahmeanforderung wird genehmigt
- Verfolgen Sie eine Ausnahmeanforderung
- Ablauf einer Ausnahmeanforderung

Ausnahme wird angefordert

Als Korrekturbesitzer können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für eine Korrekturaufgabe anfordern. Während des Genehmigungsprozesses verbleibt die Korrekturaufgabe im Status **Wird überprüft**. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wechselt die Korrekturaufgabe in den Status **Zurückgestellt**.

Wichtig:
Sie können eine Ausnahme im Arbeitsbereich für IT-Fehlerkorrekturen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Eine Ausnahmeanforderung wird genehmigt

Korrekturaufgaben, die nicht sofort korrigiert werden können, werden überprüft, auf Risiken geprüft und zur Zurückstellung genehmigt, bis sie korrigiert werden können. Das Genehmigen einer Ausnahmeanforderung kann ein zweistufiger Workflow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger für hinzu Konfigurations-Compliance.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Sie können eine Ausnahmeanforderung im Arbeitsbereich des Schwachstellenmanagers genehmigen oder ablehnen. Weitere Informationen finden Sie unter Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace.

Hinweis:

Ab Konfigurations-Compliance v13.0 wird der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert, wenn Sie die Anwendung CC zum ersten Mal bereitstellen. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern.

Sobald eine Ausnahmeanforderung für eine Korrekturaufgabe genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Löschen

Hinweis:
Ablehnungskommentare werden in den Arbeitsnotizen für eine Korrekturaufgabe angezeigt. Wenn eine Ausnahmeanforderung abgelehnt wird, wird diese Korrekturaufgabe in den vorherigen Status zurückversetzt.

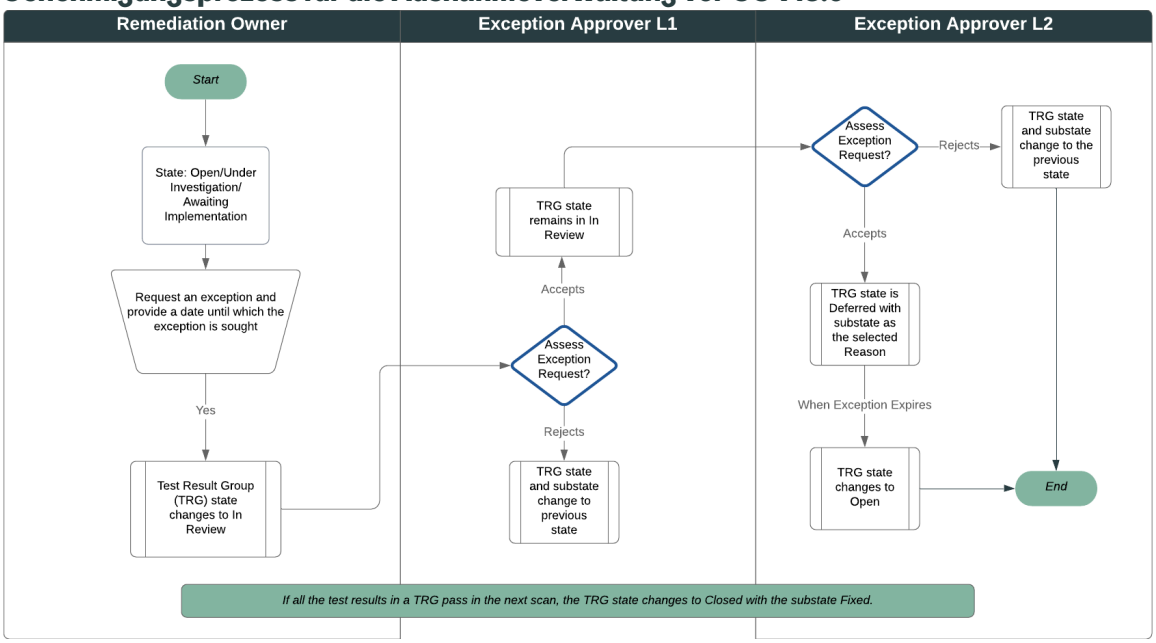
Verfolgen Sie eine Ausnahmeanforderung

Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status auf der Registerkarte **Change-Genehmigungen** im Status der Korrekturaufgabe nachverfolgen. Wenn eine Aktion für eine Korrekturaufgabe ausgeführt wird, können Sie den Status der einzelnen Testergebnisse in dieser Korrekturaufgabe nicht nachverfolgen.

Ablauf einer Ausnahmeanforderung

Wenn eine Ausnahmeanforderung für eine Korrekturaufgabe abläuft, wird die Korrekturaufgabe in den Status „ **Offen** “ zurückversetzt.

Genehmigungsprozess für die Ausnahmeverwaltung vor CC v13.0



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Change Management

Als IT-Korrekturbesitzer können Sie Change-Anforderungen (CHG) direkt aus Korrekturaufgaben (RTs) in der Anwendung Konfigurations-Compliance erstellen und verwalten.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Change-Anforderungen und den Workflow Konfigurations-Compliance .

Change-Anforderungen und Change-Management sind Teil des Nachbesserungsprozesses für den Workflow Konfigurations-Compliance. Während dieser Korrekturphase können Sie Change-Anforderungen verwenden, um Testergebnisse zu priorisieren, nachzuverfolgen und zu korrigieren.

Die Anwendung Konfigurations-Compliance arbeitet mit dem IT-Change-Management-Prozess Now Platform® zusammen, um Sie bei der Korrektur nicht konformer Software und Technologien in Ihrer Umgebung zu unterstützen.

Mit Change-Management in der Anwendung Konfigurations-Compliance können Sie Testergebnisse vorhandenen Change-Anforderungen zuordnen oder eine Korrekturaufgabe aufteilen und nur für ausgewählte Testergebnisse eine neue Korrekturaufgabe erstellen.

Weitere Informationen finden Sie unter Change-Anforderung in Konfigurations-Compliance erstellen.

Wichtige Begriffe

Tests

Tests sind Bibliotheken mit Datensätzen, die Scans von Computing-Assets organisieren. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets verwaltet werden soll. Ein Test ist alles, was verwendet werden kann, um eine Klasse von Software oder ein Hardware-Asset zu identifizieren, die nicht konform ist.

Testergebnisse

Testergebnisse werden von Drittanbieterintegrationen importiert. Sobald sie in Konfigurations-Compliancesichtbar sind, werden sie mit **Korrekturaufgaben**korrigiert. Gruppen werden zur Korrektur gemäß Zuweisungsregeln zugewiesen.

Hinweis:
Ab Version 14.9 von Konfigurations-Complianceträgt das Testergebnis die *Bezeichnung*Ergebnis.

Nachbesserungsaufgabe

Testergebnisse werden gemäß Zuweisungsregeln in Korrekturaufgaben gruppiert und automatisch Korrekturbesitzern zur Korrektur zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab Version 14.9 von Konfigurations-Compliancewird das Testergebnis als *Korrekturaufgabe*bezeichnet.

Testgruppen

Testgruppen beziehen sich auf autoritative Dokumente und Testdatensätze. Eine Gruppe von Konfigurationstests definiert Testgruppen.

Change-Anforderungen

Change-Anforderungen helfen Ihnen, kontrollierte Prozesse für die Remediation zu implementieren. Sie können Change-Anforderungen mit Korrekturaufgaben in Konfigurations-Compliance verwenden, um nicht konforme Assets (Konfigurationselemente) zu identifizieren, nachzuverfolgen und zu beheben, die zusätzliche Ressourcen erfordern oder die Sie zurückstellen möchten.

Weitere Informationen zu Testergebnissen und Korrekturaufgaben finden Sie unter Konfigurations-Compliance Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

Wann sollten Change-Anforderungen in verwendet werden? Konfigurations-Compliance

Change-Anforderungen helfen Ihnen, Korrekturaktivitäten für Ihre Testergebnisse zu initiieren und nachzuverfolgen. Wenn Korrekturbesitzer eine große Anzahl nicht korrigierter Testergebnisse oder Konfigurationselemente haben, können sie Change-Anforderungen verwenden, um Testergebnisse für die Zurückstellung zu identifizieren. Alternativ können sie Testergebnisse und Konfigurationselemente identifizieren und neu gruppieren, die mehr Ressourcen erfordern, als ursprünglich in der ursprünglichen Korrekturaufgabe identifiziert wurden.

Erstellen Sie Change-Anforderungen aus einer Korrekturaufgabe

Erstellen Sie eine Change-Anforderung direkt aus einer Korrekturaufgabe für alle Testergebnisse in der Korrekturaufgabe, oder verwenden Sie Filter, um nur Testergebnisse zu identifizieren, die bestimmten Kriterien entsprechen. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, um Ihre Untersuchung für Testergebnisse zu beschleunigen, die ein manuelles Eingreifen erfordern.

Teilen Sie eine Korrekturaufgabe auf

Identifizieren Sie in einer vorhandenen Korrekturaufgabe eine Teilmenge der Testergebnisse, die Sie in eine neue Korrekturaufgabe verschieben möchten. Durch das Erstellen einer neuen TRG können Sie mit einer bestimmten Gruppe von Testergebnissen arbeiten, ohne die ursprüngliche Korrekturaufgabe zu beeinträchtigen.

Ordnen Sie einer vorhandenen Change-Anforderung Testergebnisse zu

Ordnen Sie Testergebnisse vorhandenen Aufgaben zu, um zu vermeiden, dass bei der Lösung Ihrer Korrekturaufgaben doppelte Change-Anforderungen erstellt werden. Durch das Zuordnen einer Korrekturaufgabe zu einer Change-Anforderung, die bereits in Ihrer -Instanz verfügbar ist, können Sie eine vorhandene Aufgabenliste verwenden.

Arten von Change-Anforderungen für eine Korrekturaufgabe

Sie können Change-Anforderungen direkt von Ihnen zugewiesenen Korrekturaufgaben erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Standard Ein zuvor autorisierter Change, der als risikoarm und relativ gängig gilt und anhand eines festgelegten Verfahrens oder einer festgelegten Arbeitsanweisung implementiert wird.
- Normal Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsstufen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall Ein Change zur Lösung eines schwerwiegenden Incident.

Anwendung Konfigurations-Compliance einrichten, installieren und konfigurieren

Bevor Sie die Anwendung in der Instanz Now Platform® ausführen, müssen Sie zuerst die Anwendung Konfigurations-Compliance aus dem ServiceNow® Storeherunterladen und installieren. Diese Anwendung ist als separates Abonnement verfügbar.

Führen Sie vor der Installation die Schritte der Setup-Prüfliste aus, die in der folgenden Tabelle aufgeführt sind. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Weitere Informationen zu veröffentlichten Versionen der Anwendung Konfigurations-Compliance sowie zu Anwendungen von Drittanbietern und ServiceNow, die damit kompatibel sind, finden Sie im Artikel Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen [KB0856498] in der HI Knowledge Base.

Weitere Informationen zum Abrufen von Berechtigungen für Store-Apps finden Sie unter Security Operations und ServiceNow Store.

Richten Sie Prüflistenaufgaben ein

Setupaufgaben	Beschreibung
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn sie noch nicht zugewiesen sind, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle Konfigurations-Compliance-Administrator [sn_vulc.admin] zu. • Der Konfigurations-Compliance-Administrator [sn_vulc.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. • Der Korrekturbesitzer [sn_vulc.remediation_owner] liest und aktualisiert zugewiesene Datensätze. Die Rolle sn_vulc.remediation_owner wird auch automatisch zugewiesen, wenn einem Benutzer die Rolle itil zugewiesen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Prüflistenaufgaben ein (Fortsetzung)

Setupaufgaben	Beschreibung
Unterstützte Integrationen	Bevor Sie Konfigurations-Compliance zur Korrektur von Configuration Items verwenden können, müssen Sie die Scannerintegration einer Drittpartei installieren und mindestens einen Netzwerkscan durchführen. Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist, bevor Sie unterstützte Drittanbieterintegrationen konfigurieren. Weitere Informationen finden Sie unter Vulnerability Response installieren. Um zu überprüfen, ob Integrationsanwendungen installiert und aktiviert sind, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Weitere Informationen zu Integrationen von Drittanbietern und eine Liste der unterstützten Produkte finden Sie unter Konfigurations-Compliance-Integrationen.

Qualys Vulnerability Integration

- Wenn Qualys Vulnerability Integration bereits auf Ihrem System installiert ist und Ihre API-Anmeldeinformationen sich von denen unterscheiden, die Sie für Konfigurations-Complianceverwenden möchten, wechseln Sie zum Setup-Assistenten (in Vulnerability Response), und weisen Sie sie den einzelnen **Qualys-PC-** Integrationen zu.
- Navigieren zu **Qualys Schwachstellenintegration** > **Primäre Integrationen** und bearbeiten Sie das Feld **Qualys-API-Anmeldeinformationen** auf der Registerkarte **Qualys-REST-Details**.

Ausführliche Informationen zu Qualys Vulnerability Integrationfinden Sie unter Qualys Vulnerability Integration verstehen.

Sie können jetzt die Anwendung Konfigurations-Compliance installieren. Weitere Informationen finden Sie unter Konfigurations-Compliance installieren.

Konfigurations-Compliance installieren

Bevor Sie Konfigurations-Compliance in der Instanz Now Platform® ausführen, müssen Sie zuerst die Anwendung Konfigurations-Compliance aus dem ServiceNow Storeherunterladen und installieren. Diese Anwendung ist als separates Abonnement verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Führen Sie vor der Installation die in Anwendung Konfigurations-Compliance einrichten, installieren und konfigurieren beschriebene Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich. Erforderliche Rolle: admin

Prozedur

1. Um ServiceNow -Produkte zu aktivieren, führen Sie die Schritte in Opt in to the ServiceNow Store products aus.
2. Um eine Anwendung zu installieren, die Sie bei ServiceNow Storeerworben haben, führen Sie die Schritte in Install a ServiceNow Store application aus.
3. **Wahlweise:** Wenn Sie Ihre Berechtigung für die Anwendung Konfigurations-Compliance in anderen Instanzen Now Platform verwalten möchten, führen Sie alternativ die Schritte in Manage entitlements from your ServiceNow instance aus.
4. Wenn Sie die Anwendung Konfigurations-Compliance bereits installiert haben und aktualisieren, finden Sie weitere Informationen unter Install an update to a ServiceNow Store application .
5. Installieren Sie unterstützte Anwendungen.

   Separate Anwendungen von Drittparteien erfassen und transformieren Daten in Konfigurations-Compliance. Bevor Sie Konfigurations-Compliance zur Korrektur von Configuration Items verwenden können, müssen Sie die Scannerintegration einer Drittpartei installieren und mindestens einen Netzwerkscan durchführen.

   Informationen zur Installation von Drittanbieterintegrationen für Konfigurations-Compliancefinden Sie unter Konfigurations-Compliance-Integrationen.

Erstellen oder bearbeiten Sie Konfigurations-Compliance -Zuweisungsregeln

Erstellen Sie Regeln, um Testergebnisse basierend auf Filterbedingungen automatisch zuzuweisen. Diese Regeln weisen Testergebnisse zu, während sie importiert werden.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem enthält eine Zuweisungsregel Konfigurations-Compliance, **An CI-Supportgruppe zuweisen**, die Testergebnisse der gleichen Zuweisungsgruppe wie die CI-Supportgruppe zuweist. Diese Regel ist standardmäßig inaktiv. Sie können mithilfe von Filterbedingungen Änderungen vornehmen. Mit Zuweisungsregeln definieren Sie eine oder mehrere Zuweisungsbedingungen und die Reihenfolge der Ausführung. Sobald ein Testergebnis mit einer Regelbedingung übereinstimmt, wird die Zuweisungssuche beendet.

Hinweis:
Neue oder aktualisierte Regeln werden beim nächsten Import automatisch oder manuell über die Schaltfläche **Changes anwenden** in der Liste Zuweisungsregeln ausgewertet.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Zuweisungsregeln**.
2. Öffnen Sie die Regel **An CI-Supportgruppe zuweisen**, oder klicken Sie auf **Neu**.
3. Bearbeiten Sie die Regel **Zu CI-Supportgruppe zuweisen**, oder füllen Sie, falls **neu**, die Felder des Formulars entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance-Zuweisungsregel

Feld	Beschreibung
Name	Der Name der Zuweisungsregel
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Die niedrigste Zahl wird zuerst ausgewertet. Regeln mit hoher Priorität, Testergebnisse, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist, oder ein Testergebnis, das von der Compliance-Abteilung behandelt werden sollte, sollten zuerst ausgeführt werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist und Sie wissen, wer dafür verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel zum Zuweisen von Testergebnissen an die Gruppe, die festlegt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt.
Aktiv	Gibt an, ob die Zuweisungsregel aktiv ist.
Bedingung	
Bedingungsfelder	Bedingungen, die erfüllt werden müssen. Die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.
Neues Kriterium	Fügt weitere Bedingungsfilterfelder zur Auswahl hinzu.
Beschreibung	Text, der die Zuweisungsregel beschreibt.
Zuweisen mit	Um die Zuweisung von anhand dieser Regel erstellten Gruppen zu automatisieren, wählen Sie eine der verfügbaren Optionen aus. ○ Anwendergruppe: Wählen Sie eine Anwendergruppe aus der Suchtabelle aus ○ Anwendergruppenfeld: Wählen Sie ein Anwendergruppenfeld aus dem Dropdown-Menü aus. ○ Skript: Erstellen oder bearbeiten Sie ein Skript. **Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert das Fachwissen ServiceNow.
Anwendergruppenfeld	Wählen Sie die Anwendergruppe aus, die für die Korrektur von Tests verantwortlich ist, die den Bedingungen der Zuweisungsregeln entsprechen.

4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Korrekturzielregeln

Mit Korrekturzielregeln können Sie die erwarteten Zeitrahmen für die Korrektur von Testergebnissen festlegen. Sie können Benachrichtigungen an Benutzer und Gruppen senden, wenn Zieldaten näherkommen und überfällig sind.

Wichtig:
Als Konfigurations-Compliance-Administrator oder -Analyst können Sie im Arbeitsbereich des Schwachstellen-Managers das späteste Nachbesserungszieldatum für eine bestimmte Gruppe von Testergebnissen abrufen. Diese Methode ist effizienter als die Ausführung der Korrekturzielregeln für alle Testergebnisse in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace.

Erforderliche Rolle: Configuration Compliance-Administrator (sn_vulc_admin) oder ein -Manager mit der Rolle sn_vulc.manage_remediation_target_rules.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Korrekturzielregeln

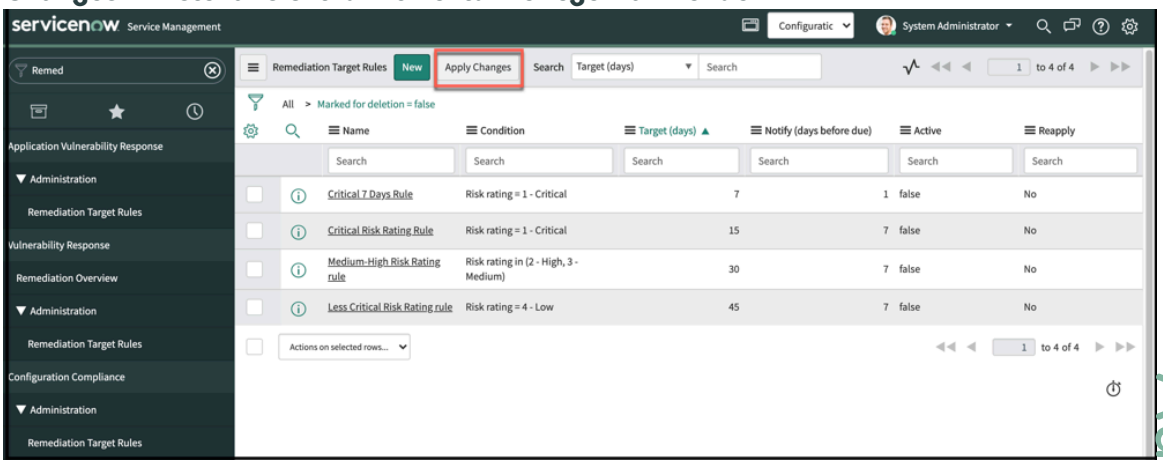
Die regelmäßige -Aufgabe *`Evaluate and notify remediation targets`*wird täglich ausgeführt und verwendet aktive Korrekturzielregeln, um aktive Testergebnisdatensätze auszuwerten. Immer wenn Testergebnisdatensätze, die Korrekturaufgaben zugeordnet sind, aktualisiert oder geändert werden, werden die geänderten Werte anhand der Zielregeln ausgewertet, und die Änderungen werden zusammengefasst und für die zugehörigen Korrekturaufgaben angezeigt.

Sie können vorhandene Korrekturzielregeln bearbeiten, deaktivieren oder löschen und neue erstellen. Wenn Sie eine Regel ändern, deaktivieren oder neu erstellen, können Sie in der Listenansicht Korrekturzielregeln **auf Änderungen anwenden** klicken und die Änderungen, die Sie vor der nächsten geplanten Aufgabe vorgenommen haben, manuell anwenden. Mit dieser Option können Sie Ihre Testergebnisdatensätze ohne Wartezeit neu auswerten. Wenn Sie Ihre Changes nicht manuell anwenden, werden Ihre Changes von der nächsten täglichen geplanten Aufgabe übernommen und angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Korrekturzielregeln** um Korrekturzielregeln anzuzeigen.

Changes in Listenansicht für Korrekturzielregeln anwenden



2. Klicken Sie in der Namensspalte auf eine Regel, um den zugehörigen Datensatz zu öffnen.
3. Aktivieren Sie das Kontrollkästchen **Aktiv** für den Datensatz der Korrekturzielregel, um deaktivierte Regeln (falsch) zu aktivieren (wahr).

Wenn Sie eine Zielregel ändern oder hinzufügen, werden Ihre Änderungen unabhängig davon, ob Sie die Änderungen manuell anwenden oder auf die nächste geplante Aufgabe warten, verwendet, um alle aktiven Testergebnisse zusammen mit allen anderen Zielregeln auszuwerten, die von Ihren Änderungen betroffen sind. Wenn Sie die Änderungen manuell anwenden, kann diese Auswertung einige Zeit in Anspruch nehmen, wenn Sie über eine große Menge aktiver Testergebnisse verfügen, da alle Regeln, die von Ihren Änderungen betroffen sind, für eine Auswertung verwendet werden.

Der Standardwert für die Tage für gezielte Korrekturen beträgt beispielsweise 30. Wenn Sie eine neue Regel erstellen, die für Gezielte Korrekturtage auch 30 hat, werden diese Regel und alle Zielregeln mit 30 Tagen oder mehr als Zieldatum jeweils auf Ihre Testergebnisse angewendet.

Deaktivierte und gelöschte Zielregeln

Wenn eine Regel aktiv ist, wird in der Spalte „Aktiv“ in der Listenansicht der Korrekturzielregeln „true“ angezeigt. Nachdem eine Regel deaktiviert wurde (false), wird sie nicht mehr auf neue Testergebnisse angewendet. Die geplante Aufgabe verfolgt jedoch weiterhin alle vorhandenen Testergebnisse, auf die die Regel angewendet wurde. Wenn die deaktivierte(n) Regel(n) anschließend erneut aktiviert wird/werden, wird jedes Testergebnis mit einem leeren Feld **für das Korrekturzieldatum** anhand der reaktivierten Regeln ausgewertet. Dies schließt Testergebnisse ein, die erstellt wurden, während die Regeln deaktiviert waren.

Wenn Regeln gelöscht werden, werden das **Zieldatum der Korrektur** und zugehörige Felder geschlossener Testergebnisse beibehalten. Das **Zieldatum der Korrektur** und zugehörige Felder für nicht geschlossene Testergebnisse werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

Um eine Regel zu deaktivieren, deaktivieren Sie im Datensatz der Korrekturzielregel das Kontrollkästchen aktiv, und klicken Sie auf **Aktualisieren**. In der Spalte „Aktiv“ in der Listenansicht „Korrekturzielregeln“ wird„falsch“ angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie zum Löschen einer Regel **auf Löschen** im Formular, oder wählen Sie alternativ in der Listenansicht die Regel(n) aus, und klicken Sie in der Liste **Aktionen für Zeilen aufLöschen**. Die Regel wird nicht mehr in der Liste angezeigt, und die nächste Regel in der Reihenfolge des Vorgangs ersetzt die gelöschte Regel.

Wenn Sie eine Regel deaktivieren oder löschen und Ihre Änderungen vor der nächsten geplanten Aufgabe anwenden, wird der Regelverweis aus dem Feld gelöscht, das Korrekturdatum und die Statusdaten bleiben jedoch erhalten. Wenn Sie Ihre Änderungen nicht manuell anwenden, wird der Regelverweis aus dem Feld mit der nächsten geplanten Aufgabe gelöscht.

Über Zielregeln und die geplante Aufgabe Korrekturziele auswerten und benachrichtigen

Die geplante Aufgabe *`Evaluate and notify remediation targets`* wird einmal täglich um 4:30:00 Uhr ausgeführt. Es ruft alle aktiven Korrekturzielregeln ab und wertet alle aktiven Testergebnisse aus, beginnend mit den Testergebnissen mit dem frühesten Korrekturzieldatum. Es wertet alle Testergebnisse aus, die die folgenden Kriterien erfüllen:

- Befinden sich nicht im Status **„Geschlossen“**.
- Hat kein Korrekturzieldatum.
- Sie weisen Korrekturzieldaten auf, die nach den Datumsangaben in den Korrekturzielregeln liegen.
- Werden erstellt, nachdem ein Scannerimport abgeschlossen wurde. Die regelmäßige Aufgabe greift auf und wertet alle neuen Testergebnisse aus, die infolge eines Imports erstellt wurden.

Nachdem eine Zielregel definiert wurde, werden Korrekturzieldaten von der geplanten Aufgabe *`Evaluate and notify remediation targets`* berechnet. Die geplante Aufgabe fügt ein Korrekturzieldatum hinzu, falls keines vorhanden ist, oder aktualisiert das vorhandene Zieldatum, wenn diese Regel ein früheres Datum als das im Datensatz enthaltene enthält.

Alle abgelaufenen Datensätze und Erinnerungsdaten, die den Zielregeln entsprechen, werden von der Aufgabe aufgenommen, und es werden Benachrichtigungen gesendet. Bei deaktivierten Regeln löscht die Aufgabe die Korrekturfelder in den Testergebnisdatensätzen und sendet keine Benachrichtigungen mehr.

Wenn die Eigenschaft „sn_sec_cmn.evaluate_targetmissed_records“ aktiviert ist, wird verhindert, dass die geplante Aufgabe *`Evaluate and notify remediation targets`* das Ziel der verfehlten Testergebnisse auswertet. Diese Eigenschaft ist standardmäßig aktiviert.

Zieldaten und Status werden in Listen- und Formularansichten angezeigt

Konfigurations-Compliance -Manager können das Zieldatum der Korrektur sowohl im Testergebnisformular als auch in der Listenansicht anzeigen. Korrekturzielregeln werden auch nach dem Import eines Scanners ausgeführt und erneut ausgeführt, wenn ein Testergebnis erneut geöffnet wird.

Die regelmäßige Aufgabe aktualisiert das **Korrekturziel** und **den Korrekturstatus** in der Listenansicht der Testergebnisse sowie die Felder **Korrekturzielregel**, **Korrekturziel**und **Korrekturstatus** im Formular „Testergebnis“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

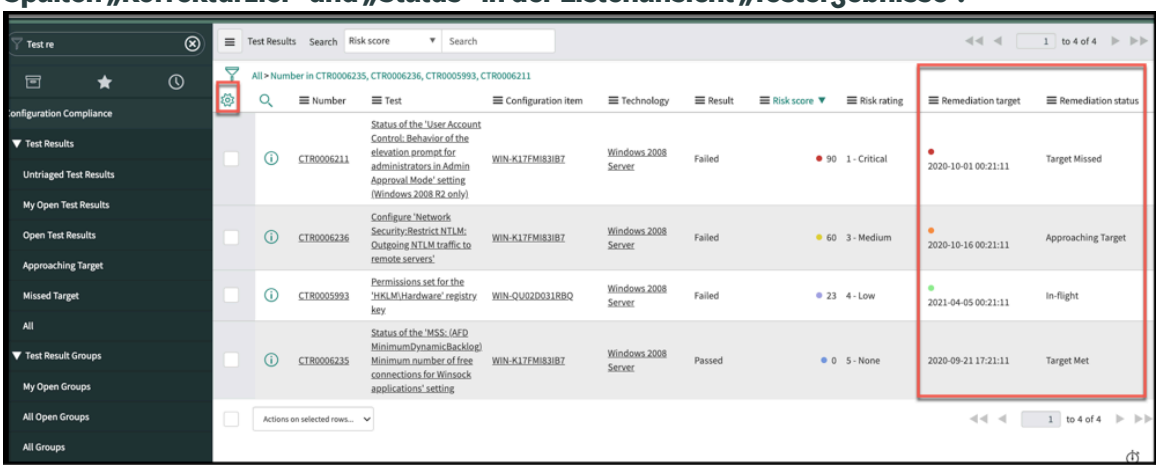
Standardmäßig werden die Spalten **„Korrekturziel“** und **„Korrekturstatus“** in der Listenansicht „Testergebnisse“ nicht angezeigt. Um diese Spalten anzuzeigen, müssen Sie sie auch der Listenansicht hinzufügen. Fügen Sie dem Testergebnisformular auf ähnliche Weise die Felder **Korrekturzielregel**, **Korrekturziel**und **Korrekturstatus** hinzu.

Verwenden Sie die Slushbuckets in den Menüs Einstellungen bzw. Zusätzliche Aktion (siehe folgende Abbildungen), um diese Spalten und Felder anzuzeigen. Klicken Sie für das Menü Zusätzliche Aktion im Testergebnisdatensatz auf das Menüsymbol, gefolgt von **Konfigurieren** und **Formularlayout,** um den Slushbucket anzuzeigen und die Felder von **Verfügbar** in **Ausgewählt**zu verschieben.

Das Zieldatum der Korrektur wird in der Listenansicht der Testergebnisse als farbige Punkte codiert:

- Testergebnisse, deren Benachrichtigungsdatum noch nicht erreicht ist, werden grün angezeigt.
- Testergebnisse, die sich dem Korrekturzieldatum nähern, werden orange angezeigt.
- Testergebnisse, die nach dem Korrekturzieldatum liegen, werden rot angezeigt.

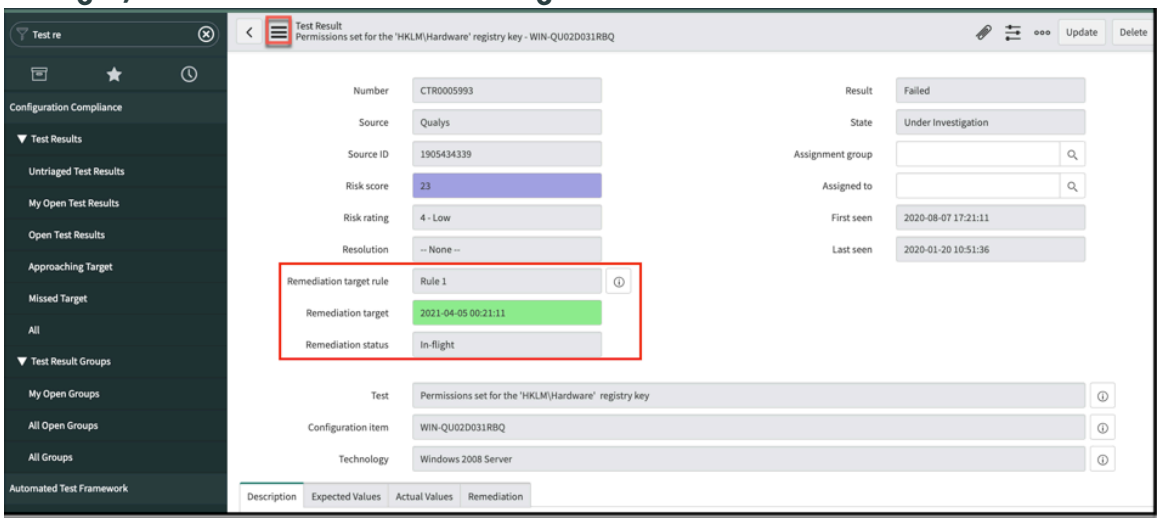
Spalten „Korrekturziel“ und „Status“ in der Listenansicht „Testergebnisse“.



- Ziel verfehlt: Das Zieldatum ist überfällig
- In Ausführung: Das Testergebnis ist in Bearbeitung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zielregel-, Ziel- und Statusfelder im Testergebnis-Datensatz



Testergebnisdatensätze werden auch visuell im Dashboard Konfigurations-Compliance angezeigt. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Übersicht** und überprüfen Sie das Dashboard auf den Status. Die Übersicht enthält vorhandene Widgets und den Korrekturstatus. Die Farben der Diagramme entsprechen den Farben, die in der Listenansicht der Testergebnisse und im Testergebnis-Datensatz angezeigt werden.

Szenario für Korrekturzielregel

Wenn mehrere Korrekturzielregeln auf dasselbe Testergebnis angewendet werden, wird die restriktivste Regel angewendet.

Wenn beispielsweise ein Testergebnis, das erstmals am 01.03.2018 identifiziert wurde, die Bedingungen für zwei Korrekturzielregeln erfüllt:

- Korrekturzielregel 1: Definiert am 03.07.2018; Korrekturziel ist 15 Tage seit der ersten Sichtung; Das berechnete Zieldatum der Korrektur ist der 16.03.2018 10:00:00.
- Korrekturzielregel 2: Definiert am 10.03.2018; Korrekturziel ist 10 Tage seit der ersten Sichtung; Das berechnete Zieldatum der Korrektur ist der 11.03.2018 10:00:00.

Hinweis:

Korrekturziele werden aus dem Datum der **letzten Anzeige** plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.

Ab V14.5 werden Korrekturziele anhand des **Ziels ab (Datum)**berechnet. Der Standardwert bleibt **Zuletzt Gesehen**. Ab v14.12 ist der Standardwert **„Letzte Übergabe“**.

In diesem Szenario gilt Korrekturzielregel 2 für das Testergebnis, da es das restriktivere Datum aufweist: 10 Tage seit der ersten Identifizierung des Testergebnisses gegenüber 15 Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen oder ändern Sie Zielregeln, und wenden Sie Änderungen erneut an

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Korrekturzielregeln** zum Anzeigen, Bearbeiten und Erstellen neuer Korrekturzielregeln.
2. Klicken Sie in der Spalte Name auf eine Regel, um eine Zielregel zu öffnen und den Datensatz zu bearbeiten, oder klicken Sie alternativ auf **Neu**, um eine neue Zielregel zu erstellen.
3. Füllen Sie das Formular aus, um den erwarteten Zeitrahmen für die Korrektur zu definieren, geben Sie an, für welche Testergebnisse diese Regel mit Bedingungen gilt, und legen Sie fest, wann Erinnerungen an Anwender und/oder Gruppen gesendet werden sollen.

Formular „Remediationszielregel“.

Feld	Beschreibung
Name	Name für Ihre Regel.
Aktiv	Aktivieren oder deaktivieren Sie die Regel. Die Regel ist standardmäßig automatisch aktiviert (wahr) und wird auf Ihre Testergebnisse angewendet, wenn Sie Änderungen manuell oder nach der nächsten geplanten Aufgabe anwenden.
Ziel (Tage)	Legen Sie die angestrebte Frist für die Remediation in Tagen fest. Der Standardwert für die Tage der gezielten Remediation ist 30. Wenn Sie beispielsweise eine neue Regel erstellen, bei der der Zielwert ebenfalls 30 ist, werden Ihre neue Regel und alle anderen vorhandenen Regeln, die ebenfalls 30 Tage oder länger als Zieldatum haben, auf Ihre Testergebnisse angewendet.
Ziel ab (Datum)	Datum, ab dem die Zieldaten berechnet werden. Sie können nur das Datum oder die Felder für den Datums- und Uhrzeittyp angeben. Ab v14.12 ist der Standardwert *Letzte Übergabe*. Wählen Sie eine der folgenden Optionen aus: ○ Zuletzt gesehen ○ Zuerst gesehen ○ Erstellt ○ Letzte Übergabe Wenn der letzte Durchlauf leer ist, wird das Erstellungsdatum für die Berechnung des Korrekturziels berücksichtigt. ○ Zuletzt geöffnet Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1642413 .
Benachrichtigen (Tage vor dem Fälligkeitsdatum)	Legen Sie eine Anzahl von Tagen vor dem Stichtag fest, um Anwender und Gruppen daran zu erinnern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Kurze Beschreibung der Regel.
Bedingung	Verwenden Sie den Bedingungsgenerator, um die Testergebnisse anzugeben, für die diese Regel gilt. Legen Sie beispielsweise ein Korrekturzieldatum von 30 Tagen für alle Testergebnisse mit Risikopunktzahlen über 70 fest. Sieben Tage vor dem Korrekturdatum Erinnerungen an Anwender und/oder Gruppen senden. Die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt. Vor v12.0 wird die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext unterstützt, den Sie im Bedingungsgenerator eingeben.
Benutzer und/oder Benutzergruppen	Wählen Sie Anwender oder Gruppen oder beides aus, um Benachrichtigungen über die von Ihnen festgelegten bevorstehenden und überfälligen Zieldaten zu senden.

4. Klicken Sie auf **Absenden**. Um bearbeitete Regeln zu speichern, klicken Sie alternativ auf **Aktualisieren**.

   Die Listenansicht wird mit Ihrer aktualisierten oder neuen Regel angezeigt. Die Regeln in der Liste werden beginnend mit der Regel mit dem niedrigsten Korrekturzieldatum sortiert und ausgeführt. Wenn Sie eine Regel deaktivieren oder löschen, ersetzt die nächste Regel in der Reihenfolge die inaktive oder gelöschte Regel.

5. Um die neuen Änderungen jetzt anzuwenden, klicken Sie auf **Änderungen übernehmen**.

Konfigurations-Compliance Rechnergruppen

Konfigurations-Compliance -Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner sind nach den Kriterien gruppiert, mit denen bestimmt wird, wie die Datensätze aktualisiert werden.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Rechnergruppen

Aus dem Datensatz des Standardrisikorechners können Rechnerregeln bei Bedarf auf alle betroffenen Testergebnisse und Sammlungen angewendet werden. Schwachstellenmanager können mit dieser Funktion die Konfiguration des Risikorechners anpassen. Sie können zu Beginn der Bereitstellung mit mehreren Priorisierungsschemata experimentieren und diese Änderungen bei Bedarf anwenden, um zu sehen, wie sie sich auf die Importergebnisse auswirken.

Die Rechnergruppe für die Risikopunktzahl wurde in Risikorechner umbenannt.

Rollup-Rechner für Risikopunktzahlen sind im Lieferumfang von Konfigurations-Complianceenthalten. Es gibt zwei Arten von einzelnen Rollup-Rechnern:

Konfigurationstest-Risiko-Rollup

Rechner, die Risikopunktzahlen für alle Testergebnisse mit demselben Konfigurationstest zusammenfassen, um eine Gesamtrisikopunktzahl für den Konfigurationstest bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt.

Rollup der Korrekturaufgaben-Risikobewertung

Diese Rechner fassen die Risikopunktzahlen für alle Testergebnisse in einer Korrekturaufgabe zusammen, um eine Gesamtrisikopunktzahl für diese Korrekturaufgabe bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt.

Sowohl die Rechnergruppe für die Risikopunktzahl als auch die Gruppe der Rollup-Rechner für die Risikopunktzahl sind standardmäßig aktiviert.

Weitere Informationen finden Sie unter den folgenden Schlüsselbegriffen für Konfigurations-Compliance -Rechner:

Testergebnis

Ein Testergebnis ist das Ergebnis des Konfigurationstests für ein Configuration Item (CI) und die zugehörige Technologie. Testergebnisse in den Status „Fehlgeschlagen“, „Fehler“ und „Unbekannt“ identifizieren Hardware, Software und Assets, die nicht mit Ihren Richtlinien übereinstimmen.

Nachbesserungsaufgabe

Testergebnisse werden zum Zeitpunkt des Datenimports basierend auf den vordefinierten Regeln für Korrekturaufgaben gruppiert. Diese Korrekturaufgaben ähneln Schwachstellen-Gruppen in Vulnerability Response. Korrekturaufgaben organisieren Testergebnisse in Gruppen für die Massenanalyse und stellen einen Satz von zu korrigierenden Elementen dar.

Risikopunktzahl in einem Testergebnis

Ein von Risikopunktzahl-Rechnern berechneter Wert, der auf dem Geschäftskontext eines Assets und dem Schweregrad des zugehörigen Tests basiert. Dies ist der Durchschnitt der Geschäftskritikalität des betroffenen Asset, wie in der CMDB definiert, und der Schweregrad des Tests, wie vom Scanner übermittelt.

Jedem Asset können mehrere Services zugeordnet sein. Die Geschäftskritikalität eines Assets wird durch den Service mit der höchsten Relevanz bestimmt.

Der berechnete Wert wird in den Feldern „Risikopunktzahl“ der Testergebnisse angezeigt. Die Punktzahlen zeigen Werte im Bereich von 0 bis 100 an. Felder sind auch farbcodiert, um Ihnen den Schweregrad auf einen Blick zu zeigen.

Risikopunktzahl in Korrekturaufgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Punktzahl wird im Datensatz der Korrekturaufgabe angezeigt und ist der zusammengefasste Wert der Risikopunktzahlen für alle aktiven Testergebnisse in einer Korrekturaufgabe. Diese Punktzahl ändert sich, wenn Testergebnisse in der Korrekturaufgabe korrigiert werden.

Risikopunktzahl im Konfigurationstest

Diese Punktzahl wird bei Konfigurationstests angezeigt und ist der zusammengefasste Wert der Risikopunktzahlen für alle aktiven Testergebnisse mit diesem Konfigurationstest. Diese Punktzahl ändert sich, wenn die Testergebnisse, die diesem Konfigurationstest zugeordnet sind, korrigiert werden.

Risikobewertung

Das Risiko, das ein fehlgeschlagenes Testergebnis für Ihr System darstellt. Sie basiert auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, die Risiken als kritisch (1) bis keine (5) bewertet. Die Punktzahl basiert auf einem Bereich von Risikopunktzahlen und wird in den Feldern Risikoeinstufung angezeigt.

Risikoeinstufungsbereiche

Risikobewertung	Risikopunktzahl
1 – Kritisch	90 bis 100
2: Hoch	70 bis 89
3: Mittel	40 bis 69
4: Niedrig	1 bis 39
5: Keine	0

Rollup-Rechner für Risikopunktzahlen

Es gibt zwei Arten von Rollup-Rechnern:

- Konfigurationstest-Risiko-Rollup: Diese Rechner fassen Risikopunktzahlen für alle Testergebnisse mit demselben Konfigurationstest zusammen, um eine Gesamtrisikopunktzahl für den Konfigurationstest bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt. Sie können die Skriptwerte für Gewichtung und Punktzahl für diese Rechner bearbeiten.
- Rollup der Risikopunktzahl für Korrekturaufgabe: Diese Rechner fassen Risikopunktzahlen für alle Testergebnisse in einer Korrekturaufgabe zusammen, um eine Gesamtrisikopunktzahl für diese Korrekturaufgabe bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt. Sie können die Skriptwerte für Gewichtung und Punktzahl für diese Rechner bearbeiten. Ein Beispiel für einen Rollup-Rechner für Risikopunktzahlen und wie er Punktzahlen berechnet, finden Sie unter Berechnungsbeispiel für Risiko-Rollup für Konfigurations-Compliance (vor v15.0).

Historische Risikopunktzahl

Die inhärente Risikopunktzahl für alle bestandenen Testergebnisse in einer Korrekturaufgabe. Dieses Feld zeigt das Ausmaß des Risikos an, das von einer Testgruppe behoben wurde. Es wird nur angezeigt, wenn sich eine Testgruppe im Status „Geschlossen“ befindet und die Risikopunktzahl null ist.

Punktzahlen werden immer dann berechnet, wenn sich die Risikopunktzahl ändert oder wenn Testergebnisse einer Korrekturaufgabe hinzugefügt oder daraus entfernt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Um ordnungsgemäß zu funktionieren, benötigt das Skript das Plugin Service-Mapping. Service-Mapping ist als separates Abonnement verfügbar und erfordert die Aktivierung durch Mitarbeiter ServiceNow von .

Erstellen Sie eine Rechnergruppe Konfigurations-Compliance .

Konfigurations-Compliance Rechnergruppen werden verwendet, um Rechner je nach Verwendungszweck zu gruppieren.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Das -Basissystem Konfigurations-Compliance enthält eine Rechnergruppe: **Risikopunktzahl**. Wenn Sie weitere Rechner erstellen, können Sie sie dieser Gruppe hinzufügen oder andere Gruppen und Rechner erstellen. In jeder Gruppe wird der erste Rechner ausgeführt, der dem Testergebnis entspricht.

Die Anwendung Configuration Compliance enthält zwei Rechnergruppen:

- Risikorechner
- Rollup-Rechner für Risikopunktzahl

Risikorechner berechnen die Risikopunktzahl und Risikobewertung eines Testergebnisses.

Rollup-Rechner für Risikopunktzahlen addieren Risikopunktzahlen für alle Testergebnisse und Korrekturaufgaben mit demselben Konfigurationstest, um eine Gesamtrisikopunktzahl bereitzustellen.

Sie können auch direkt von diesen Gruppen aus neue Rechner erstellen.

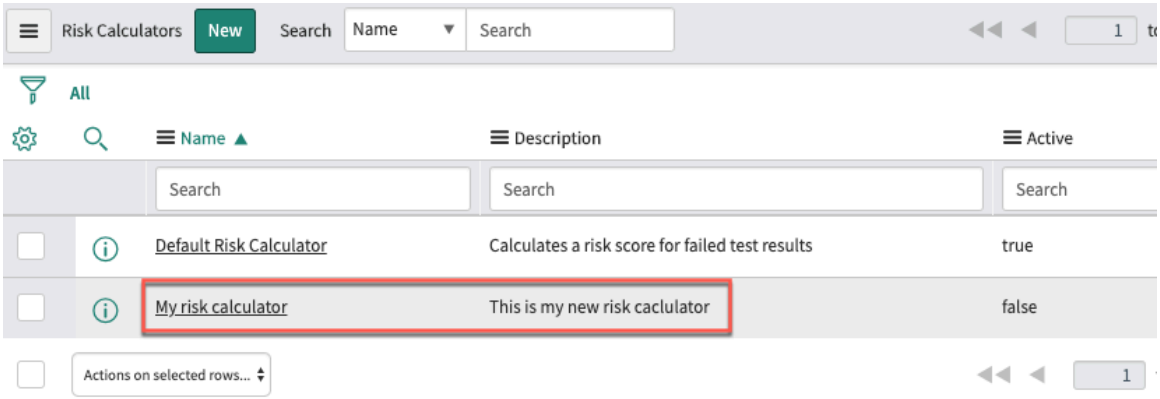
Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Rechnergruppen**.
2. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** und wählen Sie **Risikorechner** oder **Rollup-Rechner für Risikopunktzahl**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

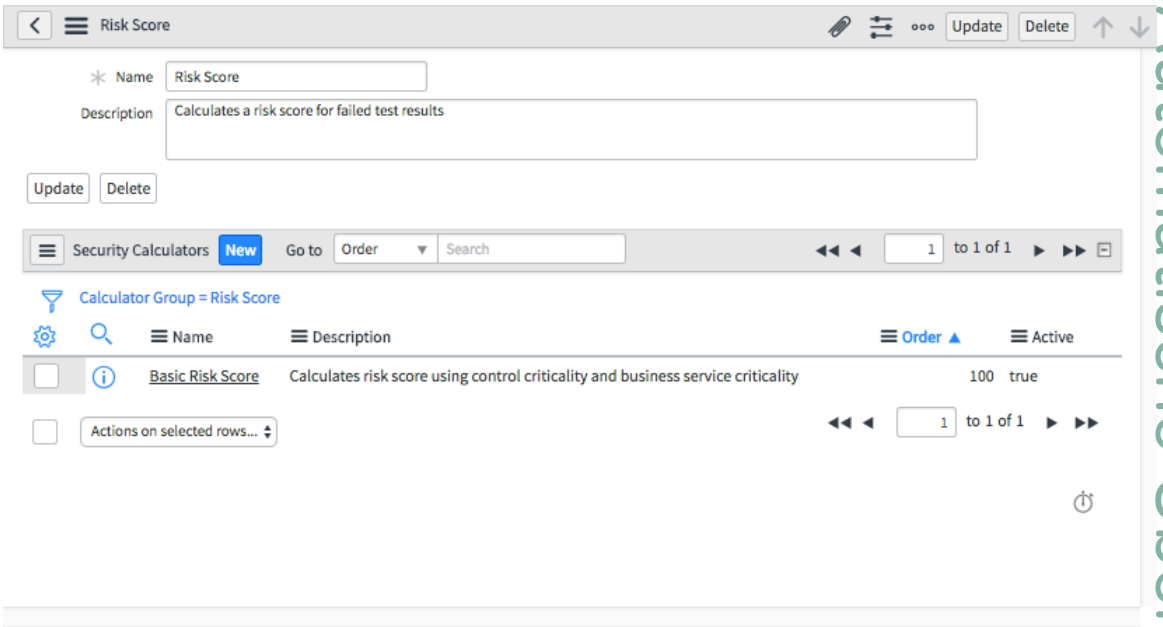
Feld	Beschreibung
Name	Der Name des Rechners.
Beschreibung	Eine Beschreibung dieser Rechnergruppe.
Aktiv	Rechnergruppe aktivieren oder deaktivieren.

5. Klicken Sie im Header des Formulars mit der rechten Maustaste **auf Speichern**, oder wählen Sie **Absenden aus**.
Die neue Rechnergruppe wird zusammen mit den anderen Rechnern in der Gruppenliste angezeigt. Klicken Sie auf den Namen der neuen Rechnergruppe, um den Datensatz zu öffnen. Unter Risikorechner für erstellen, bearbeiten und erneut anwenden Konfigurations-Compliance finden Sie weitere Informationen zum Festlegen von Bedingungen und angezeigten Werten sowie zum erneuten Anwenden von Rechnern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die zugehörige Liste **„Sicherheitsrechner“** wird angezeigt.



6. Klicken Sie auf **Neu**, um der Gruppe Rechner zusammen mit ihren Bedingungen hinzuzufügen.

Die Berücksichtigung von Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.

Automatische Übersetzung

Konfigurations-Compliance Rechner und Rechnerregeln

Konfigurations-Compliance Automatisieren Sie die Berechnung von Anfangswerten für die Felder in den Testergebnissen. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste passende Rechner wird verwendet.

Konfigurations-Compliance Rechner

Das Basissystem für Konfigurations-Compliance enthält einen Konfigurations-Compliance-Rechner (**Standardrisiko-Rechner**), der die Basis- **Risikopunktzahl** anhand des Testergebnisses festlegt. Konfigurations-Compliance-Rechner können so erstellt werden, dass sie Testergebnisse basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern priorisieren und bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle oder die Klasse des Konfigurationselements (Configuration Item, CI)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

handelt, können Sie zusätzliche Konfigurations-Compliance-Rechner erstellen, um andere Felder für Testergebnisse festzulegen, oder Sie können die vorhandenen Konfigurations-Compliance-Rechner anpassen. Ein Rechner kann so geschrieben werden, dass er jeden Satz von Prioritäten widerspiegelt.

Jeder Rechner enthält eine Liste von Rechnerregeln, wobei eine Bedingung bestimmt, wann sie angewendet wird. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel der Reihe nach ausgewertet, und die erste passende Rechnerregel wird verwendet.

Alle aktivierten Rechner für Konfigurations-Compliance legen die ausgewählten Felder jedes Mal fest, wenn ein Testergebnis erstellt wird, wenn sich ein zugeordneter CI- oder Konfigurationstest ändert oder wenn der zugehörige Link **Risikopunktzahl berechnen** in einem Testergebnis verwendet wird. Beispielsweise wird die Risikopunktzahl in Testergebnisdatensätzen automatisch aktualisiert, wenn der Wert für „control.criticality“ in einem importierten Testergebnis aktualisiert wird. Nachdem ein Testergebnisimport eine Testergebnispunktzahl aktualisiert hat, können Sie die Risikopunktzahl der Testergebnisse neu berechnen, indem Sie auf die Schaltfläche **Rechner erneut** anwenden klicken.

Wenn Sie aus einem vorhandenen Testergebnis den zugehörigen Link **Risikopunktzahl berechnen** auswählen und einer der Rechner aktiviert ist, wird das Feld Risikopunktzahl im Testergebnis aktualisiert.

Hinweis:

- Der zugehörige Link **Risikopunktzahl berechnen** ist nur sichtbar, wenn mindestens ein Konfigurations-Compliance-Rechner aktiviert ist.
- Ab v22.0 von Vulnerability Responsekönnen Sie die Risikopunktzahl für ein Testergebnis im Vulnerability Manager-Arbeitsbereich und im IT-Nachbesserungs-Arbeitsbereich aktualisieren, indem Sie in der zugehörigen Datensatzansicht auf die Schaltfläche **Risikopunktzahl berechnen** klicken.
- Ab Version 14.13 von Konfigurations-Compliancewerden bei jeder Änderung der Risikopunktzahl für ein Testergebnis die folgenden Details im Abschnitt „Hinweise“ des Testergebnisses dokumentiert:
  - Name der Rechnergruppe
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, werden dem Namen die Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und aktivieren Sie das Kontrollkästchen **Erweiterte Ansicht**. Wählen Sie im Dropdown-Feld **Werttyp** die gewünschte Option aus. Wenn **Vorlage** ausgewählt ist, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** ausgewählt ist, können Sie entweder das vorhandene Skript hinzufügen oder aktualisieren.
  - Feldwerte mit ihrer Gewichtung und ihrem Beitrag zur Risikopunktzahl
  - Endgültige Risikopunktzahl
  - Die Systemeigenschaft *sn_sec_cmn.risk_score_changes_add_worknotes* hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v15.2.1 von Konfigurations-Complianceist die Systemeigenschaft *sn_sec_cmn.risk_score_changes_add_worknotes* standardmäßig inaktiv. Wenn Sie die Option aktivieren, können Sie nur dann im Abschnitt „Arbeitsnotizen“ alle Änderungen im Zusammenhang mit der Risikopunktzahl eines Testergebnisses anzeigen. Darüber hinaus werden die Arbeitsnotizen nur aktualisiert, wenn sich die Risikopunktzahl ändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Rechnerregeln

Standardmäßig wird ein **Standardrisikorechner** für das Basissystem bereitgestellt. Wenn Sie eine Risikoregel für diesen Rechner erstellen möchten, müssen Sie das Zielfeld des **Standardrisiko-Rechners** auf **Risikopunktzahl**festlegen. Wählen Sie die Schaltfläche **Neue Risikoregel**, um eine neue Risikoregel zu erstellen. Diese Aktion erstellt eine spezielle Regel für den Testergebnis-Rechner, die als **Risikoregel**bezeichnet wird und wiederum die **Risikopunktzahl** basierend auf mehreren Werten berechnet. Standardmäßig werden die folgenden Werte für die Berechnung der Risikopunktzahl berücksichtigt:

- Business-Relevanz
- Relevanz

Sie können die Werte anpassen, die in der **Standardrisikoregel** verwendet werden sollen, und festlegen, wie viel Gewichtung jeder dieser Werte erhalten soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der Basis-**Risikopunktzahl**zählt.

Ab Konfigurations-Compliance Version 13.0 können Sie die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Felder und Gewichtungen für die Risikoregel definieren.

Zuweisen eines Gewichtungsprozentsatzes

Sie können auch einen Gewichtungsprozentsatz (0–100) auf Feldwertebene zuweisen. Beispielsweise können Sie jeder Schweregradstufe (Keine bis Kritisch) einen Gewichtungsprozentsatz zuweisen. Wenn die Kritikalitätsgewichtung für die Risikoregel 50 beträgt und die folgenden Gewichtungswerte für die Relevanzstufe zugewiesen sind:

Gewichtungsprozentsatz zuweisen

Relevanz	Risikopunktzahl
Kritisch	100
Hoch	50
Mittel	20
Keine	0

Wenn die Kritikalität kritisch ist, beträgt die entsprechende Gewichtung 50. Wenn die Relevanz hoch ist, beträgt die Gewichtung 25, und wenn sie mittel ist, beträgt die Gewichtung 10. Wenn die Relevanz „none“ ist, ist die entsprechende Gewichtung 0. Weitere Informationen finden Sie im Beispiel zur Berechnung der Risikopunktzahl für Konfigurations-Compliance.

Jede Regel hat eine Einstellung **für die Reihenfolge**. Die erste Regel, die den Bedingungen entspricht, aktualisiert jedoch das Feld **„Risikopunktzahl“** im Testergebnis. Rechnerregeln ohne Skript haben in der Regel weniger Auswirkungen auf die Leistung als Rechnerregeln mit Skript.

Der Rechner des Basissystems Konfigurations-Compliance enthält Rechnerregeln, die jeder Relevanzstufe („Keine“ bis „Kritisch“) einen Wert (0–100) für **die Risikopunktzahl** basierend auf dem Schweregrad zuweisen. Dem Schweregrad „unbekannt“ wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können wie der Standardrisikorechner angepasst werden, es können neue Rechnerregeln oder neue Risikoregeln erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen wird basierend auf Faktoren wie Schweregrad, Kritikalität, Exploit-Informationen usw. eine Risikopunktzahl und Bewertung zugewiesen. Die Geschäftsregel *Update Risk Rating from Risk Score* in der Tabelle der angreifbaren Elemente ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert waren.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Ab Version 18.0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle als cc_risk_rating geliefert. Diese Typen werden als Teil der Geschäftsregel in jeder Tabelle übergeben, in der die Risikoeinstufung berechnet wird.
- Das Skript wird so geändert, dass Sie die Einträge in der Tabelle „Risikopunktzahlgewichtungen“ für die Berechnung der Risikoeinstufung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, müssen Sie die Bezeichnungen für die neue Risikoeinstufung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Risikopunktzahlgewichtungen“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn ein Configuration Item (CI) von ohne Internetzugriff in mit Internetzugriff geändert wird.
- Wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittparteieinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer Known Exploit Vulnerability (KEV) verknüpft sind.

Definieren Sie Felder und Gewichtungen für die Risikoregel

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, um Risikopunktzahlen zu generieren, die die Test- und Assetdaten verwenden, die für Ihre Organisation eindeutig sind. Durch Auswahl der Felder, die in der Risikoregel enthalten sind, können Sie ein effektives Framework für die Risikobewertung definieren.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**.
2. Klicken Sie auf **Standardrisiko-Rechner**.
3. Wählen Sie **Risikopunktzahl**als Zielfeld aus.
   In der Tabelle „Rechnerregel“ wird die Schaltfläche **Neue Risikoregel** angezeigt.
4. Klicken Sie auf die Schaltfläche **Neue Risikoregel,** um zum Formular **Konfigurations-Compliance-Risikoregel** zu navigieren.
5. Legen Sie im Abschnitt Kriterien des Risikorechners die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung für die Berechnung der Gesamtrisikopunktzahl fest.
6. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um die Regel zu deaktivieren.
7. Klicken Sie auf **Kriterien hinzufügen**, um den Risikorechnerkriterien Risikoregelfelder hinzuzufügen.
8. Füllen Sie die Felder des Formulars aus.

Formular „Risikoregelfeld“.

Feld	Beschreibung
Referenztabelle auswählen	Die Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Wählen Sie unter den folgenden Optionen aus: ○ Testergebnis: Fügen Sie Felder hinzu, zu denen Sie direkt über das Testergebnis (TV) per Dot-Walk navigieren können. ○ Testergebnis – Konfigurationselement: Fügen Sie punktweise durchlaufbare Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. der Hardwaretabelle. Diese Felder sind nicht Teil der Basistabelle „cmdb_ci“. ○ Testergebnis – Test: Fügen Sie Dot-Walking-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. „Drittpartei-Eintrag“. Diese Felder sind nicht Teil der Konfigurationstest-Basistabelle. ○ Referenztabelle für Testergebnisse: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) oder Tabellen sind, die eine Referenz zum Testergebnis enthalten. Diese Felder sind nicht direkt vom Testergebnis aus punktweise durchlaufbar. ○ Referenztabelle für Konfigurationselement: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die einen Verweis auf cmdb_ci enthalten. Diese Felder sind nicht direkt vom TR punktweise durchlaufbar. ○ Testreferenztabelle: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von „sn_vulc_test“ sind, oder Tabellen, die einen Verweis auf „sn_vulc_test“ enthalten. Diese Felder sind nicht direkt vom TR punktweise durchlaufbar. ○ Anwenderdefinierte Bedingungen: Verwenden Sie diese Option, um der Regel durch Auswertung der Bedingung Gewichtungen zuzuweisen. Beispielsweise bestimmt der Filter mit Internetverbindung, ob ein Configuration Item (CI) extern oder intern ist.
Feld	Das für die Berechnung der Risikopunktzahl für diese Regel verwendete Feld.
Gewichtung	Gewichtung dieses Feldes innerhalb der Risikoregel. Der Wert muss eine ganze Zahl von 0 bis 100 sein.
Tabelle	○ Testergebnis > Konfigurationselement ○ Testergebnis > Test ○ Test-Ergebnisreferenztabelle ○ Referenztabelle für Konfigurationselemente ○ Test-Referenztabelle Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen eine der aufgeführten Optionen ausgewählt ist.
Aggregation	Wählen Sie den Mindest- oder Höchstwert aus, der für Berechnungen berücksichtigt werden soll, wenn das Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird. Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen eine Referenztabelle ausgewählt wird.
Definieren Sie die Wertgewichtung	Komponente zum Zuweisen von Gewichtungen zu jedem Feldwert. Definieren Sie für numerische Felder Feldwerte als Bereich (z. B. 1–5). Der Wert muss eine Ganzzahl zwischen 0 und 100 sein. Dieses Feld wird nicht angezeigt, wenn im Feld Referenztabelle auswählen die Option Anwenderdefinierte Bedingungen ausgewählt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedingungstabelle	Wählen Sie eine Bedingung aus der Liste aus. Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen die Option Anwenderdefinierte Bedingungen ausgewählt ist.
Feldname	Geben Sie einen Namen für die Risikokriterien ein. Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen die Option Anwenderdefinierte Bedingungen ausgewählt ist.
Bedingung	Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen. Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen die Option Anwenderdefinierte Bedingungen ausgewählt ist.

9. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für das aktive Testergebnis neu zu bewerten.

Risiko-Rollup-Rechner für bearbeiten Konfigurations-Compliance

Bearbeiten Sie einen vorhandenen Risiko-Rollup-Rechner.

Vorbereitungen
Erforderliche Rolle: Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** und wählen Sie **Rollup-Rechner für Risikopunktzahlen**aus.
2. Klicken Sie bei angezeigter Liste der Rollup-Rechner für Risikopunktzahlen auf einen Rechner, um den Datensatz zu öffnen und das Formular zu bearbeiten.

Feld	Beschreibung
Name	Der Name des Rechners für das Rollup von Konfigurationstests oder Korrekturaufgaben.
Beschreibung	Eine Beschreibung für den Risiko-Rollup-Rechner.
Tabelle	Tabelle, auf die der Rollup-Rechner angewendet wird.
Zurückstellung einbeziehen	Schließt zurückgestellte Testergebnisse während des Rollups der Risikopunktzahl ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Definieren Sie die Gewichtungen auf eine der folgenden Arten:
   - Weisen Sie im Abschnitt „Rollup-Gewichtungen“ Gewichtungen für Folgendes zu:

Rollup-Gewichtungen

Feld	Beschreibung	Standardgewichtung
Maximale Risikopunktzahl	Maximale Risikopunktzahl der berücksichtigten Testergebnisse.	85
Durchschnittliche Risikopunktzahl	Aggregat der Risikopunktzahlen aller berücksichtigten Testergebnisse.	0
Anzahl der Testergebnisse	Anzahl der Testergebnisse.	15

   - Aktivieren Sie das Kontrollkästchen **Erweiterte Ansicht**, und bearbeiten Sie im Editor **für Skriptwerte** die Werte im Skript nach Bedarf.

Hinweis:
Das Bearbeiten von Skripten erfordert fortgeschrittene Kenntnisse der Anwendung Now Platform und Konfigurations-Compliance.

4. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.

Rollup-Rechner sind regelmäßige Aufgaben, die stündlich ausgeführt werden, um Änderungen zu übernehmen. Diese geplanten Aufgaben enthalten auch Gesamtrisikopunktzahlen für Konfigurationstests und Korrekturaufgaben. Die Rollup-Werte werden in den Feldern Risikopunktzahl angezeigt.

Ein Beispiel für die Bestimmung der Punktzahlen mit einem Risiko-Rollup-Rechner finden Sie unter Berechnungsbeispiel für Risiko-Rollup für Konfigurations-Compliance (vor v15.0).

Risikorechner für erstellen, bearbeiten und erneut anwenden Konfigurations-Compliance

Rechnerregeln können bei Bedarf auf alle betroffenen Testergebnisse und Sammlungen angewendet werden. Schwachstellenmanager können mit dieser Funktion die Konfiguration des Risikorechners anpassen und bei Bedarf Änderungen anwenden, um Ergebnisse zu importieren.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Führen Sie die folgenden Schritte aus, um einen neuen Risikorechner zu erstellen.

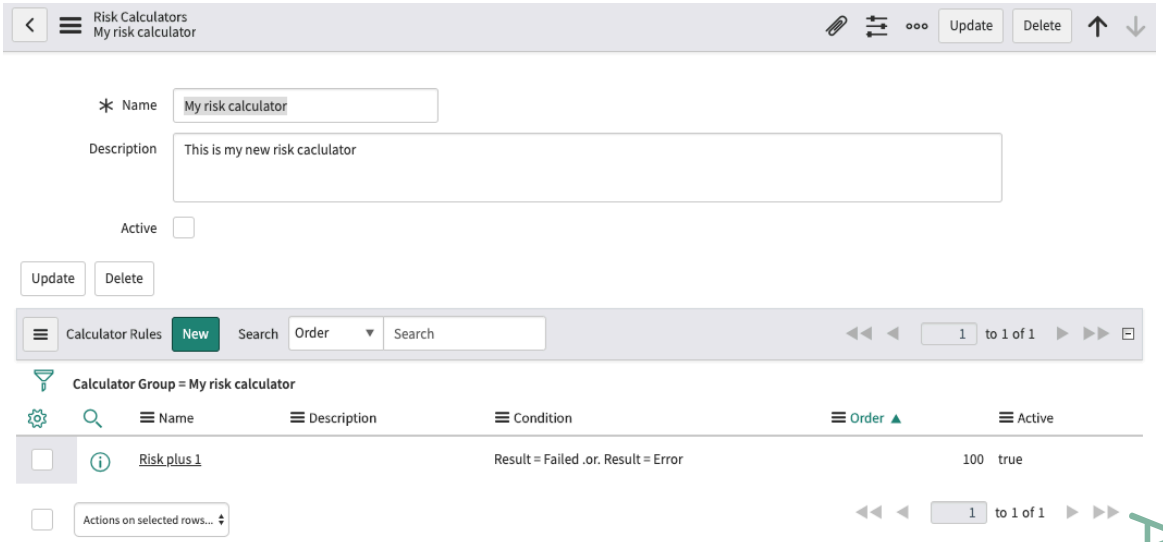
   a. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** und wählen Sie **Risikorechner**.

   b. Klicken Sie in der Liste Risikorechner auf **Neu**.

   c. Geben Sie einen Namen und eine Beschreibung für Ihren neuen Rechner ein, und klicken Sie auf **Absenden**.
   Der neue Rechner wird in der Liste Risikorechner angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Klicken Sie in der Liste auf den neuen Rechner, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt wird, und geben Sie die Felder und Werte an, die in den Testergebnisdatensätzen und Korrekturaufgaben angezeigt werden sollen.

e. Klicken Sie im angezeigten Datensatz auf **Neu**.

f. Füllen Sie die Felder auf den Registerkarten entsprechend aus.

Tab-Taste	Beschreibung
Wenn diese Bedingung erfüllt ist	Verwenden Sie den Bedingungsgenerator, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt wird. Beispiel: Ergebnis ist Fehlgeschlagen oder Ergebnis ist Fehler.
Diese Werte festlegen	Verwenden Sie die Vorlage, um die Felder und Werte auszuwählen, die angezeigt werden sollen.

g. Klicken Sie auf **Absenden**.
Der Datensatz wird mit den neuen Rechnerregeln und der Gruppe, zu der er gehört, angezeigt.

2. Führen Sie die folgenden Schritte aus, um einen vorhandenen Rechner erneut anzuwenden, um Ergebnisse zu testen oder die Regeln und angezeigten Werte für einen vorhandenen Risiko-Rechner zu bearbeiten.

a. Wählen Sie in den Listen Risiko-Rechner oder Risiko-Rollup-Rechner den Rechner aus, den Sie bearbeiten möchten.

b. Um einen Risikorechner aus dem Datensatz auf Ihre vorhandenen Testergebnisdaten erneut anzuwenden, klicken Sie auf **Rechner erneut anwenden**.
Alle Testergebnisse, die die Bedingungen des Rechners erfüllen, werden aktualisiert.

Hinweis:
Je nach Anzahl der Testergebnisse kann diese Aktualisierung einige Zeit dauern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Um die Bedingungen und Werte zu bearbeiten, klicken Sie unten links in der Spalte Name auf den Namen des Rechners.
Bei Risiko-Rechnern werden der Datensatz und die Registerkarten **Wenn diese Bedingung erfüllt ist** und **Diese Werte festlegen** angezeigt.

d. Füllen Sie das Formular entsprechend aus.

Tab-Taste	Feldbeschreibung
Wenn diese Bedingung erfüllt ist	Verwenden Sie den Generator für Filterbedingungen, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt werden soll.
Diese Werte festlegen	Wählen Sie eine, um fortzufahren. ▪ Werttyp: Vorlage. Wählen Sie Felder aus der Liste und die entsprechenden Werte aus. ▪ Skript: Geben Sie Ihre Änderungen mit dem Editor ein. **Hinweis:** Das Bearbeiten von Skripten erfordert fortgeschrittene Kenntnisse der Anwendung Now Platform und Konfigurations-Compliance.

3. **Wahlweise:** Führen Sie die folgenden Schritte aus, um die neuen Regeln bei Bedarf auf Ihre vorhandenen Testergebnisdaten anzuwenden.

a. Klicken Sie bei angezeigter Liste Risikorechner auf den Rechner, den Sie anwenden möchten.
Der Datensatz wird angezeigt.

b. Klicken Sie auf **Rechner erneut anwenden,** um Ihre Änderungen bei Bedarf zu testen und auf Ihre Importergebnisse anzuwenden.

4. Zeigen Sie Ihre Änderungen an Testergebnissen an, und bearbeiten Sie Ihre Rechner nach Bedarf weiter.

Beispiele für die Berechnung der Risikopunktzahl Konfigurations-Compliance .

Ab v13.0 von Konfigurations-Compliancekönnen Sie die Kriterien für die Standardrisikoregel anpassen. Verwenden Sie für die Berechnung der Risikopunktzahl Risikopunktzahlen von Drittanbietern wie Qualys und Tenable.

Drittanbieter wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden im Feld „Relevanz“ in der Tabelle „sn_vulc_test“ eingetragen. Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl. Um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

Fügen Sie die Quellenkritikalität als Kriterium für eine Risikoregel hinzu

Verwenden Sie von Drittanbietern bereitgestellte Punktzahlen basierend auf der Kritikalität, um Risikopunktzahlen zu berechnen.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

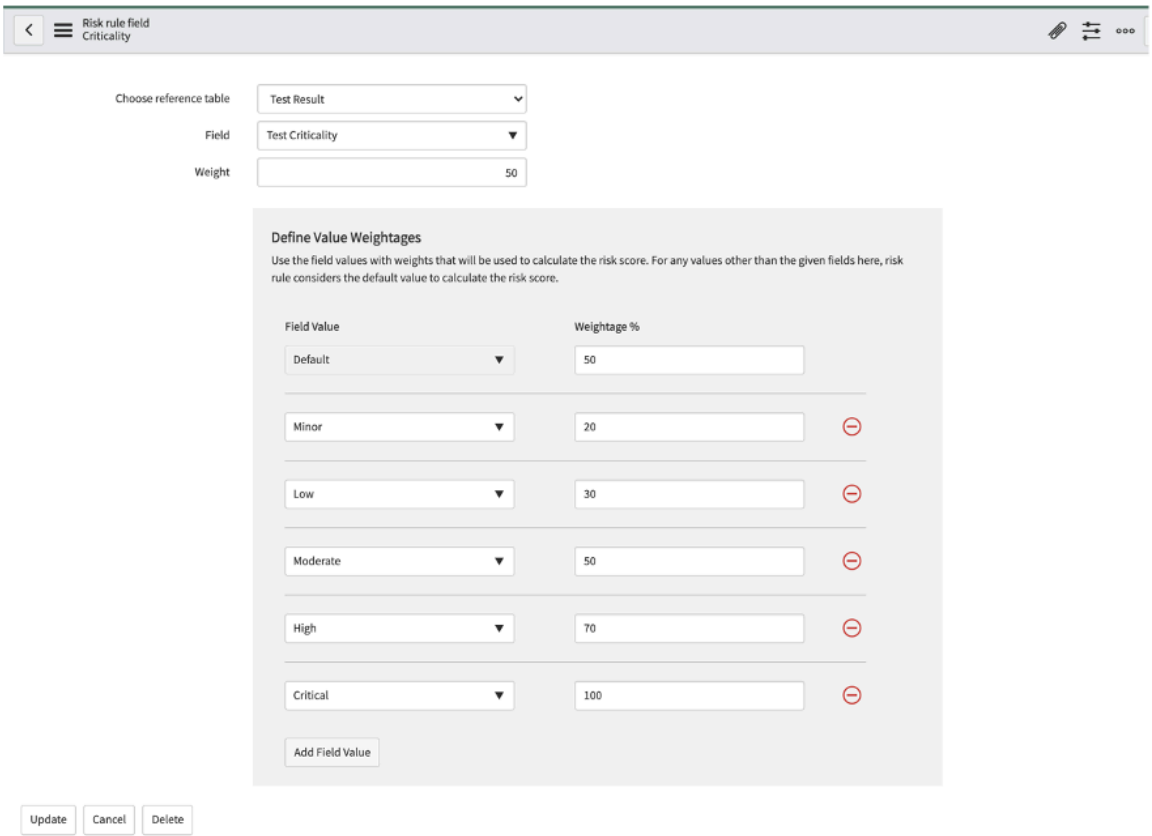
Warum und wann dieser Vorgang ausgeführt wird
Drittanbieter wie Qualys und Tenable geben ihre eigenen Risikopunktzahlen an. Diese Punktzahlen werden im Feld „Relevanz“ in der Tabelle „sn_vulc_test“ eingetragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl und Berechnung der Risikopunktzahl.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**.
2. Navigieren Sie zum Formular Risikoregel.
3. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um die Regel zu deaktivieren.
4. Klicken Sie auf **Kriterien hinzufügen**.
5. Wählen Sie in der Liste **Referenztabelle auswählendie Option Testergebnis**aus.
6. Wählen Sie in der Liste **Felddie Option Test.Relevanz**aus.
7. Geben Sie im Feld **Gewicht** die relative Bedeutung dieses Felds an.
   Der Wert muss eine ganze Zahl von 0 bis 100 sein.
8. Fügen Sie im Abschnitt **„Wertgewichtungen definieren“** Feldwerte hinzu, und weisen Sie den Feldern einen Gewichtungsprozentsatz zu.



9. Klicken Sie auf **Absenden**.

Fügen Sie die Geschäftsrelevanz als Kriterium für eine Risikoregel hinzu

Geben Sie einen Kritikalitätswert für Geschäftsservices an, und verwenden Sie die Geschäftsrelevanz, um die Risikopunktzahlen zu berechnen.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Angenommen, Ihre Organisation verfügt über viele Business-Services, und ein Configuration Item (CI) wird von den folgenden Services verwendet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Relevanz der Business-Services

Business-Service	Relevanz
Cloud-Management	1 – Sehr kritisch
E-Commerce	2 – Kritisch
Client-Services	3 – Weniger kritisch
Reisekosten und Spesen	4 – Nicht kritisch

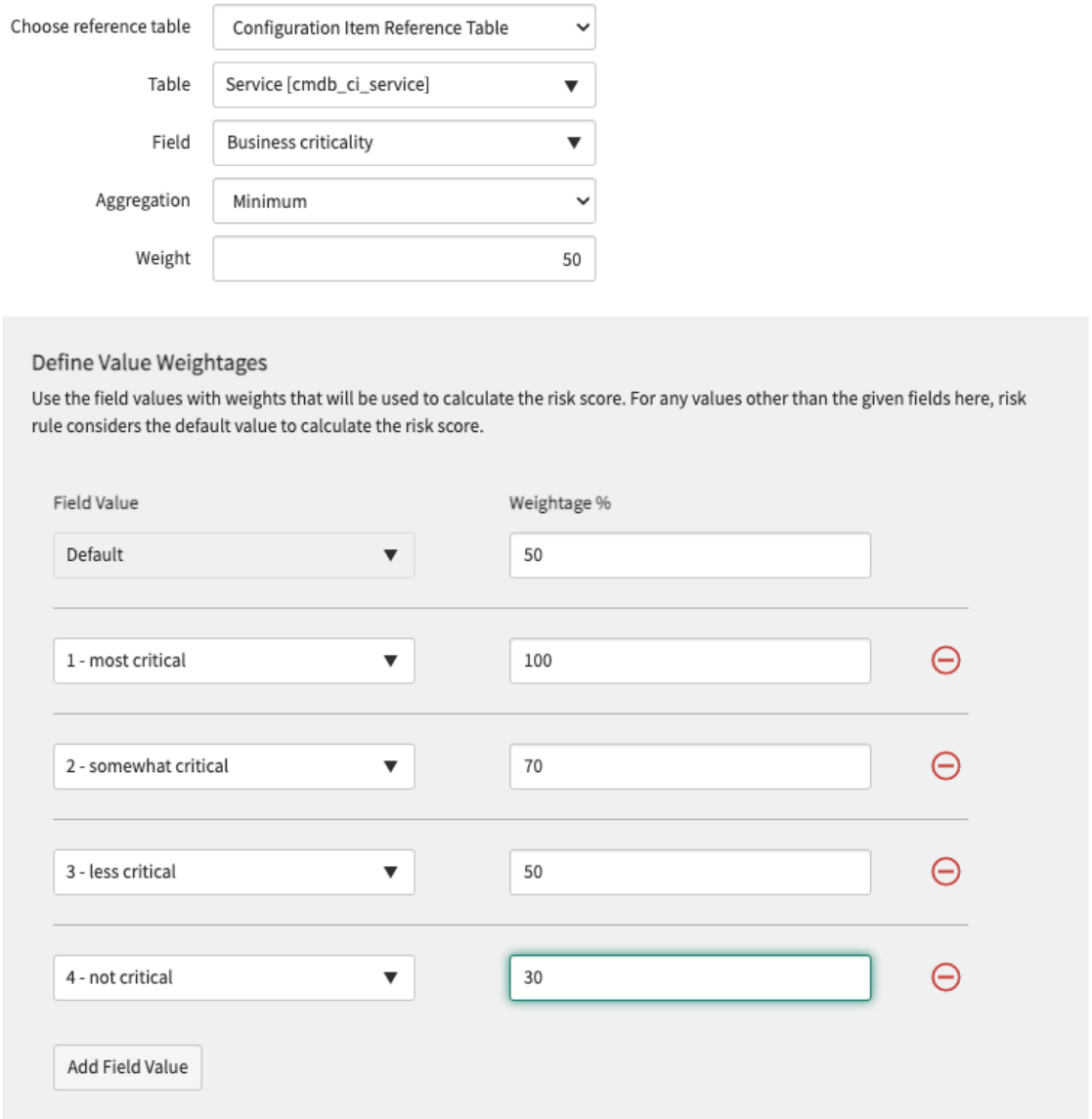
Die Zuordnung zwischen CI und Services wird in der Tabelle „Services“ [cmdb_ci_services] gespeichert. Wenn ein CI einen Konfigurationstest nicht besteht, wird ein Testergebnis (Test Result, TR) erstellt. Sie können den Wert der Geschäftskritikalität aus den betroffenen Services verwenden, um die Risikopunktzahl für dieses TR zu berechnen. Befolgen Sie das Verfahren, um den Kritikalitätswert dieser Services für die Berechnung der Risikopunktzahl zu verwenden.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**.
2. Navigieren Sie vom Abschnitt **Rechnerregeln** zum Formular Risikoregel.
3. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um die Regel zu deaktivieren.
4. Klicken Sie auf **Kriterien hinzufügen**.
5. **Wählen Sie in der Liste Referenztabelle auswählendie Option Konfigurationselement-Referenztabelle**aus.
6. Wählen Sie in der Liste **Tabelledie Option Service [cmdb_ci_service]**aus.
7. Wählen Sie in der Liste **Felddie Option Business-Relevanz**aus.
8. Wählen Sie im Feld **Zusammenfassungdie Option Minimum** aus, um den kritischsten Service für diesen Anwendungsfall abzurufen (1 – Kritischster Wert) oder **Maximum**, um den am wenigsten kritischen Service für diesen Anwendungsfall abzurufen (4 – Nicht kritischer Wert).
9. Geben Sie im Feld **Gewicht** die relative Bedeutung dieses Felds an.
   Der Wert muss eine ganze Zahl von 0 bis 100 sein.
10. Fügen Sie im Abschnitt **„Wertgewichtungen definieren“** Feldwerte hinzu, und weisen Sie Gewichtungen zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderdefinierte Gewichtung der Business-Relevanzrisikoregel



Automatische Übersetzung

11. Klicken Sie auf **Absenden**.

Fügen Sie dem Risikorechner ein bedingtes Kriterium hinzu

Verwenden Sie anwenderdefinierte Bedingungen für die Risikoregel zur Berechnung der Risikopunktzahl.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Angenommen, Ihre Organisation verfügt über mehrere Configuration Items (CIs), von denen ein externer Benutzer nur auf wenige zugreifen kann. Benutzer können Gewichtungen der Risikopunktzahl für diese nach außen gerichteten CIs hinzufügen.

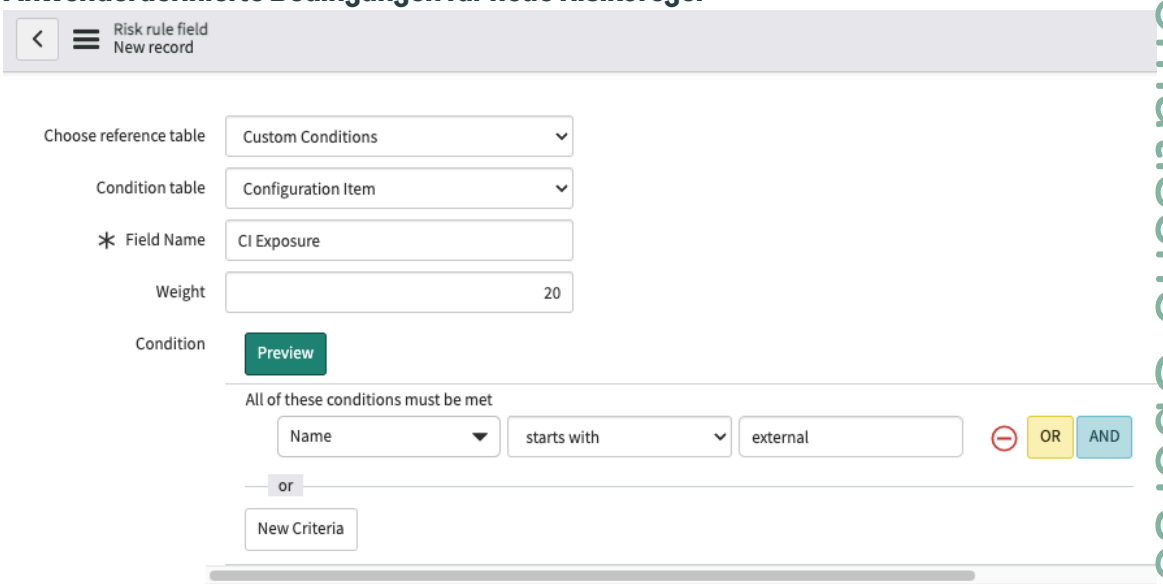
Hinweis:
Sie können diese CIs anhand ihres Namens identifizieren. Die Namen beginnen mit „external“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**.
2. Navigieren Sie zum Formular Risikoregel.
3. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um die Regel zu deaktivieren.
4. Klicken Sie auf **Kriterien hinzufügen**.
5. Wählen Sie in der Liste **Referenztabelle auswählendie Option Anwenderdefinierte Bedingungen**aus.
6. Wählen Sie in der Liste **BedingungstabelleKonfigurationselement**aus.
7. Geben Sie im **Feld** Feldname `CI Risiko`ein.
8. Geben Sie im Feld **Gewicht** die relative Bedeutung dieses Felds an.
   Der Wert muss eine ganze Zahl von 0 bis 100 sein.
9. Wählen Sie im Feld **BedingungName > beginnt mit**und geben Sie `external`als Wert an.

Anwenderdefinierte Bedingungen für neue Risikoregel



10. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Rechnergruppen für Konfigurations-Compliance

Beispiel für die Berechnung der Risikopunktzahl für Konfigurations-Compliance

Bestimmen Sie die Risikopunktzahl-Rechner, um Risikopunktzahlen zu generieren, die die für Ihre Organisation spezifischen Test- und Asset-Daten verwenden.

Beispiel für die Bestimmung der Punktzahlen von Risikoregelrechnern

Das folgende Beispiel zeigt, wie Punktzahlen für Risikoregel-Rechner ermittelt werden. Angenommen, ein Risikoregel-Rechner ist mit den Feldern in dieser Tabelle konfiguriert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestimmen Sie die Punktzahlen des Risikoregel-Rechners

Feld	Gewichtung	Gewichtungsaufgliederung
Kontrolle.Relevanz	50	Standard: 0 Kleiner: 20 Niedrig: 30 Mittel: 50 Hoch: 70 Kritisch: 100
Business_Relevanz	50	Standard: 0 Kleiner: 20 Niedrig: 30 Mittel: 50 Höhe: 70 Kritisch: 100

Angenommen, die in dieser Tabelle angezeigten Testergebnisse sind im System vorhanden.

Zuordnung von Testergebnissen

ID	Business-Relevanz	Relevanz der Steuerung
CTR0000001	1: Sehr kritisch	Geringer
CTR0000002	1: Sehr kritisch	Niedrig
CTR0000003	2: Kritisch	Geringer
CTR0000004	2: Kritisch	Mittel
CTR0000005	3: Weniger relevant	Niedrig

Die Berechnung der Risikopunktzahl für das Testergebnis basiert auf der folgenden Formel:

Risikopunktzahl = (W(control.criticality) * FV (control.criticality). + W(business_criticality) * FV(business_criticality)) / 100, wobei W für die Gewichtung und FV für den Gewichtungsprozentsatz des Feldwerts steht.

Die resultierende Risikopunktzahl für diese Testergebnisse ist wie in der folgenden Tabelle beschrieben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikopunktzahl basierend auf Testergebnissen

ID	Business-Relevanz (50 %)	Kritikalität der Steuerung (50 %)	Resultierende Risikopunktzahl
CTR0000001	1 – Am kritischsten (50 % x 100)	Gering (50 % x 20)	60
CTR0000002	1 – Am kritischsten (50 % x 100)	Niedrig (50 % x 30)	65
CTR0000003	2 – Kritisch (50 % x 70)	Gering (50 % x 30)	45
CTR0000004	2 – Kritisch (50 % x 70)	Mittel (50 % x 50)	60
CTR0000005	3 – Weniger kritisch (50 % x 50)	Niedrig (50 % x 30)	40

Wenn der Gewichtungsprozentsatz für einen der Feldwerte geändert wird, finden Sie die Ergebnisse in dieser Tabelle:

Ergebnisse für geänderten Gewichtungsprozentsatz

Feld	Gewichtung	Gewichtungsaufgliederung
Kontrolle.Relevanz	50	Standard: 0 Kleiner: 20 Niedrig: 30 Mittel: 60 Höhe: 70 Kritisch: 100
Business_Relevanz	50	Standard: 50 1 – Am kritischsten: 100 2 – Kritisch: 70 3 – Weniger relevant: 20 4 – Nicht kritisch: 30

Die Risikopunktzahl für die Testergebnisse nach dem erneuten Anwenden des Rechners wird in der folgenden Tabelle angezeigt:

Risikopunktzahl für TR beim erneuten Anwenden des Rechners

ID	Business-Relevanz (50 %)	Kritikalität der Steuerung (50 %)	Resultierende Risikopunktzahl
CTR0000001	1 – Am kritischsten (50 % x 100)	Gering (50 % x 20)	60

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikopunktzahl für TR beim erneuten Anwenden des Rechners (Fortsetzung)

ID	Business-Relevanz (50 %)	Kritikalität der Steuerung (50 %)	Resultierende Risikopunktzahl
CTR0000002	1 – Am kritischsten (50 % x 100)	Niedrig (50 % x 30)	65
CTR0000003	2 – Kritisch (50 % x 70)	Gering (50 % x 30)	45
CTR0000004	2 – Kritisch (50 % x 70)	Mittel (50 % x 60) * Überarbeiteter Wert	65 * Überarbeiteter Wert
CTR0000005	3 – Weniger kritisch (50 % x 20) * Überarbeiteter Wert	Niedrig (50 % x 30)	25 * Überarbeiteter Wert

Berechnungsbeispiel für Risiko-Rollup für Konfigurations-Compliance (vor v15.0)

Das folgende Beispiel zeigt, wie die Punktzahlen für Risiko-Rollup-Rechner ermittelt werden.

Für den folgenden Rechner für Korrekturaufgaben-Rollup lautet die Formel zur Berechnung der Risikopunktzahl für Korrekturaufgaben:

(Maximale Risikopunktzahl/100) * 85 + (Faktor * 15).

Der Faktor in der vorherigen Gleichung wird durch die Anzahl der Testergebnisse bestimmt (siehe folgende Tabelle).

Anzahl Testergebnisse	Faktor
<10	0,2
10-99	0,4
100–1000	0,6
1001-9999	0,8
>10.000	1

Für die folgende Korrekturaufgabe, TRG0003066, mit drei Testergebnissen Risikopunktzahlen, beträgt die maximale Punktzahl 90.

Nummer	Risikopunktzahl	Nachbesserungsaul	Ergebnis	Status
CTR000123	90.0	TRG0003066	Fehlgeschlagen	Öffnen
CTR000124	70	TRG0003066	Fehlgeschlagen	Öffnen
CTR000125	40	TRG0003066	Fehlgeschlagen	Öffnen

Für die Korrekturaufgabe TRG0003066:

Die Risikopunktzahl ist 79, (90/100) * 85 + 0,2 * 15 = Math.Floor (76,5 +3) =79.

Die historische Risikopunktzahl ist null, da die Korrekturaufgabe noch „Offen“ ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Datenerfassung lauten die Testergebnisse „Bestanden“, und die Korrekturaufgabe geht in den Status „Geschlossen“ über, wie in der folgenden Tabelle gezeigt.

Nummer	Risikopunktzahl (vor v15.0)	Nachbesserungsaul	Ergebnis	Status
CTR000123	0	TRG0003066	Bestanden	Abgeschlossen
CTR000124	0	TRG0003066	Bestanden	Abgeschlossen
CTR000125	0	TRG0003066	Bestanden	Abgeschlossen

In der folgenden Tabelle wird der Verlauf der Testergebnisse angezeigt.

Nummer	Risikopunktzahl	Neuestes Ergebnis	Ergebnis
CTRH000111	90.0	CTR000123	Fehlgeschlagen
CTRH000112	70	CTR000124	Fehlgeschlagen
CTRH000113	40	CTR000125	Fehlgeschlagen

Die Risikopunktzahl ist 0, da in der Korrekturaufgabe keine aktiven Testergebnisse vorhanden sind.

Für die Korrekturaufgabe TRG0003066:

Die historische Risikopunktzahl ist 79: (90/100) * 85 + 0,2 * 15 = Math.Floor (76,5 +3) =79.

Berechnungsbeispiel für Risiko-Rollup für Konfigurations-Compliance (v15.0 und höher)

Das folgende Beispiel zeigt, wie die Punktzahlen für Risiko-Rollup-Rechner ermittelt werden.

Für den folgenden Rechner für Korrekturaufgaben-Rollup lautet die Formel zur Berechnung der Risikopunktzahl für Korrekturaufgaben:

(Maximale Risikopunktzahl* 80/100) + (Durchschnittliche Risikopunktzahl* 5/100) + (Faktor * 15)

Die Gewichtungen lauten wie folgt:

- Maximale Risikopunktzahl: 80
- Durchschnittliche Risikopunktzahl: 5
- Faktor: 15

Die Standardgewichtung der durchschnittlichen Risikopunktzahl ist 0. Weitere Informationen zum Festlegen der Gewichtungen finden Sie unter Risiko-Rollup-Rechner für bearbeiten Konfigurations-Compliance.

Der Faktor in der vorherigen Gleichung wird durch die Anzahl der Testergebnisse bestimmt (siehe folgende Tabelle).

Anzahl Testergebnisse	Faktor
<10	0,2
10-99	0,4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl Testergebnisse	Faktor
100–1000	0,6
1001-9999	0,8
>10.000	1

Für die folgende Korrekturaufgabe, TRG0003066, mit drei Testergebnissen Risikopunktzahlen, beträgt die maximale Risikopunktzahl 90, und die durchschnittliche Risikopunktzahl beträgt 66,67.

Nummer	Risikopunktzahl	Nachbesserungsaul	Ergebnis	Status
CTR000123	90.0	TRG0003066	Fehlgeschlagen	Öffnen
CTR000124	70	TRG0003066	Fehlgeschlagen	Öffnen
CTR000125	40	TRG0003066	Fehlgeschlagen	Öffnen

Für die Korrekturaufgabe TRG0003066:

Die Risikopunktzahl ist 81, (90* 80/100) + (66,67* 5/100) + (0,2 * 15) = Math.level (78,3 +3) = 81.

Die historische Risikopunktzahl ist null, da die Korrekturaufgabe noch „Offen“ ist.

Nach der Datenerfassung lauten die Testergebnisse „Bestanden“, und die Korrekturaufgabe geht in den Status „Geschlossen“ über, wie in der folgenden Tabelle gezeigt. Ab v15.0 von Konfigurations-Compliancewird die Risikopunktzahl eines bestandenen Testergebnisses ausgefüllt, um das geminderte Risiko zu bestimmen.

Nummer	Risikopunktzahl	Nachbesserungsaul	Ergebnis	Status
CTR000123	90.0	TRG0003066	Bestanden	Abgeschlossen
CTR000124	70	TRG0003066	Bestanden	Abgeschlossen
CTR000125	40	TRG0003066	Bestanden	Abgeschlossen

In der folgenden Tabelle wird der Verlauf der Testergebnisse angezeigt.

Nummer	Risikopunktzahl	Neuestes Ergebnis	Ergebnis
CTRH000111	90.0	CTR000123	Fehlgeschlagen
CTRH000112	70	CTR000124	Fehlgeschlagen
CTRH000113	40	CTR000125	Fehlgeschlagen

Die Risikopunktzahl der Korrekturaufgabe ist null, da in der Korrekturaufgabe keine aktiven Testergebnisse vorhanden sind.

Für die Korrekturaufgabe TRG0003066:

Die historische Risikopunktzahl ist 81: (90* 80/100) + (66,67* 5/100) + (0,2 * 15) = Math.level (78,3 +3) = 81.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen oder bearbeiten Sie Konfigurations-Compliance Regeln für Korrekturaufgaben

Sie können Regeln erstellen, um Testergebnisse basierend auf Filterbedingungen automatisch zu gruppieren. Diese Regeln gruppieren Testergebnisse automatisch, während sie importiert werden. Verwenden Sie den Filter, um die von dieser Regel gruppierten Testergebnisse einzuschränken, z. B. um alle Testergebnisse mit Exploits auszuwählen.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Im Lieferumfang des Basissystems ist eine Regel für Korrekturaufgaben enthalten: **Zuweisungsgruppe, Test**, die Testergebnisse nach Zuweisungsgruppe (vorab ausgefüllt aus **Zuweisungsregeln**) und dem Feld **Test** gruppiert. Diese Regel kann mithilfe von Filterbedingungen und Gruppenschlüsseln geändert werden. Gruppenschlüssel sind Spalten in der Testergebnistabelle. Wählen Sie bis zu sechs Schlüssel aus, um anzugeben, welche Werte zum Gruppieren der Testergebnisse verwendet werden sollen.

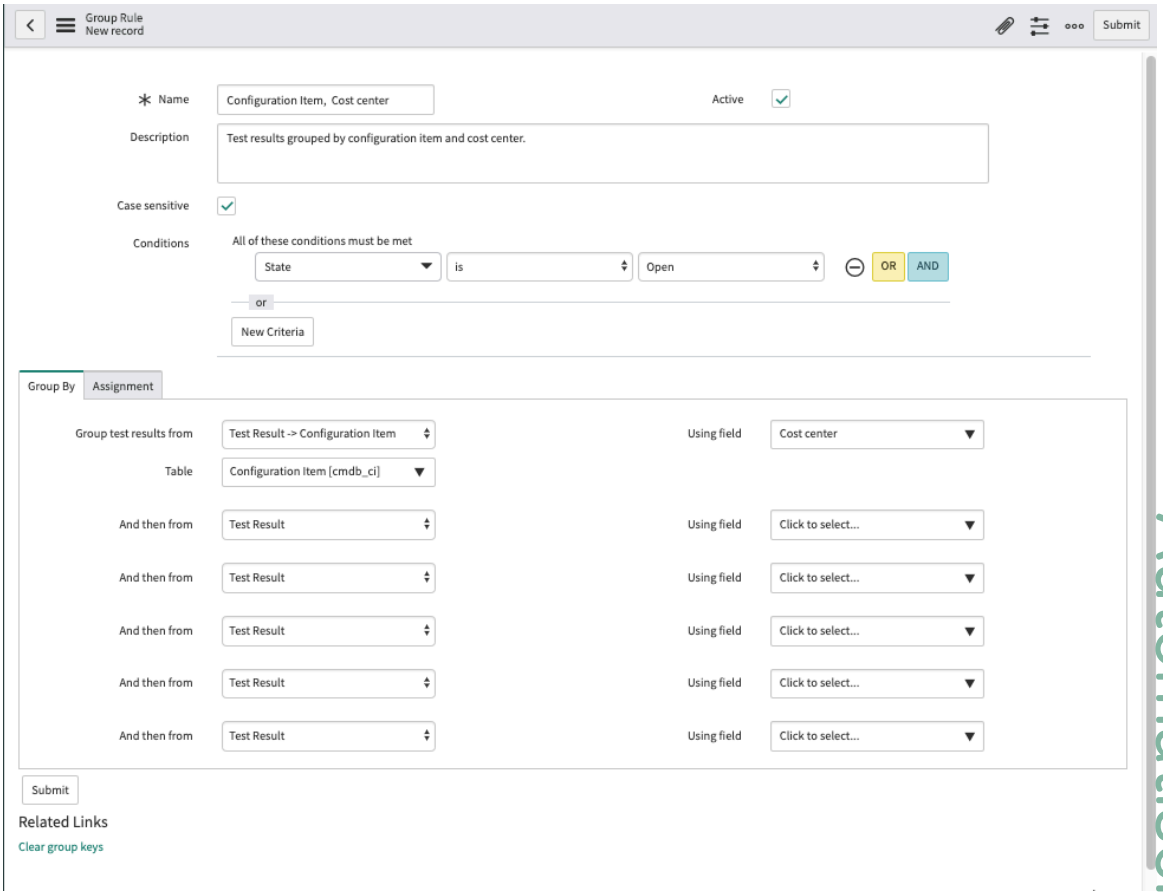
Ab Version 14.7 von Konfigurations-Complianceist die **Zuweisungsgruppe, Regel für Korrekturaufgaben testen** für Neuimplementierungen deaktiviert.

Hinweis:
Neue oder aktualisierte Regeln werden beim nächsten Import automatisch oder manuell über die Schaltfläche **Erneut** anwenden im Formular „Regel für Korrekturaufgaben“ ausgewertet.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Regeln für Korrekturaufgaben**.
2. Öffnen Sie die **Zuweisungsgruppe, Testregel**, oder klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

Konfigurations-Compliance Regel für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Regel für Korrekturaufgaben.
Aktiv	Gibt an, ob die Regel für Korrekturaufgaben aktiv ist.
Beschreibung	Textbeschreibung dieser Regel für Korrekturaufgaben.
Groß-/ Kleinschreibung beachten	Bestimmt, ob beim Regelabgleich Groß-/Kleinschreibung berücksichtigt wird oder nicht. **Hinweis:** Beim Standardwert wird zwischen Groß- und Kleinschreibung unterschieden.
Bedingungen	Bedingungen, die erfüllt werden müssen. Standardmäßig (Kontrollkästchen **„Groß-/Kleinschreibung beachten** “ ist deaktiviert) berücksichtigt der Suchtext, den Sie im Bedingungsgenerator für Korrekturaufgaben-Regeldatensätze und -formulare eingeben, Groß-/Kleinschreibung. Sie können Suchen unter Berücksichtigung von Groß-/Kleinschreibung in Gruppendatensätzen und Formularen aktivieren.
Gruppieren nach	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Testergebnisse gruppieren von	Automatisieren Sie die Erstellung von Gruppen basierend auf dieser Regel. Wählen Sie eine der verfügbaren Optionen aus. ○ Testergebnis | Feld wird verwendet ○ Testergebnis->Konfigurationselement | Tabelle | Feld wird verwendet Wenn ein erweitertes **Tabellenfeld** ausgewählt ist, werden Testergebnisse, die nicht die entsprechende erweiterte Tabelle verwenden, in einer separaten Korrekturaufgabe gruppiert.
Zuweisung	
Weisen Sie Testergebnisgruppen nach zu	Automatisieren Sie die Zuweisung von Gruppen, die auf Grundlage dieser Regel erstellt werden. Wählen Sie eine der verfügbaren Optionen aus. ○ Gruppen-Key Wenn diese Option ausgewählt ist, wird das Feld Schlüsselwert angezeigt. Verfügbare Felder werden in einem Dropdown-Menü aufgelistet. ○ Anwendergruppe Wenn diese Option ausgewählt ist, wird das Feld Anwendergruppensuche angezeigt.

4. Klicken Sie auf **Absenden**.

Hinweis:
Mit dem zugehörigen Link „Gruppierung nach Schlüssel löschen“ werden die Gruppenschlüssel aus der Registerkarte „Gruppieren nach“ im Formular entfernt.

Geben Sie die Dauer einer Ausnahme an, die für eine Korrekturaufgabe angefordert wird

Verwenden Sie die Systemeigenschaften, um die Dauer zu begrenzen, für die eine Ausnahme für eine Korrekturaufgabe angefordert wird. Die Korrektur der Korrekturaufgabe wird für den angegebenen Zeitraum zurückgestellt.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Mit der Eigenschaft `sn_vulc.exception_max_request_days` wird die maximale Anzahl von Tagen angegeben, für die eine Ausnahme für eine Korrekturaufgabe angefordert werden kann. Der Standardwert beträgt 365 Tage.

Hinweis:
Mit der Eigenschaft `sn_vulc.exception_approval_required` können Sie den Ausnahmegenehmigungs-Workflow für die Korrekturaufgabe deaktivieren, wenn er nicht erforderlich ist. Standardmäßig ist diese Eigenschaft aktiviert, und ihr Wert ist `wahr`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie auf der Seite „Systemeigenschaften“ nach sn_vulc.exception_max_request_days.
3. Klicken Sie auf den Eigenschaftsnamen, um den Datensatz „Systemeigenschaft“ zu öffnen.
4. Um diesen Datensatz bearbeiten zu können, muss Konfigurations-Compliance als aktuelle Anwendung ausgewählt sein.
5. Geben Sie einen positiven **Wert** ein, und klicken Sie auf **Aktualisieren**.
   Der Datensatz wird aktualisiert und gespeichert.

Konfigurieren Sie die Ausnahmeverwaltung für Konfigurations-Compliance

Beschränken Sie die Dauer einer angeforderten Ausnahme, und fügen Sie der Ausnahme mithilfe des Moduls Konfigurations-Complianceeinen Fragebogen hinzu . Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Vulnerability Response angefordert. Sie können auch mit der -Integration GRC: Richtlinien- und Compliance-Management eine Ausnahme anfordern.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Richtlinien- und Compliance-Management installiert ist, GRC: Richtlinien- und Compliance-Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder die falsch positive Anforderung ausgelöst hat. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für das Anfordern der Ausnahme zu verstehen.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular „Ausnahmeverwaltungskonfiguration“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option in der Liste Ausnahmen verwalten mit auswählen.
   - Vulnerability Response

     Hinweis:
     Ab Vulnerability Response22.0 können Sie auch für die Option Vulnerability Response einen Fragebogen für falsch positive Anforderungen einrichten.

   - GRC: Richtlinien- und Compliance-Management

     Hinweis:
     Sie müssen das Plugin GRC aktivieren, um mit GRC: Richtlinien- und Compliance-Management eine Ausnahme anzufordern.

Hinweis:
Das Ändern der Konfiguration hat keine Auswirkungen auf die vorhandenen Daten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder im Formular aus.

Einstellungen für das CC-Formular „Ausnahmeverwaltung“.

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens zum Anfordern einer Ausnahme. Der Ausnahmefragebogen wird standardmäßig angezeigt.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung.
Fragebogen, um falsch positive Meldung zu markieren	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens als Falsch positiv markieren. Der Fragebogen für eine falsch positive Anforderung wird standardmäßig angezeigt.

4. Wählen Sie **Speichern**.

Fügen Sie einen Ausnahmegenehmiger für hinzu Konfigurations-Compliance

Fügen Sie den Genehmigergruppen Anwender hinzu, damit Sie eine Ausnahme für eine Korrekturaufgabe in Konfigurations-Complianceanfordern können.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Eine Ausnahmeanforderung für eine Korrekturaufgabe wird mit dem standardmäßigen zweistufigen Genehmigungsworkflow genehmigt. Das Hinzufügen von Anwendern zur Gruppe der ersten Ebene ist obligatorisch. Wenn auf der zweiten Ebene keine Benutzer vorhanden sind, wird die Anforderung nach der Genehmigung auf der ersten Ebene automatisch genehmigt.

Hinweis:
Wenn es keinen Genehmiger der ersten Ebene gibt, kann keine Ausnahme angefordert werden.

Hinweis:
Bis Konfigurations-Compliance v13.0 kann keine Ausnahme angefordert werden, wenn es keinen Genehmiger der ersten Ebene gibt. Wenn Sie jedoch die CC-Anwendung ab Konfigurations-Compliance v13.0 zum ersten Mal bereitstellen, wird der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie den Flow Designer aktualisieren. In beiden Fällen können Sie ihn nicht zurück in den Workflow ändern.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Anwender und Gruppen** > **Gruppen**.
2. Suchen Sie in der Spalte Name nach **Ausnahme**, und klicken Sie auf **Ausnahmegenehmiger - Ebene 1 CC**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab Konfigurations-Compliance v14.7.5 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahmeanforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie `sn_vulc.exception_approver_L1_CC` oder `sn_vulc.exception_approver_L2_CC`, um den Eigenschaftswert zu ändern.

3. Navigieren Sie im Formular Gruppenausnahmegenehmiger – Ebene 1 CC zu **Gruppenmitglieder** > **Neu** (oder **Bearbeiten**).
4. Füllen Sie die Felder des Formulars aus.

Anwenderformular

Feld	Beschreibung
Anwender-ID	Eindeutiger Bezeichner für den Benutzer
Vorname	Vorname des Anwenders.
Nachname	Nachname des Anwenders.
Titel	Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus.
Abteilung	Abteilung des Anwenders.
Passwort	Dem Anwender zugewiesenes Passwort. Dieses Passwort kann dauerhaft oder vorübergehend sein.
Passwort muss zurückgesetzt werden	Option, mit der der Anwender das Passwort zurücksetzen kann, um die Sicherheit zu gewährleisten.
Gesperrt	Option, den Anwender für die Instanz zu sperren und alle aktiven Sitzungen des Anwenders zu beenden. Das System verhindert, dass Benutzer mit der Rolle admin sich selbst sperren.
Aktiv	Option zum Aktivieren dieses Anwenders. Nur Sie können inaktive Anwender in den folgenden Bereichen sehen: ○ Listen von Benutzern ○ Auswahlliste für Referenzfelder (Lupensymbol) ○ AutoVervollständigen Sie die Liste, die angezeigt wird, wenn Sie etwas in ein Referenzfeld eingeben
Nur Webservice-Zugang	Option, um diesen Anwender als nicht interaktiven Anwender festzulegen.
Interner Integrationsanwender	Option, um diesen Anwender als internen Integrationsanwender festzulegen.
E-Mail	E-Mail-Adresse des Anwenders.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sprache	Bevorzugte Sprache des Anwenders.
Kalenderintegration	Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook.
Zeitzone	Zeitzone für den Standort dieses Anwenders.
Datumsformat	Bevorzugtes Format des Anwenders für Datumsangaben.
Telefon (geschäftlich)	Geschäftstelefon des Benutzers.
Mobiltelefon	Mobiltelefon des Benutzers.
Foto	Foto, das Sie hochladen können, indem Sie auf **„Zum Hinzufügen klicken…" klicken**.

5. Klicken Sie auf **Absenden**.
6. **Wahlweise:** Wiederholen Sie die Schritte 1–5, um einen Ausnahmegenehmiger – Ebene 2 CC zu erstellen.

Hinweis:
Wählen Sie beim Erstellen eines Genehmigers der zweiten Ebene **Ausnahmegenehmiger – Ebene 2 CC**aus

7. **Wahlweise:** Wenn Sie **Bearbeiten**auswählen, verschieben Sie Benutzer aus der **Sammlung** in den Bereich **Gruppenmitglieder,** und klicken Sie auf **Speichern**.
Der Genehmiger muss zu navigieren **Alle** > **Konfigurations-Compliance** > **Meine Genehmigungen** und Anforderungen genehmigen.

Erstellen Sie eine Konfigurations-Compliance -Relevanzzuordnung

Die KritikalitätszuordnungKonfigurations-Compliance bietet eine Transformationszuordnung für Kritikalitätsfelder von Drittanbieterquellen für erkennbare Felder im Schweregrad Konfigurations-Compliance.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Prozedur
1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Relevanz-Zuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldzuordnung

Feld	Beschreibung
Quelle	Der Name der Quelle für die Kritikalitätszuordnung.
Quellwert	Der Kritikalitätswert der Quelle.
Zielwert	Der Zielwert. Auswahlmöglichkeiten: **Kritisch** Das mit der Kontrolle verbundene Konfigurationsproblem verursacht eine Unterbrechung bei mindestens einem geschäftskritischen CI.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hoch Das mit der Kontrolle verbundene Konfigurationsproblem stellt eine Bedrohung dar, verursacht jedoch kein Herunterfahren kritischer Netzwerkressourcen. **Mittel** Das mit der Steuerung verbundene Konfigurationsproblem stellt ein Risiko dar, stellt jedoch keine unmittelbare Bedrohung dar. **Niedrig** Das mit der Steuerung verbundene Konfigurationsproblem stellt eine Bedrohung auf niedriger Ebene dar und kann anstelle von CIs ignoriert werden, die einem höheren Risiko ausgesetzt sind. **Geringer** Das mit der Steuerung verbundene Konfigurationsproblem stellt ein geringes Risiko dar und kann bei Bedarf ignoriert werden.

4. Klicken Sie auf **Absenden**.

Erstellen Sie E-Mail-Benachrichtigungen

Schwachstellenadministratoren können die Benachrichtigung bearbeiten oder neue hinzufügen und angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können E-Mail-Vorlagen für verschiedene Arten von E-Mail-Benachrichtigungen erstellen. Weitere Informationen zum Erstellen von E-Mail-Vorlagen finden Sie unter Definieren Sie Vulnerability Response E-Mail-Vorlagen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**.
2. Wählen Sie den Benachrichtigungsdatensatz des Korrekturziels oder **Neu**aus.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie **Benachrichtigungsvorschau** aus, um die Nachricht anzuzeigen.

Ergebnisse
Ab v14.11 von Konfigurations-Compliancewerden Empfänger, die auf die Links in einer E-Mail-Benachrichtigung klicken, je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

- Links werden in Vulnerability Manager Workspace für Benutzer mit der Rolle sn_vulc.admin geöffnet.
- Links werden in IT Remediation Workspace für Benutzer mit der Rolle sn_vulc.remediation_owner geöffnet.

Wenn der Empfänger über keine der genannten Rollen verfügt, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung in Konfigurations-Compliance

Verwenden Sie ab Konfigurations-Compliance v13.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung und Ausnahmeregeln zu genehmigen. Wenn Sie CC zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie bereits -Benutzer unter Konfigurations-Compliance sind, lautet die Standardoption Workflow.

Wenn Sie Konfigurations-Compliance v13.0 oder höher bereitgestellt haben, ist der Wert der Systemeigenschaft *sn_vulc.flow_designer_activation* auf „true“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie Konfigurations-Compliance bereits vor v13.0 verwenden, ist der Wert dieser Systemeigenschaft auf „false“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in true ändern.

Hinweis:
Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmeverwaltungs-Workflow vs. Flow Designer in Konfigurations-Compliance.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

- Ausnahmegenehmigungsregeln für Korrekturaufgabe
- Genehmigungsregel für automatische Ausnahmeregeln

Hinweis:
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

Prozedur
1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln** > **Ausnahmegenehmigungsregeln für Korrekturaufgabe**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Der Standardwert ist Konfigurations-Compliance.
Regeltyp	Gibt den Regeltyp an. Beispiel: Ausnahmeverwaltung oder Ausnahmeregel.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurze Beschreibung der Genehmigungsregeln.
Genehmigungsablaufy (Tage) Ab v14.11 von Konfigurations-Compliance	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.
Genehmiger benachrichtigen (Tage) Ab v14.11 von Konfigurations-Compliance	Datum, nach dem der Genehmiger benachrichtigt wird, um Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel in Konfigurations-Compliance.

   Hinweis:
   Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Testergebnisse definieren, die bei verschiedenen Korrekturaufgaben gefunden wurden.

Erstellen Sie Konfigurationen für eine Genehmigungsregel in Konfigurations-Compliance

Definieren Sie die Bedingungen, um übereinstimmende Korrekturaufgaben für eine Genehmigungsebene herauszufiltern.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Im Modul Genehmigungskonfigurationen können Sie mehrere Genehmigungsebenen für verschiedene Konfigurationen konfigurieren. Definieren Sie bedingungsbasierte Regeln, wobei jede Regel mehrere Genehmigungsebenen enthält.

Hinweis:
Verwenden Sie das Modul Genehmigungsregeln, um Genehmigungsregeln für die Ausnahmeverwaltungs-Workflows zu konfigurieren. Informationen zum Konfigurieren von Genehmigungsregeln finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungskonfiguration“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Bestellung	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungskonfiguration verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungskonfigurationsebenen.

5. Legen Sie auf eine der folgenden Arten eine Bedingung für die Testergebnisse oder Korrekturaufgaben fest:

Feld	Beschreibung
Bedingung	Identifiziert die übereinstimmenden Testergebnisse oder Korrekturaufgaben.
Erweiterte Bedingung	Skript, das die Bedingung für die Testergebnisse oder Korrekturaufgaben definiert. **Hinweis:** Dieses Feld erscheint, wenn Sie das Kontrollkästchen **Erweitert** aktivieren.

6. Wählen Sie **Aktualisieren**.
   Sie können Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

Example:
Sie können verschiedene Genehmigungspfade für verschiedene Arten von Korrekturaufgaben definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance

Definieren Sie die Ebenen von Anwendern und Anwendergruppen, die die Ausnahmeanforderungen genehmigen.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. Wählen Sie im Abschnitt **Genehmigerebenen** eine Genehmigerebene aus.
5. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigerebene“

Feld	Beschreibung
Name	Name der Genehmigungsebene.
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ○ Ein Genehmiger erforderlich ○ Alle Anwender müssen genehmigen
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.
Bestellung	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel. Dieses Feld ist schreibgeschützt.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen. Dieses Feld ist schreibgeschützt.
Zuweisen mit	Wählen Sie eine Option aus: ○ Anwender und Anwendergruppe ○ Genehmigungstabellenfeld ○ Skript
Gruppen	Gruppe auf Genehmigerebene, die aus mehreren Anwendern besteht. Der Benutzer muss eine der folgenden Rollen für die Ausnahmeverwaltung und Ausnahmeregeln haben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ sn_vulc.exception_approver ○ sn_vulc.read ○ sn_vulc.read_auto_exception_rule
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

6. Um die Änderungen zu speichern, wählen Sie **Aktualisieren**.

Hinweis:
Vor v13.0 funktionierte der Workflow-Prozess, wenn Benutzer nur auf Ausnahmeebene 1 vorhanden sind. Ab v13.0 muss jedoch mindestens ein Benutzer auf jeder Ebene vorhanden sein.

Vor v13.0 wurde im Workflow die Korrekturaufgabe zurückgestellt, wenn es keinen Benutzer auf der zweiten Ebene gab. Wenn jedoch ab v13.0 kein Benutzer in der zweiten Ebene vorhanden ist, wird die Genehmigungsanforderung automatisch abgelehnt.

Example:
Es kann unterschiedliche Genehmigungsebenen für Korrekturaufgaben für Linux- und Windows-Server geben.

Ausnahmeverwaltungs-Workflow vs. Flow Designer in Konfigurations-Compliance

Ab Konfigurations-Compliance (CC) v13.0 wird bei der ersten Bereitstellung von CC standardmäßig der Flow Designer für die Genehmigung von Ausnahmeanforderungen in der Ausnahmeverwaltung aktiviert. Wenn Sie ein vorhandener CC-Benutzer sind, lautet die Standardoption Workflow.

Workflow im Vergleich zu Flow Designer

Überlegungen	Workflow	Flow Designer
Version	Vor v13.0 von CC.	Ab v13.0 von CC.
Standardoption	Standardoption, wenn Sie ein vorhandener CC-Benutzer sind.	Standardoption für neue CC-Benutzer ab v13.0.
Genehmigungsprozess festlegen	Die Ausnahmeverwaltung umfasst Ausnahmeanforderungen zusammen mit Ausnahmeregeln.	Umfasst die Definition verschiedener Ebenen und das Hinzufügen verschiedener Genehmiger für verschiedene Anwendungsfälle. Einfacher zu implementieren als der Workflow. Die Ausnahmeverwaltung umfasst Ausnahmeanforderungen zusammen mit Ausnahmeregeln.
Upgrade auf Flow Designer	Sie können vom Workflow ein Upgrade auf den Flow Designer durchführen. Bestehende Anforderungen können jedoch nur mit dem Workflow genehmigt werden.	Flow Designer ist standardmäßig aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow im Vergleich zu Flow Designer (Fortsetzung)

Überlegungen	Workflow	Flow Designer
Systemeigenschaft *sn_vulc.flow_designer_activation*	Wenn Sie den Workflow für die Änderungsverwaltung vor v13.0 verwendet haben, ist die Systemeigenschaft auf „false“ festgelegt. Um den Flow Designer zu aktivieren, legen Sie diese Eigenschaft auf „true“ fest. **Hinweis:** Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben.	Wenn Sie CC zum ersten Mal für v13.0 oder höher verwenden, wird der Wert der Systemeigenschaft standardmäßig auf „true“ festgelegt.
Modul „Genehmigungsregeln“.	Nachdem die Systemeigenschaft auf true festgelegt wurde, wird die geplante Aufgabe **zum Aktivieren von Modulgenehmigungsregeln** innerhalb von 24 Stunden ausgeführt. Diese geplante Aufgabe aktiviert das Modul **„Genehmigungsregeln“**. Um dieses Modul sofort zu aktivieren, führen Sie diese Aufgabe manuell aus.	Wenn Sie CC zum ersten Mal aus CC v13.0 bereitstellen, ist dieses Modul standardmäßig verfügbar.
Genehmigungsstufen	Bietet die Option, nur zwei Ebenen von Genehmigern festzulegen.	Bietet mehrere Optionen, z. B. das Festlegen einer beliebigen Anzahl von Konfigurationen, Genehmigerebenen und das dynamische Hinzufügen von Genehmigern für jede Regel.

Konfigurations-Compliance-Integrationen

Integrationen von Drittparteien importieren Konfigurationsbewertungsergebnisse, Richtlinien, Tests, Technologien, autoritative Quellen und Testergebnisse zusammen mit anderen Schwachstellendaten in die Anwendung Konfigurations-Compliance.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anwendung Konfigurations-Compliance unterstützt die folgenden Drittanbieterintegrationen:

- Ab v14.11 fördern Sie die Behebung von Sicherheitslücken in Ihren Unternehmens-Assets, die von der Anwendung zur Kontrolle des Sicherheitsstatus identifiziert wurden, indem Sie Ergebnisse als Testergebnisse in der Anwendung Konfigurations-Compliance veröffentlichen. Die Anwendung Security Posture Control und ihre unterstützten Anwendungen sind mit separaten Abonnements von ServiceNow® Storeverfügbar. Weitere Informationen finden Sie unter Sicherheitsstatus-Überwachung.
- Microsoft Defender for Cloud Integration für Security Operations
- Palo Alto Prisma – Cloud-Schwachstellen-Integration
- Integration von Konfigurations-Compliance in Qualys
- Produkt Tenable.io der Tenable-Schwachstellen-Integration

Zusätzliche Hinweise zu Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 14.8.5 von Konfigurations-Complianceregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Microsoft Defender for Cloud Integration für Security Operations

Das Produkt Microsoft Defender for Cloud Integration ist ein Sicherheitsmanagementsystem für die Infrastruktur, das den Sicherheitsstatus Ihrer Cloud-Umgebungen verbessert.

Microsoft Defender for Cloud Integration für Security Operations wird in die Anwendung Konfigurations-Compliance integriert, um zum Erstellen von Testergebnissen Tests zu Konfigurationselementen (Configuration Items, CI) zuzuordnen. Es erkennt kontinuierlich neu in den Workloads bereitgestellte Cloud-Ressourcen und bestimmt, ob sie gemäß Sicherheitsstandards wie dem Center for Internet Security (CIS) konfiguriert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Version 2.2 wird Microsoft Azure Security Center für Microsoft Defender for Cloud Integration in Security Operationsumbenannt.

Verfügbare Versionen

Anwendung	Version
Microsoft Defender for Cloud Integration für Security Operations	2.3
Konfigurations-Compliance	14.3
Security Support Common	13.2
Vulnerability Response	16.2

Mehrere Bereitstellungen der Plattform Microsoft Defender for Cloud

Wenn Sie über mehrere Bereitstellungen der Plattformanwendung Microsoft Defender for Cloud verfügen, können Sie für jede Bereitstellung eine Integration hinzufügen. Ressourcen, die von mehreren Drittanbieterbereitstellungen identifiziert wurden, werden konsolidiert und mit Ihrem Configuration Management Database (CMDB)abgeglichen. Diese Konsolidierung findet auch dann statt, wenn sich Scan-Prozesse zwischen den mehreren Bereitstellungen überschneiden.

ServiceNow Microsoft Defender for Cloud Integrationen

Microsoft Defender for Cloud Integration für Security Operations bereichert die Compliance-Daten in Ihrer Instanz durch Abrufen von Daten von Microsoft Defender for Cloud. Eine Reihe geplanter Aufgaben ruft die Integrationen automatisch auf. Sie können diese geplanten Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Korrektur von Testergebnissen, indem sie die Instanz mit Microsoft Defender for Cloudsynchronisieren.

Für jeden Integrationsdatensatz gibt es einen konfigurierten ausführenden Benutzer mit dem Standardwert **VR.System**. Dieser Wert muss gleich bleiben.

Hinweis:
Wenn Sie keinen gültigen „Ausführen als“-Anwender festlegen, werden für die Datenquellen-Datensätze doppelte oder mehrere Anhänge zum Datenabruf erstellt. Die Anzahl der Anhänge erhöht jedes Mal, wenn die Integration ausgeführt wird. Dies erhöht die Verarbeitungszeit, was zu inkonsistenten Transformationsergebnissen führt.

Microsoft Defender for Cloud Plattformintegrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_asc.configure_integration: Möglichkeit zum Lesen, Schreiben und Löschen von Datensätzen.
- sn_vul_asc.read_integration: Möglichkeit zum Lesen von Datensätzen.

Microsoft Defender for Cloud Integrationen werden angezeigt

Zeigen Sie die Integrationen an, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
Integration der Richtliniendefinition	Ruft Richtlinien ab und erstellt Richtlinieneinträge in Ihrer Instanz.
Bewertungsmetadaten-Integration	Ruft Bewertungsmetadaten ab und erstellt Tests in Ihrer Instanz.
Integration von Compliance-Standards und -Steuerungen	Ruft Standards und Steuerungen ab und erstellt die Autorisierungsquelle und Zitate. Anschließend werden sie mit den erstellten Tests verknüpft.
Bewertungsintegration	Ruft Bewertungen ab und verarbeitet sie in Ihrer Instanz. Die Ausgabe dieser Integration sind Testergebnisse.

Erstellen Sie CIs mit der Engine Identification and Reconciliation (Identifizierung und Abgleich).

Verwenden Sie die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) zum Erstellen von CIs, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der von einem Drittanbieterscanner importiert wurde.

Wenn ein CI in der CMDB nicht abgeglichen wird, wird ein CI in der Klasse *cmdb_ci_cmp_resource* erstellt. Wenn eine Discovery später dasselbe CI findet, ergänzt sie das CI oder erstellt ein anderes.

Hinweis:
Für Cloud-Ressourcen findet kein automatischer Abgleich statt.

Microsoft Defender for Cloud Integration für Security Operationsinstallieren und konfigurieren

Installieren und konfigurieren Sie Microsoft Defender for Cloud Integration für Security Operations, damit Sie die aus Microsoft Defender for Cloud importierten Daten verwenden können, um Ihre Assets zu priorisieren und Fehlkonfigurationen zu beheben.

Vorbereitungen

Erstellt eine neue App-Registrierung in Azure Active Directory. Weitere Informationen zum Registrieren einer neuen Anwendung in Azure Active Directory finden Sie, indem Sie auf der Microsoft-Dokumentationswebsite nach Client-Anwendungen in Azure Active Directory registrieren suchen. Weisen Sie die Rolle **„Sicherheitsleser“** für die neu erstellte App-Registrierung im entsprechenden Bereich zu, mit dem Sie eine Verbindung zu ServiceNowherstellen möchten. Sie kann sich auf einer Verwaltungsgruppen- oder Abonnementebene befinden.

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**.
2. Suchen Sie in der Suchleiste nach Microsoft Defender for Cloud Integration for Security Operations.
3. Wählen Sie **Installieren** aus.

   Alle Abhängigkeiten, die installiert werden, werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Navigieren zu **Alle** > **Microsoft Defender für Cloud-Integration** > **Administration** > **Konfiguration** > **Microsoft Defender für Cloud-Konfiguration**.
5. Füllen Sie die Felder des Formulars aus.

Microsoft Defender for Cloud Konfigurationsformular

Feld	Beschreibung
API-URL	Ressourcen-URL der Instanz. Beispiel: https://management.azure.com (Azure Public Cloud)
Mandanten-ID	Mandantenidentität Ihrer Organisation.
Integrationsinstanz	Standardinstanz Sie können auch eine -Instanz erstellen, um die Daten aus mehreren Microsoft Defender -Mandanten oder -Abonnements zu übernehmen.
Client-ID	Client-Identität, die nach der Registrierung der Anwendung Microsoft Defender for Cloud Integration generiert wird.
Geheimer Clientschlüssel	Geheimer Clientschlüssel, der nach der Registrierung der Anwendung Microsoft Defender for Cloud Integration generiert wird.
Importieren Sie Ergebnisse aus	Ressourcen und Bewertungen, die den ausgewählten Verwaltungsgruppen-IDs und Abonnement-IDs entsprechen und abgerufen werden sollen.
Verwaltungsgruppen-IDs	Ressourcen und Bewertungen, die den abzurufenden Verwaltungsgruppen-IDs entsprechen. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie **im Feld Ergebnisse importieren** von die **Option Bestimmte Verwaltungsgruppen** auswählen.
Abonnement-IDs	Identifikationsnummern der Abonnements, für die die Ressourcen und Bewertungen abgerufen werden sollen. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie **im Feld Ergebnisse importieren** von die **Option Bestimmte Abonnements** auswählen.
Validierungsstatus	Gibt an, ob die angegebenen Anmeldeinformationen und die Abonnement-ID gültig sind.

6. Konfigurieren Sie die Integrationen, oder führen Sie sie aus, indem Sie **Speichern und testen**auswählen.

Konfigurations-Compliance importierte Daten für Microsoft Defender for Cloud Integration

Konfigurations-Compliance importiert Richtlinien, Tests, autoritative Quellen und Testergebnisse aus Drittanbieterintegrationen und speichert sie zur Ansicht in -Modulen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Testgruppen

Eine Gruppe von Konfigurationstests stellt eine Testgruppe dar. Testgruppen beziehen sich auf autoritative Dokumente und Testdatensätze und können an die Anforderungen Ihres Unternehmens angepasst werden. Ein Konfigurationstest kann mehreren Testgruppen angehören.

Wenn Microsoft Defender for Cloud Integration installiert ist, werden Testgruppen von der geplanten Aufgabe **Integration von Richtliniendefinitionen**abgerufen und gefüllt. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Administration** > **Integrationen** > **Integration von Richtliniendefinitionen**.

Hinweis:
Wenn Sie die Integration manuell ausführen möchten, führen Sie zuerst die **Integration der Richtliniendefinitionen** aus.

Tests

Tests sind Bibliotheken mit Datensätzen, die Scans von Computing-Assets organisieren. Konfigurationstests definieren, wie Assets verwaltet werden müssen.

Ein Konfigurations-Compliance -Test ist der Mechanismus, den Integrationsanwendungen von Drittanbietern verwenden, um Assets nach dem Testergebnistyp zu gruppieren.

Wenn Microsoft Defender for Cloud Integration installiert ist, ruft die geplante Aufgabe **Bewertungsmetadatenintegration**die Tests ab. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Integration** > **Primäre Integrationen** > **Bewertungsmetadaten-Integration**.

Hinweis:
Wenn Sie die Integration manuell ausführen möchten, führen Sie die **Bewertungsmetadaten-Integration** nach der **Integration der Richtliniendefinitionen**aus.

Ab v15.0 von Konfigurations-Compliancewird die Testgruppe, zu der ein Test gehört, in der Spalte **Testgruppen** der Liste Tests angezeigt.

Autorisierende Quellen

Konfigurations-Compliance Bei der Generierung von Schwachstellenwarnungen für Tests verwenden Sie maßgebliche Quellen und Zitate. Autoritative Quellen sind normalerweise Abschnitten veröffentlichter Branchenstandards wie **ISO 27001** und **PCI DSS 3.2.1**zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardware-Konfigurationsproblemen von Experten auf dem Gebiet der Computersicherheit. Sie definieren Anforderungen für Sicherheitsrichtlinien und -verfahren.

Wenn Microsoft Defender for Cloud Integration installiert ist, ruft die geplante Aufgabe **Compliancestandards und -kontrollen**die autorisierenden Quellen und Zitate ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen** > **Integration von Compliance-Standards und -Steuerungen**.

Hinweis:
Wenn Sie die Integration manuell ausführen möchten, führen Sie die **Integration von Compliance-Standards und -Steuerungen** nach der **Integration von Bewertungsmetadaten**aus.

Assets

Die **Assessment-Integration** bietet wichtige Informationen wie Ressourcen-Tags und Cloud-Attribute. Diese Informationen werden im Formular „Erkanntes Element“ angezeigt. Es wird hauptsächlich zum Filtern in Konfigurations-Compliance Regeln für Zuweisungs- und Korrekturaufgaben verwendet.

- Ressourcen-Tags: Alle Cloud-Ressourcen-Tags werden als Host-Tags im Rahmen der **Bewertungsintegration**importiert. Die Cloud-Tags für jeden Cloud-Ressourcentyp werden hier gespeichert, unabhängig davon, ob die Ressource ein Host ist oder nicht.
  - Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein Tokyo-Tag erstellt wird, kann ein **TOKIO-**Tag nicht in der Host-Tag-Tabelle gespeichert werden. **Tokyo** und **TOKIO** gelten als dasselbe Host-Tag. Das zuerst importierte Tag gewinnen.
  - Die Verwendung von Host-Tags als Gruppenschlüssel in einer Gruppenregel kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Cloud-Attribute für Assets: Im Folgenden sind die Cloud-Attribute aufgeführt, die die Integrationen von Microsoft Defender for Cloudabrufen:
  - Cloud-Account
  - Cloud-Region
  - Cloud-Ressourcentyp
  - Cloud-Service-Provider

Testergebnisse

Konfigurations-Compliance berechnet die Testergebnisse nicht, importiert sie jedoch als Teil einer Drittanbieterintegration. Sobald sie in Konfigurations-Compliancesichtbar sind, werden sie mit **Korrekturaufgaben**korrigiert.

Wenn die Microsoft Defender for Cloud -Integration installiert ist, ruft die regelmäßige Aufgabe **Assessment Integration (Bewertungsintegration**) die Testergebnisse ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen** > **Bewertungsintegration**.

Der Import **von Bewertungsintegrationen** ist die einzige Integration, die den Parameter `Start Time` auf der Registerkarte **Integrationsdetails** verwendet. Alle anderen Konfigurations-Compliance -Importe übernehmen alle verfügbaren Daten unabhängig von `Start Time`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Import **der Bewertungsintegration** abgeschlossen ist, wird ein Ereignis gestartet, um Berechnungen für das Importende auszulösen.

Die **Bewertungsintegration** ruft die Datenbewertungen standardmäßig nur ab, wenn sich der Status der letzten erfolgreichen Integrationsausführung für den letzten Tag ändert. Wenn also die Bewertung in den letzten Tagen kontinuierlich fehlschlägt, ruft die Integration die Bewertung nicht ab, da für die Bewertung keine Statusänderung vorliegt. Um die Testergebnisse mit den Defender-Bewertungen auf dem neuesten Stand zu halten, wird eine neue **Comprehensive Assessment Integration** hinzugefügt, die die Daten aus den letzten sieben Tagen abruft. Er wird wöchentlich ausgeführt und ruft alle Testergebnisse ab, die nicht bestanden wurden.

CI-Suchregeln zum Identifizieren von CIs aus Microsoft Defender for Cloud Integrationen

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Konfigurations-Compliance mithilfe von CI-Suchregeln automatisch Ressourcendaten, um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. Diese Regeln werden verwendet, um die Configuration Items (CIs) zu identifizieren und dem Testergebnisdatensatz hinzuzufügen, um die Behebung zu erleichtern. CI-Suchregeln des Basissystems sind für Ressourcen-ID, Name und S3-Bucket verfügbar. Weitere Informationen zu CI-Suchregeln finden Sie unter CI-Sperrregeln für Microsoft Defender for Cloud Integration for Security Operations.

Vulnerability Response Integration with Palo Alto Prisma Cloud verstehen

Prisma Cloud ist eine API-basierte Sicherheitslösung für Cloud-Infrastrukturen. Es stellt eine Verbindung zu Ihrer Cloud-Umgebung her und überwacht die in öffentlichen Cloud-Umgebungen bereitgestellten Ressourcen, z. B. Amazon Web Services (AWS), Microsoft Azureusw. Sie erhalten vollständige Transparenz und Kontrolle über die Risiken innerhalb Ihrer Public Cloud-Infrastruktur.

Die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud erleichtert die Erfassung von Richtlinien und Warnungen aus Prisma Cloud als Tests bzw. Testergebnisse in der Anwendung Konfigurations-Compliance. Mit der richtigen Konfiguration können die Testergebnisse nahtlos verwaltet werden, indem entsprechende Risikopunktzahlen zugewiesen und gruppiert und relevanten Benutzern und Gruppen zugewiesen werden.

Verfügbare Versionen

Die Tabelle listet die Anwendungen auf, von denen Vulnerability Response Integration with Palo Alto Prisma Cloud abhängig ist, zusammen mit der Version der Anwendung.

Anwendung	Version
Prisma-Cloud-Integration für Security Operations	2.3
Konfigurations-Compliance	14.7
Security Support Common	13.5
Vulnerability Response	18.0

ServiceNow Prisma-Cloud-Integrationen

Die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud hilft beim Importieren der Prisma-Daten in Ihre Instanz ServiceNow, um Ihre Instanz für eine bessere Verwaltung zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ergänzen. Die Integrationen werden automatisch durch eine Reihe von geplanten Aufgaben aufgerufen. Sie können diese geplanten Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Korrektur von Testergebnissen, indem sie die Instanz auf dem neuesten Stand halten, indem sie regelmäßig Daten aus Prisma Cloud abrufen.

Prisma-Cloud-Integrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_prismacloud.configure_integration: Möglichkeit zum Lesen, Schreiben und Löschen von Datensätzen.
- sn_vul_prismacloud.read_integration: Möglichkeit zum Lesen von Datensätzen.

Integrationen anzeigen

Sie können die Integrationen anzeigen, die Teil von Vulnerability Response Integration with Palo Alto Prisma Cloud sind, indem Sie zu navigieren **Prisma-Cloud-Integration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem verfügbar.

Ausführungssequenz	Zeitplan	Integration	Beschreibung
1	Wöchentlich	Prisma-Richtlinienintegration	• Ruft Richtlinien aus Prisma Cloud ab und erstellt Testeinträge in Ihrer Instanz. • Sie bietet keine inkrementelle Unterstützung. Wenn Sie die Integration für die letzten 10 Tage ausgeführt haben, wird auch das Ergebnis für vorherige Integrationsausführungen angezeigt.
2	Täglich	Integration von Prisma-Warnungen	• Ruft Warnungen von Prisma Cloud ab und erstellt Testergebniseinträge in Ihrer Instanz. • Stellt inkrementellen Support bereit. Die Integration wird täglich nach der letzten Integrationsausführungszeit ausgeführt.

Vorbereitung der Installation von Vulnerability Response Integration with Palo Alto Prisma Cloud

Bereiten Sie die Installation von Vulnerability Response Integration with Palo Alto Prisma Cloud vor, indem Sie Setupaufgaben ausführen.

Bevor Sie beginnen

Zur Integration von Vulnerability Response mit Palo Alto Prisma Cloud muss Ihnen in Prisma eine Berechtigungsgruppe zugewiesen werden, die schreibgeschützten Zugriff auf Richtlinien- und Warnungsdaten bietet. Weitere Informationen zu Berechtigungsgruppen finden Sie unter Prisma-Cloud-Administratorrollen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausführliche Informationen zu den Rollen, die verschiedenen Berechtigungsgruppen zugewiesen sind, finden Sie auf der Seite Prisma Cloud-Administratorberechtigungen .

Darüber hinaus müssen Zugriffsschlüssel erstellt werden, um das Lesen der Warnungen zu ermöglichen. Weitere Informationen zum Erstellen von Zugriffsschlüsseln finden Sie unter Zugriffsschlüssel erstellen und verwalten .

Um Vulnerability Response Integration with Palo Alto Prisma Cloudzu installieren und zu konfigurieren, verwenden Sie die folgende Prüfliste. Stellen Sie vor der Installation der Anwendung sicher, dass die aufgeführten Elemente abgeschlossen sind.

Prüfliste für die Vorbereitung der Integration

Aufgabe	Beschreibung
☐	Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen: • API-Basis-URL • Zugangsschlüssel-ID • Geheimer Schlüssel • Anwendername und Passwort für den Zugriff auf die Prisma-Cloud. Diese Anmeldeinformationen werden verwendet, um von der Instanz Now Platform® aus eine Verbindung zur Prisma-Cloud-Instanz herzustellen. Die Zugriffsschlüssel-ID und der geheime Schlüssel müssen nach der Registrierung im Prisma-Cloud-Portal generiert werden.
☐	Wenn noch nicht installiert und aktiviert, installieren Sie die Anwendung Vulnerability Response, bevor Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 15.2.0 von Vulnerability Response oder höher.
☐	Wenn Sie die Anwendung noch nicht in Ihrer Instanz von haben, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud in Ihre Instanz Now Platform® herunter. Weitere Informationen finden Sie unter .
☐	Stellen Sie sicher, dass Sie die folgenden Plugins installiert haben, um eine reibungslose Ausführung der Integration zu gewährleisten: • Vulnerability Response • Konfigurations-Compliance • Vulnerability Response Integration with Palo Alto Prisma Cloud Die folgenden Plugins sind optional, können aber nützlich sein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Vorbereitung der Integration (Fortsetzung)

Aufgabe	Beschreibung
	• Cloud Provisioning and Governance • Muster für Discovery und Service-Mapping
☐	Schätzen Sie die Anzahl der Testergebnisse, die importiert werden sollen. Vergewissern Sie sich, dass Ihre -Instanz die Anzahl der Testergebnisse akzeptieren kann, die Sie voraussichtlich importieren werden. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support ServiceNow von .
☐	Vergewissern Sie sich, dass Sie über einen Administrator verfügen, der die Integrationen verwaltet und die Testergebnisse korrigiert: Der Administrator installiert die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud. Wenn dies nicht zugewiesen ist, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu.

Sie sind bereit für Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud ..

Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud .

Installieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud, um die aus Prisma Cloud importierten Daten zu verwenden. Verwenden Sie diese Daten, um Fehlkonfigurationen in Ihren Assets zu priorisieren und zu beheben.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Systemdefinition** > **Plugins**.
2. Suchen Sie in der Suchleiste nach Vulnerability Response Integration with Palo Alto Prisma Cloud.
3. Klicken Sie auf **Installieren**.

   Alle Abhängigkeiten, die installiert werden, werden angezeigt.
4. Navigieren zu **Alle** > **Prisma-Cloud-Integration** > **Administration** > **Konfiguration** > **Prisma-Cloud-Konfiguration**.
5. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Integrationsinstanz	Name der neuen Integrationsinstanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen.
API-URL	URL für die Integration mit der Prisma-Cloud.
Zugangsschlüssel-ID	Eindeutiger Schlüssel zur Authentifizierung der Zugriffsanforderung für die Prisma-Cloud. **Hinweis:** Sie müssen den Schlüssel nach der Anmeldung beim Prisma-Cloud-Portal generieren.
Geheimer Schlüssel	Privater Schlüssel zur Authentifizierung der Zugriffsanforderung bei der Prisma-Cloud. **Hinweis:** Sie müssen den geheimen Schlüssel generieren, nachdem Sie sich beim Prisma-Cloud-Portal angemeldet haben.

6. Klicken Sie auf **Speichern und testen**.

Nächste Maßnahme
Navigieren Sie nach Abschluss der Installation zu **Prisma-Cloud-Integration** > **Konfiguration** um mit der Konfiguration fortzufahren.

Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud .

Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud. Verwenden Sie die aus Prisma Cloud importierten Daten, um Fehlkonfigurationen in Ihren Assets zu priorisieren und zu beheben.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur
1. Navigieren zu **Prisma-Cloud-Integration** > **Konfiguration**.
2. Füllen Sie die Felder des Formulars aus.

Prisma-Cloud-Konfiguration

Feld	Beschreibung
Integrationsinstanz	Name der neuen Integrationsinstanz. Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen.
API-URL	URL für die Integration mit Prisma Cloud.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugangsschlüssel-ID	Ein eindeutiger Schlüssel zur Authentifizierung der Zugriffsanforderung für die Prisma-Cloud. Sie müssen den Schlüssel nach der Anmeldung beim Prisma-Cloud-Portal generieren.
Geheimer Schlüssel	Ein privater Schlüssel zum Authentifizieren der Zugriffsanforderung für die Prisma-Cloud. Sie müssen den geheimen Schlüssel generieren, nachdem Sie sich beim Prisma-Cloud-Portal angemeldet haben.

3. Klicken Sie auf **Speichern und testen**.

Nächste Maßnahme
Nachdem Sie die Konfiguration abgeschlossen haben, navigieren Sie zu **Prisma-Cloud-Integration** > **Integrationen** um zu überprüfen, ob die Integrationsausführung erfolgreich ist.

Überprüfen Sie den Ausführungsstatus des Imports Vulnerability Response Integration with Palo Alto Prisma Cloud .

Verwenden Sie den Importausführungsstatus Vulnerability Response Integration with Palo Alto Prisma Cloud, um den Erfolg Ihrer Integrationsausführungen zu überprüfen und etwaige Probleme zu identifizieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 14.8.5 von Konfigurations-Compliance regelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Prisma-Cloud-Integration** > **Integrationen**.
2. Klicken Sie auf **Integration von Prisma-Richtlinien**.
3. Klicken Sie auf **Jetzt ausführen**.
   Wenn diese Integration ausgeführt wird, werden die folgenden Tabellen in der angegebenen Reihenfolge ausgefüllt:
   a. sn_vulc_test.list (Konfigurationstests)
   b. sn_vulc_auth_src (Autorisierende Quelle
   c. sn_vulc_citation (Bezugsvermerke)
4. Zeigen Sie auf der Registerkarte **Items** die Anzahl der neuen Tests an, die erstellt, aktualisiert und ignoriert wurden, indem Sie auf die Ausführung der Schwachstellenintegration klicken.

   Hinweis:
   Richtlinien werden in Prisma Cloud für die ausgewählte Cloud-Instanz definiert. Die Instanz wird basierend auf den definierten Richtlinien gescannt.

5. Klicken Sie auf **Prisma-Warnungsintegration**.
6. Klicken Sie auf **Jetzt ausführen**.
   Die folgenden Tabellen werden basierend auf der Integration ausgefüllt:
   - Testergebnisse
   - Erkannte Elemente: Wenn die Configuration Items im System nicht verfügbar sind, werden sie erstellt. Die Klasse ist immer Cloud-Ressource. Auf der Seite „Erkanntes Element“ werden drei neue Felder erstellt: **Cloud-Ressourcentyp**, **Cloud-Service Provider**und **Asset-Kategorie**.

     Klicken Sie auf der Registerkarte **Elemente** auf die Ausführung der Schwachstellenintegration, um die Anzahl der neuen importierten, aktualisierten und ignorierten Testergebnisse anzuzeigen. Die Registerkarte **Configuration Items** wird auch basierend auf der Anzahl der erstellten Testergebnisse ausgefüllt.

Datenzuordnung

Die Daten aus Prisma Cloud werden im Modul Konfigurations-Compliance der Instanz ServiceNow importiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die Daten aus Prisma-Cloud werden mit einem anderen Namen in Konfigurations-Compliance importiert, wie in der Tabelle erwähnt.

Zuordnung von Prisma-Cloud-Daten in Konfigurations-Compliance

Prisma-Cloud	Konfigurations-Compliance
Richtlinie	Test
Warnung	Testergebnis
Compliance-Standard	Autorisierende Quelle
Abschnitte	Autorisierender Quelleninhalt
Asset	Discovery-Element/ Configuration Item (CI)

Tests

Eine Richtlinie in Prisma Cloud wird als Test in Konfigurations-Complianceimportiert. Richtlinien beziehen sich auf autoritative Dokumente und Testdatensätze und können an die Anforderungen Ihrer Organisation angepasst werden. Sie können die Tests anzeigen, indem Sie zu navigieren **Konfigurations-Compliance** > **Tests**.

Wenn **Vulnerability Response Integration with Palo Alto Prisma Cloud** installiert ist, ruft der Integrationsauftrag `Prisma Policy Integration` die Tests ab. Sie können diesen Integrationsauftrag anzeigen, indem Sie zu navigieren **Alle** > **Prisma-Cloud-Integrationen** > **Prisma-Richtlinienintegration**.

Testergebnisse

Eine Warnung in Prisma Cloud wird als Testergebnis in Konfigurations-Complianceimportiert. Warnungen werden mit **Korrekturaufgaben**nachgebessert. Sie können die Testergebnisse anzeigen, indem Sie zu navigieren **Konfigurations-Compliance** > **Testergebnisse**.

Konfigurations-Compliance importiert Testergebnisse als Teil einer Drittanbieterintegration. Nachdem sie in der Anwendung Konfigurations-Compliance angezeigt werden, werden sie mit Korrekturaufgaben korrigiert.

Wenn **Vulnerability Response Integration with Palo Alto Prisma Cloud** installiert ist, ruft der Integrationsauftrag **Prisma Alert Integration (Integration von Prisma-Warnungen)** die Testergebnisse ab. Sie können diesen Integrationsauftrag anzeigen, indem Sie zu navigieren **Alle** > **Prisma-Cloud-Integration** > **Integrationen** > **Prisma-Warnungsintegration**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Prisma-Warnungsintegration** ist ein Integrationsauftrag, der täglich ausgeführt wird und die Testergebnisse mit Statusänderung nach der im Feld **Startzeit** auf der Registerkarte **Integration** definierten Zeit abruft.

Hinweis:
Wenn Sie den Integrationsauftrag **Prisma-Warnungsintegration** manuell ausführen, führen Sie ihn nach dem Ausführen des Integrationsauftrags **Prisma-Richtlinienintegration**aus.

Wenn die **Prisma-Warnungsintegration** den Import der Daten abschließt, wird ein Ereignis gestartet, um Berechnungen für das Importende auszulösen. Wenn die Warnung in den letzten Tagen kontinuierlich fehlschlägt, ruft die Integration die Warnungen nicht ab, da für die Warnung keine Statusänderung vorliegt. Um die Testergebnisdaten mit den Prisma-Warnungen auf dem neuesten Stand zu halten, wird der neue Integrationsauftrag **„Prisma Comprehensive alert Integration“** hinzugefügt, der die Warnungen abruft, die in den letzten sieben Tagen aktualisiert wurden. Sie wird wöchentlich ausgeführt und ruft alle Testergebnisse ab, die nicht bestanden wurden.

Autoritative Quellen

Konfigurations-Compliance Bei der Generierung von Schwachstellenwarnungen für Tests verwenden Sie maßgebliche Quellen und Zitate. Autoritative Quellen sind normalerweise Abschnitten veröffentlichter Branchenstandards zugeordnet, z. B. ISO 27001 und PCI DSS 3.2.1.

Diese Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardware-Konfigurationsproblemen von Experten auf dem Gebiet der Computersicherheit. Die Referenzen definieren Anforderungen für Sicherheitsrichtlinien und -verfahren. Navigieren zu **Konfigurations-Compliance** > **Autoritative Quellen** um die autorisierenden Quellen anzuzeigen.

Assets

Wenn Vulnerability Response Integration with Palo Alto Prisma Cloud installiert ist, erfasst die geplante Aufgabe `Prisma Alerts Integration` die warnungsbezogenen Informationen im Modul oder in der Tabelle „Erkannte Elemente“. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Prisma-Cloud-Integration** > **Integrationen**.

Die Prisma-Warnungsintegration importiert zusätzliche Arten von Informationen, z. B. Ressourcen-Tags und Cloud-Attribute, die in Tabellen gespeichert sind. Diese Informationen werden im Formular Erkannte Elemente angezeigt.

- Host-Tags: Eine Ressource kann mehrere Tags haben. Die Host-Tags sind im Schlüssel-Wert-Paar-Format verfügbar. Beispiel: Windows 10 als Betriebssystem und Java-Version 1.8.
- Cloud-Attribute für Assets: Die folgenden Cloud-Attribute sind verfügbar:
  - Cloud-Account: Stellt die Account-ID aus der Integration bereit. Die Informationen werden anhand der Tabelle „Cloud-Accounts“ [sn_sec_cmn_cloud_account.LIST] ausgefüllt.
  - Cloud-Region: Gibt den Ort an, an dem die Ressource gehostet wurde. Die Informationen werden anhand der Tabelle „Cloud-Regionen“ [sn_sec_cmn_region.LIST] ausgefüllt.
  - Cloud-Ressourcentyp: Stellt Informationen zum Typ der Ressource bereit, z. B. ob es sich um einen virtuellen Computer oder eine Datenbankinstanz handelt usw. Die Informationen werden anhand der Tabelle „Cloud-Ressourcentyp“ [sn_sec_cmn_cloud_resource_type.LIST] ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Cloud-Service-Provider: Stellt Informationen zum Cloud-Service-Provider bereit, z. B. Amazon Web Services (AWS), Oracle Cloud usw. Die Informationen werden aus der Tabelle „Cloud Service Provider“ [sn_sec_cmn_cloud_service_provider.LIST] gefüllt.
- Cloud-Accountgruppen: Stellt Informationen zu den Accountgruppen bereit. Die Informationen werden anhand der Tabelle „Cloud-Accountgruppen“ [sn_vul_prismacloud_account_group.list] ausgefüllt.

Hinweis:
Das Attribut „Cloud-Accountgruppen“ ist nur für Prisma verfügbar.

CI-Suchregeln

Die CI-Suchregeln des Basissystems sind für Ressourcen-ID, Name und S3-Bucket verfügbar. Weitere Informationen zu den CI-Suchregeln finden Sie unter CI-Suchregeln für Microsoft Defender for Cloud Integration für Security Operations und Palo Alto Prisma Cloud.

Prisma-Cloud-REST-Nachrichten

Prisma-REST-Nachrichten werden verwendet, um Aufrufe an die Prisma-Anwendungsprogrammierschnittstelle (API) zu tätigen und die Compliance-Daten abzurufen.

Die folgenden REST-Nachrichten sind im Lieferumfang des Basissystems enthalten.

Prisma-Cloud-Integrationen

Alle Prisma-Cloud-Integrationen verwenden das JSON Web Token (JWT) zur Authentifizierung und Autorisierung.

REST-Nachricht für Prisma-Anmeldung

Endpunkt	Beschreibung	Methode	Textkörper	Link zur API-Dokumentation
/login	Ruft das JWT-Token zur Verwendung in allen nachfolgenden Integrationen ab.	*POST*	{ "username": <<access key id >>, "password": <<secret access key>>}	https://pan.dev/prisma-cloud/api/cspm/app-login/

REST-Nachricht „Prisma-Aktualisierungs-Token“.

Endpunkt	Beschreibung	Methode	Textkörper	Link zur API-Dokumentation
/auth_token/extend	Verlängert das JWT-Token bei Ablauf automatisch. Die Standarddauer für den Tokenablauf beträgt 60 Minuten.	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/extend-session/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachricht für Prisma-Richtlinie

Endpunkt	Beschreibung	Methode	Textkörper	Link zur API-Dokumentation
/v2/policy	Ruft alle Richtliniendaten aus Prisma ab.	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/get-policies/

REST-Nachricht der Prisma-Warnung

Endpunkt	Beschreibung	Methode	Textkörper	Link zur API-Dokumentation

/v2/alert	Ruft alle Warnungen von Prisma ab.	*POST*	<pre>{
			"detailed": "false",
			"filters": [
			{
			"name": "timeRange.type",
			"operator": "=",
			"value": "ALERT_STATUS_UPDATED"
			}
			],
			"sortBy": [
			"resource.id"
			],
			"pageToken": "",
			"offset": 0,
			"limit": 2000,
			"timeRange": {
			"type": "absolute",
			"value": {
			"startTime": <<Import since at integration level>>,
			"endTime": << Current integration run time>>
			}
			}
			}</pre>
				https://pan.dev/prisma-cloud/api/cspm/post-alerts/

Für die Integration von Prisma Comprehension Alert müssen die Filter im obigen POST-Text wie folgt ersetzt werden:

```
"filters": [
 {
                "name": "alert.status",
                "operator": "=",
                "value": "open"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "dismissed"
            },
            {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "name": "alert.status",
            "operator": "=",
            "value": "snoozed"
        },
        {
            "name": "alert.status",
            "operator": "=",
            "value": "pending_resolution"
        },
        {
            "name": "timeRange.type",
            "operator": "=",
            "value": "ALERT_UPDATED"
        }

    ],
```

Integration von Konfigurations-Compliance in Qualys

Qualys Richtlinien-Compliance sammelt die Daten und sendet sie automatisch an die Anwendung Qualys, die die Informationen kontinuierlich analysiert und korreliert. Es lässt sich problemlos als Qualys Integration for Security Operations integrieren, um Konfigurationsergebnisse CIs und Business-Services zuzuordnen und so die Auswirkungen und Priorität potenzieller Fehlkonfigurationen zu bestimmen.

Wenn Sie über mehrere Bereitstellungen der Anwendung Qualys Cloud Platform verfügen, können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die von mehreren Drittanbieterbereitstellungen und ihren Schwachstellen identifiziert wurden, werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scan-Prozesse zwischen den mehreren Bereitstellungen überschneiden. Daten, die aus den einzelnen Bereitstellungen stammen, werden identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

Hinweis:
Die ursprüngliche Schwachstellenintegration kann nicht gelöscht, sondern deaktiviert werden. Integrationen, die aus inaktiven Vorlagen erstellt werden, sind standardmäßig deaktiviert.

Host-Tags

Alle Host-Tags werden als Teil der Qualys -Hostlisten-Integration importiert. Host-Tags werden hauptsächlich zum Filtern in Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben verwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

Hinweis:
Die Integration der Qualys -Hostliste muss vor dem Erstellen der Regeln für Zuweisungs- oder Korrekturaufgaben in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können, und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein **San Diego** -Tag erstellt wird, kann kein **SAN DIEGO** -Tag in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das zuerst importierte Tag gewinnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft **sn_vul.import_host_tags**gesteuert. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Durch das Deaktivieren von Tags werden sie für alle Instanzen deaktiviert.

Host-Tags (auch als Asset-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Host-Assets Tags zuweisen. Dann können Sie beim Starten von Scans Tags auswählen, die den Hosts zugeordnet sind, die Sie scannen möchten. Mit dem Modul „Host-Tags“ können Sie Host-Tag-Daten von Qualys zeitplanbasiert in Ihre Instanz herunterladen.

Zuordnung eines Tests zu seiner Testgruppe

Um das Feld Testgruppe in einem Testformular auszufüllen, aktivieren Sie die Systemeigenschaft *sn_vulc.add_policy_as_key*. Weitere Informationen dazu, wie ein Test seiner Testgruppe zugeordnet wird und welche Auswirkungen die Aktivierung dieser Systemeigenschaft hat und welche Voraussetzungen erfüllt sind, finden Sie im Artikel KB1644268 .

Warnung:
Sie können die Systemeigenschaft *sn_vulc.add_policy_as_key* nicht deaktivieren, sobald sie aktiviert ist. Lesen Sie daher den Abschnitt „Auswirkung“ im KB1644268 -Artikel, bevor Sie diese Systemeigenschaft aktivieren.

Wenn Sie diese Systemeigenschaft aktivieren, wird nach der nächsten Erfassung das Feld **Testgruppe** in der Testtabelle hinzugefügt und füllt die Testgruppe, zu der ein Test gehört, aus. Daher können Sie ganz einfach:

- Durch Dot-Walking von Test zu Testgruppe die Testgruppe identifizieren, zu der ein Testergebnis gehört.
- differenziert Testdatensätze mit derselben Test-ID, die verschiedenen Testgruppen zugeordnet sind.

Qualys wird in die Anwendung ServiceNow® Konfigurations-Compliance integriert

Wenn Qualys Vulnerability Integration bereits auf Ihrem System installiert ist und Ihre API-Anmeldeinformationen sich von denen unterscheiden, die Sie für Konfigurations-Complianceverwenden möchten, wechseln Sie zum Setup-Assistenten (in Vulnerability Response), und weisen Sie sie den einzelnen **Qualys-PC-** Integrationen zu.

Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen** und bearbeiten Sie das Feld **Qualys-API-Anmeldeinformationen** auf der Registerkarte **Qualys-REST-Details**.

Konfigurieren Sie die PCRS-Parameter

Ab v12.6.3 von Qualys Integration for Security Operationskönnen Sie die Qualys PCRS-Richtlinien-Host-Integration und die Qualys-PCRS-Testergebnis-Integration für den Import von Testergebnissen mit neuen Sätzen von Qualys APIs verwenden. Diese Integrationen benötigen eine Gateway-URL, um Informationen von Qualysabzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie Qualys Integration for Security Operations für Vulnerability Responseinstallieren, können Sie die **Gateway-URL** für die neuen PCRS-Integrationen in Konfigurations-Compliancekonfigurieren. Weitere Informationen, wie Sie die Gateway-URL für Ihre API-URL finden, finden Sie unter Ihre Qualys-Plattform identifizieren .

Die Gateway-URL muss in Ihrer Instanz ServiceNow hinzugefügt werden.

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**.

   Hinweis:
   Stellen Sie sicher, dass Sie sich in dem Bereich Qualys for Security Operations befinden.

2. Öffnen Sie die Instanz, die von den PCRS-Integrationen verwendet wird.
3. Fügen Sie auf der Registerkarte Integrationsinstanzparameter die Gateway-URL für die Konfiguration **„gateway_url“** hinzu.

   Hinweis:
   Die Qualys-PCRS-Testergebnisintegration ist abhängig von der Qualys-PCRS-Richtlinienhostintegration. Wenn Sie also die Qualys-PCRS-Testergebnisse für die Integration zurückdatieren, müssen Sie sie möglicherweise erneut in derselben Reihenfolge ausführen.

Mit der Qualys Integration for Security Operations installierte Komponenten

Die folgenden Rollen, geplanten Aufgaben und Tabellen werden mit der Qualys-Integration für Security Operations installiert.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Zeigen Sie gefilterte Listen für mit einer Anwendung installierte Komponenten an

Filtern Sie die Tabelle „Anwendungsdateien“, damit nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert wurden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert werden, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie diese Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator **sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **AND**und dann aus. **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_qualys.read	Hat Lesezugriff auf die Datensätze Qualys Vulnerability Integration.	
sn_vul_qualys.user	Anwender für Qualys Vulnerability Integration. Kann Datensätze lesen und schreiben	sn_vul_qualys.read
sn_vul_qualys.admin	Administrator fürQualys Vulnerability Integration. Sie können beispielsweise Startdaten der Integration ändern und einige erweiterte Konfigurationseinstellungen vornehmen.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Kann konfigurieren Qualys Vulnerability Integration	sn_vul_qualys.admin

Geplante Aufgaben installiert

Regelmäßige Aufgabe	Beschreibung
Qualys PC-Richtlinien	Ruft Richtlinien von Qualysab. Die Ausgabe wird in der Tabelle sn_vulc_policy gespeichert. Die in dieser Integration verwendete API unterstützt keine Paginierung, sodass alle Richtlinien auf einer einzigen Seite heruntergeladen werden.
Qualys PC-Richtliniendetail	Ruft die vollständigen Richtliniendetails ab, z. B. Technologien und Abschnitte.
Qualys PC-Steuerungen	Ruft Informationen zu Compliancekontrollen für verschiedene Kontroll-IDs von Qualysab.
Qualys PC-Ergebnisse	Ruft Compliance-Situationsdatensätze von Qualysab. Die Ausgabe dieser Integration sind Testergebnisse. Standardmäßig werden die Parameterdetails an den Import von Hostinformationen, Daten/Uhrzeiten der letzten Scans, Kontroll-ID und Nachweisinformationen übergeben.
Qualys PC Comprehensive Results (PC umfassende Ergebnisse).	Ruft Compliance-Situationsdatensätze von Qualys basierend auf dem letzten Bewertungsdatum für die nicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	bestandenen Testergebnisse ab. Dieser Job wird einmal pro Woche ausgeführt. Die Ausgabe dieser Integration sind Testergebnisse. Standardmäßig werden die Parameterdetails übergeben, um die Hostinformationen, Daten/Uhrzeiten der letzten Scans, Kontroll-ID und Nachweisinformationen zu importieren.
Qualys PCRS-Richtlinien-Hostintegration	Ruft Hostdaten von Qualys ab und verarbeitet sie in Ihrer -Instanz. Die Ausgabe dieser Integration sind Richtlinien-Host-IDs. Die Daten des Qualys Hosts werden in diese Integration importiert. **Hinweis:** • Diese geplante Aufgabe wird nur angezeigt, wenn Konfigurations-Compliance installiert ist. • Konfigurieren Sie die Integrationsinstanzparameter „gateway_url“ und „pcrs_page_size“, bevor Sie diese Integration ausführen. Diese beiden Integrationen sind inaktiv. Wenn Sie eine dieser Integrationen aktivieren, werden die PC-Ergebnisintegrationen deaktiviert. Diese beiden Integrationen werden basierend auf den neuen Streaming-APIs von Qualys hinzugefügt.
Qualys Integration von PCRS-Testergebnissen	Ruft die Testergebnisse für jede Host-ID ab. Diese Integration verwendet den Parameter „Startzeit“ auf der Registerkarte „Integrationsdetails“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	Hinweis: • Diese geplante Aufgabe wird nur angezeigt, wenn Konfigurations-Compliance installiert ist. • Konfigurieren Sie die Integrationsinstanzparameter „gateway_url“ und „pcrs_page_size“, bevor Sie diese Integration ausführen. • Wenn Sie die Integration manuell ausführen möchten, führen Sie Qualys Integration der PCRS-Testergebnisse nach Qualys PC-Richtlinien, Qualys PC-Richtliniendetails und Qualys Integration des PCRS-Richtlinien-Hosts aus.

Hinweis:
Die Integrationen Qualys PCRS-Richtlinienhost und Qualys PCRS-Testergebnisse sind standardmäßig inaktiv. Diese beiden Integrationen basieren auf den neuen Streaming-APIs von Qualys. Wenn Sie eine dieser Integrationen aktivieren, wird die Integration für PC-Ergebnisse deaktiviert und umgekehrt.

Tabellen installiert

Tabelle	Beschreibung
Qualys PC-Ergebnisimport sn_vul_qualys_pc_result_import	Tabelle, die die Importsatzzeile erweitert. Die Transformation von Feldzuordnungen wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.
Richtlinien-Host-ID sn_vul_qualys_policy_host_id	Tabelle, in der die Zuordnung zwischen der Richtlinie und dem Host gespeichert wird, für den diese Richtlinie gescannt wurde. Diese Tabelle wird in der neuen Qualys PCRS-Integration verwendet. **Hinweis:** Diese Tabelle wird nur angezeigt, wenn Konfigurations-Compliance installiert ist.
Qualys PCRS-Richtlinien-Host-Import sn_vul_qualys_pcrs_policy_host_import	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet. **Hinweis:** Diese Tabelle wird nur angezeigt, wenn Konfigurations-Compliance installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Qualys PC-Richtlinienimport sn_vul_qualys_pc_policy_import	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.

Aktualisiert Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für die Qualys-Integration

Erstellen Sie eindeutige Configuration Items (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um weitere Details zu Ihren Schwachstellen zu erhalten.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig können Sie Ihre Assets in der Anwendung Vulnerability Response anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch in Ihrer CMDB als ein CI gespeichert.

Wie in den folgenden Tabellen gezeigt, können beispielsweise mehrere Assets (CI) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, verfügen jedoch über eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche in der Regel als einzelnes CI (CI 1) identifiziert und gespeichert.

Standardmäßige IP-Suche und CI-Erstellung

Quelle	IP-Adresse	NETWORK_ID	Konfigurationselement
Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	REPOSITORY_ID	Konfigurationselement
Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse aufweisen, um sie als unterschiedliche Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die geplante Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integration im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzu. Von der IRE erstellte vorhandene CIs werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Ab v14.0 von Vulnerability Response und v12.1 der Qualys Vulnerability Integration Vulnerability Integration werden die CMDB-CI-Klassenmodelle (1.0.21.) unterstützt. Die -Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

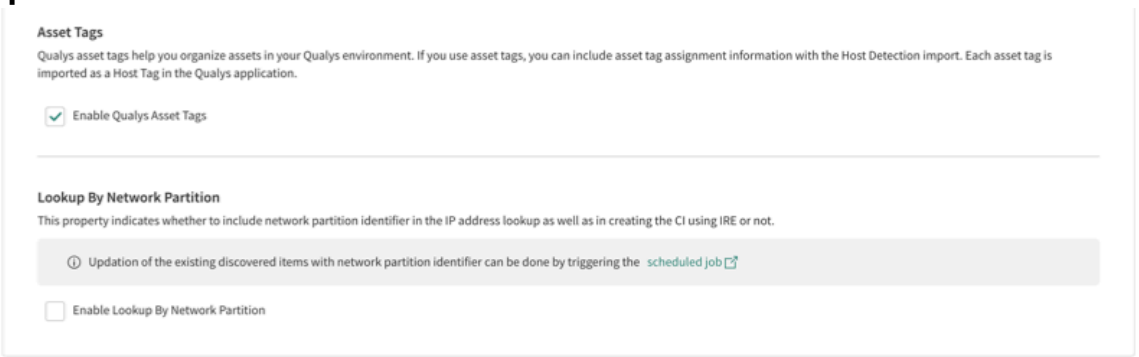
Option	Beschreibung
Geplante Aufgaben bei Bedarf ausführen.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Daten Qualys Vulnerability Integration werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartitionsbezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.
Warten Sie mit den nächsten geplanten Aufgaben auf Importe neuer Daten aus den Integrationen.	Erstellen Sie CIs für jedes neue Asset unter Verwendung des Netzwerkpartitionsbezeichners, beginnend mit der nächsten geplanten Aufgabe. CI, angreifbares Element und Erkennungsdatensätze werden mit der neuen Granularität aktualisiert. Neue CIs werden erstellt, wenn keine exakte Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Qualys Vulnerability Integrationaus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Wählen **Hosterkennungskonfiguration**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen aus **Suche nach Netzwerkpartition**



Abschnitt.

6. Klicken Sie auf **Fertigstellen**.

Die Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY_ID sind in der IP-Suche und der CI-Erstellung enthalten

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI2

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Qualys: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI2

Die Suchregeln für die IP-Adresse und die unvollständige IP-Adressen-CI-Identifizierung enthalten das Attribut des Netzwerkpartitionsbezeichners für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integrationautomatisch.

Nachdem Sie die geplante Aufgabe aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie bei Bedarf geplante Aufgaben starten. Die CIs in vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen werden automatisch aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie zusätzliche Filterparameter für Qualys -Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Qualys Vulnerability Integration an, um die Schwachstellendaten, die Sie mit den unterstützten Integrationen Qualys importieren, weiter zu verfeinern.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, um nur bestimmte Schwachstellendetails überprüfen zu können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach bestimmten IPs oder IP-Bereichen gefiltert werden. Oder Sie möchten nur Computer importieren, die sich in Ihrem Anwendungsbereich befinden, z. B. nur Computer innerhalb Ihres Unternehmensnetzwerks, die keine externen Geräte sind.

Um diese Daten zu sammeln, können Sie Qualys Parameter hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit den Parametern Qualys in Ihrem Now Platformanpassen. Sie können diese Werte in Ihrem HTTP-Methodendatensatz unter der REST-Methode für die unterstützten Qualys -Integrationen von Qualys Vulnerability Integrationändern oder hinzufügen.

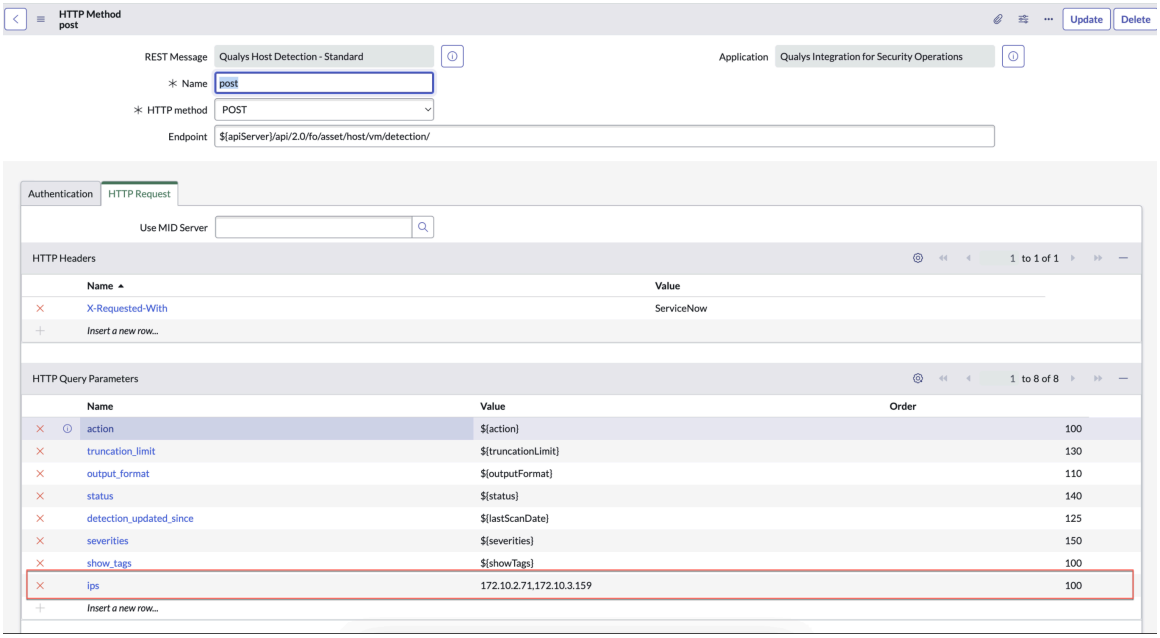
Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Suchen Sie die vom Produkt Qualys unterstützten Parameter auf der Entwickler-Site, die Sie für die Filterung verwenden möchten.
   Parameter und Werte, die Sie aus dem Produkt Qualys eingeben, werden nur auf der Ebene der Integrationsinstanz in Ihrem Now Platformunterstützt. Alle Qualys Integrationen unterstützen die Filterung anhand von Abfrageparametern.
2. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
3. Klicken Sie auf der Listenseite Qualys Integrationen auf den Datensatz für die Integration, für die Sie den Datensatz öffnen möchten.
4. Wählen Sie die Registerkarte Qualys REST-Details aus, suchen Sie das Informationssymbol (I) für die REST-Methode und anschließend auf **Datensatz öffnen,** und klicken Sie darauf, um den Datensatz für die HTTP-Methode zu öffnen.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Fügen Sie in den HTTP-Abfrageparametern für den Anforderungstext die Werte hinzu, die Sie von der Developer Site Qualys erhalten haben.

   In der folgenden Abbildung wurde als Beispiel der Parameter `ips={value}` hinzugefügt, der nur bestimmte IP-Adressen/Bereiche erfasst. In diesem Fall entspricht **der Wert** einer oder mehreren von Ihnen angegebenen IPs/Bereiche. Mehrere Einträge werden durch Kommas getrennt, 172.10.2.71, 172.10.3.159, und ein Bereich wird mit einem Bindestrich angegeben, 10.10.10.1-10.10.10.100. Weitere Informationen finden Sie auf der Entwickler-Website Qualys.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Qualys weitere Informationen zum Trennen der einzelnen Werte.

Hinweis:
Sie sollten sich Ihrer API-Anforderungen bewusst sein. Möglicherweise müssen Sie diese API-Eigenschaften den Abfrageparametern oder dem Textinhalt hinzufügen.

Einige andere Parameter, die auf der Entwicklerseite Qualys nützlich sein könnten:

- `ag_ids` Abzurufende Asset-Gruppenlisten-IDs. Dieser Parameter stellt sicher, dass nur Computer in Ihrem Bereich einbezogen werden.
- `qids` Dieser Parameter beschränkt die Ergebnisse auf bestimmte Schwachstellen (QID in der Tabelle „Drittpartei-Einträge“). Diese Einstellung verhindert, dass Ihr System mit Informationsdatensätzen überschwemmt wird.

7. Klicken Sie auf **Aktualisieren**.

[store-future: BEGIN review]

Qualys -Testergebnis mit seiner Testgruppe in Konfigurations-Complianceverknüpfen

Erstellen Sie Tests und Testergebnisse in Konfigurations-Compliance mit Zuordnung zur Testgruppe Qualys.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Qualys verwaltet eine Standardbibliothek mit Richtlinien und Steuerungen und ermöglicht gleichzeitig die Erstellung benutzerdefinierter Richtlinien und Steuerungen. Diese Steuerungen können einer Richtlinie zugeordnet werden, wodurch ein umfassendes Framework für die Bewertung der Sicherheitslage von IT-Assets bereitgestellt wird. Bei der Auswertung für ein Asset generiert die Richtlinie Qualys Positionen, die in Konfigurations-Complianceein Testergebnisse umgewandelt werden. Ein Steuerelement, das einer Richtlinie Qualys zugeordnet ist, unterscheidet sich von dem in der Bibliothek Qualys vorhandenen Standardsteuerelement. Dies ermöglicht die Flexibilität, Attribute wie Relevanz, Status (Aktiv oder Inaktiv) und Technologie für die Kontrolle auf Richtlinienebene zu definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuvor wurden in Konfigurations-ComplianceTests in der Regel für die Steuerungen der Bibliothek Qualys erstellt und nicht für die Steuerungen, die den Richtlinien Qualys zugeordnet sind. Die Testergebnisse beziehen sich auf die Tests ohne Testgruppenzuordnung. Daher sind in Konfigurations-Compliance möglicherweise weniger Testergebnisse im Vergleich zu Positionen in Qualysvorhanden.

Um Tests und Testergebnisse in Konfigurations-Compliance mit Zuordnung zur Testgruppe zu erstellen, wurde die neue Spalte „Testgruppe“ auf Testebene hinzugefügt. Das Ausfüllen dieser Spalte wird durch die Systemeigenschaft *sn_vulc.add_policy_as_key*gesteuert. Sobald diese Systemeigenschaft aktiviert ist, erstellt Konfigurations-Compliance Tests für Bibliothekssteuerungen (Testgruppe ist leer) und Steuerungen, die den Richtlinien zugeordnet sind (Testgruppe ist Richtlinien-ID). Die Testergebnisse beziehen sich auf die Tests mit Richtlinienzuordnung.

So stellen Sie sicher, dass alle Testergebnisse zu den neuen Tests mit der Testgruppenzuordnung migriert werden:

Prozedur

1. Aktivieren Sie die Systemeigenschaft sn_vulc.add_policy_as_key.
   a. Geben Sie im Filternavigator sys_properties.list ein, um die Liste der Systemeigenschaften für Ihre Instanz anzuzeigen.
   b. Suchen Sie nach der Systemeigenschaft sn_vulc.add_policy_as_key, und öffnen Sie sie.
   c. Wählen Sie den Link in der Warnmeldung aus, um die Systemeigenschaft zu bearbeiten.
   d. Setzen Sie das Feld **Wert** auf true, um die Systemeigenschaft sn_vulc.add_policy_as_key zu aktivieren.
2. **Wahlweise:** Für Kunden mit vorhandenen Daten (Tests und Testergebnisse) in Konfigurations-Compliance:
   a. Löschen Sie das Feld **Startzeit** für die Systemeigenschaft sn_vulc.add_policy_as_key.
   b. Führen Sie die Integrationen in der folgenden Reihenfolge aus:
      - Qualys PC-Richtlinien
      - Qualys PC-Steuerelemente
      - Qualys PC-Richtliniendetail
      - Integration von Qualys PC-Ergebnissen/Qualys PCRS-Testergebnissen
3. Überprüfen Sie Folgendes:
   - Überprüfen Sie nach der Ausführung von Qualys-PC-Richtlinien, ob neue Tests mit Testgruppenreferenz erstellt werden.
   - Stellen Sie nach der Ausführung der Integration von Qualys PC-Ergebnissen/Qualys PCRS-Testergebnissen sicher, dass alle Testergebnisse auf einen neuen Test mit einer ausgefüllten Testgruppenreferenz verweisen.

Ergebnisse

- Neue Tests werden mit einem Verweis auf die Testgruppe erstellt. Die zugehörige Liste „Testgruppe“ wird für die neuen Tests nicht ausgefüllt. Die neuen Tests basieren auf den Steuerungen, die Richtlinien in Qualyszugeordnet sind, und spiegeln die Relevanz, den Status (aktiv oder inaktiv) und die Technologie der Steuerung auf Richtlinienebene wider.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Test ohne die Referenz „Testgruppe“ spiegelt die Steuerungen in der Bibliothek Qualys wider.
- Alle Testergebnisse verweisen auf die neuen Tests mit Testgruppenzuordnung. Eine Testgruppe für ein Testergebnis kann durch Dot-Walking zum zugehörigen Test identifiziert werden.

[End]

Qualys Probleme mit der Vulnerability-Integration werden gelöst

Einige häufig auftretende Probleme und Problemumgehungen werden besprochen.

Anhänge werden nach dem Import nicht angezeigt

Wenn Anhänge nach dem Import von Drittparteiintegrationen für Datenquellen oder bei einem Security Incident nicht wie erwartet angezeigt werden, überprüfen Sie Ihre IP-Beschränkungen.

IP-Zugriffsbeschränkungen können verhindern, dass Anhänge sichtbar sind, es sei denn, Sie sind von einer sicheren IP angemeldet. Da bei jedem Import ein neuer Anhang hinzugefügt wird, kann dies zu Duplikaten führen, die Sie entfernen müssen.

Wenn Sie beispielsweise die Importintegration eines Drittanbieterhosts ausführen und keine Anhänge in Ihren Datenquellen angezeigt werden, überprüfen Sie die IP-Einschränkungen, und fügen Sie vor dem Import der sicheren Liste Anwender hinzu.

Ändern Sie Transformationszuordnungen

Transformationszuordnungen werden mit Basiskonfigurationen bereitgestellt und reichen normalerweise aus. Sie können die Transformationszuordnungen entsprechend den Anforderungen Ihrer Organisation ändern.

Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin + import_admin

Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Administration** > **Transformationszuordnungen** um die REST-Nachrichten anzuzeigen.
2. Filtern Sie die resultierende Liste nach Anwendung, und beschränken Sie die Liste auf die Anwendung **Qualys Vulnerability Integration**.
3. Ändern Sie die Transformationszuordnungen gemäß den Kundenanforderungen.

   Einzelheiten zu den von der Qualys-API bereitgestellten Daten finden Sie in der Dokumentation zur Qualys-API .

Überprüft die Größe der XML-Anhangeigenschaft

Überprüft, ob die XML-Anhangseigenschaft für große Dateien ausreichend ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Import Export**.
2. Scrollen Sie nach unten zu **Importeigenschaften** > **XML-Format** unten auf der Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ändern Sie den Wert bei Bedarf in 250, und klicken Sie auf **Speichern**.

Zugehörige Informationen

Verfügbare Systemeigenschaften

Einschränkungen beim Datenabruf

Standardmäßig gibt es keine Einschränkungen für den Abruf von Daten aus Qualys. Viele Datensätze können sich auf Schwachstellen mit niedrigem Schweregrad beziehen, die ein Kunde nicht bereit ist, mit seinem Vulnerability Response-Prozess zu beheben. Durch Aktualisieren der entsprechenden REST-Nachrichten-/Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/-Methode ist **Qualys Host Detection – Standard/post**. Um die Werte zu aktualisieren, fügen Sie der Post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3–5 (oder die gewünschten Schweregrade)

Qualys Knowledge Base-Integration schlägt fehl

Beheben Sie den Fehler bei Qualys der Knowledge Base-Integration, indem Sie die von Qualys empfangene Nutzlast-Anhanggröße auf den angegebenen Grenzwert reduzieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Stellen Sie sicher, dass die Anhangsgröße der Nutzlast innerhalb des angegebenen Grenzwerts liegt.
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.
   b. Wählen Sie die Registerkarte **Integrationsinstanzparameter**.
   c. Wählen Sie **max_delta_days** aus, und ändern Sie den Standardwert in 3.
2. Wenn die Integration weiterhin fehlschlägt, führen Sie die folgenden Schritte aus:
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen**.
   b. Wählen Sie **Qualys Knowledge Base**aus.
   c. Wählen Sie die Registerkarte **Integrationsdetails**.
   d. Wählen Sie im Feld **Startzeit** das aktuelle Datum aus, um die Ausführung der Ausführung für diesen Tag zu überspringen.
   e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie die Registerkarte **Integrationsinstanzparameter**.

g. Wählen Sie **kb_backfill_full_import** aus, und ändern Sie den Standardwert in „wahr“.

Ergebnisse

Durch die Ausführung der Qualys-Knowledge Base-Auffüllungsintegration werden alle Drittparteieinträge (TPEs) im System aktualisiert. Die Qualys-Host-Erkennungsintegration erstellt einen Platzhaltereintrag, die Qualys-Knowledge-Base-Auffüllungsintegration aktualisiert ihn.

Qualys Statusdiagramm der Integrationsausführung

Das Modul „Status Qualys der Integrationsausführung bietet eine grafische Ansicht des Status von Qualys Integrationsausführungen.

Um den Status von Integrationsausführungen anzuzeigen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

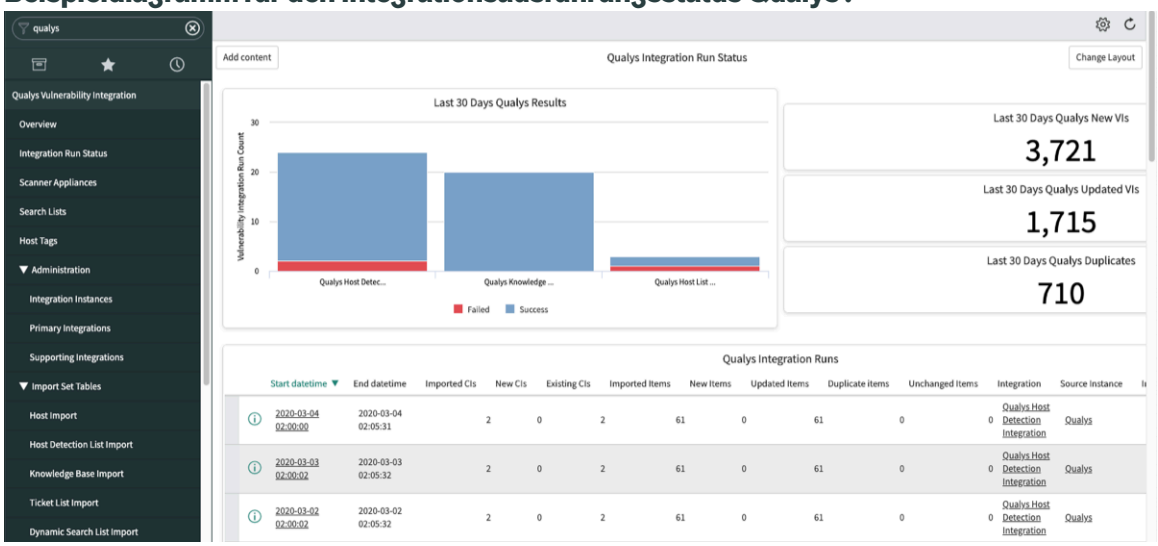
Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Zeigen Sie im Diagramm auf einen beliebigen Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Integrationsausführungsstatus Qualys zeigt den Ausführungsstatus der Schwachstellenintegration für die letzten 30 Tage an. Die von Qualys[qualys] aktualisierte VIs-Anzahl gibt die Anzahl der eindeutigen Erkennungen im selben Asset an. Das VI wird dann mit der neuen Erkennung aktualisiert.

Hinweis:
Die Anzahl der Ausführungen der Schwachstellen-Integrationen wird nur für die Integrationen angezeigt, die auf den Status „Aktiv“ festgelegt sind. Navigieren zu **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen** und legen Sie den Status auf aktiv fest.

Beispieldiagramm für den Integrationsausführungsstatus Qualys .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Werte in der Spalte „Importierte Elemente“ stellen die Gesamtzahl der Datensätze dar, die aus einer Integrationsausführung erstellt werden.
- In der Spalte Neue Elemente wird die Anzahl der Datensätze angezeigt, die aus einer Integrationsausführung erstellt wurden.
- Die Spalte „Doppelte Elemente“ ist nicht mehr ausgefüllt. Unter Umständen möchten Sie diese Spalte aus der Anzeige entfernen.
- In der Spalte Aktualisierte Elemente wird angezeigt, wie oft Datensätze während einer Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der eindeutigen Datensätze, die aktualisiert werden. Wenn beispielsweise ein Datensatz während der Integrationsausführung zweimal aktualisiert wird, wird er zweimal gezählt und als 2 aktualisierte Elemente angezeigt.
- Die Spalte „Unveränderte Elemente“ zeigt die während der Integrationsausführung gefundenen Datensätze an, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

Hinweis:
Die Integration wird für alle vier der folgenden Werte ohne Ergebnisse ausgeführt: **Neue CIs**, **Vorhandene CIs**, **Neue Elemente**und **Aktualisierte Elemente** werden aus der Liste **der Qualys-Integrationsausführungen** herausgefiltert.

Qualys Diagrammberichte zum Status der Integrationsausführung

Name	Beschreibung
Ergebnisse der letzten 30 Tage Qualys .	Die Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. In einer Balkenvisualisierung ausführen.
Letzte 30 Tage Qualys Neue AEs	Anzahl der neuen Datensätze, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Aktualisierte VIs der letzten 30 Tage Qualys	Die Anzahl der aktualisierten Datensätze, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Letzte 30 Tage Qualys Duplikate	Die Anzahl der doppelten Datensätze, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Qualys Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`. Während die Integration ausgeführt wird, ändert sich möglicherweise die Anzahl der Erkennungen oder Ergebnisse. In diesem Bericht wird die Anzahl der Erkennungen in der Spalte „Anzahl bis Datum“ in der Instanz nach Abschluss der Integrationsausführung angezeigt.
Letzte 30 Tage Qualys Angreifbares Element – Erfassungsleistungsmetriken	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage.

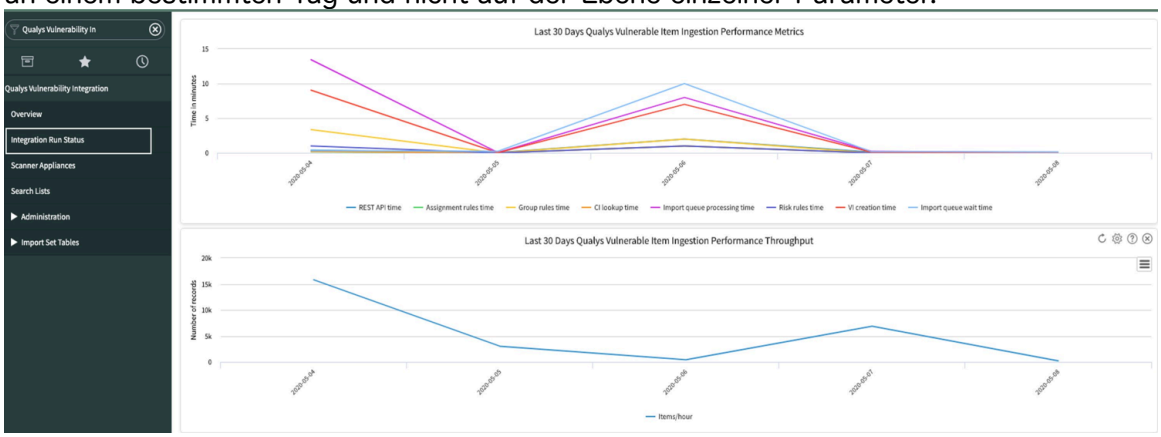
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys Diagrammberichte zum Status der Integrationsausführung (Fortsetzung)

Name	Beschreibung
Angreifbares Element – Erfassungsleistungsdurchsatz der letzten 30 Tage Qualys .	Täglicher Durchsatz bei der Erfassung von angreifbaren Elementen, gemessen für die Integration der Qualys Hosterkennung in den letzten 30 Tagen.

Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei Diagramme vergleichen die Leistungsmetriken:

- Qualys Erfassungsleistungsmetriken für angreifbare Elemente: Vergleichen Sie tägliche Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit und andere Statistiken für angreifbare Elemente für die letzten 30 Tage, um die Ursache für Leistungsabweichungen zu ermitteln. Die Leistung wird basierend auf der für jede Aktivität benötigten Zeit berechnet. Diese Parameter werden auf Integrationsausführungsebene berechnet und zugeordnet. Jeder Parameter ist zur einfachen Identifizierung farbcodiert.
- Qualys Leistungsdurchsatz bei der Erfassung von angreifbaren Elementen: Vergleichen Sie den täglichen Durchsatz bei der Erfassung von angreifbaren Elementen für die Qualys Host-Erkennungsintegration. Der Durchsatz wird in Elementen pro Stunde gemessen. Dieser Bericht zeigt die Gesamtleistung an einem bestimmten Tag und nicht auf der Ebene einzelner Parameter.



Qualys-REST-Nachrichten

Qualys-REST-Nachrichten werden verwendet, um die Qualys-API API aufzurufen und Compliance-Daten abzurufen.

Die folgenden REST-Nachrichten sind im Lieferumfang des Basissystems enthalten.

REST-Nachricht zu Qualys-PC-Richtlinien

Die REST-Nachricht „Qualys PC-Richtlinien“ ruft Richtliniendaten von Qualys ab. Die Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an Qualys gerichtete Anforderung zum Abrufen von Policeninformationen aus.

REST-Nachrichtenparameter für Qualys-PC-Richtlinien

Parametername	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachrichtenparameter für Qualys-PC-Richtlinien (Fortsetzung)

Parametername	Wert	Beschreibung
		Erforderlicher Parameter.
details	Alle	Gibt die Detailebene an, die für abgerufene Richtlinien angezeigt wird. Es ist sicher, entsprechend Ihren Anforderungen zu ändern.

REST-Nachricht für Qualys PC-Steuerelemente

Die REST-Nachricht Qualys-PC-Steuerungen ruft Informationen zu Compliancekontrollen für verschiedene Kontroll-IDs von Qualys ab.

REST-Nachrichtenparameter für Qualys PC-Steuerungen

Parametername	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter.
details	Alle	Gibt die Detailebene an, die für abgerufene Steuerungen angezeigt wird. Es ist sicher, entsprechend Ihren Anforderungen zu ändern.

REST-Nachricht mit Detail zu Qualys-PC-Richtlinien

Die REST-Nachricht Qualys PC Policies Detail ruft die vollständigen Richtliniendetails ab, z. B. Technologien und Abschnitte.

REST-Nachrichtenparameter für Qualys-PC-Richtliniendetails

Parameter	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter.
show_user_controls	Boolean	• Legen Sie den Wert auf 1 fest, um anwenderdefinierte Steuerungen (UDCs) in die XML-Ausgabe einzubeziehen. • Wenn nicht angegeben, werden UDCs nicht eingeschlossen. Dies ist ein optionaler Parameter. Es ist sicher, entsprechend Ihren Anforderungen zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachrichtenparameter für Qualys-PC-Richtliniendetails (Fortsetzung)

Parameter	Wert	Beschreibung
show_appendix	Boolean	(Optional) Legen Sie den Wert auf 1 fest, um den Abschnitt „Anhang“ in der XML-Ausgabe anzuzeigen. Wenn nicht angegeben

REST-Nachricht zu Qualys-PC-Ergebnissen

Die REST-Nachricht Qualys PC-Ergebnisse ruft Compliance-Situationsdatensätze von Qualys ab.

REST-Nachrichtenparameter für Qualys PC-Ergebnisse

Quellfeld	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Änderungen werden nicht empfohlen.
show_extended_evidence	Boolean	• Legen Sie den Wert auf 1 fest, um die erweiterten Nachweisinformationen in der Ausgabe anzuzeigen. • Auf 0 festlegen oder wenn nicht angegeben, werden die erweiterten Nachweisinformationen nicht in der Ausgabe angezeigt. **Hinweis:** • Sie können „show_extended_evidence=1“ und „hide_evidence=1“nicht in derselben Anforderung angeben. Dies führt zu einem Fehler. Der erweiterte Nachweis ist Teil der Nachweisdaten und wird nur angezeigt, wenn Nachweisdaten angezeigt werden. • Dieser Parameter ist nicht im Lieferumfang des Basissystems enthalten.
Verursacher_des_Fehlers	Boolean	Wenn Sie „1“ bestehen, gibt Qualys die Fehlerursache zurück. Wenn Sie „0“ übergeben, gibt Qualys diese Attribute nicht zurück. **Hinweis:** Dieser Parameter ist nicht im Lieferumfang des Basissystems enthalten.
policy_id		Zeigt Informationsdatensätze zur Compliance-Situation für eine angegebene Richtlinie an. Eine gültige Richtlinien-ID ist erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachrichtenparameter für Qualys PC-Ergebnisse (Fortsetzung)

Quellfeld	Wert	Beschreibung
details	Alle	Gibt die Detailebene an, die für abgerufene Positionen angezeigt wird. Es ist sicher, entsprechend Ihren Anforderungen zu ändern.
show_remediation_info		(Optional) Legen Sie den Wert auf 1 fest, um Korrekturinformationen in der XML- oder CSV-Ausgabe anzuzeigen. Standardmäßig enthält die Ausgabe keine Korrekturinformationen. Wenn nicht angegeben, werden die Korrekturinformationen nicht in die Ausgabe aufgenommen.

REST-Nachricht für Integration des Qualys-PCRS-Richtlinienhosts

Die Qualys-PCRS-Richtlinien-Host-Integration ruft Hostdaten von Qualys ab und verarbeitet sie in Ihrer -Instanz.

REST-Nachrichtenparameter für Integration des Qualys-PCRS-Richtlinien-Hosts

Parametername	Wert	Beschreibung
policyId	${lastRunDatetime}	Richtlinien-IDs für die Compliance-Bewertung.

Integration von Qualys PCRS-Testergebnissen

Die Tabelle zeigt die Anforderungsparameter, die gesendet werden.

REST-Nachrichtenparameter für Integration von Qualys-PCRS-Testergebnissen

Parametername	Wert	Beschreibung
NachweisErforderlich	${lastRunDatetime}	• Der Standardwert ist 0. Dies gibt an, dass keine Nachweisdaten für die Hoststellung abgerufen werden. • Legen Sie den Wert auf 1 fest, um die Nachweisdaten abzurufen. **Hinweis:** Wenn Sie den Wert in 1 ändern, erhöht sich die Zeit, die zum Abrufen von Statusdaten erforderlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachrichtenparameter für Integration von Qualys-PCRS-Testergebnissen (Fortsetzung)

Parametername	Wert	Beschreibung
komprimierungErforderlich		• Der Standardwert ist 1, was bedeutet, dass die Ausgabe komprimiert wird. • Legen Sie den Wert auf 0 fest, wenn die Daten nicht komprimiert werden sollen. **Hinweis:** Wenn Sie die Daten nicht komprimieren, dauert das Abrufen von Statusdaten länger.

Die Tenable-Schwachstellenintegration verstehen

Die Anwendung Vulnerability Response Integration with Tenable, die von den Entwicklern von ServiceNow für die Tenable Vulnerability Integration entwickelt wurde, verwendet Daten, die aus den Produkten Tenable.io und Tenable.sc importiert wurden, um Sie bei der Priorisierung und Behebung von Schwachstellen für Ihre Assets zu unterstützen. Die Anwendung ist mit einem separaten Abonnement aus dem ServiceNow® Storeverfügbar.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die Tenable-Schwachstellenintegration verwendet die beiden Tenable-Integrationen Tenable.io und Tenable.sc, um Scannerdaten von Drittparteien zu Ihren Assets und Schwachstellen zu importieren. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13.

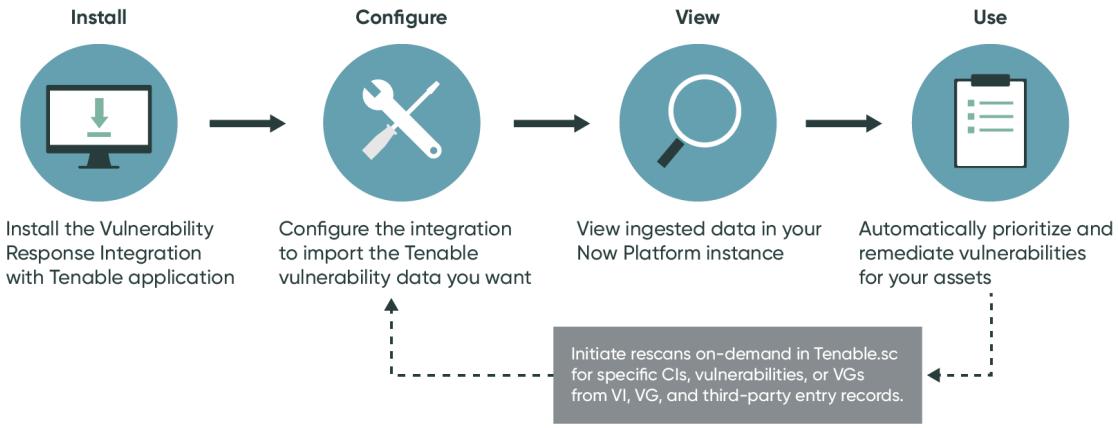
- Tenable.io ist eine cloudbasierte Unternehmensintegration.
- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID-Server verwenden.

Die Anwendung Vulnerability Response Integration with Tenable ist unter ServiceNow Store mit einem separaten Abonnement verfügbar.

Listen und Beschreibungen der Integrationen in Tenable Vulnerability Integrationfinden Sie unter Tenable.io -Integrationen mit den Anwendungen Vulnerability Response und Konfigurations-Compliance und Tenable.sc Integrationen mit der Anwendung Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable-Schwachstellen-Integration



Verfügbare Versionen für Yokohama

Freigabeversion	Release-Hinweise
Vulnerability Response Integration with Tenable v3.5, v3.6	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen

Begriffe und Schlüsselfunktionen der Integrationen

Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in Ihrer Instanz Now Platform erstellt, wenn:

- Eine importierte Schwachstelle aus einem Drittanbieterscanner wird mit einem vorhandenen Asset (einem Konfigurationselement in Ihrem CMDB) abgeglichen. Das Tenable-Produkt bezeichnet diese Übereinstimmungen als **Schwachstellen**.
- Eine importierte Schwachstelle aus einem Drittanbieterscanner wird keinem vorhandenen Asset in Ihrem CMDBzugeordnet. In diesem Fall wird zusammen mit einem angreifbaren Element auch ein nicht abgeglichenes CI erstellt.

  Für nicht abgeglichene CIs können Sie auch die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) verwenden, um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt.

Schwachstelleneinträge und Plugins von Drittparteien

Einträge für Schwachstellen von Drittparteien werden aus Scannern von Drittparteien importiert und in der Tabelle „Schwachstellen von Drittparteien“ in Ihrer Instanz Now Platform aufgeführt. Ab v24.0 von Vulnerability Responsefüllt die Spalte „Software“ in der Tabelle „Einträge von Drittanbieter-Schwachstellen“ die Common Platform Enumerations (CPEs) aus, die einem Eintrag einer Drittpartei zugeordnet sind. Schwachstelleneinträge von Drittparteien von Tenable werden in Vulnerability Response erfasst und mit vorhandenen Assets abgeglichen, die in

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihrem CMDBaufgeführt sind. Schwachstelleneinträge von Drittparteien werden von Tenable als **Plugins**bezeichnet.

Konfigurationselement bzw. Configuration Item (CI)

Konfigurationselemente sind die vorhandenen Assets, die in Ihrem CMDBaufgeführt sind.

Erkanntes Element

Aus dem Tenable-Asset-Import erfasste Assets werden mit vorhandenen Configuration Items in Ihrem CMDBabgeglichen. Importierte Assets werden aktualisiert.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der CI-Klasse ohne Übereinstimmung von CMDBerstellt. Wenn das Plugin „CMDB CI Class Models“ aktiviert ist, erstellt die Engine „Identifizierung und Abgleich“ (Identification and Reconciliation Engine, IRE) neue CIs mithilfe neuer Klassen. Weitere Informationen finden Sie unter CIs für Vulnerability Response werden mit der Engine „Identification and Reconciliation“ erstellt. Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden die Datensätze erkannter Elemente entsprechend dem Status aktualisiert. Erkannte Elemente geben Ihnen Einblick in die Art und Weise, wie Assets identifiziert und CIs in CMDBzugeordnet werden.

CI-Suchregeln

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Vulnerability Response automatisch Hostdaten (Asset-Daten), um in der Configuration Management Database (CMDB) nach Übereinstimmungen zu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und zu VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden, um Sie bei der Remediation zu unterstützen.

Erneut scannen und Korrekturscan durchführen

Sie können einen gezielten erneuten Scan-Befehl für ein bestimmtes Konfigurationselement, eine Korrekturaufgabe oder einen Drittanbietereintrag direkt aus den Datensätzen für angreifbare Elemente, Korrekturaufgaben und Schwachstelleneinträge von Drittparteien in Ihrer Instanz Now Platform initiieren. Tenable bezeichnet diesen erneuten Scan als **Korrekturscan**.

Ältere VIs automatisch schließen

Mit dem Modul Veraltete angreifbare Elemente automatisch schließen in Now Platformkönnen Sie ältere, veraltete angreifbare Elemente (VIs) bereinigen, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden. Wenn Sie diese AEs in **den Status „Geschlossen“** verschieben, können Sie die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben reduzieren und Assets in Ihrem CMDBabgleichen. Sie können alle Integrationen mit Vulnerability Response Integration with Tenable verwenden, um veraltete AEs automatisch zu schließen.

Instanz

Dieser Begriff bezieht sich auf ein bestimmtes Vorkommen Ihrer Anwendung Now Platform®.

Integration

Eine Integration ist ein produktspezifischer Verweis auf eine Integration, z. B. Tenable.io Assets Integration oder Tenable.sc Plugin Integration. Dies sind die separaten Integrationen, die zu bestimmten Tenable-Produkten in der Tenable-Schwachstellen-Integration in Ihrer Instanz gehören.

Integrationsinstanz

Dieser Begriff bezieht sich auf die separaten Tenable-Integrationen, die nach den Produkten Tenable.io und Tenable.sc aufgelistet sind.

Bereitstellung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne, eindeutige Integration als Bereitstellung Ihrer Integration bezeichnet. Der Begriff bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie in Ihrer Umgebung über mehrere Bereitstellungen verschiedener Integrationen der Produkte Tenable.io und Tenable.sc verfügen.

Die Integrationen Tenable.io und Tenable.sc enthalten außerdem die folgenden Schlüsselfunktionen:

- Konfigurationsbewertungsergebnisse, d. h. Testergebnisse sowie Richtlinien, Konfigurationstests (Steuerungen) und Zitate mit maßgeblichen Quellen, können mit dem Produkt Konfigurations-Compliance in die Anwendung Tenable.io importiert werden. Unter Tenable.io -Integrationen mit den Anwendungen Vulnerability Response und Konfigurations-Compliance und Konfigurations-Compliance erkunden finden Sie weitere Informationen darüber, wie diese Integration mit der Anwendung Konfigurations-Compliance funktioniert.
- Ab v2.1 von Tenable Vulnerability Integrationerstellen Sie eindeutige Configuration Items (CIs), die unterschiedliche Netzwerkpartitionsbezeichner für Assets in Ihrer Umgebung enthalten, die dieselbe IP-Adresse verwenden. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um weitere Details zu Ihren Schwachstellen zu erhalten.
- Sie können planen, wann die Aufgaben für alle Tenable.io - und Tenable.sc -Integrationen ausgeführt werden sollen. Sie können geplante Aufgaben bei Bedarf auch manuell ausführen.
- Für Asset-Importe mit Tenable.iokönnen Sie Asset-Tags aktivieren, um die in Ihrem CMDB aufgeführten Assets in der Umgebung Tenable.io zu organisieren und nachzuverfolgen.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie CI-Suchregeln konfigurieren, um zu definieren, wie Asset-Daten aus Drittanbieterquellen zum Identifizieren von Configuration Items (CIs) in Ihrem Now Platform CMDBverwendet werden.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie Importfilter für den Import von Schwachstellen festlegen, um nur die gewünschten Schwachstellen aus Tenable zu importieren. Für Tenable.iohaben Sie die Möglichkeit, mit dem Import von Schwachstellen **behobene** Schwachstellen aus Tenable zu importieren.
- Für Tenable.schaben Sie die Möglichkeit, bei Bedarf erneute Scans direkt aus angreifbaren Elementen, Korrekturaufgaben und Drittpartei-Eintragsdatensätzen in Ihrer Instanz Now Platform zu initiieren. Wenn VIs in den Status **„Geschlossen"/„Behoben"** versetzt wurden, in Ihrer Instanz jedoch noch nicht aktualisiert werden, können Sie überprüfen, ob Schwachstellen an bestimmten Konfigurationselementen behoben wurden. Weitere Informationen finden Sie unter Initiieren Sie den erneuten Scan für die Tenable.sc -Integration.

In den folgenden Abschnitten finden Sie weitere Details zu den Tenable-Integrationen.

Erforderliche Now Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrer Instanz Now Platform.

Administrator

Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn dies nicht zugewiesen ist, weist der Administrator im Setup-Assistenten den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu.

sn_vul.vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Zuweisung schließt der Schwachstellen-Administrator die Konfiguration der Tenable-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle VR-Anwendungen und Regeln für installierte Drittanbieterintegrationen.

sn_vul_tenable.configure_integration

Diese Rolle enthält die granulare Rolle sn_vul_tenable.read_integration, und Benutzer mit dieser Rolle können die Anwendung Vulnerability Response Integration with Tenable konfigurieren.

sn_vul_tenable.read_integration

Anwender mit diesen Rollen können Datensätze der Anwendung Vulnerability Response Integration with Tenable anzeigen (lesen), aber nicht bearbeiten.

Vulnerability Response-Gruppe

Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen „sn_vul.read_all“ und „sn_vul.remediation_owner“ automatisch.

Angreifbare Elemente

Angreifbare Elemente werden gemäß den Regeln für Korrekturaufgaben in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Vulnerability Response Übersicht über Zuweisungsregeln.

Suchregeln für Configuration Item (CI)

CI-Suchregeln identifizieren CIs und bestimmen, wann sie einem angreifbaren Element hinzugefügt werden sollen. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

Hinweis:
Einmal entfernte Regeln können nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, sollten Sie sie beim Erstellen neuer Regeln deaktivieren.

Die folgenden Tenable.io Suchregeln sind im Lieferumfang des -Basissystems enthalten.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

Hinweis:
Die Tenable.io CI-Suchregeln priorisieren und füllen die nicht leeren Netzwerkschnittstellenwerte (FDQN, IPV4 und MacAddress) gegenüber den regulären FDQN-, IPV4- und MacAddress-Werten für ein erkanntes Element aus. Wenn diese Werte für die Netzwerkschnittstelle leer sind, werden die regulären Werte für FDQN, IPV4 und MacAddress für ein erkanntes Element ausgefüllt.

Die folgenden Tenable.sc Suchregeln sind im Lieferumfang des -Basissystems enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Hinweis:
Für ein Asset werden mehrere Werte für ip_address, mac_address, fqdns und network_interfaces verwendet. Alle Werte werden in den CI-Suchregeln für die Übereinstimmung berücksichtigt. Alle Werte werden verwendet, um mehrere Netzwerkadapter mit IRE zu erstellen.

Weitere Informationen zum Konfigurieren der Kategorisierung von nicht abgeglichenen Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets aktualisieren.

Neue Eigenschaften zum Ignorieren von IP-Adressen

In Tenable.iostehen Ihnen zwei Eigenschaften zur Verfügung, wenn Sie mehrere IP-Adressen oder Mac-Adressen als Teil Ihrer CI-Suchregeln ignorieren möchten:

ignorierenIPAddress

Eine Liste der IP-Adressen, die bei der CI-Suche und CI-Erstellung ignoriert werden sollen.

ignorierenMacAddress

Eine Liste der MAC-Adressen, die für die CI-Suche oder CI-Erstellung ignoriert werden sollen.

Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus den Tenable Vulnerable Item-Integrationen und den Tenable Asset-Integrationen erkannt wurden.

Hinweis:
Der Standardfilter für diese Liste ist auf Nicht abgeglichenfestgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „Erkannte Elemente“ finden Sie unter Erkannte Elemente.

Asset-Tags

Asset-Tags (auch als Host-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Assets Tags zuweisen. Dann können Sie beim Starten von Scans Tags auswählen, die den zu scannenden Assets zugeordnet sind. Mit dem Modul „Asset Tags“ können Sie Asset-Tag-Daten von Tenable.io zeitplanbasiert in Ihre Instanz herunterladen. Asset-Daten, die Asset-Tags enthalten, werden aus Tenable.io abgerufen und mithilfe der Transformationszuordnungen der Tenable.io Asset Transform- Integration transformiert.

Alle Asset-Tags werden als Teil der Asset-Integration Tenable.io importiert. Asset-Tags werden im Allgemeinen zum Filtern in Vulnerability Response -Zuweisungsregeln und Regeln für Korrekturaufgaben verwendet. Die Tags werden im Formular „Erkanntes Element“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Führen Sie die Asset-Integration Tenable.io aus, bevor Sie in der Anwendung Vulnerability Response Zuweisungsregeln für Vulnerability Response oder Regeln für Korrekturaufgaben erstellen, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie beispielsweise ein Tag zur Beschreibung von Assets an Ihrem Standort San Diego erstellen und das San Diego -Tag erstellen, können Sie nicht auch ein SAN DIEGO -Tag erstellen und in der Asset-Tag-Tabelle speichern. San Diego und SAN DIEGO werden vom System als dasselbe Asset-Tag betrachtet. Das zuerst importierte Tag ist das Tag, das in Zukunft gespeichert und erkannt wird.
- Die Verwendung von Asset-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Asset-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Asset-Tags werden von der globalen Systemeigenschaft sn_vul.import_asset_tags gesteuert. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Durch das Deaktivieren von Tags werden sie für alle Now Platform® -Instanzen deaktiviert.

Datenabruffilter

Mithilfe der Einstellungen zum Datenabruf können Sie insbesondere den Typ und Umfang der Daten bestimmen, die Sie aus der Tenable-Anwendung in Ihre Instanz Now Platform® importieren möchten. Eine Liste der am häufigsten verwendeten Einstellungen finden Sie unter Datenabrufeinstellungen für die Tenable Vulnerability-Integration.

Schwachstellenprioritätsbewertung (VPR)

Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in Vulnerability Responseverwendet wird. Die Tenable-Risikoregel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisiko-Rechners in den Schwachstellen-Rechnern von Vulnerability Responseinstalliert.

Diese Risikoregel ist standardmäßig deaktiviert.

Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte verwendet, um die Risikopunktzahl für angreifbare Elemente zu berechnen. Standardgewichtsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Business-Relevanz = 15 %. Das Aktivieren dieser Regel des Tenable-Risikorechners kann sich auf die Leistung der Datenerfassung auswirken. Weitere Informationen zu den Rechnern Vulnerability Response und zur Regel des Tenable-Risikorechners finden Sie unter Vulnerability Response Rechner und Regeln des Schwachstellen-Rechners.

Installation und Konfiguration

Nachdem Sie Vulnerability Response Integration with Tenable von ServiceNow® Storeheruntergeladen haben, werden die Installation und Konfiguration durch den Setup-Assistenten in Vulnerability Responseunterstützt. Weitere Informationen finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

Tenable.io -Integrationen mit den Anwendungen Vulnerability Response und Konfigurations-Compliance

Die Tenable.io -Integrationen in der Anwendung Vulnerability Response Integration with Tenable sind in den Anwendungen Vulnerability Response und Konfigurations-Compliance verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste von Tenable.io Integrationen

Multi-Quelle wird für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können über den Setup-Assistenten in Vulnerability Responsemehrere Instanzen der folgenden Integrationen in Ihrer Umgebung hinzufügen und bereitstellen. Außerdem installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Tenable über den Setup-Assistenten.

Tenable.io ist eine cloudbasierte Unternehmensintegration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für das Produkt Tenable.io.

Die Tenable.io Integration für Compliance-Ergebnisse und die Tenable.io Integration für die Auffüllung von Compliance-Ergebnissen sind standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
2. Klicken Sie in der Liste „Tenable Integrations“ (Tenable-Integrationen) auf einen Integrationsnamen, um den Datensatz zu öffnen, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen auf ihren Standardwerten belassen, damit diese Integrationen gestartet werden können.

Tenable.io-Integrationen

Integration	Beschreibung
Tenable.io Assets Integration	• Ruft alle Asset-Daten, einschließlich Asset-Tags, vom Produkt Tenable.io ab und verarbeitet sie in Ihrer -Instanz. • Ab v3.0 können Sie, wenn die Tenable.io Compliance-Ergebnisintegration aktiviert ist, auch sichere Konfigurationsbewertungsdaten zusammen mit importierten Asset-Daten importieren. Diese Daten können Ihnen helfen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Asset-API • Die Ausgabe dieser Integration sind erkannte Elemente. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. • Ab v2.2 wird `Last Scan Time` nur für Assets importiert und aktualisiert, die Schwachstellen aufweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
Tenable.io Integration von Compliance-Ergebnissen	• Ab v3.0 können Sie importierte Bewertungsdaten für die sichere Konfiguration aus der Compliance-Ergebnisintegration zusammen mit importierten Daten aus der Assets-Integration dabei unterstützen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und zu beheben. • Wenn diese Option aktiviert ist, werden allgemeine Bewertungsdaten der sicheren Konfiguration abgerufen und in der Instanz Now Platform verarbeitet. Importierte Daten umfassen Testergebnisse sowie Richtlinien, Konfigurationstests (Steuerungen) und Zitate mit autorisierenden Quellen. • Bewertungsdaten für fehlende Assets oder Assets ohne Asset-IDs werden nicht importiert. • Wenn ein Testergebnis importiert wird und das entsprechende Asset in Ihrer Instanz nicht abgeglichen werden kann, wird das Testergebnis ignoriert und die ID für das fehlende Asset in einem temporären Datensatz in der Tabelle [sn_vul_tenable_missing_asset] gespeichert. • Der Gesamtwert der ignorierten (fehlenden) Assets wird im Feld **Ignorierte CIs** auf der Registerkarte **Konfiguration** im Integrationsausführungsdatensatz für diese Integration aufgeführt.
Tenable.io Integration der Auffüllung von Compliance-Ergebnissen	• Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Assets-Integration im Rahmen einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. Diese Integration gleicht Konfigurationsbewertungsdaten mit fehlenden Assets ab, die in der Tabelle [sn_vul_tenable_missing_asset] aufgeführt sind. • Importiert bis zu 200 Asset-IDs für fehlende Assets, die erkannt wurden oder in der Instanz vorhanden sind, nachdem der Asset-Integrationsimport erfolgreich abgeschlossen wurde. • Entfernt die temporären Datensätze aus der Tabelle [sn_vul_tenable_missing_asset], wenn Assets mit entsprechenden Konfigurationsbewertungsdaten abgeglichen werden können.
Tenable.io Integration von Scan-Anmeldeinformationen	• Diese Integration ruft die in Tenable.iokonfigurierten Scan-Anmeldeinformationen ab. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	• Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_tenable_scan_credential], ausgefüllt sind. • Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von Now Platforminitiiert werden. • Diese Integration soll wöchentlich ausgeführt werden.
Tenable.io Vorlagenintegration	Während des erneuten Scannens wird ein Vorlagendatensatz an Tenable.io gesendet. Diese Integration ruft verfügbare Tenable.io -Anmeldeinformationen ab, um sie für erneute Scans zu verwenden. Anmeldeinformationen sind instanzspezifisch, und ein einzelner Vorlagendatensatz wird importiert und vorübergehend in der Tabelle [sn_vul_tenable_io_template] gespeichert.
Tenable.io Plugin-Integration	• Ruft die Plugin-Daten aus dem Produkt Tenable.io ab. Abgerufene Daten basieren auf dem Datum der letzten Aktualisierung der Plugins durch eine Tenable.io Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.io Bezeichner (10 IDs) aktuell sind. • Koordiniert die REST-Nachrichtenaufrufe an die Plugin-API. • Die Ausgabe dieser Integration sind Schwachstellen von Drittparteien.
Tenable.io Integration behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status **„Offen“** und **„Erneut geöffnet“** befinden, da für diese Datensätze eine Korrektur erforderlich ist. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn die Erkennungen **behoben**sind. Angreifbare Elemente werden jedoch standardmäßig nicht für **reparierte** Erkennungen erstellt, da Tenable **behobene** Schwachstellen **als gemindert**betrachtet. • Wenn im Setup-Assistenten die **Kennzeichnung Schwachstellenzeiten für Erkennungen fester Schwachstellen erstellen** aktiviert ist, werden neue AEs im Status **„Fest“** erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. Da VIs für **feste** Erkennungen erstellt werden,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	die in Ihrer Instanz noch nicht vorhanden sind, kann sich dies negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, sodass **feste** Erkennungen nur die Status vorhandener angreifbarer Elemente aktualisieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration sind **geschlossene/reparierte** angreifbare Elemente (VIs). Außerdem werden Assets und Einträge von Drittparteien erstellt, falls diese nicht vorhanden sind. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Diese Integrationsausführung ist geplant. Es handelt sich um eine verkettete Integration. Das heißt, nach erfolgreichem Abschluss einer Ausführung wird die unten beschriebene Integration für offene Schwachstellen ausgelöst. Ab Tenable v3.3 können Sie die folgenden Informationen für die ausgeführten Schwachstellenintegrationen anzeigen: • **Blöcke gesamt:** Gesamtanzahl der von Tenable generierten Blöcke • **Verfügbare Blöcke:** Anzahl der zum Download verfügbaren Blöcke für ServiceNow
Tenable.io Integration offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss der Tenable.io Integration für behobene Schwachstellen ausgelöst. • Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration sind **Neue/Erneut geöffnete** angreifbare Elemente (VIs). Außerdem werden Konfigurationselemente und Einträge von Drittparteien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	erstellt, falls sie nicht vorhanden sind. Tenable betrachtet aktive Schwachstellen **als kumulativ** (aktuell). • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Ab Tenable v3.3 können Sie die folgenden Informationen für die ausgeführten Schwachstellenintegrationen anzeigen: • **Blöcke gesamt:** Gesamtanzahl der von Tenable generierten Blöcke • **Verfügbare Blöcke:** Anzahl der zum Download verfügbaren Blöcke für ServiceNow

Tenable.sc Integrationen mit der Anwendung Vulnerability Response

Die Tenable.sc -Integrationen in der Anwendung Vulnerability Response Integration with Tenable

Ab Vulnerability Response v20.0 wird, wenn ein Asset von einem Agent gescannt wird, in der Spalte „Agent vorhanden“ in der Liste Erkannte Elemente der Wert true angezeigt. Dies gibt an, dass es sich um einen echten Scan handelt.

Liste von Tenable.sc Integrationen

Multi-Quelle wird für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können über den Setup-Assistenten in Vulnerability Responsemehrere Instanzen der folgenden Integrationen in Ihrer Umgebung hinzufügen und bereitstellen. Außerdem installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Tenable über den Setup-Assistenten.

- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID-Server verwenden.

Tenable.sc-Integrationen

Integration	Beschreibung
Tenable.sc Assets Integration	Um zu vermeiden, dass doppelte erkannte Elemente mit importierten Asset-Daten erstellt werden, besteht die Asset-Integration des Produkts Tenable.sc aus zwei Integrationen. **Die Tenable.sc Open Assets-Integration** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable **als kumulativ** (aktuell) oder **offen**betrachtet. Die angreifbaren Elemente (VIs), die in Ihrer -Instanz mit diesen importierten Asset-Daten erstellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	werden, gelten als offen, also mit dem Status **Offen**. Diese angreifbaren Elemente müssen untersucht und möglicherweise korrigiert werden. **Tenable.sc Integration von festen Assets** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable als **verringert** (nicht mehr angreifbar) oder **behoben**ansieht. Die angreifbaren Elemente für diese Assets wechseln in Ihrer Instanz vom Status „ **Offen** “ in den Status **„Geschlossen“/ „Repariert“**, da die Ergebnisse der Scans zeigen, dass sie nicht mehr angreifbar sind. • Ruft alle Asset-Daten aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer -Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Assets-API • Die Ausgabe dieser Integration sind erkannte Elemente. • Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für die Tenable.sc Assets Integration. Nur die Assets mit den Schwachstellen, die den Bedingungen des Abfragefilters entsprechen, werden importiert.
Tenable.sc Plugin-Integration	• Ruft die Plugin-Daten aus dem Produkt Tenable.sc ab. Abgerufene Daten basieren auf dem Datum der letzten Aktualisierung der Plugins durch eine Tenable.sc Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.sc Bezeichner (10 IDs) aktuell sind und nur aktive Schwachstellen importiert werden. • Koordiniert die REST-Nachrichtenaufrufe an die Plugins-API • Die Ausgabe dieser Integration sind Schwachstellen von Drittparteien.
Tenable.sc Integration behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status **„Offen“** und **„Erneut geöffnet“** befinden, da für diese Datensätze eine Korrektur erforderlich ist. Vorhandene angreifbare Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	werden von Vulnerability Response aktualisiert, wenn die Erkennungen **behoben**sind. Angreifbare Elemente werden jedoch standardmäßig nicht für **reparierte** Erkennungen erstellt, da Tenable **behobene** Schwachstellen **als gemindert**betrachtet. • Wenn im Setup-Assistenten die **Kennzeichnung Schwachstellenzeiten für Erkennungen fester Schwachstellen erstellen** aktiviert ist, werden im Status **„Fest“** neue VIs erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. Da VIs für **feste** Erkennungen erstellt werden, die in Ihrer Instanz noch nicht vorhanden sind, kann sich dies negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, sodass **feste** Erkennungen nur die Status vorhandener angreifbarer Elemente aktualisieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration sind **geschlossene/ reparierte** angreifbare Elemente (VIs). Außerdem werden Assets und Einträge von Drittparteien erstellt, falls diese nicht vorhanden sind. Diese Integrationsausführung ist eine geplante Ausführung. Es handelt sich um eine verkettete Integration. Das heißt, nachdem eine Ausführung erfolgreich abgeschlossen wurde, wird die unten beschriebene Tenable.sc Integration offener Schwachstellen ausgelöst. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.
Tenable.sc Integration offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss der Tenable.sc Integration für behobene Schwachstellen ausgelöst. • Ruft Schwachstellendaten basierend auf den im Produkt Tenable.sc ausgewählten Abfragefiltern ab und verarbeitet sie in Ihrer Instanz. • Erstellt entsprechende angreifbare Elemente für aktive Schwachstellen. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	Netzwerkpartitionsbezeichners für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Aktualisieren/ Neu erstellen** angreifbare Elemente (VIs), wenn sie noch nicht vorhanden sind. Außerdem werden Konfigurationselemente und Einträge von Drittparteien erstellt, falls sie nicht vorhanden sind. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.
Tenable.sc Integration von Scan-Anmeldeinformationen	• Diese Integration ruft die in Tenable.sckonfigurierten Scan-Anmeldeinformationen ab. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. • Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_tenable_scan_credential] ausgefüllt sind. • Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von Now Platforminitiiert werden. • Diese Integration soll wöchentlich ausgeführt werden.
Tenable.sc Integration von Schwachstellen auffüllen	• Diese Auffüllungsintegration importiert alle offenen und behobenen Schwachstellen, die bei einem Import möglicherweise übersehen wurden. • Diese Integration importiert sowohl offene als auch behobene Schwachstellen aus den letzten sieben Tagen, um Ihre Erkennungen und angreifbaren Elemente zu aktualisieren. • Diese Integration kann sich auf Ihre Leistung auswirken. • Diese Integration ist standardmäßig deaktiviert. • Um Ihre Schwachstellendaten zu aktualisieren und potenzielle Leistungsprobleme zu vermeiden, können Sie die Ausführung der Tenable.sc-Integrationen für feste Schwachstellen und offene Schwachstellen zu einem Zeitpunkt planen, zu dem keine anderen Scans ausgeführt werden. • Die Ausgabe dieser Integration ist:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	○ **Geschlossene/behobene** angreifbare Elemente (VIs). Außerdem werden Assets und Einträge von Drittparteien erstellt, falls diese nicht vorhanden sind. ○ zum **Aktualisieren/Erstellen neuer** angreifbarer Elemente (VIs), wenn sie noch nicht vorhanden sind. Außerdem werden Konfigurationselemente und Einträge von Drittparteien erstellt, falls sie nicht vorhanden sind.

Anwenderauthentifizierung und Tenable.sc

Die Anwenderauthentifizierung wird von Ihrer Instanz Now Platform® und Version 5.13 des Produkts Tenable.sc unterstützt. Wenn Sie Version 5.12 des Produkts Tenable.sc verwenden, ist die Anwenderauthentifizierung erforderlich.

Wenn Sie die Anwenderauthentifizierung für die Tenable.sc -Integrationen auswählen, können Token ablaufen und während der Integrationsausführungen ersetzt werden. In der Spalte „Hinweise“ im Datensatz der Schwachstellenintegrationsausführung (VIN) wird für einen Prozess die folgende Meldung angezeigt, wenn ein Token abläuft: Fehler: Tokenvalidierung ist fehlgeschlagen. Es ist keine Aktion erforderlich, wenn diese Nachricht angezeigt wird. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Nachricht zeigt keine Unterbrechung oder einen Fehler beim Integrationsprozess an.

Vorbereitung der Tenable Vulnerability-Integration

Bereiten Sie sich auf die Integration von ServiceNow® Tenable Vulnerability vor, indem Sie die folgenden Setupaufgaben ausführen.

Bevor Sie beginnen

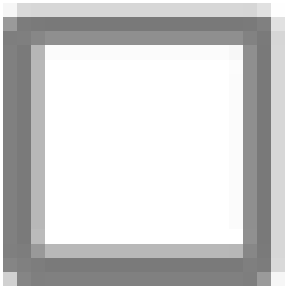
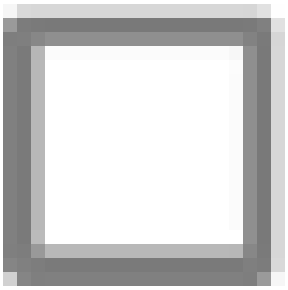
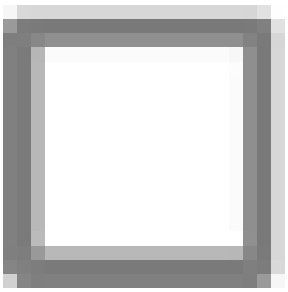
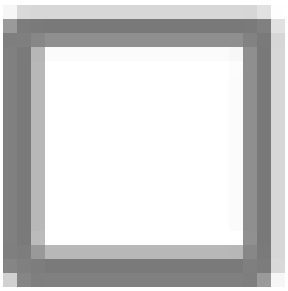
Eine erfolgreiche Integration erfordert Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Damit die Installation und Konfiguration der Anwendung Vulnerability Response Integration with Tenable reibungslos verläuft, können Sie die folgende Prüfliste ausdrucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in Ihre Instanz Now Platform® importieren.

Hinweis:
Wenn Sie Daten mit der in Tenable erstellten -Integration importiert haben und die ServiceNow® Vulnerability Response-Integration mit Tenable verwenden möchten, lesen Sie

Aktuelle Informationen zur Datenbereinigung und Migration von der in Tenable erstellten Integration zur von ServiceNowerstellten Integration finden Sie im Artikel Richtlinien für die Migration von der Tenable-Vulnerability-Response-Integration zur ServiceNow-Vulnerability-Response-Integration mit Tenable [KB0960667] .

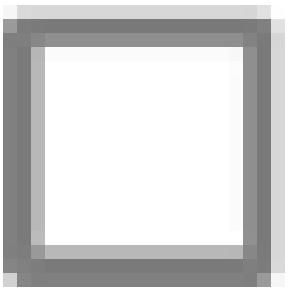
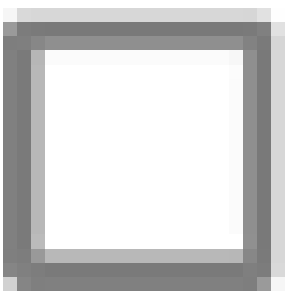
Zum Herunterladen und Installieren der Anwendung erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

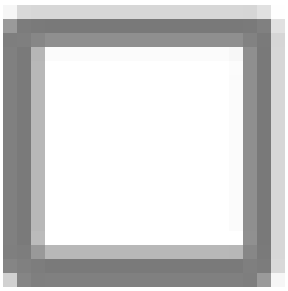
Aufgabe	Beschreibung
	(Optional) Wenn die Anwendung noch nicht installiert und aktiviert ist, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 12.1 von Vulnerability Response oder höher.
	Wenn Sie sie noch nicht in Ihrer -Instanz haben, beschaffen Sie sich Berechtigungen, und laden Sie die Anwendung Vulnerability Response Integration with Tenable auf Ihre Instanz Now Platform® herunter. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13. Weitere Informationen finden Sie unter .
	Schätzen Sie die Anzahl der angreifbaren Elemente, die importiert werden sollen. Stellen Sie sicher, dass Ihre Instanz die Anzahl der angreifbaren Elemente akzeptiert, die Sie importieren werden. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support ServiceNow® von .
	Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn dies nicht zugewiesen ist, weist der Administrator im Setup-Assistenten den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu. **sn_vul.vulnerability_admin** Nach der Zuweisung schließt der Schwachstellen-Administrator die Konfiguration der Tenable-Integrationen ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Konfiguriert alle VR-Anwendungen und Regeln sowie Integrationen von Drittparteien. **sn_vul_tenable.configure_integration** Kann Tenable Vulnerability Integration konfigurieren. Diese Rolle enthält die granulare Rolle sn_vul_tenable.read_integration.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	sn_vul_tenable.read_integration Kann Datensätze der Tenable Vulnerability-Integration anzeigen (lesen). **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen „sn_vul.read_all“ und „sn_vul.remediation_owner“ automatisch. Die erstmalige Zuweisung von Rollen zu Benutzern und Gruppen im Setup-Assistenten für die Integration wird vom Systemadministrator vorgenommen. Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Wenn dies noch nicht geschehen ist, können Sie zusätzliche Gruppen erstellen und Benutzer mit dem Benutzeradministrationsmodul in Ihrer Instanz hinzufügen, bevor Sie den Setup-Assistenten verwenden. Weitere Informationen finden Sie unter Benutzergruppen erstellen . Persona-Rollen und granulare Rollen sind verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.
	Um eine verbesserte Leistung beim ersten Import zu fördern, können Sie bestimmte Funktionen, Regeln oder Aufgaben in Ihrer Instanz deaktivieren. • Deaktivieren Sie die Schwachstellen-Rechner, wenn Sie sie nicht verwenden. Diese Rechner sowie die von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für ein angreifbares Element erstellt oder aktualisiert wird. Weitere Informationen finden Sie unter Schwachstellen-Rechner deaktivieren. • Während des ersten Imports von Datensätzen können bestimmte Benachrichtigungs-Business-Regeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Vor dem ersten Import möchten Sie möglicherweise Benachrichtigungs-Business-Regeln deaktivieren, wie in Importieren Sie Änderungen für die Tenable Vulnerability-Integrationbeschrieben.
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz von aktiviert haben, die für die Integration erforderlich sind. • Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn sich das Produkt Vulnerability Response Integration with Tenable und Ihre Instanz Now Platform in derselben Umgebung befinden. Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Umgebung befinden, müssen Sie einen MID-Server verwenden. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . • Vergewissern Sie sich, dass das IntegrationHub-Plugin installiert und aktiviert ist. Dieses Plugin ermöglicht Basissystemkomponenten das Aufrufen externer Systeme mithilfe von Integrations-APIs und aktiviert Protokollschritte wie REST. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es.
	Rufen Sie die Tenable-Anmeldeinformationen ab. Stellen Sie sicher, dass Sie über alle Accountnamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre Tenable-Produkte erforderlich sind, damit Sie darauf zugreifen können. Tenable.io erfordert Administratorzugriff mit einem Berechtigungsattribut, das größer oder gleich 64 ist. Tenable.sc erfordert Sicherheitsanalysten- oder Managerzugriff. **Hinweis:** Ab v3.8 von Vulnerability Response Integration with Tenablesind für den Zugriff auf Tenable.io keine Administratorrechte mehr erforderlich. Ein Standardbenutzer mit einem Berechtigungsattribut gleich 16 kann ebenfalls auf das Produkt zugreifen.

Sie sind bereit für Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten.

Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten

Bevor Sie die ServiceNow® Tenable Vulnerability-Integration ausführen, müssen Sie die Anwendung Vulnerability Response Integration with Tenable von der Anwendung ServiceNow Store herunterladen und mit dem Setup-Assistenten in der Anwendung Vulnerability Response installieren und konfigurieren.

Vorbereitungen

Stellen Sie vor der Installation der Anwendung Tenable sicher, dass Sie alle Elemente in der Prüfliste in Vorbereitung der Tenable Vulnerability-Integrationabgeschlossen haben.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

Erforderliche Rolle: admin für die erstmalige Zuweisung der Rolle „sn_vul.vulnerability_admin“ und die Installation der Tenable-Anwendung im Setup-Assistenten. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)), um die Anwendung nach der Installation im Setup-Assistenten zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz von verfügbar sind.

2. Suchen Sie die Kachel **Tenable (Tenable-Plattform)**, und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung Vulnerability Response Integration with Tenable installiert, die Sie aus ServiceNow Storeheruntergeladen haben.

3. Befolgen Sie die Eingabeaufforderungen im Setup-Assistenten, um mit der Installation fortzufahren.

4. Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie die Drittanbieteranwendungen Vulnerability Response mit dem Setup-Assistenten.

Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie im Setup-Assistenten zu **Integrationskonfiguration > Scanner-Integrationen,** um mit der Konfiguration fortzufahren. Weitere Informationen zu den Eingabeaufforderungen im Setup-Assistenten finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten.

Datenabrufeinstellungen für die Tenable Vulnerability-Integration

Mit den folgenden Einstellungen für den Datenabruf können Sie insbesondere den Typ und Umfang der Daten festlegen, die Sie aus der Tenable-Schwachstellen-Integration ServiceNow® in Ihre Instanz Now Platform® importieren möchten.

Mit den in den folgenden Abschnitten beschriebenen Einstellungen können Sie steuern, welche Daten Sie importieren möchten. Darüber hinaus können Sie die Werte dieser Filter unter Integrationsinstanzen festlegen. Um Integrationsinstanzen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationsinstanzen** und klicken Sie auf Ihre Integration, Tenable.io oder Tenable.sc.

Klicken Sie auf der Seite „Integrationsinstanz“, die angezeigt wird, auf die Option Integrationsinstanzparameter, um eine Liste der Parameter anzuzeigen, oder auf die Registerkarten Schwachstellenintegrationen für einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung.

Allgemeine Einstellungen und Filter für Schweregrad und Abruf für Tenable.io und Tenable.sc in Ihrer Instanz Now Platform .

Die folgenden Einstellungen sind für die Integrationen Tenable.io und Tenable.sc in Ihrer Instanz Now Platform verfügbar. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ Ihrer Instanz Now Platform angezeigt. Unter Umständen möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardwerten belassen.

Tenable.io

insert_fixed

Wenn Sie im Setup-Assistenten die Kennzeichnung **„insert_fixed** “ für die Integration des Imports von Schwachstellen aktivieren, werden neue VIs für Erkennungen im Status **„Fest“** erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

„severe_critical“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit kritischem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Festgelegte Schwachstellen zu erhalten.

severity_high

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit hohem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

„severe_mittel“

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Festgelegte Schwachstellen zu erhalten.

„severity_info“

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Fest Schwachstellen zu erhalten.

severity_low

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Fest Schwachstellen zu erhalten.

size

Diese Einstellung definiert die Anzahl der Plugin-Datensätze, die in den Ergebnissatz aus der Tenable.io Plugins-Integration aufgenommen werden sollen. Muss im Format int32 sein. Der Standardwert ist 1.000. Die maximale Größe beträgt 10.000.

num_assets

Die maximale Anzahl von Schwachstellen pro exportiertem Block aus den Integrationen Tenable.io Feste Schwachstellen und Tenable.io Offene Schwachstellen. Der Standardwert ist 50.

chunk_size

Gibt die Anzahl der Assets pro exportiertem Block durch die Tenable.io Assets Integration an. Der Standardwert ist 1.000.

Tenable.sc

async_request

Dieser Parameter ist standardmäßig inaktiv (falsch). Aktivieren oder deaktivieren Sie diesen Parameter, um asynchrone oder synchrone API-Aufrufe mit Tenable.sc durchzuführen. Wenn bei synchronen Aufrufen eine Zeitüberschreitung von 30 Sekunden auftritt, wenden Sie sich an den Support für das Tenable-Produkt, um die Box optimieren zu lassen. Sobald dieser Parameter aktiviert ist, gilt er für alle Integrationen von Tenable.sc. Für Bestandskunden, die asynchrone Anrufe verwenden, ist ein Korrekturskript verfügbar, das den vorhandenen Integrationsinstanzen Tenable.sc einen neuen Parameter „async_request“ hinzufügt. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**.

insert_fixed

Wenn Sie im Setup-Assistenten die Kennzeichnung **„insert_fixed** “ für die Integration des Imports von Schwachstellen aktivieren, werden neue VIs für Erkennungen im Status **„Fest“** erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

Offset

Gibt die Anzahl der Assets, Plugins und Schwachstellen an, die in einer Integrationsausführung importiert werden.

Abfragefilter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abfragefilter werden in der Tenable-Konsole konfiguriert. Die IDs dieser Abfragefilter können im Setup-Assistenten oder auf der Seite „Integrationsinstanzen“ in Ihrer Instanz Now Platform ausgewählt werden. Diese Filter werden beim Abrufen der Daten aus den Tenable.sc Integrationen angewendet.

REST-Nachrichten für die Tenable-Schwachstellen-Integration

Die ServiceNow® REST-Nachrichten der Tenable-Schwachstellenintegration werden verwendet, um Aufrufe an die Tenable-API zu erstellen.

Tenable.io Assets-REST-Nachricht

Mit der REST-Nachricht „ Tenable.io Assets werden Asset-Informationen für die Tenable.io Asset-Integration abgerufen. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Assets-Informationen aus. Der Exportauftrag für Assets wird mit den folgenden Filtern übermittelt:

- „is_deleted“: falsch
- „is_licensed“: wahr

Tenable.io REST-Nachricht für Plugins

Die REST-Nachricht Tenable.io „ Plugins ruft Plugin-Informationen für die Tenable.io Plugin-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Plugin-Informationen aus.

Tenable.io REST-Nachricht zu Schwachstellen

Mit der REST-Nachricht „ Tenable.io Schwachstellen ruft sie Schwachstelleninformationen für offene und geschlossene Schwachstellen aus der Schwachstellenintegration Tenable.io ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Informationen zu Schwachstellen aus.

Tenable.sc fragt die REST-Nachricht ab

Die REST-Nachricht Tenable.sc-Abfragen ruft die Abfragefilterinformationen für die Tenable.sc-Asset-Integration und die Tenable.sc-Schwachstellenintegration ab, für die der Abfragefilter konfiguriert ist.

Tenable.sc REST-Nachricht für Plugins

Die Tenable.sc Plugin-REST-Nachricht ruft Plugin-Informationen für die Tenable.sc Plugins-Integration ab. Änderungen am Datensatz der REST-Nachricht „Plugins abrufen“-Methode wirken sich auf die Anforderungen an Tenable.sc zum Abrufen von Plugins-Informationen aus.

Parametername	Wert	Beschreibung
Typ	aktiv	Gibt an, aus welcher Quelle Tenable Daten abruft. Von Code verwendet. Änderungen werden nicht empfohlen.
Felder	ID, Beschreibung, cvssVector,cvssV3Vector, cvssV3TemporalVector, Übersicht, cvssVector,	Gibt die Liste der aus Tenable importierten Felder an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
	baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, Name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs,family, riskFactor, cpe, sieheAlso, Lösung, ExploitFrameworks, ExploitFrameworks Typ, Copyright, Version, SourceFile, Abhängigkeiten, erforderlichePorts, erforderliche UDP-Ports, srcPort, dstPort,Protokoll, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, VulnPubDate, modifiedTime, md5	

Tenable.sc REST-Nachricht zu Schwachstellen

Die Tenable.sc Schwachstellen-REST-Nachricht ruft Informationen zu Schwachstellen aus der Tenable.sc Integration ab. Änderungen an der Methode zum Abrufen von REST-Nachrichten zum Abrufen von Schwachstellen oder zum Abrufen von gepatchten Schwachstellen oder, beginnend mit v14.0 Vulnerability Response und v2.2 der Tenable Vulnerability-Integration, am Datensatz „Auffüllung von Schwachstellen abrufen“ wirken sich auf die Anforderungen aus, die an Tenable.sc zum Abrufen von Informationen zu Schwachstellen gestellt werden.

Tenable.sc REST-Nachricht zum Scannen der Anmeldeinformationen

Tenable.sc REST-Nachricht für Richtlinie

Die POST-REST-Nachricht Tenable.sc policy fügt eine Richtlinie für angeforderte Plugins hinzu. Die generierte Richtlinie wird in Scan-Anforderungen für Tenable.sc verwendet.

Tenable.sc REST-Nachricht scannen

Die POST-REST-Nachricht Tenable.sc scan fügt einen Scan hinzu, der vom Zugriff und der Berechtigung abhängt, die im Anforderungstext der REST-Nachricht definiert sind. Es verwendet Richtlinie, Plugin-ID und IP(s) im Anforderungstext für die Scan-Anforderung.

Tenable.sc REST-Nachricht Scan-Ergebnis

Die Tenable.sc Scan-Ergebnis-GET-REST-Nachricht enthält Scan-Details des Scans, der mit der Scan-REST-Nachricht generiert wurde. Verwendet die scanResultId in der Antwort auf die Scan-REST-Nachrichten und ruft Scan-Details für den ausgelösten Scan ab.

Tenable.sc Anmeldeinformationen scannen

Mit der REST-Nachricht zum Scannen der Anmeldeinformationen Tenable.sc werden die Anmeldeinformationen von Tenable.scabgerufen. Änderungen am Datensatz der REST-Nachrichtmethode „Import“ wirken sich auf die Anforderungen aus, die an Tenable.sc zum Abrufen der Anmeldeinformationen gestellt werden.

Parametername	Wert	Beschreibung
Felder	ID, Name, Beschreibung, Typ	Gibt die Liste der Felder an, die aus importiert werden Tenable.sc

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
Filter	verwendbar	Gibt an, dass die Integration nur verwendbare Anmeldeinformationen aus abruft Tenable.sc Änderungen an einem der Parameter werden nicht empfohlen.

Datentransformation für die Tenable Vulnerability-Integration

Nachdem Sie die zu importierenden Daten identifiziert haben, werden sie vom Tenable-Produkt abgerufen und über eine Reihe von Datenquellen und Transformationen in Ihrer -Instanz verarbeitet.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „Normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen wandeln importierte Tenable-Schweregrade in Standard-Schweregrade zur Verarbeitung in Ihrer Instanz um. Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Vulnerability Response-Schweregradzuordnungen erstellen in der Dokumentation Vulnerability Response.

Tenable.io-Asset-Import

Importierte Asset-Daten werden zuerst in die Tenable.io-Asset-Importtabelle [sn_vul_tenable_io_asset_import] geladen.

Die Tenable.io Asset Integration-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach Tenable.io Asset Transform.

In den folgenden Tabellen sind die Transformationszuordnungsfelder nach Integration geordnet.

Tenable.io-Asset-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Tenable bietet eine eindeutige ID für Assets und Zuordnungen zum erkannten Elementdatensatz und wird für die CI-Suche verwendet.
u_ipv4s	ip_address	Ordnet den ersten IP-Wert dem Feld ip_address im Datensatz des erkannten Elements zu.
u_mac_addresses	mac_address	Ordnet den ersten Wert von „mac_address“ dem MAC-Adressfeld im Datensatz des erkannten Elements zu.
u_fqdns	fqdn	Ordnet den ersten FQDN-Wert dem FQDN-Feld im Datensatz des erkannten Elements zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Asset-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_netBIOS_Names	NetBIOS	Ordnet den ersten NetBIOS-Wert dem NetBIOS-Feld im Datensatz des erkannten Elements zu.
u_operating_systems	os	Ordnet den ersten Betriebssystemwert dem Feld „BS“ im Datensatz des erkannten Elements zu.
(Vor v14.0 Vulnerability Response und v2.2 der Tenable Vulnerability-Integration)u_last_scan_time	last_scan_date	Zuordnung zum Feld „last_scan_date“ im Datensatz des erkannten Elements.
u_last_authenticated_scan_date	last_auth_scan_date	Zuordnung zum Feld „last_auth_scan_date“ im Datensatz des erkannten Elements.
[Skript]	name	Ordnet den Hostnamen mithilfe der Logik des Skripts zu.
u_tags		Die Tags werden in „sn_sec_cmn_host_tag“ gespeichert. Die Zuordnung von Tags zu Assets wird in „sn_sec_cmn_m2m_src_ci_tag“ gespeichert.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Timing und Zweck des Skripts für die Tenable.io-Asset-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Eine Funktion, die verwendet wird, um Werte auf dem Host zu aktualisieren und zu überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Importsatz. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration von Tenable.io-Plugins

Die Transformationszuordnung für Tenable.io-Plugins wird zum Transformieren von aus Tenable.io importierten Plugins verwendet.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Art und Weise, wie von den Tenable-Plugins empfangene Daten verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach dem Tenable.io-Plugin Transformieren.

Die Nutzlast der Plugins „tenable.io“ enthält alle Felder in der Spalte „u_attributes“ der Tabelle sn_vul_tenable_io_plugin_import. Das Feld „Attribute“ wird analysiert und den Datensätzen der Drittpartei-Eintragstabelle zugeordnet, wie in der folgenden Tabelle aufgeführt.

Quellenfeld	Zielfeld	Beschreibung
id	id	Ordnet die ID der Quelle zu und fügt ihr das Präfix TEN- hinzu. Wenn beispielsweise die empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.
Beschreibung	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Die Quelle für importierte TPE ist Tenable.io.
[Skript]	source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
Familie	Kategorie	Ordnet die Plugin-Familie der Kategoriespalte zu
plugin_modification_date	last_modified	Ordnet „plugin_modification_date“ dem zuletzt geänderten Feld zu.
plugin_publication_date	date_published	Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu.
has_patch	remediation_type	Ordnet den Korrekturtyp dem has_patch-Wert zu.
synopsis	Bedrohung	Ordnet die Bedrohungsinformationen für diese Schwachstelle zu.
cvss_base__score	Punktzahl	Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
solution	solution	Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
Exploit_available	Exploit	Ordnet den vom Scanner bereitgestellten Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu
vpr.Punktzahl	source_risk_score	Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu.
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch • 4 – 7 – Mittel • 0–4: Niedrig
vpr.drivers.age_of_vuln	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner der Spalte „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.exploit_code_maturity	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.product_coverage	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner den Bedrohungsquellen in der Drittparteitabelle zu.
vpr.drivers.threat_intensity_last28	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.
vpr.drivers.threat_recency	Threat_recency	Ordnet die Bedrohungsaktualitätsinformationen vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Ordnet die cvss3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
cvss_temperal_score	cvss_temperal_score	Ordnet die temporäre Punktzahl für CVSS v2 zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
cvss_v3_template_score	v3_zeitlich_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
risk_factor	source_severity	Entspricht dem Quellschweregrad in der Drittpartei-Eintragstabelle.
name	name	Ordnet den Namen des Plugins einem Namen in der Drittpartei-Eintragstabelle zu.
stig_severity	stig_severity	Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu.
plugin_type	check_type	Ordnet den Plugin-Typ „check_type“ in der Drittpartei-Eintragstabelle zu.
unsupported_by_vendor	unsupported_by_vendor	Ordnet das Feld „unsupported_by_vendor“ der Spalte „unsupported_by_vendor“ zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.

Zusätzlich zu den direkten Feldern werden Drittparteieinträgen weitere Informationen als zugehörige Listen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie unter „sn_vul_m2m_entry_cve“.
bid	Die Liste der Fehler-Traqs wird als Referenz hinzugefügt.
siehe_also	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Eine Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Drittanbietereintrag. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Die TenableIOPluginsImportProcessor-Skripteinbindung wird vom onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe der Tenable.io-Plugin-Integration und wandelt sie in Now Platform Schwachstelleneinträge von Drittparteien um. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.io-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

Tenable.io-Schwachstellenimport

Die Tenable.io-Transformationszuordnung für angreifbare Elemente wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus Tenable.io importiert wurden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Art und Weise, wie Daten aus dem Import von Tenable-Schwachstellen verarbeitet werden.

Die gleiche Transformationszuordnung wird für die Tenable.io-Integration für feste Schwachstellen und die Tenable.io-Integration für offene Schwachstellen verwendet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Transformationszuordnung für angreifbare Tenable.io-Elemente.

Quellenfeld	Zielfeld	Beschreibung
u_asset.uuid	id	Uuid wird dem ID-Feld des cmdb_ci-Datensatzes zugeordnet.
u_asset.ipv4	ip_address	Das Feld ipv4 wird dem IP-Adressfeld des cmdb_ci-Datensatzes zugeordnet.
u_asset .last_authenticated_results	last_auth_scan_date	Das Datum des letzten authentifizierten Scans wird dem Datum des letzten Authentifizierungsscans

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		des cmdb_ci-Datensatzes zugeordnet.
u_asset.mac_address	mac_address	Die MAC-Adresse wird dem Host-MAC-Adressfeld des Datensatzes „cmdb_ci“ zugeordnet.
u_asset.netBIOS_Name	NetBIOS	NetBIOS wird dem NetBIOS-Feld des cmdb_ci-Datensatzes zugeordnet.
u._plugin.cvss3_base_score	v3_base_score	Die CVSS v3-Basispunktzahl wird der v3-Basispunktzahl des Drittpartei-Eintragsdatensatzes zugeordnet.
u._plugin.cvss3_template_score	v3_zeitlich_Punktzahl	Die temporäre CVSS v3-Punktzahl wird der v3 Temporary-Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u._plugin.cvss_base_score	Punktzahl	Die CVSS-Basispunktzahl wird dem Punktzahlfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u._plugin.cvss_template_score	temporal_score	Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_plugin.description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_plugin.family	Kategorie	Ordnet die Plugin-Familie der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu.
u_plugin.modification_date	last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittparteieintrags zugeordnet.
u_plugin.publication_date	date_published	Das Veröffentlichungsdatum wird dem Feld „Veröffentlichungsdatum“ des Drittpartei-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Eintragsdatensatzes zugeordnet.
u_plugin.risk_factor	source_severity	Der Risikofaktor wird dem Feld „source_severity“ des Drittpartei-Eintragsdatensatzes zugeordnet.
u_plugin.solution	solution	Die Lösung wird dem Lösungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u_plugin.synopsis	Bedrohung	Die Synopse wird dem Bedrohungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u_severity_id	Priorität	Die Priorität wird der Schweregrad-ID aus der Nutzlast zugeordnet. Der Standardwert ist 5.
u_plugin.exploit_available	Exploit	Ordnet den vom Scanner bereitgestellten Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
vpr.Punktzahl	source_risk_score	Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu.
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch • 4 – 7 – Mittel • 0–4: Niedrig
u_plugin.vpr.drivers.age_of_vuln	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.exploit_code_maturity	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_plugin.vpr.drivers.product_coverage	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner Bedrohungsquellen in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.threat_intensity_last28	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.threat_recency	Threat_recency	Ordnet die Informationen zur Bedrohungsaktualität vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Ordnet die CVSS3 v3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
u_plugin.type	check_type	Ordnet den Plugin-Typ „check_type“ in der Drittpartei-Eintragstabelle zu.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Ordnet das Feld „unsupported_by_vendor“ im Plugin der Spalte „unsupported_by_vendor“ zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.
u_plugin.family_id	Family_id	Ordnet die Plugin-Familien-ID der Spalte „family_id“ in der Drittpartei-Eintragstabelle zu.
port	port	Der Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
protocol	protocol	Das Protokoll wird dem Protokollfeld des Datensatzes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		des angreifbaren Elements zugeordnet.
u_first_found	first_found	„Zuerst gefunden“ wird dem Feld „Zuerst gefunden“ des Datensatzes des angreifbaren Elements zugeordnet.
u_last_found	last_found	„Zuletzt gefunden“ wird dem Feld „Zuletzt gefunden“ des Datensatzes des angreifbaren Elements zugeordnet.
u_state	state	Der Status wird dem Feld „Status“ im Datensatz des angreifbaren Elements zugeordnet
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die Quelle der aus dieser Integration erstellten angreifbaren Elemente ist Tenable.io.
[Skript]	integration_instance	„integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_plugin.name	name	Ordnet den Namen des Plugins einem Namen in der Eintragstabelle einer Drittpartei zu.
u_plugin.stig_severity	stig_severity	Ordnet den STIG-Schweregrad des Plugins der Spalte „STIG-Schweregrad“ in der Drittpartei-Eintragstabelle zu

Zusätzlich zu den direkten Feldern werden Drittparteieinträgen weitere Informationen als zugehörige Listen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie unter „sn_vul_m2m_entry_cve“.
bid	Die Liste der Fehler-Traqs wird als Referenz hinzugefügt.
siehe_also	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation löst den TenableIOVulnerabilitiesProcessor aus, der Daten aus Tenable.io mithilfe des Importsatzes importiert und jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle der angreifbaren Elemente und die Schwachstellentabelle der Drittpartei lädt.Zur internen Verwendung. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Eine Funktion zum Überprüfen, ob der Drittpartei-Eintrag und die Erkennungen bereits vorhanden sind. Andernfalls werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Anzahl der CIs, VIs und Erkennungen zu aktualisieren, wie sie aus Tenable.io importiert wurden. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Tenable.sc-Asset-Import

Aus Tenable.sc importierte Asset-Daten werden zuerst in die Tabelle „Tenable.sc-Asset-Import“ (sn_vul_tenable_sc_asset_import) geladen. Die Transformationszuordnung Tenable.sc Asset Integration wird zum Transformieren der importierten Asset-Informationen verwendet. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach Tenable.sc Asset Transformieren.

Quellenfeld	Zielfeld	Beschreibung
u_uuid	id	uuid wird nicht von der Tenable-API ausgefüllt, daher wird das Attribut „u_uniqueness“ verwendet, um ein eindeutiges uuid-Feld für Assets zu erstellen und es dem cmdb_ci-Datensatz zuzuordnen.
u_ip	ip_address	Ordnet das IP-Feld aus der API dem Feld „ip_address“ in einem cmdb_ci-Datensatz zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_macaddress	mac_address	Ordnet das Feld „macaddress“ aus der API dem Adressfeld im Datensatz „cmdb_ci“ zu.
u_dnsname	fqdn	Ordnet das Feld „dnsname“ aus der API dem Feld „fqdn“ im Datensatz „cmdb_ci“ zu.
u_netBIOSName	NetBIOS	Ordnet das NetBIOS-Feld aus der API dem NetBIOS-Feld im cmdb_ci-Datensatz zu.
u_oscpe	os	Die BS-Informationen werden aus dem Attribut oscpe in der Nutzlast extrahiert und dem Feld os im Datensatz cmdb_ci zugeordnet.
u_lastauthrun	last_auth_scan_date	Ordnet das Feld „lastauthrrun“ aus der API dem Feld „last_auth_scan_date“ im Datensatz des erkannten Elements zu.
u_lastauthrun und u_lastunauthrun	last_scan_date	„lastauthrun“ wird aus der Tenable-API oder „lastunautrun“ extrahiert. Je nachdem, welcher Wert in der Nutzlast angezeigt wird, wird das Feld „last_scan_date“ im Datensatz des erkannten Elements gefüllt.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Funktion, die verwendet wird, um die Werte auf dem Host zu aktualisieren und zu überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Importsatz. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Import von Tenable.sc-Plugins

Aus Tenable.sc importierte Plugins-Daten werden zuerst in die Tabelle „Tenable.sc-Plugin-Import“ (sn_vul_tenable_sc_plugin_import) geladen. Die Tenable.sc-Plugin-Transformationszuordnung wird verwendet, um die importierten Plugin-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Plugin-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Tenable.sc-Plugin-Transformationszuordnung.

Quellenfeld	Zielfeld	Beschreibung
u_id	id	Ordnet die ID aus der Quelle zu und fügt das Präfix TEN- hinzu. Wenn beispielsweise die empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.
u_description	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Das aus dieser Integration importierte TPE hat Tenable.sc als Quelle.
[Skript]	source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
u_family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte zu.
u_plugin_modification_date	last_modified	Ordnet „plugin_modification_date“ dem zuletzt geänderten Feld zu.
u_plugin_publication_date	date_published	Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu.
u_has_patch	remediation_type	Ordnet den Korrekturtyp dem has_patch-Wert zu.
u_synotisi	Bedrohung	Ordnet die Bedrohungsinformationen für diese Schwachstelle zu.
u_cvss_base_score	Punktzahl	Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
u_solution	solution	Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu.
u_cvss_temperal_score	cvss_temperal_score	Ordnet die temporäre Punktzahl für CVSS v2 zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_cvss_v3_template_score	v3_zeitlich_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
u_risk_factor	Quellenschweregrad	Entspricht dem Quellschweregrad in der Drittpartei-Eintragstabelle.
u_cvss_v3_base_score	v3_base_score	Ordnet die CVSS-Basispunktzahl in der Drittpartei-Eintragstabelle zu.
u_exploit_available	Exploit	Ordnet das vom Scanner bereitgestellte ExploitAvailable der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
u_vpr_score	source_risk_score	Ordnet die VPR-Punktzahl vom Scanner der Quellrisiko-Punktzahl in der Drittpartei-Eintragstabelle zu.
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch • 4 – 7 – Mittel • 0–4: Niedrig
u_vpr_context[id=age_of_vuln]	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=exploit_code_maturity]	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=product_coverage]	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_sources_last_28”]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner zu „bedrohten Quellen“ in der Drittparteitabelle zu.
u_vpr_context[id=”threat_intensity_last_28”]	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_recency”]	Threat_recency	Ordnet die Informationen zur Bedrohungsaktualität vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Ordnet die CVSS v3-Auswirkungspunktzahl vom Scanner zu „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
u_name	name	Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu.
u_stig_severity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Eintragstabelle der Drittpartei zu.
u_check_type	check_type	Ordnet den Schecktyp „check_type“ in der Drittpartei-Eintragstabelle zu.
u_family.id	family_id	Ordnet das Plugin „family_id“ dem Plugin „family_id“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.

Zusätzlich zu den direkten Feldern werden Drittparteieinträgen weitere Informationen als zugehörige Listen hinzugefügt.

Quellenfeld	Beschreibung
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_see_also	Die Liste der URLs wird als Referenz hinzugefügt.
u_exploit_frameworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	in einem Drittanbietereintrag. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von erstellten und ignorierten Plugins festzulegen. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Die TenableSCPluginsImportProcessor-Skripteinbindung wird vom onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe aus der Tenable.sc-Plugin-Integration und wandelt sie in ServiceNow-Schwachstelleneinträge von Drittparteien um. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.sc-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

Import von Tenable.sc-Schwachstellen

Die Transformationszuordnung Tenable.sc Open Vulnerabilities wird zum Transformieren importierter Daten aus der Tenable.sc-Integration für offene Schwachstellen verwendet, und die Transformationszuordnung Tenable.sc und behobene Schwachstellen wird zum Transformieren importierter Daten aus der Tenable.sc-Integration für feste Schwachstellen verwendet.

Hinweis:
Änderungen an diesen Transformationszuordnungen ändern die Art und Weise, wie Daten aus dem Import fester/offener Tenable-Schwachstellen verarbeitet werden.

Um auf die Transformationszuordnungen für offene und feste Schwachstellen von Tenable.sc zuzugreifen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationsinstanzen** > **Integration fester/offener Tenable.sc-Schwachstellen** > **Datenquellen** > **Offene/behobene Schwachstellen in Tenable.sc** > **Transformiert**.

Quellenfeld	Zielfeld	Beschreibung
u_pluginID	ID	Wird als Bezeichner für das Plugin verwendet. Dieses Feld ist der Plugin-ID im Datensatz des Drittparteieintrags zugeordnet.
u_riskfactor	source_severity	Dieses Feld ist „source_severity“ im Drittpartei-Eintragsdatensatz zugeordnet.
u_severity	Priorität	Das Prioritätsfeld ist dem Schweregrad zugeordnet. Der Standardwert ist 5.
u_hasbeenmitigated	state	Wurde dem Statusfeld des Schwachstellen-Datensatzes zugeordnet. Bei der Integration mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		behobenen Schwachstellen befinden sich alle AEs im Status „Geschlossen“.
u_ip	ip_address	Die IP-Adresse wird dem Host-IP-Feld der Tabelle „cmdb_ci“ zugeordnet.
u_port	port	Der Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_protocol	protocol	Das Protokoll wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_firstSeen	first_found	Der erste erkannte Wert wird dem ersten gefundenen Feld des VI-Datensatzes zugeordnet.
u_lastSeen	last_found	Der zuletzt erkannte Wert wird dem zuletzt gefundenen Feld des VI-Datensatzes zugeordnet.
u_exploitVerfügbar	Exploit	ExploitAvailable wird dem Exploit-Feld im Drittpartei-Eintragsdatensatz zugeordnet.
u_synotisi	Bedrohung	Die Synopse wird dem Bedrohungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_solution	solution	Die Lösung wird dem Lösungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_basescore	Punktzahl	BaseScore wird dem Punktzahlfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_temperalPunktzahl	temporal_score	Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Eintragsdatensatz zugeordnet.
u_cvssv3basescore	v3_base_score	Cvssv3basescore wird der v3-Basispunktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_cvsstemperalScore	v3_zeitlich_Punktzahl	Die Cvssv3-Punktzahl wird der temporären v3-Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_pluginpubdate	date_published	Das Plugin-Veröffentlichungsdatum wird dem Plugin-Veröffentlichungsdatum im Drittpartei-Eintragsdatensatz zugeordnet.
u_pluginmoddate	last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittparteieintrags zugeordnet.
u_dnsname	fqdn	DnsName wird dem FQDN-Feld des cmdb_ci-Datensatzes zugeordnet.
u_macaddress	mac_address	„MacAddress“ wird dem Feld „mac_address“ des Datensatzes „cmdb_ci“ zugeordnet.
u_netBIOSName	NetBIOS	NetBIOSName wird dem NETBIOS-Feld des cmdb_ci-Datensatzes zugeordnet.
u_ip	ip	IP wird dem IP-Feld des cmdb_ci-Datensatzes zugeordnet.
hostUniqueness	uuid	Die Eindeutigkeit des Hosts wird keinem Feld zugeordnet, sondern wird verwendet, um uuid für den Host zu bestimmen.
u_family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_plugintext	Nachweis	Plugin-Text wird dem Nachweis im TPE-Datensatz zugeordnet.
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die Quelle der angreifbaren Elemente, die aus dieser Integration erstellt werden, ist Tenable.sc.
[Skript]	integration_instance	„integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_vpr_score	source_risk_score	Ordnet die VPR-Punktzahl vom Scanner der Quellrisiko-Punktzahl in der Drittpartei-Eintragstabelle zu.
[Skript]	source_risk_rating	Ordnet die VPR-Punktzahl basierend auf den Punktzahlbereichen der Standardrisikoeinstufung zu: • 9 - 10: Kritisch • 7 – 9 – Hoch • 4 – 7 – Mittel • 0–4: Niedrig
u_vpr_context[id=age_of_vuln]	Alter_von_Schwachstelle	Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=exploit_code_maturity]	Exploit_code_maturity	Ordnet die Reife des Exploit-Codes vom Scanner zu „exploit_code_maturity“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=product_coverage]	product_coverage	Ordnet die Produktabdeckung vom Scanner zu „product_coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_sources_last_28]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Bedrohungsquellen in der Drittparteitabelle zu.
u_vpr_context[id=”threat_intensity_last_28]	Threat_Intensity	Ordnet die Bedrohungsstärke vom Scanner in den letzten 28 Tagen der Bedrohungsstärke in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=”threat_recency”]	Threat_recency	Ordnet die Informationen zur Bedrohungsaktualität vom Scanner „thread_recency“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Ordnet die CVSS v3-Auswirkungspunktzahl vom Scanner zu „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu.
u_pluginname	name	Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu.
u_stigseverity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Eintragstabelle der Drittpartei zu.
u_checktype	check_type	Ordnet den Schecktyp „check_type“ in der Drittpartei-Eintragstabelle zu.
u_family.id	family_id	Ordnet das Plugin „family.id“ dem Plugin „family_id“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_attack_vector	Die Spalte „exploit_attack_vector“ in der Tabelle „ third_party_entry“ wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
u_cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie unter sn_vul_m2m_entry_cve.
u_bieten	Die Liste der Fehler-Traqs wird als Referenz hinzugefügt.
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_seealso	Die Liste der URLs wird als Referenz hinzugefügt.
u_xrefs	Die Liste der X-REFs wird als Referenz hinzugefügt.
u_exploitframeworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle ist aufgeführt, wann die einzelnen Skripts ausgeführt werden und welchen Zweck sie haben.

Wenn das Skript ausgeführt wird	Zweck
onStart (wenn ein Importsatz die Transformation gestartet hat)	Diese Transformation wird verwendet, um die Werte in „import_set“ für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onBefore (bevor ein Importsatz die Transformation abgeschlossen hat)	Funktion, die verwendet wird, um die Werte in der Schwachstelle zu aktualisieren und zu überprüfen, ob die Schwachstelle bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einer Tabelle angreifbarer Elemente. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.
onComplete (wenn ein Importsatz die Transformation abgeschlossen hat)	Diese Transformation wird verwendet, um die Werte von neu erstellten VIs und von VIs, die aktualisiert und ignoriert wurden, festzulegen. Für den internen Gebrauch. Das Ändern oder Löschen von wird nicht empfohlen.

Legen Sie zusätzliche Filterparameter für Tenable.io -Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Tenable Vulnerability Integration an, um die mit dem Produkt Tenable.io importierten Schwachstellendaten weiter zu verfeinern.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, um nur bestimmte Schwachstellendetails überprüfen zu können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach `cidr_range`, `num_assets`, `indexed_at`und `plugin_family`gefiltert werden. Oder Sie möchten eine Tenable.io -Integration so ausführen, dass eine Ausführung alle vier Stunden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nur kritische Schwachstellen importiert und eine andere alle 24 Stunden ausführt, um alle anderen nicht kritischen Schwachstellen abzurufen.

Um diese Daten beim Sammeln dieser Daten zu unterstützen, können Sie von Tenable unterstützte Parameter hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Mit dieser Funktion können Sie Ihre HTTP-Anforderungsinformationen mit Tenable-Parametern in Now Platformanpassen, ohne zusätzliche API-Aufrufe oder Codierung hinzuzufügen. Die folgenden Tenable.io Integrationen unterstützen die Filterung durch Bereitstellung von JSON-Inhalten im Anforderungstext:

- Assets Integration
- Integration behobener Schwachstellen
- Integration offener Schwachstellen

Sie sollten wissen, wie JSON -Zeichenfolgen für diese Funktion verwendet werden.

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Suchen Sie die vom Produkt Tenable.io unterstützten Parameter auf der Entwickler-Site, die Sie für die Filterung verwenden möchten.

   Parameter und Werte, die Sie aus dem Produkt Tenable.io eingeben, werden nur auf Ebene der Integrationsinstanz unterstützt.

2. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
3. Klicken Sie auf der Listenseite „Tenable Integrations“ (Tenable-Integrationen) auf den Datensatz für die Integration Tenable.io, die Sie öffnen möchten.
4. Klicken Sie bei ausgewählter Registerkarte Tenable-REST-Methoden auf das Informationssymbol (I) für die REST-Methode und anschließend auf **Datensatz öffnen**.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Um den Datensatz zu bearbeiten, klicken Sie oben auf der Seite auf den Link in. Um den Datensatz zu bearbeiten, klicken Sie **hier**.
7. Geben Sie im Datensatz REST-Methode im Feld Inhalt den JSON-Inhalt ein, der Teil des Anforderungstexts sein soll.

   Beispielsweise können Sie den Schweregradparameter für importierte Schwachstellen für die Tenable.io Assets-Integration auf `{"filters": {"severity": ["critical"]}}` festlegen, damit nur kritische Schwachstellen importiert werden (CVSS-Punktzahl 10,0).

   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Tenable.io weitere Informationen zum Trennen der einzelnen Werte.

8. Klicken Sie auf **Aktualisieren**.

Berichterstellung für Tenable Vulnerability Integration

Zeigen Sie Berichte über Schwachstellen und angreifbare Elemente in den Dashboards Vulnerability Response an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen in den -Arbeitsbereichen Vulnerability Response .

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad aktiver Schwachstellen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen anzeigen, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.

Vorherige Versionen von Vulnerability Response

Das Übersichts-Dashboard für Vulnerability Response (Schwachstellenmanagement) bietet eine Ausführungsansicht für Schwachstellen und angreifbare Elemente, damit der Schwachstellenadministrator Problembereiche schnell erkennen kann. Das Vulnerability Response-Nachbesserungsdashboard (Nachbesserung von Schwachstellen) ermöglicht Nachbesserungsspezialisten, sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren, für die sie verantwortlich sind.

Weitere Informationen finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..

Erforderliche Rolle: Korrekturbesitzer.

Persona-Rollen und granulare Rollen sind verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Um das Dashboard anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Korrekturübersicht**.

Statusdiagramm der Integrationsausführung für die Tenable-Schwachstellen-Integration

Das Modul „Tenable Integration Run Status“ (Status der Tenable-Integrationsausführung) bietet Ihnen eine grafische Ansicht des Status der Tenable-Integrationsausführungen.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein Teil des Balkendiagramms klicken, wird eine Liste mit detaillierteren Informationen geöffnet.

Erforderliche Rolle: Schwachstellen-Administrator

Persona-Rollen und granulare Rollen sind verfügbar, mit denen Sie verwalten können, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten von granularen Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

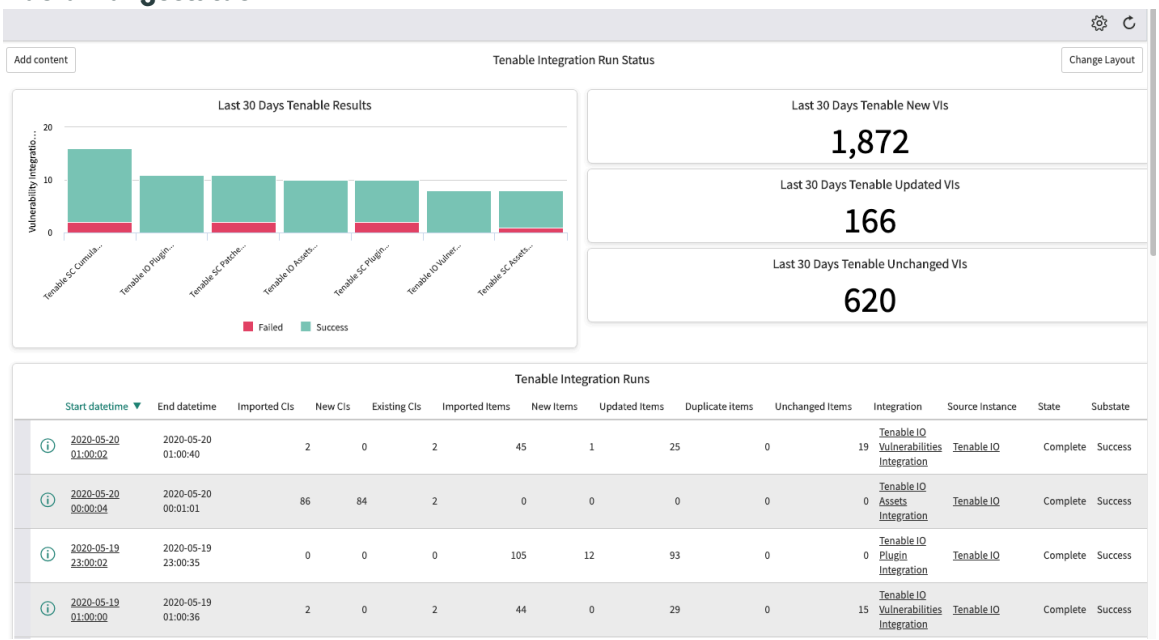
Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Status der Integrationsausführung**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Ausführungsstatus



Diagrammberichte zum Status der Tenable-Integrationsausführung

Name	Beschreibung
Tenable-Ergebnisse der letzten 30 Tage	Die Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Jede Ausführung wird als Balken im Diagramm angezeigt.
Neue Tenable-VIs der letzten 30 Tage	Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Aktualisierte Tenable-VIs der letzten 30 Tage	Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Unveränderte Tenable-VIs der letzten 30 Tage	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Als Ganzzahl angezeigt.
Tenable-Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste.

Automatische Übersetzung

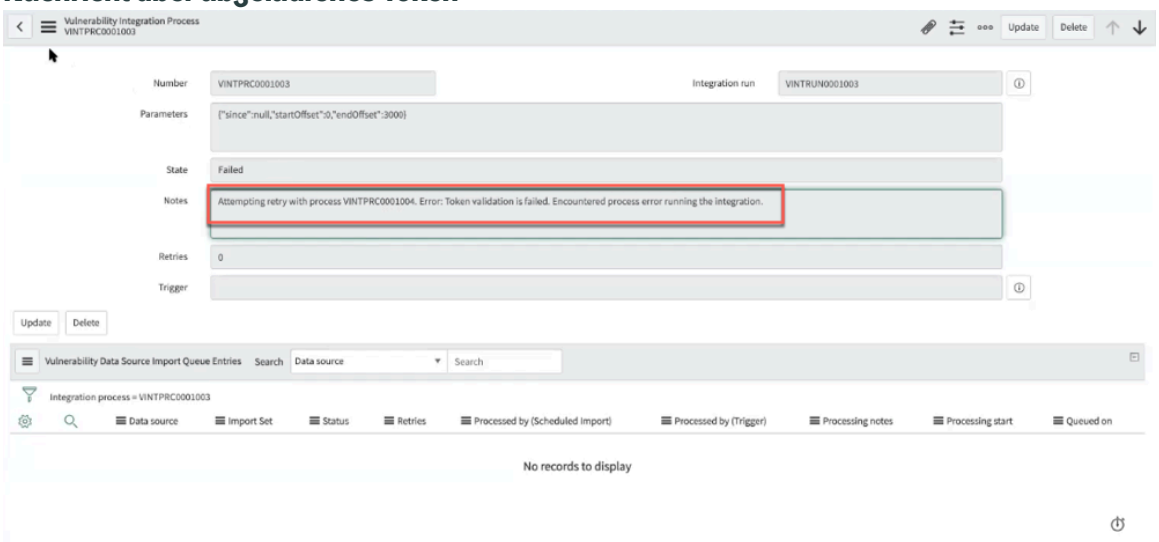
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: **V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle *sn_vul_detection*. Während die Integration ausgeführt wird, ändert sich möglicherweise die Anzahl der Erkennungen oder Ergebnisse. In diesem Bericht wird die Anzahl der Erkennungen in der Spalte „Anzahl bis Datum“ in der Instanz nach Abschluss der Integrationsausführung angezeigt.

Ablauf der Tokenvalidierung

Wenn eine Tenable.sc-Integrationsausführung aus irgendeinem Grund fehlschlägt, läuft das Authentifizierungstoken für Tenable.sc automatisch ab, und im Datensatz des Vulnerability-Integrationsprozesses wird eine Meldung angezeigt.

Nachricht über abgelaufenes Token



Für den nächsten Integrationsprozess wird automatisch ein neues Token generiert. Alle Integrationsprozesse – fehlgeschlagen und erfolgreich – werden auf der Registerkarte Vulnerability Integration Process (Schwachstellenintegrationsprozess) im Datensatz „Schwachstellenintegrationsprozess“ angezeigt.

Initiieren Sie den erneuten Scan für die Tenable.sc -Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie erneut Scans auf der Tenable-Plattform initiieren. Sie können bei Bedarf von Ihrer Instanz Now Platform® aus einen erneuten Scan auf angreifbare Elemente für das Produkt Tenable.sc initiieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.write_all oder sn_vul.write_assigned

Hinweis:

Tenable.sc bietet keine Unterstützung für das erneute Scannen auf Agent-basierten Computern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum erneuten Scannen über -Arbeitsbereiche finden Sie unter Scannen Sie die angreifbaren Elemente Tenable.io und Tenable.sc aus den Arbeitsbereichen Vulnerability Response erneut.

Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Um den Aufwand und das Volumen zu reduzieren, die mit geplanten, vollständigen Scans verbunden sind, können Nachbesserungsbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen für Assets (Konfigurationselemente) in ihren Umgebungen initiieren. Sie können erneute Scans von angreifbaren Elementen (VIs), Korrekturaufgaben (RTs), Drittparteieinträgen (TPE) oder von Datensätzen erkannter Elemente in Ihrer Instanz Now Platform initiieren.

Durch erneute Scans können Ihre für die Korrektur Verantwortlichen und Schwachstellenanalysten überprüfen, ob Ihre Korrekturaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben haben.

Beispielsweise wird Ihre gesamte Umgebung alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Now Platform für angreifbare Elemente vom Typ Tenable.sc initiieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.sc Integration für Scan-Anmeldeinformationen importiert und aktualisiert die Scanner-Anmeldeinformationen aus dem Produkt Tenable.sc in Ihrer -Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationen zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten. Die ServiceNow® Tenable.sc Integration zum Scannen von Anmeldeinformationen wird automatisch über den Setup-Assistenten in Ihrer Instanz aktiviert (Aktiv), wenn Sie die Integrationen für Tenable.sc Schwachstellen (Tenable.sc Integrationen offener und fester Schwachstellen) konfigurieren.

Beachten Sie die folgenden Informationen zu den Anmeldeinformationen, die Sie importieren, damit Ihre Benutzer sie bei Bedarf aus Ihrer Instanz Now Platform anzeigen können:

- Mit der -Administrator-Anwenderrolle Tenable.sc erstellte Anmeldeinformationen sind für Anwender in allen Ihren Organisationen verfügbar.
- Mit der Organisationsbenutzerrolle Tenable.sc erstellte Anmeldeinformationen sind nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in den Now Platform importiert, es sei denn, sie werden für den Account des Benutzers freigegeben, der für die Verbindung mit der Instanz verwendet wird.

Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.sc.

Weitere Informationen zum Konfigurieren der Anwendung Tenable.sc finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten. Um weitere Informationen zur Integration der Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Integrationen** > **Integration von Tenable.sc-Scan-Anmeldeinformationen**.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, von dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Sie können erneute Scans nur für VIs mit Tenable.sc als Quelle initiieren. Überprüfen Sie, ob Tenable.sc in der Spalte **„Quelle“** in den VI-Listenansichten oder in den Feldern **„Quelle“** in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol **Liste personalisieren** (Zahnradsymbol), und verwenden Sie den Slushbucket, um **die Quelle** von **Verfügbar** in **Ausgewählt**zu verschieben.

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Korrekturaufgabe bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die Schaltfläche **Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem Produkt Tenable.sc stammen und sich in einem anderen Status als **Geschlossen befinden**. Bei mehreren VI-Datensätzen müssen alle VIs aus dem Tenable.sc-Produkt stammen und sich in einem anderen Status als **Geschlossen befinden**.
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem beliebigen anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Tenable.sc stammen.
   - In einem TPE-Datensatz (Drittparteieintrag) muss der Datensatz über mindestens einen zugeordneten VI-Datensatz aus dem Produkt Tenable.sc in einem anderen Status als **Geschlossen**verfügen.

4. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.
   Sie werden aufgefordert, die Scanner-Anmeldeinformationen für den Zugriff auf den Scanner auszuwählen. Dies sind die Anmeldeinformationen, die von der Tenable.sc Integration mit Scan-Anmeldeinformationen importiert werden.
5. Wählen Sie im Dialogfeld die gewünschten Filter und Anmeldeinformationstypen aus.
6. Klicken Sie auf **Scan anfordern**.

   Es wird eine Nachricht angezeigt, die anzeigt, dass Ihre Prüfung verarbeitet wird. Der Status für alle erneut gescannten Elemente kann jederzeit unter den zugehörigen Scan-Listen in den VI-, RT- und TPE-Datensätzen gefunden werden, mit denen Sie die erneut gescannten Elemente gestartet haben. Klicken Sie in der Nachricht **auf Details anzeigen**,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um den Status des erneuten Scans und alle anderen von einem bestimmten Datensatz gestarteten erneuten Scans anzuzeigen.

Das Feld „Status“ im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt). Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde. Alle AEs, die in den Status „ **Geschlossen“/„Behoben“** übergegangen sind oder werden, werden mit dem nächsten geplanten Import der Tenable.sc-Integration für feste Schwachstellen importiert.

Initiieren Sie den erneuten Scan für die Tenable.io -Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie erneut Scans auf der Tenable-Plattform initiieren. Sie können bei Bedarf von Ihrer Instanz Now Platform® aus einen erneuten Scan auf angreifbare Elemente für das Produkt Tenable.io initiieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.write_all oder sn_vul.write_assigned

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

Warum und wann dieser Vorgang ausgeführt wird

- Siehe und Scannen Sie Datensätze und Korrekturaufgaben im erneut Vulnerability Manager Workspace und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace, um in den Vulnerability Response-Arbeitsbereichen einen erneuten Scan zu initiieren.
- Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Hinweis:
Tenable.io bietet keine Unterstützung für das erneute Scannen auf Agent-basierten Computern.

Um den Aufwand und das Volumen geplanter, vollständiger Scans zu reduzieren, können Sie als Besitzer der Remediation, IT-Spezialist, Schwachstellenanalyst oder Schwachstellenmanager bei Bedarf gezielte erneute Scans initiieren. können Sie Assets (Konfigurationselemente) in Ihren Umgebungen auf bestimmte Schwachstellen scannen. Sie können erneute Scans aus Datensätzen von angreifbaren Elementen (VI), Korrekturaufgaben (VUL), Drittparteieinträgen (TPE) oder erkannten Elementen (SDI) in der Instanz Now Platform initiieren. Durch erneute Scans können Sie überprüfen, ob durch Ihre Nachbesserungsaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.io Integration für Scan-Anmeldeinformationen importiert und aktualisiert die Scanner-Anmeldeinformationen aus dem Produkt Tenable.io in Ihrer -Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationen zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten.

Im Folgenden werden die Anmeldeinformationen beschrieben, die Sie importieren, damit Ihre Benutzer sie je nach Bedarf aus Ihrer Instanz Now Platform sehen können:

- Mit der -Administrator-Anwenderrolle Tenable.io erstellte Anmeldeinformationen sind für Anwender in allen Ihren Organisationen verfügbar.
- Mit der Organisationsbenutzerrolle Tenable.io erstellte Anmeldeinformationen sind nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in den Now Platform importiert, es sei denn, sie werden für den Account des Benutzers freigegeben, der für die Verbindung mit der Instanz verwendet wird.

  Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.io.

- Die Tenable.io Template Integration und die Tenable.io Scan Credential Integration müssen aktiviert werden, bevor erneute Scans initiiert werden können. Um weitere Informationen zur Integration der Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationen** > **Integration von Tenable.io Scan-Anmeldeinformationen**.

  Standardmäßig sind die Integrationen für Vorlagen- und Scan-Anmeldeinformationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für Tenable.ioeingeben, werden alle Tenable.io Integrationen automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

  1. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
  2. Suchen Sie in der angezeigten Liste nach den Tenable.io Integrationsdatensätzen, die Sie benötigen.
  3. Öffnen Sie jeden Datensatz, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren.
  4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
  5. Kehren Sie zum Setup-Assistenten zurück, um mit der Konfiguration für Tenable Vulnerability Integration mit Vulnerability Responsefortzufahren.

Weitere Informationen zum Konfigurieren der Produkte Tenable.io und Tenable.sc finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten.

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Now Platform für angreifbare Elemente vom Typ Tenable.io initiieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration behobener Schwachstellen initiiert haben.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Integrations-Timeout-Fehler führt. Die Integration verarbeitet die Daten weiterhin, auch wenn der Zeitüberschreitungsfehler aufgetreten ist. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzuzeigen, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **„Letzter verarbeiteter Datensatz“** auf der Seite „Importwarteschlangeneintrag“ wird basierend auf der Anzahl der Datensätze aktualisiert, die von der Importwarteschlange erstellt oder aktualisiert werden. Falls ein Importwarteschlangeneintrag die Zeitbegrenzung von einer Stunde überschreitet, prüft das System im Feld **Letzter verarbeiteter Datensatz**, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt und eine Zeitüberschreitung aufweist, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Hinweis:
Das Feld **„Letzter verarbeiteter Datensatz“** wird basierend auf den Einstellungen in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der das Zeitlimit für den Importwarteschlangeneintrag überschritten werden muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, von dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Wenn Sie den Scanner Tenable.io verwenden, können Sie erneute Scans für VIs nur mit Tenable.io als Quelle initiieren. Überprüfen Sie, ob Tenable.io in der Spalte **„Quelle“** in den VI-Listenansichten oder in den Feldern **„Quelle“** in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol **Liste personalisieren** (Zahnradsymbol), und verwenden Sie den Slushbucket, um **die Quelle** von **Verfügbar** in **Ausgewählt**zu verschieben.

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Datensätze, die Sie für den erneuten Scan verwenden möchten.

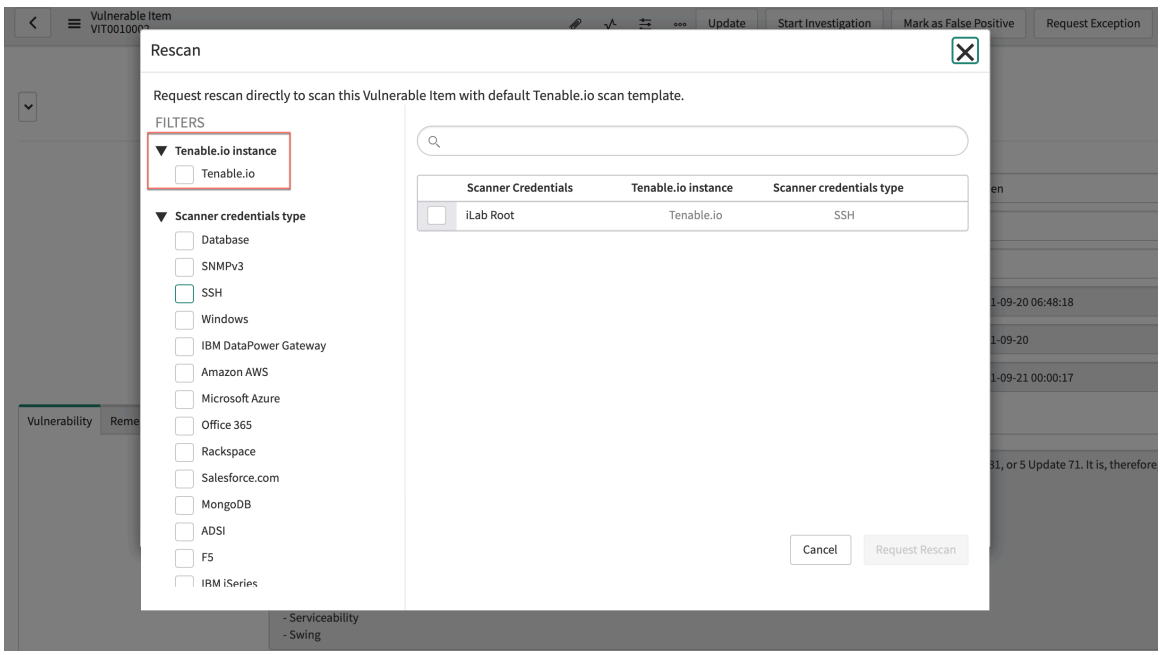
   Abhängig von Ihrer Auswahl ist die Schaltfläche **Erneut scannen** für die folgenden Datensätze verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In einem einzelnen VI-Datensatz muss sich das VI in einem anderen Status als **„Geschlossen“**befinden. Bei mehreren VI-Datensätzen müssen alle VIs aus dem Produkt Tenable.io stammen und sich in einem anderen Status als **Geschlossen befinden**.
- Für Korrekturaufgaben-Datensätze werden nur Korrekturaufgaben in einem anderen Status als **„Geschlossen“** unterstützt. Alle zugeordneten VIs müssen sich in einem anderen Status als **„Geschlossen“** befinden und Tenable.io als Quelle verwenden.
- In einem TPE-Datensatz (Drittparteieintrag) muss der Datensatz über mindestens einen zugeordneten VI-Datensatz aus dem Produkt Tenable.io in einem anderen Status als **Geschlossen**verfügen.
- Bei Datensätzen erkannter Elemente muss dem Datensatz mindestens ein VI-Datensatz aus dem Produkt Tenable.io in einem anderen Status als **„Geschlossen“**zugeordnet sein.
- In der Liste „Angreifbare Elemente“ können Sie einzelne angreifbare Elemente auswählen, die Sie erneut scannen möchten. Verwenden Sie das Menü Aktionen für ausgewählte Zeilen unten links im Bildschirm, um den erneuten Scan zu starten. Sie werden aufgefordert, Ihre Anmeldeinformationen einzugeben.

4. Klicken Sie oben rechts in einem Datensatz **auf Erneut scannen**.
   Sie werden aufgefordert, die Instanz(en) für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind diejenigen, die von der Tenable.io Integration zum Scannen von Anmeldeinformationen importiert wurden.
5. Wählen Sie im Dialogfeld die Instanz und/oder Instanzen und die Anmeldeinformationstypen aus, die Sie verwenden möchten.

   In der folgenden Abbildung ist eine Integrationsinstanz, Tenable.io, zu sehen. Wenn Sie mehr als eine Instanz Tenable.io haben, werden sie alle im Abschnitt „Tenable.io“ im Formular angezeigt.



6. Klicken Sie auf **Erneutes Scannen anfordern**.

   Es wird eine Nachricht angezeigt, die anzeigt, dass Ihr Scan verarbeitet wird und ein übergeordneter Scan-Datensatz erstellt wird. Der Status für alle untergeordneten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, Korrekturaufgaben-, TPE- und SDI-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht **auf Details anzeigen**, um den Status des erneuten Scans und alle anderen von einem bestimmten Datensatz gestarteten erneuten Scans anzuzeigen.

Das Feld „Status“ im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Jeder Scan unterstützt eine eindeutige Kombination aus Integrationsinstanz, TPE, IP und Netzwerk-ID. Möglicherweise werden in einem übergeordneten Scan-Datensatz mehrere untergeordnete Scans angezeigt. Beispiel: Die maximale Anzahl von IP-Adressen, die ein untergeordneter Scan unterstützen kann, beträgt 1000. Wenn für ein angreifbares Element 1002 IPs vorhanden sind, werden zwei untergeordnete Scans erstellt und in der zugehörigen Liste „Scans“ aufgeführt, um die Anforderung zu unterstützen. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans, und sein Status spiegelt den Status der untergeordneten Scans wider.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt). Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde. Alle AEs, die in **den Status „Geschlossen“/ „Behoben“** überführt wurden oder werden, werden mit dem nächsten geplanten Import der Tenable.io Integration behobener Schwachstellen importiert.

Bei Scans, bei denen ein Fehler auftritt, können Sie die untergeordneten Scans im übergeordneten Scan-Datensatz überprüfen. Zeigen Sie den Fehler in der Antwortnutzlast des untergeordneten Scans an.

Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration behobener Schwachstellen initiiert haben.

Aktualisieren Sie Configuration Items mit dem Netzwerkpartitionsbezeichner für Tenable Vulnerability Integration

Erstellen Sie eindeutige Configuration Items (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um weitere Details zu Ihren Schwachstellen zu erhalten.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig können Sie Ihre Assets in der Anwendung Vulnerability Response anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch in Ihrer CMDB als ein CI gespeichert.

Wie in den folgenden Tabellen gezeigt, können beispielsweise mehrere Assets (CI) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, verfügen jedoch über eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche in der Regel als einzelnes CI (CI 1) identifiziert und gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßige IP-Suche und CI-Erstellung

Quelle	IP-Adresse	Network_id	Konfigurationselement
Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	Repository-ID	Konfigurationselement
Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse aufweisen, um sie als unterschiedliche Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die geplante Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzu. Von der IRE erstellte vorhandene CIs werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Wenn Sie ein Upgrade ab v14.0 von Vulnerability Response und v2.2 der Tenable-Schwachstellenintegration durchführen, werden die CMDB-CI-Klassenmodelle (1.0.21.) unterstützt. Die -Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

Option	Beschreibung
Geplante Aufgaben bei Bedarf ausführen.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Tenable-Daten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartitionsbezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.
Warten Sie mit den nächsten geplanten Aufgaben auf Importe neuer Daten aus den Integrationen.	Erstellen Sie CIs für jedes neue Asset unter Verwendung des Netzwerkpartitionsbezeichners, beginnend mit der nächsten geplanten Aufgabe. CI,

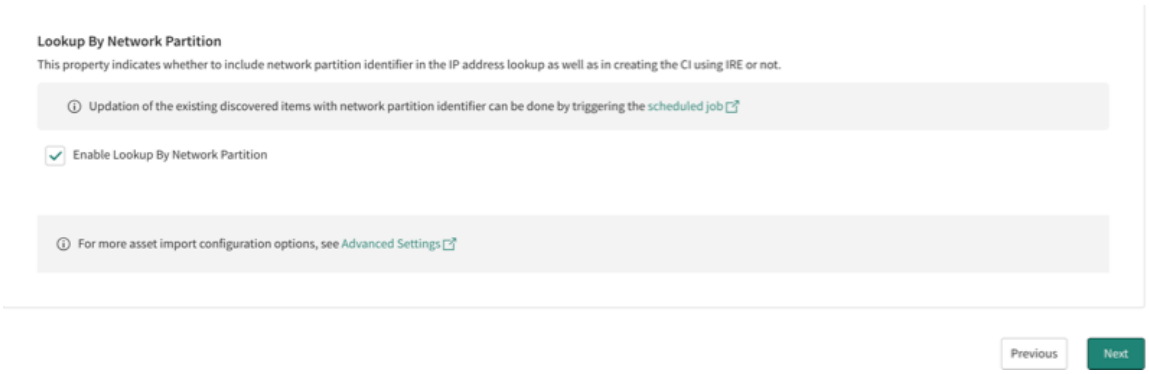
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Option	Beschreibung
	angreifbares Element und Erkennungsdatensätze werden mit der neuen Granularität aktualisiert. Neue CIs werden erstellt, wenn keine exakte Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Tenable.io integrations oder Tenable.sc integrations (Integrationen) aus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Auswahlvorgang **Konfiguration des Asset-Imports**.
5. Auswahlvorgang **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen aus **Suche nach Netzwerkpartition aktivieren** Abschnitt.



6. Klicken Sie auf **Next (Weiter)**.

Die Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY _ID sind enthalten und aktualisieren vorhandene CIs oder erstellen CIs mit der nächsten geplanten Aufgabe.

Bezeichnerattribut der Netzwerkpartition, das in die IP-Suche und CI-Erstellung einbezogen wird

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI2

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartitions	CIs-Assets mit Netzwerkpartitions
Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI2

Mit der nächsten geplanten Aufgabe fügen die Suchregeln für IP-Adresse und unvollständige IP-Adressen-CI-Identifizierung das Attribut für den Netzwerkpartitionsbezeichner für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc automatisch hinzu.

Nachdem Sie die Systemeigenschaft aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie die geplanten Aufgaben bei Bedarf starten.

Importieren Sie Änderungen für die Tenable Vulnerability-Integration

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Importintegration für Tenable-Schwachstellen in der Tenable-Schwachstellen-Integration ServiceNow®.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Gruppe von Aufgaben erfordert Programmierkenntnisse und fortgeschrittene Kenntnisse über Now Platform.

Führen Sie diese Schritte aus, um domänengetrennte Importe für die Tenable Vulnerabilities-Integrationen zu erstellen. Das folgende Beispiel bezieht sich auf die Integration „Tenable.io Open Vulnerabilities“, der Inhalt gilt jedoch auch für die anderen Tenable-Integrationen.

Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede von Ihnen erstellte Domäne einen Anwender, und weisen Sie ihn dieser Domäne zu.

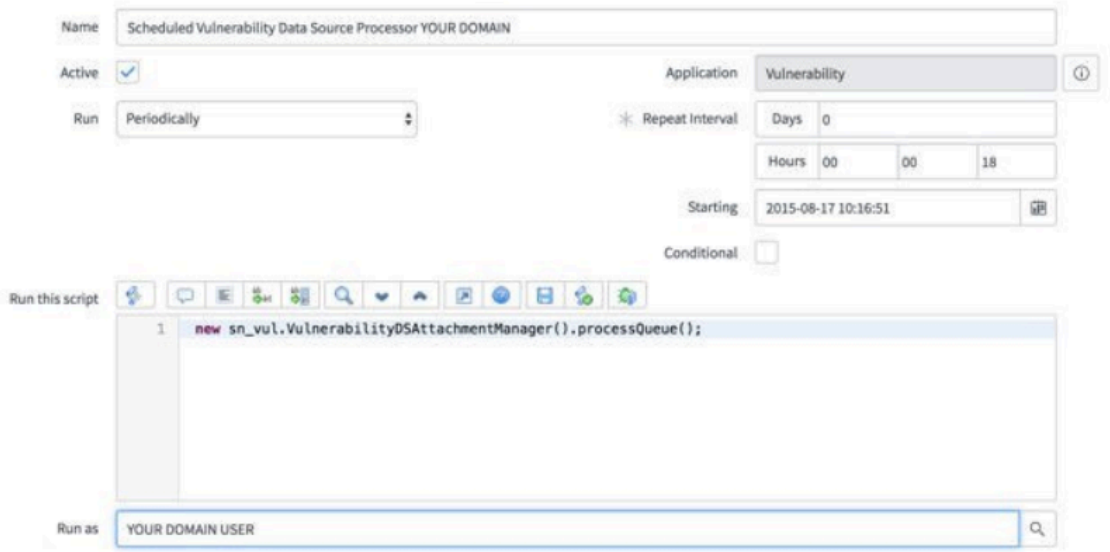
   Stellen Sie sich diesen Benutzer als run_as-Platzhalter für die Domäne in Tenable.io vor.
3. Integration offener Schwachstellen.
   Der -Benutzer entspricht dem VR.System-Benutzer in der globalen Domäne und muss die folgenden Rollen aufweisen: sn_vul.tenable_configure_integration, import_admin und sn_vul.vulnerability_write. Dieser Anwender benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   Hinweis:
   Betrachten Sie diesen Anwender als spezifisch für diese Rolle. Der Anwender darf keinen anderen Zweck haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie in jeder Domäne eine geplante Aufgabe, indem Sie den Prozessor für die geplante Schwachstellen-Datenquelle kopieren, den Sie unter finden **Systemdefinition** > **Geplante Aufgaben**.
5. Fügen Sie die Domäne an den Namen an, um die geplante Aufgabe zu identifizieren.
6. Ändern Sie den Benutzer run_as in den Benutzer, den Sie im vorherigen Schritt erstellt haben.

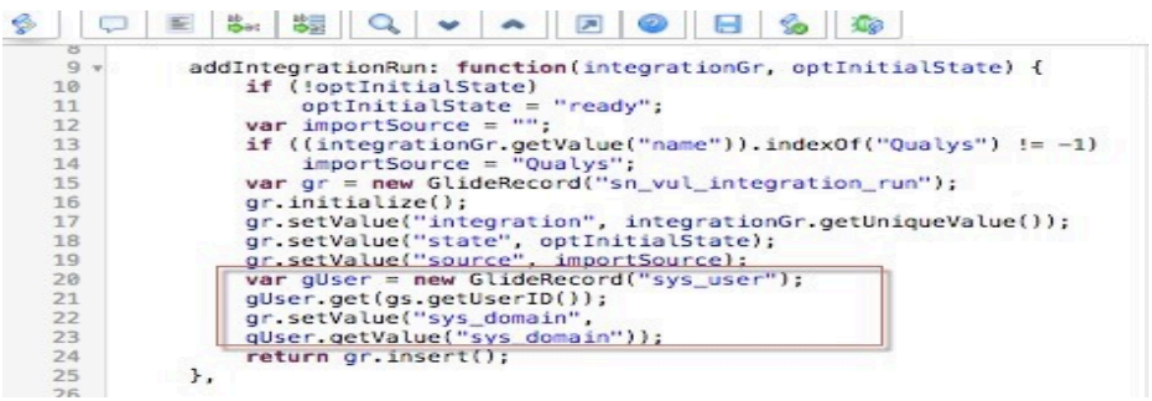
Hinweis:
Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Benutzerdomäne run_as ausgeführt wird.



7. Bearbeiten Sie die UI-Aktion „Jetzt ausführen“ in der Tenable.io Open Vulnerabilities-Integration, um diesen Codeblock am Anfang der Datei hinzuzufügen.
```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Hinweis:
Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in der Benutzerdomäne „run_as“ ausgeführt wird.

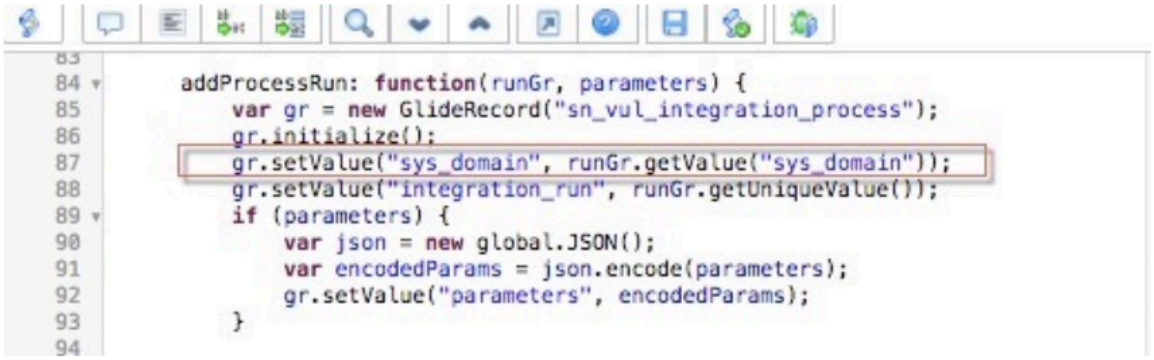
8. Bearbeiten Sie die Skripteinbindungsmethode addIntegrationRun für VulnerabilityIntegrationUtils, um den hervorgehobenen Code hinzuzufügen.



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Bearbeiten Sie die Skripteinbindungsmethode addProcessRun für VulnerabilityIntegrationUtils, um den hervorgehobenen Code hinzuzufügen.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Bearbeiten Sie die DataSourceVulnReportRefreshProcessor-Skripteinbindungsmethode _processFromDataSourceGroups, um diesen ursprünglichen Code zu ändern: Ursprünglicher _processFromDataSourcesGroups-Code in Bearbeiteter _processFromDataSourcesGroups-Code.
11. Bearbeiten Sie die Skripteinbindungsmethode VulnerabilityDSAttachmentManager, queueItem, um die folgenden hervorgehobenen Codeblöcke hinzuzufügen: queueItem, _getNext, _processQueueEntry.

Sie sind bereit für Importe der domänengetrennten Hosterkennung.

Rechner vor dem Import deaktivieren

Befolgen Sie diese Schritte, um den Standardrechner zu deaktivieren, wenn er nicht verwendet wird. Wenn Sie keine Schwachstellen-Rechner verwenden, deaktivieren Sie am besten die Standard-Rechner zusätzlich zu den anderen, die Sie definiert haben. Sicherheitsrisiko-Rechner werden jedes Mal ausgeführt, wenn auf den Datensatz eines angreifbaren Elements zugegriffen wird, und können sich auf die Leistung der Instanz auswirken.

Erforderliche Rolle: sn_vul.vulnerability_admin.

12. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellen-Rechner**.
13. Öffnen Sie die Gruppe „Schwachstellenauswirkung“.
14. Öffnen Sie den Rechner für punktzahl- und servicebasierte Auswirkung.
15. Deaktivieren Sie das Feld Aktiv, um den Rechner zu deaktivieren.
16. Klicken Sie auf Aktualisieren.

Sie haben den Standardrechner deaktiviert.

Deaktivieren Sie auf Benachrichtigungen basierende Business-Regeln vor dem ersten Import

Befolgen Sie diese Schritte, um Benachrichtigungsbezogene Business-Regeln vor dem ersten Datensatzimport zu deaktivieren. Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln viele Benachrichtigungen generieren, was sich auf die Leistung auswirkt. Diese Business-Regeln müssen geändert werden, um sie während des Imports zu deaktivieren.

Erforderliche Rolle ist sn_vul.vulnerability_admin.

17. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
18. Suchen Sie nach betroffenen CI-Benachrichtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

19. Öffnen Sie die Geschäftsregel, und fügen Sie die folgende Bedingung ein: `current.sys_class_name != “sn_vul_vulnerable_item"`.
20. Klicken Sie auf **Aktualisieren**.
21. Wiederholen Sie dieses Verfahren für die folgenden Geschäftsregeln:
    - Benachrichtigungen für betroffene Kostenstellen
    - Betroffene Gruppenbenachrichtigungen
    - Benachrichtigungen zum betroffenen Standort

> **Hinweis:**
> Nach Abschluss des ersten Datensatzimports können Sie diese Business-Regeln erneut aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und sich auf die Leistung Ihrer Instanz auswirken.

Ändern Sie ein anfängliches Startdatum

Führen Sie diese Schritte aus, um ein anfängliches Startdatum zu ändern. Während der Installation legen Sie mit dem Setup-Assistenten ein anfängliches Startdatum für die Tenable-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen, wie in den folgenden Schritten gezeigt.

22. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**.
23. Klicken Sie auf eine beliebige Integration.
24. Klicken Sie auf Integrationsdetails.
25. Legen Sie das Feld Startzeit auf einen Wert in der Vergangenheit fest, damit alle seit dieser Zeit gescannten und erkannten Schwachstellen erkannt werden.

    Wenn Sie Tenable mit dem Setup-Assistenten konfiguriert haben, ist das Feld Startzeit vorab ausgefüllt, zunächst bis drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum. Hinweis: Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass große Datenmengen die Tenable-API-Quotenbeschränkungen überschreiten und Ausführungszeitüberschreitungen ausgelöst werden.

26. Klicken Sie auf **Absenden** oder **Aktualisieren**.
27. **Wahlweise:** Klicken Sie auf **Jetzt ausführen**, um die Ausführung sofort zu starten.

Tenable-Erkennungen basierend auf der Schwachstelleninstanz aufteilen, um angreifbare Elemente aufzuteilen

ServiceNow® Vulnerability Response ermöglicht die Aufteilung von Erkennungen von Tenable-Scannern, wodurch für jede erkannte Schwachstelleninstanz ein spezifisches angreifbares Element (Unique VIT) erstellt werden kann. Diese Aufteilung ermöglicht die Zuweisung von VITs zu verschiedenen Nachbesserungsteams, wodurch die Verwaltung und Nachverfolgung von Schwachstellen verbessert wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Nutzlast des Tenable-Scanners enthält Erkennungsdaten, wobei jeder Pfad innerhalb des Nachweises zur Aufteilung der Erkennungen verwendet wird. Das Ausgabe-Tag in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutzlast gibt den Ort der Schwachstelle an und erleichtert so die genaue Identifizierung und Verwaltung von Schwachstellen entsprechend ihren spezifischen Pfaden.

Prozedur

1. Legen Sie in der Tabelle „Drittparteiintegrationen“ [sn_sec_int_integration] den Wert **Nachweis in VI-Schlüsselspalte einschließen** für Tenable.io und Tenable.scauf true fest.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.
3. Aktivieren Sie im Formular „Port einbeziehen“ das Kontrollkästchen **Port einbeziehen**, und wählen Sie den Link **Hier klicken**.
4. Wählen Sie in der Liste Nachweis zu VI-Schlüssel hinzufügen die **Option Neu**aus.
5. Fügen Sie im Formular „Nachweis zum VI-Schlüssel hinzufügen – Neuer Datensatz“ im Feld **Schwachstelle** die Tenable-ID hinzu, für die Sie den Nachweis einschließen möchten.

   Hinweis:
   Sie können die Erkennungen nur basierend auf Pfadinformationen oder durch Kombination von Pfad- und Versionsdetails aufteilen. Weitere Informationen finden Sie im Abschnitt „Erkennungen von Tenable-Scannern aufteilen“ auf dieser Seite.

6. Im Feld **Regulärer Ausdruck zur Aufteilung von Tenable-VITs** :
   - Teilen Sie die Erkennung nur basierend auf dem Pfad auf, indem Sie Pfad\s+:\s+([A \n]+) eingeben.
   - Teilen Sie die Erkennung basierend auf dem Pfad sowie den installierten und festen Versionen auf, indem Sie Pfad\s+:\s+([A\n]+)\n\s+linstalliert\s+version\s+:\s+([A\n]+) eingeben. \n\s+Repariert\s+Version\s+:\s+([A\n]+).
7. Wählen Sie **Absenden**.

Example: Erkennungen von Tenable-Scannern aufteilen

Die folgende Erkennung von einem Tenable-Scanner zeigt im Ausgabe-Tag einen Nachweis, der sowohl Pfad- als auch Versionsinformationen enthält.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                     "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                "tracked": true


            "output": "In                          C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                                Path
            "plugin":
                "bid":
                    123456


                "checks_for_default_account": false,
               "checks_for malware": false,

                 "coe":
               "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"


                "cvSs3_base_score": 7.8,
               "cvss3 temporal score": 7.0,

               "cvss3_temporal_vector": {
                    "exploitability": "Proof-of-Concept",
                    "remediation level": "Official Fix",
                     "report_confidence": "Confirmed",
                     "raw": "E: P/RL:0/RC: C"
```


Konfigurations-Compliance – Fehlerkorrektur

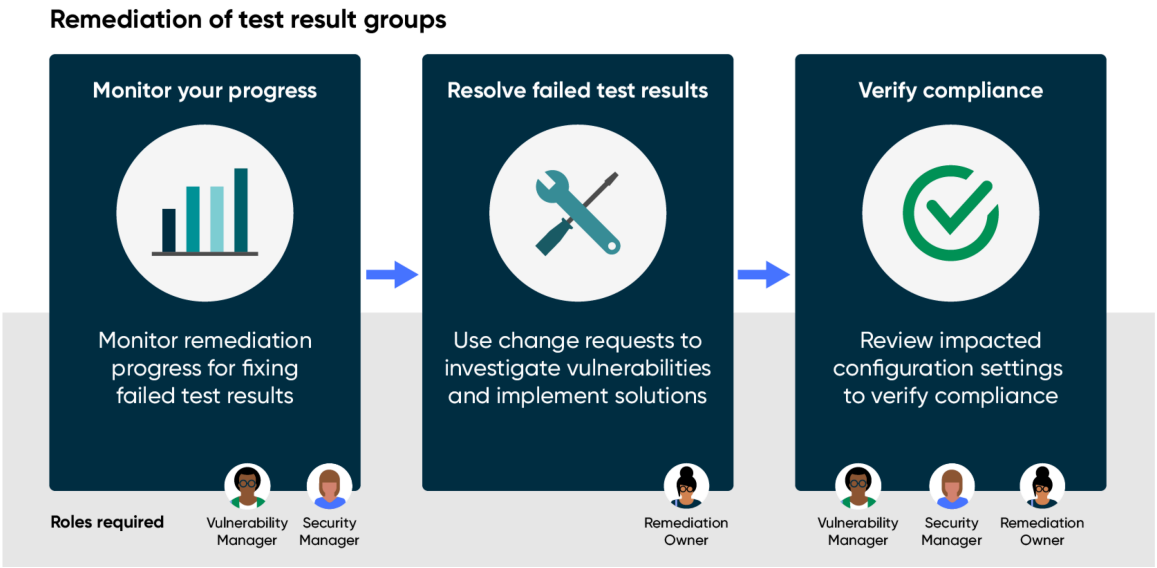
Konfigurations-Compliance Bei einer -Korrektur handelt es sich in erster Linie um einen manuellen Prozess, der durch geplante Aufgaben (Integrationen), Korrekturaufgaben, Workflows und Change-Anforderungen ergänzt wird.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Separate SCA-Plugins von Drittparteien erfassen und transformieren Daten in Konfigurations-Compliance. Bevor Sie Konfigurations-Compliance zur Korrektur von Configuration Items verwenden können, müssen Sie die Scannerintegration einer Drittpartei installieren und mindestens einen Netzwerkscan durchführen.

Verwenden Sie Change-Anforderungen, um einzelne Testfehler in Korrekturaufgaben zu beheben.

Die Status von Korrekturaufgaben werden automatisch geändert, wenn zugehörige Change-Anforderungen ihre Lebenszyklen mit Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgabendurchlaufen. Benutzer mit der Rolle „itil“ können Change-Anforderungen direkt von Korrekturaufgaben aus erstellen und verwalten.

Erstellen Sie manuell eine Korrekturaufgabe Konfigurations-Compliance .

Im Modul **„Korrekturaufgaben“** können Sie manuell eine Korrekturaufgabe erstellen und die Korrektur durchführen.

Wichtig:
Wo können Sie Korrekturaufgaben erstellen?

- Vulnerability Manager Workspace als Benutzer mit der Rolle sn_vulc.admin.
- IT Remediation Workspace als Benutzer mit der Rolle sn_vulc.remediation_owner.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie Regeln für Korrekturaufgaben verwenden, wird die Registerkarte **Testergebnisse** automatisch gefüllt. Die manuelle Erstellung ist nützlich für eine Korrekturaufgabe, die keine Regel erfordert und nicht wiederholt werden muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

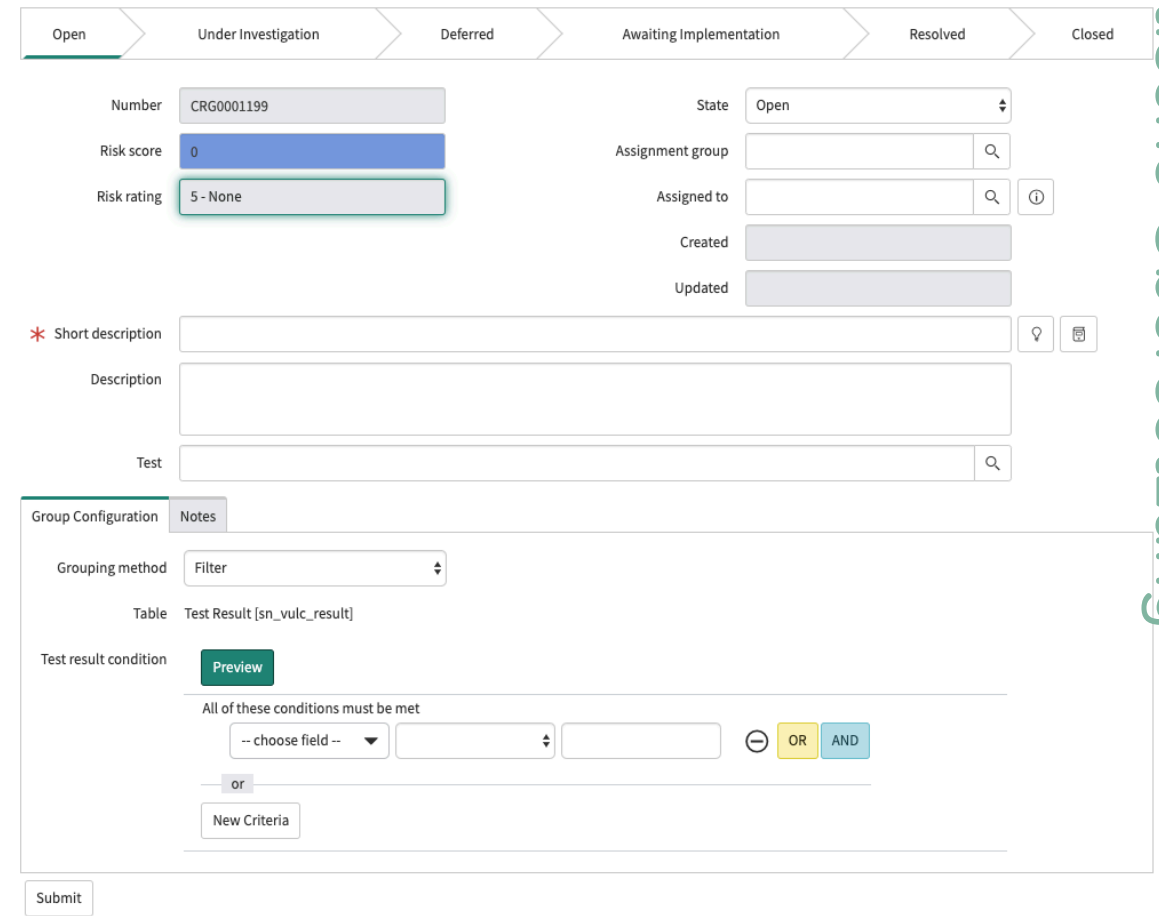
Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben**.
2. Klicken Sie im Navigationsbereich auf **Meine offenen Aufgaben** oder **Alle offenen Aufgaben,** um die Liste anzuzeigen.
3. Klicken Sie auf **Neu**.

Formular für Korrekturaufgaben



4. Füllen Sie die entsprechenden Felder im Formular „Korrekturaufgabe“ aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

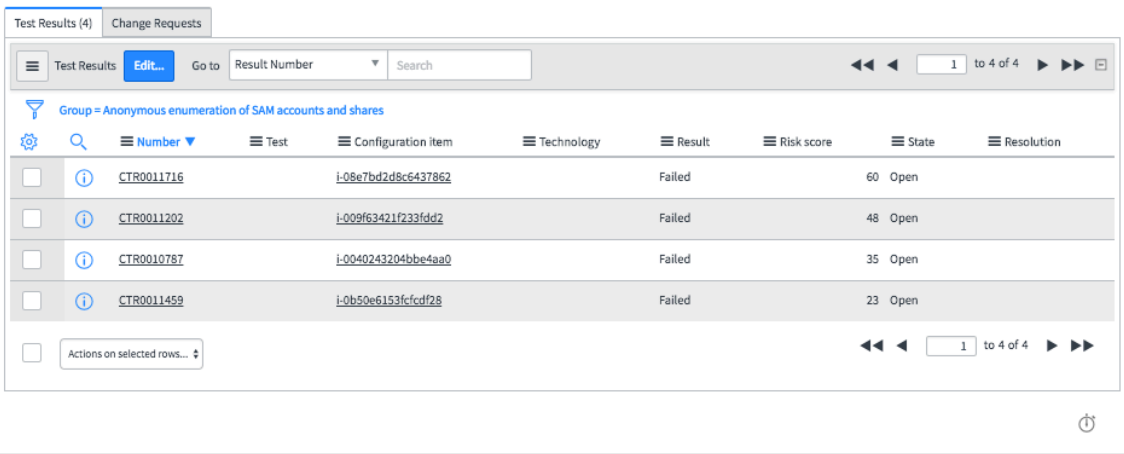
Formular „Korrekturaufgabe“.

Feld	Beschreibung
Nummer	Automatisch zugewiesene ID im System.
Risikopunktzahl	Automatisch vom Risikopunktzahl-Rechner ausgefüllt. Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl wird gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht „Geschlossen“-Testergebnisse (Offen, „In Untersuchung“, „Warten auf Implementierung“, „Zurückgestellt“, „Gelöst“) und 15 % der Punktzahl aus der Anzahl der Tests stammen Ergebnisse, die nicht „Geschlossen“ sind.
Risikobewertung	Automatisch vom Risikopunktzahl-Rechner ausgefüllt. Basierend auf einem Bereich von Risikopunktzahlen auf einer numerischen Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen.
Status	„Anfänglich **offen**“ ist der Korrekturstatus der Korrekturaufgabe. Weitere Informationen finden Sie unter Konfigurations-Compliance Status.
Zuweisungsgruppe	Weisen Sie die Korrekturaufgabe einer Korrekturgruppe zu.
Zugewiesen an	Weisen Sie Mitarbeiter für die Korrekturaufgabe zu.
Erstellt	Datum, an dem Sie diese Korrekturaufgabe erstellt haben.
Aktualisiert	Datum, an dem Sie diese Korrekturaufgabe aktualisiert haben.
Kurzbeschreibung	Name der Korrekturaufgabe.
Beschreibung	Beschreibung dieser Korrekturaufgabe.
Test	Wählen Sie einen Konfigurationstest für diese Korrekturaufgabe aus.
Zugehörige Registerkarten	
Gruppenkonfiguration	Zu verwendende Gruppierungsmethoden: ◦ Manuell (Standard): ◦ Filter- oder Gruppenregel: Tabelle: als Testergebnis vorausgewählt [sn_vulc_result] Testergebnisbedingung: Wählen Sie die zu verwendenden Filter aus. **Hinweis:** Der Link Datensätze erfüllen Bedingung oberhalb der Filterbedingungen zeigt die von Ihnen ausgewählten Testergebnisdatensätze in einem neuen Fenster an. Klicken Sie auf **Vorschau**, um zu sehen, wie viele Ergebnisse Ihre Filterkriterien zurückgeben, bevor Sie die neue Gruppe speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die zugehörige Liste „Testergebnisse“ muss manuell erstellt werden, indem Sie auf der zugehörigen Registerkarte **„Testergebnisse“** auf die Schaltfläche „ **Bearbeiten** “ klicken.
Notizen	Arbeitsnotizen im Zusammenhang mit dieser Korrekturaufgabe.

5. Klicken Sie mit der rechten Maustaste in den Header von **Speichern**, oder klicken Sie auf **Absenden,** um zu speichern und zur Liste der Korrekturaufgaben zurückzukehren.
   Zeigt die zugehörigen Listen **„Testergebnisse“** und **„Change-Anforderung“** an.



Erstellen Sie manuell eine Konfigurations-Compliance -Korrekturaufgabe aus der Liste „Testergebnisse“.

Sie können eine Korrekturaufgabe manuell aus der Liste **„Testergebnis“** erstellen und anhand der resultierenden Korrekturaufgabe eine Korrektur durchführen.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Methode erfordert die Auswahl von Testergebnissen, die enthalten sollen, und das Erstellen der Gruppe über das Menü **Aktionen für ausgewählte Zeilen...** Diese Methode eignet sich für Ergebnisse, die sich nicht leicht filtern lassen, oder für Situationen, in denen Sie Testergebnisse zur Korrektur angeben möchten.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

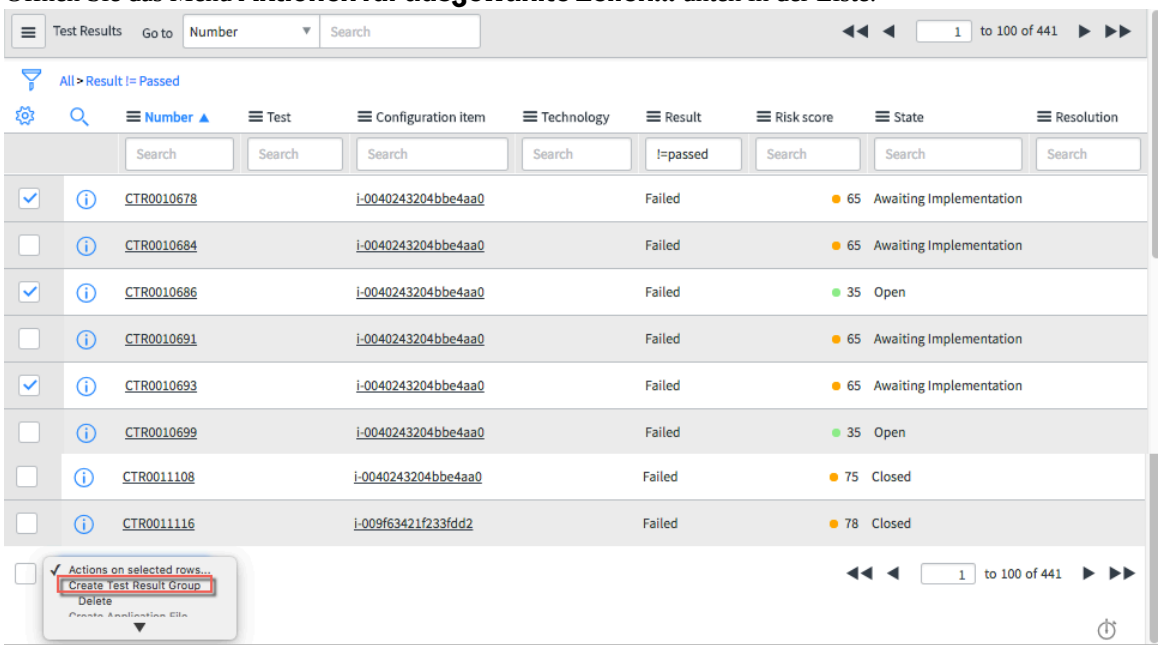
Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse**.
2. Wählen Sie im Navigationsbereich ein Testergebnismodul aus, um eine Liste zu öffnen.
3. Wählen Sie die Testergebnisse aus, die in die Korrekturaufgabe aufgenommen werden sollen, indem Sie das Kontrollkästchen neben dem jeweiligen Ergebnis aktivieren.
4. Öffnen Sie das Menü **Aktionen für ausgewählte Zeilen...** unten in der Liste.

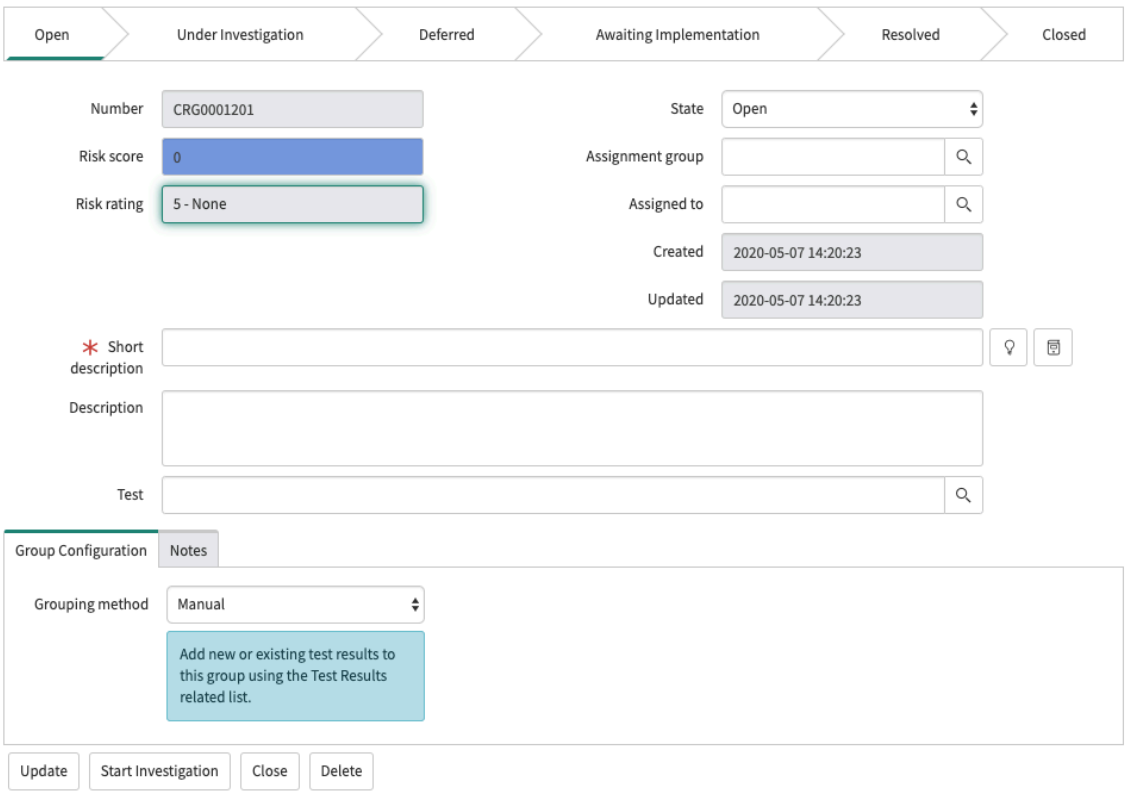


5. Wählen Sie **Korrekturaufgabe erstellen aus**.
   Die Korrekturaufgabe wird erstellt und geöffnet.

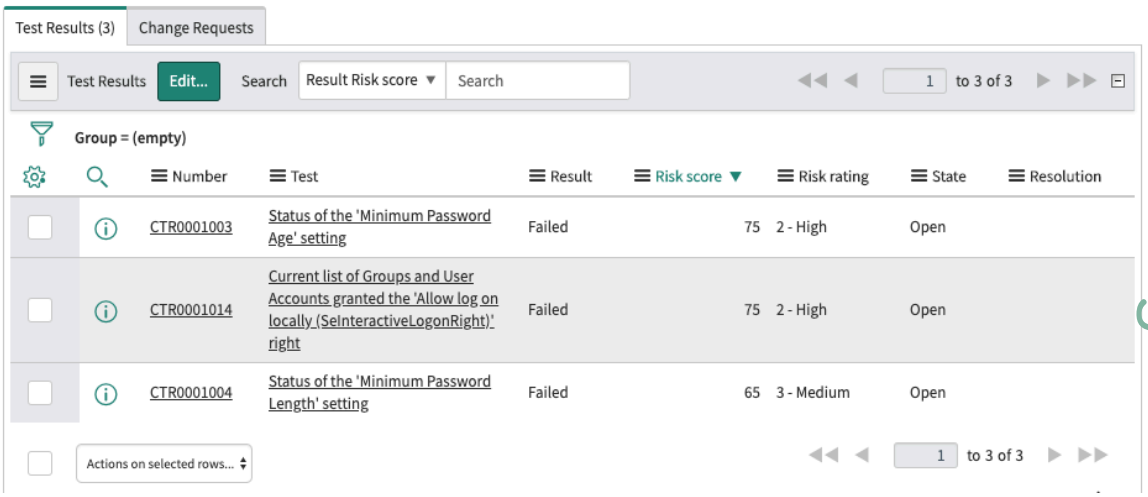
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Korrekturaufgabe“.



Die Testergebnisse, die Sie für die Korrekturaufgabe ausgewählt haben, werden zusammen mit allen zugehörigen Change-Anforderungen in der zugehörigen Liste Testergebnisse angezeigt.



6. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Nummer	Automatisch zugewiesene ID im System.
Punktzahl	Wird automatisch durch den Rollup-Rechner für die Risikopunktzahl ausgefüllt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl wird gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht „Geschlossen“-Testergebnisse (Offen, „In Untersuchung“, „Warten auf Implementierung“, „Zurückgestellt“, „Gelöst“) und 15 % der Punktzahl aus der Anzahl der Tests stammen Ergebnisse, die nicht „Geschlossen“ sind.
Bewertung	Wird automatisch durch den Rollup-Rechner für die Risikopunktzahl ausgefüllt. Basierend auf einem Bereich von Risikopunktzahlen auf einer numerischen Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen.
Historische Risikopunktzahl	Wird automatisch durch den Rollup-Rechner für die Risikopunktzahl ausgefüllt. Die inhärente Risikopunktzahl für alle bestandenen Testergebnisse in einer Korrekturaufgabe. Dieses Feld zeigt das Ausmaß des Risikos an, das von einer Testgruppe behoben wurde. Es wird nur angezeigt, wenn sich eine Testgruppe im Status „Geschlossen“ befindet und die Risikopunktzahl null ist.
Status	„Anfänglich **offen**“ ist der Korrekturstatus der Korrekturaufgabe. Weitere Informationen finden Sie unter Konfigurations-Compliance Status.
Zuweisungsgruppe	Weisen Sie die Korrekturaufgabe einer Korrekturgruppe zu.
Zugewiesen an	Weisen Sie Mitarbeiter für die Korrekturaufgabe zu.
Erstellt	Datum, an dem Sie diese Korrekturaufgabe erstellt haben.
Aktualisiert	Datum, an dem Sie diese Korrekturaufgabe aktualisiert haben.
Kurzbeschreibung	Name der Korrekturaufgabe.
Beschreibung	Textbeschreibung dieser Korrekturaufgabe.
	Wählen Sie einen Konfigurationstest für diese Korrekturaufgabe aus.
Zugehörige Registerkarten	
Gruppenkonfiguration	Zu verwendende Gruppierungsmethoden: ○ Manuell (Standard) ○ Filter Tabelle: als Testergebnis vorausgewählt Testergebnisbedingung: Wählen Sie die zu verwendenden Filter aus. **Hinweis:** Der Link Datensätze erfüllen Bedingung oberhalb der Filterbedingungen zeigt die von Ihnen ausgewählten Testergebnisdatensätze in einem neuen Fenster an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Klicken Sie auf **Vorschau**, um zu sehen, wie viele Ergebnisse Ihre Filterkriterien zurückgeben, bevor Sie die neue Korrekturaufgabe speichern.
Notizen	Arbeitsnotizen im Zusammenhang mit dieser Korrekturaufgabe.
Zugehörige Listen	
Testergebnisse	Testergebnisse, die in dieser Korrekturaufgabe enthalten sind.
Change-Anforderungen	Change-Anforderungen, die dieser Korrekturaufgabe zugeordnet sind.

7. Klicken Sie mit der rechten Maustaste auf den Header zu **Speichern**, oder klicken Sie auf **Absenden,** um zu speichern und zur Liste der Korrekturaufgaben zurückzukehren.

Change-Anforderung in Konfigurations-Compliance erstellen

Sie können eine Change-Anforderung aus einer Korrekturaufgabe in der Anwendung Konfigurations-Compliance erstellen.

Vorbereitungen
Erforderliche Rolle: Benutzer mit der Rolle „itil“.

Warum und wann dieser Vorgang ausgeführt wird
Erstellen Sie als IT- oder Korrekturspezialist eine Change-Anforderung (CHG) direkt aus einer Korrekturaufgabe für alle darin enthaltenen Testergebnisse. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, um Ihre Untersuchung auf Schwachstellen zu beschleunigen, die manuelles Eingreifen erfordern.

Sie können Change-Anforderungen direkt von Ihnen zugewiesenen Korrekturaufgaben erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

Standard

Ein zuvor autorisierter Change, der als risikoarm und relativ gängig gilt und anhand eines festgelegten Verfahrens oder einer festgelegten Arbeitsanweisung implementiert wird.

Normal

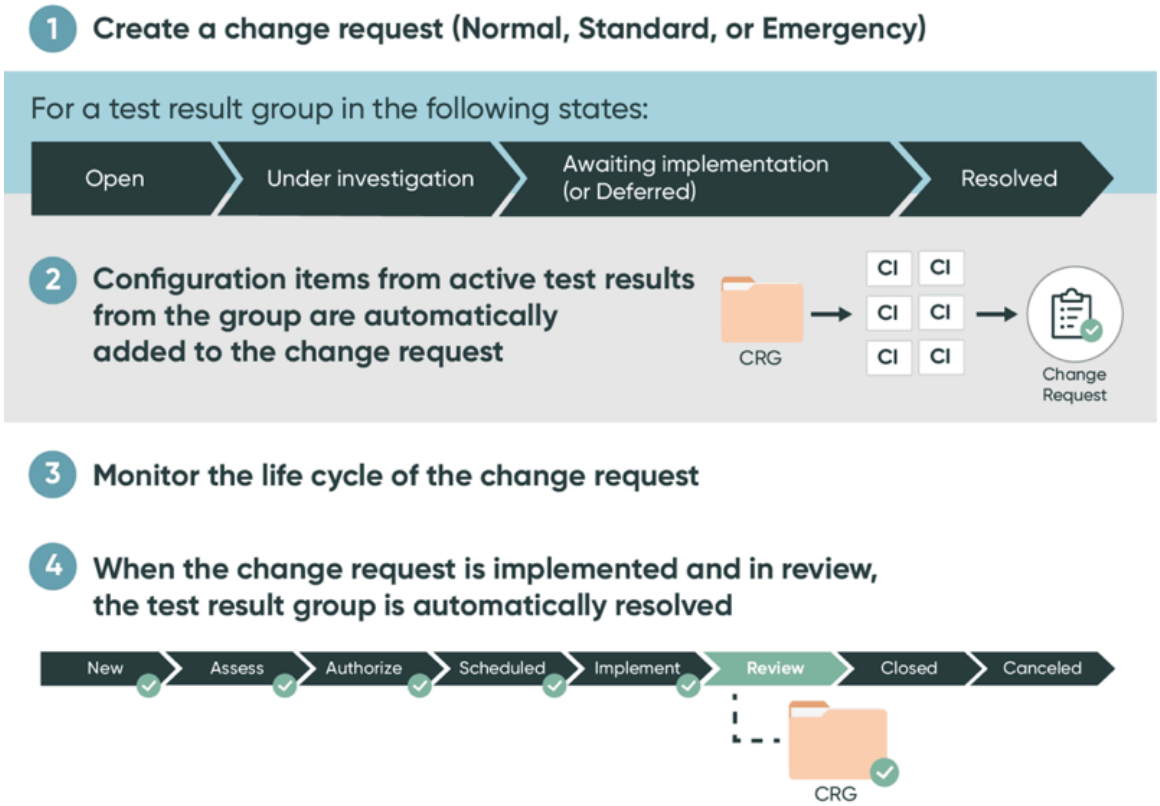
Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsstufen erfordert, bevor sie implementiert, überprüft und geschlossen werden.

Notfall

Ein Change zur Lösung eines schwerwiegenden Incident.

Die folgende Abbildung zeigt den Basis-Flow zum Erstellen einer Change-Anforderung aus einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow finden Sie in der Abbildung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ab Version 19.0 von Vulnerability Responsekönnen Sie Change-Anforderungen für Korrekturaufgaben im IT-Korrekturarbeitsbereich erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung im IT Remediation Workspace.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**.
   Die Liste der Korrekturaufgaben, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Korrekturaufgabe, für die Sie eine Change-Anforderung erstellen möchten.
   Sie können Change-Anforderungen aus Korrekturaufgaben in jedem anderen Status als **Geschlossen** oder **Wird überprüft**erstellen.

   Der Datensatz für die Korrekturaufgabe wird angezeigt.
3. Klicken Sie oben rechts im Datensatz **auf Change erstellen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Formular „Change-Anforderung“ wird angezeigt.

4. Füllen Sie die Felder aus.

   a. Wählen Sie aus der Liste des **Felds Gilt für** eines aus, um fortzufahren.

5. Wählen Sie für das Kontrollkästchen **CIs zu CR hinzufügen** aus, um fortzufahren.

6. Wählen Sie aus der Liste für das Feld **Change-Typ** einen aus, um fortzufahren.

   Die Funktion liest automatisch die Typen von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change Management eingerichtet haben. Wenn Sie beispielsweise den Namen für Ihre Standard-Change-Anforderungen in ITSM von Standard in Vorgenehmigtändern, wird Ihr neuer Name automatisch in der Liste Change-Typ im Formular Change-Anforderung erstellen angezeigt.

7. Die Felder im Abschnitt „Vorschau auf Change-Anforderung“ des Formulars sind bereits mit Informationen aus der Korrekturaufgabe ausgefüllt.
   Bearbeiten Sie diese Felder bei Bedarf.

8. Klicken Sie auf **Change erstellen**.
   Die Change-Anforderung wird angezeigt. In der zugehörigen Liste Betroffene CIs werden die CIs aus den Testergebnissen angezeigt, die Ihren Kriterien entsprechen. Wenn für die Change-Anforderung eine Genehmigung erforderlich ist, wird die Schaltfläche **Genehmigung anfordern** angezeigt.

   Nachdem die Change-Anforderung erstellt wurde, wechselt die Testergebnisgruppe in den Status **Warten auf Implementierung**. Nachdem die Change-Anforderung für diese Korrekturaufgabe gelöst wurde und keine weiteren offenen Change-Anforderungen mit dieser Korrekturaufgabe verknüpft sind, wird die Korrekturaufgabe ebenfalls in den Status **Gelöst** versetzt.

   Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

   Hinweis:
   Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung ihren Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder aus entfernen Bei einer Korrekturaufgabe kann die Statussynchronisierung Ihr manuelles Eingreifen möglicherweise überschreiben. Die Status von Change-Anforderungen verschieben die Korrekturaufgabe jedoch nicht automatisch aus den Status „Geschlossen“ oder „Zurückgestellt“.

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe in der Anwendung Konfigurations-Compliance zu.

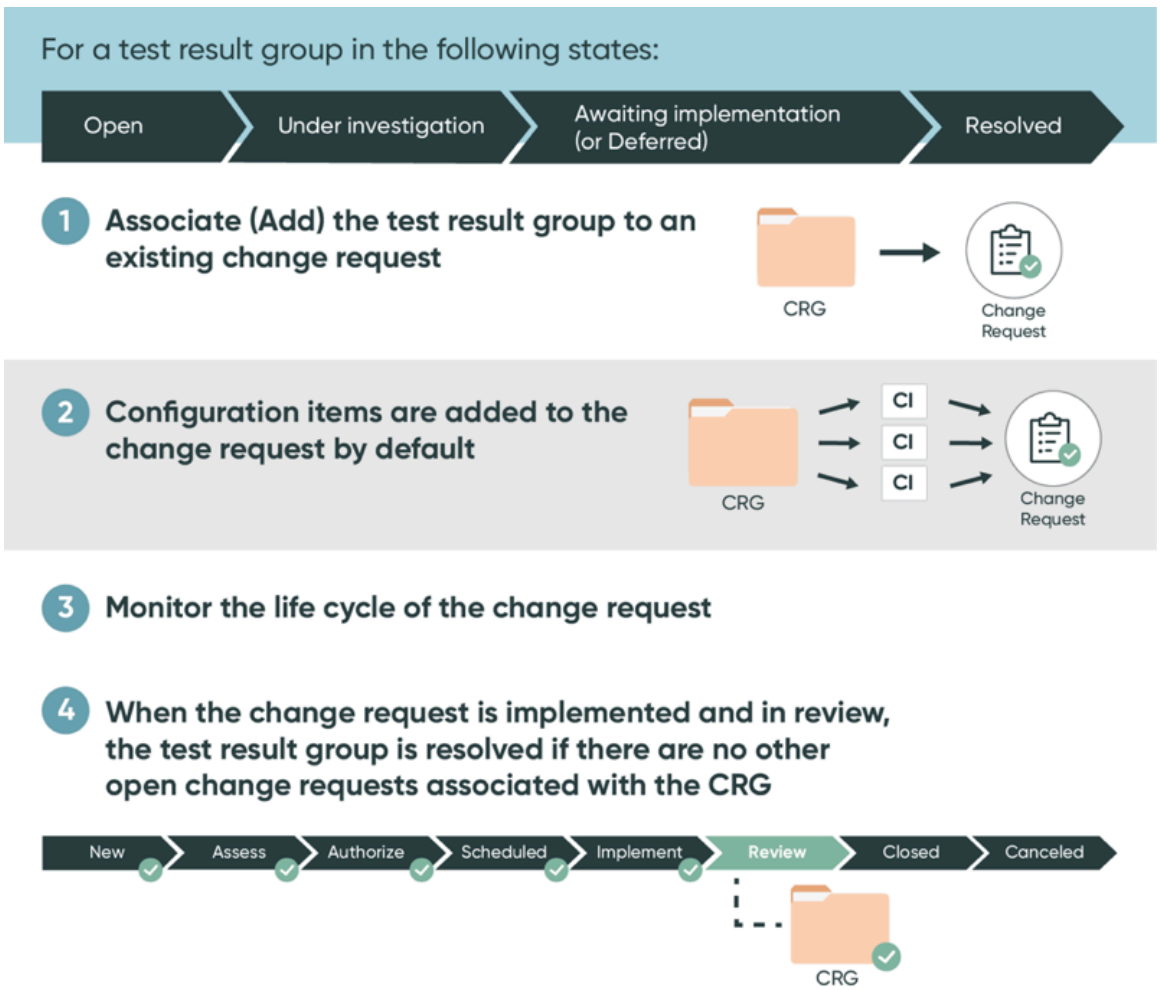
Vorbereitungen
Erforderliche Rolle: ein Benutzer mit der Rolle „itil“.

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie IT- oder Korrekturspezialist sind, vermeiden Sie die Erstellung von doppelten Change-Anforderungen (CHG), während Sie an der Lösung Ihrer Korrekturaufgaben arbeiten, indem Sie einer bereits in Ihrer -Instanz verfügbaren Change-Anforderung eine Korrekturaufgabe (RT) zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Korrekturaufgaben, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, direkt aus den Korrekturaufgaben-Datensätzen mit vorhandenen Change-Anforderungen verknüpfen. Die folgende Abbildung zeigt den Basis-Flow zum Zuordnen eines vorhandenen Change Request zu einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow finden Sie in der Abbildung.

Hinweis:
Sie können eine vorhandene Change-Anforderung einer Korrekturaufgabe in jedem anderen Status als **Abgebrochen** (**Offen**, **In Untersuchung**, **Warten auf Implementierung**, **Geschlossen**und **Zurückgestellt**) zuordnen. Change-Anforderungen, einschließlich solcher, die innerhalb der letzten 90 Tage geschlossen wurden, können über das Formular zugeordnet werden. Wenn Sie eine Change-Anforderung einer vorhandenen Korrekturaufgabe zuordnen, werden nur die aktiven Testergebnisse und ihre Configuration Items zur Change-Anforderung hinzugefügt.



Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**.
   Die Liste der Korrekturaufgaben, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Korrekturaufgabe, für die Sie eine Change-Anforderung erstellen möchten.

   Der Datensatz für die Korrekturaufgabe wird angezeigt.
3. Klicken Sie oben rechts im Datensatz **auf Change erstellen**.
   Das Formular „Change-Anforderung“ wird angezeigt.
4. Scrollen Sie zur zugehörigen Liste Change-Anforderungen, und wählen Sie sie aus.
   Alle Change-Anforderungen, die der Korrekturaufgabe zugeordnet sind, werden zusammen mit der Schaltfläche **Hinzufügen** angezeigt.
5. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld „Vorhandene Change-Anforderung zu Korrekturaufgabe hinzufügen“ wird angezeigt.
6. Klicken Sie auf das Suchsymbol, und wählen Sie ein Element aus der Liste aus.
   Sie können die angezeigte Liste filtern, um Ihre Suche einzugrenzen.
7. Klicken Sie auf **Absenden**.
   Die TRG wird zusammen mit einer Meldung angezeigt, die darauf hinweist, dass die Change-Anforderung erfolgreich der Korrekturaufgabe zugeordnet wurde. Unter der zugehörigen Liste „Change-Anforderungen“ wird die neue Change-Anforderung angezeigt. Die CIs aus der Korrekturaufgabe werden standardmäßig der Change-Anforderung hinzugefügt und in der zugehörigen Liste Betroffene CIs angezeigt. Sie können dem Change Request auch CIs aus dieser zugehörigen Liste hinzufügen. Eine Nachricht gibt die Anzahl der Testergebnisse an, die in die neue Korrekturaufgabe verschoben wurden, und die neue RT wird angezeigt.

   Hinweis:
   Bei weniger als 200 Testergebnissen wird der Teilungsvorgang synchron durchgeführt, und die Testergebnisse werden in der neuen Korrekturaufgabe angezeigt.

   Bei über 200 Testergebnissen wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die Testergebnisse in der neuen Korrekturaufgabe angezeigt werden. Die folgende Nachricht wird ebenfalls angezeigt: n Testergebnisse werden in Kürze von TRGxxxxxxxx in die neue Korrekturaufgabe GRCxxxxx verschoben.

Sie können der Korrekturaufgabe beliebige Change-Anforderungen zuordnen, mit den folgenden Ausnahmen:

- Change-Anforderungen im Status „ **Abgebrochen** “.
- Change-Anforderungen im Status **„Geschlossen** “, die älter als 90 Tage sind.
- Change-Anforderungen sind bereits RT zugeordnet. Das System lässt nicht zu, dass Sie eine Change-Anforderung zuordnen, die bereits dem RT zugeordnet ist.

Nachdem die Change-Anforderung für diese Korrekturaufgabe gelöst wurde und keine weiteren offenen Change-Anforderungen mit dieser Korrekturaufgabe verknüpft sind, wird die Korrekturaufgabe ebenfalls in den Status**Gelöst** versetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung ihren Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder aus entfernen Bei einer Korrekturaufgabe kann die Statussynchronisierung Ihr manuelles Eingreifen möglicherweise überschreiben. Die Status von Change-Anforderungen verschieben die Korrekturaufgabe jedoch nicht automatisch aus den Status „Geschlossen“ oder „Zurückgestellt“.

Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Teilen Sie eine Korrekturaufgabe auf

Identifizieren Sie aus einer vorhandenen Korrekturaufgabe in der Anwendung Konfigurations-Compliance eine Teilmenge der Testergebnisse, die Sie in eine neue Korrekturaufgabe verschieben möchten.

Wichtig:
Als Administrator und Korrekturbesitzer können Sie eine Korrekturaufgabe aus dem Vulnerability Manager Workspace bzw. IT-Korrekturarbeitsbereich aufteilen.

Vorbereitungen
Erforderliche Rolle: ein Benutzer mit der Rolle „itil“.

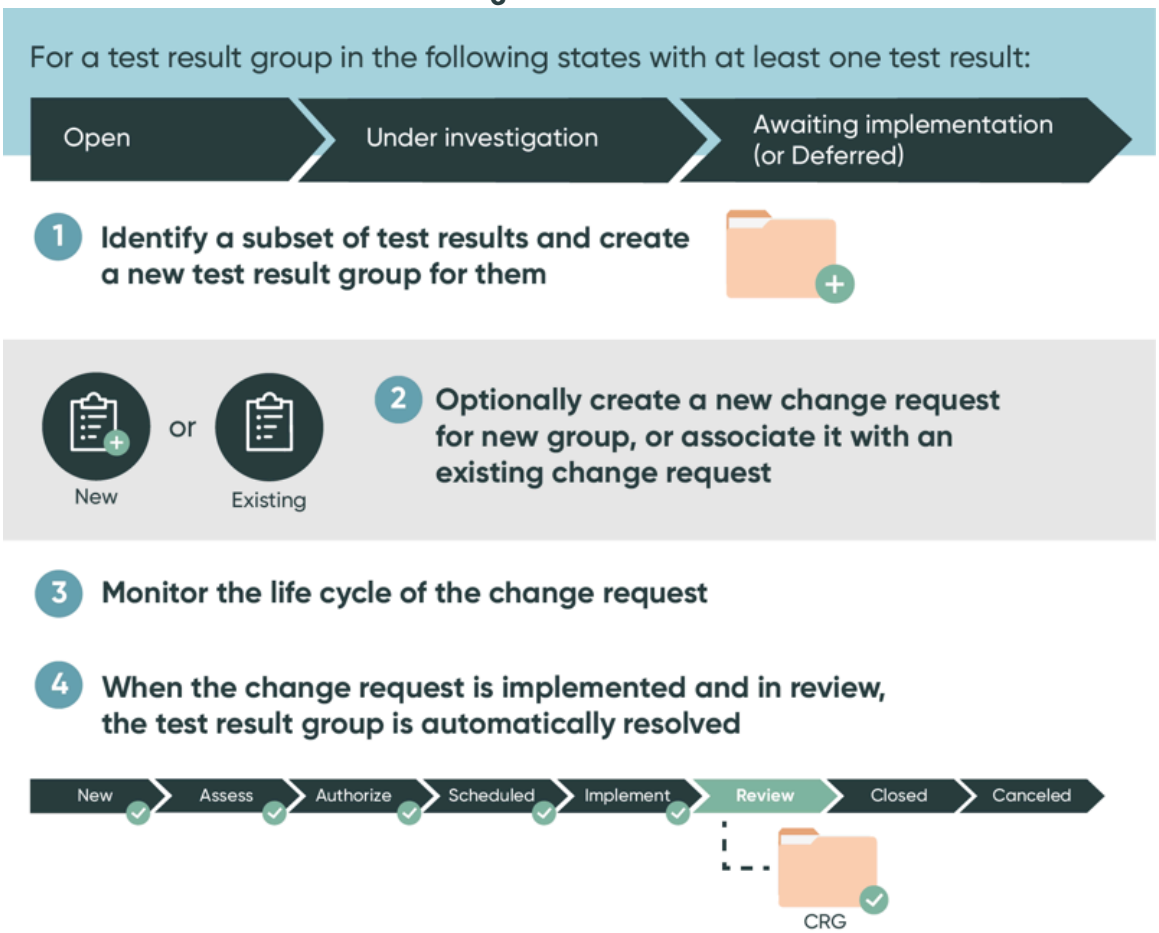
Warum und wann dieser Vorgang ausgeführt wird
Als IT- oder Korrekturspezialist können Sie vorhandene Korrekturaufgaben in den Status **„Offen“**, **„Wird untersucht“**oder **„Warten auf Implementierung“** mit mehr als einem Testergebnis aufteilen. Durch Erstellen einer neuen Korrekturaufgabe mit Testergebnissen, die bestimmten Kriterien entsprechen, können Sie mit einer bestimmten Gruppe von Testergebnissen arbeiten, ohne die ursprüngliche Korrekturaufgabe zu beeinträchtigen.

Wenn Sie die Bedingungen für die Testergebnisse angeben, die Sie mit dem Bedingungsgenerator in eine neue Korrekturaufgabe verschieben möchten, werden nur die aktiven Testergebnisse, die Ihren Kriterien entsprechen, in die neue Aufgabe verschoben. Sie müssen keine Change-Anforderungen (CHGs) erstellen, wenn Sie eine Korrekturaufgabe aufteilen. Sie können zum Teilen einer Korrekturaufgabe gleichzeitig mit dem Erstellen einer Change-Anforderung eine Korrekturaufgabe aufteilen oder eine Korrekturaufgabe aufteilen, ohne eine Change-Anforderung zu erstellen.

Die folgende Abbildung zeigt den Basis-Flow für die Aufteilung einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow finden Sie in der Abbildung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow zum Aufteilen einer Korrekturaufgabe



Anwendungsfälle für die Aufteilung von Testergebnissen aus vorhandenen Korrekturaufgaben in neue Aufgaben können die folgenden Beispiele umfassen:

- Wenn Sie eine Change-Anforderung oder Change-Anforderungen für eine Aufgabe aufteilen möchten.
- Wenn Sie eine aufgeteilte Aufgabe einem anderen Benutzer in Ihrer Zuweisungsgruppe zuweisen.
- Wenn Sie eine Zurückstellung oder Ausnahme für eine aufgeteilte Aufgabe anfordern, weil Sie wissen, dass einige Testergebnisse für bestimmte Configuration Items (CI) in einem bestimmten Zeitrahmen nicht nachgebessert werden können.

[store-future: BEGIN review]Ab Version 19.0 von Vulnerability Responsekönnen Sie Korrekturaufgaben im IT-Korrekturarbeitsbereich aufteilen.[End]

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Tests** > **Korrekturaufgaben** > **Meine offenen Aufgaben**.
   Die Liste der Ihren Gruppen zugewiesenen Korrekturaufgaben wird angezeigt.
2. Klicken Sie in der Spalte Anzahl auf die Korrekturaufgabe, die Sie aufteilen möchten.

   Der Datensatz für die Korrekturaufgabe wird angezeigt.
3. Führen Sie die folgenden Schritte aus, um eine Teilmenge der Testergebnisse für eine neue Aufgabe zu erstellen, die bestimmten Kriterien entspricht.

   Klicken Sie oben rechts im Datensatz auf **Split Task (Aufgabe teilen)**.

   Unter Umständen bevorzugen Sie diese Methode zum Erstellen einer neuen Korrekturaufgabe, wenn Sie mit einer großen Gruppe mit mehreren Testergebnissen arbeiten.

   Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.
4. Geben Sie bei angezeigtem Bedingungsgenerator die Bedingungen für die Testergebnisse an, die Sie in eine neue Korrekturaufgabe verschieben möchten.

   Beispielsweise können Sie nur Testergebnisse herausfiltern, die den folgenden Bedingungen entsprechen:

   - Im Status „ **Offen** “.
   - Risikopunktzahlen über 75.
   - Ergebnis ist **Fehlgeschlagen**.

   Wenn Testergebnisse nach Eingabe der Bedingungen Ihrem Filter entsprechen, wird eine Meldung mit der Anzahl der übereinstimmenden Testergebnisse angezeigt.

   Wenn eine Meldung angezeigt wird, dass keine Testergebnisse Ihrem Filter entsprechen oder dass alle Ihre Testergebnisse Ihren Kriterien entsprechen, passen Sie die Bedingungen so an, dass mindestens ein Testergebnis Ihren Filterkriterien entspricht.
5. Klicken Sie auf **Vorschauelemente,** um die übereinstimmenden Testergebnisse anzuzeigen.
   In einem neuen Fenster mit dem Titel „Korrekturaufgaben“ werden die Elemente angezeigt.
6. Um eine Vorschau der Details zu den Testergebnissen anzuzeigen, die Ihren Filterkriterien entsprechen, führen Sie diese Schritte aus, bevor Sie auf **Aufgabe aufteilen** klicken, um die neue Gruppe zu erstellen. Diese Details umfassen die Zuweisungsgruppe und die Person, der das Testergebnis zugewiesen ist. Durch das Anzeigen dieser Informationen in der Vorschau können Sie sicherstellen, dass die neue Aufgabe ordnungsgemäß zugewiesen ist.

   a. Klicken Sie bei angezeigter Liste der Fehlerkorrekturen in der Vorschau auf ein Element in der Spalte Ergebnis.
      Der Datensatz Testergebnis wird angezeigt.

   b. Stellen Sie sicher, dass die Felder **Zuweisungsgruppe** und **Zugewiesen an** korrekt sind.

   c. Klicken Sie auf **Aktualisieren**.
7. Wenn Sie bereit sind, die neue Korrekturaufgabe zu erstellen, klicken Sie auf **Aufgabe aufteilen**.
   Eine Nachricht gibt die Anzahl der Testergebnisse an, die in die neue Korrekturaufgabe verschoben wurden, und die neue Korrekturaufgabe wird angezeigt. Damit Sie die neue Aufgabe leichter identifizieren können,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie den Text im Feld **Kurzbeschreibung** bearbeiten und die Felder Zuweisungsgruppe oder Zugewiesen an bei Bedarf erneut bearbeiten.

Hinweis:
Bei weniger als 200 Testergebnissen wird der Teilungsvorgang synchron durchgeführt, und die Testergebnisse werden in der neuen Aufgabe angezeigt.

Bei über 200 Testergebnissen wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die Testergebnisse in der neuen Aufgabe angezeigt werden. Die folgende Nachricht wird ebenfalls angezeigt: n Testergebnisse werden in Kürze von TRGxxxxxxxx in die neue Korrekturaufgabe GRCxxxxx verschoben.

8. Alternativ können Sie eine neue Korrekturaufgabe erstellen, indem Sie Testergebnisse direkt aus der zugehörigen Liste „Testergebnisse“ in einer Korrekturaufgabe auswählen.

   Möglicherweise bevorzugen Sie diese Methode, wenn Sie nur wenige Testergebnisse in einer Korrekturaufgabe haben oder genau wissen, welche Tests Sie in eine neue Korrekturaufgabe verschieben möchten.

   a. Scrollen Sie bei angezeigtem Datensatz der Korrekturaufgabe zur zugehörigen Liste „Testergebnisse“.

   b. Aktivieren Sie in der Spalte ganz links die Kontrollkästchen für die Testergebnisse, für die Sie eine neue Korrekturaufgabe erstellen möchten.

   c. Klicken Sie in der Liste Aktionen für ausgewählte Zeilen unten links im Datensatz **auf Aufgabe teilen**.

   d. Im Formular „Korrekturaufgabe aufteilen“, das angezeigt wird, können Sie den Text im Feld **Kurzbeschreibung** bearbeiten, damit Sie die neue Gruppe leichter identifizieren können.

   e. Klicken Sie auf **Aufgabe aufteilen**.
   Eine Nachricht gibt die Anzahl der Testergebnisse an, die in die neue Aufgabe verschoben wurden, und die neue Korrekturaufgabe wird angezeigt.

   Nachdem die Change-Anforderung für diese Korrekturaufgabe gelöst wurde und keine weiteren offenen Change-Anforderungen mit dieser Korrekturaufgabe verknüpft sind, wird die Korrekturaufgabe ebenfalls in den Status **Gelöst** versetzt.

   Hinweis:
   Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung ihren Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder aus entfernen Bei einer Korrekturaufgabe kann die Statussynchronisierung Ihr manuelles Eingreifen möglicherweise überschreiben. Die Status von Change-Anforderungen verschieben die Korrekturaufgabe jedoch nicht automatisch aus den Status „Geschlossen“ oder „Zurückgestellt“.

   Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Nächste Maßnahme

Sie können Change-Anforderungen für Ihre neuen Korrekturaufgaben erstellen oder zuordnen. Weitere Informationen finden Sie unter Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu und Change-Anforderung in Konfigurations-Compliance erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entfernen Sie Zuweisungen aus Korrekturaufgaben für Sie oder Ihre Gruppen

Weisen Sie die Testergebnisdatensätze in der Anwendung Konfigurations-Compliance erneut zu, wenn die Datensätze Ihnen oder Ihrer Gruppe nicht korrekt zugewiesen wurden.

Vorbereitungen

Erforderliche Rolle: sn_vulc.remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Ab v14.3 der Anwendung Konfigurations-Compliance, Wenn Sie feststellen, dass Korrekturaufgaben und die zugehörigen Testergebnisse nicht in Ihrem Korrekturbereich liegen, oder wenn Sie der Meinung sind, dass Ihnen oder Ihren Gruppen Datensätze nicht korrekt zugewiesen wurden, sollten Sie sich oder Ihre Gruppen aus entfernen die Felder Zugewiesen an und Zuweisungsgruppe in RT-Datensätzen.

Die Schaltfläche „ **Zuweisung aufheben“** wird für Korrekturaufgaben-Datensätze in jedem anderen Status als Geschlossen oder Gelöst angezeigt.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren Sie zu einem Ihnen zugewiesenen Korrekturaufgaben-Datensatz, der sich in einem anderen Status als „Geschlossen“ oder „Gelöst“ befindet.
2. Um die Felder **Zugewiesen an** und **Zuweisungsgruppe** zu löschen, wählen Sie oben im Datensatz **Zuweisung aufheben**aus.
3. Geben Sie im Dialogfeld **„Zuweisung aufheben“** Arbeitsnotizen an, und wählen Sie **Absenden aus**.
   - Die von Ihnen bereitgestellten Arbeitsnotizen werden im Abschnitt Notizen angezeigt.
   - Auf der Registerkarte **Change-Genehmigung** zeigt der Status-Change-Genehmigungsdatensatz (CA#) den Status Wird überprüft an, was Ihnen hilft, den Genehmigungs-Workflow nachzuverfolgen.
   - Auf der Registerkarte **Angeforderte Genehmigungen** wird Ihr Antrag auf Entfernung von Ihnen oder Ihrer Zuweisungsgruppe als Status Angefordert angezeigt.

Ergebnisse

Die Anforderung wird mithilfe eines standardmäßigen, einstufigen Genehmigungsworkflows genehmigt. Weitere Informationen hierzu finden Sie unter Anforderung zum Aufheben der Zuweisung genehmigen in Konfigurations-Compliance.

- Wenn Ihre Anforderung genehmigt wird, werden der Status-Change-Genehmigungsdatensatz und der Datensatz für die angeforderte Genehmigung in **den Status Genehmigt**geändert. Sie und Ihre Gruppen werden aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** entfernt. Nicht zugewiesen wird im Feld **Zuweisungstyp** angezeigt,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und die Korrekturaufgabe wird in der Liste des nicht zugewiesenen Moduls für die Anwendung Konfigurations-Compliance angezeigt.

Benachrichtigungen, dass die Zuweisung von Datensätzen aufgehoben wird, werden automatisch an Schwachstellenmanager oder Analysten in der Benachrichtigungsgruppe „Zuweisung aufheben“ gesendet. Weitere Informationen zu den Benachrichtigungen und den Eigenschaften für diese Funktion finden Sie unter Zuweisungen von Konfigurations-Compliance-Testergebnisgruppen entfernen.

- Wenn Ihre Anforderung abgelehnt wird, werden der Datensatz für die Statusänderung und der Datensatz für die angeforderte Genehmigung in den Status Abgelehnt geändert.

Hinweis:
Als Schwachstellenadministrator können Sie die Systemeigenschaft `sn_vulc.unassign_test_result_group.approval_required` auf **„false“** festlegen, um den Genehmigungsprozess zu deaktivieren.

Nächste Maßnahme
Navigieren Sie zum Modul Nicht zugewiesen für die Anwendung Konfigurations-Compliance, überwachen Sie alle nicht zugewiesenen Datensätze für Elemente, die möglicherweise in Ihren Bereich fallen, und weisen Sie sie dann neu zu.

Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in Konfigurations-Compliance

Genehmigen Sie Anforderungen zum Entfernen von Korrekturaufgaben aus einer Zuweisungsgruppe oder einem einzelnen Benutzer in der Anwendung Konfigurations-Compliance.

Vorbereitungen
Erforderliche Rolle: sn_vulc.Unassign_approver

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt. Zum Aufheben der Zuweisung von Genehmigungen ist ein Genehmiger in der Genehmigungsgruppe „Genehmiger – Ebene 1“ erforderlich. Standardmäßig wird die Genehmigungsgruppe zum Aufheben der Zuweisung (Zuweisung des Genehmigers CC aufheben – Ebene 1) erstellt, und Anwender, die Teil dieser Gruppe sind, können die Anforderung genehmigen. Standardmäßig enthält diese Gruppe die Genehmigerrolle zum Aufheben der Zuweisung (sn_vulc.unassign_approver). Sie können eine Gruppe ändern oder erstellen und die Genehmigungskonfiguration aktualisieren, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln** > **Change-Anforderung für Korrekturaufgabenfeld** > **Zuweisung der Korrekturaufgabe aufheben**.

Prozedur
1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie ab, indem Sie die entsprechenden Kommentare hinzufügen.

Automatisches Schließen von Testergebnissen

Sie können Testergebnisse (TRs), die stillgelegten Configuration Items (CIs) zugeordnet sind, automatisch schließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Option zum automatischen Schließen zu konfigurieren, navigieren Sie zur Systemeigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs,** und setzen Sie sie auf „true“. Informationen zum automatischen Schließen von TRs im Zusammenhang mit stillgelegten CIs finden Sie unter Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen.

Informationen zum Arbeiten mit deaktivierten Configuration Items finden Sie unter Arbeiten mit deaktivierten Configuration Items in Configuration Compliance.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Arbeiten mit deaktivierten Configuration Items in Configuration Compliance

Außer Betrieb genommene Configuration Items (CIs) werden in den Status „Stillgelegt“, „Archiviert“ oder „Gelöscht“ in Configuration Management Database (CMDB)verschoben. Konfigurations-Compliance enthält Testergebnisse (Testergebnisse, Testergebnisse), die aus CIs bestehen. Wenn der Status eines CI auf „Deaktiviert“ aktualisiert wird, werden die zugehörigen TRs mit dem Substatus „CI außer Betrieb genommen“ geschlossen.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Wenn die CMDB den Status der Lebenszyklusphase eines CI in „Deaktiviert“ ändert, können Sie die zugehörigen TRs automatisch schließen. Weitere Informationen zum automatischen Schließen der zugeordneten TRs finden Sie unter Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen.

Das stillgelegte CI wird schließlich archiviert oder dauerhaft aus CMDBgelöscht.

Auswirkung der Außerkraftsetzung der CIs:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Auswirkung auf erkannte Elemente:** Wenn das CI außer Betrieb genommen wird, wird der zugehörige DI als „CI außer Betrieb genommen“ markiert.
- **Auswirkung auf Testergebnisse:** Wenn der Status eines DI auf „CI stillgelegt“ aktualisiert wird, wird das zugehörige TR geschlossen und der Abschnitt „Hinweise“ wird automatisch aktualisiert.

Hinweis:
Der Status eines DI wird automatisch auf „CI stillgelegt“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Dagegen wird der Status eines TR nur dann auf Geschlossen aktualisiert, wenn die Eigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** auf true festgelegt ist. Weitere Informationen zum automatischen Schließen der zugeordneten TRs finden Sie unter Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen.

Die regelmäßige Aufgabe `Close Test Results for decommissioned CIs` wird täglich für die aktualisierten DIs ausgeführt. Wenn die Konfigurationsoption für das automatische Schließen für stillgelegte CIs aktiviert ist, wird der DI identifiziert, der ein stillgelegtes CI enthält, und das zugehörige TR wird mit dem Substatus „CI stillgelegt“ geschlossen. Wenn alle TRs in einer Korrekturaufgabe geschlossen sind und ihr Substatus „CI außer Betrieb genommen“ ist, wird die Korrekturaufgabe auch mit dem Substatus „Abgebrochen“ geschlossen.

Hinweis:
Wenn ein CI aus dem Status „Stillgelegt“ in den ursprünglichen Status zurückkehrt, wird auch der Eintrag „Erkannte Elemente“ aktualisiert. TRs werden automatisch geöffnet, wenn Daten erneut vom Scanner erfasst werden.

Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen

Wenn Configuration Management Database (CMDB) den Status der Lebenszyklusphase eines Configuration Items (CI) in „Deaktiviert“ ändert, können Sie die zugehörigen Testergebnisse (Testergebnisse, TRs) automatisch schließen.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Um die zugeordneten TRs automatisch zu schließen, müssen Sie die Systemeigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** aktivieren, um TRs, die stillgelegten CIs zugeordnet sind, automatisch zu schließen. Wenn diese Option aktiviert ist, werden neue und vorhandene TRs, die für dasselbe CI gemeldet werden, automatisch erstellt oder im Status „Geschlossen“ aktualisiert. Diese basieren auf der Asset-ID in der Scanner-Payload und dem Eintragsstatus für erkannte Elemente. Weitere Informationen zu den Auswirkungen stillgelegter CIs finden Sie unter Arbeiten mit deaktivierten Configuration Items in Configuration Compliance.

Hinweis:
Der Status eines DI wird bei jeder Aktualisierung des Lebenszyklusstatus eines CI auf „CI außer Betrieb genommen“ aktualisiert. Dagegen wird der Status eines TR nur dann auf Geschlossen aktualisiert, wenn die Systemeigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** und filtern Sie nach `sn_vulc.auto_close_test_results_linked_to_retired_CIs` in der Namensspalte.
2. Wählen Sie die Eigenschaft aus.
3. Um Testergebnisse, die stillgelegten CIs zugeordnet sind, automatisch zu schließen, legen Sie den Wert der Eigenschaft auf „true“ fest.

Veraltete Testergebnisse in werden automatisch geschlossen Konfigurations-Compliance

Sie können die Funktion Veraltete Testergebnisse automatisch schließen aktivieren, um ältere Testergebnisse, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden, automatisch zu schließen. Wenn Sie diese Testergebnisse in **den Status „Geschlossen – Veraltet“** verschieben, verringert sich die Anzahl der aktiven Testergebnisse und Korrekturaufgaben in Ihrer Instanz und hilft Ihnen, Assets in Ihrem Configuration Management Database (CMDB)abzugleichen.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Übersicht

Mit dem Modul Veraltete Testergebnisse automatisch schließen können Sie ältere, veraltete Testergebnisse, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden, automatisch schließen. Testergebnisse werden basierend auf den von Ihnen im Bedingungsgenerator festgelegten Bedingungen in den Status **Geschlossen – Veraltet** verschoben.

Wichtige Begriffe

Testergebnis

Testergebnisse sind importierte Ergebnisse aus Bibliotheken von Konfigurationstests, die Frameworks, Richtlinien und autoritativen Quellen zugeordnet sind, die definieren, wie eine Klasse von Technologie-Assets gesteuert werden soll. Die Anwendung Konfigurations-Compliance berechnet die Testergebnisse nicht, importiert sie jedoch mit Drittanbieterintegrationen.

Datum des letzten Asset-Scans

Bezieht sich auf den Wert der Spalte „Datum des letzten Konfigurations-Compliance-Scans“ der Tabelle „Erkanntes Element“, die sich auf das Testergebnis bezieht. Dieses Datum bezieht sich auf das aktuelle Datum und die Uhrzeit, zu der ein Asset zuletzt von einem Drittanbieter-Scanner gescannt wurde.

Datum des letzten Fehlschlags

Bezieht sich auf das Datum der Spalte „Zuletzt angezeigt“ der Tabelle „Testergebnisse“, wenn der Feldwert „ **Ergebnis“** [fehlgeschlagen] ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veraltete Testergebnisse

Bezieht sich auf Testergebnisse in Ihrer Instanz, die veraltet sind und von Integrationsscans von Drittanbietern längere Zeit nicht gefunden, aktualisiert oder erkannt wurden.

Zuletzt gefundene Testergebnisse

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner eines Drittanbieters bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuellste oder späteste Datum (vor Tagen), an dem Testergebnisse erneut vom Scanner gefunden wurden. Dieser Parameter kann konfiguriert werden.

Anwendungsfall

Manchmal werden Assets (Konfigurationselemente) in Ihrer Umgebung außer Betrieb genommen oder von Scannern von Drittanbietern gelöscht. In diesem Fall werden die Konfigurationstestergebnisse der Assets in der Anwendung Konfigurations-Compliance nicht durch importierte Erkennungen aktualisiert, sondern werden inaktiv (veraltet).

Um die Anzahl der aktiven Testergebnisse (TRs) und Korrekturaufgaben (RTs) in Ihrer Instanz zu reduzieren, aktivieren Sie die Funktion Veraltete Testergebnisse automatisch schließen. Diese Funktion schließt automatisch veraltete Testergebnisse, die einen unveränderten Status haben oder nicht kürzlich von Ihren Integrationen importiert wurden.

Angenommen, ein bestimmtes Konfigurationselement (Configuration Item, CI) weist mehrere Asset-IDs auf, und eine dieser IDs wurde in den letzten 90 Tagen nicht bei Erkennungen von einem Drittanbieterscanner importiert. Wenn Sie den Bedingungsgenerator im Modul Veraltete Testergebnisse automatisch schließen so festlegen, dass Testergebnisse geschlossen werden, die in den letzten 90 Tagen nicht gefunden oder aktualisiert wurden, schließt diese Funktion automatisch alle Testergebnisse, die dieser Filterung entsprechen.

Hinweis:
Diese Funktion schließt Testergebniserkennungen nur basierend auf den Filterbedingungen, die Sie im Bedingungsgenerator festgelegt haben und die von Ihren Drittanbieter-Scanner-Integrationen erkannt werden.

Feld Lösung

Um zwischen den Erkennungen zu unterscheiden, die von Drittanbieterscannern geschlossen werden, z. B. den Produkten Qualys und Tenable.io, und der Funktion Veraltete Testergebnisse automatisch schließen in Ihrer Instanz, weist ein neuer Wert für das Feld **Lösung**, [Closed-Stale], den Wert auf wurde hinzugefügt. **„Geschlossen – Veraltet“** gibt an, dass ein TR von der Funktion zum automatischen Schließen geschlossen wurde. **„Geschlossen“** oder **„Fest geschlossen“** gibt an, dass ein TR von einem Scanner geschlossen wurde.

Rollup von TR-Status zu TRGs mit der Funktion „Automatisches Schließen“.

Statusfortschritt und Rangfolge für Testergebnisse: **Öffnen** > **Abgeschlossen** > **Fest-Geschlossen** > **Als veraltet geschlossen**.

1. Wenn TRs in einer TRG **„Offen“**sind, wird der TRG-Status nicht geändert.
2. Wenn mindestens ein TR **Geschlossen – Behoben** und die übrigen **Geschlossen – Veraltet**sind, wechselt der Status des TRG zu **Geschlossen – Behoben**.
3. Wenn alle TRs in einer TRG **Geschlossen – Veraltet**sind, wechselt der Status des TRG zu **Geschlossen – Abgebrochen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Integrationen

Weitere Informationen zu Drittanbieterintegrationen, die diese Funktion unterstützen, finden Sie unter Qualys Vulnerability Integration verstehen und Tenable.io -Integrationen mit den Anwendungen Vulnerability Response und Konfigurations-Compliance.

Verwenden Sie veraltete Testergebnisse automatisch schließen in Konfigurations-Compliance

Aktivieren Sie Veraltete Testergebnisse automatisch schließen (Veraltete Testergebnisse automatisch schließen), um ältere Testergebnisse basierend auf von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

Vorbereitungen

Weitere Informationen zu dieser Funktion, zu wichtigen Begriffen und zu allen Setups, die für Ihre Drittanbieterintegrationen zum Importieren von Testergebnisdaten erforderlich sind, finden Sie unter Veraltete Testergebnisse in werden automatisch geschlossen Konfigurations-Compliance.

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Veraltete Testergebnisse automatisch schließen**.
2. Füllen Sie die Felder aus

Feld	Wert
Name	Name für diesen Konfigurationsdatensatz.
Aktiv	Wenn diese Option ausgewählt ist, ist dieser Datensatz aktiv, und alle Testergebnisse werden automatisch geschlossen, die seinen Filterkriterien entsprechen.
Veraltete TRs für zurückgestellte TRs ignorieren	Wenn diese Option ausgewählt ist, werden alle TRs ignoriert und nicht geschlossen, die den Status **„Wird überprüft“** oder **„Zurückgestellt“** zugeordnet sind. Wenn Sie diese Option deaktivieren, werden alle TRs geschlossen, die Ihren Kriterien entsprechen.
Ausführungsreihenfolge	100 ist der Standardwert. Dieser Wert bestimmt die Reihenfolge der Ausführung in aufsteigender Reihenfolge für jeden Konfigurationsdatensatz, der zum Suchen und Markieren von veralteten Testergebnissen verwendet wird.
Beschreibung	Eine Beschreibung für diesen Datensatz. Dieser Text hilft Ihnen möglicherweise, es leichter wiederzufinden, wenn Sie eine größere Anzahl von Datensätzen erstellen.
Bedingung	Die Filterbedingungen zum Suchen von TRs, die geschlossen werden sollen. Der Standardfilter ist **Erkanntes Element** > **Zuletzt gescannt** > .

3. Klicken Sie auf **Absenden**.

Die regelmäßige -Aufgabe *Auto-Close Stale Test Results*wird täglich ausgeführt. Dieser Auftrag identifiziert die TRs basierend auf den von Ihnen angegebenen Bedingungen und überführt diejenigen, die übereinstimmen in Status: **Geschlossen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem TRs als Status: **Geschlossen – Veraltet**markiert wurden und der Scanner diese TRs erneut findet, werden die Testergebnisse erneut geöffnet, und die Status werden zurück in**Offen geändert**.

Wenn ein TR als Status: **Geschlossen – Veraltet**markiert ist und der Scanner feststellt, dass es behoben wurde (Lösung: **Behoben**), wechselt das TR zu Status: **Geschlossen** Lösung: **Behoben**. TRs mit **Ergebnis„ Bestanden"** verbleiben im Status: **Geschlossen** Lösung: **Behoben**. Die Status werden auch für Korrekturaufgaben zusammengefasst, wie in der folgenden Liste beschrieben:

a. Wenn TRs in einer Korrekturaufgabe **Offen**sind, wird der Status der Korrekturaufgabe nicht geändert.

b. Wenn mindestens ein TR Status: **Geschlossen** Lösung: **Behoben ist** und der Rest **Geschlossen – Veraltet**ist, geht der Status der Korrekturaufgabe in **Geschlossen** Lösung: **Behoben über**.

c. Wenn alle TRs in einer Korrekturaufgabe **Geschlossen** Lösung: **Behoben sind**, geht der Status TRG in Status: **Geschlossen** Lösung: **Abgebrochen über**.

Weitere Informationen zu Statusübergängen finden Sie unter Testergebnis- und Statusübergänge für Korrekturaufgaben in der Anwendung Konfigurations-Compliance ..

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das mit einer Korrekturaufgabe verbundene Problem ohne weitere Analyse sofort geschlossen werden kann, können Sie die Funktion **Schließen** verwenden.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin
- sn_vulc.remediation_owner

Hinweis:
Mit der Rolle sn_vulc.remediation_owner können Sie Korrekturaufgaben, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind, neu zuweisen oder schließen.

Warum und wann dieser Vorgang ausgeführt wird

Ab v15.0 von Konfigurations-Compliancewurde die Schaltfläche **Schließen** für Korrekturaufgaben entfernt.

Wenn Sie eine Korrekturaufgabe lösen, werden die Lösungsnotizen in den Arbeitsnotizen aller zugehörigen Testergebnisse angezeigt.

Prozedur

1. Öffnen Sie den Datensatz für die Korrekturaufgabe.
2. Wählen Sie die Schaltfläche **Schließen** aus.
3. Beschreiben Sie, warum das Problem im Popup-Fenster geschlossen wird.
4. Wählen Sie **Schließen**.

Zugehörige Informationen

Konfigurations-Compliance Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausnahme für eine Korrekturaufgabe anfordern und genehmigen

Sie können anfordern, die Korrektur einer Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen. Benutzer, die Teil der Genehmigergruppe sind, können Ausnahmeanforderungen genehmigen.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Informationen zum Anfordern oder Genehmigen von Ausnahmeanforderungen finden Sie unter:

- Fordern Sie eine Ausnahme für eine Korrekturaufgabe in an Konfigurations-Compliance
- Genehmigen Sie eine Ausnahmeanforderung in Konfigurations-Compliance

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail mit dem Hinweis, dass eine Ausnahme angefordert wurde.

Ab v14.11 von Konfigurations-Compliancekönnen Sie die Zeitrahmen für die Genehmigung von Ausnahmen konfigurieren und E-Mail-Benachrichtigungen nach einer festgelegten Anzahl von Tagen für den Genehmiger und die anfordernde Person senden. Wenn eine Anforderung ausgelöst wird, ändert sich das Testergebnis in den Status Wird überprüft, und ein Datensatz für die Statusänderung wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das Testergebnis auf den Status Offen zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für die Ausnahmeverwaltung.

Fordern Sie eine Ausnahme für eine Korrekturaufgabe in an Konfigurations-Compliance

Fordern Sie eine Ausnahme an, um die Korrektur einer Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort behoben werden kann.

Vorbereitungen
Erforderliche Rolle: sn_vulc.remediation_owner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wichtig:
Sie können eine Ausnahme anfordern für:

- Korrekturaufgaben in Vulnerability Manager Workspace und IT Remediation Workspace. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.
- mehrere Testergebnisse gleichzeitig aus Vulnerability Manager Workspace. Weitere Informationen finden Sie unter Massenausnahme im Arbeitsbereich des Schwachstellenmanagers anfordern.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben** > **Alle Aufgaben**.
2. Wählen Sie die Korrekturaufgabe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Klicken Sie im Formular „Korrekturaufgabe“ **auf Ausnahme anfordern**.

   Hinweis:
   Je nachdem, ob Vulnerability Response oder GRC: Richtlinien- und Compliance-Management in ausgewählt ist **Konfigurations-Compliance** > **Ausnahmenverwaltung** Im Bildschirm „Ausnahme anfordern“ ändert sich das Formular „Ausnahme anfordern“. Siehe Konfigurieren Sie die Ausnahmeverwaltung für Konfigurations-Compliance

4. Wenn Vulnerability Response im Bildschirm „Ausnahmeverwaltung“ ausgewählt ist, gehen Sie wie folgt vor:

   a. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in ausgewählten Dauer liegen **Alle** > **Konfigurations-Compliance** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, wird die Korrekturaufgabe in den Status „Offen“ zurückversetzt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Ab Version 14.7 von Konfigurations-Compliance (CC) ändert sich der Status der Korrekturaufgabe von Offen in Zurückgestellt, wenn sie von einem Scanner erneut geöffnet wird, bevor das Ausnahmefenster abläuft. Diese Funktionalität ist standardmäßig deaktiviert. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft `sn_vulc.auto_defer_test_result_in_active_exc` auf „true“ fest. Außerdem bleibt das Datum für „Zurückgestellt bis“ auch dann erhalten, wenn die Korrekturaufgabe nach dem Ablaufdatum erneut geöffnet wird.
Grund	Grund für die Ausnahme. Die Auswahlmöglichkeiten lauten wie folgt: ▪ Risiko akzeptiert ▪ Warten auf Wartungsfenster ▪ Behebung nicht verfügbar ▪ Ausgleichende Steuerung vorhanden ▪ Sonstige Informationen zum Hinzufügen neuer Gründe finden Sie unter Definieren Sie Zuordnungen von Richtliniengrund.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Korrektur aktualisiert werden.

b. Senden Sie die Ausnahmeanforderung, indem Sie **auf Genehmigung anfordern**klicken.

Ergebnisse

Der Status der Korrekturaufgabe ändert sich in Wird überprüft. Verwenden Sie die Registerkarte **Change-Genehmigung**, um den Status der Ausnahmeanforderung zu verfolgen.

Fordern Sie eine Verlängerung für eine Korrekturaufgabe an

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht ist. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben**.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status „Zurückstellen“ abläuft und die Korrekturaufgabe erneut aktiviert wird.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Genehmigung anfordern**.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Korrekturaufgabe erneut verlängert wird, erhöht sich die Anzahl der Zurückstellungen verlängern im Back-End.

Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Konfigurations-Compliance

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht ist. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Arbeitsbereiche Vulnerability Response anfordern. Weitere Informationen finden Sie unter Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an.

Hinweis:

Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Ausnahmeregeln**.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern**aus.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein. Zur Auswahl stehen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und Zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Korrekturaufgaben aktualisiert. Außerdem wird bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers eine E-Mail ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Wenn eine zurückgestellte Ausnahmeregel erneut verlängert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.

Fordern Sie mit eine Ausnahme für Korrekturaufgaben an GRC: Richtlinien- und Compliance-Management

Fordern Sie mit der Funktion zur Verwaltung von Richtlinienausnahmen GRC in der Anwendung Richtlinien- und Compliance-Management innerhalb von Konfigurations-ComplianceRichtlinienausnahmen an.

Vorbereitungen

Bevor Sie die Integration für Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Richtlinien- und Compliance-Management von ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vulc.remediation_owner

Sie können Ausnahmen auch in der klassischen Anwenderoberfläche anfordern.

Warum und wann dieser Vorgang ausgeführt wird

Wichtig:
Als Administrator und Korrekturbesitzer können Sie im Vulnerability Manager Workspace bzw. IT Remediation Workspace eine Richtlinienausnahme für eine Korrekturaufgabe (Remediation Task, RT) anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Anwendungselemente** (oder **Korrekturaufgaben**) >**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular **auf Ausnahme anfordern**.
3. Wenn GRC: Richtlinien- und Compliance-Management im Bildschirm Ausnahmeverwaltung ausgewählt ist, gehen Sie wie folgt vor.

   a. Füllen Sie die Felder des Formulars aus.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Richtlinie	Richtlinie für Schwachstellenmanagement, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und wann der Status des angreifbaren Elements oder der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ wechselt. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)**, die Sie für die Richtlinie in Richtlinien und Compliance festgelegt haben, nicht überschreiten. Weitere Informationen finden Sie unter Richtlinie erstellen .
Grund	Grund für das Anfordern einer Ausnahme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Remediation ausgefüllt werden.

b. Senden Sie die Ausnahmeanforderung, indem Sie **auf Genehmigung anfordern**klicken.
Der Status der Korrekturaufgabe ändert sich in Wird überprüft, und es wird eine Richtlinienausnahme erstellt. Verwenden Sie die Registerkarte **Change-Genehmigung**, um den Status der Ausnahmeanforderung zu verfolgen.

c. Zeigen Sie die Richtlinienausnahme an, indem Sie auf die zugehörige Liste Richtlinienausnahmen klicken.

d. Klicken Sie auf die Nummer der Richtlinienausnahme.

e. Wählen Sie im Feld **Genehmiger** den Namen des Genehmigers aus.

f. Klicken Sie auf die Registerkarte Quelle, und wählen Sie im Feld **Kontrollziel** ein Kontrollziel aus.

g. Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie die Risikobewertung im Feld **Risikobewertung** aus.

h. Speichern Sie das Formular.

i. Klicken Sie auf die Registerkarte **Betroffene Steuerungen**.

j. Fügen Sie die Steuerungen hinzu, indem Sie auf **Hinzufügen**klicken.

k. Speichern Sie das Formular.

Hinweis:
Sie können eine Compliance-Überprüfung veranlassen, indem Sie **auf Compliance-Überprüfung anfordern**klicken.

Das Genehmigungsformular wird an den Genehmiger gesendet.

Der Genehmiger kann entweder die Anforderung genehmigen, indem er auf **Genehmigen** klickt, oder eine zusätzliche Genehmigung anfordern, indem er **auf Zusätzliche Genehmigung anfordern**klickt.

Der Datensatzstatus ändert sich in Zurückgestellt. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die Registerkarte **Zurückstellung** enthält zusätzliche Hinweise zum Datensatz.

Hinweis:
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

4. Klicken Sie auf **Absenden**.
Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Korrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigen Sie eine Ausnahmeanforderung in Konfigurations-Compliance

Genehmigen Sie Ausnahmeanforderungen für Korrekturaufgaben, die nicht sofort behoben werden können. Sie müssen diese Anforderungen auf Risiken bewerten und dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Wichtig:
Als Administrator oder Analyst können Sie im Arbeitsbereich des Schwachstellenmanagers eine Ausnahmeanforderung genehmigen oder ablehnen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Vorbereitungen
Erforderliche Rolle: sn_vulc.exception_approver

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Meine Genehmigungen**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Hinweis:
Im Falle eines zweistufigen Genehmigungs-Workflows wird die Anforderung nach der Genehmigung auf erster Ebene zur weiteren Genehmigung an die zweite Ebene übermittelt. Wenn auf der zweiten Ebene keine Benutzer vorhanden sind, wird die Anforderung nach der Genehmigung auf der ersten Ebene automatisch genehmigt.

Nachdem die Anforderung genehmigt wurde, wird die Korrekturaufgabe in den Status „Zurückgestellt“ versetzt. Im Falle einer Ablehnung wird die Korrekturaufgabe in ihren früheren Status zurückversetzt.

Definieren Sie Zuordnungen von Richtliniengrund

Sie können die Grundauswahlmöglichkeiten so definieren, dass sie für jeden Anwender verfügbar sind, der eine Ausnahme anfordert.

Vorbereitungen
Erforderliche Rolle: sn_vul.compliance.manager und sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**.

Hinweis:
Sie können entweder einen Grund aus den in der Tabelle „Grundauswahlmöglichkeiten“ verfügbaren Gründen auswählen oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Registrierung Container Vulnerability Response – CVIT-Integration.
3. Um eine vorhandene Grundauswahl hinzuzufügen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie in der Liste „Grund – Auswahlmöglichkeiten“ auf **Neu**.
   b. Klicken Sie auf das Lupensymbol, um einen Grund auszuwählen.
4. Um der Tabelle „Grundauswahlmöglichkeiten“ neue Gründe hinzuzufügen, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Liste „Grund-Auswahlmöglichkeiten“ auf **Neu**.

b. Klicken Sie auf das Lupensymbol.

c. Klicken Sie auf **Neu**.

d. Füllen Sie die Felder des Formulars aus.

Formular „Grund – Auswahlliste“.

Feld	Beschreibung
Bezeichnung	Eindeutige Bezeichnung für diese Auswahl.
Wert	Eindeutiger Wert für diese Auswahl. Dieser Wert wird in der Tabelle „Zuordnungen der Richtlinienausnahmegründe“ für die jeweiligen Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie im Filternavigator sn_sec_cmn_policy_reason_mapping.LIST ein.
Bestellung	Reihenfolge für diese Auswahl. Die Gründe werden basierend auf dieser Nummer sortiert.
Standard	Option, um anzugeben, dass diese Grundauswahl verfügbar ist, wenn eine bedarfsgesteuerte Richtlinienausnahme angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, sind alle Grundauswahlmöglichkeiten verfügbar, bei denen das Feld **„Standard“** ausgewählt ist.
Aktiv	Option zum Anzeigen der Auswahl in der Liste der Grundauswahlmöglichkeiten.

5. Klicken Sie auf **Absenden**.

Berichterstellung und Analytics für Konfigurations-Compliance

Die folgenden Berichte werden für die Überwachung bereitgestellt.

Zeigen Sie Richtlinien, CIs, Tests und Testergebnisse in den Konfigurations-Compliance Übersichtsberichten an.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Konfigurations-Compliance Berichterstellung

Die Homepage Konfigurations-Compliance bietet eine Ausführungsansicht für Richtlinien, CIs, Tests und Testergebnisse, damit Sicherheitsmitarbeiter Problembereiche schnell erkennen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können. Konfigurations-Compliance Signifikanzdiagramme können nach Bedarf hinzugefügt werden. Sie können -bezogene Informationen Konfigurations-Compliance auch mithilfe der globalen Suchfunktion zurückgeben.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

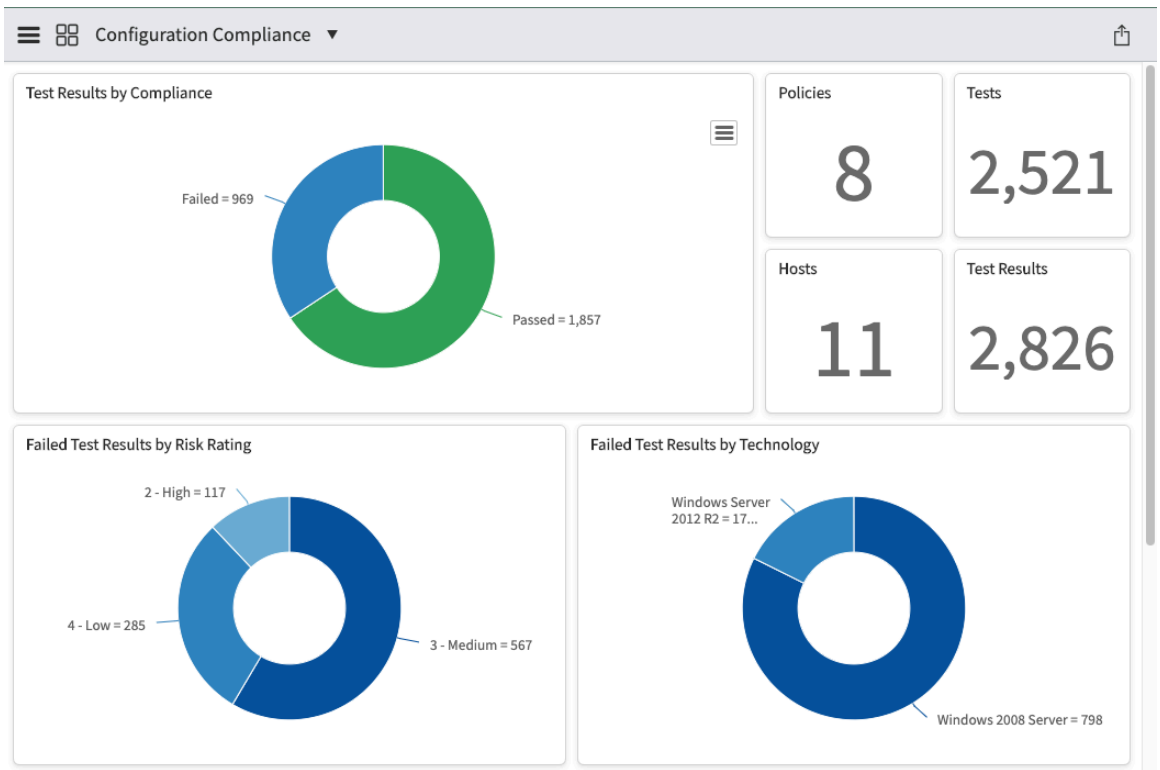
Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

In jedem Diagramm können Sie auf einen beliebigen Teil des Diagramms (Balken, Kreis, Datenpunkt) zeigen, um allgemeine Daten anzuzeigen, die für diesen Teil des Diagramms spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

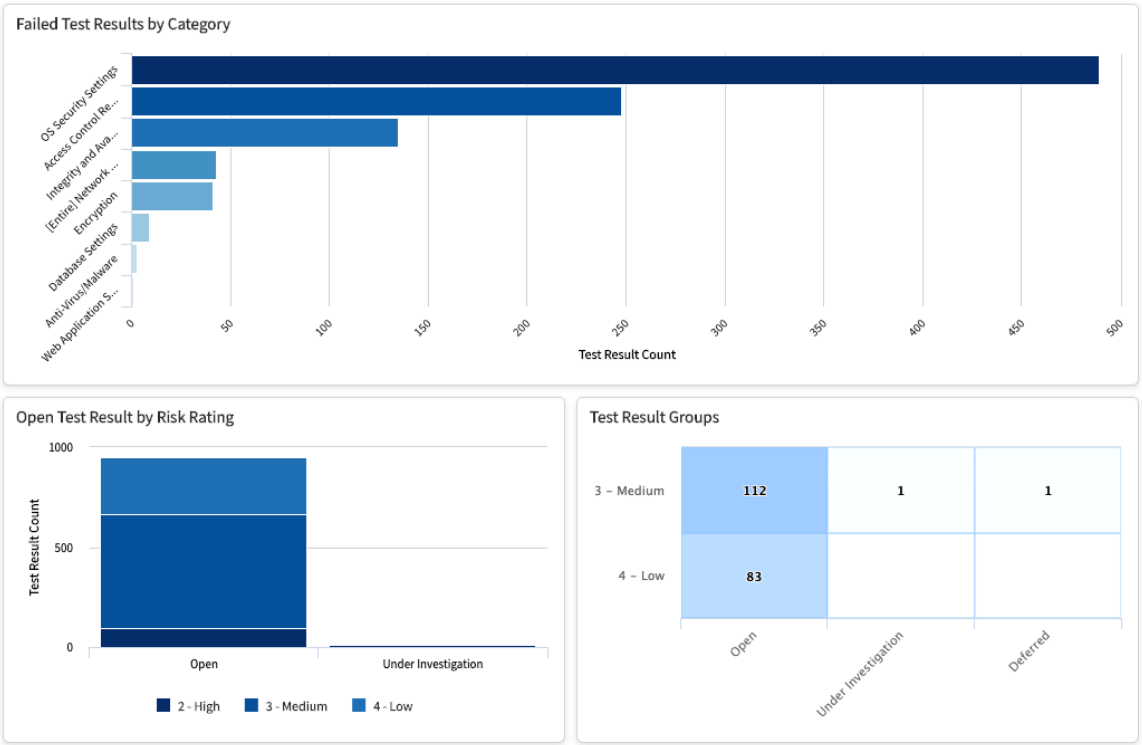
Hinweis:
Jeder mit der Rolle sn_vulc.read kann das Dashboard anzeigen. Jeder mit der Rolle sn_vulc.write oder sn_vulc.admin kann Dashboards erstellen und bearbeiten. Nur sn_vulc.admin kann ein Dashboard löschen.

Berichte mit Schwachstellenübersicht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance-Bericht



Berichte mit Schwachstellenübersicht

Name	Visuell	Beschreibung
Testergebnisse nach Compliance	Ring	Zeigt die Anzahl der offenen Tests an, die bestanden oder fehlgeschlagen sind.
Policen	Nummer	Anzahl der Richtlinien mit Ergebnissen fehlgeschlagener Tests.
Tests	Nummer	Anzahl der Tests mit fehlgeschlagenen Testergebnissen.
Hosts	Nummer	Anzahl der Hosts mit Ergebnissen von fehlgeschlagenen Tests.
Testergebnisse	Nummer	Zeigt die Anzahl der Testergebnisse an.
Ergebnisse fehlgeschlagener Tests nach Risikobewertung	Ring	Zeigt die Anzahl der fehlgeschlagenen Tests nach Risikobewertung an.
Ergebnisse fehlgeschlagener Tests nach Technologie	Ring	Zeigt Modelle mit fehlgeschlagenen Tests an.
Ergebnisse fehlgeschlagener Tests nach Kategorie	Balkendiagramm	Zeigt Kategorien mit den meisten fehlgeschlagenen Testergebnissen an.
Testergebnis nach Risikobewertung öffnen	Balkendiagramm	Zeigt die Anzahl der offenen Testergebnisse nach Risikobewertung an.
Korrekturaufgaben	Diagramm	Zeigt Korrekturaufgaben nach Status und Risikobewertung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Dashboard

Dieser Platform Analytics-Lösung enthält vorgefertigte Performance Analytics - und Reporting -Inhalte zur Verwendung mit anderen Now Platform -Produkten. Platform Analytics-Lösung bietet Einblick in nicht konforme Konfigurationen auf Hostebene und Cloud-Steuerungsebene.

Diese Platform Analytics-Lösung enthält vorgefertigte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten. Diese Platform Analytics-Lösung bietet Einblick in nicht konforme Konfigurationen auf Hostebene und Cloud-Steuerungsebene.

Das Dashboard „Performance Analytics for Configuration Compliance“ enthält mehrere Widgets, die Daten für verschiedene Dimensionen darstellen. Sie bietet einen umfassenden Überblick über Compliance-Trends, Konfigurationsprobleme, Nachbesserungstrends und Ausnahmeverwaltung.

Hinweis:
Das Plugin Performance Analytics for Konfigurations-Compliance muss installiert sein, um das Dashboard Konfigurations-Compliance [PA] im Framework Next Experience anzuzeigen. Wenn dies nicht installiert ist, können Sie das vorhandene Dashboard anzeigen, das mit dem Reporting-Framework erstellt wird.

Performance Analytics für Konfigurations-Compliance aktivieren

Aktivieren Sie die Anwendung ServiceNow Store des Inhaltspakets für Platform Analytics-Lösung.

Vorbereitungen

Aktivieren Sie die vollständige Abonnementversion von Performance Analytics auf der Instanz, auf der Sie diese Platform Analytics-Lösung aktivieren. Sie können Performance Analytics in einer Instanz außerhalb der Produktion aktivieren, ohne ein Abonnement zu erwerben. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

Sie benötigen ein Konto Now Support und die Berechtigung, um -Anwendungen für die betreffenden Instanzen anzufordern. Der Account Now Support und die Instanz müssen Teil desselben Unternehmens sein. Weitere Informationen finden Sie unter Install a ServiceNow Product (ServiceNow-Produkte installieren) im ServiceNow Store.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie Performance Analytics für das Dashboard Konfigurations-Compliance, um Berichte zu den Korrekturaufgaben, dem Compliance-Status, den Korrekturaktionen und den Ausnahmeanforderungen zu generieren.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **ServiceNow Store**.
2. Suchen Sie nach Performance Analytics dem, Konfigurations-Compliance und vergewissern Sie sich, dass Sie über die gültigen Berechtigungen verfügen.
3. Suchen Sie nach Performance Analytics for Configuration Compliance.
4. Installieren Sie die Anwendung.

   Wenn Sie diese Anwendung installieren, aktivieren Sie auch die Anwendung Konfigurations-Compliance.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Performance Analytics für Konfigurations-Compliance -Dashboard anzeigen

Sie können Ihre wichtigsten Konfigurationsprobleme verwalten und schnell beheben, indem Sie die Berichte im Dashboard Konfigurations-Compliance Performance Analytics (PA) anzeigen.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Erforderliche Now Platform-Rollen

Die folgenden Rollen sind für das Dashboard Konfigurations-Compliance Performance Analytics erforderlich:

- -Administrator: Ein -Administrator kann Performance Analytics für Konfigurations-Compliance installieren und aktivieren sowie Änderungen an den Systemeigenschaften vornehmen.
- pa_admin: Ein Performance Analytics-Administrator kann Hintergrundaufträge, Indikatoren, Aufgliederungen, Widgets und Dashboards erstellen und überprüfen. Dieser Administrator kann auch die Datenerfassung einrichten und starten.
- sn_vulc.read: Ein Benutzer mit der Leserolle kann die Dashboard-Daten überprüfen.

Greifen Sie auf das Dashboard Konfigurations-Compliance zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Konfigurations-Compliance** > **Übersicht**.

Wichtig:

Ab Version 14.9 von Konfigurations-Complianceкann dieses Dashboard auch in der Next Experience-UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das **Dashboard** -Symbol. Je nach Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdownliste neben dem Namen des Dashboards. Weitere Informationen finden Sie unter Dashboards im Arbeitsbereich des Schwachstellenmanagers und Dashboards im Arbeitsbereich für IT-Fehlerkorrekturen.

Hinweis:
Wenn Sie sich in Tokyobefinden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit etwas Funktionsverlust.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance [PA] Dashboard-Registerkarten

Registerkarte „Übersicht“

Die Registerkarte **Übersicht** bietet fünf Filter. Diese Filter sind „Asset-Kategorie“, „Cloud-Ressourcentyp“, „Cloud-Service Provider“, „Cloud-Account“ und „Cloud-Region“, die Sie anwenden können, um die Berichte für die angewendeten Filter zu visualisieren. Wenn Sie eine Kategorie auswählen und die Änderungen anwenden, werden alle Widgets aktualisiert, die diese Kategorie unterstützen. Jedes Widget zeigt den angewendeten Filter unten und die Anzahl der angewendeten Filter auf dem Filtersymbol des Widgets an. Klicken Sie in einem Widget auf den Bericht, um die zusätzlichen Informationen auf der Registerkarte **KPI-Details** anzuzeigen. Auf der Registerkarte **KPI-Details** haben Sie folgende Möglichkeiten:

- Zeigen Sie die Datensätze an.
- Vergleichen Sie die Datensätze.
- Ändern Sie den Diagrammtyp.
- Wählen Sie den Datumsbereich aus.
- Zeigen Sie die Trends an, die auf der Dauer basieren.
- Wenden Sie die zusätzlichen Filter einschließlich der Filter an, die auf der Registerkarte **„Übersicht“** nicht verfügbar sind. Ein Beispiel ist das Host-Tag.

Das folgende Beispiel zeigt, wie Sie die Filter auf der Registerkarte **Übersicht** anwenden und die Aktionen auf der Registerkarte **KPI-Details** ausführen können.

Registerkarte „Übersicht“ im Dashboard „Konfigurations-Compliance“.

Registerkarte „Compliance“.

Auf der Registerkarte **„Compliance“** wird der Compliance-Prozentsatz für die verschiedenen maßgeblichen Quellen angezeigt, z. B. Health Insurance Portability and Accountability Act (HIPAA) und Data Interchange Standards Association (DISA). Sie können diese Liste verfeinern, indem Sie die Spaltenheaderfilter verwenden und eine Kategorie auswählen.

Das folgende Beispiel zeigt, wie Sie die Daten auf der Registerkarte **Compliance** filtern können.

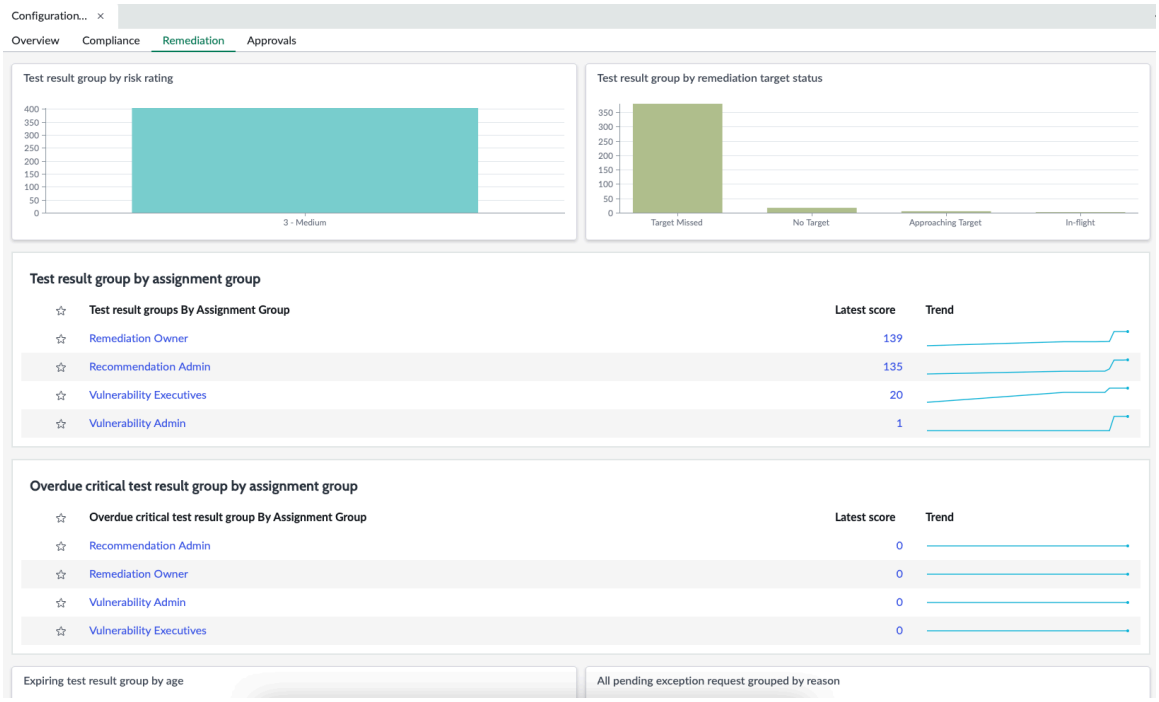
Registerkarte „Compliance“ im Dashboard „Konfigurations-Compliance“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Remediation“

Auf der Registerkarte **„Remediation“** werden Informationen zum Fortschritt der Remediation angezeigt. Sie können diese Registerkarte verwenden, um die Hygiene der Fehlkonfigurationskorrektur anzuzeigen.

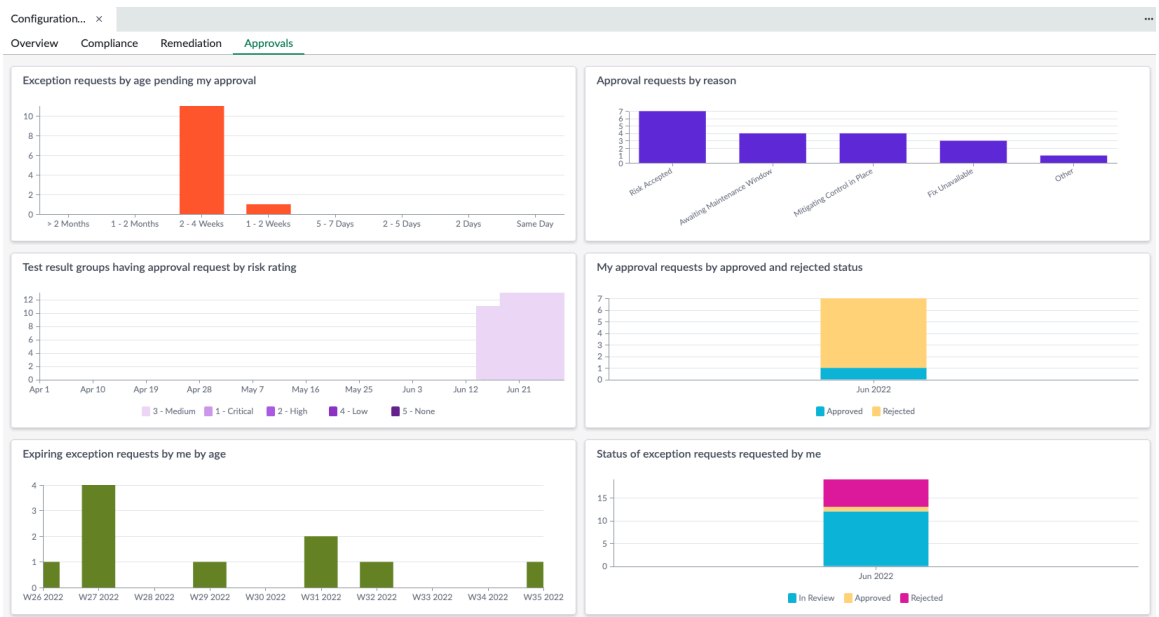
Das folgende Beispiel zeigt die Registerkarte **Nachbesserung**.



Registerkarte Genehmigungen

Die Berichte auf der Registerkarte **Genehmigungen** zeigen die Informationen zu den Ausnahmeanforderungen und deren Genehmigungsstatus an.

Das folgende Beispiel zeigt die Registerkarte **Genehmigungen**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederungen

Die folgenden Aufgliederungen werden von den -Indikatoren verwendet:

- Grund für Zurückstellung
- Alter
- Zuweisungsgruppe
- Korrekturstatus
- Ergebnis
- Risikobewertung
- Asset-Kategorie
- Host-Tag
- Konfigurationstest
- Cloud-Service-Provider
- Cloud-Region
- Cloud-Account
- Cloud-Ressourcentyp

Hinweis:
Das Anpassen von „Alter“ und „Berechnung des Alters geschlossen“ für Testergebnisse kann zu einem starken Anstieg oder Rückgang der Performance Analytics-Berichte (PA) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von Alter und Alter geschlossen für Testergebnisse finden Sie im KB-Artikel KB1703270 .

Filter

Auf der Registerkarte **Übersicht** können Sie die folgenden Filter auf die Widgets anwenden, um die gefilterten Daten zu visualisieren.

Name	Typ	Beschreibung
Asset-Kategorie	Auswahl	Art des Assets. Die vier Optionen sind: • Cloud • Behälter • Infra • OT
Cloud-Ressourcentyp	Auswahl	Typ der Ressource. Ein Beispiel ist ein virtueller Computer. Die Daten im Filter werden gefüllt, wenn Sie die Integration ausführen.

Automatische Übersetzung

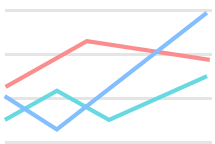
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Cloud-Service-Provider	Auswahl	Service Provider für die Cloud Die drei Optionen sind: • Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)
Cloud-Account	Auswahl	Account-ID, die erstellt wird, wenn ein Account in einem Cloud-Service erstellt wird. Beispiel: AWS. Die Account-ID-Daten werden in den Filter eingetragen, wenn Sie die Integration ausführen.
Cloud-Region	Auswahl	Standort, an dem die Ressource gehostet wird.

Hinweis:
Sie können mehrere Optionen aus den Filtern auswählen und **Anwenden**wählen. Jedes Widget zeigt die Filter, die angewendet werden, und die Filter, die nicht angewendet werden. Der Bericht wird abhängig von den verfügbaren Daten generiert. Das Widget zeigt auch die Anzahl der unterstützten Filter an.

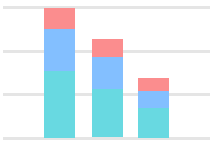
Datenvisualisierungen

Visualisierungen der Registerkarte „Übersicht“.

Berichtname	Typ	Quelltabelle	Beschreibung
Compliance-Trend	Liniendiagramm 	Testergebnisse	Informationen zum Compliance-Trend: • Ressourcen: Gesamtzahl der Ressourcen, die im System verfügbar sind. • Fehler: Anzahl der Ressourcen mit mindestens einem fehlgeschlagenen Testergebnis. • Bestanden: Anzahl der Ressourcen, bei denen alle Testergebnisse den Status „Bestanden“ aufweisen.
Korrekturaufgabe	Einzelne Punktzahl	Testergebnisse	Anzahl der Korrekturaufgaben, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

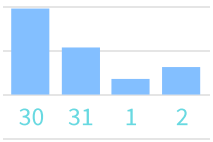
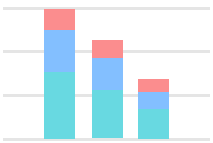
Visualisierungen der Registerkarte „Übersicht“. (Fortsetzung)

Berichtname	Typ	Quelltabelle	Beschreibung
			im System vorhanden sind und sich in einem aktiven Status befinden.
Kritische Korrekturaufgaben kurz vor der Fälligkeit	Einzelne Punktzahl	Testergebnisse	Anzahl der Korrekturaufgaben, bei denen die Risikobewertung „kritisch“ ist und der Korrekturstatus „Ziel erreicht“ lautet.
Testergebnisse nach Risikobewertung	Balkendiagramm 	Testergebnisse	Testergebnisse im Status „Fehlgeschlagen“, die nach der Risikobewertung gruppiert sind.
Testergebnisse nach Alter	Balkendiagramm	Testergebnisse	Testergebnisse im Status „Fehlgeschlagen“, gruppiert nach dem Zeitpunkt der Erstellung der Testergebnisse.

Automatische Übersetzung

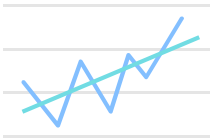
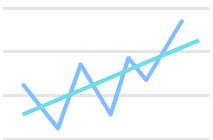
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Übersicht“. (Fortsetzung)

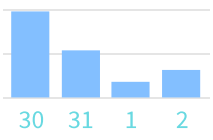
Berichtname	Typ	Quelltabelle	Beschreibung
			**Hinweis:** Das Anpassen von „Alter“ und „Berechnung des Alters geschlossen“ für Testergebnisse kann zu einem starken Anstieg oder Rückgang der Performance Analytics-Berichte (PA) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von Alter und Alter geschlossen für Testergebnisse finden Sie im KB-Artikel KB1703270 .
Geschlossene Testergebnisse nach Einhaltung des Korrekturziels	Balkendiagramm 	Testergebnisse	Testergebnisse im Status „Bestanden“, was bedeutet, dass der Test geschlossen ist.
Überfällige kritische Testergebnisse nach Zuweisungsgruppe	Liste und Punktzahl	Testergebnisse	Anzahl der Testergebnisse, bei denen die Risikobewertung „kritisch“ und der Korrekturstatus „Ziel verfehlt“ ist. Der Bericht gibt an, dass sich die Testergebnisse im Status „Offen“ befinden. Wenn die Testergebnisse das Zieldatum der Korrektur überschreiten, gilt dies als überfällig.
Überfällige Testergebnisse – Services	Liste, Punktzahl und Trend	PA-Dashboard-Datenbankansicht für Services	Anzahl der Testergebnisse für Services, bei denen der Korrekturstatus „Ziel verfehlt“ lautet. Dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Übersicht“. (Fortsetzung)

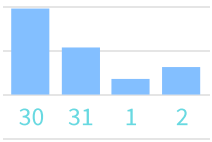
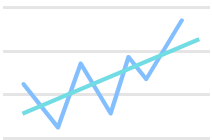
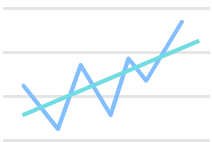
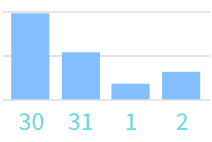
Berichtname	Typ	Quelltabelle	Beschreibung
			Bericht zeigt auch den Namen der Services oder Abteilungen mit den höchsten Testergebnissen an.
Überfällige Testergebnisse – Serviceverantwortliche	Liste, Punktzahl und Trend 	PA-Dashboard-Datenbankansicht für Services	Anzahl der Testergebnisse für Serviceverantwortliche, deren Korrekturstatus „Ziel verfehlt“ lautet. Dieser Bericht zeigt auch den Namen der Services oder Abteilungen mit den höchsten Testergebnissen an.

Visualisierungen der Registerkarte „Nachbesserung“.

Titel	Typ	Quelltabelle	Beschreibung
Korrekturaufgabe nach Risikobewertung	Balkendiagramm 	Nachbesserungsaufgabe	Aufgliederung der Risikobewertungen aller Testergebnisgruppen, die sich im Status „Aktiv“ befinden.
Korrekturaufgabe nach Status des Korrekturziels	Balkendiagramm	Nachbesserungsaufgabe	Aufgliederung der Korrekturziele aller Testergebnisgruppen, die das Ziel verfehlt haben, kein Ziel haben und sich dem Ziel nähern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

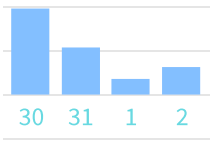
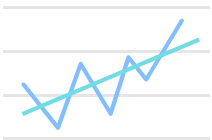
Visualisierungen der Registerkarte „Nachbesserung“. (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			
Korrekturaufgabe nach Zuweisungsgruppe	Liste, Punktzahl und Trend 	Nachbesserungsaufgabe	Aufgliederung der Korrekturaufgaben basierend auf einer Zuweisungsgruppe.
Überfällige kritische Korrekturaufgabe nach Zuweisungsgruppe	Liste, Punktzahl und Trend 	Nachbesserungsaufgabe	Aufgliederung der Korrekturaufgaben basierend auf einer Zuweisungsgruppe. Diese Korrekturaufgaben haben eine Risikobewertung als „kritisch“, und ihr Korrekturziel wurde nicht erfüllt.
Auslaufende Korrekturaufgaben nach Alter	Balkendiagramm 	Korrekturaufgabe	Korrekturaufgaben, die innerhalb eines bestimmten Zeitraums ablaufen. Es können maximal 10 Dauer-Buckets erstellt werden.
Alle ausstehenden Ausnahmeanforderungen nach Grund gruppiert	Balkendiagramm	Genehmigung der Statusänderung	Status-Change-Genehmigungsanforderungen, die nach dem Grund für

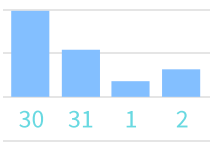
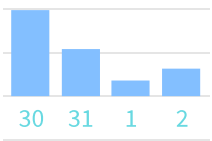
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Nachbesserung“. (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			die Ausnahme gruppiert sind.
Kritische Ausnahmen bei Testergebnissen nach Zuweisungsgruppe	Liste, Punktzahl und Trend 	Testergebnisse	Testergebnisse, die sich im Status „Zurückgestellt“ und „Kritisch“ befinden und basierend auf der Zuweisungsgruppe gruppiert sind.

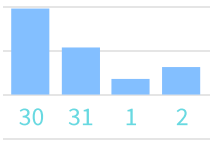
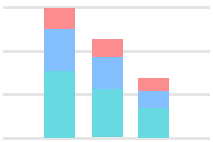
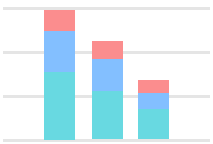
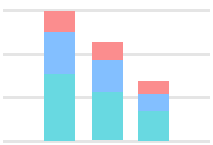
Visualisierungen der Registerkarte „Genehmigungen“.

Berichte	Typ	Quelltabelle	Beschreibung
Ausnahmeanforderungen nach Alter, für die meine Genehmigung aussteht	Balkendiagramm 	Genehmigung	Ausnahmeanforderungen, die von Ihnen erstellt wurden und deren Genehmigung aussteht. Die Anforderungen werden nach der Dauer der Anforderung gruppiert.
Genehmigungsanforderungen nach Grund	Balkendiagramm 	Genehmigung der Statusänderung	Status-Change-Genehmigungsanforderungen für das Erstellen einer Ausnahme und geben Sie den Grund für die Ausnahme an.
Korrekturaufgaben mit Genehmigungsanforderung nach Risikobewertung	Balkendiagramm	Nachbesserungsaufgabe	Korrekturaufgaben, die eine Genehmigungsanforderung haben, die auf der Kritikalität basiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Genehmigungen“. (Fortsetzung)

Berichte	Typ	Quelltabelle	Beschreibung
			
Meine Genehmigungsanforderungen nach Status „Genehmigt“ und „Abgelehnt“	Balkendiagramm 	Genehmigung der Statusänderung	Ausnahmeanforderungen, die nach den Status „Genehmigt“ und „Abgelehnt“ gruppiert sind.
Ablaufende Ausnahmeanforderungen von mir nach Alter	Balkendiagramm 	Genehmigung der Statusänderung	Ausnahmeanforderungen, die in den kommenden Wochen ablaufen. Die Ausnahmeanforderungen werden basierend auf Wochen gruppiert. Wenn eine Ausnahmeanforderung erstellt wird, wird ein Datum für die Gültigkeit der Ausnahmeanforderung ausgewählt. Die Berechnung des Alters der Anforderung basiert auf diesem Datum.
Status der von mir angeforderten Ausnahmeanforderungen	Balkendiagramm 	Genehmigung der Statusänderung	Ausnahmeanforderungen, die von Ihnen erstellt werden und die nach den folgenden Status gruppiert sind: • Wird überprüft • Genehmigt • Abgelehnt

Framework für zusammengefasste Berichte für Konfigurations-Compliance

Mit dem Framework für aggregierte Berichte können Sie Berichte für die Daten erstellen, die komplexe und zeitaufwändige On-the-fly-Abfragen beinhalten, um eine bessere Leistung zu erzielen.

Das Framework für aggregierte Berichte verbessert die Leistung durch:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ressourcenverbrauch und Berichte werden schneller erstellt,
- die Daten zusammenzufassen und Zusammenfassungen und Aufgliederungen wiederzuverwenden (Gruppieren nach) und
- Dadurch werden weniger Abfragen an die Datenbank durchgeführt

Wenn Sie mehr als eine Million Konfigurationstestergebnisse haben, verwenden Sie zusätzlich zu den Standardberichten das Framework für aggregierte Berichte.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- Now Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics -Administrator (pa_admin): Zusammenfassungen, Widgets und Dashboards überprüfen Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- VR-Lesevorgang (sn_vul_cmn.read): Überprüfen Sie die Daten in „Zusammenfassungen“ und „Aggregierte Ergebnisse“.
- Schwachstellenanalyst (sn_vul.vulnerability_analyst): Aggregierte Ergebnisse überprüfen.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Konfigurations-Compliance Referenzinformationen

Bei der Aktivierung der Anwendung Konfigurations-Compliance werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen, geplanten Aufgaben und Anwenderrollen.

Die folgenden Themen enthalten Referenzinformationen, Problembehandlung sowie Felddaten in den Formularen und Datensätzen in Konfigurations-Compliance.

- Mit Konfigurations-Compliance installierte Komponenten
- Formularfelder „Testergebnis“.
- Konfigurations-Compliance Importprobleme werden gelöst
- Ändern Sie das Startdatum der Qualys PC-Ergebnisse

Mit Konfigurations-Compliance installierte Komponenten

Bei der Aktivierung des Konfigurations-Compliance-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

Ab v15.1.5 von Konfigurations-Complianceсind die am häufigsten verwendeten Systemeigenschaften jetzt in der Anwendung Konfigurations-Compliance zugänglich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Konfigurations-Compliance**Eigenschaften**.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Zeigen Sie gefilterte Listen für mit einer Anwendung installierte Komponenten an

Filtern Sie die Tabelle „Anwendungsdateien“, damit nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert wurden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert werden, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie diese Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator **sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **AND**und dann aus. **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Konfigurations-Compliance-Administrator [sn_vulc.admin]	Kann Anwendungseigenschaften, Konfiguration, Update-Regeln und Integrationen der Anwendung Konfigurations-Compliance ändern. Ab v15.0 können	sn_vulc.write **Hinweis:** Erbt die Rollen, die für die Verwaltung der Datensätze in der Anwendung Configuration Compliance erforderlich sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Administratoren keine Quelldatensätze wie Explosions, CVEs usw. löschen.	
gelesen [sn_vulc.read]	Lese Listen und Datensätze in Configuration Compliance. **Wichtig:** Ab v24.0 von Vulnerability Responsehat die Rolle sn_vulc.read die Berechtigung zum Zugriff auf Vulnerability Manager Workspace.	• sn_sec_cmn.calc_read • sn_vul.view_manager_workspace
Schreiben sn_vulc.write	Schreiben Sie Listen und Datensätze in Configuration Compliance.	• sn_vulc.read • sn_vulc.remediation_owner
Zuweisung schreiben [sn_vulc.write_assignment]	In Zuweisungsfelder für Testergebnis schreiben.	Enthalten in der Rolle sn_vulc.remediation_owner.
Korrekturbesitzer sn_vulc.remediation_owner	Zeigen Sie Berechtigungen für Testergebnisse an, die Ihnen oder Ihrer Gruppe zugewiesen sind, und aktualisieren Sie sie.	Enthalten in der Rolle itil. Enthält: • sn_sec_cmn.read • sn_vulc.write_assignment • sn_vul.view_rem_workspace
CC.System sn_vulc.import_admin	Führt alle geplanten Aufgaben in der Konfigurations-Compliance-Anwendung aus. **Hinweis:** Dieser Anwender ist der standardmäßige „Ausführen als“-Anwender für jede geplante Aufgabe in Konfigurations-Compliance.	• sn_vulc.write • import_admin • sn_vul_tenable.read_integration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
VRAllgemein.System sn_vul_cmn.admin	Standardmäßige Ausführung als Benutzer für alle geplanten Aufgaben in der allgemeinen Vulnerability Response-Anwendung.	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin
SecCommon.System sn_sec_cmn.admin	Standardmäßige Ausführung als Anwender für alle geplanten Aufgaben, die für die Funktion für Hintergrundaufgaben in der allgemeinen Anwendung Security Support verwendet werden	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calc_write • sn_sec_core.read_dictionary • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.manage_classification_rules • sn_sec_cmn.manage_background_job
V14.7: sn_vulc.edit_watch_topic	Bearbeiten Sie Überwachungsthemen für Konfigurations-Compliance.	sn_vulc.read_watch_topic
V14.7: sn_vulc.read_watch_topic	Lesen Sie die Überwachungsthemen für Konfigurations-Compliance.	cmdb_read
V14.7: sn_vulc.create_watch_topic	Erstellen Sie Überwachungsthemen für Konfigurations-Compliance.	sn_vulc.read_watch_topic
sn_vulc.auditor	Lassen Sie das Lesen für alle Konfigurations-Compliance-Module zu	sn_vulc.read sn_vulc.advanced_read
sn_vulc.advanced_read	Lassen Sie den Lesezugriff für alle Konfigurations-Compliance-Verwaltungsmodule zu	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
		sn_vulc.read_test_criticality_mapping sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete sn_vulc.read_remediation_target_rules
sn_vulc.read_test_criticality_mapping	Lesen für Testkritikalitätszuordnung zulassen	
sn_vulc.read_task_rules	Lesen für Regeln für Korrekturaufgaben zulassen	
sn_vulc.read_assignment_rules	Lassen Sie das Lesen für Zuweisungsregeln zu	
sn_vulc.read_risk_score_configuration	Lassen Sie das Lesen für die Konfiguration der Risikopunktzahl zu	
sn_vulc.read_auto_close_rules	Lassen Sie das Lesen für die Konfiguration des automatischen Schließens zu	
sn_vulc.false_positive_approver	Ermöglicht das Genehmigen/Ablehnen des Schließens von Korrekturaufgaben als falsch positiv	sn_vul.view_manager_workspace
sn_vulc.exception_approver	Ausnahmeanforderungen genehmigt oder abgelehnt.	sn_vul.view_manager_workspace
sn_vulc.delete	Löscht Quelldatensätze.	

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
V15.0: Testgruppe bei Konfigurationstests aktualisieren	Aktualisiert die Testgruppe bei Tests für die Tenable- und Microsoft Defender-Quelle. Dies ist eine einmalige Aufgabe.
V15.0: Vorhandene Testergebnisfelder ausfüllen	Aktualisiert Werte in neu hinzugefügten Spalten (z. B. Alter, Alter geschlossen, Aktiv usw.) in der Tabelle „Testergebnisse“ sowie in gespeicherten Filtern und Modulen. Dies ist eine einmalige Aufgabe.
V15.0: Tabelle „Angreifbare CIs ausfüllen“: Löschen und für Testergebnisse erneut ausfüllen	Füllt die Gesamtzahl der Datensätze in der Tabelle der angreifbaren CIs aus. Dies ist eine einmalige Aufgabe.
Version 12.0	Berechnet und aktualisiert Werte für Statusmetriken in Korrekturaufgaben-Datensätzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Berechnen Sie die Korrekturmetriken für alle Testergebnisgruppen	
Version 12.0: Berechnen Sie Korrekturmetriken für alle Testergebnisse	Berechnet und aktualisiert Werte für Statusmetriken in Testergebnisdatensätzen.
Version 12.0: Statussynchronisierung von Change-Anforderungen	On-Demand-Auftrag, der die Status aller vorhandenen Korrekturaufgaben (RTs) mit Change-Anforderungen (CHGs) synchronisiert. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie automatisch auch die Status aller zugehörigen Korrekturaufgaben. Aktiviert die Statussynchronisierung in der Zukunft.
Version 11.1: Überprüfen Sie die Zurückstellung von Testergebnisgruppen Ablauf	Sendet Benachrichtigungen, wenn Korrekturaufgaben abgelaufen sind (und in einer Woche ablaufen).
Anzahl der Konfigurations-Compliance-CIs	Füllt die Anzahl der eindeutigen Konfigurationselemente (Configuration Item, CI) und den gleitenden Durchschnitt für 90 Tage in der Tabelle „Anzahl der Konfigurationselemente“ [sn_vulc_cc_configuration_item_count] aus.
Version 11.1: Korrekturziele bewerten und benachrichtigen	Legt für alle Testergebnisse Korrekturzieldaten fest oder aktualisiert sie. Bestimmt den Status von Korrekturzieldaten anhand von Regeln. Sendet Benachrichtigungen
V14.7: Testergebnisgruppen in einheitliche Korrekturaufgabe einfügen	Einmalige geplante Aufgabe zum Einfügen aller in der klassischen Anwenderoberfläche erstellten Korrekturaufgaben in die einheitliche Korrekturaufgabe (sn_vul_remediation_task).
Version 12.0: CR-TRG m2m für CR und CR-Parent ausfüllen	Füllt Change-Anforderungen für Korrekturaufgaben aus.
In v11.1 entfernt: Zurückgestellte Testergebnisgruppen erneut öffnen **Hinweis:** Für Versionen vor 11.1 veraltet Nicht verwenden.	Öffnet zurückgestellte Gruppen erneut, wenn das Fälligkeitsdatum verstrichen ist.
Wenden Sie alle Zuweisungsregeln erneut an	Wendet alle Zuweisungsregeln erneut an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Version 14.3: Anzahl der Neuzuweisungen für Zuweisungsregeln	Wird täglich ausgeführt und postet die Gesamtzahl der Testergebnisse und Korrekturaufgaben, deren Zuweisung von dieser Funktion für eine bestimmte Zuweisungsregel aufgehoben wurde.
Bewerten Sie den Status der Testergebnisgruppen neu	Bewertet den Status von Korrekturaufgaben für Einträge neu, bei denen **Assess_state** auf „false“ festgelegt ist. Wird alle 15 Minuten ausgeführt.
Rollup der Testergebnis-Risikopunktzahl zu Testergebnisgruppe und -konfiguration Test	Wird stündlich ausgeführt und berechnet die Rollup-Punktzahlen für die geänderten Konfigurationstests und Korrekturaufgaben. • Berechnet die Rollup-Risikopunktzahl für alle Tests in „sn_vulc_test_manifest“ und löscht den Manifestdatensatz nach Abschluss. • Berechnet die Rollup-Risikopunktzahl für alle Tests in sn_vulc_result_group_manifest und löscht das Manifest nach Abschluss.
Version 12.0: Aktualisieren Sie die Richtlinien-Korrekturmetriken	Ab v15.0 von Konfigurations-Compliancewurde diese geplante Aufgabe in Korrekturmetriken aktualisieren umbenannt. • Berechnet und aktualisiert Werte für Statusmetriken in Richtliniendatensätzen. • Berechnet den Prozentsatz der Testergebnis-Compliance eines CI für das erkannte Element.
Version 14.3: Anzahl der Zurückstellungen festlegen	Erfasst die Anzahl der Zurückstellungen eines Testergebnisses oder einer Korrekturaufgabe.
Aktualisieren Sie die Risikobewertung für Testergebnisse	Aktualisiert die Risikobewertung für Testergebnisse.
Aktualisiert die Rollup-Risikopunktzahl für alle nicht geschlossenen Ergebnisgruppen und Konfigurationstests.	Aktualisiert die Rollup-Risikopunktzahl für alle nicht geschlossenen Ergebnisgruppen und Konfigurations-Compliance -Tests.

Installierte Tabellen

Tabelle	Beschreibung
Zuweisungsregel sn_vulc_assignment_rule	Enthält den Satz von Regeln, die zum Festlegen der Zuweisungsgruppe für Testergebnisse ausgewertet wurden.
Autoritative Quelle sn_vulc_auth_src	Importierte autoritative Quellen speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Rechner [sn_vulc_calculator_risk_score]	Enthält den Rechner, der bestimmte Testergebnisfelder festlegt, wenn bestimmte Bedingungen erfüllt sind.
CC-Konfigurationselement: Anzahl [sn_vulc_cc_configuration_item_count]	Enthält die Gesamtanzahl der Configuration Items.
Version 12.0: Change-Anforderungszuordnung [sn_vulc_action_associate_cr]	Bereitstellungstabelle, die zum Zuordnen von Change-Anforderungen zu Korrekturaufgaben verwendet wird.
Version 12.0: Erstellung von Change-Anforderungen [sn_vulc_action_create_cr]	Bereitstellungstabelle, die zum Erstellen von Change-Anforderungsformularen verwendet wird.
Version 12.0: Formular für Change-Anforderungen sn_vulc_cr_form	Basistabelle für die Verwaltung von Change-Anforderungen.
Autorisierender Quelleninhalt sn_vulc_citation	Enthält importierte Zitate
Konfigurationstest sn_vulc_test	Enthält importierte Konfigurationstestdaten.
Konfigurationstest-Manifest sn_vulc_test_manifest	Enthält die Konfigurationstests, für die die Rollup-Risikopunktzahl berechnet werden muss.
Version 12.2 Fehlende Asset-Tabelle [sn_vul_missing_asset]	Enthält temporäre Asset-Datensätze für importierte Compliance-Bewertungsdaten für Konfigurationen mit nicht abgeglichenen Assets.
Konfigurationstest Technologie sn_vulc_test_technologie	Enthält importierte Konfigurationstesttechnologien.
Regel für Korrekturaufgaben sn_vulc_grouping_rule	Enthält die Regeln, die die Kriterien definieren, mit denen Gruppen automatisch für eine Reihe von Testergebnissen erstellt werden.
Testgruppen sn_vulc_policy	Enthält importierte Richtlinien.
Richtlinienkonfigurationstest	Enthält importierte Testdaten zur Richtlinienkonfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vulc_policy_test	
Korrekturzielregel sn_vulc_ttr_rule	Definiert den erwarteten Zeitrahmen für die Korrektur eines Testergebnisses.
Risikorechner sn_vulc_calculator_group	Enthält die Gruppierung von Konfigurations-Compliance -Rechnern. Die Reihenfolge der Rechnergruppe bestimmt, welche Gruppe zuerst ausgewertet wird, und in jeder Gruppe wird höchstens ein Rechner verwendet.
Rollup-Rechner für Risikopunktzahl [sn_vulc_risk_score_rollup]	Enthält Konfigurationen des Rollup-Rechners.
Korrekturaufgaben aufteilen [sn_vulc_action_split_trg]	Bereitstellungstabelle für die Aufteilung von Korrekturaufgaben.
Genehmigung der Zustandsänderung sn_vulc_state_change_approval]	Enthält Prozessdaten für den Genehmigungsstatus.
Technologie sn_vulc_technologie	Enthält importierte Technologien.
Relevanz-Zuordnung testen [sn_vulc_test_criticality_map]	Enthält Relevanzkartendaten.
Testergebnis sn_vulc_result	Enthält importierte Testergebnisse.
Korrekturaufgaben sn_vulc_result_group]	Enthält importierte Korrekturaufgaben.
Version 12.0: Change-Anforderungen für Korrekturaufgaben	Enthält Change-Anforderungen für Korrekturaufgaben.
Korrekturaufgabenmanifest sn_vulc_result_group_manifest]	Enthält die Korrekturaufgaben, für die die Rollup-Risikopunktzahl berechnet werden muss.
Korrekturaufgaben	Enthält Daten zu Korrekturaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_vulc_m2m_result_result_group]	
Testergebnisverlauf sn_vulc_result_history]	Enthält den importierten Testergebnisverlauf.
Testergebnis Korrekturstatus	Status des Testergebnisses im Vergleich zur nächsten angewendeten Korrekturzielregel.
V14.7: Testanzahl Überwachungsthemen [sn_vulc_wt_test_counts]	Cache-Tabelle für die Registerkarte „Unterschiedliche Konfigurationstests“ im Arbeitsbereich des Schwachstellenmanagers.

Zeigen Sie Konfigurations-Compliance Testgruppen an

Nachdem Sie die Ergebnisse eines Drittanbieter-Scans in Ihre Instanz importiert haben, können Sie Ihre Test-Compliance auf Testgruppenebene anzeigen. Verwenden Sie diese Ansicht vor einem Audit dieser Testgruppe und aller zugehörigen Testdatensätze.

Vorbereitungen

Erforderliche Rolle: sn_vulc.read und sn_vulc.remediation_owner für die Anzeige

Warum und wann dieser Vorgang ausgeführt wird

Richtlinien sind importierte Datensätze und können in Konfigurations-Compliancenicht bearbeitet werden.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testgruppen**.
   Die Liste der Testergebnisse wird angezeigt. Ab v15.0 von Konfigurations-Compliancezeigt die Spalte **% Compliance von Testergebnissen** den Prozentsatz der Testergebnisse an, die mit den Tests in einer Testgruppe konform sind.

   % Compliance von Testergebnissen = (Anzahl der in einer Testgruppe geschlossenen Testergebnisse/ Gesamtzahl der Testergebnisse, die einer Testgruppe zugeordnet sind) * 100

2. Klicken Sie auf die **Kurzbeschreibung** der Testgruppe, die Sie anzeigen möchten.

Konfigurations-Compliance Formularfelder „Testgruppe“.

Feld	Beschreibung
Quelle	Systemname des Drittanbieterscanners oder der im Plugin ServiceNow für die API eingegebene Name, der zur Kommunikation mit Konfigurations-Complianceverwendet wird.
Technologien	Liste der Technologien, die der Testgruppe in der Drittanbieter-Scanner-Anwendung zugeordnet sind.
Quell-ID	Bezeichner, der dieser Testgruppe vom Drittanbieter-Scanner zugewiesen wurde.
Quelle erstellt	Zeitpunkt (Datum und Uhrzeit), zu dem die Testgruppe in der Scanner-Anwendung der Drittpartei definiert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle aktualisiert	Zeitpunkt (Datum und Uhrzeit), zu dem die Testgruppe zuletzt in der Drittrichtlinien-Scanner-Anwendung geändert wurde.
Kurzbeschreibung	Zusammenfassungsbeschreibung oder Titel, die der Testgruppe in der Drittanbieter-Scanneranwendung zugewiesen ist.
Beschreibung	Detaillierte Beschreibung der Testgruppe, wie in der Scanneranwendung der Drittpartei definiert.
Tests	Liste der Tests, die auf diese Testgruppe verweisen. Importiert vom Scanner einer Drittpartei. Bei Bedarf können Sie in der Liste zu detaillierten Informationen zu einem bestimmten Test navigieren.
Korrekturstatus (Version 12.0)	
Zurückgestellte sind ausgeschlossen	Diese Werte enthalten keine CIs aus zurückgestellten Testergebnissen. ○ **Verbleibende CIs**: Die Anzahl (Anzahl) von Configuration Items (CIs) mit aktiven Testergebnissen (anderer Status als **„Geschlossen**“) für diese Richtlinie. ○ **Behobene CIs in Prozent**: Prozentsatz der konformen CIs für diese Testgruppe. Diese Zahl schließt CIs mit zurückgestellten Testergebnissen aus. ○ **CIs insgesamt**: Die Gesamtzahl der CIs, die von dieser Testgruppe betroffen sind. Diese Anzahl schließt zurückgestellte Testergebnisse aus.
Beinhaltet Zurückgestellte	Die Werte stellen CIs aus allen aktiven Testergebnissen dar (alle anderen Status als **Geschlossen**). ○ **Verbleibende CIs**: Die Anzahl der eindeutigen CIs, die mindestens einem nicht geschlossenen Testergebnis zugeordnet sind, auf das diese Testgruppe angewendet wurde. ○ **Behobene CIs in Prozent**: Der Prozentsatz der konformen CIs für diese Testgruppe. ○ **CIs insgesamt**: Gesamtzahl der CIs, die von dieser Testgruppe betroffen sind.

Um diese Werte ab Version 12.0 bei Bedarf zu aktualisieren, klicken Sie unter der Registerkarte Korrekturstatus auf den zugehörigen Link **Status aktualisieren**. Eine Nachricht zeigt an, dass die Daten aktualisiert werden. Klicken Sie auf den Link **Status anzeigen,** um den Fortschritt der Aktualisierung anzuzeigen. Nach einigen Minuten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden alle Daten, die sich seit der letzten geplanten Aufgabe geändert oder aktualisiert haben, im Datensatz aktualisiert. Aktualisierte Feldwerte werden aktualisiert.

3. **Wahlweise:** Deaktivieren Sie den Import von Testergebnissen für eine Testgruppe, indem Sie auf die Schaltfläche **Import deaktivieren** klicken.

   (Optional) Der Wert in der Spalte **Ist Import deaktiviert** ändert sich in *wahr*. Die Testergebnisse für die Testgruppe werden nicht aus der bevorstehenden Erfassung importiert.

   Hinweis:
   Die Schaltfläche **Import deaktivieren** ist nur für die Testergebnisse verfügbar, die mit dem Scanner Qualys erstellt wurden.

   Ab v23.0 von Vulnerability Response:

   - Sie können den Import von Testergebnissen für eine Qualys -Testgruppe in Vulnerability Manager Workspaceaktivieren oder deaktivieren. Weitere Informationen finden Sie unter Aktivieren oder deaktivieren Sie den Import von Testergebnissen für eine Qualys -Testgruppe.
   - Die Schaltfläche **Als veraltet markieren** wird in **Import deaktivieren**umbenannt.
   - Die Spalte **„Ist veraltet“** wird in **„Ist Import deaktiviert“**umbenannt.

Zeigen Sie Konfigurations-Compliance autoritative Quellen an

Verwenden Sie dieses Modul, um Zusammenfassungsinformationen zu jeder autorisierten Quelle anzuzeigen und die Quellveröffentlichungen zu recherchieren, die zum Erstellen des Datensatzes verwendet wurden.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zu aktualisieren
- sn_vulc.remediation_owner zum Anzeigen

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Unterstützungsdaten** > **Autoritative Quellen**.
2. Klicken Sie auf die **Kurzbeschreibung** der autorisierenden Quelle, die Sie anzeigen möchten.

Konfigurations-Compliance autoritative Quellen Formularfelder

Feld	Beschreibung
Nummer	ID-Nummer, die der autorisierenden Quelle von Ihrer Instanz während des Importvorgangs zugewiesen wurde.
Quelle	Systemname der Scanneranwendung einer Drittpartei oder der im Scanner-Plugin eingegebene Name für die API, die mit Konfigurations-Compliancekommuniziert.
Quell-ID	Bezeichner, der der autorisierenden Quelle vom Drittanbieterscanner zugewiesen wurde.
Kurzbeschreibung	Name, der dieser autorisierenden Quelle im Drittparteiscanner zugewiesen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Herausgeber	Name der Organisation oder Veröffentlichung, die die ursprüngliche Informationsquelle für diese autorisierte Quelle war.
Bezugsvermerke	Liste der Zitatinformationen zu den Testergebnissen. Importiert vom Scanner einer Drittpartei. Bei Bedarf können Sie in dieser Liste zu detaillierten Informationen zu einem bestimmten Test navigieren.

3. **Wahlweise:** Fügen Sie einen **Herausgeber**hinzu.
4. Klicken Sie auf **Aktualisieren**.
5. Sie können diesen Datensatz löschen, indem Sie auf **Löschen**klicken.
   Entfernt den Datensatz aus Ihrer -Instanz. Wenn er in Ihrer Drittanbieterintegration noch verwendet wird, wird er beim nächsten Import zurückgegeben

Zeigen Sie die Technologien Konfigurations-Compliance an

Verwenden Sie dieses Modul, um Zusammenfassungsinformationen zu allen maßgeblichen Quellen und Zitaten (in Qualys auch als Framework bezeichnet) anzuzeigen. Sie können die Quellveröffentlichungen recherchieren, die zum Erstellen des Datensatzes verwendet wurden.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zu aktualisieren
- sn_vulc.remediation_owner zum Anzeigen

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Unterstützungsdaten** > **Technologien**.
2. Klicken Sie auf die **Kurzbeschreibung** der autorisierenden Quelle, die Sie anzeigen möchten.

Konfigurations-Compliance autoritative Quellen Formularfelder

Feld	Beschreibung
Nummer	ID-Nummer, die der autorisierenden Quelle von Ihrer Instanz während des Importvorgangs zugewiesen wurde.
Quelle	Systemname des Drittanbieterscanners oder der im Plugin des Drittanbieterscanners für die API eingegebene Name, der mit Konfigurations-Compliancekommuniziert.
Quell-ID	Bezeichner, der der autorisierenden Quelle vom Drittanbieterscanner zugewiesen wurde.

3. Sie können diesen Datensatz löschen, indem Sie auf **Löschen**klicken.
   Entfernt den Datensatz aus Ihrer -Instanz. Wenn er in Ihrer Drittanbieterintegration noch verwendet wird, wird er beim nächsten Import zurückgegeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Konfigurations-Compliance Tests an

Verwenden Sie dieses Modul, um detaillierte Informationen zu diesen Tests zu erhalten. Enthalten sind die Quellenzitat der Experten, die bei der Erstellung verwendet wurden, die Konfigurationsrichtlinien der Drittpartei, in denen sie verwendet werden, und die Ergebnisse des Scans.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zu aktualisieren
- sn_vulc.remediation_owner zum Anzeigen

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Kontrollen**.
2. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Tests**
3. Öffnen Sie in der Liste das Steuerelement (Compliance-Test), das Sie anzeigen möchten.

Um diese Werte ab Version 12.0 bei Bedarf zu aktualisieren, klicken Sie unter der Registerkarte Korrekturstatus auf den Link Zugehöriger **Status Update**. Eine Nachricht zeigt an, dass die Daten aktualisiert werden. Klicken Sie auf den Link **Status anzeigen,** um den Fortschritt der Aktualisierung anzuzeigen. Nach einigen Minuten werden alle Daten, die sich seit der letzten geplanten Aufgabe geändert oder aktualisiert haben, im Datensatz aktualisiert. Feldwerte wie**Risikopunktzahl**, **Risikobewertung**, **Zieldatum der Korrektur**und **Status**sowie die Felder auf der Registerkarte **Korrekturstatus** werden aktualisiert.

Konfigurations-Compliance Formularfelder testen

Feld	Beschreibung
Nummer	Nummer, die der Kontrolle während des Importvorgangs zugewiesen wurde.
Ergebnis	Status des Scans. „Bestanden“ oder „Nicht bestanden“. Wenn dieser Test zu mehreren Korrekturaufgaben gehört, wird sein Status anhand einer Rangfolgebestimmt.
Quelle	Systemname der Drittanbieter-Integrationsanwendung oder der im Plugin für die API eingegebene Name, die für die Kommunikation mit Konfigurations-Complianceverwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Relevanz	Schweregrad des Konfigurationsproblems oder der Probleme, die mit der Kontrolle verbunden sind, wie in der Drittparteiintegration definiert. Die Relevanzstufe wird an die Granularität ähnlicher Schwachstellenindikatoren angepasst, die in Vulnerability Responseverfügbar sind. Mögliche Ebenen: **Kritisch** Das mit der Kontrolle verbundene Konfigurationsproblem verursacht eine Unterbrechung bei mindestens einem geschäftskritischen CI. **Hoch** Das mit der Kontrolle verbundene Konfigurationsproblem stellt eine Bedrohung dar, verursacht jedoch kein Herunterfahren kritischer Netzwerkressourcen. **Mittel** Das mit der Steuerung verbundene Konfigurationsproblem stellt ein Risiko dar, stellt jedoch keine unmittelbare Bedrohung dar. **Niedrig** Das mit der Steuerung verbundene Konfigurationsproblem stellt eine Bedrohung auf niedriger Ebene dar und kann anstelle von CIs ignoriert werden, die einem höheren Risiko ausgesetzt sind. **Geringer** Das mit der Steuerung verbundene Konfigurationsproblem stellt ein geringes Risiko dar und kann bei Bedarf ignoriert werden.
Quell-ID	Bezeichner, der dem Steuerelement von der Drittparteiintegration zugewiesen wurde.
Kategorie	Wichtige Klassifizierungskategorie, die dieser Art der Kontrolle vom Drittanbieter zugewiesen wurde.
Risikopunktzahl	Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl wird gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht „Geschlossen“-Testergebnisse (Offen, „In Untersuchung“, „Warten auf Implementierung“, „Zurückgestellt“, „Gelöst“) und 15 % der Punktzahl aus der Anzahl der Tests stammen Ergebnisse, die nicht „Geschlossen“ sind. Von Risikopunktzahl-Rechnern berechneter Wert, der auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	den Geschäftsrelevanz- und Testrelevanzwerten der Testergebnisse basiert.
Unterkategorie	Unterkategorie, die dieser Testklasse vom Drittanbieter zugewiesen wurde.
Risikobewertung	Basierend auf einem Bereich von Risikopunktzahlen auf einer numerischen Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen.
Technologien	Liste der von diesem Test abgedeckten Technologien.
Quelle erstellt	Datum, an dem der Test zum ersten Mal in der Drittparteiintegration definiert wurde.
Quelle aktualisiert	Datum der letzten Aktualisierung des Tests in der Drittparteiintegration.
Kurzbeschreibung	Zusammenfassungsbeschreibung oder Titel, die bzw. der dem Test in der Drittparteiintegration eingegeben oder dem Test zugewiesen wurde.
Korrekturstatus (v 12.0)	
Zurückgestellte sind ausgeschlossen	Diese Werte enthalten keine zurückgestellten Testergebnisse. ○ **Offene Testergebnisse**: Die Anzahl (Anzahl) der aktiven (anderer Status als **„Geschlossen“**) Testergebnisse für diesen Konfigurationstest. ○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse**: Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Beinhaltet Zurückgestellte	Diese Werte enthalten zurückgestellte Testergebnisse. ○ **Offene Testergebnisse**: Die Anzahl (Anzahl) aller aktiven Testergebnisse (jeder andere Status als **„Geschlossen“**) für diese Korrekturaufgabe. ○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse**: Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Beschreibung	Ausführliche Beschreibung des Tests. Bei der Qualys-Schwachstellenintegration ist dieses Feld standardmäßig auf den Inhalt des Deckblatts Qualys Cloud Platform gesetzt.
Korrektur	Schrittanweisungen, die beschreiben, wie die Nichteinhaltung behoben werden kann.
Zugehörige Registerkarten	
Bezugsvermerke	Liste der Zitate, die für jede autorisierte Quelle eingegeben wurden, die dem Test zugeordnet ist.
Testgruppen	Liste von Konfigurations-Compliance Testgruppen, die diesen Test verwenden.
Testergebnisse	Liste der CIs, die von dem Konfigurationsproblem oder den Konfigurationsproblemen betroffen sind, die diesem Test zugeordnet sind. Bei Bedarf können Sie auf einzelne Tests, Configuration Items ServiceNow oder die Liste der betroffenen Technologien zugreifen.
GRC-Richtlinienanweisungen	Wenn das Plugin GRC Richtlinien- und Compliance-Management „ installiert ist, enthält diese Registerkarte die zugehörige Richtlinie GRC. Sie können diese Liste bearbeiten, um Richtlinienanweisungen hinzuzufügen oder zu entfernen.

Zeigen Sie Konfigurations-Compliance Testergebnisse an

Zeigen Sie Konfigurations-Compliance -Testergebnisse für Auditing und Korrektur an. Die Testergebnisse werden während des Imports von Drittpartei-Schwachstellenintegrationen automatisch erstellt.

Wichtig:
Sie können die Testergebnisse, die während des Imports der Drittanbieter-Schwachstellenintegrationen erstellt wurden, im Arbeitsbereich des Schwachstellenmanagers anzeigen. Weitere Informationen finden Sie unter Listenseite im Vulnerability Manager Workspace.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.read zum Anzeigen
- sn_vulc.remediation_owner zum Anzeigen und Aktualisieren
- sn_vulc.delete zum Löschen von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Konfigurations-Compliance erstellt oder aktualisiert die Testergebnisse nicht, importiert sie jedoch als Teil einer Drittanbieterintegration. Sobald sie in Konfigurations-Compliancesichtbar sind, werden sie mithilfe von **Testergebnisgruppen**korrigiert.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse**.
   Ab v15.0 von Konfigurations-Compliancewerden in der Liste der Testergebnisse die folgenden Spalten angezeigt.

Liste mit Testergebnissen

Spalte	Beschreibung
Aktiv	Gibt an, ob ein Testergebnis aktiv ist. Ein Testergebnis wird markiert: ○ True: Wenn der Status nicht „Geschlossen“ lautet. ○ False: Wenn der Status „Geschlossen“ lautet.
Alter	Zeitraum, für den ein Testergebnis aktiv ist, seit es zuletzt geöffnet wurde. Dieses Feld ist für ein geschlossenes Testergebnis leer. Format: Tage HH:MM: SS Weitere Informationen zum Anpassen der Berechnung des Alters finden Sie im Artikel KB1703270.
Alter der Schließung	Zeitraum, für den ein Testergebnis aktiv war, bevor es in den Status „Geschlossen“ geändert wurde. Wenn das Testergebnis in „Geschlossen“ wechselt, wird der Wert aus der Spalte „Alter“ im Feld „Als geschlossen“ angezeigt. Dieses Feld ist für ein aktives Testergebnis leer. Format: Tage HH:MM: SS

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	Weitere Informationen zum Anpassen der Berechnung „Alter geschlossener“ finden Sie im Artikel KB1703270 .
Abgeschlossen	Zeitstempel, zu dem ein Testergebnis geschlossen wird. Format: JJJJ-MM-TT HH:MM: SS
Zuletzt geöffnet	Zeitstempel, zu dem ein Testergebnis geöffnet wird, d. h. wenn der Feldwert **Aktiv** in *true*geändert wird.

2. Öffnen Sie das Steuerelement, das Sie anzeigen möchten.

Konfigurations-Compliance Testergebnisformularfelder

Feld	Beschreibung
Nummer	Die Nummer, die dem Test während des Importvorgangs zugewiesen wurde.
Quelle	Der Systemname der SCA-Anwendung einer Drittpartei oder der im Anwendungs-Plugin eingegebene Name für die API, die für die Kommunikation mit Konfigurations-Complianceverwendet wird.
Quell-ID	Der Bezeichner, der dem Steuerelement von der SCA-Anwendung zugewiesen wurde.
Ergebnis	Bestanden, Fehlgeschlagen, Fehler oder Unbekannt. Importiert aus Qualys.
Risikopunktzahl	Rechnerergebnis für diesen Test. Vor v15.0 von Konfigurations-Compliancewird die Risikopunktzahl für ein bestandenes Testergebnis auf „0“ festgelegt. Ab v15.0 von Konfigurations-Compliancewird die Risikopunktzahl des Ergebnisses eines bestandenen Tests nicht in „0“ geändert, sodass Sie das geminderte Risiko schätzen können. Die Risikopunktzahl des Ergebnisses des bestandenen Tests wird bei der Berechnung der Risikopunktzahl einer Korrekturaufgabe nicht berücksichtigt.
Risikobewertung	Basierend auf einem Bereich von Risikopunktzahlen auf einer numerischen Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen.
Status	Wird anhand der Korrekturaufgaben berechnet, zu denen das Testergebnis gehört. Wenn das

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Testergebnis zu mehreren Gruppen gehört, wird eine Rangfolge angewendet, um den Status zu bestimmen.
Lösung	Wird anhand der Korrekturaufgaben berechnet, zu denen das Testergebnis gehört. Wenn das Testergebnis zu mehreren Gruppen gehört, wird eine Rangfolge angewendet, um die Lösung zu bestimmen.
Zuerst gesehen	Datum des ersten Imports in Konfigurations-Compliance. Ab v13.1.1 zeigt das Feld **Erstmals angezeigt** das vom Scanner bereitgestellte Datum an. Andernfalls wird das Datum des ersten Imports in Konfigurations-Compliance angezeigt.
Zuletzt gesehen	Datum des letzten Imports in Konfigurations-Compliance. Ab v13.1.1 zeigt das Feld **Zuletzt gesehen** das vom Scanner bereitgestellte Datum an. Andernfalls wird das Datum des letzten Imports in Konfigurations-Compliance angezeigt.
Letzte Übergabe	Spätestes Datum, an dem das Testergebnis bestanden wird.
Test	Name des Tests.
Konfigurationselement	Name des an den Test angehängten CI.
Technologie	Softwareversion, die auf dem CI ausgeführt wird.
Beschreibung	Beschreibung des Tests
Erwartete Werte	Erwartete Werte, die in Qualys konfiguriert und von Konfigurations-Complianceimportiert wurden. Dieser Wert ist ein boolescher Ausdruck, der, wenn er als „wahr“ ausgewertet wird, das Testergebnis **Bestanden** macht. Der Ausdruck kann eine Kombination aus logischen, festgelegten oder regulären Ausdrucksoperatoren sein.
Ist-Werte	Vom Test zurückgegebene Werte. Diese Werte werden in den booleschen Ausdruck für die erwarteten Werte eingefügt, um zu bestimmen, ob das Ergebnis erfolgreich ist oder nicht. Sie werden aus Qualys importiert. Ab Version 14.9 von Konfigurations-Compliance werden die Werte „Erweiterter Nachweis“ und „Fehlerursache“ in der Spalte „Ist-Werte“ hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Korrektur	Korrekturanweisungen.
Zugehörige Registerkarten	
Korrekturaufgaben	Korrekturaufgaben, die diesem Testergebnis zugeordnet sind.
Testergebnisverlauf	Zugehörige Liste von Testergebnissen, die den Verlauf der Bestanden/Nicht bestanden-Ergebnisse für dasselbe CI/Technologie/Test zeigen.

Zeigen Sie eine Korrekturaufgabe an

Sie können eine Korrekturaufgabe anzeigen oder alternativ eine erstellen und die Korrektur durchführen.

Wichtig:
Sie können die Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers anzeigen. Weitere Informationen finden Sie unter Listenseite im Vulnerability Manager Workspace.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zum Aktualisieren oder Erstellen
- sn_vulc.remediation_owner zum Anzeigen

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben**.
2. Klicken Sie in der Liste auf den Datensatz, den Sie anzeigen möchten.
3. Klicken Sie alternativ auf **Neu**, um eine neue Korrekturaufgabe zu erstellen und die Felder auszufüllen.

Formularfelder für Korrekturaufgabe für Konfigurations-Compliance

Feld	Beschreibung
Nummer	Die automatisch generierte Nummer für diesen Datensatz.
Status	Fortschrittsstatus der Korrekturaufgabe. ○ Öffnen ○ Wird untersucht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Warten auf Implementierung ○ Zurückgestellt ○ Gelöst ○ Abgeschlossen
Risikopunktzahl	Diese Punktzahl ist der Rollup-Wert der Risikopunktzahlen für alle aktiven Testergebnisse in einer Korrekturaufgabe. Diese Punktzahl ändert sich, wenn die Testergebnisse in der Korrekturaufgabe korrigiert werden.
Zuweisungsgruppe	Gruppe für die Bearbeitung dieser Korrekturaufgabe ausgewählt.
Risikobewertung	Das Risiko, das ein fehlgeschlagenes Testergebnis für Ihr System darstellt. Sie basiert auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, die Risiken als kritisch (1) bis keine (5) bewertet.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an diesem Aufgabensatz arbeitet.
Korrekturziel	Datum, bis zu dem die Testergebnisse korrigiert werden sollten, ab der ersten Identifizierung.
Erstellt	Datum und Uhrzeit der Erstellung dieser Korrekturaufgabe.
Korrekturstatus	Status der Korrektur für die Gruppe. Sie wird durch das Testergebnis mit dem nächsten Fälligkeitsdatum bestimmt. Für offene Gruppen gibt es folgende Status: „In der Luft“, „Ziel rückt näher“ und „Ziel verfehlt“. Geschlossene Gruppen haben folgende Status: „Kein Ziel“, „Ziel erfüllt“ und „Ziel verfehlt“. Für berechnete Korrekturzieldaten gilt: Wenn die Korrekturaufgabe geschlossen ist, wird der Gesamtkorrekturstatus aller geschlossenen Testergebnisse in der Korrekturaufgabe angezeigt. Diese bestimmen, ob die Gruppe ihr Datum eingehalten hat oder nicht. Der Korrekturstatus einer geschlossenen Korrekturaufgabe ist **„Kein Ziel“**, wenn keines der geschlossenen Ergebnisse ein Korrekturzieldatum aufwies. Es ist **„Ziel verfehlt“**, wenn bei einem der geschlossenen Ergebnisse das Zieldatum verfehlt wurde. Sie ist **Ziel erfüllt,** wenn mindestens ein geschlossenes Ergebnis

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	sein Ziel erreicht hat und keines der anderen es verfehlt hat.
Aktualisiert	Datum und Uhrzeit der letzten Änderung dieses Datensatzes.
Kurzbeschreibung	Kurze Beschreibung dieser Korrekturaufgabe.
Beschreibung	Ausführliche Beschreibung der Korrekturaufgabe, die die Liste der Software enthält, die dieser Korrekturaufgabe zugeordnet ist.
Test	Der Konfigurationstest, der dieser Korrekturaufgabe zugeordnet ist.
Korrekturstatus (Version 12.0)	
Zurückgestellte sind ausgeschlossen	Diese Werte enthalten keine zurückgestellten Testergebnisse. ○ **Offene Testergebnisse**: Die Anzahl (Anzahl) der aktiven (anderer Status als **„Geschlossen“**) Testergebnisse für diese Korrekturaufgabe. ○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten (geschlossenen) Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse**: Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Beinhaltet Zurückgestellte	Die Werte stellen alle aktiven Testergebnisse dar (alle anderen Status als **Geschlossen**). ○ **Offene Testergebnisse**: Die Anzahl (Anzahl) der aktiven (anderer Status als **„Geschlossen“**) Testergebnisse für diese Korrekturaufgabe. ○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten (geschlossenen) Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse**: Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Gruppenkonfiguration	Die Art der Filterung, die zur Auswahl der Testergebnisse für die Korrekturaufgabe verwendet wird.
Gruppierungsmethode	Name der verwendeten Methode.
Gruppenregel	Name der verwendeten Gruppenregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Notizen	Systemhinweise, die dem Datensatz zugeordnet sind.
Zugehörige Links	**Version 12.0: Statuslink aktualisieren**. Aktualisieren Sie die Werte im Testergebnis-Datensatz bei Bedarf. Zeigen Sie alle Daten an, die sich seit der letzten geplanten Aufgabe geändert oder aktualisiert haben.
Testergebnisse	Die Testergebnisse in dieser Korrekturaufgabe.
Change-Anforderungen (v 12.0)	Liste der Change-Anforderungen, die dieser Korrekturaufgabe zugeordnet sind.
Status Change-Genehmigungen (v 12.0)	Status und Status der Genehmigungen von Change-Anforderungen, die dieser Korrekturaufgabe zugeordnet sind.

Testergebnis- und Statusübergänge für Korrekturaufgaben in der Anwendung Konfigurations-Compliance .

Die Status von Konfigurationstestdatensätzen und der zugehörigen Korrekturaufgaben (RTs) werden beeinflusst, wenn Testergebnisdatensätze zurückgestellt, gelöst, erneut geöffnet und an andere Korrekturmaßnahmen (REs) übertragen werden.

Statusübergangsszenarien zwischen Testergebnissen und Korrekturaufgaben

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die folgende Tabelle beschreibt die Übergänge der Status und Substatus zwischen Konfigurationstestergebnissen und Korrekturaufgaben.

Wenn der Status einer Korrekturaufgabe von übergeht ...	...zu Status/ Substatus	Die zugehörigen Testergebnisstatus gehen über von ...	...zu Status/ Substatus	Beschreibung
Öffnen	Wird untersucht	Öffnen	Wird untersucht	Statusübergänge erfolgen bidirektional.
Öffnen	Wird überprüft	Öffnen	Wird überprüft	Statusübergänge erfolgen bidirektional.
Öffnen	Zurückgestellt/mit einem beliebigen	Öffnen	Zurückgestellt	Bei Testergebnissen bleibt der Lösungsgrund

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Status einer Korrekturaufgabe von übergeht ...	...zu Status/ Substatus	Die zugehörigen Testergebnisstatus gehen über von ...	...zu Status/ Substatus	Beschreibung
	Grund für die Lösung ausgewählt			mit der Korrekturaufgabe identisch.
Zurückgestellt/mit beliebigem Grund für die Lösung	Öffnen	Testergebnisse bleiben Zurückgestellt		Testergebnisse behalten die gleiche Lösung wie die Korrekturaufgabe.
Öffnen	Gelöst/Behoben	Öffnen	Gelöst	Status/Substatus gehen bidirektional über.
Öffnen	Gelöst und Gelöst zu Geschlossen/ Behoben	Öffnen	Gelöst	Wenn eine Korrekturaufgabe in den Status „Geschlossen“/ „Behoben“ übergeht, kann sie zurück in den Status „Offen“ übergehen. Wenn die Aufgabe in den Status „Offen“ übergeht, werden die zugehörigen Testergebnisse von „Gelöst“ zurück in „Offen“ geändert.
Öffnen	Gelöst	Offen	Gelöst	Status/Substatus gehen bidirektional über.
Öffnen	Gelöst/Abgebrochen	Öffnen	Gelöst	Status/Substatus gehen bidirektional über.
Öffnen	„Gelöst“ und „Gelöst“ zu „Geschlossen“.	Öffnen	Gelöst	Wenn eine Korrekturaufgabe automatisch in den Status „Geschlossen“ übergeht, können die zugehörigen Testergebnisse zurück in den Status „Offen“ übergehen.
Öffnen	„Gelöst“ und „Gelöst“ zu „Geschlossen“/ „Ergebnis ungültig“.	Öffnen	„Gelöst“ und „Gelöst“ zu „Geschlossen“/ „Ergebnis ungültig“.	Wenn eine Korrekturaufgabe in den Status „Gelöst“ übergeht, kann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Status einer Korrekturaufgabe von übergeht ...	...zu Status/ Substatus	Die zugehörigen Testergebnisstatus gehen über von ...	...zu Status/ Substatus	Beschreibung
				sie zurück in den Status „Offen“ übergehen. Wenn eine Korrekturaufgabe in den Status „Geschlossen“/ „Ergebnis ungültig“ übergeht, können sie und die zugehörigen Testergebnisse nicht erneut geöffnet werden.
Öffnen	Geschlossen/ Behoben	Testergebnisse bleiben offen		

Hinweis:

- Ab v14.12 von Konfigurations-Compliancewird die Option **Ergebnis ungültig** im Feld **Lösung** im modalen Element Schließen entfernt.
- Ab v14.12 von Konfigurations-Complianceist der Workflow **„Statusgenehmigung für Korrekturaufgabe“** veraltet und wird durch den Flow „Statusgenehmigung für Korrekturaufgabe“ im Flow Designer ersetzt.

Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

Es besteht eine synchronisierte Beziehung zwischen den Statusfeldern von Korrekturaufgaben und den Statusfeldern von Change-Anforderungen in der Anwendung Konfigurations-Compliance.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie automatisch auch den Status aller zugehörigen Korrekturaufgaben. Die Statussynchronisierung wird standardmäßig in Ihrer Instanz durch eine Systemeigenschaft aktiviert, wenn Sie die Anwendung Konfigurations-Compliance ab v12.0 von ServiceNow Store herunterladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Statussynchronisierung aktiviert ist, ändert das Feld CHG Status das Feld Status der Korrekturaufgabe in den folgenden Fällen automatisch:

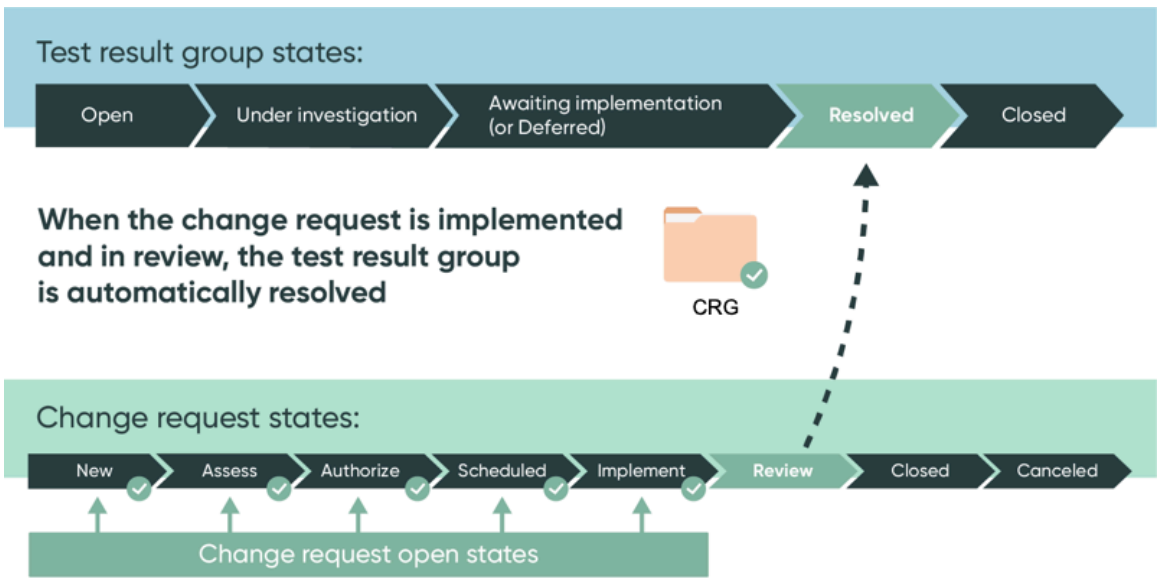
- Wenn eine neue Change-Anforderung für eine Korrekturaufgabe erstellt wird und sich nicht im **Status Warten auf Implementierung**befindet, wird der Status der Korrekturaufgabe in **Warte auf Implementierung**verschoben.
- Wenn eine vorhandene Change-Anforderung mit einer Korrekturaufgabe verknüpft ist und sich nicht im **Status Warten auf Implementierung**befindet, wird der Status der Korrekturaufgabe in **Warte auf Implementierung**verschoben.
- Nachdem die Aufgaben für eine Change-Anforderung abgeschlossen wurden (Implementiert) und das CHG in den Status **Überprüfen** versetzt wird, wird die Korrekturaufgabe in **den Status Gelöst**verschoben.

Weitere Informationen und Beispiele zur Statussynchronisierung finden Sie in den folgenden Abschnitten.

Hinweis:
Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung ihren Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder aus entfernen Bei einer Korrekturaufgabe kann die Statussynchronisierung Ihr manuelles Eingreifen möglicherweise überschreiben. Change-Anforderungsstatus verschieben die Korrekturaufgabe jedoch nicht automatisch aus **Geschlossen**.

Statussynchronisierung weiterleiten

Die folgende Abbildung zeigt, wie CHG-Status den Status von Korrekturaufgaben automatisch in einem Lebenszyklus nach vorn verschieben, d. h. von **Offen** nach **Gelöst**.



Sie können neue Change-Anforderungen für jede Korrekturaufgabe in einem anderen Status als **Gelöst** oder **Geschlossen**erstellen. Die Statussynchronisierung verschiebt das TRG automatisch bidirektional durch die Status **„Offen“**, **„Wird untersucht“**, **„Warten auf Implementierung“**und **„Gelöst“**. Diese Verschiebung basiert auf bestimmten Werten des Statusfelds im Change Request. Die Statussynchronisierung zwischen Change-Anforderung und Korrekturaufgabe wird automatisch aktiviert, es sei denn, das Kontrollkästchen (**CIs zu CR hinzufügen**) wird in einem Formular angezeigt und Sie deaktivieren das Kontrollkästchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Korrekturaufgabe rückt nicht in den Status **„Gelöst“** vor, wenn sich ein CHG im Status „Offen“ befindet. Alle CHG-Status vor der **Überprüfung** in ihrem Lebenszyklus wie **Neu**, **Bewerten**, **Autorisieren**, **Geplant** oder **Implementieren**, wie in der vorherigen Abbildung dargestellt, gelten für das CHG als Status „offen“. Offene Status verschieben das Statusfeld in der Korrekturaufgabe nicht, da Untersuchungen oder Aufgaben im CHG nicht abgeschlossen sind. Die Statussynchronisierung wird aufgerufen, wenn ein CHG für die Korrekturaufgabe erstellt oder ihr zugeordnet wird oder wenn sich der Status einer vorhandenen Beziehung im CHG ändert. Die abgeschlossenen CHG-Status sind **„Überprüfung“** und „Erfolgreich **geschlossen“**. Wenn ein CHG erfolgreich geschlossen wird, lauten seine Geschlossencodes: **Erfolgreich**oder **Erfolgreich mit Problemen**. In diesem Fall wechselt die Korrekturaufgabe zu **Gelöst**.

Rückwärts gerichtete Statussynchronisierung

Da ein CHG während seines Lebenszyklus verarbeitet wird, kann es irgendwann abgebrochen werden. Wenn in diesem Fall das CHG **Abgebrochen**oder **Geschlossen** ist (mit dem Abschlusscode **Nicht erfolgreich**), wird die Korrekturaufgabe automatisch zurück in **den Status Untersucht**verschoben. Die Korrekturaufgabe wird zurück in **den Status „Wird untersucht“**verschoben, da kein aktiver Plan zur Korrektur der Schwachstelle vorhanden ist.

Wenn sich eine Korrekturaufgabe im Status **„Gelöst“** befindet und Sie ein neues CHG erstellen oder sie einem vorhandenen CHG in einem der anfänglichen offenen Status zuordnen, wechselt die Korrekturaufgabe automatisch zurück in **den Status „Warten auf Implementierung“**. Die Korrekturaufgabe wird in diesen Status zurückversetzt, da dem CHG jetzt mehr Arbeit zugewiesen ist.

Korrekturaufgaben mit mehr als einem CHG

Wenn einer Korrekturaufgabe in **Warten auf Implementierung** mehr als ein CHG zugeordnet ist, basiert die Statussynchronisierung auf dem Status des CHG im frühesten Status seines Lebenszyklus. Angenommen, einer Korrekturaufgabe sind vier CHGs zugeordnet: CHG1, CHG2, CHG3 und CHG4, wie in der folgenden Tabelle gezeigt.

CHG-Nummer	CHG-Status
1	**Implementieren**
2	**Abgebrochen**
3	Geschlossen (Lösungscode von **„Nicht erfolgreich“**)
4	Geschlossen (Lösungscode **nicht erfolgreich**)

Die Statussynchronisierung zwischen CHG und Korrekturaufgabe basiert in diesem Fall auf CHG1, dem frühesten Status der vier CHGs (**Implementieren**). In diesem Fall verbleibt die Korrekturaufgabe im **Status Warten auf Implementierung**.

In einem anderen Beispiel gilt: Wenn sich eine Korrekturaufgabe im Status **„Gelöst“** befindet und über ein vorhandenes CHG verfügt, das implementiert wurde und sich im Status **„Überprüfung** “ befindet, und ein neues CHG erstellt wird, wird die Korrekturaufgabe von **„Gelöst“** zurück zu **„Warten auf Implementierung“**verschoben. Die Statussynchronisierung basiert auf dem CHG im Status **„Neu“**, dem CHG im frühesten Status.

CHG-Nummer	CHG-Status
1	Prüfung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CHG-Nummer	CHG-Status
2	Neu

Wenn Korrekturaufgaben mehr als ein CHG haben, wechselt außerdem der Status der Korrekturaufgabe in den folgenden Fällen automatisch:

- Wenn ein CHG zur **Überprüfung**wechselt und alle anderen CHGs, die der Korrekturaufgabe zugeordnet sind, sich im Status **„Überprüfen"** oder **„Geschlossen"** befinden (mit einem erfolgreichen Abschlusscode), die Korrekturaufgabe automatisch in den **Status „Gelöst"**übergeht . Alle anderen zugehörigen CHGs, die abgebrochen oder nicht erfolgreich geschlossen wurden, werden ignoriert.
- Wenn ein CHG in den Status **„Abgebrochen"** oder**„Geschlossen"** (Abschlusscode „ **Nicht erfolgreich**" wechselt) und alle anderen CHGs, die der Korrekturaufgabe zugeordnet sind, sich im selben Status befinden, wird die Korrekturaufgabe automatisch in **den Status „Wird untersucht"**zurückversetzt.

Weitere Informationen zu den Status von Korrekturaufgaben und den möglichen Aktionen in den einzelnen Status finden Sie unter Konfigurations-Compliance Status.

Domain Separation und Konfigurations-Compliance

Die Domänentrennung wird in Konfigurations-Compliance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Support-Stufe: Standard

- Umfasst alle Aspekte des **Basis** -Supports.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Konfigurations-Compliance

Mit Domain Separation können Sie (Konfigurations-Compliance) Verfahren für den gesamten Kundenstamm standardisieren, um die Betriebskosten zu senken und die Servicequalität zu erhöhen.

Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt sind und niemals für andere Clients verfügbar sind.

Unterstützung für Domain Separation in Konfigurations-Compliance nach Versionsreleases

Release	Support-Stufe	Notizen
Orlando	Standard	
Paris	Standard	
Quebec	Standard	
Rom	Standard	
San Diego	Standard	
Tokio	Standard	
Utah	Standard	
Vancouver	Standard	

Die Domänentrennung für die Anwendung Konfigurations-Compliance deckt die folgenden Produktfunktionen ab:

- Erfasst die Testergebnisse von Drittanbieterscannern (Qualys) in der richtigen Domäne.

  Die Daten werden in derselben Domäne erfasst wie der Integrationsbenutzer, dessen Anmeldeinformationen für die Integration verwendet werden.
- Scannt bestimmte Hosts von Konfigurations-Compliance in der Domäne, von der der Vorgang angefordert wurde, erneut.
- Verwendet den CMDB-CI-Suchprozess, um sicherzustellen, dass die CI-Informationen von den Scannern mit den CIs in CMDB der Domäne des Integrationsbenutzers übereinstimmen.
- Berechnet Risikopunktzahlen auf Testergebnisebene gemäß dem Risikopunktzahl-Rechner, der in derselben Domäne wie der Integrationsbenutzer definiert ist.
- Regeln für Korrekturaufgaben können in derselben Domäne wie in der Domäne des Integrationsbenutzers definiert und zugewiesen werden und bleiben in derselben Domäne.
- Korrekturaufgaben, die mit den Regeln für Dokumentkorrekturaufgaben erstellt wurden, bleiben in derselben Domäne, in der die Regeln für Korrekturaufgaben erstellt werden.
- Der Zurückstellungs-Workflow durchläuft den Genehmigungsprozess in derselben Domäne, für die die Zurückstellung angefordert wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Berichte und Dashboards zeigen die Testergebnisstatus an, z. B. Alter der Testergebnisse, offene Testergebnisse nach CI, Testergebnisse nach Auswirkung in der Domäne, zu der sie gehören.
- Wissen von Drittpartei-Scannern (Qualys) kann in der globalen Domäne erfasst werden, und Daten können von mehreren Clients gemeinsam genutzt werden.

Hinweis:
In allen oben genannten Fällen gelten die übergeordneten Prinzipien der Transparenz in getrennten Domänentrennung in der NOW Platform.

Anwendungsfälle

Die Anwendung Konfigurations-Compliance verwaltet den Lebenszyklus eines Testergebnisses End-to-End. Die folgenden Anwendungsfälle berücksichtigen die Domänentrennung:

- Testergebnisse aus Qualys**erfassen**
  - Erfassen Sie Daten aus mehreren Instanzen
  - Deduplizieren Sie die Testergebnisse
  - Mit CMDB-CI abgleichen
- **Anreicherung** von Testergebnissen mit Risikopunktzahlen
  - Asset-Ergänzung (CMDB)
  - Risikopunktzahl
- **Gruppieren Sie** Testergebnisse, und weisen Sie die Korrekturaufgabe zu
  - Testergebnisse automatisch gruppieren
  - Korrekturaufgabe automatisch zuweisen
- **Beheben**
  - Korrekturaufgabe als Korrekturaufgabe zugewiesen
  - Umfassender Korrekturlebenszyklus
  - Zurückstellungs-Workflow
- **Messen Sie** die Sicherheitslage der Organisation und des Compliance-Management-Programms
  - Ergebnistrend nach Compliance, Kategorie, Relevanz und Technologie
  - Status und Verteilung für Richtlinien, Tests, Hosts, Testergebnisse und Risikopunktzahlen

Setup

Das Einrichten von Domain Separation für Konfigurations-Compliance erfordert keine zusätzlichen Schritte. Alle Konfigurations-Compliance -Tabellen erwerben die Spalte „Domäne“, nachdem die Instanz domänengetrennt wurde. Sie können Importdaten für die Testergebnisintegration an bestimmte Domänen richten. Weitere Informationen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration. Weitere Informationen zu zusätzlichen Vorsichtsmaßnahmen und Einstellungen finden Sie unter Zusätzliche Einstellungen für Domain Separation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänengetrennte Daten

Daten können domänengetrennt sein. Das bedeutet:

- Von Drittanbieter-Scannern erfasste Testergebnisse verbleiben in derselben Domäne wie die Domäne des Integrationsbenutzers und sind von keiner anderen Domäne aus zugänglich.
- Testergebnisse oder Hosts in einer Domäne können nicht in anderen Domänen angezeigt werden.
- Der Risikobewertungsalgorithmus und die Gruppenregeln für Testergebnisse können von niemandem außerhalb der Domäne angezeigt werden.
- Zurückstellungs-Workflows, die in einer Domäne erstellt wurden, sind in einer anderen Domäne nicht sichtbar.
- Alle E-Mail-Benachrichtigungen sind in der Domäne enthalten, zu der sie gehören.

Wie Compliance-Analysten ihre eigenen Anwendungsdaten verwalten

- Analysten erstellen ihre eigenen Regeln für die Anwendungsinstallation, für die Verwaltung von Anwendungen mit mehreren Quellen und für die CI-Suche.
- Analysten können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Analysten können ihre eigenen Workflows für Zurückstellungen und Change-Management erstellen.
- Analysten können eigene Regeln für Korrekturaufgaben und Risikobewertungslogik erstellen, um Ergebnisse genau zu priorisieren, Korrekturaufgaben automatisch zuzuweisen und sie der richtigen Zuweisungsgruppe zuzuweisen.
- Domänenbenutzer erstellen eine manuelle Korrekturaufgabe und schließen sie dann.

Geschäftslogik und -prozesse, die nach Instanzbesitzern domänengetrennt werden können

- Konfigurations-Compliance Benutzer und Gruppen
- Konfigurations-Compliance -Integrationen (ab Madrid-Release)
- Setupkonfiguration abschließen (Benutzer- und Gruppenverwaltung, Anwendungsinstallation, Anwendungsverwaltung mit mehreren Quellen, CI-Suchregeln, Regeln für Korrekturaufgaben, Risikorechner usw.)
- Vollständiger Korrekturlebenszyklus einschließlich Zurückstellung

Zugehörige Informationen

Domänentrennung für Service Provider

Konfigurations-Compliance Kritikalitätszuordnungen

Die KritikalitätszuordnungKonfigurations-Compliance wandelt Kritikalitätsfelder aus der Quelle in Felder in Konfigurations-Complianceum.

Das Basissystem Konfigurations-Compliance wird mit einer Zuordnung von Standard Qualys Cloud Platform zu Standard ServiceNow geliefert. Das Erstellen oder Bearbeiten einer Kritikalitätszuordnung ist nur für anwenderdefinierte oder nicht standardmäßige Drittpartei-Zuordnungen in Ihrer Umgebung vorgesehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Status

Mit Konfigurations-Compliancekönnen Sie ein Statusmodell anzeigen, um zu erfahren, wie der Status der Korrekturaufgabe zu einem bestimmten Zeitpunkt ist. Die Status der Korrekturaufgaben steuern die Testergebnisstatus nach Priorität.

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

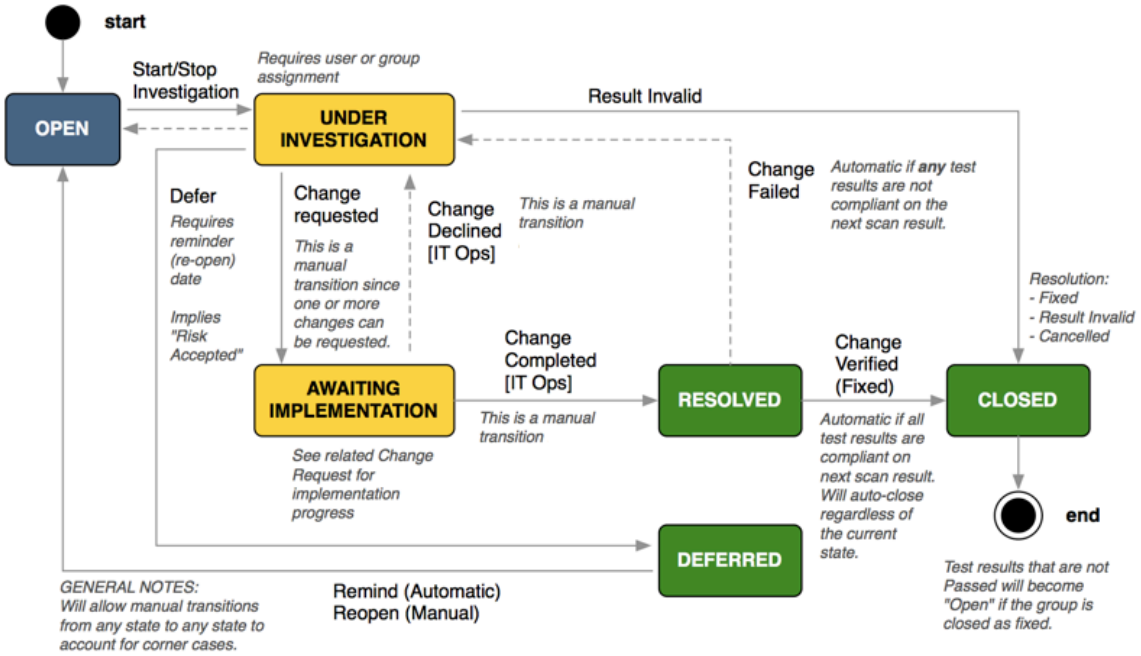
Status der Korrekturaufgaben

Korrekturaufgaben haben viele mögliche Status. Der automatische Übergang ist vom Status Gelöst basierend auf den nächsten Scan-Ergebnissen verfügbar. Wenn alle Testergebnisse beim nächsten Scan erfolgreich sind, wird die Korrekturaufgabe geschlossen. Andernfalls geht er in den Status „Wird untersucht“ über. Das System verifiziert diesen Status „Geschlossen“, wertet jedoch den Status der Korrekturaufgabe neu aus, wenn der Korrekturaufgabe ein Testergebnis hinzugefügt oder daraus gelöscht wird. Die Arbeitsnotizen werden aktualisiert, um den Übergang widerzuspiegeln.

Die folgende Abbildung zeigt, wie der Status einer Korrekturaufgabe vom Status „Offen“ in den Status „Geschlossen“ übergeht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow des Konfigurations-Compliance-Status (vor v15.0)



Hinweis:

- Jedes Korrekturaufgabenformular enthält die Schaltflächen **Folgen** und **Aktualisieren**, die bei ServiceNow -Aufgaben standardmäßig verwendet werden.
- Ab v15.0 von Konfigurations-Compliancewurde Folgendes entfernt:
  - Schaltfläche „**Schließen** “.
  - das Feld **Lösung** im Modal „Lösen“.

In der folgenden Tabelle sind die Status Konfigurations-Compliance aufgelistet.

Konfigurations-Compliance-Status

Status	Beschreibung
Öffnen	Status beim Erstellen.
Wird untersucht	Wird durch die Schaltfläche **„Untersuchung starten“** ausgelöst. In diesem Status können Sie: **Erstellt eine Change-Anforderung** Weitere Informationen finden Sie unter Change-Anforderung in Konfigurations-Compliance erstellen. **Ausnahme anfordern** Geben Sie einen Grund an, und wählen Sie ein Datum der Wiedereröffnung aus. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. **Als falsch positiv markieren** Geben Sie einen Grund und Notizen an. Markiert die Korrekturaufgabe als falsch positiv.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance-Status (Fortsetzung)

Status	Beschreibung
Zurückgestellt	Wird durch die Schaltfläche **„Zurückstellen“** ausgelöst. In diesem Status können Sie: **Erneut öffnen** Wechseln Sie zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Gruppe. Aufschubinformationen werden unter der zugehörigen Registerkarte **Zurückstellen/Schließen** angezeigt. Am Zurückstellungsdatum wird die Gruppe erneut zur Korrektur geöffnet.
Warten auf Implementierung	Wird durch die Schaltfläche **Warten auf Implementierung** ausgelöst. In diesem Status können Sie: **Security Incident** Weitere Informationen hierzu finden Sie unter Security Incidents erstellen. **Erstellt eine Change-Anforderung** Weitere Informationen finden Sie unter Change-Anforderung in Konfigurations-Compliance erstellen. **Lösen** Fügen Sie in den **Lösungshinweisen**den Grund hinzu, aus dem Sie die Korrekturaufgabe lösen. Der Status wird zu Gelöst. Hinweise werden unter der Registerkarte **Lösungsbezogen** angezeigt. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.
Gelöst	Wird über die Schaltfläche **„Lösen“** ausgelöst. In diesem Status können Sie: **Security Incident** Weitere Informationen hierzu finden Sie unter Security Incidents erstellen. **Erneut öffnen** Wechseln Sie zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. Notizen werden unter der zugehörigen **Registerkarte** Notizen angezeigt. Lösungsinformationen werden unter der Registerkarte **Lösungszugehörig** angezeigt. Die Notizen werden in den **Arbeitsnotizen** aller Testergebnisse angezeigt, die der Korrekturaufgabe zugeordnet sind.
Abgeschlossen	Wird über die Schaltfläche **„Schließen“** oder **„Als falsch positiv markieren“** ausgelöst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance-Status (Fortsetzung)

Status	Beschreibung
	Ab v14.12 von Konfigurations-Compliancekönnen Sie eine Korrekturaufgabe schließen, indem Sie sie als falsch positiv markieren. In diesem Status können Sie: **Erneut öffnen** Wechseln Sie zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Gruppe. Abschlussinformationen werden unter der zugehörigen Registerkarte **Zurückstellen/Schließen** angezeigt. Die Notizen werden in den **Arbeitsnotizen** aller Testergebnisse angezeigt, die der Korrekturaufgabe zugeordnet sind.

- Wenn die Korrekturaufgabe als Geschlossen oder Behoben markiert ist und das hinzugefügte Testergebnis nicht selbst Geschlossen oder Behoben ist, ändert sich der Status des Testergebnisses nicht, und der Status der Korrekturaufgabe wird in Offen geändert.
- Wenn Sie eine neue Korrekturaufgabe erstellen oder eine Korrekturaufgabe aufteilen, werden die Felder **Grund**und **Bis** für neue und alte Korrekturaufgaben neu ausgewertet. Wenn der Status aller Testergebnisse Zurückgestellt ist, wird für den Wert in den Feldern **Grund** und **Bis** ein Rollup für die Korrekturaufgabe durchgeführt.
  - Wenn alle Testergebnisse in einer Korrekturaufgabe zurückgestellt sind und denselben **Grund**aufweisen, wird der Korrekturaufgabe derselbe **Grund**zugewiesen. Andernfalls wird das Feld **Grund** in **Keine**geändert.
  - Das Datum im Feld **Bis** wird mit dem nächsten Bis-Datum aller Korrekturaufgaben aktualisiert, zu denen die Testergebnisse gehören.

Hinweis:
Diese Auswertung erfolgt durch die geplante Aufgabe *`Rollup test result values to test result group and configuration test`*, die jede Stunde ausgeführt wird.

- Wenn für ein gelöstes Testergebnis das Datum **Zuletzt gesehen** nach dem **Lösungsdatum** liegt, wird das Testergebnis erneut geöffnet. Wenn in einer gelösten Korrekturaufgabe mindestens ein Testergebnis während der Erfassung erneut geöffnet wird, wird die Korrekturaufgabe in den Status Wird untersucht verschoben.

Testergebnisstatus

Der Status einer Korrekturaufgabe ändert auch den Status der zugehörigen Testergebnisse. Dieser Mechanismus hat zwei Fälle:

Testergebnisse, die nur zu einer Korrekturaufgabe gehören

Die Ergebnisse stimmen mit dem Status der Korrekturaufgabe mit drei Ausnahmen überein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Korrekturaufgabe ihren Status in Geschlossen und ihre Lösung (Substatus) in Behoben ändert, ignoriert das Element diese Änderung und fällt dann in den Status Offen zurück.
- Wenn die Korrekturaufgabe ihren Status in Geschlossen und ihre Lösung (Substatus) in Abgebrochen ändert, ignoriert das Element diese Änderung und fällt dann in den Status Offen zurück.
- Wenn der Status der Testergebnisquelle „Fest“ lautet (durch Scan oder Import aktualisiert), ändert das Testergebnis seinen Status in Geschlossen (Behoben), wenn die Korrekturaufgabe ihren Status ändert, unabhängig davon, in welchem Status sich die Korrekturaufgabe befindet .

Testergebnisse, die zu mehreren Korrekturaufgaben gehören

Testergebnisse stimmen nicht automatisch mit dem Status der Korrekturaufgabe überein. Stattdessen wird in allen zugeordneten Gruppen nach dem Status mit der höchsten anzuwendenden Priorität gesucht. Dies ist der Prioritätsstatus:

Geschlossen (Substatus: Ergebnis ungültig) > **Geschlossen (Substatus: Falsch positiv)** > **Zurückgestellt** > **Gelöst** > **Warten auf Implementierung** > **Wird untersucht** > **Öffnen**

Hinweis:
Geschlossen (Substatus: Repariert) und **Geschlossen (Substatus: Abgebrochen)** sind zwei Sonderfälle.

Hinweis:
Ab v15.0 von Konfigurations-Complianceist der Substatus **„Ergebnis ungültig“** veraltet.

Beispiele für Korrekturaufgabenstatus

Zum Beispiel:

Status der Korrekturaufgaben	Status des Testergebnisses
Gruppe A: **Öffnen** > **Wird untersucht** Gruppe B: **Offen**	**Wird untersucht** Wenn für Gruppe A der Status „Wird untersucht“ und für Gruppe B der Status „Offen“ festgelegt ist, ändert sich das Testergebnis in „Wird untersucht“, da nach der Suche zwischen Gruppe A und Gruppe B Gruppe A den Status mit der höchsten Priorität hat.
Gruppe A: **Wird untersucht** Gruppe B: **Öffnen** > **Wird untersucht**	**Wird untersucht** Wenn Gruppe B auf „Wird untersucht“ und Gruppe A auf „Wird untersucht“ gesetzt ist, bleibt das Testergebnis „Wird untersucht“, da nach der Suche zwischen Gruppe A und Gruppe B beide den Status mit der gleichen Priorität haben.
Gruppe A: **Wird untersucht**	**Warten auf Implementierung**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Korrekturaufgaben	Status des Testergebnisses
Gruppe B: **Wird untersucht** > **Warten auf Implementierung**	Wenn Gruppe B „Warten auf Implementierung“ ist und Gruppe A „Wird untersucht“ wird, ändert sich das Testergebnis in „Warten auf Implementierung“, da Gruppe B nach der Suche zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität hat.
Gruppe A: **Wird untersucht** > **Zurückgestellt** Gruppe B: **Warten auf Implementierung**	**Zurückgestellt** Wenn Gruppe A auf Zurückgestellt und Gruppe B auf Implementierung wartend gesetzt ist, ändert sich das Testergebnis in Zurückgestellt, da Element 1 nach der Suche herausgefunden hat, dass Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität hat
Gruppe A: **Zurückgestellt** Gruppe B: **Warten auf Implementierung** > **Geschlossen (Ergebnis ungültig)**	**Geschlossen (Ergebnis ungültig)** > **Zurückgestellt** Wenn Gruppe B den Status Geschlossen hat und die Lösung (Substatus) Ergebnis ungültig ist und Gruppe A Zurückgestellt ist, ändert sich das Testergebnis in Geschlossen (Ergebnis ungültig), da Gruppe B nach der Suche zwischen Gruppe A und Gruppe B den Status mit hat die höchste Priorität.
Gruppe A: **Zurückgestellt** Gruppe B: **Geschlossen (Ergebnis ungültig)** > **Öffnen (über Erneut öffnen)**	**Zurückgestellt** Wenn Gruppe B erneut geöffnet wird und ihr Status in Offen und Gruppe A in Zurückgestellt geändert wird, ändert sich das Testergebnis in Zurückgestellt, da Gruppe A nach der Suche zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität hat.
Gruppe A: **Zurückgestellt** Gruppe B: **Warten auf Implementierung** > **Geschlossen (falsch positiv)**	**Geschlossen (falsch positiv)** Wenn Gruppe B geschlossen ist und die Lösung (Substatus) Falsch positiv ist und Gruppe A zurückgestellt ist, ändert sich das Testergebnis in Geschlossen (Falsch positiv), da Gruppe B nach der Suche zwischen Gruppe A und Gruppe B den Status mit hat höchste Priorität.

Testergebnisstatus Sonderfälle

Status der Korrekturaufgabe	Testergebnisstatus
Gruppe A: **Wird untersucht** Gruppe B: **Warten auf Implementierung** > **Geschlossen (repariert oder storniert)**	**Wird untersucht** Wenn Gruppe B geschlossen ist (Substatus Fest oder Substatus Abgebrochen) und Gruppe A den Status „Wird untersucht“ hat, ändert sich das Testergebnis von Warten auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testergebnisstatus Sonderfälle (Fortsetzung)

Status der Korrekturaufgabe	Testergebnisstatus
	Implementierung (früher, die höchste Priorität) in Wird untersucht (derzeit die höchste Priorität).
Gruppe A: jeder Status Gruppe B: beliebiger Status	Wenn der Status der Testergebnisquelle „Fest“ lautet (durch Scan oder Import aktualisiert), wenn die Korrekturaufgabe ihren Status ändert, ändert das Testergebnis seinen Status in Geschlossen (Repariert), unabhängig vom Status der anderen zugeordneten Korrekturaufgaben. sind in. Die Suche nach Testergebnissen für den Status der Korrekturaufgabe findet nicht statt.

Konfigurations-Compliance Importprobleme werden gelöst

Beheben Sie Probleme mit dem Import von Drittparteiintegrationen.

Importieren Sie die Problemlösung

Problem	Lösung
Testergebnisse fehlen	Überprüfen Sie *`Start Time`* in der Integration der **Qualys-PC-Ergebnisse**. Möglicherweise ist er nicht weit genug zurückgesetzt. Weitere Informationen finden Sie unter Ändern Sie das Startdatum der Qualys PC-Ergebnisse.
Die Integration schlägt fehl	Überprüfen Sie den Status **der Ausführung der Schwachstellenintegration**. Einzelne Integrationsprozesseinträge enthalten die importierte XML, die auf unerwartete Informationen untersucht werden kann. Navigieren zu **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **QualysPC-Ergebnisse** > **Ausführungen der Schwachstellen-Integration** Zugehörige Registerkarte Wählen Sie die letzte Ausführung aus. Untersuchen Sie den Status und die Notizen der Einträge in der zugehörigen Liste **Integrationsprozess für Schwachstellen** auf Anomalien. .

Ändern Sie das Startdatum der Qualys PC-Ergebnisse

Wenn im Import der Qualys PC-Ergebnisse Daten für das Startdatum fehlen, können sie geändert werden.

Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
2. Klicken Sie auf **Qualys PC-Ergebnisse** Integration.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Integrationsdetails**.
4. Legen Sie das Feld **Startzeit** auf einen Wert in der Vergangenheit fest, damit alle gescannten und erkannten Testergebnisse seit diesem Zeitpunkt erkannt werden.

> **Hinweis:**
> Wenn das Datum leer gelassen wird, werden bei der ersten Ausführung keine Daten zurückgegeben. Legen Sie den Wert auf maximal einen Monat in der Vergangenheit fest. Diese Einstellung verhindert, dass große Datenmengen die Qualys-API-Quotenbegrenzungen überschreiten und Ausführungszeitüberschreitungen auslösen.

5. Klicken Sie auf **Absenden** oder **Aktualisieren**.
6. **Wahlweise:** Klicken Sie auf **Jetzt ausführen**, um die Ausführung sofort zu starten.

CI-Suchregeln für Microsoft Defender for Cloud Integration für Security Operations und Palo Alto Prisma Cloud

Sie können die Suchregeln für Configuration Item (CI) für die Integrationen Microsoft Defender for Cloud Integration und Palo Alto Prisma Cloud verwenden, um eine richtige Übereinstimmung mit häufig verwendeten Ressourcentypen in Configuration Management Database (CMDB)zu finden.

Übersicht

Das Modul CI-Suchregeln enthält die Regeln, mit denen Sie die Felder mit den übereinstimmenden Daten in Configuration Management Database (CMDB)definieren können. Sie können diese Regeln verwenden, um die Anwendungen und Anwendungsreleases zu identifizieren. Alle Microsoft Defender for Cloud Integration - und Palo Alto Prisma Cloud -Assets werden durch die Kombination aus Objekt-ID, Cloud-Account und logischem Rechenzentrum in der ServiceNow -Plattformeindeutig identifiziert. Die Discovery ServiceNow füllt die Ressourcen-ID in der Spalte `Object_id` von CMDB in unterschiedlichen Formaten für die unterschiedlichen Ressourcentypen aus. Die folgende Tabelle zeigt die Objekt-ID-Formate häufig verwendeter Ressourcentypen, die der Discovery-Service zum Ausfüllen der Spalte `Object_id` des CI verwendet. Jeder Scanner, der ein Asset eines bestimmten Ressourcentyps suchen möchte, muss mithilfe des richtigen Objekt-ID-Formats suchen. Sie können das richtige Objekt-ID-Format erhalten, indem Sie in der Objekt-ID-Spalte der entsprechenden CMDB CI-Klasse suchen und dann versuchen, die Objekt-ID mit den vom Scanner empfangenen Werten zu erstellen.

Objekt-ID-Format für verschiedene Ressourcentypen

Ressourcentyp	Format
AWS::EC2::Instance	Objekt-ID
AWS::ElasticLoadBalancing::LoadBalancer	Name des Lastenausgleichsmoduls
AWS::S3::Bucket	arn:aws:s3:::<Bucket Name>

Die CI-Übereinstimmung für ein Testergebnis wird in Configuration Management Database (CMDB) möglicherweise nicht genau gefunden, es sei denn, das gleiche Format der `object_id` wird in der Suchregel verwendet. Meistens finden die OOB CI-Suchregeln eine Übereinstimmung für die am häufigsten verwendeten Ressourcentypen für Microsoft Defender for Cloud Integration und Palo Alto Prisma Cloud. Wenn die folgenden CI-Suchregeln die CIs in CMDB für Ihre Testergebnisse nicht finden, können Sie eine CI-Suchregel für einen Ressourcentyp

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellen. Weitere Informationen zum Erstellen einer CI-Suchregel finden Sie unter CI-Suchregel erstellen.

CI-Suchregeln

Die folgenden CI-Suchregeln gelten spezifisch für Microsoft Defender for Cloud Integration und Palo Alto Prisma Cloud.

S3-Bucket

Diese Suchregel versucht, das CI in CMDB anhand des Werts zu finden, der durch Verketten von `arn:aws:s3:::` und Ressourcenname erhalten wurde. Der erhaltene Wert wird in der Spalte „`object_id` “ der Tabelle „`cmdb_ci_cloud_object_storage`“ gesucht. Diese Suchregel gilt nur, wenn der Ressourcentyp `AWS::S3::Bucket`ist.

Name

Diese Suchregel versucht, das CI in CMDB anhand des Namens zu finden. Der Name, der in der Spalte `Object_id` der CI-Klasse gesucht wird, entspricht einem Ressourcentyp in der Tabelle `sn_capi_resource_type`.

Hinweis:
Für die Anwendung Palo Alto Prisma Cloud wird diese CI-Suchregel nur für die Ressourcentypen `AWS::RDS::DBInstance`, `AWS::ElasticLoadBalancing::LoadBalancer`und `AWS::CloudTrail::Trail` ausgeführt. Sie können die Ressourcentypen hinzufügen, für die Sie diese CI-Suchregel ausführen möchten.

Ressourcen-ID

Diese Suchregel versucht, das CI in CMDB anhand der Ressourcen-ID zu finden. Die Ressourcen-ID, die in der Spalte `Object_id` der CI-Klasse gesucht wird, entspricht einem Ressourcentyp in der Tabelle `sn_capi_resource_type`.

Hinweis:
Sie können die Priorität für eine CI-Suchregel im Feld **Reihenfolge** festlegen. Die CI-Suchregel mit dem niedrigsten Reihenfolgewert wird zuerst ausgeführt.

Vulnerability Response Arbeitsbereiche

Vulnerability Response-Arbeitsbereiche bieten eine konsolidierte Ansicht der Funktionen, mit der Sie im selben Bereich mehrere Aufgaben durchführen können, wodurch die Produktivität gesteigert und Zeit gespart wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Arbeitsbereiche

Arbeitsbereich des Schwachstellenmanagers	Arbeitsbereich für IT-Korrekturen	Arbeitsbereich der Schwachstellenbewertung
Erfahren Sie mehr über den Arbeitsbereich des Schwachstellenmanagers	Erfahren Sie mehr über den Arbeitsbereich für IT-Fehlerkorrekturen	Erfahren Sie mehr über den Arbeitsbereich der Schwachstellenbewertung

Bevor Sie beginnen

Bevor Sie die Arbeitsbereiche verwenden können:

- Sie müssen einige Konfigurationsaufgaben ausführen. Weitere Informationen finden Sie unter Konfigurieren Sie die Arbeitsbereiche Vulnerability Response ..
- Überprüfen Sie wichtige Informationen über Aktualisierungen von Korrekturaufgaben, Regeln für Korrekturaufgaben sowie wichtige Begriffe und Konzepte zu den Arbeitsbereichen in Vulnerability Response Arbeitsbereiche und Updates für Korrekturaufgaben und Regeln für Korrekturaufgaben.

Problembehandlung und Hilfe

- Security Operations in der ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Vulnerability Response Übersicht über -Arbeitsbereiche

Die Arbeitsbereiche für Schwachstellenmanager und IT-Nachbesserungen unterstützen Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance.

Die Arbeitsbereiche für Schwachstellenmanager, IT-Nachbesserung und Schwachstellenbewertung

Vulnerability Manager Workspace

Schützen Sie als Schwachstellenmanager die Assets Ihres Unternehmens vor Malware und böswilligen Angriffen. In einem zentralen Arbeitsbereich in Ihrem Now Platform®können Sie mit der Anwendung Vulnerability Response zusammen mit aktuellen Schwachstellendaten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die aus Schwachstellenbibliotheken und Scannerdatenanwendungen von Drittanbietern in Ihre Instanz importiert wurden, kritische Schwachstellen und Fehlkonfigurationen identifizieren, priorisieren und Listen mit Korrekturmaßnahmen senden Aufgaben an die IT übergeben, damit ihre Spezialisten sie bearbeiten können.

IT Remediation Workspace

Als IT-Spezialist können Sie Listen oder Korrekturaufgaben (RT) verwenden, die von Schwachstellenmanagern gesendet werden, um kritische Schwachstellen zu überwachen und zu beheben, die Ihnen oder Ihren Gruppen zugewiesen sind. Korrigieren Sie Gruppen von angreifbaren Elementen mit Patches, Lösungen, erneuten Scans von Schwachstellen, Change-Anforderungen, Ausnahmen und anderen Tools, um angreifbare Elemente zu korrigieren und die Testergebnisse von einem zentralen Ort aus zu testen.

Arbeitsbereich der Schwachstellenbewertung

Führen Sie als Manager für Schwachstellenereignisse Bewertungen des Gefahrenpotenzials durch, und verwalten Sie proaktiv kritische Schwachstellenereignisse, insbesondere während kritischer Schwachstellenereignisse wie Zero-Day-Ereignisse.

Schlüsselfunktionen

Die Arbeitsbereiche Vulnerability Response enthalten die folgenden Funktionen und Erweiterungen.

- Verwenden Sie die Funktion Massenbearbeitung in Vulnerability Manager Workspace, um mehrere Datensätze gleichzeitig zu aktualisieren. Weitere Informationen finden Sie unter Massenbearbeitung in verwenden Vulnerability Manager Workspace.
- Zeigen Sie die Dashboards für Schwachstellenmanagement (PA), Schwachstellengenehmigungen, CISO, Übersicht über Container-Schwachstellenmanagement, Dashboard für Anwendungsschwachstellenmanagement, Unified Vulnerability Response und Integrität in der Next Experience-UI auf der Seite „Dashboards“ des Arbeitsbereichs des Schwachstellenmanagers an. Weitere Informationen finden Sie unter Seite „Dashboards“ im Vulnerability Manager Workspace.
- Zeigen Sie das Dashboard zur Schwachstellenkorrektur in der Next Experience-UI auf der Seite „Dashboards“ des IT-Korrekturarbeitsbereichs an. Weitere Informationen finden Sie unter Seite „Dashboards“ im IT Remediation Workspace.
- Erstellen Sie die Korrekturaufgaben (VUL, AVUL, CVUL oder CRG) manuell in Vulnerability Manager Workspace und IT Remediation Workspace. Weitere Informationen finden Sie unter Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Manager Workspace und Erstellen Sie manuell eine Korrekturaufgabe in IT Remediation Workspace.
- Teilen Sie die Korrekturaufgaben (VUL, AVUL, CVUL und CRG) in Vulnerability Manager Workspace und IT Remediation Workspaceauf. Weitere Informationen finden Sie unter Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace bzw. Teilen Sie eine Korrekturaufgabe in in IT Remediation Workspace.
- Fordern Sie in den Arbeitsbereichen für Schwachstellenmanager und IT-Korrekturrichtlinienausnahmen für angreifbare Elemente (VITs, AVITs und CVITs) und Korrekturaufgaben (VUL, AVUL, CVUL und CRG) an. Weitere Informationen finden Sie unter Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace bzw. Ausnahme anfordern mit GRC: Richtlinien- und Compliance-Management in IT Remediation Workspace.
- Erstellen und verfolgen Sie kritische Schwachstellenereignisse über das Krisenmanagement für Schwachstellen (Vulnerability Crisis Management, VCM). Weitere Informationen finden Sie unter Erkunden Sie den Arbeitsbereich der Schwachstellenbewertung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fügen Sie der Bibliothek für Ausgleichssteuerungen in Vulnerability Manager WorkspaceAusgleichssteuerungen hinzu. Weitere Informationen finden Sie unter Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu.
- Fordern Sie im Arbeitsbereich für IT-Korrekturen eine Risikominderung für ein angreifbares Hostelement und eine Korrekturaufgabe an. Weitere Informationen finden Sie unter Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an.
- Erstellen Sie ein Agile-Problem und ein Jira-Problem für angreifbare Elemente in Anwendungen und Containern aus Vulnerability Manager Workspace. Weitere Informationen finden Sie unter Erstellen Sie ein Agile-Problem manuell mithilfe einer Formularaktion und Erstellen Sie ein Agile-Problem manuell mithilfe einer Listenaktion.

Weitere Informationen zur Versionskompatibilität mit den Familienreleases finden Sie im Artikel KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen in der HI Knowledge Base.

Patchen Sie die Orchestrierung mit den -Arbeitsbereichen Vulnerability Response .

Sie können Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen Ihrer Assets mit -Patch-Orchestrierung mit Vulnerability Responseverwalten.

Patch-Orchestrierung in den -Arbeitsbereichen

Bei der Patch-Orchestrierung mit der Anwendung Vulnerability Response werden geplante Importe von Lösungsintegrationen von Drittanbietern, Patch-Lieferanten und Schwachstellen-Scannern verwendet.

Die Patch-Orchestrierung mit der Anwendung Vulnerability Response wird sowohl in der klassischen Umgebung als auch in den Arbeitsbereichen Vulnerability Response unterstützt. Korrelierte Daten werden zusammengefasst und sowohl in den Arbeitsbereichen als auch in der klassischen Umgebung angezeigt. Eine Übersicht über die Funktionen, Anforderungen und Informationen zur Patch-Orchestrierung in der klassischen Umgebung finden Sie unter Patch-Orchestrierung mit Vulnerability Response.

- Weitere Informationen zu den unterstützten Integrationen mit Patch-Anbietern finden Sie unter Informationen zur Integration der HCL BigFix Patch Orchestration in mit Vulnerability Response und Informationen zur Integration der Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM.
- Informationen zum Planen von Patches für Formulardatensätze in den -Arbeitsbereichen finden Sie unter Planen Sie Patches mit der MicrosoftMicrosoft Azure Event Hubs SCCM-Integration mit Vulnerability Response und Planen Sie -Patches mit der Vulnerability Response Patch Orchestration Integration HCL BigFix.

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

Zum Anzeigen von Patch Orchestration-Daten und verfügbaren Updates (Patches) in den Arbeitsbereichen in Vulnerability Responsesind die folgenden Anwendungen erforderlich. Alle aufgeführten Anwendungen sind unter ServiceNow® Storeverfügbar. Einige Anwendungen erfordern separate Abonnements. Weitere Informationen finden Sie unter Patch-Orchestrierung mit Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rollen

Zusätzlich zu den für die Arbeitsbereiche Vulnerability Response erforderlichen Rollen sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin benötigen Benutzer Rollen, die spezifisch für die Patch Orchestration-Integrationen sind, die Sie zum Anzeigen von Daten und Planen von Patches verwenden. Weitere Informationen zu diesen Rollen finden Sie in den folgenden unterstützten Integrationen.

Siehe Informationen zur Integration der HCL BigFix Patch Orchestration in mit Vulnerability Response und Informationen zur Integration der Vulnerability Response Patch Orchestration mit MicrosoftMicrosoft Azure Event Hubs SCCM.

Patchen Sie Daten in den -Arbeitsbereichen Vulnerability Response .

Im Arbeitsbereich für IT-Korrekturenkönnen Sie Patchdaten in den folgenden Arbeitsbereichen anzeigen:

- Klicken Sie in der Ansicht Homepage auf Bewertungslisten, um Datensätze für Bevorzugte Lösungen für VIs, Angreifbare CIs und Bevorzugte Patches für VIs anzuzeigen.
- Zeigen Sie in der Listenansicht alle Patch-Update-Datensätze (VPUs) und die angreifbaren Elemente an, die Ihnen zugewiesen sind und die Patches von den verfügbaren Links enthalten.

Sie können Patches von den folgenden Datensätzen aus planen:

- Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkanntes Element (SDI)

Im Arbeitsbereich des Schwachstellenmanagers, können Sie Patches anzeigen:

- In der Ansicht „Startseite“ zu Überwachungsthemen auf der Registerkarte „Angreifbare Elemente“ können Sie bevorzugte und potenzielle Patches, geplante Patch-Daten und andere Informationen anzeigen.
- In der Listenansicht für Korrekturmaßnahmen-Datensätze können Sie Patch-Daten für VIT-Datensätze auf der Registerkarte Angreifbare Elemente anzeigen.

Vulnerability Response Arbeitsbereiche und Updates für Korrekturaufgaben und Regeln für Korrekturaufgaben

Korrekturaufgaben bündeln Datensätze (VITs, AVITs, CVITs oder CTRs) in den Vulnerability Response -Arbeitsbereichen.

Schlüsselbegriffe für die -Arbeitsbereiche Vulnerability Response .

Vulnerability Response-Arbeitsbereiche oder -Arbeitsbereiche

Vulnerability Response unterstützt die Vulnerability Response -Arbeitsbereiche. Sie können entweder die klassische Experience Core-UI oder die -Arbeitsbereiche verwenden.

Klassische Anwenderoberfläche (veraltet).

Bezieht sich auf die Experience Core-UI. In der klassischen Umgebung führen Sie dennoch einige Aktionen aus und zeigen einige Listen an.

Arbeitsbereich des Schwachstellenmanagers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Arbeitsbereich überwachen Manager gezielte Schwachstellen und wählen die VIs und Testergebnisse aus, die für sie am wichtigsten sind, um sie der IT zuzuweisen.

Arbeitsbereich für IT-Korrekturen

In diesem Arbeitsbereich können sich IT-Teams auf die wichtigsten Schwachstellen konzentrieren, die ihnen durch die Sicherheit zugewiesen wurden. IT-orientierte Informationen, zu denen betroffene, unterschiedliche Configuration Items (CIs), Lösungen und Korrekturfortschritt gehören, sind für Korrekturbesitzer in diesem Arbeitsbereich leicht verfügbar.

Arbeitsbereich der Schwachstellenbewertung

In diesem Arbeitsbereich können Schwachstellenanalysten während der Zero-Day-Schwachstellenanalyse eine Schwachstellenbewertung durchführen. Nachdem eine Zero-Day-Schwachstelle identifiziert wurde, können sie die potenziellen Auswirkungen und Risiken bewerten, die mit der Schwachstelle verbunden sind. Die Analysten können die betroffenen System-, Anwendungs- oder Netzwerkkomponenten analysieren, um den Schweregrad und mögliche Angriffsvektoren innerhalb der Organisation zu verstehen.

Überwachungsthema

Überwachungsthemen definieren ein Segment der angreifbaren Elemente, die Schwachstellenmanager und Analysten im Arbeitsbereich des Schwachstellenmanagers überwachen möchten. Überwachungsthemen zeigen einen fokussierten Übersichtssatz von Berichten, die sich auf ein Segment von VIs und Testergebnisse beziehen, sowie Statistiken zu Trends, CI und Schwachstellen. Die Dashboards zu diesen Themen können zur Überwachung von Trends verwendet werden. Die Dashboards helfen Managern auch bei folgenden Aufgaben:

- Zeigen Sie den Korrekturfortschritt für kritische Elemente an
- Ermitteln Sie das Vorhandensein von Schwachstellen in kritischen Systemen
- Sehen Sie, wenn ein neuer Exploit veröffentlicht wird
- Schnelle Reaktion auf die Behebung einer bestimmten Gruppe von Schwachstellen fördern

Korrekturaufwand (RE)

Nachbesserungsmaßnahmen werden von Schwachstellenmanagern erstellt, wenn sie feststellen, dass es für die IT an der Zeit ist, die in einem Überwachungsthema aufgeführten Schwachstellen zu beheben. Schwachstellenmanager und -analysten können auswählen, wie sie Korrekturaufgaben erstellen möchten, z. B. nach Zuweisungsgruppe und Schwachstelle. Korrekturaufgaben sind in der Korrekturmaßnahme enthalten.

Korrekturaufgabe (VUL)

IT-Teams verwenden Korrekturaufgaben, um die ihnen von der Sicherheitsabteilung zugewiesenen Schwachstellen zu beheben. Korrekturaufgaben sind Listen der Aktionen, die zum Beheben von Schwachstellen erforderlich sind. Korrekturaufgaben werden automatisch erstellt, wenn Sicherheitsmanager Korrekturmaßnahmen erstellen.

Entwicklung der -Arbeitsbereiche

In früheren Versionen von Vulnerability Responsehatten Sie zwei Möglichkeiten, eine Reihe von Datensätzen (VITs, AVITs, CVITs oder CTRs) als Sicherheits- und Schwachstellenanalyst zu überwachen:

- Dashboard Übersicht, das alle VIs zusammenfasst
- Korrekturaufgaben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbare Elemente wurden gemäß Ihren vordefinierten Regeln für Korrekturaufgaben automatisch in Korrekturaufgaben sortiert. Korrekturaufgaben wurden entwickelt, um IT-Teams bei der Korrektur verwaltbarer Blöcke angreifbarer Elemente zu unterstützen.

Diese Automatisierung ermöglichte es, eine sehr große Anzahl von Datensätzen automatisch für Massenzuweisungen und -korrekturen zu gruppieren. Für Schwachstellenanalysten und -manager war es jedoch schwierig, den gesamten Satz von Datensätzen aus Korrekturaufgaben zu überwachen. Zusätzlich zu den Leistungsproblemen bei großen Gruppen kann es schwierig sein, funktionale Regeln für Korrekturaufgaben zu erstellen, die nur die Schwachstellen herausfiltern, die Sie am kritischsten gefunden haben.

Die Arbeitsbereiche Vulnerability Response :

- Helfen Sie Sicherheitsmanagern, aktive VIs und Testergebnisse im Laufe der Zeit herauszufiltern, zu überwachen und die Nachbesserung für die ihrer Meinung nach wichtigsten Schwachstellen voranzutreiben.
- Stellen Sie IT-Teams IT-orientierte Informationen an einem Ort bereit, mit denen sie die Schwachstellen beheben können, die ihnen von der Sicherheitsabteilung zugewiesen wurden.

Aktualisiert Korrekturaufgaben in den Arbeitsbereichen

Im Arbeitsbereich des Schwachstellenmanagers verwenden Schwachstellenanalysten und -manager *„Überwachungsthemen“* und *„Korrekturmaßnahmen“* als zwei neue Methoden zur Überwachung und Zuweisung von VIs zur Korrektur.

Schwachstellen-Gruppen werden umbenannt, *Korrekturaufgaben*. Diese Änderung gilt für Bezeichnungen in Listen, Datensätzen und Regeln sowohl in der Legacy-UI als auch in den Arbeitsbereichen. Korrekturaufgaben werden so eingerichtet, dass IT-Teams im IT-Korrekturarbeitsbereich mit ihnen arbeiten können. Die folgende Liste zeigt, wie Sie als Schwachstellenmanager oder Schwachstellenanalyst Schwachstellen und Testergebnisse überwachen, filtern und zuweisen können:

1. Im Arbeitsbereich des Schwachstellenmanagers überwachen Manager importierte Schwachstellen und Fehlkonfigurationen für Überwachungsthemen. Manager und Analysten verwenden Überwachungsthemen, um einen dynamischen Satz gefilterter Datensätze im Zeitverlauf zu überwachen, die ihrer Meinung nach am kritischsten sind.
2. Mit Überwachungsthemen können Sicherheitsmanager bestimmen, wann und welche Arten von VIs in Korrekturmaßnahmen an IT-Teams übergeben werden sollen. Diese REs sind statische Listen der VIs, die die Sicherheit von IT-Teams beheben möchte.

   Aus Korrekturmaßnahmen haben Manager vier Optionen, um Datensätze in Korrekturaufgaben (VULs, AVULs, CVULs oder CRGs) zu bündeln. Korrekturaufgaben werden IT-Teams automatisch basierend auf den Zuweisungsgruppen zugewiesen, die den Datensätzen ursprünglich zugeordnet waren.
3. IT-Teams arbeiten im IT-Fehlerkorrektur-Arbeitsbereich an Korrekturaufgaben, ohne alle Datensätze sortieren zu müssen.

   Eine Korrekturaufgabe durchläuft dieselben Status wie die Korrekturaufgabe in früheren Versionen von Vulnerability Response. Wenn alle Datensätze in einer Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen und auf **Inaktiv**gesetzt.

   Der Korrekturfortschritt wird in den Datenvisualisierungen zu den Überwachungsthemen und auf der Homepage für IT-Korrekturen aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisiert die Regeln für Korrekturaufgaben in den Arbeitsbereichen

Die Regeln für Schwachstellengruppen werden als *Regeln für Korrekturaufgaben*bezeichnet. Diese Änderung gilt für die Bezeichnungen von Listen, Datensätzen und Regeln sowohl in der Legacy-UI als auch in den Arbeitsbereichen.

Tabellennamen, z. B. [sn_vul_m2m_vul_group_item], werden nicht geändert.

Wenn Sie Schwachstellengruppen-Regeln in einer früheren Version von Vulnerability Responseerstellt haben, stehen sie Ihnen weiterhin zur Verfügung und werden als Korrekturaufgaben-Regeln bezeichnet.

In Arbeitsbereichen werden Korrekturaufgabenregeln jedoch nicht mehr als primäre Methode zum Organisieren einer großen Menge von Datensätzen für Korrekturaufgaben verwendet. Möglicherweise möchten Sie Ihre Regeln für Korrekturaufgaben inaktiv lassen, wenn Sie sich an die Arbeitsbereiche gefährden.

Möglicherweise möchten Sie stattdessen schrittweise die Vulnerability Response -Arbeitsbereiche verwenden.

1. Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Response durchführen, bleiben Ihre vorhandenen Regeln für Korrekturaufgaben erhalten. Sie stehen Ihnen weiterhin in den Arbeitsbereichen zur Verfügung. Die Standardgruppenregel Vulnerability ist standardmäßig inaktiv.
2. Konfigurieren Sie Zuweisungsregeln und, falls gewünscht, Risikoregeln, und führen Sie dann einen Import durch.
3. Als Schwachstellenmanager oder Analyst können Sie aus den Überwachungsthemen im Arbeitsbereich des Schwachstellenmanagers zu überwachende Segmente auswählen. Sie können Überwachungsthemen als eigenständige Funktionen verwenden. Wählen Sie eine beliebige Teilmenge von Datensätzen aus und verwenden Sie das Dashboard zur Überwachung von Trends. Mit ihnen können Sie entscheiden, wo und wann der Schwerpunkt der Korrekturmaßnahmen liegen soll.
4. Als Schwachstellenmanager oder -analyst erstellen Sie Korrekturmaßnahmen aus Überwachungsthemen, wenn Sie entscheiden, dass es an der Zeit ist, eine Teilmenge von Datensätzen zu korrigieren. Außerdem wird automatisch eine Korrekturaufgabe zur Übergabe an die IT erstellt, wenn Sie eine Korrekturmaßnahme erstellen.
5. Im Laufe der Zeit entdecken Sie als Schwachstellenmanager oder Analyst möglicherweise einige Routinemuster, die Sie automatisch mit Regeln für Korrekturaufgaben behandeln können.

Um Ihre Regeln für Korrekturaufgaben anzuzeigen, navigieren Sie im Menü **Alle** zu den entsprechenden Modulen **„Regeln für Korrekturaufgaben“** in Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance.

Weitere Informationen zu Zuweisungsregeln, Regeln für Korrekturaufgaben, Korrekturmaßnahmen und angreifbaren Elementen in den Vulnerability Response -Arbeitsbereichen

- Datensätze für Korrekturaufgaben werden in Listen und Datensätzen sowohl in der klassischen Umgebung als auch in den Arbeitsbereichen angezeigt.
- Eine Korrekturaufgabe durchläuft dieselben Status wie eine Schwachstellengruppe. Wenn alle Datensätze in einer Korrekturaufgabe geschlossen werden, geht die Korrekturaufgabe in den Status „Inaktiv“ über.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um Ihre Teams bei der Korrektur zu unterstützen, kann ein angreifbares Element nur in einer Korrekturmaßnahme enthalten sein. Sobald es sich in einer Korrekturmaßnahme befindet, wird ein angreifbares Element keinen anderen von Ihnen erstellten Korrekturmaßnahmen hinzugefügt.
- Wenn Sie eine Korrekturmaßnahme löschen, wird die Korrekturmaßnahme inaktiv, und alle aktiven AEs sind für neue Korrekturmaßnahmen verfügbar.
- Ein Datensatz (VIT, AVIT, CVIT oder CTR) kann Teil mehrerer Korrekturaufgaben sein.
- Korrekturaufgaben werden IT-Teams automatisch basierend auf der Zuweisungsgruppe zugewiesen, die einem angreifbaren Element in einer Korrekturmaßnahme zugeordnet ist. Wenn Sie bei Bedarf eine Korrekturaufgabe erstellen, wählen Sie die Zuweisungsgruppe aus.
- Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Responsedurchführen, wurden Ihre Zuweisungsregeln in der Legacy-UI beibehalten.
- Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Responsedurchführen, werden Ihre aktuellen Benutzer und Gruppen geerbt und sind für Sie in den Arbeitsbereichen zugänglich.

Weitere Informationen zu den Lebenszyklen von Korrekturmaßnahmen finden Sie unter Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen.

Konfiguration und Setup für die Vulnerability Response -Arbeitsbereiche

Weitere Informationen zu Zuweisungsregeln und Regeln für Korrekturaufgaben finden Sie unter Konfigurieren Sie die Arbeitsbereiche Vulnerability Response . und Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn Sie ein neuer Kunde sind und noch keine Kunden hinzugefügt haben, müssen Sie Benutzer und Gruppen so einrichten, dass angreifbare Elemente und Korrekturaufgaben den gewünschten Korrekturgruppen zugewiesen werden. Vulnerability Response-Zuweisungsregeln werden verwendet, um Gruppen Arbeit zuzuweisen.

Konfigurieren Sie die Arbeitsbereiche Vulnerability Response .

Bevor Sie die Arbeitsbereiche verwenden können, bestätigen Sie, dass Sie die folgenden Setupaufgaben abgeschlossen haben.

Vorbereitungen
Erforderliche Rolle: admin zum Zuweisen von Rollen an Benutzer und Gruppen sowie für Benutzer an Gruppen.

sn_vul.vulnerability_admin für die Bearbeitung, das Erstellen von Regeln und die Konfiguration der Anwendung Vulnerability Response.

Bestätigen Sie, dass Sie die folgenden Setupaufgaben abgeschlossen haben. Weitere Informationen zur Ausführung dieser Aufgaben finden Sie in den Schritten nach der Liste.

Aufgabe	Beschreibung
☐	Wenn noch nicht zugewiesen, weisen Sie Anwendern und Gruppen die richtigen Rollen zu, damit sie Zugriff auf die -Arbeitsbereiche haben.

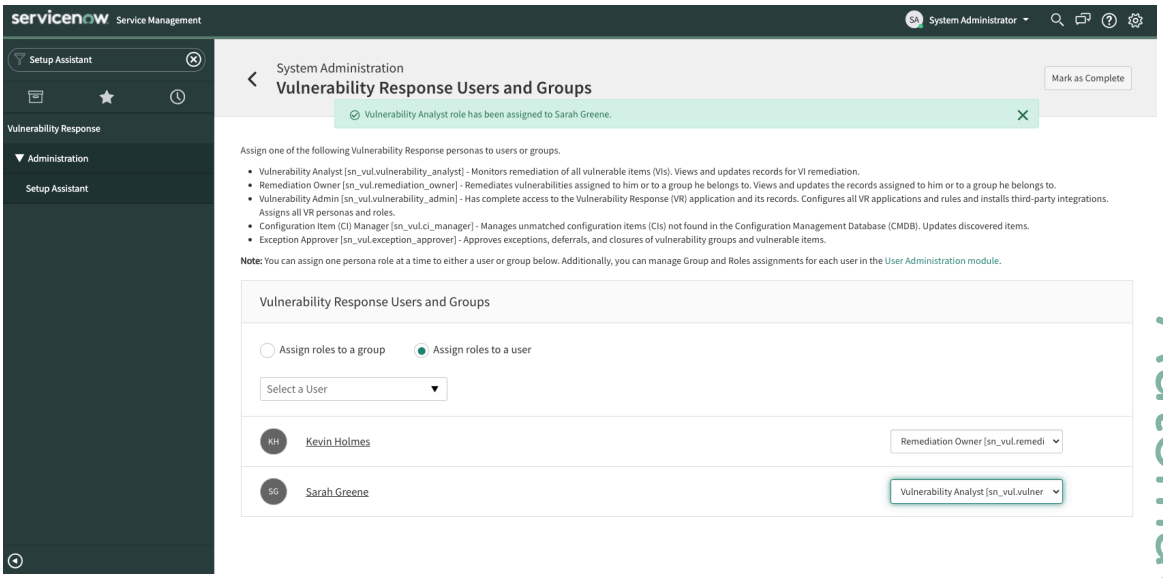
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Erforderliche Rolle: admin. Weitere Informationen finden Sie in den folgenden Schritten.
☐	Richten Sie Zuweisungsregeln ein, damit angreifbare Elemente den richtigen Gruppen zur Korrektur zugewiesen werden. Erforderliche Rolle: sn_vul.vulnerability_admin. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Sie erstellen und bearbeiten Zuweisungsregeln in der klassischen Umgebung.
☐	(Optional): Bearbeiten oder erstellen Sie Ihre Regeln für Korrekturaufgaben. Erforderliche Rolle: sn_vul.vulnerability_admin. **Hinweis:** Funktional funktionieren Korrekturaufgabenregeln genau wie Korrekturaufgabenregeln in früheren Versionen von Vulnerability Response. Im Gegensatz zu den Schwachstellen-Gruppen, die automatisch aus den Regeln für Korrekturaufgaben erstellt wurden, werden Korrekturaufgaben jedoch erstellt, wenn Sie Korrekturmaßnahmen erstellen. Sie haben folgende Optionen, um die angreifbaren Elemente in einer Korrekturmaßnahme in Korrekturaufgaben zu bündeln: • Nach Zuweisungsgruppe • Nach Zuweisungsgruppe und Configuration Item • Nach Zuweisungsgruppe und Schwachstelle • Keine: Verwenden Sie diese Option, wenn Sie einer Korrekturaufgabe manuell VIs hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace. Weitere Informationen zur automatischen Gruppierung von VIs und zur erneuten Anwendung der Gruppenregeln in der klassischen Umgebung finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.
☐	Bearbeiten Sie die Korrekturzielregeln. Erforderliche Rolle: sn_vul.vulnerability_admin. Fügen Sie in der klassischen Umgebung Korrekturzielregeln hinzu. Weitere Informationen zu Korrekturzielregeln finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Nachdem Sie die Anwendung Vulnerability Response installiert und aktiviert haben, navigieren Sie in der klassischen Umgebung als Benutzer mit der Administratorrolle zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.



2. Weisen Sie im Setup-Assistenten Benutzer den folgenden Gruppen zu.

Hinweis:
1000 ist der Grenzwert für die Anzahl der Anwendergruppen, denen ein Benutzer in den Vulnerability Response-Arbeitsbereichen zugewiesen werden kann.

Die folgenden Gruppen werden mit der Anwendung Vulnerability Response bereitgestellt und in den -Arbeitsbereichen verwendet. Im Setup-Assistenten können Sie Benutzer zuweisen:

- Korrekturbesitzer – Diese Gruppe ist für IT-Korrekturbesitzer im IT-Korrektur-Arbeitsbereich vorgesehen. Benutzer mit dieser Rolle beheben Schwachstellen, die ihnen in Korrekturaufgaben zugewiesen wurden.

  Hinweis:

  Wenn Sie möchten, dass Ihre Remediationsbesitzer Change-Anforderungen erstellen und anzeigen sowie Daten zu angreifbaren Konfigurationselementen (Configuration Item, CI) im IT-Korrekturarbeitsbereich und in der klassischen Umgebung anzeigen, weisen Sie ihnen die Rolle itil zu. Unter Umständen möchten Sie die Rolle itil einzelnen Benutzern anstatt allen Mitgliedern einer Gruppe zuweisen. Die Rolle cmdb_read ist auch eine Option für Benutzer zum Anzeigen von CI-Daten in den Arbeitsbereichen.

- Ab v16.1 können Sie E-Mail-Erinnerungen für Ihre IT-Korrekturbesitzer einrichten. Informationen zum Einrichten von E-Mail-Benachrichtigungen für die Arbeitsbereiche finden Sie unter Richten Sie E-Mail-Benachrichtigungen in den -Arbeitsbereichen Vulnerability Response ein.
- Schwachstellenadministrator: Diese Gruppe ist für Schwachstellenmanager vorgesehen. Diese Rolle konfiguriert die Anwendung Vulnerability Response im Setup-Assistenten. Diese Rolle verfügt auch über die Berechtigung zur Verarbeitung von Ausnahme- und falsch positiven Anforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schwachstellenanalyst: Diese Gruppe ist für Sicherheitsmanager, Schwachstellenmanager und Analysten im Arbeitsbereich des Schwachstellenmanagers vorgesehen. Diese Rolle überwacht Schwachstellen, erstellt Überwachungsthemen und Korrekturmaßnahmen und überwacht den Fortschritt der Korrektur.
- Falsch-positiv-Genehmiger: Anwender in dieser Gruppe verarbeiten falsch-positive Anforderungen für angreifbare Elemente oder Korrekturaufgaben. Eine falsch positive Anforderung erfordert einen einstufigen Genehmigungsprozess. Sie können das Zuweisen von Anwendern zu dieser Gruppe außerhalb des Setup-Assistenten in **der Anwenderverwaltung**verwalten.
- Ausnahmegenehmiger: Eine Ausnahmeanforderung für ein angreifbares Element oder eine Korrekturaufgabe wird mit einem standardmäßigen, zweistufigen Genehmigungsworkflow genehmigt. Die Ausnahmeanforderung erfordert zwei Ebenen von Genehmigern. Fügen Sie beiden Genehmigungsgruppen Benutzer hinzu: „Ausnahmegenehmiger – Ebene 1“ und „Ausnahmegenehmiger – Ebene – 2“. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der zweiten Ebene gesendet. Das Zuweisen von Anwendern zu dieser Gruppe verwalten Sie außerhalb des Setup-Assistenten in **Anwenderadministration**.

Hinweis:
Fügen Sie den Genehmigungsgruppen Anwender hinzu, bevor Sie falsch positive Ergebnisse und Ausnahmeanforderungen übermitteln. Wenn Sie Anforderungen erstellen, bevor Sie Benutzer mit Genehmigungsberechtigung zuweisen, sind die Anforderungen für diese möglicherweise nicht sichtbar.

Klicken Sie alternativ auf den Link **Benutzeradministration**, um die folgenden granularen Rollen zu verwalten und Ihren Anwendern und vorhandenen Gruppen zuzuweisen. Mit diesen Rollen können Benutzer bestimmte Aktionen in der Anwendung Vulnerability Response und in Arbeitsbereichen ausführen.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Um Change-Anforderungen im IT-Arbeitsbereich für Korrekturen und in der klassischen Umgebung zu erstellen und anzuzeigen, weisen Sie ihnen die Rolle itil zu.

Unter Vulnerability Response Personae und granulare Rollen und Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu finden Sie weitere Informationen über das Zuweisen von Persona-Rollen zu Benutzern und von Benutzern zu Gruppen.

3. Korrekturaufgaben werden bei der Erstellung automatisch zur Verarbeitung an IT-Korrekturzuweisungsgruppen übergeben.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Configuration Item
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine: Verwenden Sie diese Option, wenn Sie einer Korrekturaufgabe manuell VIs hinzufügen möchten.

   Hinweis:
   Für Version 18.0 von Vulnerability Responseist die Option **Keine** nicht verfügbar.

   Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Responsedurchführen, bleiben Ihre Zuweisungsgruppen erhalten. Möglicherweise möchten Sie diese Gruppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

jedoch so bearbeiten, dass angreifbare Elemente bestimmten Zuweisungsgruppen zugeordnet werden, bis Sie sich mit der Funktionsweise von Überwachungsthemen und Korrekturmaßnahmen vertraut gemacht haben. Beispielsweise können Sie Zuweisungsgruppen nach Produkt oder Region erstellen, Sie können aber auch beliebige Kriterien verwenden, die für Ihre Organisation am besten geeignet sind.

Sie können auch Zuweisungsregeln verwenden, um Gruppen Korrekturaufgaben zuzuweisen. Unter Umständen möchten Sie nur Regeln mit hoher Priorität für die folgenden Elemente ausführen:

- Elemente, die eine besondere Behandlung erfordern
- Elemente, bei denen das Risiko kritisch ist oder bei denen ein AE eine Behandlung durch Compliance-Abteilungen erfordert

Die folgenden mit der Anwendung bereitgestellten Zuweisungsregeln sind standardmäßig aktiv:

- Stillgelegte CI-Zuweisungsregel
- An CI-Supportgruppe zuweisen
- Zuweisungsregel für Arbeitsplatz-PCs
- Datenbank-Zuweisungsregel
- Zuweisungsregel für Webanwendungen
- Windows Server-Zuweisungsregel
- Zuweisungsregel für Nicht-Windows-Server
- Alle Zuweisungsregeln erfassen

Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Sie erstellen und bearbeiten Zuweisungsregeln in der klassischen Umgebung.

4. **Wahlweise:** Bearbeiten oder erstellen Sie Ihre Regeln für Korrekturaufgaben.

   (Optional) In den Arbeitsbereichen werden Korrekturaufgaben erstellt, wenn Sie Korrekturmaßnahmen erstellen. Sie haben folgende Optionen, um die angreifbaren Elemente in einer Korrekturmaßnahme in Korrekturaufgaben zu bündeln:

   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Configuration Item
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine: Verwenden Sie diese Option, wenn Sie einer Korrekturaufgabe manuell VIs hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace.

   Hinweis:
   InVersion 18.0 von Vulnerability Responseist die Option **Keine** nicht verfügbar.

   Weitere Informationen zur automatischen Gruppierung von VIs und zur erneuten Anwendung der Gruppenregeln in der klassischen Umgebung finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

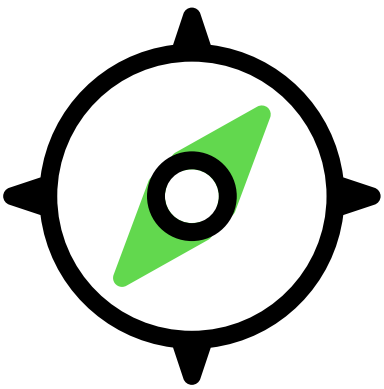
Vulnerability Manager Workspace

Mit Vulnerability Manager Workspace können Schwachstellenmanager und -analysten die Schwachstellen und Fehlkonfigurationen überwachen, die für sie am wichtigsten sind, und strategisch entscheiden, welche Schwachstellen sie an IT-Teams senden, um sie zu beheben.

V18.0 Arbeitsbereich des Schwachstellenmanagers – Demo

Erste Schritte

Untersuchen

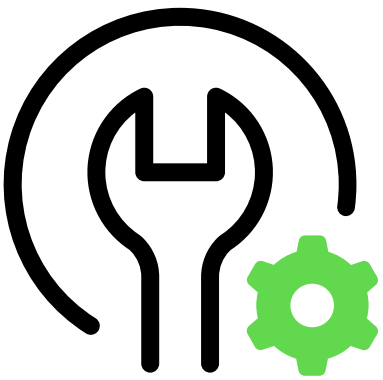


Erfahren Sie mehr über die Funktionen in Vulnerability Manager Workspace

Überwachen und verwalten

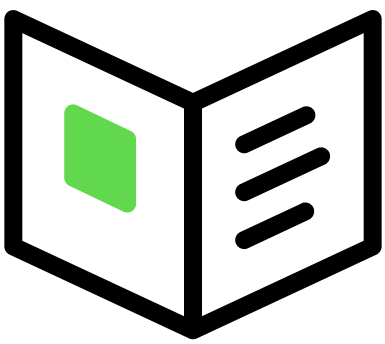
Erfahren Sie, wie Sie angreifbare Elemente (VITs, AVITs und CVITs) und Testergebnisse in überwachen und verwalten Vulnerability Manager Workspace

Beheben



Erfahren Sie, wie Sie angreifbare Elemente (VITs, AVITs und CVITs) und Testergebnisse in korrigieren Vulnerability Manager Workspace

Referenz



Erfahren Sie mehr über die zusätzlichen Informationen, die für die Verwendung von erforderlich sind Vulnerability Manager Workspace

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations in der ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Vulnerability Manager Workspace erkunden

Als Schwachstellenmanager und -analyst erhalten Sie eine einheitliche Ansicht aller Schwachstellentypen in der Vulnerability Manager Workspace. Sie können Schwachstellen bei Hosts, Anwendungen und Containern sowie Konfigurationsprobleme anzeigen, Überwachungsthemen für diese Schwachstellen und Fehlkonfigurationen erstellen sowie Korrekturmaßnahmen und Korrekturaufgaben erstellen.

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Sie können Vulnerability Manager Workspace anzeigen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.

Vulnerability Manager Workspace besteht aus den folgenden Seiten:

Homepage

Besteht aus vordefinierten Filtern, die zur Visualisierung der Zusammenfassung von Host-Schwachstellen, Anwendungsschwachstellen, Container-Schwachstellen und Konfigurationstestergebnissen verwendet werden.

Weitere Informationen zur Homepage finden Sie unter Homepage im Vulnerability Manager Workspace.

Hinweis:
Ab v21.0 von Vulnerability Responsewerden die Überwachungsthemen auf der Seite „Überwachungsthemen“ angezeigt.

Seite „Überwachungsthemen“.

Besteht aus einer Liste von Überwachungsthemen, die in vier Module kategorisiert sind: Host-Schwachstellen, Anwendungsschwachstellen, Container-Schwachstellen und Konfigurationstestergebnisse.

Weitere Informationen zu Überwachungsthemen finden Sie unter Seite „Überwachungsthemen“ im Vulnerability Manager Workspace.

Seite „Dashboards“.

Besteht aus den Dashboards für Schwachstellenmanagement, Schwachstellenmanagement (PA), Schwachstellengenehmigungen, CISO, Container Vulnerability Management (Übersicht), Application Vulnerability Management, Unified Vulnerability Response und Integrität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Seite „Dashboards“ im Vulnerability Manager Workspace.

Hinweis:
Die Seite „Dashboards“ wird ab Version 19.0 von Vulnerability Responseangezeigt.

Listen-Seite

Besteht aus den standardmäßigen und anwenderdefinierten Listenseiten für Korrekturmaßnahmen, Korrekturaufgaben, angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente, Konfigurationstestergebnisse, Ausnahmen, Genehmigungen und Bibliotheken.

Weitere Informationen finden Sie unter Listenseite im Vulnerability Manager Workspace.

Zeigen Sie ein Workflow-Beispiel in an Vulnerability Manager Workspace

Sehen Sie sich ein Beispiel für einen End-to-End-Workflow im Vulnerability Manager Workspacean. Erfahren Sie, wie ein Schwachstellenmanager oder Analyst den Arbeitsbereich zur Überwachung kritischer Datensätze und zur Erstellung von Korrekturaufgaben zur Übergabe an die IT-Abteilung verwenden kann.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

Klicken Sie auf das folgende Video, um die Schritte des Workflows anzuzeigen.
Vulnerability Manager Workspace Demo

Das vorherige Video enthält die folgenden Aufgaben:

a. Klicken Sie auf ein Überwachungsthema auf der Seite **Überwachungsthemen** des Arbeitsbereichs, um Daten in einem Dashboard anzuzeigen.

b. Erstellen Sie mithilfe von Filterbedingungen ein Überwachungsthema, und zeigen Sie eine Vorschau der übereinstimmenden Datensätze an. Weitere Informationen zum Erstellen eines Überwachungsthemas finden Sie unter Erstellen Sie ein Überwachungsthema in Vulnerability Manager Workspace.

c. Zeigen Sie Daten zu Datensätzen und den zugehörigen Configuration Items auf der Registerkarte **„Betroffene CIs“** für ein Überwachungsthema an. Weitere Informationen zu den Visualisierungen finden Sie unter Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema.

d. Zeigen Sie Daten zu Schwachstellen auf der Registerkarte **„Eindeutige Schwachstellen“** für ein Überwachungsthema an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Zeigen Sie die mit dem Überwachungsthema verknüpften Datensätze auf der Registerkarte **Angreifbare Elemente** oder **Konfigurationstestergebnisse** für ein Überwachungsthema an. Scrollen Sie nach rechts, um in der Spalte Korrekturmaßnahme anzuzeigen, welche Datensätze sich bereits in einer Korrekturmaßnahme befinden.

f. Wählen Sie **Korrekturmaßnahme erstellen** für ein Überwachungsthema aus, wenn Sie bereit sind, Aufgaben für bestimmte Arten von Datensätzen zu erstellen und sie der IT zur Korrektur zuzuweisen. Weitere Informationen zum Erstellen von Korrekturmaßnahmen finden Sie unter Erstellen Sie eine Korrekturmaßnahme in Vulnerability Manager Workspace.

g. Wählen Sie die **Listenansicht** aus, um Listen Ihrer Korrekturbemühungen, Korrekturaufgaben, Datensätze, Ausnahmen und Genehmigungen anzuzeigen. Weitere Informationen zur Seite Listen finden Sie unter Listenseite im Vulnerability Manager Workspace.

h. Wählen Sie in der Listenansicht die Liste **Aktive** Korrekturmaßnahme aus, um einen Datensatz für eine Korrekturmaßnahme zu öffnen und den Status und Informationen zum Datensatz anzuzeigen. Weitere Informationen finden Sie unter Listenseite im Vulnerability Manager Workspace.

i. Wählen Sie im Datensatz der **Korrekturmaßnahme** die Registerkarte Korrekturaufgabe aus, um die mit dem Korrekturdatensatz verknüpften Korrekturaufgaben anzuzeigen. Weitere Informationen finden Sie unter Listenseite im Vulnerability Manager Workspace.

j. Wählen Sie im jeweiligen Korrekturmaßnahmen-Datensatz die Registerkarte **„Angreifbare Elemente“**, **„Angreifbare Anwendungselemente** “, **„Angreifbare Container-Elemente** “ oder **„Konfigurationstestergebnisse“,** um eine Liste der Datensätze anzuzeigen, die einer Korrekturmaßnahme zugeordnet sind. Weitere Informationen finden Sie unter Listenseite im Vulnerability Manager Workspace.

k. Wenn Sie bei Bedarf aus der Korrekturmaßnahme für eine Teilmenge von Datensätzen eine neue Korrekturaufgabe erstellen möchten, wählen Sie die zu verschiebenden Datensätze aus, und klicken Sie auf **Korrekturaufgabe erstellen**. Weitere Informationen finden Sie unter Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace

Homepage im Vulnerability Manager Workspace

Die Homepage im Vulnerability Manager Workspace bietet eine Zusammenfassung der aktiven Datensätze. Dazu werden Visualisierungen von Risikobewertungen, Korrekturfortschritten, Zuweisungen zu Zuweisungsgruppen, Datensätzen in Korrekturaufgaben und Schwachstellen aus Cloud-Ressourcen angezeigt.

Auf der Homepage können Sie die Visualisierungen für die vorgefilterten angreifbaren Host-Elemente, angreifbaren Container-Elemente, angreifbaren Anwendungselemente und die Ergebnisse der Konfigurationstests anzeigen. Sie können auch Visualisierungen für eine Reihe von gewünschten Datensätzen anzeigen, indem Sie Filter erstellen und anwenden. Weitere Informationen zum Erstellen, Aktualisieren, Anwenden und Löschen von Filtern finden Sie unter Zusammenfassung aktiver Datensätze (VITs, AVITs, CVITs und CTRs) erstellen und anwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp:

Wenn die Systemeigenschaft *sn_vul_cmn_ws.navigate_to_workspace* vom Administrator auf true festgelegt wird, werden nach Auswahl der vordefinierten Filterlinks in den Modulen „Angreifbare Elemente“, „Angreifbare Anwendungselemente“, „Angreifbare Container-Elemente“ und „Testergebnisse“ im Menü „ **Alle** “ diese Links in Vulnerability Manager Workspacegeöffnet Startseite mit automatischer Auswahl des entsprechenden gespeicherten Filters.

Zum Beispiel, wenn Sie **Hohes Risiko** auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente**, dieser Link wird zur Homepage von Vulnerability Manager Workspace mit automatischer Auswahl des Filters **Hohes Risiko** auf der Registerkarte Host-Schwachstellen weitergeleitet.

Auf der Homepage können Sie:

- Rufen Sie Detailinformationen zu den Daten ab, und zeigen Sie die Liste der Datensätze an, indem Sie auf die Visualisierungen klicken.
- Navigieren Sie zur Liste der aktiven Datensätze in der klassischen Anwenderoberfläche, indem Sie den Link **Klassische Liste anzeigen** auswählen.
- Öffnen Sie die Liste der aktiven Datensätze in Vulnerability Manager Workspace, indem Sie die Anzahl der aktiven Datensätze neben der Dropdown- **Liste Anzeigen** nach auswählen.
- Aktualisieren Sie die Visualisierungen, indem Sie das Symbol **Ausgewählten gespeicherten Filter aktualisieren** wählen.
- Zeigen Sie die neuesten Informationen an, indem Sie im Menü mit den drei Punkten eines Widgets die Option **Aktualisieren** auswählen.

Host-Schwachstellen

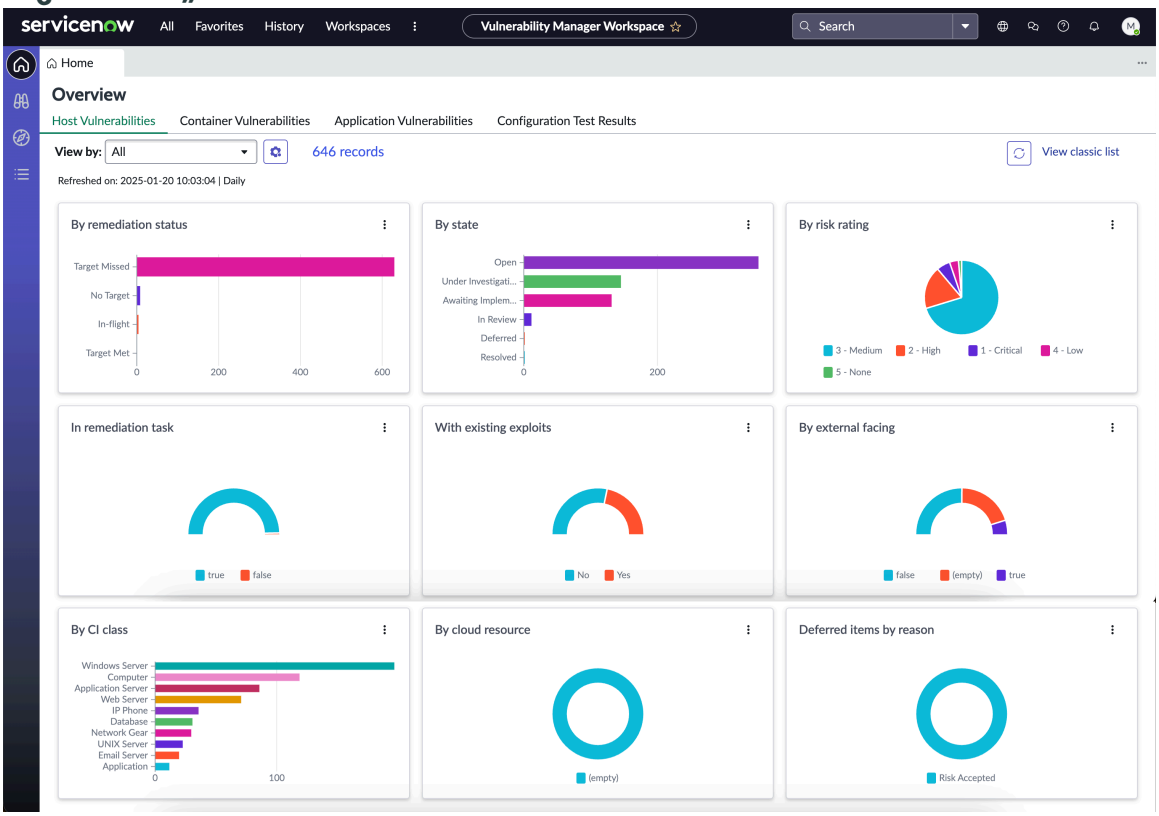
Die Registerkarte **„Host-Schwachstellen“** enthält Visualisierungen, die eine allgemeine Zusammenfassung der aktiven Host-Schwachstellen bieten.

Erforderliche Rollen:

- sn_vul.vulnerability_analyst und sn_vul.vulnerability_admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul.read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Host-Schwachstellen“.



In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage von beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.

Visualisierungen auf der Registerkarte „Host-Schwachstellen“ auf der Homepage von

Visualisierung	Typ	Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind und nach dem Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine)
In Korrekturaufgabe	Halbkreisring	Aktive Datensätze, die Teil der Korrekturaufgabe sind und nicht.
Mit vorhandenen Exploits	Halbkreisring	Aktive Datensätze mit und ohne bekannte Exploits.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen auf der Registerkarte „Host-Schwachstellen“ auf der Homepage von (Fortsetzung)

Visualisierung	Typ	Beschreibung
Nach außen gerichtet	Halbkreisring	Aktive Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet.
Nach CI-Klasse	Balkendiagramm	Aktive Datensätze nach CI-Klassen kategorisiert.
Nach Cloud-Ressource	Ringdiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze nach Grund gruppiert.

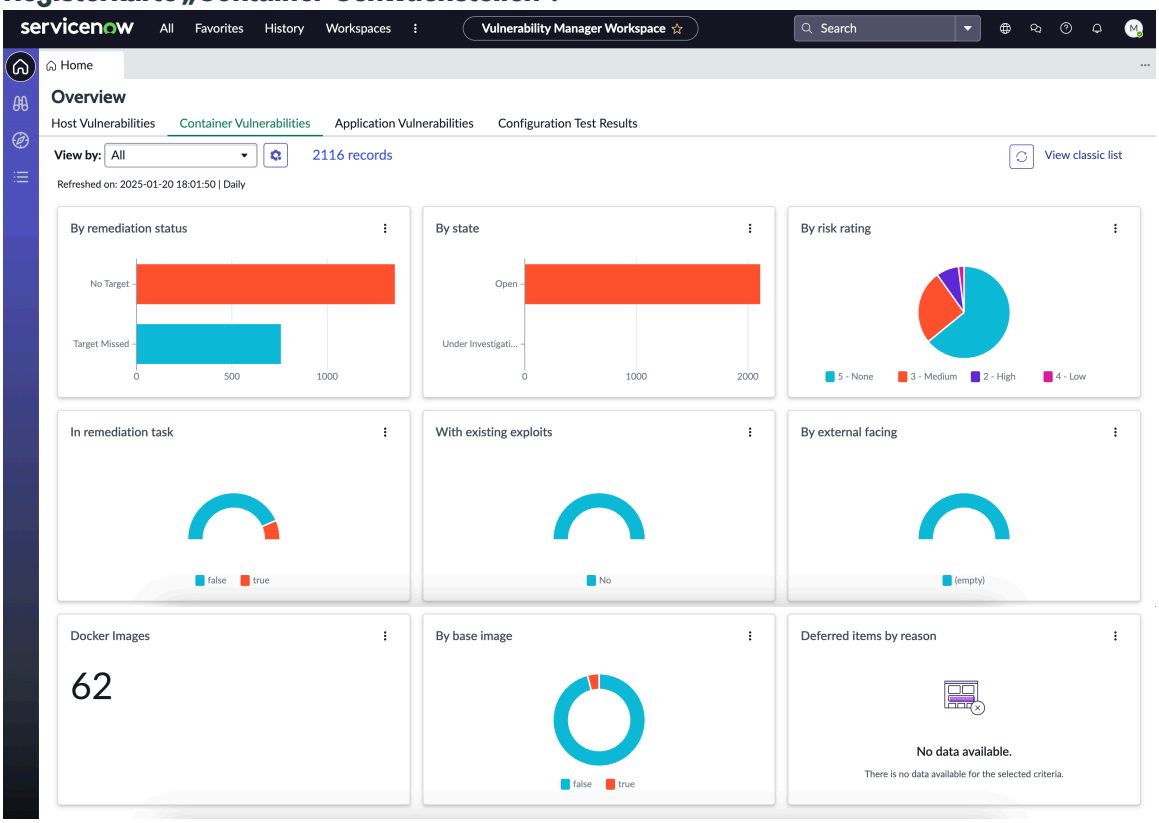
Container-Schwachstellen

Die Registerkarte **„Container-Schwachstellen“** enthält Visualisierungen, die eine Gesamtzusammenfassung der aktiven angreifbaren Container-Elemente bieten.

Erforderliche Rollen:

- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle „sn_vul_container.read_all“ zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

Registerkarte „Container-Schwachstellen“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage von beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.

Visualisierungen auf der Registerkarte „Container-Schwachstellen“ auf der Homepage von

Visualisierung	Typ	Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind und nach dem Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine)
In Korrekturaufgabe	Halbkreisring	Aktive Datensätze, die Teil der Korrekturaufgabe sind und nicht.
Mit vorhandenen Exploits	Halbkreisring	Aktive Datensätze mit und ohne bekannte Exploits.
Nach außen gerichtet	Halbkreisring	Aktive Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet.
Docker-Images	Anzahl	Anzahl der eindeutigen Docker-Images.
Nach Basis-Image	Ringdiagramm	Aktive Datensätze, kategorisiert nach dem Typ des Bildes.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze nach Grund gruppiert.

Anwendungsschwachstellen

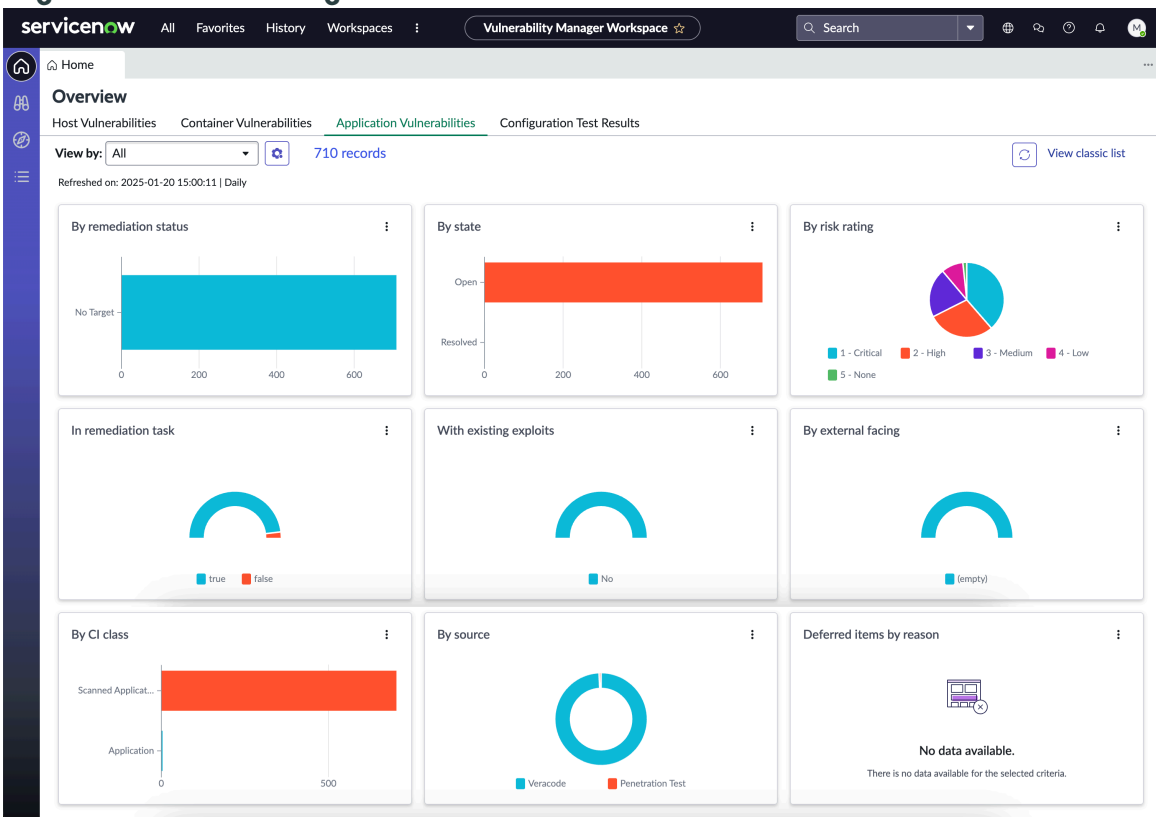
Die Registerkarte **„Anwendungsschwachstellen“** enthält Visualisierungen, die einen Gesamtzusammenfassung der Anwendungsschwachstellen bieten.

Erforderliche Rollen:

- sn_vul.app_sec_manager, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul.app_read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte Anwendungsschwachstellen



In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage von beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.

Visualisierungen auf der Registerkarte „Anwendungsschwachstellen“ auf der Homepage von

Visualisierung	Typ	Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind und nach dem Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine)
In Korrekturaufgabe	Halbkreisring	Aktive Datensätze, die Teil der Korrekturaufgabe sind und nicht.
Mit vorhandenen Exploits	Halbkreisring	Aktive Datensätze mit und ohne bekannte Exploits.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen auf der Registerkarte „Anwendungsschwachstellen“ auf der Homepage von (Fortsetzung)

Visualisierung	Typ	Beschreibung
Nach außen gerichtet	Halbkreisring	Aktive Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet.
Nach CI-Klasse	Balkendiagramm	Aktive Datensätze nach CI-Klassen kategorisiert.
Nach Cloud-Ressource	Ringdiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze nach Grund gruppiert.

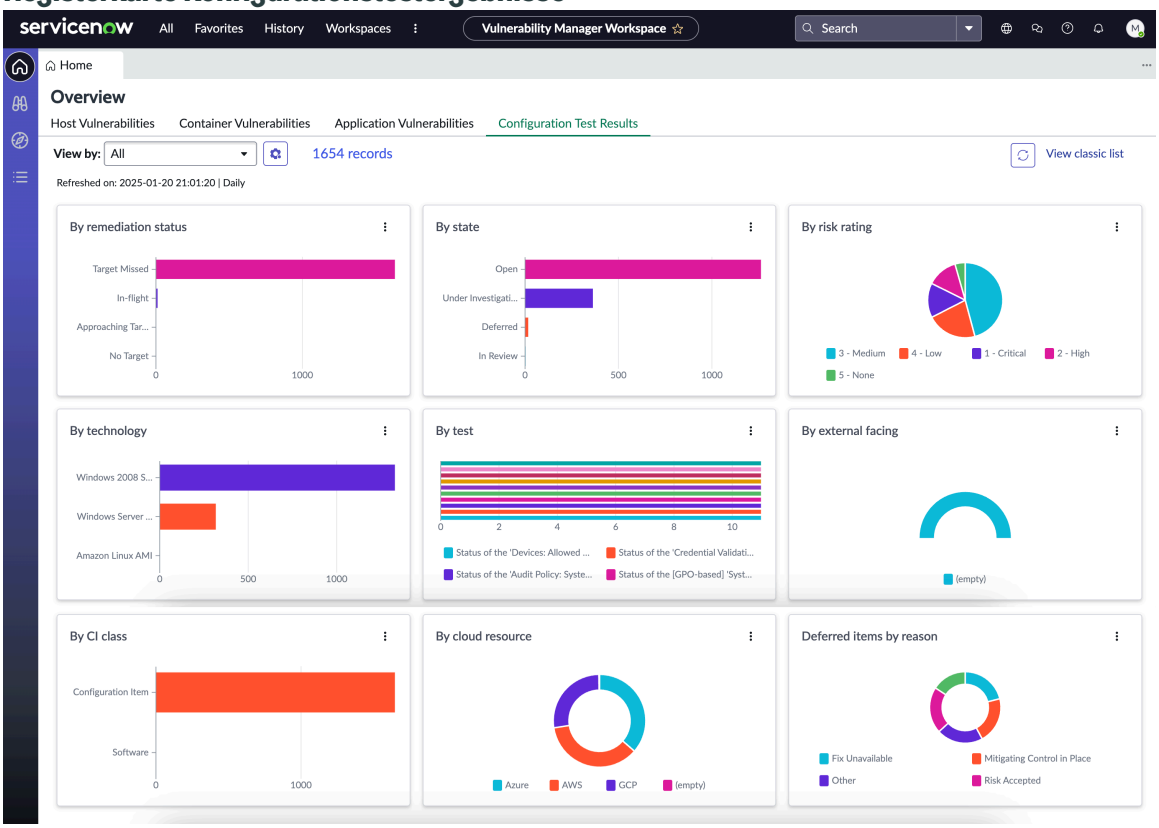
Konfigurationstestergebnisse

Die Registerkarte **Konfigurationstestergebnisse** enthält Visualisierungen, die eine Gesamtzusammenfassung der aktiven Fehlkonfigurationen der Assets in Ihrer Organisation bieten.

Erforderliche Rollen:

- sn_vulc.admin, um Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vulc.read zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

Registerkarte Konfigurationstestergebnisse



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte Konfigurationstestergebnisse auf der -Homepage beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.

Visualisierungen auf der Registerkarte Konfigurationstestergebnisse auf der Homepage

Visualisierung		Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind und nach dem Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine)
Durch Technologie	Balkendiagramm	Aktive Datensätze nach Technologie kategorisiert.
Durch Test	Balkendiagramm	Aktive Datensätze nach Tests kategorisiert.
Nach außen gerichtet	Halbkreisring	Aktive Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet.
Nach CI-Klasse	Balkendiagramm	Aktive Datensätze nach CI-Klassen kategorisiert.
Nach Cloud-Ressource	Ringdiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze nach Grund gruppiert.

Seite „Überwachungsthemen“ im Vulnerability Manager Workspace

Auf der Seite Überwachungsthemen in Vulnerability Manager Workspace können Sie ein Überwachungsthema erstellen und bearbeiten. Ein *Überwachungsthema* ist ein Satz von Datenvisualisierungen, mit dem Sie einen gefilterten Satz von Datensätzen (VITs, AVITs, CVITs und CTRs) im Zeitverlauf in einem Dashboard überwachen können, die für Ihre Organisation von besonderem Interesse oder Priorität sein könnten.

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Die in den Datenvisualisierungen zu den Überwachungsthemen angezeigten Daten werden beim Import dynamisch aktualisiert, wenn sich die Schwachstellendaten ändern. Verwenden Sie die -Dashboards, um Trends, Umfang und Typen von Schwachstellen und Konfigurationselementen für das ausgewählte Überwachungsthema zu überwachen. Mithilfe dieser Informationen können Sie feststellen, wie sich die Schwachstellen in den einzelnen Überwachungsthemen auf Ihre Umgebung auswirken. Die Seite „Überwachungsthemen“ besteht aus vier Modulen: Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen, Konfigurationstestergebnisse und Inaktiv. Weitere Informationen zu den Registerkarten für zugehörige Elemente und ihren Visualisierungen in einem Überwachungsthema finden Sie unter Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema.

Die folgenden Überwachungsthemen werden mit dem Basissystem im Modul „Host-Schwachstellen“ auf der Seite „Überwachungsthemen“ bereitgestellt:

- Schwachstellen bei nach außen gerichteten Assets
- Schwachstellen mit verfügbaren Exploits
- Schwachstellen auf Windows-Servern
- Schwachstellen auf LINUX-Servern
- Kritische überfällige Schwachstellen
- Kritische Schwachstellen nicht in Korrekturaufgaben

Hinweis:
Wenn eine Datenvisualisierung zeigt, dass für diese Kategorie keine Datensätze vorhanden sind, Sie jedoch eine Liste der Datensätze anzeigen können, wenn Sie auf das Diagrammsymbol klicken, überprüfen Sie die Spalte mit dem Namen des Überwachungsthemas in der angezeigten Liste. Stellen Sie sicher, dass der Wert für alle Datensätze, die in der Spalte des Überwachungsthemas aufgeführt sind, z. B. mit Internetverbindung, falseist. Dieser Wert in diesem Beispiel gibt an, dass für dieses Überwachungsthema keine Datensätze mit Internetverbindung vorhanden sind.

Um die Remediation zu starten oder wenn ein kritischer Bedarf an Datensätzen in einem Überwachungsthema besteht, können Sie eine *Korrekturmaßnahme* aus einem Überwachungsthema erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturmaßnahme in Vulnerability Manager Workspace.

Zugehörige Informationen

Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema

Überwachungsthemen in Vulnerability Manager Workspaceverwenden

Erstellen Sie ein Überwachungsthema in Vulnerability Manager Workspace

Bearbeiten oder löschen Sie ein Überwachungsthema in Vulnerability Manager Workspace

Deaktivieren oder aktivieren Sie ein Überwachungsthema

Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema

Auf der Seite „Überwachungsthemen“ von Vulnerability Manager Workspacekönnen Sie Überwachungsthemen erstellen, die in vier Module unterteilt sind: „Host-Schwachstellen“, „Contain-Schwachstellen“, „Anwendungs-Schwachstellen“ und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Konfigurationstestergebnisse“. Die Registerkarten für zugehörige Elemente in einem Überwachungsthema unterscheiden sich für jedes Modul.

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Der Navigationsbereich auf der Seite „Überwachungsthemen“ enthält die folgenden Module:

- Host-Schwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Host-Elemente enthalten.
- Container-Schwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Container-Elemente enthalten.
- Anwendungsschwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Anwendungselemente enthalten.
- Konfigurationstestergebnisse: Zeigt die Überwachungsthemen an, die die Konfigurationselemente enthalten.
- Inaktiv: Zeigt die inaktiven Überwachungsthemen aus allen vier Modulen an.

Die folgende Tabelle zeigt die Registerkarten für zugehörige Elemente, die für verschiedene Überwachungsthemamodule verfügbar sind:

Überwachungsthema und zugehörige Elemente

Überwachungsthema	Registerkarten für zugehörige Elemente
Host-Schwachstellen	Übersicht, Betroffene CIs, Eindeutige Schwachstellen und Angreifbare Elemente
Container-Schwachstellen	Übersicht, Betroffene CIs, Eindeutige Schwachstellen und Angreifbare Elemente
Anwendungsschwachstellen	Übersicht und angreifbare Elemente
Konfigurationstestergebnisse	Übersicht, betroffene CIs, verschiedene Konfigurationstests und Konfigurationstestergebnisse

Die folgende Tabelle enthält eine Beschreibung der Registerkarten für zugehörige Elemente und der Visualisierungen in einem Überwachungsthema.

Registerkarten und Visualisierung zugehöriger Elemente in einem Überwachungsthema

Registerkarte „Zugehörige Elemente“ und Visualisierung	Beschreibung
Übersicht	
Aktive angreifbare Elemente im Laufe der Zeit	Anzahl der aktiven angreifbaren Elemente (VIs) im Zeitverlauf. Sie können die Trends aus diesen Daten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarten und Visualisierung zugehöriger Elemente in einem Überwachungsthema (Fortsetzung)

Registerkarte „Zugehörige Elemente“ und Visualisierung	Beschreibung
	für die letzten 30 Tage überwachen. Sie können die Daten auch mithilfe der Filter Asset-Kategorie filtern.
VIs in Korrekturmaßnahmen	Anzahl der aktiven VIs aus der Gesamtzahl der VIs, für die sich bereits aktive Korrekturmaßnahmen befinden.
Aktive Korrekturmaßnahmen	Liste der aktiven Korrekturmaßnahmen.
Betroffene CIs	
Eindeutige CIs	Anzahl der Konfigurationselemente (CIs) (Assets), die von diesen Schwachstellen betroffen sind.
VIs pro CI-Klasse	Anzahl der angreifbaren Elemente (VIs) für jede Configuration Management Database (CMDB) CI-Klasse. **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul für Host-, Anwendungs- und Container-Schwachstellen angezeigt.
Konfigurationsprobleme pro CI-Klasse	Anzahl der CIs für jede Configuration Management Database (CMDB) CI-Klasse. **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul Konfigurationsprobleme angezeigt.
VIs mit Internetzugriff	Anzahl der aktiven VIs aus der Gesamtzahl der VIs für Ihre Assets, die im Internet verfügbar gemacht werden. **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul für Host-, Anwendungs- und Container-Schwachstellen angezeigt.
Konfigurationsprobleme mit Internetzugriff	Anzahl der aktiven CIs aus der Gesamtzahl der CIs für Ihre Assets, die im Internet verfügbar gemacht werden. **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul Konfigurationsprobleme angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarten und Visualisierung zugehöriger Elemente in einem Überwachungsthema (Fortsetzung)

Registerkarte „Zugehörige Elemente“ und Visualisierung	Beschreibung
Eindeutige Schwachstellen	
VIs mit vorhandenen Exploits	Aktive AEs mit bekannten Schwachstellen.
Eindeutige Schwachstellen	Anzahl der einzelnen, unterschiedlichen Schwachstellen, die Ihren Assets zugeordnet sind. Die unterschiedlichen Schwachstellen können basierend auf dem Problemtyp gefiltert werden.
VIs mit PCI-Schwachstellen	Anzahl einzelner, eindeutiger Assets, die aktive AEs mit Schwachstellen in der Zahlungskartenbranche aufweisen.
Angreifbare Elemente	
Angreifbare Host-Elemente	Liste aller angreifbaren Host-Elemente. Sie können diese Liste filtern, sodass nur die Datensätze angezeigt werden, die Sie sehen möchten. **Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Host-Schwachstellen“ angezeigt.
Angreifbare Anwendungselemente	Liste aller angreifbaren Anwendungselemente. Sie können diese Liste filtern, sodass nur die Datensätze angezeigt werden, die Sie sehen möchten. **Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Anwendungsschwachstellen“ angezeigt.
Angreifbare Container-Elemente	Liste aller angreifbaren Container-Elemente. Sie können diese Liste so filtern, dass nur die Datensätze angezeigt werden, die Sie sehen möchten. **Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Container-Schwachstellen“ angezeigt.
Registerkarte **„Übersicht“** in einem Überwachungsthema im Modul „Konfigurationstestergebnisse“	
Aktive Konfigurationstestergebnisse im Zeitverlauf	Anzahl der aktiven Konfigurationstestergebnisse im Zeitverlauf. Sie können die Trends aus diesen Daten für die letzten 30 Tage überwachen.
Konfigurationstestergebnisse bei Korrekturmaßnahmen	Anzahl der aktiven Konfigurationstestergebnisse aus der Gesamtzahl der Datensätze, für die sich bereits aktive Korrekturmaßnahmen befinden.
Aktive Korrekturmaßnahmen	Liste der aktiven Korrekturmaßnahmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarten und Visualisierung zugehöriger Elemente in einem Überwachungsthema (Fortsetzung)

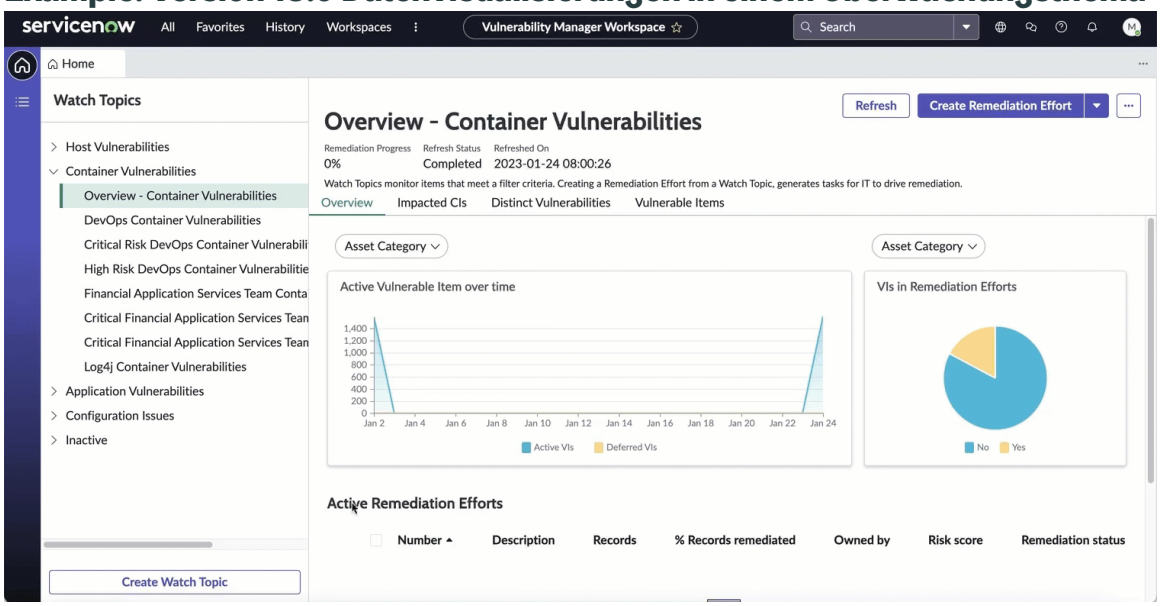
Registerkarte „Zugehörige Elemente“ und Visualisierung	Beschreibung
Registerkarte **„Unterschiedliche Konfigurationstests“** in einem Überwachungsthema im Modul „Konfigurationstestergebnisse“.	
Konfigurationstestergebnisse über Testrelevanz	Konfigurationstestergebnisse, die auf der Relevanz der Probleme basieren.
Unterschiedliche Konfigurationstests	Anzahl der unterschiedlichen Konfigurationstests.
Registerkarte **„Konfigurationstestergebnisse“** in einem Überwachungsthema im Modul „Konfigurationstestergebnisse“.	Liste der Konfigurationstestergebnisse.

Sie können die neuesten Details zu einem Überwachungsthema abrufen, indem Sie auf die Schaltfläche **„Aktualisieren“** klicken. Der aktuelle Aktualisierungsstatus und der Zeitstempel werden unter dem Namen des Überwachungsthemas angezeigt. Wenn Sie ein Überwachungsthema aktualisieren, werden alle Details des Überwachungsthemas, einschließlich der Diagramme und Korrekturmaßnahmen, aktualisiert. Ein Überwachungsthema wird automatisch aktualisiert, wenn es erstellt oder aktualisiert wird.

Hinweis:
Da Sie ein inaktives Überwachungsthema nicht aktualisieren können, ist die Schaltfläche **„Aktualisieren“** für ein inaktives Überwachungsthema inaktiv.

Klicken Sie in einem der Widgets auf eine Datenzeichnung, um zusätzliche Informationen zu den Datensätzen anzuzeigen.

Example: Version 18.0 Datenvisualisierungen in einem Überwachungsthema



Korrekturmaßnahmen im Vulnerability Manager Workspace

Eine Korrekturmaßnahme ist eine Reihe von Datensätzen, die einem Überwachungsthema zugeordnet sind. Die in einer Korrekturmaßnahme aufgeführten Datensätze sind statisch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie werden nicht durch neue Importdaten oder Änderungen aktualisiert, die Sie an Überwachungsthemen vornehmen.

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Wählen Sie unter der Liste **Korrekturmaßnahmen** auf der Seite Liste die **Option Aktiv** aus, und klicken Sie auf den Link einer Korrekturmaßnahme, um sie zu öffnen. Um die Korrekturmaßnahmen in angreifbare Hostelemente (VITs), angreifbare Anwendungselemente (AVITs), angreifbare Containerelemente (CVITs) und Konfigurationstestergebnisse (CTRs) zu kategorisieren, wählen Sie das Menü mit den drei Punkten in der **Spalte Datensatztyp** und dann **Gruppieren nach aus Datensatztyp**.

Über die zugehörigen Listenelemente im Datensatz für die Korrekturmaßnahme können Sie den Gesamtfortschritt und Status der Korrektur für die zugehörigen Datensätze anzeigen.

- Überwachen Sie auf der Registerkarte **Übersicht** die Datensätze, die dieser Korrekturmaßnahme zugeordnet sind und im Laufe der Zeit geschlossen wurden. Klicken Sie rechts neben dem Datensatz im Diagramm auf das Filtersymbol, um die auf die Datenvisualisierung angewendeten Filter anzuzeigen.
- Zeigen Sie auf der Registerkarte **Details** Details zur Korrekturmaßnahme einschließlich des zugehörigen Überwachungsthemas und Status (Aktiv oder Inaktiv) an. Sie können eine Korrekturmaßnahme auf dieser Seite deaktivieren. Wenn Sie die Korrekturmaßnahme deaktivieren, bevor alle Datensätze geschlossen wurden, werden alle aktiven Datensätze verfügbar und können neuen Korrekturmaßnahmen hinzugefügt werden.
- Zeigen Sie auf der Registerkarte **Korrekturaufgaben** die Korrekturaufgaben an, die dieser Korrekturmaßnahme zugeordnet sind. Zeigen Sie den Prozentsatz der korrigierten Datensätze an, die dieser Aufgabe zugeordnet sind.
- Zeigen Sie auf der Registerkarte **„Angreifbare Elemente“** die Datensätze an, die dieser Korrekturmaßnahme zugeordnet sind. Wenn alle Datensätze in einer Korrekturaufgabe abgeschlossen und geschlossen sind, wird die Korrekturmaßnahme in den Status „Inaktiv“ geändert. Wenn eine Korrekturmaßnahme inaktiv ist, können nicht alle geschlossenen Datensätze, die der Korrekturmaßnahme zugeordnet sind, neuen Korrekturmaßnahmen hinzugefügt werden.

  Hinweis:
  Die Registerkarte **„Angreifbare Elemente“** wird für die Korrekturmaßnahmen angezeigt, die mit Überwachungsthemen in den Modulen „Host-Schwachstellen“, „Anwendungsschwachstellen“ und „Container-Schwachstellen“ verknüpft sind.

- Zeigen Sie auf der Registerkarte **Konfigurationstestergebnisse** die Konfigurationstestergebnisse an, die der Korrekturmaßnahme zugeordnet sind. Wenn alle Datensätze in einer Korrekturaufgabe abgeschlossen und geschlossen sind, wird die Korrekturmaßnahme in den Status „Inaktiv“ geändert. Wenn eine Korrekturmaßnahme

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

inaktiv ist, können nicht alle geschlossenen Datensätze, die der Korrekturmaßnahme zugeordnet sind, neuen Korrekturmaßnahmen hinzugefügt werden.

Hinweis:
Die Registerkarte **Konfigurationstestergebnisse** wird für die Korrekturmaßnahmen angezeigt, die den Überwachungsthemen im Modul Konfigurationstestergebnisse zugeordnet sind.

Weitere Details und UI-Aktionen, die Sie aus einer Korrekturmaßnahme ausführen können, finden Sie unter Verwenden Sie Datensätze für Korrekturmaßnahmen.

Zugehörige Informationen

Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen

Erstellen Sie eine Korrekturmaßnahme in Vulnerability Manager Workspace

Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace

Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Vulnerability Manager Workspace

Übertragen Sie Datensätze an Korrekturmaßnahmen im Vulnerability Manager Workspace

Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen

Die Status von Datensätzen und die zugehörigen Korrekturaufgaben (RTs) werden beeinflusst, wenn Datensätze zurückgestellt, gelöst, erneut geöffnet und an andere Korrekturmaßnahmen (REs) übertragen werden.

Erforderliche Rollen:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Erstellen von Korrekturmaßnahmen

Wie sich die Status und Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen auswirken, hängt davon ab, wie eine Korrekturmaßnahme erstellt wird, wann sie erstellt wird und ob sie deaktiviert ist.

Aus der Liste oben rechts bei einem Überwachungsthema können Sie eine Korrekturmaßnahme erstellen, indem **Sie auf Korrekturmaßnahme erstellen** oder **Wiederkehrende Maßnahme erstellen**klicken. Sie können eine wiederkehrende Korrekturmaßnahme pro Überwachungsthema erstellen. Wenn Sie eine wiederkehrende Korrekturmaßnahme erstellen, werden nachfolgende Korrekturmaßnahmen für das zugehörige Überwachungsthema automatisch basierend auf den von Ihnen festgelegten Kriterien erstellt. In beiden Fällen:

- Um die Remediation zu erleichtern, werden den Remediationsbemühungen nur aktive Datensätze hinzugefügt.
- Alle Datensätze in neuen Korrekturmaßnahmen werden in neuen Korrekturaufgaben platziert. Datensätze können in mehreren Korrekturaufgaben vorhanden sein, aber nur ein Datensatz kann einer Korrekturmaßnahme zugeordnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Eine Korrekturmaßnahme wird automatisch deaktiviert, wenn keine aktiven Datensätze vorhanden sind.

Datensätze werden übertragen oder Datensatz übertragen

Sie können Datensätze von einer Korrekturmaßnahme zu einer anderen übertragen, wenn Sie eine Korrekturmaßnahme erstellen, indem Sie das Kontrollkästchen **Übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen** übertragen aktivieren. Weitere Informationen zum Übertragen der Datensätze finden Sie unter Übertragen Sie Datensätze an Korrekturmaßnahmen im Vulnerability Manager Workspace. Wenn Datensätze von einer Korrekturmaßnahme übertragen oder in wiederkehrende Korrekturmaßnahmen übertragen werden:

Zu einer neuen Korrekturmaßnahme im gleichen Überwachungsthema

- Alle Korrekturaufgaben aus der alten Korrekturmaßnahme werden in die neue Korrekturmaßnahme verschoben.
- Neue Korrekturaufgaben werden basierend auf den ausgewählten Gruppierungskriterien für die Datensätze erstellt, die zuvor nicht Teil einer Korrekturaufgabe waren.
- Die alte Korrekturmaßnahme ist deaktiviert.

Zu einer neuen Korrekturmaßnahme in einem anderen Überwachungsthema

Alle Datensätze aus der alten Korrekturmaßnahme werden in die neue Korrekturmaßnahme verschoben, und es werden Korrekturaufgaben basierend auf den ausgewählten Gruppierungskriterien erstellt.

- Wenn alle Datensätze in den Korrekturaufgaben, die der alten Korrekturmaßnahme zugeordnet sind, übertragen werden, werden diese Korrekturaufgaben geschlossen/abgebrochen.
- Wenn nur eine Teilmenge der Datensätze übertragen wird, werden die der alten Korrekturmaßnahme zugeordneten Korrekturaufgaben aufgeteilt und bleiben aktiv.

Die geschlossenen Korrekturaufgaben, die der alten Korrekturmaßnahme zugeordnet sind, sind nicht betroffen.

Hinweis:
Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Sie können jedoch Datensätze aus vorhandenen, nicht wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Weitere Informationen zum Übertragen von Datensätzen finden Sie unter Übertragen Sie Datensätze an Korrekturmaßnahmen im Vulnerability Manager Workspace.

Seite „Dashboards“ im Vulnerability Manager Workspace

Auf der Seite „Dashboards“ von Vulnerability Manager Workspacekönnen Sie in der Anwenderoberfläche Next Experience von die Dashboards anzeigen und mithilfe dieser Dashboards die Schwachstellen nachverfolgen und analysieren.

Erforderliche Rollen:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Greifen Sie auf die Dashboards in Vulnerability Manager Workspace zu, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und wählen Sie das **Dashboard** -Symbol. Das Standard-Dashboard wird basierend auf Ihrer Rolle angezeigt.

Die folgende Tabelle zeigt das Standarddashboard, das für eine bestimmte Rolle angezeigt wird.

Standard-Dashboard

Standard-Dashboard	Rolle
Einheitliches Dashboard	sn_vul_cmn_vulnerability_admin oder sn_vul_cmn_vulnerability_analyst
Schwachstellen-PA-Dashboard	sn_vul_vulnerability_admin oder sn_vul_vulnerability_analyst
Bewerbungsübersicht	sn_vul_app_sec_manager
Containerübersicht	sn_vul_container_vulnerability_admin oder sn_vul_container_analyst

Sie können die folgenden Dashboards für die Aufgaben anzeigen, die Sie ausführen möchten, indem Sie sie in der Dropdownliste auf der Seite „Dashboards“ auswählen.

Dashboards im Vulnerability Manager Workspace

Dashboard	Beschreibung
Schwachstellenmanagement (PA)	Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Host-Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Behebung. Weitere Informationen finden Sie unter Vulnerability Management (PA) -Dashboard.
Schwachstellengenehmigungen	Zeigen Sie die Anzahl der für Sie genehmigten, abgelehnten und ausstehenden Genehmigungsanforderungen an. Weitere Informationen finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..
CISO-Dashboard	Zeigt die allgemeine Sicherheitslage Ihrer Organisation an, einschließlich Sicherheitsschwachstelle und Incidents. Weitere Informationen finden Sie unter Vulnerability Management CISO- Dashboard.
Container-Schwachstellenmanagement – Übersicht	Verfolgen Sie Volumen, Leistung und Fortschritt der Container-Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Behebung. Weitere Informationen finden Sie unter Container Vulnerability Response-Dashboard.
Dashboard für Anwendungsschwachstellenmanagement	Verfolgen Sie Volumen, Leistung und Fortschritt der Anwendungsschwachstellen von der ersten Analyse

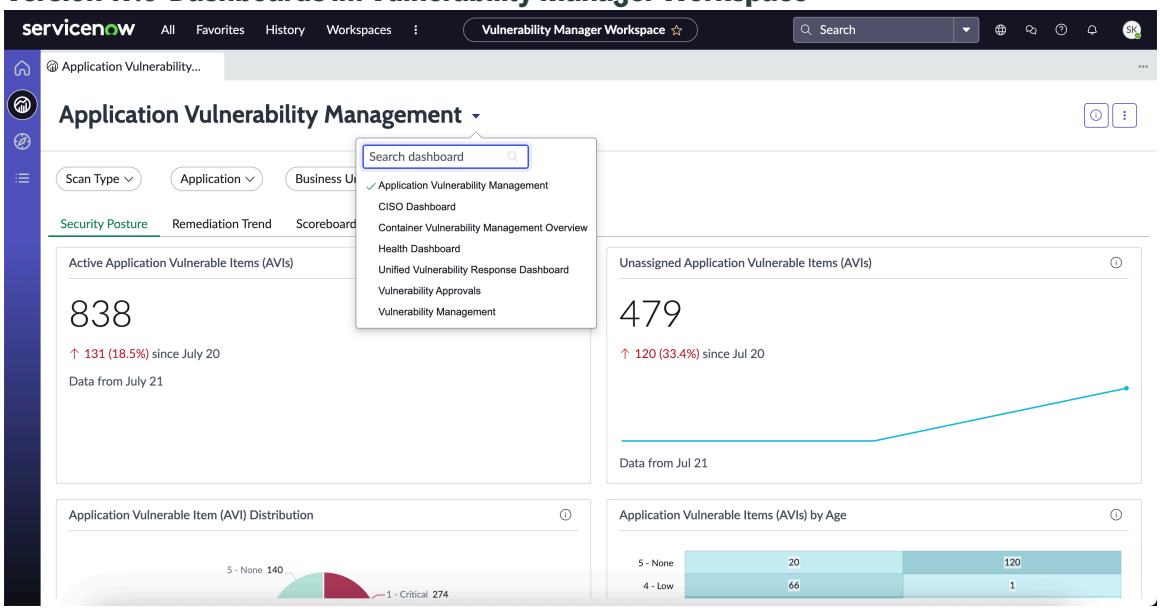
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboards im Vulnerability Manager Workspace (Fortsetzung)

Dashboard	Beschreibung
	und Erkennung bis zur Eindämmung oder Behebung. Weitere Informationen finden Sie unter Application Vulnerability Management (PA)-Dashboard
Einheitliches Vulnerability Response-Dashboard	Bietet Transparenz aus mehreren Schwachstellenscannern und Sicherheitstools, um einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation zu erhalten. Weitere Informationen finden Sie unter Analyse- und Berichterstellungslösungen für das Unified Vulnerability Response-Dashboard.
Vulnerability Response-Integritäts-Dashboard	Zeigt die Gesamtintegritätspunktzahl der Vulnerability Response-Anwendung an. Weitere Informationen finden Sie unter Integritäts-Dashboard von SecOps Vulnerability Response.

Die folgende Abbildung zeigt die Seite „Dashboards“ in Vulnerability Manager Workspace.

Version 19.0-Dashboards im Vulnerability Manager Workspace



Sie können auch ein anwenderdefiniertes Dashboard erstellen, indem Sie das Symbol „Weitere Optionen“ und dann **Neues Dashboard erstellen**wählen.

Listenseite im Vulnerability Manager Workspace

Auf der Seite „Liste“ in Vulnerability Manager Workspace können Schwachstellen- und Sicherheitsmanager sowie Analysten den Korrekturfortschritt für Datensätze einsehen, Detailinformationen zu Datensätzen anzeigen und den Status ihrer Genehmigungsanforderungen und Ausnahmen anzeigen.

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Diese Listen und Links bieten Ihnen einfachen Zugriff auf Datensätze und Aufgaben. Sie enthält zwei Registerkarten:

- **Registerkarte** Listen: Zeigt die Standardlisten für Korrekturbemühungen, Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse, Lösungen, Ausnahmen und Bibliotheken an.
- Registerkarte**Meine Listen** : Zeigt alle Listen an, die Sie auf der Registerkarte Listen umbenannt haben, sowie alle von Ihnen erstellten Listen.

  Sie können auch eine eigene Liste erstellen, um den Korrekturfortschritt zu überwachen. Weitere Informationen finden Sie unter Erstellen Sie eine anwenderdefinierte Liste von Datensätzen.

Registerkarte Listen

Die folgende Tabelle zeigt die Listen, die auf der Registerkarte Listen der Listenseite verfügbar sind:

Tipp:

Wenn die Systemeigenschaft *sn_vul_cmn_ws.navigate_to_workspace* von einem Administrator auf „true“ festgelegt wird und die vordefinierten Filterlinks in den Modulen Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response und Configuration Compliance im Menü **Alle** ausgewählt werden, werden diese Links auf der Listenseite von geöffnet Vulnerability Manager Workspace basierend auf Ihrer Rolle.

Zum Beispiel, wenn Sie **Zugewiesen an Meine Gruppen** auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**, dieser Link wird an Vulnerability Manager Workspaceumgeleitet. Die Liste **„Meinen Gruppen zugewiesen“** im Modul **„Korrekturaufgaben“** wird auf der Seite „Liste“ des Arbeitsbereichs des Schwachstellenmanagers geöffnet, wenn Sie die Rolle „Schwachstellenadministrator“ oder „Analyst“ innehaben. Um die Host-Korrekturaufgaben anzuzeigen, gruppieren Sie die Aufgaben nach Datensatztyp.

Mit der Systemeigenschaft *glide.ui.list.seismic.omit.count* können Sie die Datensatzanzahl in den Listen ausblenden. Weitere Informationen zum Deaktivieren/Aktivieren der Datensatzanzahl in einer Liste finden Sie im KB-Artikel KBB0010402 .

Listen

Listenelement	Beschreibung	Module	Erforderliche Rollen
Korrekturmaßnahmen (REs)	Liste der aktiven REs und aller REs, die Ihren Zuweisungsgruppen zugewiesen sind. Gruppieren Sie die Korrekturmaßnahmen nach **Datensatztyp**, um sie nach angreifbaren	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs) • sn_vul.app_sec_manager für angreifbare Elemente in der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Hostelementen, angreifbaren Anwendungselementen, angreifbaren Containerelementen und Konfigurationstestergebnissen zu kategorisieren.		Anwendung (AVITs) • sn_vul_container.vulnerability_analy oder sn_vul_container.vulnerability_admi für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)
Korrekturaufgaben	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven Korrekturaufgaben für Host, Anwendung, Container und Testergebnis. • Alle: Liste der aktiven und inaktiven Korrekturaufgaben für Host, Anwendung, Container und Testergebnis. • Mir zugewiesen: Liste der Korrekturaufgaben, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Korrekturaufgaben, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind. Gruppieren Sie die Korrekturaufgaben nach **Datensatztyp**, um sie nach angreifbaren Hostelementen,	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs) • sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.vulnerability_analy oder sn_vul_container.vulnerability_admi für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	angreifbaren Anwendungselementen, angreifbaren Containerelementen und Konfigurationstestergebnissen zu kategorisieren. **Hinweis:** Die Liste der Korrekturaufgaben enthält Aufgaben, die während der Erstellung der Korrekturmaßnahme in Vulnerability Manager Workspacegeneriert wurden, sowie Aufgaben, die manuell und durch Regeln für Korrekturaufgaben und andere Prozesse in der klassischen Anwenderoberfläche erstellt wurden. Die Spalte „Korrekturaufwand“ ist für alle Korrekturaufgaben leer, die nicht als Teil der Korrekturmaßnahme erstellt wurden.		
Angreifbare Host-Elemente	Enthält die folgenden Listen • Aktiv: Liste aller aktiven angreifbaren Host-Elemente. • Alle: Liste der aktiven und inaktiven angreifbaren Host-Elemente. • Mir zugewiesen: Liste der angreifbaren Host-	Vulnerability Response	sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Elemente, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der angreifbaren Host-Elemente, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind.		
Angreifbare Anwendungselemente	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven angreifbaren Anwendungselemente. • Alle: Liste der aktiven und inaktiven angreifbaren Anwendungselemente. • Mir zugewiesen: Liste der angreifbaren Anwendungselemente, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der angreifbaren Anwendungselemente, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind. Sie können ein neues angreifbares Anwendungselement erstellen, indem Sie auf die Schaltfläche **Neu** klicken.	Application Vulnerability Response	sn_vul.app_sec_manager
Angreifbare Container-Elemente	Enthält die folgenden Listen:	Container Vulnerability Response	sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	• Aktiv: Liste aller aktiven angreifbaren Container-Elemente. • Alle: Liste der aktiven und inaktiven angreifbaren Container-Elemente. • Mir zugewiesen: Liste der angreifbaren Container-Elemente, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der angreifbaren Container-Elemente, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind.		
Konfigurationstestergebnisse	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven Testergebnisse. • Alle: Liste aller aktiven und inaktiven Testergebnisse • Mir zugewiesen: Liste der Testergebnisse, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der Testergebnisse, die Ihren	Konfigurations-Compliance	sn_vulc.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Zuweisungsgruppen zur Korrektur zugewiesen sind.		
Lösungen	Enthält die folgenden Listen: • Alle: Zeigt alle verfügbaren Lösungen an, mit denen Sie die angreifbaren Host-Elemente korrigieren können. • Höchste Ersetzung: Zeigt alle Lösungen an, die für die ausgefüllten bevorzugten Lösungen verwendet werden. • Mit angreifbaren Elementen: Zeigt die Lösungen an, die als bevorzugte Lösung für angreifbare Elemente verwendet werden.	Vulnerability Response	sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin
Ausnahmen	Zeigt die Genehmigungsstatus für alle Ausnahme- und falsch positiven Anforderungen an, die Ihren Zuweisungsgruppen zugeordnet sind. • Alle: Liste der Genehmigungsanforderungen für Ausnahmen, falsch positive Ergebnisse und Aufhebung der Zuweisung in Bezug auf VITs, AVITs und CVITs und ihre	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs) • sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.vulnerability_analy oder sn_vul_container.vulnerability_admin für angreifbare

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Korrekturaufgaben (VUL, AVUL und CVUL). • Alle (Konfigurations-Compliance): Liste der Ausnahmen, falsch positiven Ergebnisse und der Aufhebung der Zuweisung von Genehmigungsanforderungen im Zusammenhang mit Testergebnissen und Korrekturaufgaben (CTR#). Gruppieren Sie die Ausnahmen nach **Datensatztyp**, um sie nach angreifbaren Hostelementen, angreifbaren Anwendungselementen, angreifbaren Containerelementen und Konfigurationstestergebnissen zu kategorisieren.		Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)
Genehmigungen	Mir zugewiesen: Zeigt die Genehmigungsanforderungen an, die Ihnen zur Verarbeitung zugewiesen sind. Informationen zum Verarbeiten Ihrer Genehmigungen im Arbeitsbereich finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs) • sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.vulnerability_analy oder sn_vul_container.vulnerability_admi für angreifbare

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
			Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)
Bibliotheken	Besteht aus den folgenden Listen: • CVEs (NVD): Liste aller Common Vulnerability and Exposures (CVE) aus Vulnerability Response, Application Vulnerability Responseund Container Vulnerability Response. • TPEs: Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs. • CWEs: Liste aller Common Weakness Enumerations (CWEs) aus Vulnerability Response, Application Vulnerability Responseund Container Vulnerability Response. • App-Schwachstellen: Liste aller Einträge für Anwendungsschwachstellen von Drittparteien. • Testgruppen: Liste aller Konfigurations-	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs) • sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.vulnerability_analy oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Compliance -Testgruppen. In der Datensatzansicht können Sie den Prozentsatz der CI-Compliance und der Testergebnis-Compliance für eine Testgruppe anzeigen. • Tests: Liste aller Tests von Konfigurations-Compliance Sie können den Prozentsatz der Compliance von Testergebnissen für einen Test in der Datensatzansicht anzeigen. • Ausgleichssteuerungen: Liste aller Ausgleichssteuerungen, die für Risikominderungsanforderungen verwendet werden können. Sie können eine Ausgleichssteuerung hinzufügen, indem Sie auf **Neu**klicken. Weitere Informationen zum Hinzufügen einer Ausgleichssteuerung finden Sie unter Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu.		
CMDB	Enthält die folgenden Listen • **Erkannte Elemente**: Liste aller erkannten Elemente.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	• **Erkannte Container-Images**: Liste der Container-Images. Diese Container-Images enthalten Informationen über die Image-ID, das Docker-Image und das Image-Repository zusammen mit den Ebeneninformationen.		• sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.vulnerability_analy oder sn_vul_container.vulnerability_admir für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)
Anforderungen für Penetrationstestbewertung	Enthält die folgenden Listen: • **Aktiv**: Liste der aktiven Anforderungen für Penetrationstestbewertung. • **Alle**: Liste aller aktiven und inaktiven Penetrationstest-Bewertungsanforderungen • **Mir zugewiesen**: Liste der von Ihnen ausgelösten Penetrationstest-Bewertungsanforderungen. • **Meiner Gruppe zugewiesen**: Liste der Penetrationstest-Bewertungsanforderungen, die von den Anwendern in Ihren Zuweisungsgruppen ausgelöst wurden. Informationen zum Erstellen einer Bewertungsanforderung für Penetrationstests finden Sie unter Neue Anforderung für	Application Vulnerability Response	sn_vul.app_sec_manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Penetrationstestbewertung erstellen.		
Penetrationstest-Ergebnisse	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven Penetrationstest-Ergebnisse. • Alle: Liste der aktiven und inaktiven Penetrationstest-Ergebnisse. • Mir zugewiesen: Liste der Penetrationstest-Ergebnisse, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der Penetrationstest-Ergebnisse, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind. Informationen zum Erstellen von Ergebnissen für Penetrationstests finden Sie unter Erstellen Sie Penetrationstestergebnisse basierend auf einem Bewertungsfragebogen.	Application Vulnerability Response	sn_vul.app_sec_manager
Patches	Alle: Liste aller verfügbaren Patches, die zur Korrektur angreifbarer Host-Elemente verwendet werden können.	Vulnerability Response	sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin
Unterstützungsdaten	Enthält die folgenden Listen:	Konfigurations-Compliance	sn_vulc.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	• **Autoritative Quellen**: Liste der autorisierten Quellen, die Zusammenfassungsinformationen bereitstellen, die für die Recherche der Quellveröffentlichungen nützlich sind. • **Technologien**: Liste der Technologien, die die Zusammenfassungsinformationen zu allen maßgeblichen Quellen und Quelleninhalten bereitstellen (in Qualys auch als Framework bezeichnet)		

Zugehörige Informationen

Verwenden Sie die Listenansicht in Vulnerability Manager Workspace

Massenbearbeitung in Vulnerability Manager Workspace

In Vulnerability Manager Workspacekönnen Sie mithilfe der Massenbearbeitungsfunktion mehrere angreifbare Elemente (VITs, AVITs oder CVITs) oder Konfigurationstestergebnisse (TRs) gleichzeitig aktualisieren und so den Verwaltungs- und Nachbesserungsprozess optimieren.

Mittels der Massenbearbeitung können Sie mehrere Schwachstellen auswählen und konsistente Änderungen anwenden, z. B. das Zuweisen von Korrekturbesitzern, das Aktualisieren des Status, das Hinzufügen von Arbeitsnotizen, das Anfordern von Ausnahmen und das Anfordern von falsch positiven Meldungen. Dies spart Zeit und Aufwand, da angreifbare Elemente nicht mehr einzeln bearbeitet werden müssen, was zu einem effizienten und konsistenten Management von Schwachstellen führt.

Die Massenbearbeitungsfunktion ist verfügbar für:

- Host angreifbare Elemente (VITs) ab v21.0 von Vulnerability Response.
- angreifbare Elemente in Anwendungen (AVITs) und angreifbare Elemente in Containern (CVITs) ab v22.0 von Vulnerability Response.
- Testergebnisse (TRs) ab v23.0 von Vulnerability Response.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Mit der Massenbearbeitungsfunktion in Vulnerability Manager Workspacekönnen Sie die folgenden Aufgaben ausführen:

- Datensätze einer Zuweisungsgruppe massenweise zuweisen
- Massenausnahme im Arbeitsbereich des Schwachstellenmanagers anfordern
- Entfernen Sie Zuweisungen für angreifbare Host-Elemente massenweise
- Massenbearbeitung für falsch positive Werte im Arbeitsbereich des Schwachstellenmanagers
- Massenschließung von Datensätzen im Vulnerability Manager Workspace

Ausgleichssteuerungen zur Risikoreduzierung verstehen

Ausgleichssteuerungen sind die Maßnahmen, die ergriffen werden, um das Risiko zu reduzieren, das durch Schwachstellen entsteht, die nicht sofort gepatcht werden können. Sie können verwendet werden, um die Wahrscheinlichkeit oder die Auswirkungen eines erfolgreichen Exploits zu minimieren.

Hinweis:
Die Ausgleichssteuerungen sind nur für Host-Schwachstellen verfügbar.

Das Anwenden von Ausgleichssteuerungen kann das Risiko einer Schwachstelle reduzieren.

Die folgende Tabelle zeigt die Anwendungsfälle für Ausgleichssteuerungen:

Anwendungsfälle für Ausgleichssteuerungen

Anwendungsfall	Ausgleichssteuerung
Eine Schwachstelle in einem Webserver, die es Angreifern ermöglicht, beliebigen Code auszuführen.	Implementieren Sie eine Web Application Firewall (WAF), um schädliche Anforderungen an den Webserver zu blockieren.
Eine Schwachstelle in einem Betriebssystem, die es Angreifern ermöglicht, Berechtigungen für den Stamm zu eskalieren.	Implementieren Sie eine Anwendungssteuerung, um die Ausführung von Anwendungen auf dem Hostsystem einzuschränken.
Eine Schwachstelle in einem Datenbankserver, die Angreifern den Zugriff auf vertrauliche Daten ermöglicht.	Implementieren Sie eine Netzwerksegmentierung, um den Datenbankserver von anderen Hosts und kritischen Systemen zu isolieren.

Weitere Informationen zu den Auswirkungen von Ausgleichssteuerungen auf die Risikopunktzahl eines angreifbaren Elements und einer Korrekturaufgabe finden Sie unter Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikominderungsanforderungen zu

Risikominderung für ein CVE oder TPE aktivieren oder deaktivieren

Analyse- und Berichterstellungslösungen für das Unified Vulnerability Response-Dashboard

Das Unified Vulnerability Response-Dashboard ist ein zentralisiertes, zusammengefasstes Dashboard, das Transparenz aus mehreren Schwachstellenscannern und Sicherheitstools bietet, um einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation zu erhalten.

Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet. Sie sind zum Anzeigen und Freigeben der Berichte erforderlich:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Zugehörige Informationen

Analytics- und Reporting-Lösungen

Einheitliches Vulnerability Response-Dashboard

Das Unified Vulnerability Response-Dashboard bietet einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation. Die Schwachstellen in Bezug auf Infrastruktur, Cloud, Anwendungen und Container können in einem zentralen Dashboard angezeigt werden, um für mehr Transparenz und Korrekturen zu sorgen.

Sehen Sie sich dieses vierminütige Video an, um mehr über das Unified Vulnerability Response-Dashboard zu erfahren.

https://player.vimeo.com/video/1046083623?h=74c3349c9c&badge=0&autopause=0&player_id=0&app_id=58479

Erforderliche Now Platform-Rollen

Die folgenden Rollen sind dieser Lösung zugeordnet. Sie sind zum Anzeigen, Bearbeiten und Freigeben der Berichte erforderlich:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin

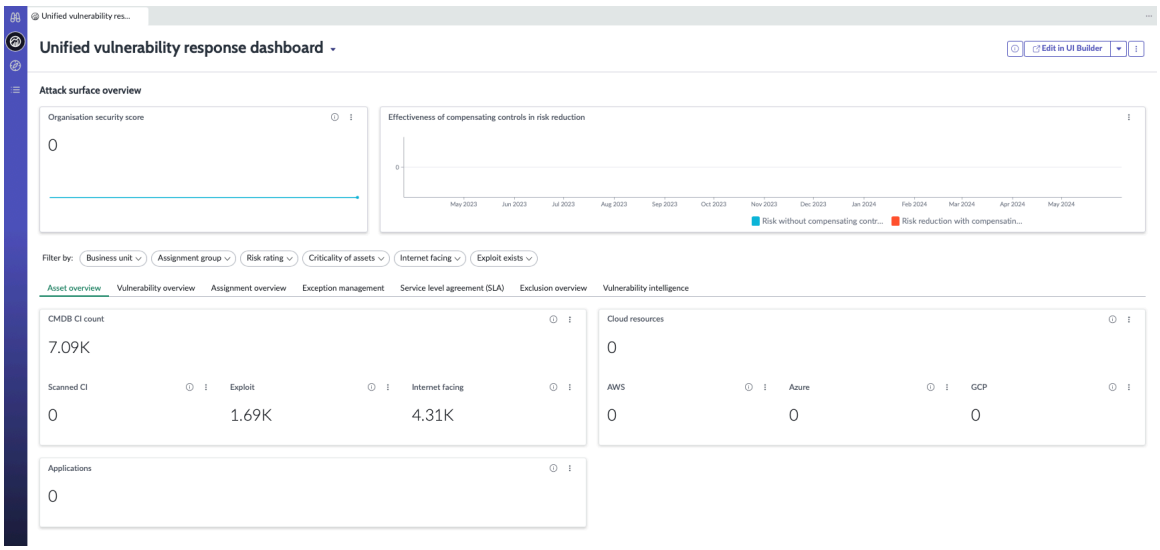
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Greifen Sie auf das Dashboard Unified Vulnerability Responsezu

Um das Dashboard zu öffnen, navigieren Sie zu einem der folgenden Optionen:

- **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** und wählen Sie das **Dashboardsymbol**. Je nach Rolle wird das Standard-Dashboard angezeigt. Um das Unified Vulnerability Response-Dashboard anzuzeigen, wählen Sie die Dropdownliste neben dem Namen des Dashboards.
- **Arbeitsbereiche** > **Platform Analytics-Arbeitsbereich** > **Dashboards** > **Einheitliches Vulnerability Response-Dashboard**.



Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
• Schwachstellenmanager • Schwachstellenanalysten	• Bietet Echtzeittransparenz der Risiken in Infrastruktur, Anwendungen, Konfigurationen und Containern. Ermöglicht Schwachstellenmanagern und Schwachstellenanalysten, Schwachstellen rechtzeitig zu priorisieren und zu beheben. • Stellt eine Angriffsoberflächenübersicht über kritische Assets bereit, die zur Nachverfolgung des Fortschritts und der Maßnahmen zur Nachbesserung verwendet werden können.

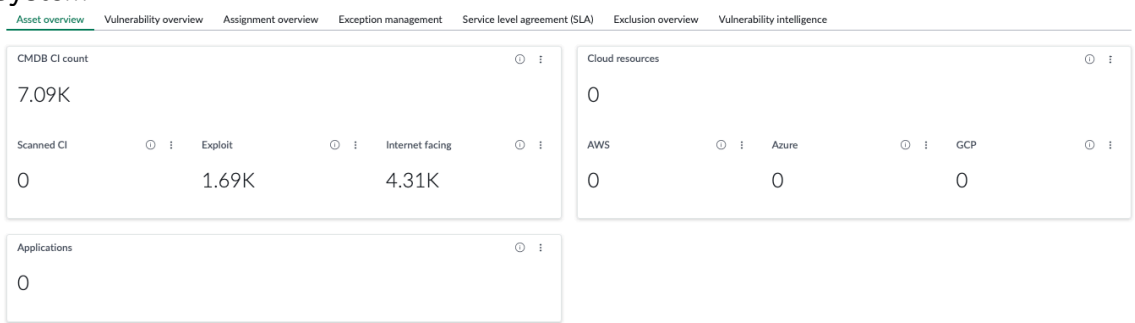
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
	• Bietet eine Übersicht über Risiken in allen Geschäftsbereichen (Business Units, BUs). Sie können Filter verwenden, um BUs auszuwählen und den Fortschritt zu vergleichen, um bei Bedarf Ressourcen neu zuzuweisen. Der Zugriff auf Rollenebene muss dem BU-Leiter gewährt werden. • Bietet Einblick in die potenziellen Auswirkungen nach BUs. Sie können den Filter Common Vulnerability and Exposure (CVE) verwenden, um Risiken im gesamten Unternehmen zu identifizieren. • Bietet Einblick in die EPSS-Punktzahlen, die von angreifbaren Einträgen im CISA-KEV-Katalog für angreifbare Anwendungs-, Host- und Container-Elemente erreicht werden.

Registerkarten im Dashboard von Unified Vulnerability Response

Mit diesem Dashboard können Sie die Schwachstellen oder Probleme anzeigen, die in Hosts, Clouds, Konfigurationen, Anwendungen und Containern vorhanden sind. Sie können die Schwachstellen basierend auf dem Geschäftsbereich, der Zuweisungsgruppe, der Risikobewertung, der Relevanz und danach, ob ein Exploit für die Schwachstellen vorhanden ist, anzeigen.

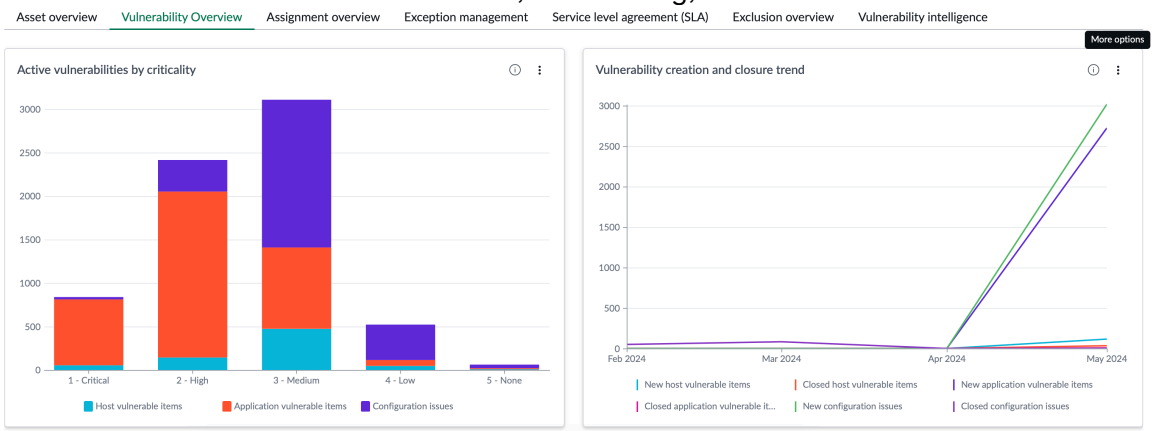
Die Registerkarte **„Asset-Übersicht“** zeigt den Gesamtstatus der Configuration Items (CIs) im System



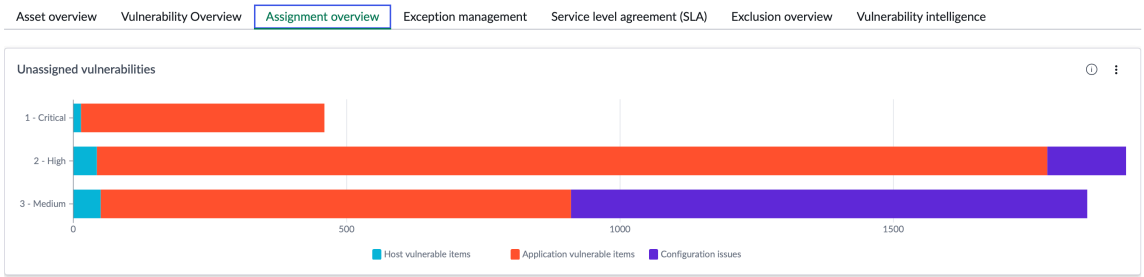
an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

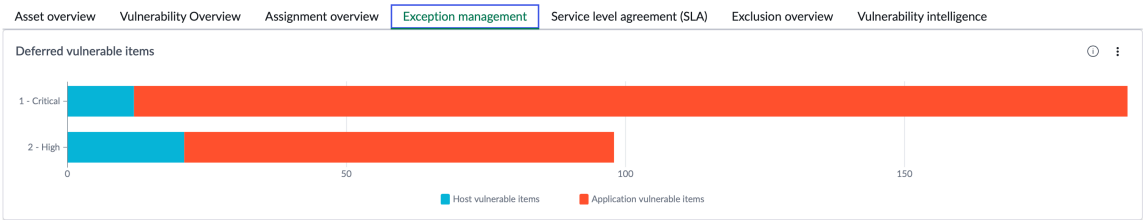
Die Registerkarte **„Schwachstellenübersicht“** enthält einen Status für die Arten von Schwachstellen wie Host, Anwendung, Container.



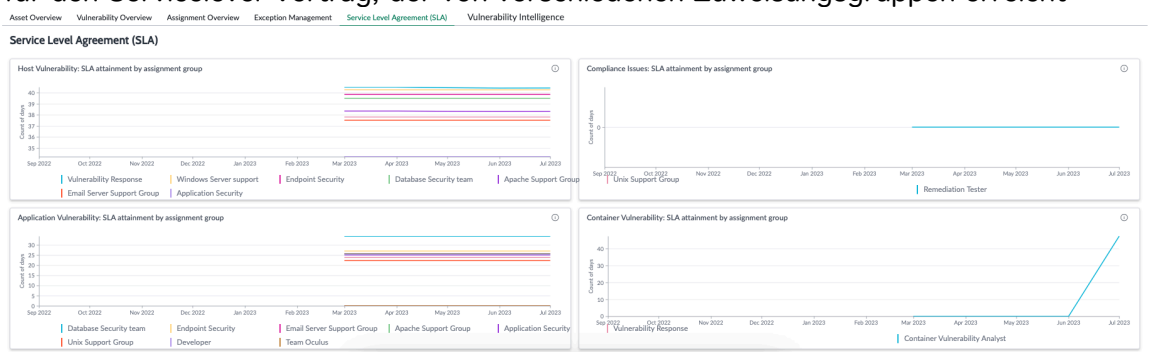
Die Registerkarte **„Zuweisungsübersicht“** zeigt einen Status für die Zuweisung der Schwachstellen an.



Die Registerkarte **„Ausnahmeverwaltung“** zeigt einen Status für die zurückgestellten Schwachstellen an.



Die Registerkarte **Servicelevel-Vereinbarung (Service Level Agreement, SLA)** bietet einen Status für den Servicelevel-Vertrag, der von verschiedenen Zuweisungsgruppen erreicht wurde.

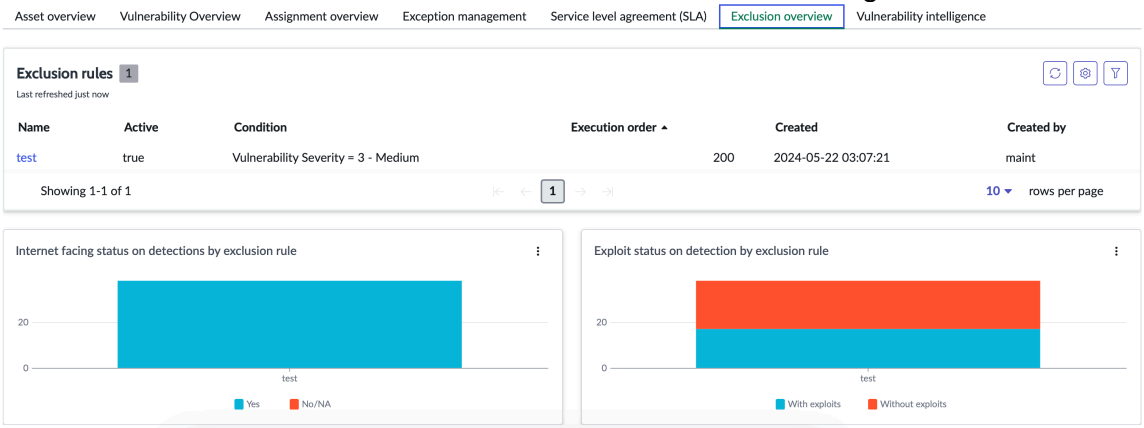


Die Registerkarte **Ausschlussübersicht** zeigt einen Status der von Ihnen erstellten Ausschlussregeln sowie der Regeln an, die sich auf Erkennungen auswirken, die

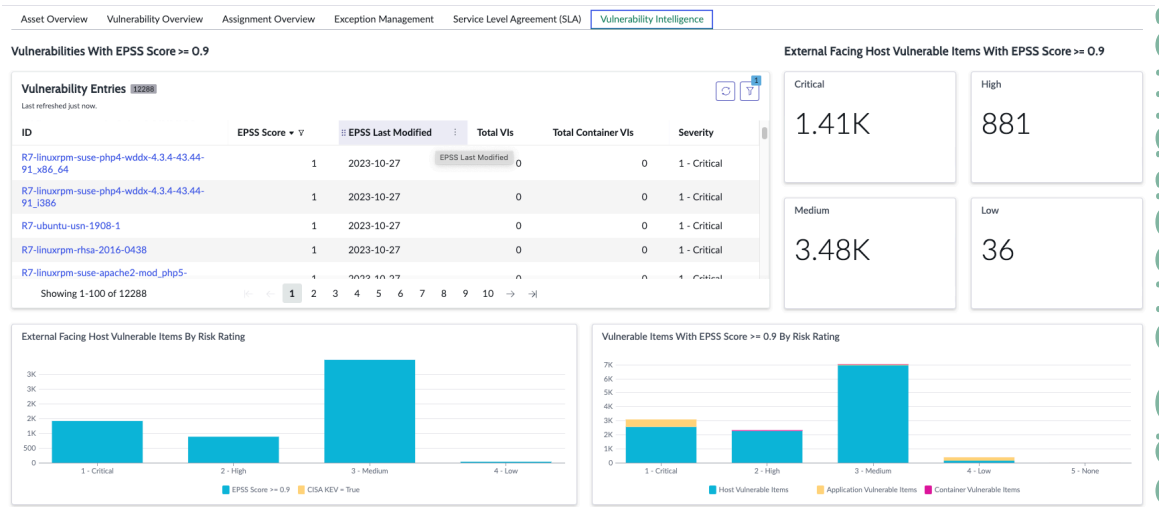
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit dem Internet verbunden sind und für die Schwachstellen verfügbar sind.



Die Registerkarte **„Vulnerability Intelligence“** bietet einen Status für die EPSS-Punktzahlen, die von Schwachstellen mit der CISA-KEV-Kennzeichnung „wahr“ und einer EPSS-Punktzahl >= 0,9 für angreifbare Elemente in den Bereichen Anwendung, Host und Container erreicht wurden.



Filter

Sie können die Widgets basierend auf den folgenden Kriterien filtern:

- Geschäftsbereich
- Zuweisungsgruppe
- Risikobewertung
- Relevanz von Assets
- Mit Internetzugriff
- Exploit vorhanden

Wenn ein Filter ausgewählt wird, werden die Daten in allen Widgets aktualisiert. Wenn ein Filter jedoch nicht auf ein Widget anwendbar ist, wird neben dem Filternamen ein Kreuzsymbol angezeigt.

Hinweis:
In Tokyosind nur Filter für Geschäftsbereiche und Zuweisungsgruppen verfügbar. Alle Filter sind ab Utah verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Indikatoren

Gescannte Assets

Formelindikator für in den letzten 60 Tagen gescannte Assets. Enthält gescannte erkannte Element-Assets, gescannte Anwendungs-Release-Assets und gescannte erkannte Container-Image-Assets als beitragende Indikatoren.

Assets – Exploit vorhanden

Formelindikator für Assets, für die ein Exploit in den Schwachstellen vorhanden ist. Enthält Host-Assets – Exploit vorhanden, Anwendungs-Assets – Exploit vorhanden, Container-Assets – Exploit vorhanden als beitragende Indikatoren.

Infra-Asset – mit Internetzugriff

Indikator zum Abrufen der Anzahl von Assets, die mit dem Internet verbunden sind.

Erkannte Elemente basierend auf Cloud-Ressourcentyp

Indikator zum Abrufen der Anzahl von Assets mit einer Asset-Kategorie wie Cloud.

Basis-Images

Indikator zum Abrufen der Anzahl der Basis-Images.

CISA-KEVs-Asset-Typ

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen für die Schwachstelle die Kennzeichnung CISA KEV (BOD 22-01) auf „wahr“ gesetzt ist. Enthält „CISA vorhanden – CVR“ und „CISA vorhanden – Angreifbare Elemente“ als beitragende Indikatoren.

CISA vorhanden – Angreifbare Elemente – Nicht zugewiesen

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen für die Schwachstelle die Kennzeichnung „CISA KEV (BOD 22-01)“ auf „wahr“ festgelegt ist und die Zuweisung der angreifbaren Elemente aufgehoben ist. Enthält nicht zugewiesene angreifbare Container-Elemente und nicht zugewiesene angreifbare Host-Elemente als beitragende Indikatoren.

CISA vorhanden – Angreifbare Elemente – Ziel verfehlt

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen für die Schwachstelle die Kennzeichnung „CISA KEV (BOD 22-01)“ auf „wahr“ festgelegt ist und die angreifbaren Elemente das Ziel verfehlt haben. Enthält „CISA vorhanden – Vul Items“, „CISA vorhanden – CVR“ als beitragende Indikatoren.

Aktive Host-VITs

Anzahl der aktiven angreifbaren Elemente des Hosts (VITs).

Aktive Anwendungs-VITs

Anzahl der aktiven angreifbaren Elemente in einer Anwendung (Application Vulnerable Items, AVITs).

Aktive Container-VITs

Anzahl der aktiven angreifbaren Container-Elemente (CVITs).

Neue VITs

Anzahl der VITs, die an einem Tag geöffnet wurden.

Neue AVITs

Anzahl der AVITs, die an einem Tag geöffnet wurden.

Neue CVITs

Anzahl der CVITs, die an einem Tag geöffnet wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Testergebnisse

Anzahl der Testergebnisse (Testergebnisse, TRs), die an einem Tag erstellt wurden.

Geschlossene AVITs

Anzahl der an einem Tag geschlossenen VITs.

Geschlossene VITs

Anzahl der an einem Tag geschlossenen AVITs.

Geschlossene CVITs

Anzahl der an einem Tag geschlossenen CVITs.

Geschlossene Testergebnisse

Anzahl der an einem Tag geschlossenen TRs.

Offene Konfigurationsprobleme – Testergebnisse

Anzahl aller offenen Testergebnisse, die sich im Status „Fehlgeschlagen“ befinden.

Risikopunktzahl der Organisation

Risikopunktzahl einer Organisation aus der Tabelle „Rollup-Anwendungsrisikopunktzahl“.

Nicht zugewiesene angreifbare Anwendungselemente

AVITs ohne Zuweisungsgruppe oder zugewiesen an.

Nicht zugewiesene angreifbare Host-Elemente

VITs ohne Zuweisungsgruppe oder zugewiesen zu.

Nicht zugewiesene angreifbare Container-Elemente

CVITs ohne Zuweisungsgruppe oder zugewiesen an.

Nicht zugewiesene Konfigurationsprobleme

TRs ohne Zuweisungsgruppe oder zugewiesen an.

Zurückgestellte VITs

VITs im Status „Zurückgestellt“.

Zurückgestellte AVITs

AVITs im Status „Zurückgestellt“.

Zurückgestellte CVITs

CVITs im Status „Zurückgestellt“.

Host-SLA – Geschlossen

Durchschnittliches Alter der geschlossenen von geschlossenen VITs.

Anwendungs-SLA – Geschlossen

Durchschnittsalter geschlossener von geschlossenen AVITs.

Container-SLA – Geschlossen

Durchschnittsalter geschlossener von geschlossenen CVITs.

Testergebnis-SLA – Bestanden

Durchschnittliches Alter der geschlossenen von bestandenen TRs.

Host-SLA – Geschlossen (Kritisch und Hoch)

Durchschnittliches Alter der geschlossenen kritischen und hohen VITs.

Anwendungs-SLA – Geschlossen (Kritisch und Hoch)

Durchschnittliches Alter der Schließung von kritischen und hohen AVITs.

Container-SLA – Geschlossen (Kritisch und Hoch)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durchschnittliches Alter der geschlossenen CVITs mit Status „Kritisch“ und „Hoch“.

Testergebnis-SLA – Bestanden (Kritisch und Hoch)

Durchschnittliches geschlossenes Alter von bestandenen kritischen und hohen TRs.

Aggregierte MTTR

Durchschnittliches Alter der geschlossenen VITs, AVITs, CVITs und TRs.

SLA verfehlt

Durchschnittliches Alter der geschlossenen und verfehlten VITs, AVITs, CVITs und TRs.

Schwachstellen mit EPSS-Punktzahlen >= 0,9

Anzahl der Schwachstelleneinträge mit EPSS-Punktzahlen größer oder gleich 0,9.

Aufgliederungen

- VIT-Typ (einheitlich)
- Mit Internetzugriff (einheitlich)
- Risikobewertung (einheitlich)
- Exploit vorhanden (einheitlich)
- Cloud-Ressourcentyp des erkannten Elements (einheitlich)
- CISA vorhanden (einheitlich)
- CMDB-Klasse (einheitlich)
- Geschäftsbereich (einheitlich)
- Business-Relevanz (einheitlich)
- Grund für Zurückstellung (einheitlich)
- Zuweisungsgruppe (einheitlich)
- Korrekturstatus (einheitlich)

Datenvisualisierungen

Registerkarte „Asset-Übersicht“.

Titel	Typ	Beschreibung
Angriffsoberfläche – Übersicht	Einzelwert	Zahl, die die aggregierte Punktzahl für die Sicherheit einer Organisation darstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

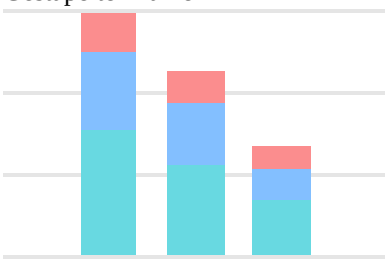
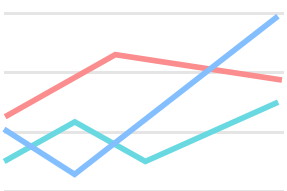
Registerkarte „Asset-Übersicht". (Fortsetzung)

Titel	Typ	Beschreibung
CMDB-CI-Anzahl	Einzelwert	Anzahl der CIs in der Organisation, die in Configuration Management Database (CMDB)registriert sind und nachverfolgt werden. Stellt eine Aufgliederung der folgenden CIs bereit: • Gescannte CIs: Anzahl der gescannten CIs • Exploit: Anzahl der verfügbaren Exploits • Mit Internetzugriff: Anzahl der CIs mit Internetzugriff
Cloud-Ressource	Einzelwert	Anzahl der CIs mit Asset-Kategorie wie Cloud. Stellt eine Aufgliederung der folgenden Cloud-Assets bereit: • AWS • Azure • GCP
Docker-Bild	Einzelwert	Anzahl der Docker-Images einschließlich Anzahl der Basis-Images.
Anwendungen	Einzelwert	Anzahl der Anwendungen in der Organisation.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

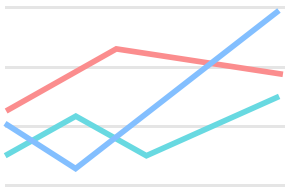
Registerkarte „Schwachstellenübersicht“.

Titel	Typ	Beschreibung
CISA-KEVs	Kreisdiagramm	Anzahl der Schwachstellen, die mit dem Katalog CISA und der CISA-Kennzeichnung als „wahr“ gekennzeichnet sind. Stellt eine Aufgliederung basierend auf den folgenden Elementen bereit: • CISA-Schwachstelle: Arten von Schwachstellen mit CISA-Kennzeichnung als „wahr“. • Host-CIs – mit Internetzugriff: CIs mit Internetzugriff • Nicht zugewiesene VITs: Nicht zugewiesene VITs mit CISA-Kennzeichnung als „wahr“. • VITs mit verfehltem Ziel: VITs, die das Ziel verfehlt haben, mit „wahr“ für CISA
Aktive Schwachstellen nach Relevanz	Gestapelter Balken 	Anzahl der aktiven VITs, AVITs und CVITs basierend auf der Kritikalität.
Trend bei der Erstellung und Schließung von Schwachstellen	Mehrzeilig 	Anzahl der neuen und geschlossenen Schwachstellen für alle Anwendungen. Stellt einen Trend für die letzten drei Monate bereit.

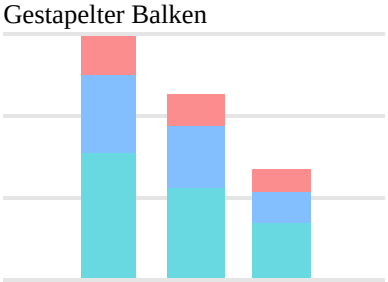
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Schwachstellenübersicht“. (Fortsetzung)

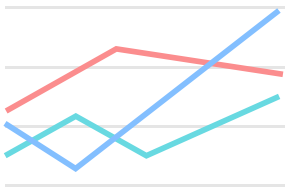
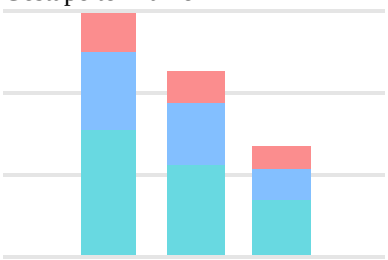
Titel	Typ	Beschreibung
Falsche Konfiguration nach Cloud-Plattform	Mehrzeilig 	Anzahl der Konfigurationsprobleme basierend auf Risikobewertung für jedes Cloud-Asset.
Cloud-Compliance	Tabelle	Liste der Ressourcen mit der Asset-Kategorie „Cloud“ mit den folgenden Details: • Ressourcenname • Klasse • Schwachstellenprobleme: Anzahl der in der Ressource vorhandenen Probleme, die basierend auf der Risikobewertung aggregiert werden. • Konfigurationsprobleme: Anzahl der Ressourcen mit Konfigurationsproblemen zusammen mit Risikobewertung. • Cloud-Account: Cloud-Account-ID. • Cloud-Region: Speicherort der Cloud-Ressourcen. • Cloud-Anbieter: Name des Cloud-Anbieters.

Registerkarte „Zuweisungsübersicht“.

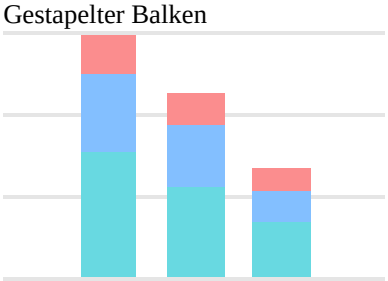
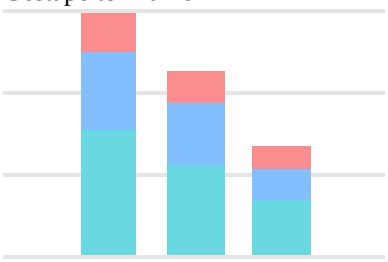
Titel	Typ	Beschreibung
Nicht zugewiesene VITs	Gestapelter Balken 	Anzahl der Schwachstellen, die keiner Gruppe oder Person zugewiesen sind, zusammen mit der Risikobewertung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Zuweisungsübersicht“. (Fortsetzung)

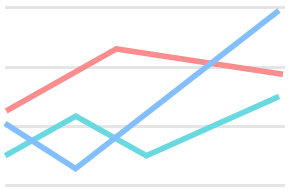
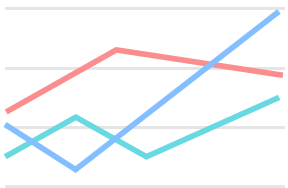
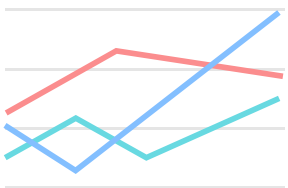
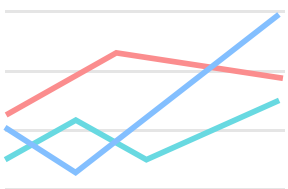
Titel	Typ	Beschreibung
MTTR nach Zuweisungsgruppe – Top 10	Mehrzeilig 	Durchschnittliche Zeit, die eine Zuweisungsgruppe benötigt, um die Sicherheitsschwachstellen oder -probleme zu identifizieren und zu beheben. Es werden die 10 Zuweisungsgruppen mit der längsten durchschnittlichen Zeit für Korrekturen angezeigt.
Top-10-Zuweisungsgruppen ohne SLA (als „kritisch“ und „hoch“ eingestufte Schwachstelle)	Gestapelter Balken 	Top 10 Zuweisungsgruppen, bei denen das Zieldatum für die Korrektur von Schwachstellen mit Status „kritisch“ und „hoch“ verfehlt wurde.

Registerkarte „Ausnahmeverwaltung“.

Titel	Typ	Beschreibung
Zurückgestellte VITs	Gestapelter Balken 	Anzahl der Schwachstellen im Status „Zurückgestellt“ basierend auf Risikobewertung.
Als „kritisch“ und „hoch“ eingestufte zurückgestellte VITs nach Zuweisungsgruppe	Gestapelter Balken 	Anzahl der Schwachstellen mit Risikobewertungen „Kritisch“ und „Hoch“ im Status „Zurückgestellt“, kategorisiert auf Grundlage der Zuweisungsgruppen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte Servicelevel-Vereinbarung (Service Level Agreement, SLA).

Titel	Typ	Beschreibung
Host-Schwachstelle: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe zum Korrigieren von Host-Schwachstellen benötigt. Stellt einen Trend für die letzten 10 Monate bereit.
Compliance-Probleme: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe zur Behebung von Compliance-Problemen benötigt. Stellt einen Trend für die letzten 10 Monate bereit.
Anwendungsschwachstelle: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe zum Beheben von Anwendungsschwachstellen benötigt. Stellt einen Trend für die letzten 10 Monate bereit.
Container-Schwachstelle: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe zum Beheben von Container-Schwachstellen benötigt. Stellt einen Trend für die letzten 10 Monate bereit.

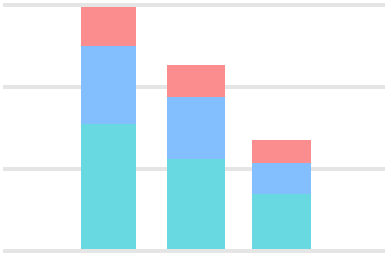
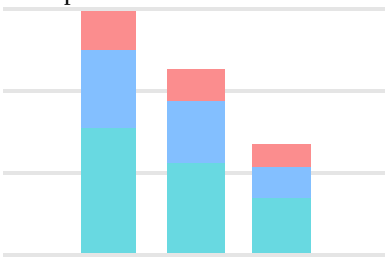
Registerkarte „Ausschlussübersicht“.

Titel	Typ	Beschreibung
Ausschlussregeln	Tabelle	Liste aller von Ihnen erstellten Ausschlussregeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Ausschlussübersicht“. (Fortsetzung)

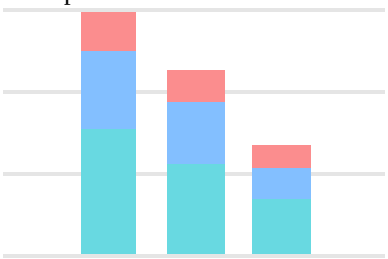
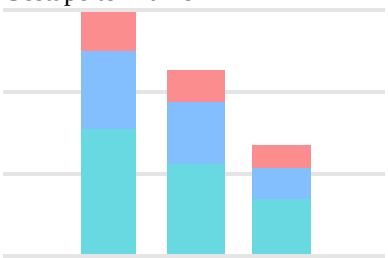
Titel	Typ	Beschreibung
Ausschlussregeln vs. mit Internetzugriff	Gestapelter Balken 	Ausschlussregeln, die sich auf Erkennungen auswirken, die zu Assets mit Internetzugriff gehören.
Ausschlussregeln vs. Exploits vorhanden	Gestapelter Balken 	Ausschlussregeln, die sich auf Erkennungen auswirken, die für vorhandene Exploits angreifbar sind.

Registerkarte „Vulnerability Intelligence“.

Titel	Typ	Beschreibung
Schwachstellen mit EPSS-Punktzahl >= 0,9	Tabelle	Vollständige Listenansicht aller angreifbaren Einträge (CVE oder TPE), die eine EPSS-Punktzahl größer oder gleich 0,9 aufweisen, zusammen mit den folgenden Details. • ID: CVE-ID der Schwachstelle • EPSS-Punktzahl • EPSS – Zuletzt geändert • CISA KEV BOD 22-01: Gibt an, ob der Eintrag im CISA KEV BOD vorhanden ist (verbindliche operative Direktive 22-01) • VIs gesamt: Gesamtanzahl der VIs, die für diesen Schwachstelleneintrag vorhanden sind. • Container-VIs gesamt: Gesamtanzahl der Container-VIs, die für diesen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Vulnerability Intelligence“. (Fortsetzung)

Titel	Typ	Beschreibung
		Schwachstelleneintrag vorhanden sind. • Schweregrad
Nach außen gerichtete angreifbare Host-Elemente mit einer EPSS-Punktzahl >= 0,9	Einzelwert	Zahl, die die Gesamtanzahl der nach außen gerichteten angreifbaren Host-Elemente mit einer EPSS-Punktzahl größer oder gleich 0,9 angibt. Stellt einzelne Punktzahlen sortiert nach Schweregrad der Risikoeinstufung bereit.
Nach außen gerichtete angreifbare Host-Elemente nach Risikobewertung	Gestapelter Balken 	Anzahl der nach außen gerichteten angreifbaren Host-Elemente nach Risikobewertung. Die Stapelbalken werden nach EPSS-Punktzahl >= 0,9 und CISA KEV = Wahr kategorisiert.
Angreifbare Elemente mit EPSS-Punktzahl >= 0,9 nach Risikobewertung	Gestapelter Balken 	Anzahl der Schwachstellen mit einer EPSS-Punktzahl größer oder gleich 0,9, sortiert nach Risikobewertung. Stellt eine Aufgliederung nach angreifbaren Host-Elementen, angreifbaren Anwendungselementen und angreifbaren Container-Elementen bereit.

Geplante Aufgaben für die Datensammlung

Datensammlungsaufträge sammeln automatisch Punkte für automatisierte Indikatoren und Aufgliederungen. Die folgenden geplanten Aufgaben werden ausgeführt, um automatisch Punktzahlen für neue Daten zu sammeln.

Warnung:
Standardmäßig sind die folgenden Datensammlungsaufgaben im Basissystem deaktiviert:

- Tägliche Datensammlung des einheitlichen Dashboards
- Wöchentliche Datensammlung des einheitlichen Dashboards
- Sammlung historischer Daten im einheitlichen Dashboard

Lesen Sie vor dem Aktivieren der Aufträge die KB .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Häufigkeit	Beschreibung
Sammlung historischer Daten im einheitlichen Dashboard	Einmal	Sammelt Punktzahlen und Snapshots für vorhandene Datensätze.
Wöchentliche Datensammlung des einheitlichen Dashboards	Wöchentlich	Erfasst wöchentlich Daten.
Tägliche Datensammlung des einheitlichen Dashboards	Täglich	Erfasst täglich Daten.
Rollup von Risikopunktzahlen zu Organisation	Täglich	Erfasst die zusammengefasste Risikopunktzahl für eine Organisation
Tägliche Cloud-Compliance-Anzahlen ausfüllen	Täglich	Sammelt Daten für Cloud-Compliance
EPSS – Täglicher Auftrag	Täglich	Erfasst EPSS-Daten von First.org

In Vulnerability Common Scope wird eine neue Tabelle mit der Rollup-Anwendungsrisikopunktzahl [sn_vul_cmn_rollup_app_risk_score] erstellt. Diese Tabelle wird mit den folgenden Rollup-Rechnern täglich über die geplanten Aufgaben gefüllt.

Name des Rollup-Rechners	Beschreibung
Rollup für Risikopunktzahl der Organisation	Fasst die Risikopunktzahlen für alle angreifbaren Elemente und Konfigurationsprobleme in einer Organisation zusammen. Bietet eine Gesamtrisikopunktzahl für eine Organisation.
Rollup für angreifbare Elemente	Fasst die Risikopunktzahlen für alle angreifbaren Elemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.
Rollup für angreifbare Anwendungselemente	Fasst die Risikopunktzahlen für alle angreifbaren Anwendungselemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.
Rollup für angreifbare Container-Elemente	Fasst die Risikopunktzahlen für alle angreifbaren Container-Elemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.
Testergebnis-Rollup	Fasst die Risikopunktzahlen für alle Testergebnisse in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.
Rollup von EPSS-Punktzahlen von NVDs zu TPEs	Rollup von EPSS-Punktzahlen von NVDs zu TPEs, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen und Verwalten von angreifbaren Elementen und Testergebnissen in Vulnerability Manager Workspace

Mit Vulnerability Manager Workspace können Sie angreifbare Elemente (VITs, AVITs und CVITs) und Testergebnisse (TRs) mithilfe von Überwachungsthemen überwachen und ihren Korrekturfortschritt durch Erstellen von Korrekturmaßnahmen nachverfolgen und verwalten.

Öffnen Sie Suchergebnisse in Vulnerability Manager Workspace

Öffnen Sie Suchergebnisse in Vulnerability Manager Workspace anstelle der klassischen Anwenderoberfläche, indem Sie den Anwendungsbereich ändern.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin oder sn_vul.read_all für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager oder sn_vul.app_read_all für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin oder sn_vul_container.read_all für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin oder sn_vulc.read für Konfigurationstestergebnisse (TRs)

Warum und wann dieser Vorgang ausgeführt wird

Beispiel: Wenn Sie nach einem angreifbaren Host-Element suchen, dessen Nummer im **Suchfeld** angegeben ist, indem Sie den Anwendungsbereich auf Vulnerability Manager Workspacefestlegen, wird das VIT in seiner Datensatzansicht in Vulnerability Manager Workspacegeöffnet.

Prozedur

1. Wählen Sie in der zentralen Navigationsleiste das Globussymbol Symbol .
2. Wählen Sie **Anwendungsbereich**aus.
3. Legen Sie den Bereich auf **Arbeitsbereich des Schwachstellenmanagers**fest.

Nächste Maßnahme

Wenn Sie im Feld Suchen der zentralen Navigationsleiste nach Datensätzen wie VITs, Korrekturaufgaben, Genehmigungen von Statusänderungen usw. **suchen**, werden die Datensätze in Vulnerability Manager Workspacegeöffnet.

Wenn der Bereich nicht Global ist, wird das Globussymbol mit einem roten Ring angezeigt. . Wählen Sie es erneut aus, um den Umfang zu ändern.

Zusammenfassung aktiver Datensätze (VITs, AVITs, CVITs und CTRs) erstellen und anwenden

Als Schwachstellenmanager und -analyst können Sie die gewünschten Datensätze filtern, um ihre Zusammenfassung auf der Homepage von Vulnerability Manager Workspacezu visualisieren.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Homepage**.
2. Wählen Sie das Zahnradsymbol und dann **Filter erstellen** auf den Registerkarten Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen oder Ergebnisse der Konfigurationstests.
3. Füllen Sie die Felder im Popup-Fenster „Filter erstellen“ aus.

Popup-Fenster „Filter erstellen“.

Feld	Beschreibung
Filtername	Name für den Filter.
Bedingungen	Bedingung zum Anzeigen nur der Datensätze, für die Sie Visualisierungen anzeigen möchten.
Täglich aktualisieren	Aktualisieren Sie die Visualisierungsinformationen täglich.

4. Wählen Sie **Speichern**.
5. Zeigen Sie die Visualisierungen für die gefilterten Datensätze an, indem Sie den neuen Filter im Feld **Anzeigen** nach auswählen.
   Weitere Informationen zu den Widgets finden Sie unter Homepage im Vulnerability Manager Workspace.
6. So aktualisieren oder löschen Sie einen Filter:

   a. Wählen Sie das Zahnradsymbol und dann **Filter bearbeiten**aus.

   b. Wählen Sie im Popup-Fenster „Gespeicherte Filter“ den Filter aus, den Sie aktualisieren oder löschen möchten.

   c. Aktualisieren oder löschen Sie den Filter.

Aktion	Schritte
Löschen Sie den Filter.	Wählen Sie **Löschen**.
Ändern Sie den Filternamen	Bearbeiten Sie den Filternamen, und wählen Sie **Aktualisieren**aus.
Ändern Sie die Filterbedingungen	Bearbeiten Sie die Bedingung so, dass nur Informationen für bestimmte Datensätze angezeigt werden, und wählen Sie **Aktualisieren**aus.
Täglich aktualisieren	Legen Sie fest, ob die Visualisierungsinformationen täglich aktualisiert werden sollen, und wählen Sie **Aktualisieren**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Homepage im Vulnerability Manager Workspace

Überwachungsthemen in Vulnerability Manager Workspaceverwenden

Verwenden Sie Überwachungsthemen in Vulnerability Manager Workspace, um Schwachstellen und Fehlkonfigurationen anzuzeigen, die aus Ihren importierten Daten anhand der von Ihnen festgelegten Kriterien gefiltert werden. Verwenden Sie diese Informationen, um zu bestimmen, wie sich die Schwachstellen und Fehlkonfigurationen in den einzelnen Überwachungsthemen auf Ihre Umgebung auswirken können.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Auf der Seite „Überwachungsthemen“ können Sie die folgenden Aufgaben ausführen:

- Überwachen Sie die Anzahl der Korrekturmaßnahmen und -datensätze (VITs, AVITs, CVITs und TRs), um den Fortschritt der Korrektur Ihrer Schwachstelle anzuzeigen.
- Bearbeiten oder löschen Sie Ihre vorhandenen Überwachungsthemen, und erstellen Sie Überwachungsthemen.
- Erstellen Sie die Nachbesserungsmaßnahmen, und übergeben Sie die Nachbesserungsaufgaben automatisch an Ihre IT-Teams, und zwar nur für die Schwachstellen, die Sie beheben möchten.

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie das Symbol für Überwachungsthemen.
3. Wählen Sie auf der Seite Überwachungsthemen auf den Registerkarten Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen oder Konfigurationstestergebnisse ein Überwachungsthema aus.

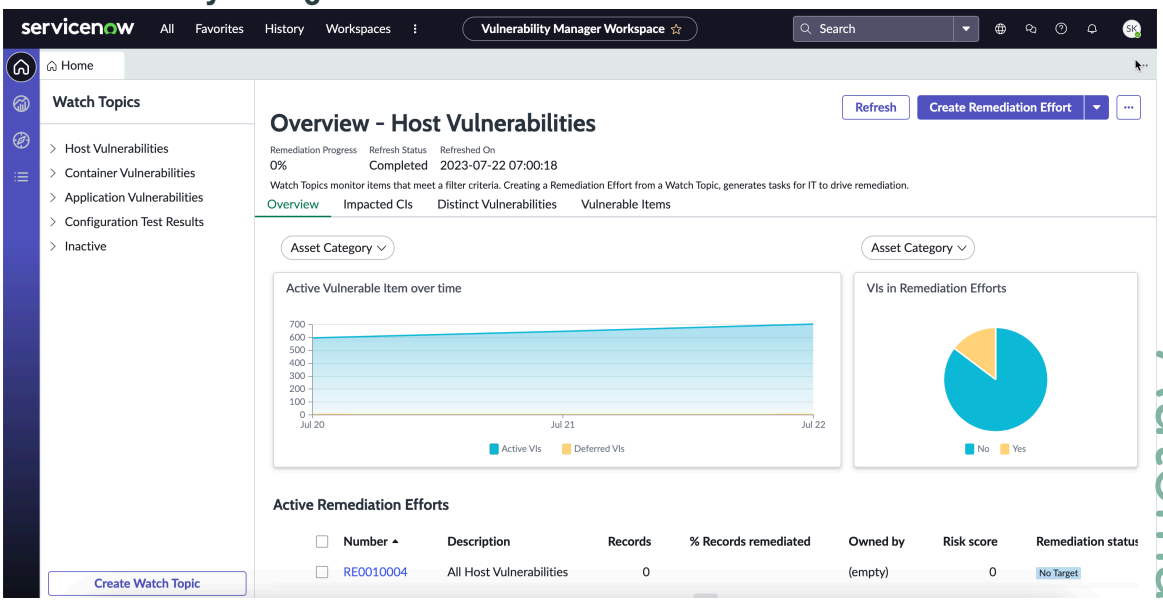
   Wenn Sie ein Überwachungsthema auswählen, wird standardmäßig die Registerkarte **Übersicht** angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu den Überwachungsthemen finden Sie unter Seite „Überwachungsthemen“ im Vulnerability Manager Workspace.

Version 19.0 – Registerkarte „Übersicht“ auf der Startseite des Arbeitsbereichs des Vulnerability-Managers



Die Dashboards sind dynamisch, und neue Schwachstellendaten werden beim Import aktualisiert.

4. Wählen Sie die **Registerkarte Zugehörige Elemente** aus, um weitere Daten anzuzeigen.

   Weitere Informationen zur Liste zugehöriger Elemente und zu Visualisierungen in einem Überwachungsthema finden Sie unter Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema.

5. Führen Sie die UI-Aktionen auf der Seite „Überwachungsthemen“ aus.

6. **Wahlweise:** Wählen Sie einen Datensatz aus, um weitere Details anzuzeigen.

Erstellen Sie ein Überwachungsthema in Vulnerability Manager Workspace

Schwachstellenmanager und Analysten können Überwachungsthemen mit einer Reihe von Bedingungen erstellen, um Teilmengen von Datensätzen (VITs, AVITs, CVITs oder CTRs) herauszufiltern, die sie überwachen möchten.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Auf der Registerkarte „Übersicht“ der Überwachungsthemen zeigt ein jede Nacht aktualisierter Trendbericht zusammen mit anderen Berichten den aktuellen Status der Datensätze für dieses Überwachungsthema an.

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**.
2. **Wahlweise:** Alternativ klicken Sie rechts neben der Schaltfläche Korrekturmaßnahme erstellen auf das ... und anschließend auf Bearbeiten, um ein vorhandenes Überwachungsthema zu ändern.

   Hinweis:
   Möglicherweise stellen Sie eine Verzögerung fest, bevor aktuelle Daten für ein Überwachungsthema angezeigt werden, nachdem Sie die Filterung geändert haben.

3. Wählen Sie unten links auf der Seite **Überwachungsthema erstellen aus**.
4. Füllen Sie die Felder im angezeigten Modal aus.
   Weitere Informationen zu den modalen Feldern „Überwachungsthema erstellen“ finden Sie unterFormularfelder „Überwachungsthema erstellen“..
5. Definieren Sie Bedingungen für die ausgewählte Datensatzkategorie.

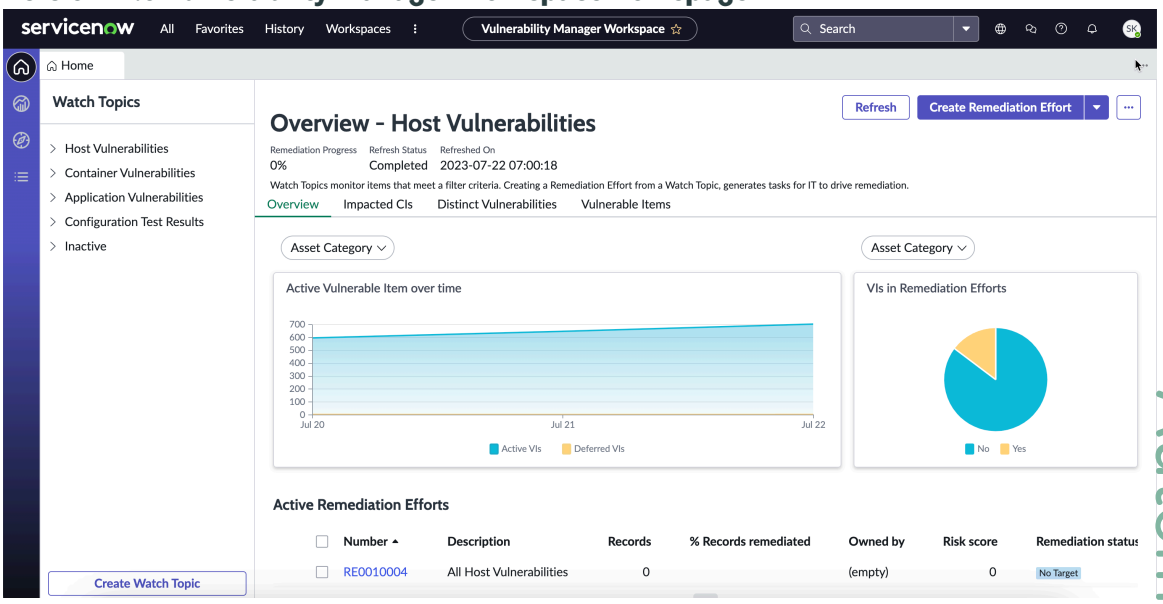
   Hinweis:
   Wenn Sie in Ihrem Überwachungsthema keine Bedingungen festlegen, werden keine Daten in das Dashboard abgerufen.

6. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihr neues Überwachungsthema wird auf der Zielseite der Homepage angezeigt. Tie Überwachungsthemen sind im Navigationsbereich nach Datensatztyp kategorisiert.

Version 19.0 Vulnerability Manager Workspace Homepage



Nächste Maßnahme

Erstellen Sie eine Korrekturmaßnahme.

Bearbeiten oder löschen Sie ein Überwachungsthema in Vulnerability Manager Workspace

Sie können ein vorhandenes Überwachungsthema unter Vulnerability Manager Workspacebearbeiten oder löschen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein vorhandenes Überwachungsthema bearbeiten:

- Die Daten im Dashboard werden entsprechend Ihren Änderungen aktualisiert.
- Die Datensätze, die sich derzeit in den vorhandenen Korrekturmaßnahmen befinden, bleiben unverändert.
- Die Datensätze, die sich derzeit nicht in Korrekturmaßnahmen befinden, werden basierend auf den Kriterien angezeigt, die Sie im Bedingungsgenerator eingeben.

Wenn Sie ein Überwachungsthema löschen, bevor alle zugehörigen Datensätze korrigiert wurden, sind die Datensätze, die mit diesem Überwachungsthema angezeigt werden, nicht betroffen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**.
2. Öffnen Sie das Überwachungsthema, das Sie bearbeiten möchten.
3. Klicken Sie auf das ... und dann auf **Bearbeiten**.

   Hinweis:
   Sie können ein inaktives Überwachungsthema nicht bearbeiten.

4. Ändern Sie im Modal „Überwachungsthema bearbeiten“ die Felder.
5. Klicken Sie auf **Absenden**.

   Hinweis:
   Möglicherweise stellen Sie eine Verzögerung fest, bevor aktuelle Daten für ein Überwachungsthema angezeigt werden, nachdem Sie die Filterung geändert haben.

   Sie können auch vorhandene wiederkehrende Korrekturmaßnahmen bearbeiten. Wenn für ein Überwachungsthema eine wiederkehrende Korrekturmaßnahme vorhanden ist, ist **„Wiederkehrende Maßnahme bearbeiten“** im Menü verfügbar. Wählen Sie diese Option aus, um die wiederkehrende Maßnahme zu bearbeiten.

   Alle Änderungen, die Sie im Datensatz der Korrekturmaßnahme vornehmen und speichern, wirken sich nicht auf andere Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

6. **Wahlweise:** Um ein Überwachungsthema zu löschen, wählen Sie das Drei-Punkte-Menü- ... im Überwachungsthema, und wählen Sie **Löschen aus**.

Deaktivieren oder aktivieren Sie ein Überwachungsthema

Sie können ein Überwachungsthema im Arbeitsbereich des Schwachstellenmanagers deaktivieren oder aktivieren.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

- Alle inaktiven Überwachungsthemen werden im Modul **Inaktiv** im Navigationsbereich angezeigt.
- Sie können keine Korrekturmaßnahme oder wiederkehrende Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen.
- Sie können ein inaktives Überwachungsthema nicht aktualisieren.
- Die Details eines inaktiven Überwachungsthemas und der zugehörigen Korrekturmaßnahmen werden nicht aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**.
2. Öffnen Sie das Überwachungsthema, das Sie deaktivieren möchten.
3. Klicken Sie auf die drei Punkte und anschließend auf **Deaktivieren**.
   Das Überwachungsthema wird im Modul Inaktiv angezeigt.
4. Um ein Überwachungsthema zu aktivieren, wählen Sie im Modul Inaktiv ein Überwachungsthema aus, wählen Sie das Menü mit den drei Punkten aus, und wählen Sie **Aktivieren**aus.
   Das aktivierte Überwachungsthema wird in das entsprechende Modul im Navigationsbereich verschoben.

Verwenden Sie Datensätze für Korrekturmaßnahmen

Wenn Schwachstellenmanager und Analysten Korrekturmaßnahmen (REs) erstellen, werden Korrekturaufgaben (VUL, AVUL, CVUL und CRG) den IT-Teams automatisch zur Korrektur zugewiesen.

Vorbereitungen

Sie müssen eine Korrekturmaßnahme erstellen, bevor Sie sie zur Überwachung des Korrekturfortschritts für Korrekturaufgaben verwenden können.

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Wenn diese Option nicht ausgewählt ist, klicken Sie oben links auf das Listensymbol.

   Die Listenansicht mit aktiven Datensätzen der Korrekturmaßnahme wird angezeigt.

2. Wählen Sie in der Spalte Datensatztyp das Menü mit den drei Punkten aus, und wählen Sie **Nach Datensatztyp gruppieren**aus.
   Die Korrekturmaßnahmen werden in angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Konfigurationstestergebnisse kategorisiert.
3. Klicken Sie auf der Zielseite der Listenansicht, während in den gefilterten Listen Aktive Korrekturmaßnahmen ausgewählt sind, auf einen Datensatz, um ihn zu öffnen.
   Der Datensatz wird angezeigt. Sie können die Korrekturaufgaben und die -Datensätze anzeigen, die der ausgewählten Korrekturmaßnahme zugeordnet sind.
4. In der folgenden Tabelle finden Sie die Aktionen, die Sie für den Datensatz der Korrekturmaßnahme ausführen können.

   Nachdem Sie einen Datensatz erstellt haben, kann es einige Minuten dauern, bis die Korrekturaufgaben und eine große Anzahl von Datensätzen angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Aktion	Beschreibung
Fügen Sie ein Tag hinzu	Klicken Sie rechts neben dem Header auf das kleine Tag-Symbol. Sie können Text hinzufügen, der Ihnen dabei hilft, diesen Datensatz weiter zu identifizieren. Sie können beispielsweise ein Tag hinzufügen, das angibt, dass dieser Datensatz PCI- oder andere kritische Daten enthält.
Fügen Sie dem Datensatz eine Arbeitsnotiz hinzu	Klicken Sie ganz rechts auf dem Bildschirm auf das Symbol **Aktivität** (Blinksymbol), und geben Sie eine Arbeitsnotiz ein. Klicken Sie auf das Symbol, um den Bereich ein-/auszublenden.
Datensatz aktualisieren	Klicken Sie auf der Registerkarte **Details** für alle bearbeitbaren Felder auf ein Feld, um es auszuwählen, nehmen Sie Ihre Änderungen vor, und klicken Sie auf **Speichern**, um den Datensatz zu aktualisieren.
Klicken Sie bei der Anzeige auf das Filtersymbol, um die Daten auf der angezeigten Seite zu verfeinern	Klicken Sie ganz rechts auf eine der Registerkarten Korrekturaufgaben, Angreifbare Elemente oderr Konfigurationstestergebnisse, und klicken Sie auf das Filtersymbol, um die Filter anzuzeigen, die für die Registerkarte gelten. Klicken Sie im angezeigten Bereich auf **Erweiterte Ansicht**, um Filterbedingungen für die Elemente auf der Seite hinzuzufügen oder zu ändern. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern. Beispielsweise können Sie auf der Registerkarte **„Angreifbare Elemente“** das Feld Alter hinzufügen und einen Bereich eingeben, um nur Datensätze aus einem bestimmten Zeitraum anzuzeigen. Datensätze, die den von Ihnen festgelegten Bedingungen entsprechen, werden in der Liste angezeigt.
Verfeinern Sie die Filter für Elemente in einer Spalte	Wählen Sie eine Spalte aus, klicken Sie auf das Menü mit den drei vertikalen Punkten, um sie zu erweitern, und geben Sie Bedingungen ein, um die Daten in der Spalte zu verfeinern und zu gruppieren.
Filtern Sie Elemente heraus, oder gleichen Sie Elemente aus einer Zeile in einer Spalte ab	Angenommen, Sie möchten nur Datensätze anzeigen, die eine bestimmte Schwachstelle aufweisen. Wählen Sie aus der Liste der Datensätze die Zeile des Datensatzes in der **Spalte** Zusammenfassung aus. Klicken Sie auf das angezeigte vertikale Punktmenü, und wählen Sie eines aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Aktion	Beschreibung
	○ **Übereinstimmungen anzeigen** : Zeigt alle anderen Datensätze an, die diese Schwachstelle aufweisen. ○ **Herausfiltern** : Zeigt alle Datensätze an, die diese Schwachstelle nicht aufweisen.

5. Auf den Registerkarten „Korrekturaufgaben“, „Angreifbare Elemente“ und „Konfigurationstestergebnisse“ können Sie Detailinformationen zu einer einzelnen Korrekturaufgabe (VUL, AVUL, CVUL oder CRG), einem angreifbaren Element (VIT, AVIT oder CVIT) und einem Testergebnis (CTR.) anzeigen) Datensätze.

Nächste Maßnahme

Wenn Sie bei Bedarf aus einer Korrekturmaßnahme eine Korrekturaufgabe erstellen möchten, lesen Sie Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace. Sie können auch Erstellen Sie eine anwenderdefinierte Liste von Datensätzen, um den Korrekturfortschritt zu überwachen.

Erstellen Sie eine Korrekturmaßnahme in Vulnerability Manager Workspace

Ein Datensatz für eine Korrekturmaßnahme ist eine statische Liste von Datensätzen, die Sie aus einem Überwachungsthema in Vulnerability Manager Workspaceerstellen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Sie verwenden Korrekturmaßnahmen, um die Aufgaben zu übergeben, mit denen IT-Teams Schwachstellen und Fehlkonfigurationen beheben.

- Sie können vorhandene Korrekturmaßnahmen bearbeiten.
- Erstellen Sie Korrekturmaßnahmen, die automatisch zu von Ihnen festgelegten Daten und Uhrzeiten erstellt werden.
- Übertragen Sie Datensätze aus vorhandenen Korrekturmaßnahmen in eine neue Korrekturmaßnahme.

Ab Version 18.0 ist die Schaltfläche **Korrekturmaßnahmen erstellen** inaktiv, da Sie keine Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen können.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**.
2. Wählen Sie auf der Seite „Überwachungsthemen“ ein Überwachungsthema aus, für das Sie eine Korrekturmaßnahme erstellen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um die Datensätze anzuzeigen, die dem ausgewählten Überwachungsthema zugeordnet sind, klicken Sie unter dem Datensatz-Header in den jeweiligen Überwachungsthemen auf die Registerkarte **Angreifbare Elemente**, **Angreifbare Anwendungselemente**, **Angreifbare Container-Elemente** oder **Konfigurationstestergebnisse**.

   Die Datensätze werden angezeigt.

   Beispielsweise können Sie im Header unter der Registerkarte Angreifbare Elemente die Gesamtzahl der Datensätze anzeigen, die dieses Überwachungsthema aufweist.

   Die folgenden Spalten und Daten werden angezeigt:

Spalten auf der Registerkarte „Angreifbare Elemente“.

Spalte	Beschreibung
Nummer	Die Datensatznummer.
Zusammenfassung	Beschreibung der Schwachstelle.
Konfigurationselement	Das Asset, das der Schwachstelle zugeordnet ist.
Risikobewertung	Quantifizierte Risikopunktzahl, die Datensätze in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt.
Status	Status des Datensatzes.
Korrekturstatus	Status der Korrektur für einen Datensatz.
Zuweisungsgruppe	Zuweisungsgruppen, die für die Korrektur verantwortlich sind. Die Zuweisung von Datensätzen zu Gruppen basiert auf den von Ihnen erstellten Zuweisungsregeln.
Korrekturmaßnahme	Wenn er einer Korrekturmaßnahme zugewiesen ist, listet jeder Datensatz die ihm zugewiesene Korrekturmaßnahme auf. Nachdem ein Datensatz einer Korrekturmaßnahme hinzugefügt wurde, wird er keinen anderen von Ihnen erstellten Korrekturmaßnahmen hinzugefügt.
Zuweisungsgruppe	Zuweisungsgruppen, die für die Korrektur verantwortlich sind. Die Zuweisung von Datensätzen zu Gruppen basiert auf den von Ihnen erstellten Zuweisungsregeln.
Korrekturmaßnahme	Wenn er einer Korrekturmaßnahme zugewiesen ist, listet jeder Datensatz die ihm zugewiesene Korrekturmaßnahme auf. Nachdem ein Datensatz einer Korrekturmaßnahme hinzugefügt wurde, wird er keinen anderen von Ihnen erstellten Korrekturmaßnahmen hinzugefügt.
In Korrekturaufgabe	Bei „wahr“gibt dieser Wert an, dass sich ein Datensatz bereits in einer Korrekturaufgabe befindet. Datensätze können in mehreren Korrekturaufgaben enthalten sein, aber ein Datensatz kann nur einer Korrekturmaßnahme hinzugefügt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Exploit vorhanden	Gibt an, ob ein Known Exploit für einen Datensatz vorhanden ist.
Zuletzt geöffnet	Datum, an dem der Datensatz zuletzt in Ihrem Now Platformgeöffnet wurde. Wenn der Datensatz geschlossen und dann erneut geöffnet wurde, ist dies der Zeitpunkt, zu dem der Datensatz zuletzt erneut geöffnet wurde.

4. Klicken Sie auf Korrekturmaßnahme erstellen, um eine **Korrekturmaßnahme zu erstellen**.

   Wenn Sie eine Korrekturmaßnahme erstellen, werden Datensätze, die sich bereits in Korrekturmaßnahmen befinden, keinen neuen Korrekturmaßnahmen hinzugefügt, die Sie aus diesem Überwachungsthema erstellen.

   Wenn in Überwachungsthemen Datensätze aktualisiert oder neue Datensätze erstellt werden, können Sie Korrekturmaßnahmen erstellen.

5. Alternativ können Sie Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Vulnerability Manager Workspace.

   Die Schaltfläche **„Bearbeiten“** ist im Menü für vorhandene Korrekturmaßnahmen verfügbar. Sie haben die Möglichkeit, die Felder und Bedingungen in einem angezeigten modalen Element zu ändern. Alle Änderungen, die Sie im Datensatz der Korrekturmaßnahme vornehmen und speichern, wirken sich nicht auf andere Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

6. Füllen Sie in Schritt 1 des Modals „Korrekturmaßnahme erstellen“ die Felder aus.

   Geben Sie im Feld Kurzbeschreibung einen Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt und Ihnen hilft, sie in der Maßnahmenliste zu finden und nachzuverfolgen.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie in der Liste der Korrekturmaßnahmen leicht finden können.

7. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die Datensätze in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme generieren, nachdem sie erstellt wurde.

8. Um die doppelten angreifbaren Hostelemente automatisch zu aktualisieren, müssen Sie das Kontrollkästchen **Doppelte angreifbare Elemente für erstellte Korrekturaufgaben automatisch aktualisieren** aktivieren.

   Hinweis:
   Dieses Kontrollkästchen ist nur für Host-Schwachstellen verfügbar.

9. Überprüfen Sie in Schritt 3, Übertragung, wie viele Datensätze Sie der Korrekturmaßnahme hinzufügen möchten, und prüfen Sie, wie viele Datensätze von anderen aktiven Korrekturmaßnahmen für den Transfer verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

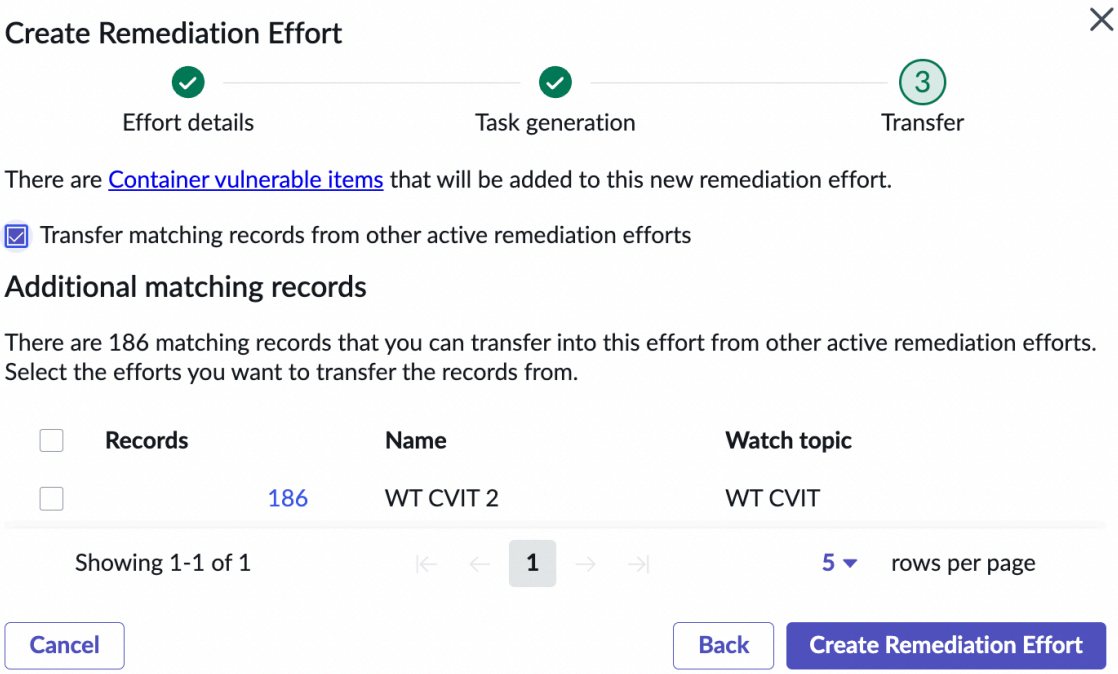
Wenn keine neuen, aktiven Datensätze zum Hinzufügen vorhanden sind, wird der folgende Text angezeigt:

Es gibt keine verfügbaren aktiven Datensätze, die dieser neuen Korrekturmaßnahme hinzugefügt werden können.

Alle zusätzlichen Datensätze, die für die Übertragung an diese Maßnahme verfügbar sind, werden unter Zusätzliche übereinstimmende Datensätze aufgeführt.

Aktivieren Sie das Kontrollkästchen **Übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen übertragen,** und aktivieren Sie dann die Kontrollkästchen für die Datensätze, die Sie aus anderen aktiven Korrekturmaßnahmen übertragen möchten.

Version 18.0 Korrekturmaßnahme erstellen



Nachdem Sie **auf Korrekturmaßnahmen erstellen**geklickt haben, wird in wenigen Minuten die neue Korrekturmaßnahme angezeigt. Je nach Anzahl der Datensätze kann das Füllen des neuen Datensatzes einige Zeit dauern. Eine Meldung gibt an, ob der Datensatz noch gefüllt wird.

Die neue Korrekturmaßnahme wird mit allen Datensätzen erstellt, die aus dem Überwachungsthema verfügbar sind, mit dem sie erstellt wurde, zusätzlich zu allen Datensätzen, die Sie für die Übertragung aus vorhandenen Maßnahmen ausgewählt haben.

Wenn Sie die zu übertragenden Datensätze aus einer vorhandenen Maßnahme auswählen und die vorhandene Maßnahme alle ihre Datensätze in die neue Maßnahme überträgt, wird die Korrekturmaßnahme geschlossen, aus der Sie die Datensätze verschoben haben. Weitere Informationen dazu, wie sich die Übertragung von Datensätzen auf die mit den Korrekturmaßnahmen verknüpften Korrekturaufgaben auswirkt, finden Sie unter Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn aus dem Überwachungsthema keine Datensätze verfügbar sind oder keine Datensätze zur Übertragung ausgewählt wurden, ist die Schaltfläche **Korrekturmaßnahme erstellen** deaktiviert.

Die geplante Aufgabe `Populate Efforts` wird alle 10 Minuten ausgeführt, um die Daten in den Widgets basierend auf der ausgewählten Bedingung auszufüllen.

Klicken Sie auf die Registerkarte Korrekturfortschritt, um den Fortschritt der Korrektur anzuzeigen. Klicken Sie auf ein beliebiges Element, um Details wie Datensatztyp, Risikopunktzahl, Risikobewertung, Prozentsatz der korrigierten Datensätze, Datensätze im Status „Zurückgestellt“ und „Nicht zurückgestellt“ sowie die Gesamtzahl der Datensätze, die im Überwachungsthema verwendeten Bedingungen und den Korrekturstatus anzuzeigen. Die Informationen zum Korrekturstatus, z. B. Korrekturziel und Korrekturstatus, werden aus der Tabelle „Angreifbare Elemente“ zusammengefasst. Die höchste Risikopunktzahl für Datensätze wird in der Tabelle „Schwachstellen-Rechner“ zusammengefasst, die Risikopunktzahl hingegen in **Rechner für Schwachstellen-Rollup** > **Rollup von Korrekturmaßnahme** .

Auf der Registerkarte Korrekturaufgaben werden die Aufgaben für alle Arten von Problemen angezeigt. Die Felder werden gefüllt, wenn die folgenden geplanten Aufgaben ausgeführt werden. Sie werden automatisch alle 15 Minuten ausgeführt:

- Rollup der Werte von angreifbaren Anwendungselementen zu Schwachstelle und Gruppe.
- Rollup der Werte von angreifbaren Container-Elementen zu Schwachstelle und Gruppe.
- Rollup von Testergebniswerten zur Testergebnisgruppe und zum Konfigurationstest.
- Rollup der Werte von angreifbaren Elementen zu Schwachstelle und Gruppe.

In der Listenansicht können Sie Korrekturmaßnahmen, Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse usw. anzeigen. Sie können eine Korrekturaufgabe oder ein angreifbares Element öffnen und die Seite „Details“ anzeigen. Klicken Sie auf die Ellipsen „Weitere Aktionen“ und anschließend **auf Untersuchung starten,** um eine Korrekturaufgabe zu lösen.

10. **Wahlweise:** Sie können auch vorhandene wiederkehrende Korrekturmaßnahmen bearbeiten.

    (Optional) Wenn für ein Überwachungsthema eine wiederkehrende Korrekturmaßnahme vorhanden ist, ist **„Wiederkehrende Maßnahme bearbeiten“** im Menü oben rechts neben einem Überwachungsthema verfügbar. Wählen Sie diese Option, um die wiederkehrende Maßnahme zu bearbeiten.

    Alle Änderungen, die Sie im Datensatz der Korrekturmaßnahme vornehmen und speichern, wirken sich nicht auf andere Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace

Erstellen Sie bei Bedarf eine Korrekturaufgabe aus einer Korrekturmaßnahme. Wenn Sie bei Bedarf eine Korrekturaufgabe erstellen, wählen Sie die Datensätze, die Sie hinzufügen möchten, manuell aus.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Ab Version 18.0 von Vulnerability Responsekönnen Sie keine Korrekturaufgabe in der Datensatzansicht einer Korrekturmaßnahme erstellen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Klicken Sie oben links im Arbeitsbereich bei angezeigter Homepage auf das Symbol **Listenansicht**, um die Zielseite der Liste anzuzeigen.
3. Klicken Sie unter Korrekturmaßnahmen entweder **auf Aktiv** oder **auf Alle**.
4. Klicken Sie in der angezeigten Liste auf einen Datensatz, um ihn zu öffnen.
   Die Registerkarte „Übersicht“ des Datensatzes wird angezeigt.
5. Klicken Sie auf die Registerkarte **Angreifbare Elemente**.
   Die Liste der Datensätze wird angezeigt.
6. Um eine neue Korrekturaufgabe zu erstellen, wählen Sie in der Spalte Anzahl die Datensätze aus, die Sie hinzufügen möchten.
7. Klicken Sie auf **Korrekturaufgabe erstellen**.
8. Füllen Sie im angezeigten Modal die Felder aus.
9. Klicken Sie auf **Erstellen**.
10. Die neue Korrekturaufgabe wird mit den von Ihnen ausgewählten aktiven Datensätzen angezeigt.

Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Vulnerability Manager Workspace

Sie können wiederkehrende Korrekturmaßnahmen erstellen und planen, die automatisch zu von Ihnen festgelegten Daten und Uhrzeiten generiert werden.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Sie können automatisch wiederkehrende Korrekturmaßnahmen nach einem Zeitplan erstellen, um Schwachstellen nachzuverfolgen, die auftreten und sofortige und kontinuierliche Aufmerksamkeit erfordern.

Ab Version 18.0 ist die Option „ **Wiederkehrende Maßnahme erstellen“** inaktiv, da Sie keine wiederkehrende Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen können. Wenn Sie ein Überwachungsthema deaktivieren, für das bereits eine wiederkehrende Maßnahme geplant ist, wird erst dann eine neue Korrekturmaßnahme erstellt, wenn das Überwachungsthema aktiviert wird. Außerdem werden die Details **Aufwandsserie** und **Nächstes Wiederholungsdatum** oben rechts ausgeblendet. Nachdem Sie das Überwachungsthema aktiviert haben, wird im bevorstehenden Zeitplan eine Korrekturmaßnahme erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**.
2. Wählen Sie auf der Seite „Überwachungsthemen“ ein Überwachungsthema aus, für das Sie eine wiederkehrende Korrekturmaßnahme erstellen möchten.

   Sie können eine wiederkehrende Korrekturmaßnahme pro Überwachungsthema erstellen.

   Hinweis:
   Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Sie können jedoch Datensätze aus vorhandenen, nicht wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Weitere Informationen zum Übertragen von Datensätzen finden Sie unter Übertragen Sie Datensätze an Korrekturmaßnahmen im Vulnerability Manager Workspace.

3. Wählen Sie in einem Überwachungsthema oben rechts in der Liste Korrekturmaßnahme erstellen **die Option Wiederkehrende Maßnahme erstellen aus**.

   Das Modal „Wiederkehrende Maßnahme erstellen“ wird angezeigt.

4. Füllen Sie in Schritt 1, Aufwandsdetails, die erforderlichen Felder aus.

   Geben Sie im Feld Kurzbeschreibung den Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt, mit der Sie sie finden und in der Aufwandsliste nachverfolgen können.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie in der Liste der Korrekturmaßnahmen leicht finden können. Beispiel: Schwachstellen bei extern ausgerichteten Assets.

5. Klicken Sie auf **Next (Weiter)**.
   Details zur Aufgabengenerierung werden angezeigt.
6. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die angreifbaren Elemente in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme generieren, nachdem sie erstellt wurde.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Configuration Item
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine (Es werden keine Korrekturaufgaben erstellt). Verwenden Sie diese Methode, wenn Sie einer Korrekturaufgabe für diese Maßnahme manuell Datensätze hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace.
7. Um die doppelten angreifbaren Host-Elemente automatisch zu aktualisieren, müssen Sie die Option **Doppelte angreifbare Elemente automatisch aktualisieren für erstellte Korrekturaufgaben** auswählen.

   Hinweis:
   Dieses Kontrollkästchen ist nur für Host-Schwachstellen verfügbar.

8. Klicken Sie auf **Weiter**, um fortzufahren.
9. Wählen Sie in Schritt 3, Wiederholung, die Häufigkeit aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf **Wiederholung planen**.
    Es wird eine Meldung angezeigt, dass der wiederkehrende Korrekturdatensatz erstellt wurde. Die neue Korrekturmaßnahme wird nicht sofort angezeigt. Sie wird zu dem Zeitpunkt erstellt, zu dem Sie sie geplant haben. Es wird in Ihren Listen angezeigt, nachdem es von der geplanten Aufgabe erstellt wurde.

    Das Datum, an dem die Korrekturmaßnahmen erstellt wird, wird unter dem entsprechenden Überwachungsthema angezeigt. Weitere Informationen dazu, wie sich die Datensatzübertragung auf die mit den Korrekturmaßnahmen verknüpften Korrekturaufgaben auswirkt, finden Sie unter Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen.

Übertragen Sie Datensätze an Korrekturmaßnahmen im Vulnerability Manager Workspace

Sie können Datensätze aus vorhandenen Korrekturmaßnahmen in neue Korrekturmaßnahmen im Vulnerability Manager Workspaceübertragen.

Vorbereitungen
Wenn Sie mit einer Zero-Day-Bedrohung oder einer sehr kritischen Schwachstelle konfrontiert werden, die Sie schnell beheben möchten, können Sie alle aktiven Datensätze, die Sie bereits für diese Schwachstelle haben, in einer Korrekturmaßnahme zusammenfassen. Jeder Datensatz kann jedoch nur in einem Versuch enthalten sein, und Datensätze können sich zwischen Überwachungsthemen überschneiden. Um sie alle zu sammeln, müssen Sie diese Datensätze aus mehreren vorhandenen Maßnahmen in eine einzige Korrekturmaßnahme übertragen.

Angenommen, Sie haben eine Korrekturmaßnahme erstellt, die eine Schwachstelle mit hoher Priorität enthält. Da diese Schwachstelle weit verbreitet ist und sich möglicherweise auf andere Bereiche in Ihrer Umgebung auswirkt, verfügen Sie möglicherweise über Datensätze, die mit dieser Schwachstelle bereits in Korrekturmaßnahmen in Zusammenhang stehen. Um diese Datensätze so zu kombinieren, dass sie sich alle in einer Korrekturmaßnahme befinden, können Sie Datensätze aus vorhandenen Korrekturmaßnahmen in eine neue Korrekturmaßnahme übertragen.

Hinweis:
Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Weitere Informationen finden Sie unter Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Vulnerability Manager Workspace.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie das Symbol für Überwachungsthemen.
3. Wählen Sie auf der Seite „Überwachungsthemen“ ein Überwachungsthema aus, für das Sie eine wiederkehrende Korrekturmaßnahme erstellen möchten.
4. Klicken Sie auf **Korrekturmaßnahme erstellen**.
   Das Modal „Korrekturmaßnahme erstellen“ wird angezeigt.
5. Füllen Sie im ersten Schritt, Aufwandsdetails, die erforderlichen Felder aus.

   Geben Sie im Feld Kurzbeschreibung einen Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt, mit der Sie sie finden und in der Aufwandsliste nachverfolgen können.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie in der Liste der Korrekturmaßnahmen leicht finden können. Beispiel: `Aktive Log4J-Schwachstellen`.

   a. Geben Sie im Feld Name einen Namen für Ihre neue Korrekturmaßnahme ein.
   Standardmäßig wird der Name des Überwachungsthemas angezeigt.

   b. Geben Sie im Feld Beschreibung Text ein, mit dem Sie diese Korrekturmaßnahme in der Liste der Korrekturmaßnahmen leicht finden können.

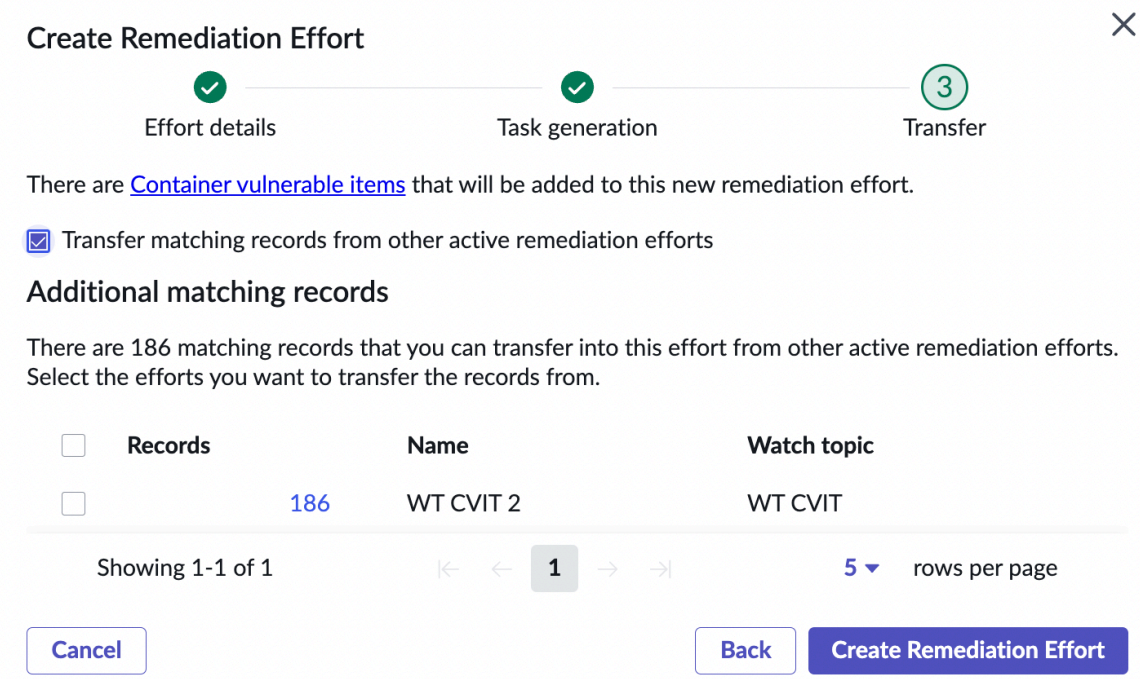
6. Klicken Sie auf **Next (Weiter)**.
   Details zur Aufgabengenerierung werden angezeigt.
7. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die Datensätze in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme generieren, nachdem sie erstellt wurde.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Configuration Item
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine (Es werden keine Korrekturaufgaben erstellt). Verwenden Sie diese Methode, wenn Sie einer Korrekturaufgabe für diese Maßnahme manuell Datensätze hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie bei Bedarf eine Korrekturaufgabe unter Korrekturmaßnahme in Vulnerability Manager Workspace.
8. Um die doppelten angreifbaren Elemente automatisch zu aktualisieren, müssen Sie die Option **Doppelte angreifbare Elemente automatisch aktualisieren für erstellte Korrekturaufgaben** auswählen.
9. Klicken Sie auf **Next (Weiter)**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Überprüfen Sie in Schritt 3, Übertragung, wie viele Datensätze der Korrekturmaßnahmen hinzugefügt werden und wie viele Datensätze von anderen aktiven Korrekturmaßnahmen für den Transfer verfügbar sind.
11. Um Datensätze aus anderen Projekten zu übertragen, aktivieren Sie in der Liste die Kontrollkästchen für die gewünschten Datensätze.

    Aktivieren Sie das Kontrollkästchen **Übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen übertragen,** und aktivieren Sie dann die Kontrollkästchen für die Datensätze, die Sie aus anderen aktiven Korrekturmaßnahmen übertragen möchten.

    Version 18.0 Korrekturmaßnahme erstellen

12. Klicken Sie auf **Korrekturmaßnahme erstellen**.

    Nach einigen Minuten wird die neue Korrekturmaßnahme angezeigt. Je nach Anzahl der Datensätze kann dies einige Zeit dauern. Eine Meldung gibt an, dass der Datensatz gefüllt wird.

    Die neue Korrekturmaßnahme wird mit allen Datensätzen erstellt, die aus dem Überwachungsthema verfügbar sind, mit dem sie erstellt wurde, zusätzlich zu allen Datensätzen, die Sie für die Übertragung aus vorhandenen Maßnahmen ausgewählt haben.

    Wenn Sie die zu übertragenden Datensätze aus einer vorhandenen Maßnahme auswählen und die vorhandene Maßnahme alle ihre Datensätze in die neue Maßnahme überträgt, wird die Korrekturmaßnahme geschlossen, aus der Sie die Datensätze verschoben haben.

    Hinweis:
    Wenn weder Datensätze aus dem Überwachungsthema verfügbar sind noch Datensätze zur Übertragung ausgewählt wurden, ist die Schaltfläche **Korrekturmaßnahme erstellen** deaktiviert.

    Weitere Informationen dazu, wie sich die Datensatzübertragung auf die Korrekturaufgaben auswirkt, die den Korrekturmaßnahmen zugeordnet sind, finden Sie unter Datensätze übertragen oder Datensatz-Übertragung durchführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Fügen Sie als Schwachstellenmanager oder -analyst der Bibliothek für Ausgleichssteuerungen in Vulnerability Manager Workspaceeine Liste von Ausgleichssteuerungen hinzu, die zur Risikominderung von angreifbaren Hostelementen und für Korrekturaufgaben angewendet werden können.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Einige häufig verwendete Ausgleichssteuerungen sind im Lieferumfang des Basissystems enthalten. Sie können diese Ausgleichssteuerungen anzeigen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Listen** > **Bibliotheken** > **Ausgleichssteuerungen**. Sie können diese Ausgleichssteuerungen je nach Bedarf aktivieren oder deaktivieren.

Hinweis:
Die Ausgleichssteuerungen sind nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie auf der Listenseite unter „Bibliotheken“ **Ausgleichssteuerungen**aus.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder im Formular „Ausgleichssteuerungen erstellen“ aus.

Formularfelder „Ausgleichssteuerungen erstellen“.

Feld	Beschreibung
Name	Name der Ausgleichssteuerung, die als Option in der Dropdown-Liste **Ausgleichssteuerungen** des Modals Ausnahme anfordern angezeigt wird.
Beschreibung	Kurze Informationen, die Details zur Ausgleichssteuerung enthalten.
Aktiv	Status der Ausgleichssteuerung. In der Dropdown-Liste **Ausgleichssteuerungen** des Modals Ausnahme anfordern werden nur aktive Steuerungen angezeigt.

5. Wählen Sie **Speichern**.
6. Wählen Sie in der Liste „Ausgleichssteuerungen“ unter „Bibliotheken“ die gewünschte Ausgleichssteuerung aus, und wählen Sie **Bearbeiten**, aktivieren oder deaktivieren Sie eine Ausgleichssteuerung, und klicken Sie auf **Speichern**, um die Ausgleichssteuerungen zu ändern.
   Alle aktiven Ausgleichssteuerungen werden als Option in der Dropdown-Liste **Ausgleichssteuerungen** des Modals Ausnahme anfordern für Risikominderungsanforderungen angezeigt.

Nächste Maßnahme

Ab v21.0 von Vulnerability Responsekönnen Sie Ausgleichssteuerungen CVEs oder TPEs zuordnen, nachdem Sie der Bibliothek Ausgleichssteuerungen hinzugefügt haben. Weitere Informationen zum Zuordnen von Ausgleichssteuerungen finden Sie unter Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikominderungsanforderungen zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Ausgleichssteuerungen zur Risikoreduzierung verstehen

Risikominderung für ein CVE oder TPE aktivieren oder deaktivieren

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikominderungsanforderungen zu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikominderungsanforderungen zu

Als Schwachstellenmanager oder -analyst können Sie relevante Ausgleichskontrollen mit einem Common Vulnerability-Eintrag (CVE) oder einem Drittanbietereintrag (TPE) in Vulnerability Manager Workspaceverknüpfen, die zur Reduzierung des von einer Schwachstelle ausgehenden Risikos verwendet werden können.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

- Wenn Sie keine Ausgleichssteuerungen mit einem CVE oder TPE verknüpfen, werden alle aktiven Steuerungen im Feld Ausgleichssteuerungen auswählen des Formulars Ausnahme anfordern angezeigt.
- Wenn Sie einem CVE eine Ausgleichssteuerung zuordnen, wird diese Ausgleichssteuerung automatisch dem TPE zugeordnet, das dem CVE zugeordnet ist.

Hinweis:
Die Ausgleichssteuerungen sind nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Öffnen Sie auf der Seite „Listen“ unter „Bibliotheken“ eines der folgenden Elemente, für das Sie die Steuerelemente zuordnen möchten:
   - **CVE** aus der CVEs-Liste.
   - **TPE** aus der TPE-Liste.
3. Wählen Sie **Steuerungen zuordnen**aus.

   Hinweis:
   Die Schaltfläche **Steuerungen zuordnen** wird nur angezeigt, wenn die Risikominderung für ein CVE oder TPE aktiviert ist. Mit anderen Worten: Sie können Ausgleichssteuerungen nur zuordnen, wenn die Risikominderung für ein CVE oder TPE aktiviert ist. Wenn die Schaltfläche **Steuerungen zuordnen** nicht sichtbar ist, wählen Sie **Risikominderung aktivieren**aus.

4. Wählen Sie im Modal „Steuerungen zuordnen“ die Ausgleichssteuerungen aus, die auf Schwachstellen angewendet werden können, die dem CVE oder TPE zugeordnet sind, um das Risiko zu reduzieren.
5. Wählen Sie **Absenden**.
   - Die zugeordneten Ausgleichssteuerungen werden auf der Registerkarte Anwendbare Ausgleichssteuerungen in der Datensatzansicht des CVE und TPE angezeigt.
   - Während ein Korrekturbesitzer eine Risikominderung anfordert, werden diese zugehörigen Ausgleichssteuerungen im Feld „Ausgleichssteuerungen auswählen“ im Modal „Ausnahme anfordern“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Ausgleichssteuerungen zur Risikoreduzierung verstehen

Risikominderung für ein CVE oder TPE aktivieren oder deaktivieren

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Risikominderung für ein CVE oder TPE aktivieren oder deaktivieren

Als Schwachstellenmanager und -analyst können Sie die Risikominderungsanforderungen für die Host-Schwachstellen, die einem Common Vulnerability Eintrag (CVE) oder einem Drittparteieintrag (TPE) in Vulnerability Manager Workspacezugeordnet sind, deaktivieren oder aktivieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Risikominderung für CVE und TPE ist standardmäßig aktiviert.

Hinweis:
Die Ausgleichssteuerungen sind nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
   Öffnen Sie auf der Seite „Listen“ unter „Bibliotheken“ eine der folgenden Optionen, für die Sie die Risikominderungsanforderungen deaktivieren möchten:
   - **CVE** aus der CVEs-Liste.
   - **TPEs** aus der TPEs-Liste.
2. Wählen Sie **Risikominderung deaktivieren**aus.
   Der Besitzer der Korrektur kann keine Risikominderung für die angreifbaren Host-Elemente anfordern, die sich auf dieses CVE oder TPE beziehen. Mit anderen Worten: Das Kontrollkästchen Risikominderung anfordern wird nicht angezeigt, wenn im Modal „Ausnahme anfordern“ als **Grund** die Option Ausgleichende Steuerung vorhanden ausgewählt ist.
3. Um die Risikominderungsanforderungen für angreifbare Host-Elemente zu aktivieren, wählen Sie **Risikominderung aktivieren**aus.

Zugehörige Informationen

Ausgleichssteuerungen zur Risikoreduzierung verstehen

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikominderungsanforderungen zu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Scannen Sie Datensätze und Korrekturaufgaben im erneut Vulnerability Manager Workspace

Um sicherzustellen, dass Ihre Korrekturaufgaben und Datensätze zwischen geplanten Scan-Zyklen gelöst wurden, initiieren Sie bei Bedarf erneute Scans von Ihrem Now Platform.

Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin.

Durch erneute Scans können Sie überprüfen, ob durch Ihre Nachbesserungsaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Scanner Rapid7 und Qualys sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die Schaltfläche **Erneut scannen** nicht verfügbar.

Um diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin zu aktivieren:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in den Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

Erneutes Scannen wird für Datensätze und Korrekturaufgaben mit den folgenden Integrationen in Vulnerability Manager Workspaceunterstützt. Weitere Informationen finden Sie in den folgenden Themen:

- Scannen Sie Rapid7 angreifbare Elemente aus den Arbeitsbereichen Vulnerability Response erneut
- Scannen Sie Qualys angreifbare Elemente aus den Arbeitsbereichen Vulnerability Response erneut
- Scannen Sie die angreifbaren Elemente Tenable.io und Tenable.sc aus den Arbeitsbereichen Vulnerability Response erneut

Um erneute Scans in Vulnerability Manager Workspace aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, benötigen die Datensätze einen unterstützten Scanner als Quelle.

Unter Umständen möchten Sie eine gefilterte Liste erstellen, die Datensätze nach ihrer Quelle anzeigt. Ein Beispiel zum Erstellen einer Liste finden Sie unter Erstellen Sie eine anwenderdefinierte Liste von Datensätzen.

Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace

Bewerten Sie die Zuweisungen, das Zieldatum der Korrektur, die Korrekturaufgaben, die Ausnahmen und die Risikopunktzahl für eine Reihe von Datensätzen (VITs, AVITs, CVITs oder TRs) in Vulnerability Manager Workspace.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Vor Version 23.0 von Vulnerability Response war es erforderlich, die Regeln auf alle Datensätze anzuwenden, um die aktuellen Zuweisungen, Korrekturzieldaten,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikopunktzahlen und Korrekturaufgaben zu erhalten. Dies war ein zeitaufwändiger Prozess. Ab Version 23.0 können Sie diese Eigenschaften für bestimmte Datensätze selektiv auswerten und aktualisieren und so die Verarbeitungszeit reduzieren. Darüber hinaus können Sie den Nachbesserungsprozess basierend auf diesen aktualisierten Eigenschaften verfeinern. Ab v24.0.6 von Vulnerability Response können Sie die Ausnahmeregeln für ausgewählte Datensätze im Vulnerability Manager Workspaceauswerten.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Öffnen Sie auf der Listenseite die Liste Aktiv oder Alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Anwendungselemente
   - Angreifbare Container-Elemente
   - Konfigurationstestergebnisse
3. **Wahlweise:** Aktivieren Sie das Kontrollkästchen der gewünschten Datensätze, um nur die ausgewählten Datensätze zu aktualisieren, indem Sie im Modal die Option Ausgewählte Elemente aktivieren.
4. Wählen Sie die Schaltfläche **Erneut auswerten** aus.
5. Wählen Sie im modalen Dialogfeld „Korrektureigenschaften erneut auswerten und aktualisieren“ die Eigenschaften aus, die Sie für die ausgewählten Datensätze aktualisieren möchten.

   Hinweis:
   Wenn Sie eine Eigenschaft auswählen, werden die abhängigen Eigenschaften automatisch ausgewählt.

6. Wählen Sie **Übernehmen**.

Ergebnisse

Die Eigenschaften werden für die ausgewählten Datensätze aktualisiert. Sie können in den **Arbeitsnotizen** der Datensätze nach den vorherigen und aktuellen Werten der aktualisierten Korrektureigenschaften suchen.

Verwenden Sie die Listenansicht in Vulnerability Manager Workspace

Die Listenansicht in Vulnerability Manager Workspace ermöglicht es Schwachstellen- und Sicherheitsmanagern sowie Analysten, den Korrekturfortschritt für Datensätze anzuzeigen, Detailinformationen zu Vulnerability Response-Datensätzen anzuzeigen und den Status ihrer Genehmigungsanforderungen und Ausnahmen anzuzeigen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Klicken Sie bei angezeigter Homepage oben links im Arbeitsbereich auf das **Listensymbol**.
3. **Wahlweise:** Klicken Sie auf **Meine Listen,** um eine Liste zu erstellen.
   Weitere Informationen zum Erstellen einer Liste finden Sie unter Erstellen Sie eine anwenderdefinierte Liste von Datensätzen.
4. In der folgenden Tabelle finden Sie die Aktionen, die Sie auf der Listenseite ausführen können.

UI-Aktion	Beschreibung
Öffnen Sie eine Korrekturmaßnahme	
Führen Sie den Mauszeiger über eine Zeile, und klicken Sie links neben der Spalte Nummer, während eine Liste angezeigt wird, auf das kleine Informationssymbol **(i)** für einen Datensatz.	Details zu den Datensätzen werden im rechten Seitenbereich der Seite angezeigt. Zu den Details gehören: ○ Zuweisungsgruppe ○ Schwachstelle ○ Zugewiesen an ○ Kurzbeschreibung ○ Beschreibung Sie können die Felder bearbeiten. Wenn das Kontrollkästchen Aktiv angezeigt wird, können Sie den Datensatz aktivieren oder deaktivieren. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
Liste aktualisieren	Laden Sie die aktuelle Seite mit dem Aktualisierungssymbol oben rechts auf der Seite neu.
Breiten zurücksetzen	Klicken Sie auf das Zahnradsymbol, um die Spaltenbreiten in Ihren Listen anzupassen. Eine Kopie der ursprünglichen Liste wird unter **Ihre Listen**gespeichert.
Kopieren Sie die URL für die angezeigte Seite	Kopieren Sie die URL zur Verwendung an anderer Stelle.
Exportieren Sie die Seite	Geben Sie im Modal die Datei und die Liefertypen ein und klicken Sie auf **Exportieren**.
Verfeinern Sie die Filter für die Daten auf der Seite.	Wählen Sie eine Spalte aus, und erweitern Sie das Menü mit den drei vertikalen Punkten, um Optionen anzuzeigen, mit denen die Daten in der Spalte weiter gefiltert werden. Beispielsweise können Sie die Spalte „Zuweisungsgruppe“ aus der Liste der aktiven Korrekturaufgaben nach einer bestimmten Zuweisungsgruppe filtern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Aktion	Beschreibung
Filtern Sie Elemente heraus, oder gleichen Sie Elemente aus einer Zeile in einer Spalte ab	Wählen Sie eine Zelle in einer Spalte aus, und verfeinern Sie die angezeigten Daten, indem Sie eine auswählen: ○ Übereinstimmungen anzeigen: Zeigt nur Elemente an, die der ausgewählten Zelle in der Spalte entsprechen. ○ Herausfiltern: Filtert die Elemente aus der Spalte heraus, die der ausgewählten Zelle in der Spalte entsprechen.

5. Erstellen Sie ein angreifbares Anwendungselement aus der Liste **„Aktiv“** oder **„Alle“** unter *`Application Vulnerable items`*, indem Sie oben rechts auf die Schaltfläche **Neu** klicken.

Erstellen Sie eine anwenderdefinierte Liste von Datensätzen

Eine anwenderdefinierte Liste können Sie im Vulnerability Manager Workspaceerstellen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie das **Listensymbol** aus, und klicken Sie auf **Meine Listen**.
3. Wählen Sie **Neue Liste**aus.
4. Klicken Sie im Modal Neue Liste **auf Von vorhandener beginnen**, und suchen Sie in der Liste Listenauswahl nach einer vorhandenen Liste, die Sie als Vorlage verwenden können.
5. Bearbeiten Sie den Listennamen.
6. Fügen Sie Filter hinzu.
   Beispielsweise können Sie eine Liste der aktiven Datensätze für einen bestimmten Scanner erstellen, den Sie auf erneute Scans überwachen möchten. Sie können die folgenden Filter verwenden: „Aktiv“ ist „true“und „Quelle enthält (Name Ihres Scanners)“.
7. Bearbeiten Sie die Spalten, die in Ihrer Liste angezeigt werden sollen.
8. Klicken Sie auf **Erstellen**.
   Ihre neue Liste wird angezeigt.
9. Alternativ klicken Sie auf **Selbst erstellen**, geben Sie einen Namen ein und wählen Sie **Quelle auswählen**.
10. Beginnen Sie mit der Eingabe in dem Feld, und wählen Sie aus den Quellen aus, die für Ihre neue Liste angezeigt werden.
11. Klicken Sie auf **Erstellen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihre neue Liste wird angezeigt.

Hinweis:
Wenn Sie das Listenmodul verlassen, entspricht die Liste, die beim Beenden angezeigt wird, der Liste, die Sie bei der Rückkehr sehen.

12. Um eine Liste zu löschen, klicken Sie bei angezeigter Liste auf das Zahnradsymbol oben rechts auf der Seite.

Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Manager Workspace

Ab v25.0.4 von Vulnerability Responsekönnen Sie Korrekturaufgaben manuell aus den Listen der angreifbaren Host-Elemente, angreifbaren Anwendungselemente, Container-angreifbaren Elemente und Konfigurationstestergebnisse auf der Listenseite von Vulnerability Manager Workspaceerstellen. Sie können Korrekturaufgaben auch aus den Drilldown-Listen erstellen, die angezeigt werden, wenn Sie auf die Visualisierungen auf der Homepage klicken.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.write_all, sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_write_all oder sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs)
- sn_vul_container.write_all, sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.write oder sn_vulc.admin für Konfigurationstestergebnisse (Configuration Test Results, TRs)

Warum und wann dieser Vorgang ausgeführt wird
Die manuelle Erstellung von Korrekturaufgaben (RTs) in Vulnerability Manager Workspace bietet eine präzise Kontrolle über das Management von Korrekturaufgaben, indem Sie es Ihnen ermöglichen, Datensätze (VITs, CVITs, AVITs oder TRs) dynamisch in Echtzeit in Korrekturaufgaben zu gruppieren.

Sie können eine Korrekturaufgabe manuell erstellen, wenn Sie Folgendes tun möchten:

- angreifbare Elemente nach etwas anderem als den Kriterien für Regeln für Korrekturaufgaben zu gruppieren. Sie können beispielsweise Korrekturaufgaben für einen bestimmten Manager oder für aktive, neue Exploits wie Ransomware erstellen, die verschiedene Schwachstellen enthalten.
- nicht gruppierte Datensätze gruppieren.
- Regeln für Korrekturaufgaben sind inaktiv.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**.
2. Öffnen Sie auf der Listenseite die Liste **Aktiv** oder **Alle** in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Anwendungselemente
   - Angreifbare Container-Elemente
   - Konfigurationstestergebnisse

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Aktivieren Sie das Kontrollkästchen der Datensätze, die Sie aktualisieren möchten, und wählen Sie dann im Modal „Korrekturaufgabe erstellen“ im Feld „Datensatzauswahl“ die Option Ausgewählte Elemente aus.
4. Wählen Sie **Korrekturaufgabe erstellen aus**.
5. Füllen Sie im Modal „Korrekturaufgabe erstellen“ die folgenden Details aus.

Modal „Korrekturaufgabe erstellen“.

Feld	Beschreibung
Datensatzauswahl	○ **Ausgewählte Elemente**: Aktualisiert nur die ausgewählten Datensätze. ○ **Alle Elemente**: Aktualisiert alle Datensätze in der Liste.
Kurzbeschreibung	Kurze Notiz zu den Korrekturaufgaben.
Gruppierungskriterien	Die Auswahlmöglichkeiten lauten wie folgt: ○ **Zuweisungsgruppe**: Datensätze mit derselben Zuweisungsgruppe werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Konfigurationselement**: Datensätze mit derselben Zuweisungsgruppe und demselben Konfigurationselement werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Schwachstelle**: Datensätze mit derselben Zuweisungsgruppe und Schwachstelle werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Risikobewertung**: Datensätze mit derselben Zuweisungsgruppe und Risikobewertung werden in einer Korrekturaufgabe gruppiert.
Datensätze in anderen Korrekturaufgaben verwalten	Die Auswahlmöglichkeiten lauten wie folgt: ○ **Datensätze für neue Korrekturaufgaben überspringen**: Für die Datensätze, die Teil anderer Korrekturaufgaben sind, wird keine Aktion ausgeführt. ○ **Zu neuen Korrekturaufgaben verschieben**: Datensätze, die Teil anderer Korrekturaufgaben sind, werden zu neuen Korrekturaufgaben übertragen. ○ **Sowohl in aktuellen als auch in neuen Korrekturaufgaben beibehalten**: Datensätze, die Teil anderer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Korrekturaufgaben sind, werden sowohl in alten als auch in neuen Korrekturaufgaben aufbewahrt.

6. Wählen Sie **Korrekturaufgabe erstellen aus**.

Ergebnisse

Korrekturaufgaben werden auf Grundlage der Gruppierungskriterien erstellt. An die Korrekturbesitzer in der Zuweisungsgruppe wird eine E-Mail-Benachrichtigung gesendet, in der sie darüber informiert werden, dass eine Korrekturaufgabe erstellt und ihrer Gruppe zugewiesen wurde. Beispiele dafür, wie Korrekturaufgaben basierend auf den Gruppierungskriterien erstellt werden, finden Sie unter Beispiele für die Erstellung von Korrekturaufgaben in Vulnerability Manager Workspace und IT Remediation Workspace.

Aktivieren oder deaktivieren Sie den Import von Testergebnissen für eine Qualys -Testgruppe

Ab v23.0 von Vulnerability Responsesteuern Sie den Import der Testergebnisse für die Tests in einer Testgruppe Qualys mithilfe der Schaltfläche **Import aktivieren/deaktivieren**, die in der Datensatzansicht der Testgruppe verfügbar ist.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Listen**.
2. Öffnen Sie in den Bibliotheken unter der Liste Testgruppen die Testgruppe Qualys in der Datensatzansicht.
3. Deaktivieren Sie den Import der Testergebnisse, die einer Qualys -Testgruppe zugeordnet sind, indem Sie auf die Schaltfläche **Import deaktivieren** klicken.
   Aus der bevorstehenden Datenerfassung werden die Testergebnisse nicht für die Testgruppe Qualys importiert.
   Der Wert im Feld **Ist Import deaktiviert** ändert sich in *wahr*.
4. **Wahlweise:** Aktivieren Sie den Import der Testergebnisse, indem Sie auf die Schaltfläche **Import aktivieren** klicken.

Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace

Genehmigen Sie Anforderungen, die von Korrekturbesitzern übermittelt werden, oder lehnen Sie sie ab.

Vorbereitungen

Erforderliche Rollen:

Für verschiedene Genehmigungsanforderungen sind Genehmigerrollen erforderlich

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
Falsch positive Genehmigungen	Eins	• Granulare Rolle „sn_vul.false_positive_approver“ für angreifbare Elemente (VITs).	-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für verschiedene Genehmigungsanforderungen sind Genehmigerrollen erforderlich (Fortsetzung)

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
		• Rolle „sn_vul.app_false_positive_approver“ für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs) • Rolle „sn_vul_container.false_positive_approver“ für angreifbare Container-Elemente (CVITs) • sn_vulc.false_positive_approver für Konfigurationstestergebnisse Oder Genehmiger müssen in der Anwendergruppe „Falsch positive Genehmiger“ sein.	
Ausnahmegenehmigungen (Zurückstellungen)	Zwei	• In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich • In der Gruppe „Genehmiger – Ebene 2“ ist ein Genehmiger erforderlich	Eine Ausnahmeanforderung für einen Datensatz oder eine Korrekturaufgabe wird mithilfe eines standardmäßigen, zweistufigen Genehmigungsworkflows genehmigt. Die Ausnahmeanforderung erfordert zwei Ebenen von Genehmigern. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der zweiten Ebene gesendet und ist dann in der Warteschlange des Genehmigers 2 sichtbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für verschiedene Genehmigungsanforderungen sind Genehmigerrollen erforderlich (Fortsetzung)

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
Heben Sie die Zuweisung von Genehmigungen auf	Ein Genehmiger in der Gruppe „Genehmiger – Ebene 1“ ist erforderlich	• sn_vul.unassign_appr für AVITs und VITs • sn_vul_container.unas für CVITs • sn_vulc.unassign_app für Konfigurationsproble (CIs)	**Hinweis:** Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt, und es wird eine Genehmigungsgruppe zum Aufheben der Zuweisung erstellt. Anwender (Genehmiger „Zuweisung aufheben“ – Ebene 1) dieser Gruppe können die Anforderung genehmigen. Diese Gruppe enthält standardmäßig die Genehmiger-Rolle zum Aufheben der Zuweisung, sn_vul.unassign_approver. Sie können eine neue Gruppe erstellen oder ändern und die Genehmigungskonfiguration aktualisieren. Um Genehmigungsregeln zu konfigurieren, navigieren Sie zum entsprechenden Modul Genehmigungsregeln, wählen Sie eine der folgenden Genehmigungsregeln aus, und navigieren Sie zur Genehmigungskonfiguration auf der Registerkarte **Genehmigungskonfigurationen** : • *Vulnerable item field change request* für ein angreifbares Element. • *Vulnerability*

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc. in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für verschiedene Genehmigungsanforderungen sind Genehmigerrollen erforderlich (Fortsetzung)

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
Risikominderungs-Genehmigungen	Zwei	• In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich • In der Gruppe „Genehmiger – Ebene 2“ ist ein Genehmiger erforderlich	Der Genehmigungs-Flow für die Risikominderung entspricht den Ausnahmegenehmigungen (Zurückstellungen).

Unter Vulnerability Response Personae und granulare Rollen und Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu finden Sie weitere Informationen über das Zuweisen von Persona-Rollen zu Benutzern und von Benutzern zu Gruppen.

Hinweis:
Fügen Sie den Genehmigungsgruppen Benutzer hinzu, bevor Sie Genehmigungsanforderungen übermitteln. Wenn Sie Anforderungen erstellen, bevor Sie den Genehmigungsgruppen Benutzer hinzufügen, sind sie für Benutzer mit Genehmigungsberechtigungen möglicherweise nicht sichtbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
   Wenn ein Genehmiger keinen Zugriff auf den -Arbeitsbereich hat, können Genehmigungen unter verarbeitet werden **Vulnerability Response** > **Meine Genehmigungen** in der klassischen Umgebung.
2. Wählen Sie das Listenansichtssymbol ( ).
   Die Listenseite wird angezeigt.
3. Wählen Sie in der gefilterten Liste Genehmigungen die **Option Mir zugewiesen aus**.
4. Suchen Sie eine Anforderung, die Sie verarbeiten möchten, und wählen Sie dann den Link in der Spalte Status.
   Der Datensatz für die Sicherheitsrisikostatus-Change-Genehmigung (VCA#) wird angezeigt.
5. Wählen Sie eine der folgenden Optionen aus, um die Anforderung zu genehmigen oder abzulehnen.

Richten Sie E-Mail-Benachrichtigungen in den -Arbeitsbereichen Vulnerability Response ein

Identifizieren Sie Benutzer für automatische E-Mail-Erinnerungen, die an Benutzer in der Benutzergruppe Korrekturbesitzer gesendet werden.

Vorbereitungen
Erforderliche Rolle: Administrator

Diese Funktion generiert automatisch einen E-Mail-Digest für Benutzer in der Benutzergruppe „Korrekturbesitzer“. Fügen Sie alle Anwender hinzu, die E-Mail-Benachrichtigungen erhalten möchten, wie in Verwenden Sie den E-Mail-Digest in den Vulnerability Response-Arbeitsbereichenbeschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergewissern Sie sich, dass für Benutzer eine aktive E-Mail-Adresse in ihrem Benutzerdatensatz eingegeben wurde und dass Sie sie der Benutzergruppe „Korrekturbesitzer“ hinzugefügt haben.

Wenn Sie die Zustellhäufigkeit, den Tag oder die Uhrzeit der E-Mails ändern oder die Funktion deaktivieren möchten, gehen Sie wie folgt vor.

Prozedur

1. Navigieren zu **Alle** > **Geplante Aufgaben**.
2. Suchen Sie den **Korrektur-Digest generieren** und klicken Sie darauf, um den Datensatz zu öffnen.

   Möglicherweise möchten Sie die Standardeinstellungen für die Felder beibehalten, bis Sie überprüft haben, ob Benachrichtigungen gesendet werden. Standardmäßig werden E-Mails wöchentlich am Montagvormittag um 9:00 Uhr in der Zeitzone der Instanz gesendet, die den Auftrag ausführt.
3. Ändern Sie die Felder im Formular.
   Weitere Informationen zu den Formularfeldern finden Sie unterGenerieren Sie Korrektur-Digest-Formularfelder.
4. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme

Falls Sie verifiziert haben, dass alle zuvor aufgeführten Informationen korrekt sind, und Sie Anwender in der Anwendergruppe „Korrekturbesitzer“ haben, die E-Mails jedoch nicht wie erwartet gesendet werden, überprüfen Sie, ob Kanäle für den Empfang von E-Mail-Benachrichtigungen aktiviert sind. Weitere Informationen finden Sie unter Create notification channels .

Angreifbare Elemente und Testergebnisse werden in korrigiert Vulnerability Manager Workspace

In Vulnerability Manager Workspacekönnen Sie angreifbare Elemente und Testergebnisse in einem Überwachungsthema korrigieren, indem Sie eine Bedingung definieren, und Sie können ihren Korrekturfortschritt verfolgen, indem Sie Korrekturmaßnahmen erstellen.

Massenbearbeitung in verwenden Vulnerability Manager Workspace

In Vulnerability Manager Workspacekönnen Sie den Status der Datensätze aktualisieren, Ausnahmen und falsch positive Meldungen anfordern und Datensätze mithilfe der Massenbearbeitungsfunktion gleichzeitig mehreren angreifbaren Elementen (VITs, AVITs oder CVITs) zuweisen.

Die Massenbearbeitungsfunktion ist verfügbar für:

- Host angreifbare Elemente (VITs) ab v21.0 von Vulnerability Response.
- angreifbare Elemente in Anwendungen (AVITs) und angreifbare Elemente in Containern (CVITs) ab v22.0 von Vulnerability Response.
- -Testergebnisse ab v23.0 von Vulnerability Response.

Massenstatus von Datensätzen in aktualisieren Vulnerability Manager Workspace

Aktualisieren Sie den Status mehrerer Datensätze (VITs, AVITs oder CVITs) gleichzeitig entsprechend ihrem Korrekturfortschritt mithilfe der Massenbearbeitungsfunktion in Vulnerability Manager Workspace.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente
- sn_vul.app_sec_manager für angreifbare Anwendungselemente
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**.
2. Öffnen Sie auf der Listenseite die Liste Aktiv oder Alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld **„Datensatzauswahl“** verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option **Alle angreifbaren Elemente, die dem Filter entsprechen** im Feld **Datensatzauswahl** verwenden möchten.
4. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
5. Füllen Sie im Modal „Massenbearbeitung“ die folgenden Felder aus, um den Status der Datensätze zu aktualisieren.

Modale Felder zur Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren und dann die gewünschte Korrekturaufgabe im Feld **Korrekturaufgabe** auswählen möchten. ○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im Feld **Schwachstelleneintrag** aus. **Hinweis:** Datensätze mit ungültigem CI oder stillgelegtem CI werden nicht aktualisiert.
Status	Change für den **Status** im Datensatz. Die Auswahlmöglichkeiten lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Nicht aktualisieren ○ Öffnen ○ Wird untersucht ○ Warten auf Implementierung ○ Zurückgestellt Weitere Informationen finden Sie unter Massenausnahme im Arbeitsbereich des Schwachstellenmanagers anfordern. ○ Abgeschlossen Weitere Informationen finden Sie unter Massenbearbeitung für falsch positive Werte im Arbeitsbereich des Schwachstellenmanagers ○ Gelöst **Hinweis:** Nur die Datensätze, für die der Statusübergang gültig ist, werden aktualisiert.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Wählen Sie **Bearbeiten**aus.

Ein asynchroner Massenbearbeitungsauftrag aktualisiert die ausgewählten Datensätze.

Massenbearbeitung angreifbarer Host-Elemente mit Patches und Lösungen durchführen

Empfehlen Sie einen Patch oder eine Lösung für mehrere angreifbare Host-Elemente gleichzeitig mithilfe der Massenbearbeitungsfunktion in Vulnerability Manager Workspace.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin und jede Rolle mit der granularen Rolle sn_vul.bulk_edit.

Warum und wann dieser Vorgang ausgeführt wird

Im modalen Fenster Massenbearbeitung können Sie beim Hinzufügen einer bevorzugten Lösung und eines Patch die Zuweisung mehrerer angreifbarer Host-Elemente (Host VITs) aufheben oder diese gleichzeitig einer Zuweisungsgruppe zuweisen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.

   Hinweis: Die ausgewählten Datensätze müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.

2. Öffnen Sie auf der Seite Liste unter Angreifbare Host-Elemente die Liste Aktiv oder Alle.
3. Führen Sie einen der folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld **„Datensatzauswahl“** verwenden möchten.
- Wenden Sie Filter an, wenn Sie die Option **Alle angreifbaren Elemente, die dem Filter entsprechen** im Feld **Datensatzauswahl** verwenden möchten.
- Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld Datensatzauswahl des Modals „Massenbearbeitung“ verwenden möchten.
- Wenden Sie Filter an, wenn Sie die Option **Alle angreifbaren Elemente, die dem Filter entsprechen** im Feld Datensatzauswahl des Modals Massenbearbeitung verwenden möchten.

4. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
5. Füllen Sie im Modal „Massenbearbeitung“ die Felder aus, um einen Patch oder eine Lösung für mehrere angreifbare Host-Elemente zu empfehlen.

Modale Felder zur Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren und dann die gewünschte Korrekturaufgabe im Feld **Korrekturaufgabe** auswählen möchten. ○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im Feld **Schwachstelleneintrag** aus. **Hinweis:** ○ Datensätze mit ungültigem CI oder stillgelegtem CI werden nicht aktualisiert. ○ Nur die Datensätze (VITs) im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung “ werden aktualisiert.
Status	Änderung des **Status** der angreifbaren Host-Elemente. Sie können die bevorzugte Lösung und den Patch nur hinzufügen, wenn Sie die folgenden Status wählen. ○ Nicht aktualisieren ○ Öffnen ○ Wird untersucht ○ Warten auf Implementierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bevorzugte Lösung	Lösung zur Korrektur aller für die Massenbearbeitung ausgewählten angreifbaren Elemente. Wählen Sie den Change für das Feld **Preferred Solution (Bevorzugte Lösung)** im angreifbaren Element aus. Die Auswahlmöglichkeiten stammen aus einer Nachschlageliste der verfügbaren bevorzugten Lösungen für die ausgewählten VITs. **Hinweis:** ◦ Der Satz der verfügbaren bevorzugten Lösungen ist eine Schnittmenge aller potenziellen Lösungen für die Schwachstellen in allen ausgewählten VITs. ◦ Beim Auswählen von **Datensatzauswahl** > **Schwachstelleneintrag** Bei einer Massenbearbeitung werden alle VITs für die Schwachstelle auf die ausgewählte bevorzugte Lösung festgelegt. **Hinweis:** Durch diesen Vorgang wird die **bevorzugte Lösung** nicht auf der Ebene des Schwachstelleneintrags festgelegt. Durch das Festlegen der **bevorzugten Lösung** auf der Ebene des Schwachstelleneintrags wird die **bevorzugte Lösung** für alle neuen VITs in Zukunft festgelegt. Durch die Massenbearbeitung wird nur der aktuelle Satz von VITs geändert. ◦ Eindeutige Schwachstellen, die über die Auswahlkriterien hinweg auf 500 beschränkt sind. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, VITs mit unterschiedlichen Kriterien für die Festlegung der **Lösung Preferred**auszuwählen. ◦ Die Gesamtzahl der Lösungen, die in der Suchliste angezeigt werden können, ist auf 170 beschränkt. Wenn mehr als 170 Lösungen vorhanden sind, wird eine Warnmeldung angezeigt. Der aktualisierte Wert wird in der Listenansicht der angreifbaren Elemente angezeigt.
Bevorzugter Patch	Patch, das auf die Korrektur aller für die Massenbearbeitung ausgewählten Schwachstellenelemente abzielt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ◦ Sie müssen Patch Orchestration installieren, um die Liste der bevorzugten Patches anzuzeigen. ◦ Der Satz der verfügbaren bevorzugten Patches ist eine Schnittmenge aller potenziellen Patches für alle ausgewählten VITs. ◦ Eindeutige Schwachstellen, die über die Auswahlkriterien hinweg auf 500 beschränkt sind. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, werden Sie in einer Warnmeldung aufgefordert, VITs mit unterschiedlichen Kriterien für die Festlegung des **bevorzugten Patch**auszuwählen. ◦ Die Gesamtzahl der Patches, die in der Suchliste angezeigt werden können, ist auf 170 beschränkt. Wenn mehr als 170 Patches vorhanden sind, wird eine Warnmeldung angezeigt.
Zuweisung aufheben	Die Zuweisung aller ausgewählten Elemente wird für die Zuweisungsgruppe und den Korrekturbesitzer aufgehoben. **Hinweis:** ◦ Dieses Feld wird angezeigt, wenn Sie als Status Nicht aktualisieren auswählen. ◦ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt, die zur Genehmigung gesendet wird. Weitere Informationen finden Sie unter Entfernen Sie Zuweisungen für angreifbare Host-Elemente massenweise
Zuweisungsgruppe	Zuweisungsgruppe für die Datensätze. Alle aktiven Zuweisungsgruppen werden in diesem Feld angezeigt. **Hinweis:** Dieses Feld wird deaktiviert, wenn Sie das Kontrollkästchen Zuweisung aufheben aktivieren.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Wählen Sie **Bearbeiten**.

Ergebnisse

Eine asynchrone Massenbearbeitungsaufgabe aktualisiert die ausgewählten angreifbaren Host-Elemente (VITs). Die bevorzugte Lösung und der Patch werden den relevanten angreifbaren Elementen des Hosts (VITs) hinzugefügt. Öffnen Sie ein angreifbares Host-Element, und zeigen Sie die bevorzugte Lösung und den Patch im Abschnitt „Nachbesserung“ der Registerkarte Details an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze einer Zuweisungsgruppe massenweise zuweisen

Weisen Sie einer Zuweisungsgruppe mehrere Datensätze (VITs, AVITs, CVITs oder TRs) gleichzeitig zu, indem Sie die Massenbearbeitungsfunktion in Vulnerability Manager Workspaceverwenden.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**.
2. Öffnen Sie auf der Listenseite die Liste Aktiv oder Alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
   - Konfigurationstestergebnisse
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld Datensatzauswahl verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option **Alle Datensätze, die der Filteroption entsprechen** im Feld Datensatzauswahl verwenden möchten.
4. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
5. Füllen Sie die Felder des Formulars aus, um die Datensätze einer Zuweisungsgruppe zuzuweisen.

Modale Felder zur Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ *Nur ausgewählte Elemente*: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die Sie mit dem Kontrollkästchen ausgewählt haben. ○ *Alle Datensätze, die dem Filter entsprechen*: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ *Korrekturaufgabe*: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe im Feld **Korrekturaufgabe** aus. ○ *Schwachstelleneintrag*: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für eine Schwachstelleoder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	spezifisch sind, und wählen Sie dann ein CVE oder TPE im Feld **Schwachstelleneintrag** aus. **Hinweis:** Dieses Feld wird für angreifbare Host-Elemente, angreifbare Anwendungselemente und angreifbare Container-Elemente angezeigt. ○ *Konfigurationstest*: Wählen Sie diese Option aus, wenn Sie die für einen Test spezifischen Testergebnisse aktualisieren und dann einen Test im Feld **Konfigurationstest** auswählen möchten. **Hinweis:** Diese Option wird nur für Konfigurationstestergebnisse angezeigt. **Hinweis:** ○ Datensätze mit ungültigem CI oder stillgelegtem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „Wird untersucht“, „Warten auf Implementierung“ oder „Zurückgestellt“ werden aktualisiert.
Zuweisungsgruppe	Zuweisungsgruppe für die Datensätze. Alle aktiven Zuweisungsgruppen werden in diesem Feld angezeigt. **Hinweis:** Dieses Feld wird deaktiviert, wenn Sie das Kontrollkästchen Aufheben der Zuweisung für VITsaktivieren.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie **auf Bearbeiten**.

Ergebnisse
Öffnen Sie einen Datensatz, für den Sie die Zuweisungsgruppe aktualisiert haben, und navigieren Sie zur Registerkarte Übersicht. Die Benutzergruppe, der der Datensatz zugewiesen ist, wird im Feld **Zuweisungsgruppe** angezeigt.

Entfernen Sie Zuweisungen für angreifbare Host-Elemente massenweise

Entfernen Sie sich oder Ihre Gruppen aus den Feldern **„Zugewiesen an“** und **„Zuweisungsgruppe“** für angreifbare Elemente des Hosts (VITs) oder Korrekturaufgaben (VUL), wenn Sie feststellen, dass die Datensätze nicht in Ihrem Korrekturbereich liegen oder wenn Sie der Meinung sind, dass Datensätze falsch erstellt wurden Ihnen oder Ihren Gruppen zugewiesen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_analyst und sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Funktion „Zuweisung aufheben“ gilt für Datensätze in einem anderen Status als „Geschlossen“ oder „Gelöst“. Wenn Sie Zuweisungen für angreifbare Host-Elemente mithilfe der Massenbearbeitungsfunktion entfernen, werden nur relevante Datensätze aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Öffnen Sie auf der Seite Liste unter Angreifbare Host-Elemente die Liste Aktiv oder Alle.
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld „Datensatzauswahl“ verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option **Alle angreifbaren Elemente, die dem Filter entsprechen** im Feld Datensatzauswahl verwenden möchten.
4. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
5. Füllen Sie die Felder im Formular aus, um Massenzuweisungen zu entfernen.

Modale Felder zur Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren und dann die gewünschte Korrekturaufgabe im Feld **Korrekturaufgabe** auswählen möchten. ○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im Feld **Schwachstelleneintrag** aus. **Hinweis:** ○ Datensätze mit ungültigem CI oder stillgelegtem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „Wird untersucht“, „Warten auf Implementierung“ oder „Zurückgestellt“ werden aktualisiert.
Status	Wählen Sie als Status Nicht aktualisieren aus.
Zuweisung aufheben	Die Zuweisung aller ausgewählten angreifbaren Elemente wird zur Zuweisungsgruppe und zum Korrekturbesitzer aufgehoben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Dieses Feld wird angezeigt, wenn Sie als Status Nicht aktualisieren auswählen. ○ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt, die zur Genehmigung gesendet wird.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie **auf Bearbeiten**.
   Es wird eine Korrekturaufgabe mit den ausgewählten angreifbaren Host-Elementen (VITs) erstellt.

   Ihre Anforderung wird zur Genehmigung übermittelt, und der Genehmiger erhält eine E-Mail-Benachrichtigung zu Ihrer Anforderung.

   Der Status der angreifbaren Elemente des Hosts (VITs) und der Korrekturaufgabe wechselt zu In Überprüfung. Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, werden die Felder**Zugewiesen an** und **Zuweisungsgruppe** für alle zugehörigen VITs nach Genehmigung Ihrer Anforderung ebenfalls gelöscht.

Ergebnisse
Navigieren Sie im Arbeitsbereich des Schwachstellenmanagers auf der Seite Liste zu **Ausnahmeanforderungen** > **Alle** und öffnen Sie den entsprechenden Status-Change-Genehmigungsdatensatz (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Die Felder **„Zugewiesen an“** und **„Zuweisungsgruppe“** aller angreifbaren Host-Elemente werden gelöscht.
Abgelehnt	Die Felder **„Zugewiesen an“** und **„Zuweisungsgruppe“** aller angreifbaren Hostelemente werden nicht aktualisiert.

Im **Aktivitätenstrom** eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow Ihrer Anforderung anzeigen.

Massenausnahme im Arbeitsbereich des Schwachstellenmanagers anfordern

Fordern Sie eine Ausnahme für mehrere Datensätze (VITs, AVITs, CVITs oder TRs) an, indem Sie die Massenbearbeitungsfunktion verwenden, anstatt jeden Datensatz manuell auszuwählen.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie aus dem Modal Massenbearbeitung eine Ausnahme für einen oder mehrere Datensätze anfordern, wird eine Korrekturaufgabe mit den ausgewählten Datensätzen erstellt.

Hinweis:
Die angreifbaren Elemente in der Anwendung (Application Vulnerable Items, AVITs) aus den Scannern, für die der Parameter **„Ausnahmen in ServiceNow verwalten"** auf „falsch" festgelegt ist, werden nicht aktualisiert.

- Wenn Sie AVITs aus verschiedenen Scannern auswählen, von denen einige den Parameter „ **Ausnahmen in ServiceNow verwalten** " auf „wahr" und andere auf „falsch" festgelegt haben, werden die AVITs, die mit den Scannern verknüpft sind, bei denen der Parameter **„Ausnahmen in ServiceNow verwalten** " auf „falsch" festgelegt ist, nicht aktualisiert.
- Wenn Sie AVITs nur aus den Scannern auswählen, für die der Parameter **Ausnahmen in ServiceNow verwalten** auf falsch festgelegt ist, wird die Option *Zurückstellen* im Feld **Status** im Modal Massenbearbeitung nicht angezeigt.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Öffnen Sie auf der Seite Liste in einer der folgenden Listen die Liste Aktiv oder Alle:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
   - Konfigurationstestergebnisse
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option *Nur ausgewählte Elemente* im Feld Datensatzauswahl verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option *Alle Datensätze, die der Filteroption entsprechen* im Feld Datensatzauswahl verwenden möchten.
4. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
5. Füllen Sie die folgenden Felder des Formulars aus, um eine Ausnahme für mehrere Datensätze (VITs, AVITs, CVITs oder TRs) gleichzeitig anzufordern.

Modale Felder zur Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ *Nur ausgewählte Elemente*: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die Sie mit dem Kontrollkästchen ausgewählt haben. ○ *Alle Datensätze, die dem Filter entsprechen*: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ *Korrekturaufgabe*: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe im Feld **Korrekturaufgabe** aus. ○ *Schwachstelleneintrag*: Wählen Sie diese Option aus, wenn Sie die für eine Schwachstelle spezifischen Datensätze aktualisieren möchten, und wählen Sie dann im Feld **Schwachstelleneintrag** ein CVE oder TPE aus. **Hinweis:** Dieses Feld wird für angreifbare Host-Elemente, angreifbare Anwendungselemente und angreifbare Container-Elemente angezeigt. ○ *Konfigurationstest*: Wählen Sie diese Option aus, wenn Sie die für einen Test spezifischen Testergebnisse aktualisieren und dann einen Test im Feld **Konfigurationstest** auswählen möchten. **Hinweis:** Diese Option wird nur für Konfigurationstestergebnisse angezeigt. **Hinweis:** ○ Datensätze mit ungültigem CI oder stillgelegtem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ werden aktualisiert.
Status	Wählen Sie den Status *Zurückgestellt* aus, um eine Ausnahme für die ausgewählten Datensätze anzufordern. **Hinweis:** ○ Wenn Sie diese Option auswählen, werden die Felder Grund, Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt. ○ Wenn Sie Datensätze zurückstellen, wird eine Korrekturaufgabe erstellt, und diese Aufgabe wird zur Genehmigung gesendet.
Grund	Grund für das Zurückstellen von Datensätzen: ○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Risiko akzeptiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Ausgleichende Steuerung vorhanden ○ Sonstige **Hinweis:** Das Feld **Grund** wird angezeigt, wenn Sie als Status Zurückgestellt wählen.
Kurzbeschreibung	Kurze Notiz, in der die Gründe für die Zurückstellungsanforderung beschrieben werden. Diese Informationen werden im Feld **Beschreibung** der Korrekturaufgabe angezeigt, die für eine Zurückstellungsanforderung erstellt wird. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie als Status Zurückgestellt und Geschlossen – Falsch positiv auswählen.
Bis	Datum, bis zu dem der Datensatz zurückgestellt bleibt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie als Status Zurückgestellt auswählen.
Zusätzliche Information	Alle weiteren erforderlichen Informationen. Diese Informationen werden im Feld Zusätzliche Informationen auf der Registerkarte Übersicht der Korrekturaufgabe angezeigt, die für Zurückstellungsanforderungen und geschlossene falsch positive Anforderungen erstellt wird. Wenn Ihre Zurückstellungsanforderung genehmigt wird, werden diese zusätzlichen Informationen als Zurückstellungsnotizen für VIT und Korrekturaufgabe angezeigt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie als Status Zurückgestellt und Geschlossen – Falsch positiv auswählen.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie **auf Bearbeiten**.
7. Beantworten Sie im Modal „Fragebogen ausfüllen“ die Fragen, und klicken Sie auf **Absenden**.

   Es wird eine Korrekturaufgabe erstellt, die die von Ihnen ausgewählten Datensätze enthält. Die Anforderung wird zur Genehmigung übermittelt, und der Status der Datensätze ändert sich in Wird überprüft.

   Hinweis:
   Das Modal **„Fragebogen ausfüllen“** wird nur angezeigt, wenn der Fragebogen im Formular „Ausnahmeverwaltung“ für Ausnahmeanforderungen aktiviert ist. Weitere Informationen zum Konfigurieren eines Fragebogens für Ausnahmeanforderungen finden Sie unter Konfigurieren Sie die Ausnahmeverwaltung für Vulnerability Response, Konfigurieren Sie die Ausnahmeverwaltung für Application Vulnerability Responseund Konfigurieren Sie die Ausnahmeverwaltung für Container Vulnerability Responseund Konfigurations-Compliance Übersicht über Ausnahmeverwaltung.

   Der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

Ergebnisse
Navigieren Sie im Arbeitsbereich des Schwachstellenmanagers auf der Seite Liste zu **Ausnahmen** > **Alle**, öffnen Sie den entsprechenden Status-Change-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigungsdatensatz (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Der Status der Korrekturaufgabe wechselt in „Zurückgestellt“ mit dem angegebenen Grund als Substatus. Der Status und der Grund werden auf die Datensätze heruntergerollt.
Abgelehnt	Der Status der Korrekturaufgabe und ihrer Datensätze ändert sich nicht.

Im **Aktivitätenstrom** eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow Ihrer Anforderung anzeigen.

Massenbearbeitung für falsch positive Werte im Arbeitsbereich des Schwachstellenmanagers

Markieren Sie einen oder mehrere Datensätze (VITs, AVITs, CVITs oder TRs) gleichzeitig als falsch positiv, indem Sie die Massenbearbeitungsfunktion im Arbeitsbereich des Schwachstellenmanagers verwenden, anstatt jedes Element manuell auszuwählen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie im modalen Fenster Massenbearbeitung eine falsch positive Anforderung für einen oder mehrere Datensätze stellen, wird eine Korrekturaufgabe mit den ausgewählten Datensätzen erstellt.

Hinweis:

Wenn Sie mit der Massenbearbeitungsfunktion eine falsch positive Anforderung für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs) stellen, werden die AVITs von den Scannern, für die der Parameter **„Falsch positive Elemente mit ServiceNow verwalten“** auf „falsch“ festgelegt ist, nicht aktualisiert.

- Wenn Sie AVITs aus verschiedenen Scannern auswählen, von denen einige **„Falsch positive Werte mit ServiceNow-Parameter verwalten** “ auf „wahr“ und andere auf „falsch“ festgelegt ist, werden die AVITs, die mit den Scannern verknüpft sind, für die **„Falsch positive Werte mit ServiceNow-Parameter verwalten“** auf „falsch“ festgelegt ist, nicht aktualisiert.
- Wenn Sie AVITs nur aus den Scannern auswählen, für die der Parameter **Manage False positive with Servicenow (Falsch positiv mit ServiceNow-** Parameter verwalten) auf false festgelegt ist, wird die Option *Falsch positiv (Falsch positiv)* im Modal „Massenbearbeitung“ nicht im Feld **Grund** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**.

   Hinweis:
   Die ausgewählten Datensätze müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.

2. Öffnen Sie auf der Listenseite die Liste Aktiv oder Alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
   - Konfigurationstestergebnisse
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option *Nur ausgewählte Elemente* im Feld **Datensatzauswahl** verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option *Alle Datensätze, die der Filteroption entsprechen* im Feld **Datensatzauswahl** verwenden möchten.
4. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
5. Füllen Sie die Felder des Formulars aus, um falsch positive Werte für mehrere Datensätze anzufordern.

Modale Felder zur Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ *Nur ausgewählte Elemente*: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die Sie mit dem Kontrollkästchen ausgewählt haben. ○ *Alle Datensätze, die dem Filter entsprechen*: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ *Korrekturaufgabe*: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe im Feld **Korrekturaufgabe** aus. ○ *Schwachstelleneintrag*: Wählen Sie diese Option aus, wenn Sie die für eine Schwachstelle spezifischen Datensätze aktualisieren möchten, und wählen Sie dann im Feld **Schwachstelleneintrag** ein CVE oder TPE aus. **Hinweis:** Dieses Feld wird für angreifbare Host-Elemente, angreifbare Anwendungselemente und angreifbare Container-Elemente angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ *Konfigurationstest*: Wählen Sie diese Option aus, wenn Sie die für einen Test spezifischen Testergebnisse aktualisieren und dann einen Test im Feld **Konfigurationstest** auswählen möchten. **Hinweis:** Diese Option wird nur für Konfigurationstestergebnisse angezeigt. **Hinweis:** ○ Datensätze mit ungültigem CI oder stillgelegtem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ werden aktualisiert.
Status	Wählen Sie den Status **Geschlossen** aus.
Grund	Wählen Sie als Grund Falsch positiv aus. **Hinweis:** ○ Wenn Sie diese Option auswählen, werden die Felder Kurzbeschreibung und Zusätzliche Informationen angezeigt. ○ Eine Korrekturaufgabe wird erstellt, wenn Sie die Datensätze als Falsch positiv markieren und diese Aufgabe zur Genehmigung gesendet wird. **Hinweis:** Das Feld **Grund** wird angezeigt, wenn Sie für den Status Zurückgestellt oder Geschlossen auswählen.
Kurzbeschreibung	Kurze Notiz, in der die Gründe für die Anforderung „Als falsch positiv geschlossen“ beschrieben werden. Diese Informationen werden im Feld **„Beschreibung“** der Korrekturaufgabe angezeigt, die für eine positive Anforderung des Typs „Falsch geschlossen“ erstellt wird. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als „Zurückgestellt“ oder „Geschlossen – Falsch positiv“ auswählen.
Zusätzliche Information	Alle weiteren erforderlichen Informationen. Diese Informationen werden im Feld „Zusätzliche Informationen“ auf der Registerkarte „Übersicht“ der Korrekturaufgabe angezeigt, die für die positive Anforderung „Als falsch geschlossen“ erstellt wird. Wenn Ihre falsch positive Anforderung genehmigt wird, werden diese zusätzlichen Informationen als Notizen sowohl für die VIT als auch für die Korrekturaufgabe angezeigt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als „Zurückgestellt“ oder „Geschlossen – Falsch positiv“ auswählen.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie **auf Bearbeiten**.
7. Beantworten Sie im Modal „Fragebogen ausfüllen“ die Fragen, und wählen Sie **Absenden**aus.
   Mit den ausgewählten Datensätzen wird eine Korrekturaufgabe erstellt. Ihre Anforderung wird zur Genehmigung übermittelt, und der Status der Korrekturaufgabe ändert sich in „Wird überprüft“.

Hinweis:
Das Modal **„Fragebogen ausfüllen“** wird nur angezeigt, wenn der Fragebogen im Formular „Ausnahmeverwaltung“ für falsch positive Anforderungen aktiviert ist. Weitere Informationen zum Konfigurieren eines Fragebogens für falsch positive Anforderungen finden Sie unter Konfigurieren Sie die Ausnahmeverwaltung für Vulnerability Response, Konfigurieren Sie die Ausnahmeverwaltung für Application Vulnerability Responseund Konfigurieren Sie die Ausnahmeverwaltung für Container Vulnerability Response.

Der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

Ergebnisse
Navigieren Sie im Arbeitsbereich des Schwachstellenmanagers auf der Seite Liste zu **Ausnahmen** > **Alle**, öffnen Sie den entsprechenden Status-Change-Genehmigungsdatensatz (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Der Status der Korrekturaufgabe geht in „Geschlossen“ über, und der Grund ist „Falsch positiv“. Der Status und der Grund werden auf die Datensätze heruntergerollt.
Abgelehnt	Der Status der Korrekturaufgabe und ihrer Datensätze ändert sich nicht.

Im **Aktivitätenstrom** eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow Ihrer Anforderung anzeigen.

Massenschließung von Datensätzen im Vulnerability Manager Workspace

Schließen Sie mehrere Datensätze (VITs, AVITs oder CVITs) gleichzeitig mit der Massenbearbeitungsfunktion in Vulnerability Manager Workspace.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**.
2. Öffnen Sie auf der Listenseite die Liste Aktiv oder Alle in einer der folgenden Listen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Angreifbare Host-Elemente
- Angreifbare Container-Elemente
- Angreifbare Anwendungselemente

3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option Nur ausgewählte Elemente im Feld **„Datensatzauswahl“** verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option Alle angreifbaren Elemente, die dem Filter entsprechen im Feld **Datensatzauswahl** verwenden möchten.
4. Wählen Sie die Schaltfläche **Massenbearbeitung** aus.
5. Füllen Sie die Felder des Formulars aus, um die ausgewählten Datensätze zu schließen.

Modale Felder zur Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren und dann die gewünschte Korrekturaufgabe im Feld **Korrekturaufgabe** auswählen möchten. ○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im Feld **Schwachstelleneintrag** aus. **Hinweis:** ○ Datensätze mit ungültigem CI oder stillgelegtem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ werden aktualisiert.
Status	Wählen Sie als Status Geschlossen aus.
Grund	Grund für das Schließen von Datensätzen: ○ Falsch positiv **Hinweis:** Wenn Sie diese Option auswählen, um die Datensätze als falsch positiv zu kennzeichnen, werden die Felder Grund, Kurzbeschreibung und Zusätzliche Informationen angezeigt. Weitere Informationen zur Massenbearbeitung für falsch positive Ergebnisse finden Sie unter Massenbearbeitung für falsch positive Werte im Arbeitsbereich des Schwachstellenmanagers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Storniert ○ Behoben **Hinweis:** Die Gründe „Abgebrochen“ und „Behoben“ gelten nicht für CVITs.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie **auf Bearbeiten**.

Ein asynchroner Massenbearbeitungsauftrag aktualisiert die relevanten Datensätze.

Ausnahmen für Korrekturaufgaben und Datensätze in anfordern Vulnerability Manager Workspace

Über Vulnerability Manager Workspacekönnen Schwachstellenmanager und Analysten Ausnahmen und falsch positive Meldungen für eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) und einen Datensatz (VIT, CVIT, AVIT oder CTR) anfordern. Sie können eine Korrekturaufgabe auch aufteilen und Change-Anforderungen erstellen.

Erforderliche Rolle:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für angreifbare Host-Elemente (VITs)
- sn_vul.app_sec_manager für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

In Vulnerability Manager Workspacekönnen Sie für die -Datensätze und Korrekturaufgaben Folgendes ausführen:

- Eine Korrekturaufgabe aufteilen (VUL, AVUL, CVUL und CRG).
- Fordern Sie eine Ausnahme für einen Datensatz (VIT, AVIT oder CVIT) oder eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) an.
- Fordern Sie eine Richtlinienausnahme für Datensätze (VIT, AVIT oder CVIT) oder Korrekturaufgaben (VUL, AVUL, CVUL oder CRG) an.
- Risikominderung für ein angreifbares Host-Element (VIT) und eine Korrekturaufgabe (VUL) anfordern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie eine Change-Anforderung für die Korrekturaufgabe (VUL, CVUL oder CRG).
- Fordern Sie ein falsch positives Ergebnis für den Datensatz (VIT, AVIT oder CVIT) oder die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) an.

Hinweis:
Sie können falsch positive Anforderungen für eine Reihe von Testergebnissen aus einer Korrekturaufgabe (CRG) stellen.

Sie initiieren diese UI-Aktionen aus Datensätzen in Vulnerability Manager Workspaceauf die gleiche Weise, wie Korrekturbesitzer diese Aufgaben in IT Remediation Workspaceausführen.

Weitere Informationen finden Sie in den folgenden Themen:

- Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an
- Fordern Sie eine Ausnahme in an IT Remediation Workspace
- Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an
- Teilen Sie eine Korrekturaufgabe in in IT Remediation Workspace
- Erstellen Sie eine Change-Anforderung im IT Remediation Workspace
- Ausnahme anfordern mit GRC: Richtlinien- und Compliance-Management in IT Remediation Workspace
- Fordern Sie ein falsch positives Ergebnis für eine Reihe von Testergebnissen an

Zugehörige Informationen

Übersicht über Ausnahmeverwaltung

Konfigurations-Compliance Übersicht über Ausnahmeverwaltung

Massenausnahme im Arbeitsbereich des Schwachstellenmanagers anfordern

Massenbearbeitung für falsch positive Werte im Arbeitsbereich des Schwachstellenmanagers

Fordern Sie im Arbeitsbereich des Schwachstellenmanagers eine Erweiterung für ein zurückgestelltes angreifbares Element an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an, bevor das Fälligkeitsdatum für „Zurückgestellt bis“ erreicht wird. Als Besitzer der Korrektur müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch aus der klassischen Umgebung anfordern.

Verwenden Sie das gleiche Verfahren, um eine Erweiterung für ein angreifbares Anwendungselement, ein angreifbares Containerelement, eine Testergebnisgruppe und eine Korrekturaufgabe anzufordern.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereiche des Schwachstellenmanagers**.
2. Wählen Sie Listen aus.
3. Wählen Sie unter Angreifbare Host-Elemente die **Option Alle**aus.
4. Filtern Sie die Liste, indem Sie in der Spalte Status die Option Zurückgestellt auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie ein zurückgestelltes angreifbares Element aus.

> **Hinweis:**
> Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Elements Zurückgestellt ist.

6. Wählen Sie die Schaltfläche **Verlängerung anfordern** aus.
7. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten angreifbaren Elements verlängert werden muss.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

8. Wählen Sie **Verlängerung anfordern**aus.
   Bei der Übermittlung der Anforderung und der anschließenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

> **Hinweis:**
> ○ Die Anforderung durchläuft zwei Genehmigungsebenen.
> ○ Wenn ein zurückgestelltes angreifbares Element erneut erweitert wird, erhöht sich die Anzahl der Verlängerungsrückstellungen im Back-End.

9. Nachdem die Anforderung genehmigt wurde, werden die Hinweise Bis, Grund und Zurückstellung aktualisiert.

Vulnerability Manager Workspace Referenzinformationen

Die folgenden Themen enthalten Links und Referenzinformationen sowie Felddaten für die Formulare und Datensätze in Vulnerability Manager Workspace.

[store-future: BEGIN review]

Umleitung zu Vulnerability Manager Workspace aus dem Menü „Alle“.

Wenn ein Administrator die Systemeigenschaft `sn_vul_cmn_ws.navigate_to_workspace` auf `true`setzt, werden Sie zu Vulnerability Manager Workspace weitergeleitet, sobald Sie im Menü

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle die vordefinierten Filterlinks in den Modulen Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance auswählen.

Umleitung zur Homepage des Vulnerability Manager Workspace

Als Benutzer mit der Rolle sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin, wenn Sie im Modul Angreifbare Elemente die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente**, werden diese Links auf der Homepage von Vulnerability Manager Workspacemit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte Host-Schwachstellen geöffnet:

- Kritisches Risiko
- Ziel verfehlt
- Mehrere Zurückstellungen
- Älter als 90 Tage
- Nicht zugewiesen
- Nicht gruppiert
- Hohes Risiko
- Innerhalb der letzten 90 Tage
- Außer Betrieb genommen
- Ziel rückt näher
- Nutzbar

Als Benutzer mit der Rolle sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin, wenn Sie im Modul Angreifbare Container-Elemente die folgenden vordefinierten Filter-Links auswählen, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**, werden diese Links auf der Homepage von Vulnerability Manager Workspacemit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte Container-Schwachstellen geöffnet:

- Nicht zugewiesen
- Kritisches und hohes Risiko
- Nutzbar
- Ziel rückt näher
- Ziel verfehlt
- Mehrfache Zurückstellung
- Alle

Als Benutzer mit der Rolle sn_vul.app_sec_manager, wenn Sie im Modul Angreifbare Anwendungselemente die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**, werden diese Links auf der Homepage von Vulnerability Manager Workspacemit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte Anwendungsschwachstellen geöffnet:

- Aktiv
- Datum der Korrekturzusage vergangen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mehrfache Zurückstellung
- Nicht zugewiesen
- Alle

Als Benutzer mit der Rolle sn_vulc.admin, wenn Sie im Modul Testergebnisse die folgenden Links für vordefinierte Filter auswählen, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance** > **Testergebnisse**, werden diese Links auf der Homepage von Vulnerability Manager Workspacemit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte Konfigurationstestergebnisse geöffnet:

- Nicht selektierte Testergebnisse
- Offene Testergebnisse
- Ziel rückt näher
- Ziel verfehlt
- Mehrfache Zurückstellung
- Nicht zugewiesen
- Alle

Es wird zur Listenseite von umgeleitet Vulnerability Manager Workspace

Als Benutzer mit der Rolle sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin, wenn Sie im Modul Vulnerability Response die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response**, diese Links werden auf der Listenseite von Vulnerability Manager Workspacegeöffnet:

- Korrekturaufgaben: „Aktiv“, „Mir zugewiesen“, „Meinen Gruppen zugewiesen“ und „Alle“.
- Angreifbare Elemente: „Mir zugewiesen“ und „Meine Gruppen zugewiesen“.
- Bibliotheken – NVD, CWE, Drittanbieter und angreifbare Software
- Lösungen: Alle, Ersatz durch höchste Priorität und Mit angreifbaren Elementen
- Meine Genehmigungen

Als Benutzer mit der Rolle sn_vul_container.vulnerability_analyst oder sn_vul_container.vulnerability_admin, wenn Sie im Modul Container Vulnerability Response die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Container Vulnerability Response**, diese Links werden auf der Listenseite von Vulnerability Manager Workspacegeöffnet:

- Container-Korrekturaufgaben: „Aktiv“, „Mir zugewiesen“, „Meinen Gruppen zugewiesen“ und „Alle“.
- Angreifbare Container-Elemente – Mir zugewiesen und Meinen Gruppen zugewiesen
- Bibliotheken – NVD, CWE und Drittpartei
- Meine Genehmigungen

Als Benutzer mit der Rolle sn_vul.app_sec_manager, wenn Sie im Modul Application Vulnerability Response die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Application Vulnerability Response**, diese Links werden auf der Listenseite von Vulnerability Manager Workspacegeöffnet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Korrekturaufgaben: „Aktiv“, „Mir zugewiesen“, „Meinen Gruppen zugewiesen“ und „Alle“.
- Angreifbare Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Meine Genehmigungen
- Bibliotheken – NVD, CWE und Drittpartei
- Bewertungsanforderungen für Penetrationstests: „Aktiv“, „Alle mir zugewiesen“ und „Meine Gruppen zugewiesen“.
- Penetrationstestergebnisse – Aktiv, Validierung ausstehend, Mir zugewiesen, Meiner Gruppe zugewiesen und Alle

Als Benutzer mit der Rolle sn_vul.app_sec_manager, wenn Sie im Modul Konfigurations-Compliance die folgenden vordefinierten Filter-Links auswählen, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance**, diese Links werden auf der Listenseite von Vulnerability Manager Workspacegeöffnet:

- Korrekturaufgaben: „Meine offenen Aufgaben“, „Alle offenen Aufgaben“, „Mehrere Zurückstellungen“ und „Alle Aufgaben“.
- Tests
- Testgruppen
- Unterstützungsdaten – Autorisierende Quellen und Technologien

[End]

Formularfelder „Überwachungsthema erstellen“.

In der folgenden Tabelle werden die Felder im Formular „Überwachungsthema erstellen“ in Vulnerability Manager Workspacebeschrieben.

Feld	Beschreibung
Name	Name für Ihr Überwachungsthema, z. B. Kritische AEs.
Eigentum von	Der Name des Anwenders, der das Überwachungsthema besitzt.
Anzeigereihenfolge	Geben Sie einen Wert zwischen 100 und 1000 ein. 100 ist der Standardwert. Niedrigere Werte beginnen mit 100 und werden in Listen in aufsteigender Reihenfolge angezeigt.
Verantwortliche Gruppe	Der Name der Gruppe, die das Überwachungsthema besitzt.
Aktiv	Aktivieren oder deaktivieren Sie das Überwachungsthema. Standard ist ausgewählt (Aktiv).
Beobachtungsliste	Fügen Sie Namen von Anwendern hinzu, die Benachrichtigungen erhalten und das Überwachungsthema anzeigen können.
Beschreibung	Text, der Ihr Überwachungsthema beschreibt. Dieser Text wird im Feld Beschreibung angezeigt, wenn Sie eine Korrekturmaßnahme aus diesem Überwachungsthema erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kategorie	Typ des Datensatzes, für den das Überwachungsthema erstellt wird.

Zugehörige Informationen

Erstellen Sie ein Überwachungsthema in Vulnerability Manager Workspace

GRC – Felder des Formulars „Ausnahme anfordern“.

Die folgende Tabelle enthält die Feldbeschreibungen für das Formular „GRC – Ausnahme anfordern“.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Richtlinie	Richtlinie für Schwachstellenmanagement, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von Zurückgestellt in Offen wechselt. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)**, die Sie für die Richtlinie in Richtlinien und Compliance festgelegt haben, nicht überschreiten. Weitere Informationen finden Sie unter Richtlinie erstellen .
Grund	Grund für das Anfordern einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Besitzer der Remediation ausgefüllt werden.

Generieren Sie Korrektur-Digest-Formularfelder

Die folgende Tabelle zeigt die Felder im Formular „Nachbesserungs-Digest generieren“.

Generieren Sie Korrektur-Digest-Felder

Feld	Beschreibung
Aktives Kontrollkästchen	Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie keine E-Mail-Benachrichtigungen senden möchten, deaktivieren Sie dieses Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Generieren Sie Korrektur-Digest-Felder (Fortsetzung)

Feld	Beschreibung
Ausführen	Wöchentlich ist die Standardeinstellung. Wählen Sie eine Option aus der Liste aus.
Tag	Standard ist Montag. Wählen Sie eine Option aus der Liste aus.
Zeit	Legen Sie eine Zeit für die Zustellung der E-Mails fest. Wählen Sie eine Zeitzone aus, wenn Sie eine andere Zeitzone als die Zeitzone verwenden möchten, die von der Instanz verwendet wird, die den Job ausführt.

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Als Korrekturbesitzer können Sie eine Risikominderung für ein angreifbares Host-Element oder eine Korrekturaufgabe anfordern. Und der Schwachstellenmanager oder Analyst kann diese Risikominderungsanforderungen genehmigen.

Weitere Informationen zum Anfordern der Risikominderung und zum Genehmigen der Genehmigung für die Risikominderung finden Sie unter Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an bzw. Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Wenn eine Risikominderungsanforderung genehmigt wird, wird die Risikopunktzahl gemäß dem **gewünschten Wert** (Risikobewertung) im Datensatz „Status Change-Genehmigung“ (VCA#) reduziert. Die höchste Risikopunktzahl der gewünschten Risikobewertung wird dem Datensatz zugewiesen, wenn Ihre Risikominderungsanforderung genehmigt wird. Das folgende Beispiel zeigt, wie Risikopunktzahl und Ursprüngliche Risikopunktzahl aktualisiert werden, wenn Ausgleichssteuerungen angewendet werden. Im folgenden Beispiel werden die standardmäßigen höchsten Risikopunktzahlen der Risikoeinstufungen verwendet.

Auswirkung von Ausgleichssteuerungen auf Risikopunktzahl und ursprüngliche Risikopunktzahl

Szenario	Risikobewertung	Risikopunktzahl	Ursprüngliche Risikopunktzahl (Berechnete Risikopunktzahl)
Daten vor v20.0	2 – Hoch	80	Das Feld ist vor v20.0 nicht verfügbar.
Nach dem Upgrade auf v20.0	2 – Hoch	80	NULL
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 90	1 – Kritisch	90.0	NULL
Wenn Sie Ausgleichssteuerungen anwenden	3 – Mittel	69	90.0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswirkung von Ausgleichssteuerungen auf Risikopunktzahl und ursprüngliche Risikopunktzahl (Fortsetzung)

Szenario	Risikobewertung	Risikopunktzahl	Ursprüngliche Risikopunktzahl (Berechnete Risikopunktzahl)
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 70	3 – Mittel	69	70
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 50	3 – Mittel	50	50
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 80	3 – Mittel	50	80
Wenn Ausgleichssteuerungen am **Bis-Datum für Risikominderung**ablaufen	2 – Hoch	80	NULL

Auswirkung von Ausgleichssteuerungen auf eine Korrekturaufgabe

Wenn Ihre Anforderung zur Risikominderung für eine Korrekturaufgabe genehmigt wird, wirken sich Ausgleichssteuerungen auf die angreifbaren Elemente wie folgt aus:

- Die auf die Korrekturaufgabe angewendeten Ausgleichssteuerungen werden auf die angreifbaren Elemente (außer denen im Status „Geschlossen“) angewendet, deren Risikopunktzahl höher ist als die Risikopunktzahl, die dem **gewünschten Wert** in der Status-Change-Genehmigung einer Korrekturaufgabe entspricht. Die Risikopunktzahl dieser angreifbaren Elemente wird entsprechend dem **gewünschten Wert**reduziert.
- Das **Bis-Datum für die Risikominderung** bleibt für die angreifbaren Elemente, auf die bereits eine Ausgleichssteuerung angewendet wird, unverändert. Es wird nicht mit dem **Bis-Datum für die Risikominderung** der Korrekturaufgabe aktualisiert.
- Das **Bis-Datum für die Risikominderung** wird nur dann auf die angreifbaren Elemente heruntergerollt, wenn zuvor keine Ausgleichssteuerung auf ein angreifbares Element angewendet wurde. Wenn Sie die Ausgleichssteuerungen erneut auf die Korrekturaufgabe anwenden, wird das **Bis-Datum für die Risikominderung** nicht auf die angreifbaren Elemente heruntergerollt, da das vorhandene **Bis-Datum für die Risikominderung** der angreifbaren Elemente Priorität erhält.
- Wenn ein neues angreifbares Element zu einer Korrekturaufgabe hinzugefügt wird, auf die bereits Ausgleichssteuerungen angewendet wurden, wird das Risiko nicht auf das angreifbare Element heruntergerollt.

Auswirkung einer Ausgleichssteuerung auf ein angreifbares Element

Wenn Ihre Anforderung zur Risikominderung für ein angreifbares Element genehmigt wird:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die neue Risikopunktzahl wird im Feld **Risikopunktzahl** angezeigt, und die alte Risikopunktzahl (berechnete Risikopunktzahl) wird in das Feld **Ursprüngliche Risikopunktzahl** verschoben. Diese Änderung gilt bis zu dem Datum, das im Feld **Bis-Datum für Risikominderung** angegeben ist.
- Wenn auf ein angreifbares Element bereits Ausgleichssteuerungen angewendet werden, geschieht während der Erfassung Folgendes:
  - Wenn die berechnete Risikopunktzahl größer als die Risikopunktzahl ist, bleibt die Risikopunktzahl unverändert, und die ursprüngliche Risikopunktzahl wird mit der berechneten Risikopunktzahl aktualisiert.
  - Wenn die berechnete Risikopunktzahl kleiner als die Risikopunktzahl ist, werden sowohl die Risikopunktzahl als auch die ursprüngliche Risikopunktzahl mit der berechneten Risikopunktzahl aktualisiert.
- Wenn ein Configuration Item (CI) für ein angreifbares Element geändert wird, auf das bereits eine Ausgleichssteuerung angewendet wird:
  - Das CI wird für ein angreifbares Element standardmäßig aktualisiert, wenn die Systemeigenschaft *sn_sec_cmn.update_on_ci_change* auf „true“ festgelegt ist.

    Die Ausgleichssteuerung gilt weiterhin für das angreifbare Element.
  - Das angreifbare Element wird geschlossen, und ein neues angreifbares Element wird erstellt, wenn die Systemeigenschaft *sn_sec_cmn.update_on_ci_change* auf „false“ festgelegt ist.

    Die auf das alte angreifbare Element angewendete Ausgleichssteuerung wird auf das neue angreifbare Element angewendet, und das **Bis-Datum für Risikominderung**, **die ursprüngliche Risikopunktzahl** und **die Risikopunktzahl** bleiben unverändert.
- Wenn ein angreifbares Element vom Scanner erneut geöffnet wird und auf das bereits eine Ausgleichssteuerung angewendet wurde, wird nach dem erneuten Öffnen dieselbe Ausgleichssteuerung angewendet.

Zugehörige Informationen

Ausgleichssteuerungen zur Risikoreduzierung verstehen

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikominderungsanforderungen zu

Risikominderung für ein CVE oder TPE aktivieren oder deaktivieren

#unique_135_Connect_42_li-risk-reduction-vmws

Beispiele für die Erstellung von Korrekturaufgaben in Vulnerability Manager Workspace und IT Remediation Workspace

Wenn Sie Korrekturaufgaben manuell in Vulnerability Manager Workspace und IT Remediation Workspaceerstellen, werden Datensätze basierend auf den von Ihnen ausgewählten Gruppierungskriterien in einer Korrekturaufgabe gruppiert.

Betrachten Sie das folgende Beispiel, in dem 10 Datensätze für die Erstellung von Korrekturaufgaben ausgewählt werden. Nachdem Sie die Details zur Datensatzauswahl und eine kurze Beschreibung angegeben haben, wählen Sie die **Gruppierungskriterien** entsprechend Ihren Anforderungen aus, und wählen Sie dann aus, wie Sie die Datensätze verwalten möchten, die bereits Teil vorhandener Korrekturaufgaben sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Erstellung der Korrekturaufgabe basierend auf den Gruppierungskriterien

Angreifbare Elemente, die für die Erstellung von Korrekturaufgaben ausgewählt wurden

ID des angreifbaren Elements	Vorhandene Korrekturaufgab	Zuweisungsgrup	Konfigurationsel	Schwachstelle	Risikobewertung
VIT10001	VUL10021, VUL10022	Nachbesserungsmanager	APSV-NY-1672	CVE-2018-9020	4
VIT10002	-	Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10003	VUL10021	LDAP-Administratoren	DEV-IBM-NY-682	CVE-2012-5357	1
VIT10004	-	Nachbesserungsmanager	GBMBK-SD-4210	CVE-2013-1710	4
VIT10005	VUL10022	Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10006	-	Nachbesserungsmanager	GBMBK-SD-4210	CVE-2013-1710	2
VIT10007	-	LDAP-Administratoren	DEV-SAP-SD-9388	CVE-2013-3906	1
VIT10008	-	LDAP-Administratoren	DEV-IBM-NY-682	CVE-2013-3906	1
VIT10009	-	Nachbesserungsmanager	GBMBK-SD-4210	CVE-2013-1710	2
VIT10010	-	LDAP-Administratoren	DEV-SAP-SD-9388	CVE-2013-3906	4

Die folgende Liste zeigt, wie die Datensätze basierend auf den beim Erstellen der Korrekturaufgabe ausgewählten Gruppierungskriterien in Korrekturaufgaben gruppiert werden.

Szenario 1: „Zuweisungsgruppe“ ist für Gruppierungskriterien ausgewählt, und für das Verwalten von Datensätzen in anderen Korrekturaufgaben ist „Datensätze für neue Korrekturaufgaben überspringen“ ausgewählt.

Die Datensätze mit derselben Zuweisungsgruppe werden in einer Korrekturaufgabe gruppiert. Die Datensätze, die bereits Teil vorhandener Korrekturaufgaben sind, werden den neuen Korrekturaufgaben nicht hinzugefügt. Hier werden drei Korrekturaufgaben erstellt, die jeweils die Datensätze enthalten, die dem **Korrekturmanager**, **den LDAP-Administratoren**und **den Vulnerability Response** -Zuweisungsgruppen zugewiesen sind.

Korrekturaufgabe in Szenario 1 erstellt

Korrekturaufgaben erstellt	Datensätze in der Korrekturaufgabe
Korrekturaufgabe 1 – VUL10001	Diese Korrekturaufgabe enthält die Datensätze, die der **Korrekturmanager**-Zuweisungsgruppe zugewiesen sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgabe in Szenario 1 erstellt (Fortsetzung)

Korrekturaufgaben erstellt	Datensätze in der Korrekturaufgabe
	• VIT10004 • VIT10006 • VIT10009 Der VIT10001-Datensatz wird nicht in die VUL10001-Korrekturaufgabe verschoben.
Korrekturaufgabe 2 – VUL10002	Diese Korrekturaufgabe enthält den VIT10002-Datensatz, der der **Vulnerability Response-** Zuweisungsgruppe zugewiesen ist. Der VIT10005-Datensatz wird nicht in die VUL10002-Aufgabe verschoben.
Korrekturaufgabe 3 – VUL10003	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe **„LDAP-Administratoren“** zugewiesen sind: • VIT10007 • VIT10008 • VIT10010 Der VIT10003-Datensatz wird nicht in die Korrekturaufgabe VUL10003 verschoben.

Szenario 2: „Zuweisungsgruppe und Konfigurationselement“ wird für Gruppierungskriterien ausgewählt und „Datensätze in anderen Korrekturaufgaben verwalten“ wird als „Datensätze an die neuen Korrekturaufgaben übertragen“ ausgewählt.

Die Datensätze mit demselben Configuration Item, die derselben Zuweisungsgruppe zugewiesen sind, werden in einer Korrekturaufgabe gruppiert. Die Datensätze VIT10001, VIT10003 und VIT10005 werden aus ihren alten Korrekturaufgaben entfernt und in die neuen Korrekturaufgaben verschoben. Hier werden fünf Korrekturaufgaben erstellt.

In Szenario 2 erstellte Korrekturaufgaben

Korrekturaufgaben erstellt	Zeichnet einen Teil der Korrekturaufgabe auf
Korrekturaufgabe 1 – VUL10004	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe für **Korrekturbesitzer** und dem Konfigurationselement **APSVR-NY-1672** zugewiesen sind. • VIT10001 • [store-future: BEGIN review][End]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Szenario 2 erstellte Korrekturaufgaben (Fortsetzung)

Korrekturaufgaben erstellt	Zeichnet einen Teil der Korrekturaufgabe auf
	Der VIT10001-Datensatz wird aus den Korrekturaufgaben VUL10021 und VUL10022 entfernt.
Korrekturaufgabe 2 – VUL10005	Diese Korrekturaufgabe enthält die Datensätze, die der **Vulnerability Response-** Zuweisungsgruppe und dem Konfigurationselement **DEV-IBM-NY-682** zugewiesen sind. • VIT10002 • VIT10005 Der VIT10005-Datensatz wird aus der Korrekturaufgabe VUL10022 entfernt.
Korrekturaufgabe 3 – VUL10006	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe **„LDAP-Administratoren“** und dem Konfigurationselement **DEV-IBM-NY-682** zugewiesen sind. • VIT10003 • VIT10008 Der VIT10003-Datensatz wird aus der Korrekturaufgabe VUL10021 entfernt.
Korrekturaufgabe 4 – VUL10007	Diese Korrekturaufgabe enthält die Datensätze, die der **Korrekturmanager-** Zuweisungsgruppe und dem Konfigurationselement **CRMBK-SD-4210** zugewiesen sind. • VIT10004 • VIT10006 • VIT10009
Korrekturaufgabe 5 – VUL10008	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe **„LDAP-Administratoren“** und dem Konfigurationselement **DEV-SAP-SD-9388** zugewiesen sind. • VIT10007 • VIT10010

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario 3: „Zuweisungsgruppe und Schwachstelle“ ist für Gruppierungskriterien ausgewählt, und für „Datensätze in aktuellen und neuen Korrekturaufgaben beibehalten“ ist „Datensätze in anderen Korrekturaufgaben verwalten“ ausgewählt.

Die Datensätze mit derselben Schwachstelle, die derselben Zuweisungsgruppe zugewiesen sind, werden in einer Korrekturaufgabe gruppiert. Die Datensätze VIT10001, VIT10003 und VIT10005 werden ihren jeweiligen neuen Korrekturaufgaben hinzugefügt, ohne aus ihren alten Korrekturaufgaben entfernt zu werden. Hier werden fünf Korrekturaufgaben erstellt.

In Szenario 3 erstellte Korrekturaufgaben

Korrekturaufgaben erstellt	Zeichnet einen Teil der Korrekturaufgabe auf
Korrekturaufgabe 1 – VUL10009	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe für **Korrekturbesitzer** zugewiesen sind und die Schwachstelle **CVE-2018-9020** aufweisen. • VIT10001 • [store-future: BEGIN review][End] Der VIT10001-Datensatz bleibt auch Teil der Korrekturaufgaben für VUL10021 und VUL10022.
Korrekturaufgabe 2 – VUL10010	Diese Korrekturaufgabe enthält die Datensätze, die der **Vulnerability Response-** Zuweisungsgruppe zugewiesen sind und die Schwachstelle **CVE-2018-9020** aufweisen. • VIT10002 • VIT10005 Der VIT10005-Datensatz bleibt auch Teil der Korrekturaufgabe VUL10022.
Korrekturaufgabe 3 – VUL10011	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe **„LDAP-Administratoren“** zugewiesen sind und die Schwachstelle **CVE-2012-5357** aufweisen. • VIT10003 • [store-future: BEGIN review][End] Der VIT10003-Datensatz ist auch weiterhin Teil der VUL10021-Korrekturaufgabe.
Korrekturaufgabe 4 – VUL10012	Diese Korrekturaufgabe enthält die Datensätze, die der **Korrekturmanager-** Zuweisungsgruppe und der Schwachstelle **CVE-2013-1710** zugewiesen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Szenario 3 erstellte Korrekturaufgaben (Fortsetzung)

Korrekturaufgaben erstellt	Zeichnet einen Teil der Korrekturaufgabe auf
	• VIT10004 • VIT10006 • VIT10009
Korrekturaufgabe 5 – VUL10013	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe **„LDAP-Administratoren“** zugewiesen sind und die Schwachstelle **CVE-2013-3906** aufweisen. • VIT10007 • VIT10008 • VIT10010

Szenario 4: „Zuweisungsgruppe und Risikobewertung“ für Gruppierungskriterien, und für das Verwalten von Datensätzen in anderen Korrekturaufgaben ist „Datensätze in aktuellen und neuen Korrekturaufgaben beibehalten“ ausgewählt.

Die Datensätze mit derselben Risikobewertung, die derselben Zuweisungsgruppe zugewiesen sind, werden in einer Korrekturaufgabe gruppiert. Die Datensätze VIT10001, VIT10003 und VIT10005 werden ihren jeweiligen neuen Korrekturaufgaben hinzugefügt, ohne aus ihren alten Korrekturaufgaben entfernt zu werden. Hier werden fünf Korrekturaufgaben erstellt.

In Szenario 4 erstellte Korrekturaufgabe

Korrekturaufgaben erstellt	Zeichnet einen Teil der Korrekturaufgabe auf
Korrekturaufgabe 1 – VUL10014	Diese Korrekturaufgabe enthält die Datensätze, die der Zuweisungsgruppe für **Korrekturbesitzer** zugewiesen sind und eine Risikobewertung von **4** aufweisen. • VIT10001 • VIT10004 Der VIT10001-Datensatz ist weiterhin Teil der Korrekturaufgaben VUL10021 und VUL10022.
Korrekturaufgabe 2 – VUL10015	Diese Korrekturaufgabe enthält die Datensätze, die der **Vulnerability Response-** Zuweisungsgruppe zugewiesen sind und eine Risikobewertung von **2** aufweisen. • VIT10002 • VIT10005

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Szenario 4 erstellte Korrekturaufgabe (Fortsetzung)

Korrekturaufgaben erstellt	Zeichnet einen Teil der Korrekturaufgabe auf
	Der VIT10005-Datensatz ist weiterhin Teil der Korrekturaufgabe für VUL10022.
Korrekturaufgabe 3 – VUL10016	Diese Korrekturaufgabe enthält die Datensätze, die der **LDAP-Administratorzuweisungsgruppe** zugewiesen sind und **1** Risikobewertung aufweisen. • VIT10003 • VIT10007 • VIT10008 Der VIT10003-Datensatz ist weiterhin Teil der Korrekturaufgabe VUL10021.
Korrekturaufgabe 4 – VUL10017	Diese Korrekturaufgabe enthält die Datensätze, die der **Korrekturmanager-**Zuweisungsgruppe zugewiesen sind und eine Risikobewertung **von 2** aufweisen. • VIT10006 • VIT10009
Korrekturaufgabe 5 – VUL10018	Diese Korrekturaufgabe enthält die Datensätze, die der **LDAP-Administratorzuweisungsgruppe** zugewiesen sind und eine Risikobewertung von **4** aufweisen. • VIT10010 • [store-future: BEGIN review][End]

Zugehörige Informationen

Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Manager Workspace

Erstellen Sie manuell eine Korrekturaufgabe in IT Remediation Workspace

Die Ausnahmen für ausgewählte Datensätze in werden erneut ausgewertet Vulnerability Manager Workspace

Wenn Sie in Vulnerability Manager Workspacedie Ausnahmeregeln für eine Reihe von Datensätzen im Modal „Korrektureigenschaften erneut auswerten und aktualisieren“ auswerten, werden deren Zurückstellungsstatus und das Bis-Datum der Zurückstellung gemäß den neuesten Ausnahmeregeln aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenarien

Die folgenden Szenarien können auftreten, wenn Sie die Ausnahmen für eine ausgewählte Gruppe von Datensätzen im Modal „Korrektureigenschaften erneut auswerten und Korrektureigenschaften aktualisieren“ in Vulnerability Manager Workspaceauswerten:

Szenario 1: Wenn die ausgewählten Datensätze bereits manuell zurückgestellt wurden und der Bedingung einer Ausnahmeregel entsprechen, verbleiben diese Datensätze ohne Änderungen im Status „Zurückgestellt“.

Szenario 2: Wenn die ausgewählten Datensätze mit der Bedingung in den Ausnahmeregeln übereinstimmen und sich diese Datensätze im Status „Nicht zurückstellen“ befinden (z. B. „Offen“, „Wird überprüft“, „Wird untersucht“), werden diese Datensätze bis zu dem in der Ausnahmeregel definierten Datum zurückgestellt.

Szenario 3: Wenn sich die ausgewählten Datensätze bereits im Status „Zurückgestellt“ befinden (die mithilfe der Ausnahmeregel A zurückgestellt werden), verbleiben sie in den folgenden Szenarien im Status „Zurückgestellt“:

- Die Ausnahmeregel läuft ab, und die Datensätze stimmen nicht mit der Bedingung überein
- die Ausnahmeregel läuft ab und die Datensätze entsprechen der Bedingung
- die Ausnahmeregel A abläuft und Datensätze mit der Bedingung einer anderen Ausnahmeregel B übereinstimmen.

Szenario 4: Angenommen, die Datensätze werden mithilfe einer Ausnahmeregel zurückgestellt. Wenn Sie die Bedingung der Ausnahmeregel so ändern, dass der Status „Zurückgestellt“ der Datensätze nicht mehr gültig ist, und dann die Ausnahmeregeln für diese Datensätze neu auswerten, geschieht Folgendes:

- werden die Datensätze in den Status Offen verschoben
- das Bis-Datum, Zurückstellungsdatum, Zurückstellungsanzahl und andere Felder werden aktualisiert.

Example: Beachten Sie, dass Sie die Ausnahmen für die folgenden angreifbaren Hostelemente (VITs) bewerten.

Betrachten Sie die Ausnahmeregel mit den folgenden Details:

Details zur Ausnahmeregel

Feld	Beschreibung	Wert
Name	Name der Ausnahmeregel.	Kritische VITs werden zurückgestellt
Gültig ab	Datum, ab dem diese Regel aktiv ist, um die AEs zurückzustellen.	20-08-2024
Gültig bis	Datum, ab dem die Korrekturaufgabe die Annahme neuer AEs beendet.	30-11-2024
Grund	Grund für die Erstellung dieser Ausnahmeregel.	Risiko akzeptiert
Zuweisungsgruppe	Gruppe, der die zur Nachverfolgung der	Korrekturgruppe 1

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details zur Ausnahmeregel (Fortsetzung)

Feld	Beschreibung	Wert
	zurückgestellten AEs erstellte Korrekturaufgabe zugewiesen ist.	
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen.	Diese Regel wurde erstellt, um kritische VITs automatisch zurückzustellen.
Bedingung	Filterbedingung für die VIs, die während der Verarbeitung der VIs definiert werden kann.	Risikobewertung = 5 – Kritisch
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für bereits vorhandene Daten ausführen können.	Ja
Status	Status der Ausnahmeregel.	Genehmigt
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel.	100
Zurückgestellt bis	Datum, bis zu dem die VULs und VIs zurückgestellt werden. An diesem Datum wird die erstellte VUL geschlossen, alle VIs werden aus der Gruppe entfernt, und Gruppenregeln werden erneut angewendet.	2024-12-23 16:10:29

Die folgende Tabelle zeigt, wie sich der Status ändert, wenn die Ausnahmeregeln für mehrere VITs gleichzeitig neu ausgewertet werden:

Datensätze, für die Ausnahmen neu ausgewertet werden

VIT-Nummer	Status	Risikobewertung	Aktualisierter Status nach erneuter Auswertung der Ausnahmen –1	Bis-Datum: 1
VIT120067	Öffnen	2 - Niedrig	Öffnen	-
VIT120068	Wird überprüft	3 – Mittel	Wird überprüft	-
VIT120069	Wird untersucht	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120070	Zurückgestellt	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120071	Zurückgestellt	2 - Niedrig	Zurückgestellt	2024-10-02 16:10:29 (Manuell zurückgestellt)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze, für die Ausnahmen neu ausgewertet werden (Fortsetzung)

VIT-Nummer	Status	Risikobewertung	Aktualisierter Status nach erneuter Auswertung der Ausnahmen –1	Bis-Datum: 1
VIT120072	Abgeschlossen	5: Kritisch	Abgeschlossen	-

Wenn die Bedingung in der vorhergehenden Ausnahmeregel in `Risikobewertung = 2 - Niedrig` und **Zurückgestellt bis** in `2024-12-31 14:10:23` geändert wird, werden die Datensätze wie folgt aktualisiert:

Datensätze, für die Ausnahmen neu ausgewertet werden

VIT-Nummer	Aktualisierter Status nach erneuter Auswertung der Ausnahmen –1	Risikobewertung	Aktualisierter Status nach erneuter Auswertung der Ausnahmen – 2	Bis-Datum: 2
VIT120067	Öffnen	2 - Niedrig	Zurückgestellt	2024-12-31 14:10:23
VIT120068	Wird überprüft	3 – Mittel	Wird überprüft	-
VIT120069	Zurückgestellt	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120070	Zurückgestellt	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120071	Zurückgestellt	2 - Niedrig	Zurückgestellt (keine Änderung des Status)	02.10.2024 16:10:29 (Keine Änderung des Bis-Datums)
VIT120072	Abgeschlossen	5: Kritisch	Abgeschlossen	-

Zugehörige Informationen

Bewerten Sie die Korrektureigenschaften der Datensätze in neu Vulnerability Manager Workspace

Übersicht über Ausnahmeregeln

Konfigurations-Compliance Übersicht über Ausnahmeverwaltung

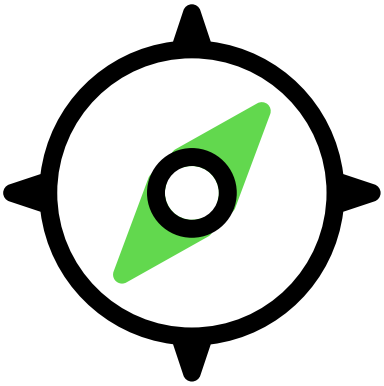
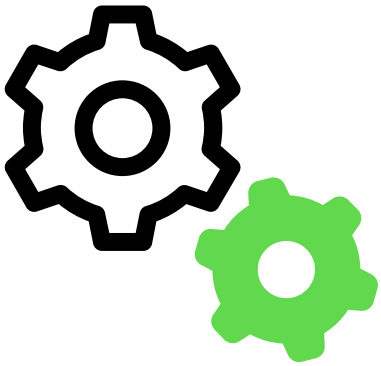
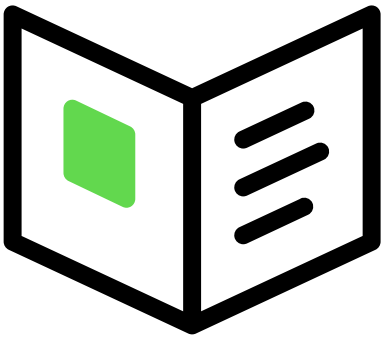
IT Remediation Workspace

IT-Teams können bei der Behebung von IT-bezogenen Schwachstellen Zeit sparen, indem sie von IT Remediation Workspaceaus ganz einfach Change-Anforderungen erstellen, angreifbare Elemente erneut scannen und Ausnahmeanforderungen übermitteln.

v18.0 IT-Nachbesserungs-Arbeitsbereich – Demo

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Beheben	Referenz
		
Erfahren Sie mehr über IT Remediation Workspace	Erfahren Sie, wie Sie Schwachstellen und Fehlkonfigurationen im beheben können IT Remediation Workspace	Erhalten Sie zusätzliche Informationen, die Sie zum Konfigurieren und Verwalten von verwenden IT Remediation Workspace

Problembehandlung und Hilfe

- Security Operations in der ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

IT Remediation Workspace erkunden

IT Remediation Workspace richtet sich an IT-Korrekturbesitzer und IT-Gruppen. Sie besteht aus Homepage- und Listenansichten sowie Datenvisualisierungen, auf die Sie klicken können, um die Ihnen zugewiesenen Korrekturaufgaben und die Anzahl der Ihnen zugewiesenen Datensätze mit Lösungen anzuzeigen.

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

IT Remediation Workspace besteht aus den folgenden Seiten, Listen und Formularen:

Zielseite (Homepage).

Die Homepage besteht aus der Karte Zugewiesene Korrekturaufgaben, der Karte Bevorzugte Lösungen auf VIs, der Karte Betroffene CIs, der Karte Bevorzugte Patches auf VIs und der Liste der Korrekturaufgaben. Weitere Informationen zur Homepage finden Sie unter Homepage im IT Remediation Workspace.

Seite „Dashboards“.

Die Seite „Dashboards“ besteht aus dem Dashboard für Schwachstellenkorrekturen. Weitere Informationen zur Seite „Dashboards“ finden Sie unter Seite „Dashboards“ im IT Remediation Workspace.

Listen-Seite

Diese Ansicht besteht aus standardmäßigen und anwenderdefinierten Listen von Korrekturaufgaben, angreifbaren Host-Elementen, angreifbaren Anwendungselementen, angreifbaren Container-Elementen, Konfigurationstestergebnissen, Lösungen, Ausnahmeanforderungen usw. Weitere Informationen zur Listenseite finden Sie unter Listenseite im IT Remediation Workspace. Weitere Informationen zu den Aktionen auf dieser Seite finden Sie unter Erstellen Sie eine Liste in IT Remediation Workspace.

Zeigen Sie ein Workflow-Beispiel in an IT Remediation Workspace

Sehen Sie sich ein Beispiel für einen End-to-End-Workflow im IT Remediation Workspacean. Erfahren Sie, wie IT-Spezialisten den -Arbeitsbereich verwenden können, um kritische angreifbare Elemente (VITs, AVITs und CVITs) und Testergebnisse (TRs) zu überwachen und die ihnen zugewiesenen Schwachstellen zu beheben.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

Klicken Sie auf die folgende Abbildung, um die Schritte des Workflows anzuzeigen.
Arbeitsbereich für IT-Fehlerkorrekturen

Das -Bild enthält die folgenden Aufgaben:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie auf der Homepage (Zielseite für IT-Korrekturbesitzer) die Ihnen zugewiesenen Korrekturaufgaben an. Wechseln Sie zwischen Arbeit, die Ihnen und Ihrer Gruppe zugewiesen ist. Sehen Sie sich die Host-Korrekturaufgaben mit Lösungen an. Weitere Informationen zur Homepage finden Sie unter Homepage im IT Remediation Workspace.
- Wählen Sie die **Listenansicht** aus, um die Listen der Ihnen zugewiesenen Arbeit anzuzeigen.
- Wählen Sie in der Listenansicht in der Liste Korrekturaufgaben die Liste **Meiner Gruppe zugewiesen** und identifizieren Sie sie, und weisen Sie sich selbst Arbeit zu. Weitere Informationen zur Listenseite finden Sie unter Listenseite im IT Remediation Workspace.
- Korrekturaufgaben nach Datensatztyp gruppieren: Wählen Sie das Menü mit den drei Punkten in der Spalte **„Datensatztyp“** und dann **Nach Datensatztyp gruppieren**aus.
- Bei einer offenen Korrekturaufgabe (VUL, AVUL, CVUL und CRG):
  - Wählen Sie die Registerkarte **Übersicht** aus, um die Datensätze (VITs, AVITs, CVITs und TRs) und die betroffenen Configuration Items (CIs) anzuzeigen, die dem Datensatz zugeordnet sind.
  - Wählen Sie die Registerkarte **Lösungen**, um bevorzugte und potenzielle Lösungen für eine Hostkorrekturaufgabe anzuzeigen.
  - Wählen Sie die Registerkarte **Details** aus, um bearbeitbare Felder wie Status, Zuweisungsgruppe, Zugewiesen an und Kurzbeschreibung zu ändern und die für eine Korrekturaufgabe ausgeführten Aktionen anzuzeigen.
  - Wählen Sie die Registerkarte **Status-Change-Genehmigung** aus, um die Status-Change-Genehmigungsdatensätze (CA#) anzuzeigen, mit denen Sie den Genehmigungs-Workflow nachverfolgen können.
  - Wählen Sie die Registerkarte **Change-Anforderungen**, um den Genehmigungsstatus der Change-Anforderungen anzuzeigen und um eine neue Change-Anforderung zu erstellen, indem Sie auf die Schaltfläche **Neu** klicken.
  - Wählen Sie die folgenden UI-Aktionen aus: **Als Falsch positiv markieren**, **Change erstellen**, **Aufgabe aufteilen**, **Status aktualisieren**,**Ausnahme anfordern**, **Löschen** usw. Befolgen Sie die Eingabeaufforderungen in den Dialogfeldern, um bei der Korrektur zu helfen.

Homepage im IT Remediation Workspace

Die Homepage in IT Remediation Workspace enthält eine konsolidierte Liste von Korrekturaufgaben für Hosts, Anwendungen, Container und Testergebnisse, die Ihnen und Ihren Zuweisungsgruppen zugewiesen sind.

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Die Homepage besteht aus den folgenden Karten und der Liste der Ihnen und Ihren Zuweisungsgruppen zugewiesenen Korrekturaufgaben sowie der Ihnen zugewiesenen Datensätze und Lösungen.

Karte „Zugewiesene Korrekturaufgaben“.

Anzahl der Ihnen zugewiesenen aktiven Korrekturaufgaben. Wählen Sie die Kachel aus, um die Liste der Korrekturaufgaben anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bevorzugte Lösungen auf Karte für AEs

Anzahl der bevorzugten Lösungen, die zur Korrektur der angreifbaren Host-Elemente verfügbar sind. Die Lösungsliste wird angezeigt, wenn die Anwendung Vulnerability Solution Management installiert ist. Diese Karte zeigt Lösungsdaten, potenzielle und bevorzugte Lösungen von Drittanbietern zu Ihren angreifbaren Elementen.

Karte „Betroffene CIs“.

Die Anzahl der Konfigurationselemente mit VIs, die Ihnen oder Ihren Gruppen zugewiesen sind. Weitere Informationen finden Sie unter Zeigen Sie Konfigurationselemente mit Schwachstellen in an IT Remediation Workspace.

Bevorzugte Patches auf VIs-Karte

Anzahl der verfügbaren bevorzugten Patches, die zur Korrektur der angreifbaren Host-Elemente verwendet werden können.

Liste der Korrekturaufgaben

Liste der Korrekturaufgaben, die Ihnen und Ihren Zuweisungsgruppen zugewiesen sind. Sie können die Datensätze filtern, indem Sie die Optionen **Mir zugewiesen** und **Meinen Gruppen zugewiesen** auswählen.

Sie können auf eine Korrekturaufgabe klicken, um Details anzuzeigen und eine Untersuchung zu starten. In der Listenansicht können Sie Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse usw. anzeigen. Sie können eine Korrekturaufgabe öffnen und **auf Mir zuweisen** klicken, um sich die Aufgabe selbst zuzuweisen und die Untersuchung zu starten.

Hinweis:
Wenn Sie sich die Aufgabe in der Korrekturaufgabe nicht selbst zuweisen, können Sie keine UI-Aktionen auf Datensatzebene anzeigen.

Klicken Sie auf die Ellipsen „Weitere Aktionen“ und anschließend **auf Untersuchung starten,** um eine Korrekturaufgabe zu lösen.

Weitere Informationen zu den Funktionen auf der Homepage finden Sie unter Verwenden Sie Datensätze für Korrekturaufgaben in IT Remediation Workspace.

Seite „Dashboards“ im IT Remediation Workspace

Auf der Seite „Dashboards“ in IT Remediation Workspace finden Sie das Dashboard „Schwachstellenkorrektur“ in der Anwenderoberfläche Next Experience, mit dem Sie sich auf Korrekturaufgaben und angreifbare Elemente konzentrieren können.

Als Korrekturverantwortlicher (sn_vul.remediation_owner) können Sie auf das Dashboard **für Schwachstellenkorrekturen** zugreifen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen** und wählen Sie das Dashboard-Symbol. Weitere Informationen zum Dashboard für die Schwachstellenkorrektur finden Sie unter Verwendung der Standard-Dashboards Vulnerability Response ..

Sie können ein anwenderdefiniertes Dashboard erstellen, indem Sie das Symbol „Weitere Optionen“ ⋮ wählen und **dann Neu erstellen**auswählen.

Listenseite im IT Remediation Workspace

Über die Listenansicht in IT Remediation Workspace können Korrekturbesitzer die ihnen und ihren Zuweisungsgruppen zugewiesenen Datensätze (VITs, AVITs, CVITs und TRs) anzeigen und diese Schwachstellen und Fehlkonfigurationen beheben. Sie können auch die Liste der bevorzugten Lösungen anzeigen, die für die Korrektur angreifbarer Hostelemente (VITs) empfohlen werden. Neben diesen Listen können Sie die Liste der von Ihnen ausgelösten Ausnahmeanforderungen und Bewertungsanforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für Penetrationstests, die mit Ihren Bewertungsanforderungen für Penetrationstests verknüpften Penetrationstestergebnisse, die unterstützten Bibliotheken und andere unterstützte Daten anzeigen.

Erforderliche Rollen:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Die Listen und Links auf der Listenseite bieten Ihnen einfachen Zugriff auf Datensätze und Aufgaben. Sie enthält zwei Registerkarten:

- **Registerkarte** Listen: Zeigt die Standardlisten für Korrekturmaßnahmen, Korrekturaufgaben, angreifbare Elemente (VITs, AVITs oder CVITs), Lösungen, Ausnahmen und Konfigurationstestergebnisse (Configuration Test Results, TRs) usw. an. Weitere Informationen finden Sie in der folgenden Tabelle.
- Registerkarte**Meine Listen** : Zeigt alle Listen an, die Sie auf der Registerkarte Liste umbenannt haben, sowie alle von Ihnen erstellten Listen.

  Sie können auch eine eigene Liste von Datensätzen erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Liste in IT Remediation Workspace.

Tipp:

Wenn die Systemeigenschaft *sn_vul_cmn_ws.navigate_to_workspace* vom Administrator auf true festgelegt ist, werden nach Auswahl der vordefinierten Filterlinks im Modul Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Testergebnisse in Konfigurations-Compliance im Menü **Alle** diese Links auf der Listenseite geöffnet in der IT Remediation Workspace.

Zum Beispiel, wenn Sie **Zugewiesen an Meine Gruppen** auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**, dieser Link wird an IT Remediation Workspaceumgeleitet. Die Liste Meiner Gruppe zugewiesen im Modul Korrekturaufgaben wird auf der Listenseite des Arbeitsbereichs für IT-Korrekturen geöffnet, wenn Sie die Rolle des Korrekturbesitzers innehaben. Um die Host-Korrekturaufgaben anzuzeigen, gruppieren Sie die Aufgaben nach **Datensatztyp**.

Mit der Systemeigenschaft *glide.ui.list.seismic.omit.count* können Sie die Anzahl der Datensätze in einer Liste ausblenden. Weitere Informationen zum Deaktivieren/Aktivieren der Anzeige der Datensatzanzahl in einer Liste finden Sie im KB-Artikel KBB0010402 .

Registerkarte Listen

Die folgenden Listen werden angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
Korrekturaufgaben	Zeigen Sie die Liste der Korrekturaufgaben an, und navigieren Sie zur gewünschten Aufgabe, um mit der Bearbeitung zu beginnen. Die folgenden Listen sind verfügbar: • **Ihnen zugewiesen**: Listet alle Ihnen zugewiesenen Korrekturaufgaben für Host, Anwendung, Container und Testergebnis auf. • **Meiner Gruppe zugewiesen**: Listet alle Korrekturaufgaben für Hosts, Anwendungen, Container und Testergebnisse auf, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören. Gruppieren Sie die Aufgaben nach dem Datensatztyp, um sie in Korrekturaufgaben für Host-, Anwendungs-, Container- und Konfigurationstestergebnisse zu kategorisieren. Korrekturaufgaben, die von den Regeln für Korrekturaufgaben in der klassischen Anwenderoberfläche erstellt werden, haben eine leere Korrekturmaßnahme.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.remediation_owner für angreifbare Host-Elemente (VITs) • sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
Betroffene Assets	Zeigen Sie die Liste der betroffenen Assets an. Die folgenden Listen sind verfügbar: • **Ihnen zugewiesen**: Liste der betroffenen Configuration Items, die Ihnen zugewiesen sind • **Meiner Gruppe zugewiesen**: Liste der betroffenen Configuration Items, die Ihren Zuweisungsgruppen zugewiesen sind.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.remediation_owner für angreifbare Host-Elemente (VITs) • sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)
Angreifbare Host-Elemente	Zeigen Sie die Liste der angreifbaren Host-Elemente an, und navigieren Sie zum gewünschten Element, um mit der Bearbeitung zu beginnen. Diese Listen sind verfügbar: • **Mir zugewiesen**: Liste der angreifbaren Host-Elemente, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen**: Liste der angreifbaren Host-Elemente, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.	Vulnerability Response	sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
Angreifbare Anwendungselemente	Zeigen Sie die Liste der angreifbaren Host-Elemente an, und navigieren Sie zum gewünschten Element,	Application Vulnerability Response	sn_vul.app_security_Champion

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
	um mit der Bearbeitung zu beginnen. Die folgenden Listen sind verfügbar: • **Mir zugewiesen**: Liste der angreifbaren Anwendungselemente, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen**: Liste der angreifbaren Anwendungselemente, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.		
Angreifbare Container-Elemente	Zeigen Sie die Liste der angreifbaren Container-Elemente an, und navigieren Sie zum gewünschten Element, um mit der Bearbeitung zu beginnen. Diese Listenansicht enthält: • **Mir zugewiesen**: Liste der angreifbaren Container-Elemente, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen**: Liste der angreifbaren Container-Elemente, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.	Container Vulnerability Response	sn_vul_container.remediation_owner Zeigen Sie die Liste der Bewertungen an, die für die Überprüfung nach Incidents erforderlich sind.
Konfigurationstestergebnisse	Zeigen Sie die Liste der Testergebnisse an,	Konfigurations-Compliance	sn_vulc.remediation_owner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
	und navigieren Sie zum gewünschten Datensatz, um die Ergebnisse zu bearbeiten. Diese Listenansicht enthält: • **Mir zugewiesen**: Liste der Konfigurationstestergebnisse, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen**: Liste der Konfigurationstestergebnisse, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.		
Lösungen	Listet die Lösungen aus der Lösungsmanagement-Anwendung auf. Die Lösungsliste wird angezeigt, wenn die Anwendung Vulnerability Solution Management installiert ist. • **Alle**: Zeigt alle verfügbaren Lösungen an, die Sie zum Korrigieren der angreifbaren Host-Elemente verwenden. • **Höchste Ersatzlösung**: Zeigt alle Lösungen an, die für die ausgefüllten bevorzugten Lösungen verwendet werden.	Vulnerability Response	sn_vul.remediation_owner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
	• **Mit angreifbaren Elementen**: Zeigt die Lösungen an, die als bevorzugte Lösung für angreifbare Elemente verwendet werden.		
Ausnahmeanforderungen	• **Meine Anforderungen**: Liste aller von Ihnen erstellten Genehmigungsanforderungen für Ausnahmen, falsch positive Ergebnisse und das Aufheben von Zuweisungen für angreifbare Host-, Anwendungs- und Container-Elemente und deren Korrekturaufgaben. • **Meine Anforderungen (Konfigurations-Compliance)**: Liste aller von Ihnen erstellten Ausnahmen, falsch positiven und nicht zugewiesenen Genehmigungsanforderungen für die Testergebnisse und deren Korrekturaufgaben, an denen Sie arbeiten.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.remediation_owner für angreifbare Host-Elemente (VITs) • sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)
Bibliotheken	Enthält die folgenden Listen: • **NVDs**: Eine umfassende Bibliothek von Schwachstelleninformationen.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.remediation_owner für angreifbare Host-Elemente (VITs) • sn_vul.app_security_Champion für angreifbare

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
	die vom National Institute of Standards and Technology (NIST) verwaltet wird. Liste der von NVD gefundenen Schwachstellen, einschließlich Sicherheitsprüflisten, sicherheitsbezogener Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits. • **CWEs**: Liste der von der Community entwickelten Software-Schwachstellentypen. Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. • **App-Schwachstellen**: Liste aller Schwachstelleneinträge für Drittanbieteranwendungen. • **TPEs**: Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs. • **Tests**: Aus Drittanbieterintegrationen importierte Tests, denen die		Elemente in der Anwendung (AVITs) • sn_vul_container.remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
	Testergebnisse entsprechen müssen. • **Testgruppen**: Liste der Testgruppen/-richtlinien, die aus den Drittanbieterintegrationen importiert wurden. Eine Testgruppe enthält eine Reihe von Tests.		
CMDB	• **Erkannte Elemente**: Liste aller erkannten Elemente. • **Erkannte Containerbilder**:	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance	• sn_vul.remediation_owner für angreifbare Host-Elemente (VITs) • sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs) • sn_vul_container.remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.remediation_owne für Konfigurationstestergebnisse (CTRs)
Anforderungen für Penetrationstestbewertung	Bewertungsanforderungen für Penetrationstests, die von Ihnen an das Sicherheitsteam übermittelt wurden, um eine Sicherheitsbewertung einer Geschäftsanwendung durchzuführen. Diese Liste enthält: • **Mir zugewiesen**: Liste der von Ihnen ausgelösten Penetrationstest-Bewertungsanforderungen.	Application Vulnerability Response	sn_vul.app_security_Champion

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
	• **Meinen Gruppen zugewiesen**: Liste der Penetrationstest-Bewertungsanforderungen, die von den Anwendern in Ihren Zuweisungsgruppen ausgelöst wurden.		
Penetrationstest-Ergebnisse	Liste der Schwachstellen, die während der vom Sicherheitsteam durchgeführten Pen-Testbewertung identifiziert wurden: • **Mir zugewiesen**: Liste der Penetrationstest-Ergebnisse, die Ihnen zur Korrektur zugewiesen sind. • **Meinen Gruppen zugewiesen**: Liste der Penetrationstest-Ergebnisse, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind.	Application Vulnerability Response	sn_vul.app_security_Champion
Unterstützungsdaten	Diese Listenansicht enthält: • **Autoritative Quellen**: Liste der autorisierten Quellen, die Zusammenfassungsinformationen bereitstellen, die für die Recherche der Quellveröffentlichungen nützlich sind, die zum Erstellen	Konfigurations-Compliance	sn_vulc.remediation_owner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle erforderlich
	des Datensatzes verwendet wurden. • **Technologien**: Liste der Technologien, die die Zusammenfassungsinformationen zu allen maßgeblichen Quellen und Quelleninhalten bereitstellen (in Qualys auch als Framework bezeichnet)		

Zugehörige Informationen

Verwenden Sie die Listenansicht in Vulnerability Manager Workspace

IT Remediation Workspace verwenden

IT Remediation Workspace enthält eine konsolidierte Liste von Hostschwachstellen, Anwendungsschwachstellen, Containerschwachstellen und Fehlkonfigurationen, die Ihnen und Ihrer Gruppe zugewiesen sind. Sie können diesen Arbeitsbereich verwenden, um Schwachstellen und Fehlkonfigurationen zu beheben und Ausnahmen für sie anzufordern.

Öffnen Sie Suchergebnisse in IT Remediation Workspace

Legen Sie den Anwendungsbereich auf IT Remediation Workspace fest, um Ihre Suchergebnisse in IT Remediation Workspace anstelle der klassischen Anwenderoberfläche zu öffnen, indem Sie den Anwendungsbereich ändern.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie beispielsweise nach einem angreifbaren Host-Element suchen, dessen Nummer im **Suchfeld** angegeben ist, indem Sie den Anwendungsbereich auf IT Remediation Workspacefestlegen, wird das VIT in seiner Datensatzansicht in IT Remediation Workspacegeöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie in der zentralen Navigationsleiste das Globussymbol .
2. Wählen Sie **Anwendungsbereich**aus, und legen Sie dann den Bereich auf **Arbeitsbereich für IT-Nachbesserungen**fest.

Ergebnisse

Wenn Sie im Feld Suchen der zentralen Navigationsleiste nach Datensätzen wie VITs, Korrekturaufgaben, Genehmigungen von Statusänderungen usw. **suchen**, werden die Datensätze in IT Remediation Workspacegeöffnet.

Wenn der Bereich nicht Global ist, wird das Globussymbol mit einem roten Ring angezeigt. . Wählen Sie es erneut aus, um den Umfang zu ändern.

Verwenden Sie den E-Mail-Digest in den Vulnerability Response-Arbeitsbereichen

Verwenden Sie E-Mail-Benachrichtigungen, um Ihren Korrekturfortschritt anzuzeigen und sich daran zu erinnern, wenn Aufgaben näherkommen oder SLA überschritten werden.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Melden Sie sich als Besitzer der Korrektur in Ihrem Arbeitsbereich an, und sehen Sie sich Ihre E-Mail-Benachrichtigung als Zusammenfassung Ihrer Arbeit an. Sehen Sie, was Sie erreicht haben, was bevorsteht und was überfällig ist. Verwenden Sie die Benachrichtigung, um Ihre kritischen Korrekturaktionen zu organisieren und zu priorisieren. Klicken Sie auf einen Link in der E-Mail, um direkt zu in Ihren -Arbeitsbereich zu gelangen. Benachrichtigungen können IT-Spezialisten helfen, den Status ihrer Arbeit auf einen Blick zu sehen. Als Schwachstellenmanager helfen Sie Ihren IT-Spezialisten, für Korrekturaufgaben direkt über den E-Mail-Service auf die Plattform zu gelangen.

Weitere Informationen zur Konfiguration dieser Funktion finden Sie unter Richten Sie E-Mail-Benachrichtigungen in den -Arbeitsbereichen Vulnerability Response ein.

In der E-Mail werden standardmäßig die von Ihnen geschlossenen Aufgaben, die Gesamtzahl der aktiven Ihnen und Ihren Gruppen zugewiesenen Aufgaben, neu zugewiesene Aufgaben, geschlossene VITs und andere Informationen angezeigt.

Prozedur

1. Navigieren Sie zu Ihrer E-Mail, suchen Sie eine Benachrichtigung, und klicken Sie darauf, um sie zu öffnen. In der Benachrichtigung werden Informationen zu Ihrem Arbeitsstatus angezeigt.
2. Klicken Sie **auf Zum Arbeitsbereich wechseln,** um zu Ihrem Arbeitsbereich zu navigieren.

Erstellen Sie eine Liste in IT Remediation Workspace

Mit der Listenansicht in IT Remediation Workspacekönnen Sie Korrekturaufgaben und Datensätze anzeigen, die Ihnen und Ihren Gruppen zugewiesen sind. Sie können auch Ihre Ausnahme- und falsch positiven Anforderungen für Korrekturaufgaben (VUL, AVUL,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CVUL und CRG), angreifbare Elemente (VIT, AVIT und CVIT) und Testergebnisse (TRs) nachverfolgen und Lösungen anzeigen.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie das Listensymbol ( ) aus.
   Die Listenansicht wird angezeigt.
   - Klicken Sie auf eine gefilterte Liste, um die Gesamtzahl der aktiven Korrekturaufgaben oder Datensätze anzuzeigen, die Ihnen oder Ihrer Gruppe zugewiesen sind. Unter Verwenden Sie Datensätze für Korrekturaufgaben in IT Remediation Workspace finden Sie weitere Informationen darüber, was Sie mit diesen Datensätzen tun können.
   - Zeigen Sie die Gesamtzahl der Ihnen oder Ihren Gruppen zugewiesenen VIs mit Lösungen an. Klicken Sie auf die Karte **Bevorzugte Lösungen auf VIs,** um die Liste anzuzeigen.
   - Die Ihnen und Ihren Gruppen zugewiesenen angreifbaren CIs mit Schwachstellen finden Sie auf der Registerkarte **Angreifbare CIs** oder in der Liste Ihnen und Ihrer Gruppe zugewiesener angreifbarer CIs in der Listenansicht.
3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie **Neue Liste hinzufügen**.
5. Erstellen Sie die Liste entweder basierend auf einer vorhandenen Liste oder basierend auf Ihrem eigenen Setup.
6. **Wahlweise:** Erstellen Sie eine gefilterte Liste.
   a. Legen Sie im Feld **Spalten auswählen** fest, welche Spalten in der Liste angezeigt werden, indem Sie alle Felder löschen, die nicht angezeigt werden sollen.
   b. Geben Sie Bedingungen zum Filtern der Liste an.
      (Optional) Um mehr als eine Bedingung hinzuzufügen, wählen Sie **Neuer Bedingungssatz**aus.
      Wenn Sie beispielsweise eine Liste aktiver angreifbarer Elemente für einen zu überwachenden Scanner erstellen möchten, können Sie die Bedingungen **[Aktiv][ist][wahr]** und **[Quelle][enthält][Scanner-Name]**eingeben.
   c. Wählen Sie **Erstellen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihre neue Liste wird angezeigt.

Hinweis:
Wenn Sie das Listenmodul verlassen, entspricht die Liste, die beim Beenden angezeigt wird, der Liste, die Sie bei der Rückkehr sehen. Um die von Ihnen erstellten anwenderdefinierten Listen zu löschen, wählen Sie bei angezeigter Liste rechts im Bereich das Zahnradsymbol und dann **Löschen aus**.

7. Der folgenden Tabelle können Sie entnehmen, was Sie in der Listenansicht tun können.

Verwenden Sie Datensätze in der IT Remediation Workspace

Verwenden Sie Datensätze, um Ihren Nachbesserungsfortschritt und die Auswirkungen angreifbarer Elemente auf Ihre Assets anzuzeigen.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren Sie in Ihrer Instanz von Now Platform zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
   Die Zielseite der Homepage wird angezeigt.
2. Navigieren Sie zu einem Datensatz für ein angreifbares Element, und öffnen Sie ihn entweder auf der Zielseite der Homepage oder in der Listenansicht.

   Die Registerkarte „Details“ enthält im Formular-Header oben Informationen, die sich auf die Art der Schwachstelle beziehen, z. B. CVE-2013-5014 gefunden unter LINUX-DAL-4331. Unter dem Formularheader werden Werte für Status, Risikobewertung und Korrekturzieldatum angezeigt.
3. In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie für den Datensatz der Korrekturaufgabe ausführen können.

Erstellen Sie manuell eine Korrekturaufgabe in IT Remediation Workspace

Ab v25.0.4 von Vulnerability Responsekönnen Sie Korrekturaufgaben manuell über die Listen Angreifbare Host-Elemente, Angreifbare Anwendungselemente, Angreifbare Container-Elemente und Konfigurationstestergebnisse auf der Listenseite von IT Remediation Workspaceerstellen.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.write_assigned oder sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_write_assigned oder sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.writer_assigned oder sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen** > **Liste**.
2. Öffnen Sie auf der Listenseite die Liste Aktiv oder Alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Anwendungselemente
   - Angreifbare Container-Elemente
   - Konfigurationstestergebnisse
3. Aktivieren Sie das Kontrollkästchen der Datensätze, die Sie aktualisieren möchten, und wählen Sie dann im Modal „Korrekturaufgabe erstellen“ im Feld „Datensatzauswahl“ die Option Ausgewählte Elemente aus.
4. Wählen Sie **Korrekturaufgabe erstellen aus**.
5. Füllen Sie im Modal „Korrekturaufgabe erstellen“ die folgenden Details aus.

Modal „Korrekturaufgabe erstellen“.

Feld	Beschreibung
Datensatzauswahl	**Ausgewählte Elemente**: Aktualisiert nur die ausgewählten Datensätze.
Kurzbeschreibung	Kurze Notiz zu den Korrekturaufgaben.
Gruppierungskriterien	Die Auswahlmöglichkeiten lauten wie folgt: ○ **Zuweisungsgruppe**: Datensätze mit derselben Zuweisungsgruppe werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Konfigurationselement**: Datensätze mit derselben Zuweisungsgruppe und demselben Konfigurationselement werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Schwachstelle**: Datensätze mit derselben Zuweisungsgruppe und Schwachstelle werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Risikobewertung**: Datensätze mit derselben Zuweisungsgruppe und Risikobewertung werden in einer Korrekturaufgabe gruppiert.
Datensätze in anderen Korrekturaufgaben verwalten	Die Auswahlmöglichkeiten lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Datensätze für neue Korrekturaufgaben überspringen**: Für die Datensätze, die Teil anderer Korrekturaufgaben sind, wird keine Aktion ausgeführt. ○ **Zu neuen Korrekturaufgaben verschieben**: Datensätze, die Teil anderer Korrekturaufgaben sind, werden zu neuen Korrekturaufgaben übertragen. ○ **Sowohl in aktuellen als auch in neuen Korrekturaufgaben beibehalten**: Datensätze, die Teil anderer Korrekturaufgaben sind, werden sowohl in alten als auch in neuen Korrekturaufgaben aufbewahrt.

6. Wählen Sie **Korrekturaufgabe erstellen aus**.

Ergebnisse

Korrekturaufgaben werden auf Grundlage der Gruppierungskriterien erstellt. An die Korrekturbesitzer in der Zuweisungsgruppe wird eine E-Mail-Benachrichtigung gesendet, in der sie darüber informiert werden, dass eine Korrekturaufgabe erstellt und ihrer Gruppe zugewiesen wurde. Beispiele dafür, wie Korrekturaufgaben basierend auf den Gruppierungskriterien und den Datensatzverwaltungskriterien erstellt werden, finden Sie unter Beispiele für die Erstellung von Korrekturaufgaben in Vulnerability Manager Workspace und IT Remediation Workspace.

Verwenden Sie Datensätze für Korrekturaufgaben in IT Remediation Workspace

Korrekturaufgaben werden automatisch aus Korrekturmaßnahmen erstellt und zugewiesen. IT-Teams und Korrekturbesitzer können Korrekturaufgaben im IT Remediation Workspaceanzeigen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Schwachstellenmanager und Analysten Korrekturmaßnahmen erstellen, um die Nachbesserung voranzutreiben, werden automatisch Korrekturaufgaben erstellt und den IT-Teams auf Grundlage der Gruppe zugewiesen, die den Datensätzen in einer Korrekturmaßnahme zugeordnet ist.

Die Ihnen und Ihren Gruppen zugewiesenen angreifbaren CIs mit Schwachstellen finden Sie auf der Registerkarte **Angreifbare CIs** oder in der Liste Ihnen und Ihrer Gruppe zugewiesener angreifbarer CIs in der Listenansicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie in Ihrer Instanz von Now Platform zu **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
   Die Zielseite der Homepage wird angezeigt.
2. Klicken Sie im Abschnitt „Korrekturaufgaben“ auf eine Korrekturaufgabe, um sie zu öffnen.
3. **Wahlweise:** Alternativ können Sie auf der Homepage oben links auf das Listensymbol klicken, um alle Korrekturaufgaben (VULs, AVULs, CVULs und CRGs) und Datensätze (VITs, AVITs, CVITs und TRs) anzuzeigen, die Ihnen und Ihren Gruppen zugewiesen sind .
   Weitere Informationen zur Verwendung der Listenansicht finden Sie unter Erstellen Sie eine Liste in IT Remediation Workspace.
4. Klicken Sie entweder auf der Homepage oder in der Listenansicht auf eine Korrekturaufgabe, um sie zu öffnen.

   Auf der Registerkarte **„Details** “ können Sie einige der Informationen im Datensatz aktualisieren, z. B. Zuweisungsgruppe, Status, Kurzbeschreibung usw. Klicken Sie auf **Speichern**, um Ihre Änderungen anzuwenden.
5. In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie aus dem Korrekturaufgaben-Datensatz ausführen können.

   Die Registerkarte „Lösungen“ in einer Host-Korrekturaufgabe zeigt Informationen zu bevorzugten und potenziellen Lösungen, die der mit der Korrekturaufgabe verknüpften Schwachstelle am besten entsprechen. Lösungen sind Patches, die Ihre IT-Teams anwenden, um Schwachstellen zu beheben.

   Wenn die Anwendung Vulnerability Solution Management installiert ist, sind *Bevorzugte Lösungen* die höchsten Ersatzlösungen, die auf angreifbare Elemente angewendet werden. Die Liste der Lösungen basiert auf den angreifbaren Elementen in der Host-Korrekturaufgabe.

   Potenzielle Lösungen sind die Liste aller Lösungen, die für VITs in einer Host-Korrekturaufgabe verfügbar sind.

   Sie können die CIs (Assets), die von dieser Schwachstelle betroffen sind, in der Korrekturaufgabe anzeigen, indem Sie zu navigieren **Übersicht** > **Betroffene CIs**.

Weisen Sie sich im eine Korrekturaufgabe oder einen Datensatz selbst zu IT Remediation Workspace

Weisen Sie sich auf der Seite Listen im -Arbeitsbereich IT Remediation Workspace selbst eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) oder einen Datensatz (VIT, AVIT, CVIT oder TR) zu.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen** > **Liste** > **Korrekturaufgaben** > **Meiner Gruppe zugewiesen**.
2. Öffnen Sie eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) in der Liste der Korrekturaufgaben.
3. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite **auf Mir zuweisen**.

   Die Schaltfläche **Mir zuweisen** ist nur verfügbar, wenn Ihnen der Datensatz noch nicht zugewiesen ist.

   Die Korrekturaufgabe wird in der Liste Mir zugewiesen unter Korrekturaufgaben angezeigt.
4. Sie können sich auch selbst einen Datensatz (VIT, AVIT, CVIT oder TR) zuweisen, indem Sie die gleichen Schritte von einem geöffneten Datensatz aus ausführen.
   Die Schaltfläche **Mir zuweisen** ist nur verfügbar, wenn Ihnen der Datensatz noch nicht zugewiesen ist.

Zeigen Sie Konfigurationselemente mit Schwachstellen in an IT Remediation Workspace

Die folgenden Verbesserungen wurden Korrekturaufgaben mit Version 16.1 der Anwendung Vulnerability Response hinzugefügt.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Die Rolle itil oder cmdb_read ist ebenfalls erforderlich, wenn Sie CI-Daten in den Arbeitsbereichen anzeigen möchten.

Warum und wann dieser Vorgang ausgeführt wird

Sehen Sie sich die Ihnen zugewiesenen Configuration Items (CIs) an, die Schwachstellen aufweisen. Klicken Sie auf **Betroffene CIs** -Bewertungsliste. Klicken Sie auf die Filterliste oben links, um zwischen **Mir zugewiesen** und **Meinen Gruppen zugewiesen**zu wechseln. Klicken Sie in der Listenansicht auf die Links.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
   Die Zielseite der Homepage wird angezeigt.
2. Alternativ können Sie diese Listen über die Links in der Listenansicht anzeigen oder indem Sie zu den entsprechenden Modulen navigieren, z. B. **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
3. Wählen Sie eine, um fortzufahren.
   Je nachdem, was beim Filterwechsel ausgewählt ist, können Sie die Listen der folgenden Datensätze anzeigen, die Ihnen oder Ihnen und Ihren Gruppen zugewiesen sind.
4. Klicken Sie auf die Bewertungsliste **Betroffene CIs**.

   Die Liste der CI-Datensätze wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf ein Configuration Item, um den zugehörigen Datensatz zu öffnen.
   Der Datensatz wird angezeigt.

   In den zugehörigen Listen können Sie Details und verschiedene zugehörige Datensätze anzeigen. Zu den neuen verfügbaren Daten für diesen Datensatz mit diesem Release gehören:

   - Eine Zeitleiste, die die letzte Aktivität für diesen Datensatz zeigt.
   - Alle Change-Anforderungen, die diesem CI zugeordnet sind.
   - Navigieren Sie einfach zu Bewertungslisten, und zeigen Sie die Korrekturaufgaben, angreifbaren Elemente und bevorzugten Lösungen an, die diesem CI zugeordnet sind.
   - Sie können zu den Bewertungslisten navigieren und die bevorzugten Patches anzeigen, die diesem CI zugeordnet sind. Bevorzugte Patches sind die Patches, die den angreifbaren Elementen zugeordnet sind. Auf der Registerkarte Patches in der zugehörigen Liste werden die installierten und fehlenden Patches für die CIs angezeigt.
   - Informationen zum CI, einschließlich Klasse, Standort, Internetverbindung, Umgebung und Wartungsplan.

Erstellen Sie eine Change-Anforderung im IT Remediation Workspace

Erstellen Sie aus einer Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) eine Change-Anforderung. Alternativ können Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe hinzufügen.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Hinweis:
Die Rolle itli ist erforderlich, wenn Sie Change-Anforderungen von IT Remediation Workspaceübermitteln möchten.

Warum und wann dieser Vorgang ausgeführt wird
Es kann verschiedene Gründe geben, aus denen Sie eine Change-Anforderung für eine Korrekturaufgabe erstellen möchten. Normalerweise liegt dies daran, dass Ihre Untersuchung manuelles Eingreifen erfordert, um die Schwachstellen zu beheben.

Weitere Informationen zu Change-Anforderungen und zum Erstellen von Change-Anforderungen in der klassischen Umgebung finden Sie unter Change Management für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie das Listensymbol.
3. Suchen Sie auf der Seite Liste in der Liste Korrekturaufgaben nach einer Korrekturaufgabe (VUL, AVUL, CVUL oder CRG), für die Sie eine Change-Anforderung erstellen möchten.
4. Erweitern Sie in den UI-Aktionsschaltflächen auf der rechten Seite die Liste, und wählen Sie eine aus:
   - Klicken Sie **auf Change erstellen**
   - **Zu vorhandenem Change hinzufügen**
5. Um eine neue Change-Anforderung zu erstellen, füllen Sie im angezeigten Modal die Felder aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Formularfelder für Change-Anforderung erstellen.
6. Wählen Sie **Change-Anforderung erstellen aus**.
   Der Datensatz für die Korrekturaufgabe wird angezeigt, und eine Nachricht gibt an, dass die Change-Anforderung erfolgreich erstellt wurde.

   Klicken Sie auf den zugehörigen Link Change-Anforderungen für einen Datensatz, um alle mit dem Datensatz verknüpften Change-Anforderungen anzuzeigen.
7. Alternativ können Sie diese Korrekturaufgabe einer vorhandenen Change-Anforderung hinzufügen, indem Sie die folgenden Schritte ausführen.

   a. Klicken Sie auf den Abwärtspfeil, um die Liste auf der Schaltfläche **Change erstellen** zu erweitern.

   b. Wählen Sie **Zu vorhandenem Change hinzufügen**.

   c. Klicken Sie im angezeigten Modal auf das Suchsymbol, um die Liste der vorhandenen Change-Anforderungen anzuzeigen.

   d. Um der Liste Bedingungen hinzuzufügen, um die Liste der Change-Anforderungen zu fokussieren, klicken Sie oben rechts im Modal auf das Filtersymbol (Trichter).

   e. Klicken Sie im neuen Fenster, das angezeigt wird, auf **Erweiterte Ansicht**.

   f. Verwenden Sie den Bedingungsgenerator, um Ihre Bedingungen zu erstellen.

   g. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Klicken Sie in der Liste auf eine Change-Anforderung, um sie auszuwählen.
Ein aktualisiertes Modal wird mit Ihrer Auswahl angezeigt.

i. Wahlweise: Aktivieren Sie im Modal das Kontrollkästchen CIs zu CR hinzufügen, um dem Change Request Konfigurationselemente aus allen aktiven angreifbaren Elementen hinzuzufügen.

j. Wählen Sie **Change hinzufügen**aus.
Der Korrekturdatensatz wird angezeigt, und eine Nachricht gibt an, dass die Change-Anforderung erfolgreich erstellt und zur Genehmigung übermittelt wurde.

- Klicken Sie in der Nachricht auf den Link **Change anzeigen,** um den Datensatz für die Change-Anforderung (CHG) zu öffnen.
- Wählen Sie im Datensatz der Korrekturaufgabe den Menülink Zugehöriges Element **Change-Anforderungen** aus, um alle dem Datensatz zugeordneten Change-Anforderungen anzuzeigen.

Alternativ können Sie in der klassischen Umgebung zu navigieren **Selfservice** > **Meine Anforderungen**. Nachdem Sie den Change gesendet haben und er implementiert ist, wird die Korrekturaufgabe automatisch in den StatusGelöst verschoben, wenn die Statussynchronisierung aktiviert ist. Weitere Informationen zu Status und Statussynchronisierung in Change-Anforderungen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe.

Teilen Sie eine Korrekturaufgabe in in IT Remediation Workspace

Identifizieren Sie in einer Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) eine Teilmenge der Datensätze, und erstellen Sie eine neue Korrekturaufgabe dafür.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Sie können einzelne Datensätze auf der Registerkarte Übersicht einer Korrekturaufgabe auswählen und in eine neue Korrekturaufgabe verschieben.

Anwendungsfälle für die Aufteilung von Datensätzen (VITs, AVITs, CVITs oder CTRs) aus vorhandenen Korrekturaufgaben in neue Aufgaben können die folgenden Beispiele umfassen:

- Sie möchten eine Change-Anforderung oder Change-Anforderungen für eine aufgeteilte Aufgabe erstellen.
- Sie möchten eine aufgeteilte Aufgabe einem anderen Benutzer in Ihrer Zuweisungsgruppe zuweisen.
- Sie fordern eine Zurückstellung oder eine Ausnahme für eine aufgeteilte Aufgabe an, da Sie wissen, dass einige Schwachstellen in bestimmten Configuration Items (CIs) nicht bis zum Zieldatum behoben werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu Change-Anforderungen und zur Aufteilung von Korrekturaufgaben in der klassischen Umgebung und für Versionen von Vulnerability Response vor v15.0 finden Sie unter Teilen Sie eine Korrekturaufgabe auf.

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Öffnen Sie eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) auf der Homepage oder der Listenseite.
3. Wählen Sie auf der Registerkarte Übersicht die Datensätze (VITs, AVITs, CVITs oder CTRs) aus, die Sie in eine neue Korrekturaufgabe verschieben möchten.
4. Klicken Sie auf **Aufgabe aufteilen**.
5. Im angezeigten Dialogfeld wird die Anzahl der Datensätze (VITs, AVITs, CVITs oder CTRs) angezeigt, die Sie aus der Liste ausgewählt haben.
6. Klicken Sie erneut **auf Aufgabe aufteilen**.
   Es wird eine Bestätigungsmeldung mit einem Link zur neuen Korrekturaufgabe angezeigt.

   Alternativ können Sie den Bedingungsgenerator verwenden, um Datensätze (VITs, AVITs, CVITs oder CTRs) zu filtern.
7. Suchen Sie eine Korrekturaufgabe, die Sie aufteilen möchten.
8. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite **auf Aufgabe aufteilen**.
   Nach einigen Minuten wird der Bedingungsgenerator angezeigt.
9. Verwenden Sie im angezeigten Modal den Bedingungsgenerator, um die Teilmenge der Datensätze (VITs, AVITs, CVITs oder CTRs) zu identifizieren, die bis einer neuen Korrekturaufgabe hinzufügen sollen.
10. Klicken Sie auf **Aufgabe aufteilen**.
    Wenn eine Meldung angezeigt wird, dass keine Datensätze Ihren Bedingungen entsprechen, müssen Sie Ihre Kriterien anpassen und erneut **auf Aufgabe aufteilen** klicken. Bearbeiten Sie das Feld Kurzbeschreibung nach Bedarf. Dieses Feld kann Ihnen helfen, Ihre neue Korrekturaufgabe zu finden, nachdem sie erstellt wurde.

    Wenn Datensätze Ihren Bedingungen entsprechen, wird die Anzahl der übereinstimmenden Datensätze in einer Nachricht angezeigt.
11. **Wahlweise:** Klicken Sie auf den Link **Vorschauelemente,** um die Datensätze anzuzeigen, die Ihren Filterbedingungen entsprechen.
    Die neue Korrekturaufgabe wird als neue Registerkarte angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an

Geben Sie eine falsch positive Anforderung für ein angreifbares Host-Element (VIT), ein angreifbares Anwendungselement (AVIT), ein angreifbares Container-Element (CVIT) oder eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) in IT Remediation Workspacean. Ein falsch positives Ergebnis ist ein Zustand, bei dem ein Scanner aufgrund von Situationen wie einer falschen Klassifizierung, einer falschen Logik oder eines Algorithmus im Scanner fälschlicherweise meldet, dass im System eine Schwachstelle vorhanden ist.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Anfordern eines falsch positiven Ergebnisses für eine Reihe von Testergebnissen finden Sie unter Fordern Sie ein falsch positives Ergebnis für eine Reihe von Testergebnissen an.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie das Listensymbol ( ).
3. Wählen Sie die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) oder das angreifbare Element (VIT, AVIT oder CVIT) aus.
4. Wählen Sie **Als Falsch positiv markieren**aus.
5. Geben Sie Informationen zur Anforderung ein.
6. Wählen Sie **Genehmigung anfordern**.
7. Stellen Sie dem Genehmiger zusätzliche Informationen zu Ihrer Anforderung, und wählen Sie **Absenden**aus.

Hinweis:
Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn im Formular „Konfiguration der Ausnahmeverwaltung“ das **Kontrollkästchen Fragebogen zum Markieren von falsch positiv** aktivieren aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren Sie die Ausnahmeverwaltung für Vulnerability Response,Konfigurieren Sie die Ausnahmeverwaltung für Application Vulnerability Response, Konfigurieren Sie die Ausnahmeverwaltung für Container Vulnerability Responseund Konfigurieren Sie die Ausnahmeverwaltung für Konfigurations-Compliance.

Ergebnisse

Der Status des angreifbaren Elements (VIT, AVIT oder CVIT) oder der Korrekturaufgabe (VUL, AVUL oder CVUL) wechselt zu „Wird überprüft“.

Ihre Anforderung wird zur Genehmigung übermittelt, und der Genehmiger erhält eine E-Mail-Benachrichtigung zu Ihrer Anforderung.

Sie erhalten eine E-Mail-Benachrichtigung, wenn Ihre Anforderung genehmigt oder abgelehnt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Navigieren Sie im Arbeitsbereich für IT-Nachbesserungen auf der Seite Liste zu **Ausnahmeanforderungen** > **Meine Anforderungen** und öffnen Sie den entsprechenden Status-Change-Genehmigungsdatensatz (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Datensatz (VIT, AVIT oder CVIT)	Korrekturaufgabe (VUL, AVUL, CVUL oder CRG)
Genehmigt	Der Status des Datensatzes ändert sich in Geschlossen mit Grund als Falsch positiv.	Der Status der Korrekturaufgabe geht in „Geschlossen“ mit dem Grund „Falsch positiv“ über. Für den Status wird entsprechend ein Rolldown für die Datensätze in der Korrekturaufgabe durchgeführt. Navigieren Sie zur Registerkarte Details einer Korrekturaufgabe, und legen Sie im Feld **Bis** bei Bedarf das Ablaufdatum für falsch positive Meldungen fest. Die Korrekturaufgabe wird nach dem angegebenen Datum in den Status „Offen“ versetzt, und für den Status wird ein Rolldown zu den Testergebnissen durchgeführt.
Abgelehnt	Der Status des Datensatzes ändert sich nicht.	Der Status der Korrekturaufgabe und ihrer Datensätze werden auf den vorherigen Status zurückgesetzt.

Im **Aktivitätenstrom** eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow der falsch positiven Anforderung anzeigen.

Zugehörige Informationen

Falsch positiv – Übersicht

Fordern Sie ein falsch positives Ergebnis für eine Reihe von Testergebnissen an

Lösen Sie eine falsch positive Anforderung für eine Reihe von Testergebnissen innerhalb einer Korrekturaufgabe in IT Remediation Workspaceaus.

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Bedingungen müssen erfüllt sein, damit Sie für eine Reihe von Testergebnissen in einer Korrekturaufgabe ein falsch positives Ergebnis anfordern können:

- Version 22.0 von Vulnerability Response muss installiert sein.
- Mindestens ein ausgewähltes Testergebnis muss sich im Status „Aktiv“ befinden
- Die Korrekturaufgabe muss mindestens zwei Testergebnisse aufweisen
- Mindestens ein Testergebnis ist nicht ausgewählt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vulc.remediation_owner

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie das Listensymbol ( ) aus.
3. Wählen Sie auf der Seite „Liste“ die Korrekturaufgabe Konfigurations-Compliance aus.
4. Wählen Sie in der zugehörigen Liste „Übersicht“ auf der Registerkarte „Testergebnisse“ die Testergebnisse aus, die Sie als falsch positiv markieren möchten.
5. Klicken Sie auf der Registerkarte Konfigurationstestergebnisse auf die Schaltfläche **Als falsch positiv markieren**.
6. Geben Sie im angezeigten Dialogfeld Informationen zur Anforderung ein, und wählen Sie **Genehmigung anfordern**aus.
7. Beantworten Sie im Modal „Fragebogen ausfüllen“ die Fragen, um dem Genehmiger zusätzliche Informationen über Ihre Anforderung zu geben, und wählen Sie **Absenden**aus.

Hinweis:
Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn im Formular „Konfiguration der Ausnahmeverwaltung“ das **Kontrollkästchen Fragebogen zum Markieren von falsch positiv** aktivieren aktiviert ist. Weitere Informationen zur Konfiguration von Fragebogen finden Sie unter Konfigurieren Sie die Ausnahmeverwaltung für Konfigurations-Compliance.

Ergebnisse

Die ausgewählten Testergebnisse werden in eine neue Korrekturaufgabe verschoben, und Ihre Anforderung wird zur Genehmigung übermittelt. Die Aufgabennummer wird im **Aktivitätenstrom** der alten Korrekturaufgabe angezeigt. Der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

Sie erhalten eine E-Mail-Benachrichtigung über die Genehmigung oder Ablehnung Ihrer Anforderung. Im **Aktivitätenstrom** eines Testergebnisses oder einer Korrekturaufgabe können Sie den gesamten Workflow der falsch positiven Anforderung anzeigen.

Nächste Maßnahme

1. Navigieren Sie in IT Remediation Workspaceauf der Seite Liste zu **Ausnahmeanforderungen** > **Meine Anforderungen**.
2. Öffnen Sie den entsprechenden Datensatz für die Statusänderungsgenehmigung (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Der Status der neuen Korrekturaufgabe wechselt in „Geschlossen“ mit dem Grund „Falsch positiv“.
Abgelehnt	Der Status der neuen Korrekturaufgabe ändert sich in Offen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Nachdem die Anforderung genehmigt wurde, navigieren Sie zur Registerkarte Details der neuen Korrekturaufgabe, und legen Sie im Feld **Bis** bei Bedarf das Ablaufdatum für falsch positive Meldungen fest.

   Die Korrekturaufgabe wird nach dem angegebenen Datum in den Status „Offen“ zurückversetzt, und der Status wird auf die Testergebnisse heruntergerollt.

Fordern Sie eine Ausnahme in an IT Remediation Workspace

Fordern Sie eine Ausnahme für das angreifbare Element des Hosts (VIT), das angreifbare Element der Anwendung (AVIT), das angreifbare Element des Containers (CVIT) und die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) von IT Remediation Workspacean.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird
Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Oder Sie stellen fest, dass eine Korrekturaufgabe bis zu ihrem Zieldatum nicht gelöst werden kann. Wenn Ihre Nachbesserung einer veröffentlichten Richtlinie, einem Standard oder einer Leitlinie für das Schwachstellenmanagement oder der Sicherheit nicht entspricht, können Sie eine Ausnahme anfordern.

Sie können bei IT Remediation Workspace, die Ihnen zugewiesen sind, Ausnahmen für Korrekturaufgaben (VUL, AVUL, CVUL oder CRG) und angreifbare Elemente (VIT, AVIT oder CVIT) anfordern.

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Ab Version 18.0können Sie Ausnahmen für angreifbare Elemente in der Anwendung und für angreifbare Container-Elemente anfordern.

Weitere Informationen zum Anfordern von Ausnahmen in der klassischen Umgebung finden Sie unter Fordern Sie eine Ausnahme für eine Korrekturaufgabe an.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie das Listensymbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie in der Liste der Korrekturaufgaben eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) oder einen Datensatz (VITs, AVITs oder CVITs), für die Sie eine Ausnahme anfordern möchten.
4. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite **auf Ausnahme anfordern**.
5. Geben Sie im angezeigten Dialogfeld das Enddatum für die Ausnahme ein, wählen Sie einen Grund aus der Liste aus, und fügen Sie alle weiteren erforderlichen Informationen hinzu.
6. Klicken Sie auf **Ausnahme anfordern**.
7. Beantworten Sie im Modal **„Fragebogen ausfüllen“** die Fragen, und klicken Sie auf **Absenden**.

Hinweis:
Das Modal **„Fragebogen ausfüllen“** wird nur angezeigt, wenn im Formular **„Konfiguration der Ausnahmeverwaltung“** das Kontrollkästchen **Fragebogen zum Anfordern einer Ausnahme aktivieren** aktiviert ist.

In einer Nachricht wird angezeigt, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde.

Eine Ausnahmeanforderung für eine Korrekturaufgabe wird mit einem standardmäßigen, zweistufigen Genehmigungsworkflow genehmigt. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der Ebene 2 gesendet.

- Die Korrekturaufgabe oder der Korrekturdatensatz wechselt in den Status „Wird überprüft“, während die Ausnahmeanforderung geöffnet ist.
- Die Korrekturaufgabe oder der Korrekturdatensatz wechselt in den Status „Zurückgestellt“, wenn die Anforderung genehmigt wird.
- Der Ausnahmeanforderungsdatensatz (VCA#) wird geschlossen, nachdem Ihre Ausnahmeanforderung genehmigt wurde.

Um den Status Ihrer Genehmigungsanforderungen anzuzeigen, klicken Sie unter „Ausnahmeanforderungen“ auf der Listenseite auf **Meine Anforderungen**. Die Nummer für die Anforderung (VCA#) wird angezeigt, wenn Sie den Datensatz oder die Korrekturaufgabe aus der Liste öffnen.

- Wenn die Anforderung abgelehnt wird, zeigt der Anforderungsdatensatz (VCA#) in der Spalte Genehmigungsstatus in der Listenansicht unter Meine Anforderungen **den Wert Abgelehnt an**.
- Sie müssen eine neue Ausnahmeanforderung übermitteln, wenn Sie dieses Element dennoch zurückstellen möchten.

Ausnahme anfordern mit GRC: Richtlinien- und Compliance-Management in IT Remediation Workspace

Fordern Sie eine Richtlinienausnahme für das angreifbare Element des Hosts (VIT), das angreifbare Element der Anwendung (AVIT), das angreifbare Element des Containers (CVIT) oder die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) von IT Remediation Workspacean.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.remediation_owner für angreifbare Host-Elemente (VITs)
- sn_vul.app_security_Champion für angreifbare Elemente in der Anwendung (AVITs)
- sn_vul_container.remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.remediation_owner für Konfigurationstestergebnisse (CTRs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie ab v19.0
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie im Anwendungsnavigator das Listensymbol ( ).
3. Wählen Sie auf der Seite „Liste“ unter „Angreifbare Host-Elemente“, „Angreifbare Anwendungselemente“, „Angreifbare Container-Elemente“ oder „Korrekturaufgaben“ (VUL, AVUL, CVUL oder CRG) den Datensatz aus, für den Sie eine Ausnahme anfordern möchten.
   Der von Ihnen ausgewählte Datensatz muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
4. Wählen Sie die Schaltfläche **Ausnahme anfordern** aus.
5. Füllen Sie die Felder des Formulars aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Formularfelder „Ausnahme anfordern“ für Richtlinienausnahmen.
6. Wählen Sie **Ausnahme anfordern**aus.
7. Beantworten Sie im Modal „Fragebogen ausfüllen“ die Fragen, um zusätzliche Informationen zu Ihrer Anforderung bereitzustellen, und wählen Sie **Absenden aus**.

   Hinweis:
   Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn die Fragebogendetails der jeweiligen Integrationsregistrierung hinzugefügt werden.

   Es wird eine Meldung angezeigt, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde.

   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Korrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an

Fordern Sie eine Risikominderung für ein angreifbares Host-Element oder eine Korrekturaufgabe in IT Remediation Workspacean.

Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Ab v21.0 von Vulnerability Responsekönnen Sie eine Risikominderung nur für die folgenden Elementeanfordern:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine Korrekturaufgabe kann nur dann werden , wenn alle ihre angreifbaren Elemente dem dem gleichen Common Vulnerability Eintrag (CVE) zugeordnet sind, unabhängig davon, ob die Risikominderung für CVEs aktiviert ist.
- Eine Drittpartei (TPE), für die die Risikominderung aktiviert ist.

Hinweis:
Die Ausgleichssteuerungen sind nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie das Listensymbol ( ) aus.
3. Öffnen Sie auf der Listenseite ein angreifbares Host-Element oder eine Korrekturaufgabe.
4. Wählen Sie das Symbol Weitere Optionen und dann **Ausnahme anfordern**aus.
5. Füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.
   Eine Beschreibung der Feldwerte finden Sie unter Formular „Ausnahme anfordern “ für Risikominderung.
6. Wählen Sie **Ausnahme anfordern**aus.
7. Wenn das Modal „Fragebogen ausfüllen“ angezeigt wird, beantworten Sie die Fragen, um zusätzliche Informationen zu Ihrer Anforderung bereitzustellen, und wählen Sie **Absenden**aus.

   Hinweis:
   Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn für den Fragebogen die Ausnahmeverwaltung aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren Sie die Ausnahmeverwaltung für Vulnerability Response.

Ergebnisse

Es wird eine Meldung angezeigt, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde. An den Genehmiger wird eine Benachrichtigung über Ihre Anforderung gesendet.

- Wenn Sie eine Zurückstellung und Risikominderung anfordern:
  - Für Zurückstellung und Risikominderung werden Change-Genehmigungen mit zwei Status (VCA#) erstellt.
  - Der Status des Datensatzes ändert sich in Wird überprüft.
- Wenn Ihre Anforderung nur der Risikoreduzierung dient:
  - Eine Status-Change-Genehmigung (VCA#) wird erstellt.
  - Der Status ändert sich nicht.

Bei Genehmigung oder Ablehnung Ihrer Anforderung erhalten Sie eine Benachrichtigung. Weitere Informationen zum Genehmigungsprozess finden Sie unter Genehmigen Sie Anforderungen in, oder lehnen Sie sie ab Vulnerability Manager Workspace.

Weitere Informationen dazu, wie das **Bis-Datum für Risikominderung** für eine Korrekturaufgabe und ein angreifbares Element aktualisiert wird, wenn eine Risikominderungsanforderung genehmigt wird, finden Sie unter Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Ausgleichssteuerungen zur Risikoreduzierung verstehen

Risikominderung für ein CVE oder TPE aktivieren oder deaktivieren

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie bei Bedarf erneute Scans von IT Remediation Workspace in Ihrem Now Platform.

Durch erneute Scans können Sie überprüfen, ob durch Ihre Nachbesserungsaktivitäten, Patches und andere Aktionen bestimmte Schwachstellen in Ihren Configuration Items (CIs) erfolgreich behoben wurden.

Erneutes Scannen wird für die folgenden Integrationen in IT Remediation Workspaceunterstützt. Weitere Informationen finden Sie in den folgenden Themen:

- Scannen Sie Qualys angreifbare Elemente aus den Arbeitsbereichen Vulnerability Response erneut
- Scannen Sie Rapid7 angreifbare Elemente aus den Arbeitsbereichen Vulnerability Response erneut
- Scannen Sie die angreifbaren Elemente Tenable.io und Tenable.sc aus den Arbeitsbereichen Vulnerability Response erneut

Erforderliche Rolle: sn_vul.remediation_owner für IT Remediation Workspace.

Scannen Sie Qualys angreifbare Elemente aus den Arbeitsbereichen Vulnerability Response erneut

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie bei Bedarf in Qualys in Ihrer Instanz von IT Remediation Workspace erneut Scans im Produkt Now Platform.

Vorbereitungen

Informationen zum erneuten Scannen für das Produkt Qualys aus der klassischen Umgebung finden Sie unter Initiieren Sie den erneuten Scan für Qualys Vulnerability Integration.

Die Qualys -Scanner sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die Schaltfläche **Erneut scannen** nicht verfügbar.

Um diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin zu aktivieren:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in den Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Einrichten des Scanners Qualys finden Sie unter Richten Sie Scanner-Appliances ein und Erweiterte Konfigurationen und Änderungen Qualys ..

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben, deren Quelle das Produkt Qualys ist, aus dem IT Remediation Workspace in Ihrem Now Platforminitiieren.
- In einem Korrekturaufgabendatensatz kann sich der Datensatz in einem beliebigen anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Qualys stammen.
- Um im Arbeitsbereich für IT-Korrekturen erneut Scans aus Datensätzen zu angreifbaren Elementen und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen sein.

Erforderliche Rollen:

- sn_vul.remediation_owner für IT Remediation Workspace.
- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin aus dem Arbeitsbereich des Schwachstellenmanagers.

Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, das Ihnen zugewiesen wurde, und öffnen Sie es.

   Hinweis:
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle diesem Datensatz zugeordneten VIs gescannt.

2. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.
3. Wählen Sie im Modal „Erneut scannen“ ein Optionsprofil aus.
   Ein Optionsprofil ist erforderlich, wenn Sie einen Qualys -Scan von Ihrem Now Platform® aus initiieren. Optionsprofile enthalten Qualys Scan-Einstellungen.
4. Klicken Sie im Modal Erneut scannen **auf Erneutes Scannen anfordern**.
   Die Meldung Die Scan-Anforderung wird verarbeitet wird angezeigt.
5. Klicken Sie in der Nachricht auf den Link **Status anzeigen,** um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCan#) wird angezeigt. Unterhalb des Datensatz-Headers mit der Scan-Nummer zeigen die zugehörigen Elementlisten die folgenden Informationen an:

   - In der Liste Details werden die Scan-Nummer des übergeordneten Scans, die Scannerquelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt Scan-Zusammenfassung an.
   - In der Liste „Scans“ werden untergeordnete Scans und deren Status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, ändert sich der Status des übergeordneten Scans in Abgeschlossen.
   - Die Liste „Quelle“ zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die zugehörige Schwachstelle, den Status des VI und seinen Nachbesserungsstatus an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt).

Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde.

Alle AEs, die in den Status „Geschlossen“/„Behoben“ übergingen oder übergehen werden, werden mit dem nächsten geplanten Import der Qualys Integrationen importiert.

Scannen Sie Rapid7 angreifbare Elemente aus den Arbeitsbereichen Vulnerability Response erneut

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie bei Bedarf im -Arbeitsbereich für IT-Fehlerkorrekturen in Ihrer -Instanz Now Platform erneut Scans im Produkt Rapid7.

Vorbereitungen
Informationen zum erneuten Scannen für das Produkt aus der klassischen Umgebung finden Sie unter Initiieren Sie den erneuten Scan für die Rapid7 Vulnerability Integration. Dieses Thema enthält auch Informationen zum Planen von Prüfungen mit den Integrationsparametern in der Integrationsinstanz Rapid7.

Die Rapid7 -Scanner sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die die Anwendung Rapid7 als Quelle haben, ist die Schaltfläche **Erneut scannen** nicht verfügbar.

Um diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin zu aktivieren:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in den Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben, deren Quelle das Produkt Rapid7 InsightVM ist, aus dem IT-Korrekturarbeitsbereich in Ihrem Now Platforminitiieren.
- In einem Korrekturaufgabendatensatz kann sich der Datensatz in einem beliebigen anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Rapid7 stammen.
- Um im Arbeitsbereich für IT-Korrekturen erneut Scans aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen werden.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.remediation_owner für den Arbeitsbereich „IT-Korrektur“.
- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin aus dem Arbeitsbereich des Schwachstellenmanagers

Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, das Ihnen zugewiesen wurde, und öffnen Sie es.

   Hinweis:
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle diesem Datensatz zugeordneten VIs gescannt.

2. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.
3. Klicken Sie im modalen Fenster „Erneutes Scannen bestätigen **“ auf Erneutes Scannen anfordern**. Die Meldung Die Scan-Anforderung wird verarbeitet wird angezeigt.
4. Klicken Sie in der Nachricht auf den Link **Status anzeigen,** um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCan#) wird angezeigt. Unterhalb des Datensatz-Headers mit der Scan-Nummer zeigen die zugehörigen Elementlisten die folgenden Informationen an:

   - In der Liste Details werden die Scan-Nummer des übergeordneten Scans, die Scannerquelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt Scan-Zusammenfassung an.
   - In der Liste „Scans“ werden untergeordnete Scans und deren Status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, ändert sich der Status des übergeordneten Scans in Abgeschlossen.
   - Die Liste „Quelle“ zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die zugehörige Schwachstelle, den Status des VI und seinen Nachbesserungsstatus an.

   Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt).

   Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde.

   Alle AEs, die in den Status „Geschlossen“/„Behoben“ übergingen oder übergehen werden, werden mit dem nächsten geplanten Import der Rapid7 Integrationen importiert.

Scannen Sie die angreifbaren Elemente Tenable.io und Tenable.sc aus den Arbeitsbereichen Vulnerability Response erneut

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie bei Bedarf im Arbeitsbereich für IT-Fehlerkorrekturen in Ihrer Instanz Now Platform erneut Scans in den -Produkten Tenable.io und Tenable.sc.

Vorbereitungen

Informationen zum erneuten Scannen für die -Produkte Tenable.io und Tenable.sc aus der klassischen Umgebung von Vulnerability Responsefinden Sie unter Initiieren Sie den erneuten Scan für die Tenable.sc -Integration und Initiieren Sie den erneuten Scan für die Tenable.io -Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um erneut Scans von Ihrem Now Platformdurchzuführen, benötigen Sie Ihre Tenable-Anmeldeinformationen. Weitere Informationen zum Einrichten der Scanner Tenable.io und Tenable.sc und zum Importieren Ihrer Anmeldeinformationen aus Tenable finden Sie unter Konfigurieren Sie die Tenable-Schwachstellen-Integration mit dem Setup-Assistenten.

- Sie können bei Bedarf im IT-Korrekturarbeitsbereich in Ihrem Now Platformbei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben mit dem Produkt Tenable.io oder Tenable.sc als Quelle initiieren.
- In einem Korrekturaufgabendatensatz kann sich der Datensatz in einem beliebigen anderen Status als **Geschlossen**befinden, und alle zugehörigen VIs müssen aus dem Produkt Tenable.io oder Tenable.sc stammen.
- Um erneute Scans in IT Remediation Workspace aus Datensätzen zu angreifbaren Elementen und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen werden.

Erforderliche Rollen:

- sn_vul.remediation_owner für IT Remediation Workspace
- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin aus dem Arbeitsbereich des Schwachstellenmanagers

Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, das Ihnen zugewiesen wurde, und öffnen Sie es.

   Hinweis:
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle diesem Datensatz zugeordneten VIs gescannt.

2. Klicken Sie oben rechts in einem Datensatz **auf Erneut scannen**.
   Sie werden aufgefordert, die Instanz(en) für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind diejenigen, die von den Integrationen zum Scannen von Anmeldeinformationen Tenable.io für und Tenable.sc importiert wurden.
3. Klicken Sie im modalen Fenster auf das Suchsymbol.

   Verwenden Sie im angezeigten modalen Element Scan-Anmeldeinformationen auswählen die Filter in den Spaltenüberschriften, um den Namen, die Instanz und/oder die Instanzen sowie die Anmeldeinformationstypen auszuwählen, die Sie verwenden möchten.

   Weitere Informationen finden Sie in der folgenden Tabelle.

4. Klicken Sie im aktualisierten Modal „Erneut scannen **“ auf Erneutes Scannen anfordern**.
   Die Meldung Die Scan-Anforderung wird verarbeitet wird angezeigt.
5. Klicken Sie in der Nachricht auf den Link **Status anzeigen,** um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCan#) wird angezeigt. Unterhalb des Datensatz-Headers mit der Scan-Nummer zeigen die zugehörigen Elementlisten die folgenden Informationen an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In der Liste Details werden die Scan-Nummer des übergeordneten Scans, die Scannerquelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt Scan-Zusammenfassung an.
- In der Liste „Scans“ werden untergeordnete Scans und deren Status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, ändert sich der Status des übergeordneten Scans in Abgeschlossen.
- Die Liste „Quelle“ zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die zugehörige Schwachstelle, den Status des VI und seinen Nachbesserungsstatus an.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums (je nachdem, was zuerst eintritt).

Die Zeitüberschreitung beendet den Scanvorgang nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung des Status des erneuten Scannens beendet hat, und nicht darauf, wann der tatsächliche erneute Scan beendet wurde.

Alle VIs, die in den Status „Geschlossen“/„Behoben“ übergegangen sind oder in den Status „Geschlossen“ übergehen werden, werden mit dem nächsten geplanten Import der Tenable.io - oder Tenable.sc -Integrationen importiert.

IT Remediation Workspace Referenzinformationen

Die folgenden Themen enthalten Links und Referenzinformationen sowie Felddaten für die Formulare und Datensätze in IT Remediation Workspace.

[store-future: BEGIN review]

Umleitung zu IT Remediation Workspace aus dem Menü „Alle“.

Wenn ein Administrator die Systemeigenschaft *sn_vul_cmn_ws.navigate_to_workspace* auf truesetzt, werden Sie zu IT Remediation Workspace weitergeleitet, sobald Sie im Menü **Alle** die vordefinierten Filterlinks in den Modulen Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Konfigurations-Compliance auswählen.

Es wird zur Listenseite von umgeleitet IT Remediation Workspace

Als Benutzer mit der Rolle sn_vul.remediation_owner, wenn Sie im Modul Vulnerability Response die folgenden Links für vordefinierte Filter auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response**, diese Links werden auf der Listenseite von IT Remediation Workspacegeöffnet:

- Korrekturaufgaben: „Mir zugewiesen“ und „Meine Gruppen zugewiesen“.
- Angreifbare Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Bibliotheken – NVD, CWE und Drittpartei
- Lösungen: Alle, Ersatz durch höchste Priorität und Mit angreifbaren Elementen
- Meine Genehmigungen

Als Benutzer mit der Rolle sn_vul_container.remediation_owner, wenn Sie im Modul Container Vulnerability Response die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Container Vulnerability Response**, diese Links werden auf der Listenseite von IT Remediation Workspacegeöffnet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Container-Korrekturaufgaben: „Aktiv“, „Mir zugewiesen“, „Meinen Gruppen zugewiesen“ und „Alle“.
- Angreifbare Container-Elemente – Mir zugewiesen und Meinen Gruppen zugewiesen
- Meine Genehmigungen
- Bibliotheken – NVD, CWE und Drittpartei

Als Benutzer mit der Rolle sn_vul.app_security_Champion, wenn Sie im Modul Application Vulnerability Response die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Application Vulnerability Response**, diese Links werden auf der Listenseite von IT Remediation Workspacegeöffnet:

- Korrekturaufgaben: „Aktiv“, „Mir zugewiesen“, „Meinen Gruppen zugewiesen“ und „Alle“.
- Angreifbare Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Meine Genehmigungen
- Bibliotheken – NVD, CWE und Drittpartei
- Penetrationstest-Bewertungsanforderungen: „Aktiv“, „Alle mir zugewiesen“ und „Meine Gruppen zugewiesen“.
- Penetrationstestergebnisse – Aktiv, Validierung ausstehend, Mir zugewiesen, Meiner Gruppe zugewiesen und Alle

Als Benutzer mit der Rolle sn_vulc.remediation_owner, wenn Sie im Modul Konfigurations-Compliance die folgenden Links für vordefinierte Filter auswählen, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance**, diese Links werden auf der Listenseite von IT Remediation Workspacegeöffnet:

- Korrekturaufgaben: „Meine offenen Aufgaben“, „Alle offenen Aufgaben“, „Mehrere Zurückstellungen“ und „Alle Aufgaben“.
- Tests
- Testgruppen
- Unterstützungsdaten – Autorisierende Quellen und Technologien

[End]

Formularfelder für Change-Anforderung erstellen

Die folgende Tabelle zeigt die Felder und ihre Beschreibung im Formular „Change-Anforderung erstellen“.

Feld	Beschreibung
Änderungstyp	Normal: Dies ist der Standardwert. Standard: Es werden zwei zusätzliche Felder angezeigt: Standard-Change-Kategorie – Wählen Sie eine Kategorie aus der Liste aus Standard-Change-Vorlage: Wählen Sie in der Auswahlliste eine Vorlage aus, die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	für diese Change-Anforderung verwendet werden soll Notfall: Kritische Priorität
CIs zu Change-Anforderung hinzufügen	Der Standardwert ist aktiviert. Wenn diese Option aktiviert ist, fügt die Change-Anforderung alle Konfigurationselemente (Configuration Items, CI) hinzu, die zu aktiven angreifbaren Elementen in dieser Korrekturmaßnahme gehören.
Priorität	Der Standardwert ist „Hoch“. Wählen Sie eine Priorität aus der Liste aus.
Zuweisungsgruppe	Die Zuweisungsgruppe wird standardmäßig aus dem Überwachungsthema übernommen. Klicken Sie auf das Suchsymbol, und wählen Sie im modalen Fenster eine andere Zuweisungsgruppe aus.
Geplantes Enddatum	Klicken Sie auf das Kalendersymbol, um ein geplantes Enddatum auszuwählen.
Zugewiesen an	Der aktuelle Benutzer ist standardmäßig der Korrekturaufgabe zugewiesen. Klicken Sie auf das Suchsymbol, und wählen Sie im modalen Fenster einen anderen Anwender aus.
Kurzbeschreibung	Die Kurzbeschreibung stammt aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten.
Beschreibung	Die Beschreibung stammt aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten.
Begründung	Begründung aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten.
Implementierungsplan	Vorausgefüllt mit Informationen zur bevorzugten Lösung, falls verfügbar. Zeigen Sie die Lösung an, oder geben Sie einen Begründungsplan ein.

Zugehörige Informationen

Erstellen Sie eine Change-Anforderung im IT Remediation Workspace

Formularfelder „Ausnahme anfordern“ für Richtlinienausnahmen

Die folgende Tabelle zeigt die Felder, die Sie im Formular „Ausnahme anfordern“ für Richtlinienausnahmen ausfüllen müssen.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Richtlinie	Richtlinie für Schwachstellenmanagement, für die Sie eine Ausnahme anfordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahme anfordern“. (Fortsetzung)

Feld	Beschreibung
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von Zurückgestellt in Offen wechselt. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf den Wert im Feld **Maximale Ausnahmedauer (Tage)**, den Sie für die Richtlinie festgelegt haben, nicht überschreiten. Weitere Informationen finden Sie unter Richtlinie erstellen .
Grund	Grund für das Anfordern einer Ausnahme.
Begründung	Details zum Grund, aus dem diese Ausnahme angefordert wird. Dieses Feld muss vom Besitzer der Remediation ausgefüllt werden.

Zugehörige Informationen

Ausnahme anfordern mit GRC: Richtlinien- und Compliance-Management in IT Remediation Workspace

Formular „Ausnahme anfordern “ für Risikominderung

Die folgende Tabelle zeigt die Felder, die Sie im Formular „Ausnahme anfordern“ für Risikominderungsanforderungen ausfüllen müssen.

Formular „Ausnahme anfordern“.

Feld	Beschreibung
Grund	Grund für Ihre Ausnahmeanforderung. Wählen Sie *die vorhandene ausgleichende Steuerung* für die Risikominderungsanforderung aus. Informationen zum Hinzufügen neuer Gründe finden Sie unter Definieren Sie die Zuordnung von Richtliniengrund.
Zurückstellungsanforderung	Stellen Sie den Datensatz zurück. Dieses Feld ist standardmäßig ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahme anfordern“. (Fortsetzung)

Feld	Beschreibung
	Hinweis: Dieses Feld wird nur angezeigt, wenn im Feld **Grund** die Option *Ausgleichende Steuerung vorhanden* ausgewählt ist.
Risikominderungsanforderung	Ermöglicht das Anfordern der Reduzierung der Risikopunktzahl. **Hinweis:** Diese Checkbox wird nur angezeigt, wenn im Feld **Grund** die Option *Ausgleichende Steuerung vorhanden* ausgewählt ist.
Aktuelle Risikobewertung	Aktueller Schweregrad des Risikos. **Hinweis:** Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Risikominderung anfordern** aktiviert ist.
Gewünschte Risikobewertung	Neue Risikobewertung, die Sie dem Datensatz zuweisen möchten. Die höchste Risikopunktzahl in diesem Risikobewertungsbereich wird auf den Datensatz angewendet, wenn Ihre Anforderung genehmigt wird. **Hinweis:** Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Risikominderung anfordern** aktiviert ist.
Wählen Sie Ausgleichssteuerungen	Grund für Ihre Anforderung zur Reduzierung der Risikobewertung.
Bis	Datum, an dem die Zurückstellungs- oder Risikominderungsanforderung abläuft. Wenn die Ausnahmeanforderung abläuft: • Der Datensatz wird in den Status Offen zurückversetzt. • Die Ausgleichssteuerungen laufen ab. • Die berechnete Punktzahl ersetzt eine reduzierte Punktzahl.
Hinweise zur Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an

Erkunden Sie den Arbeitsbereich der Schwachstellenbewertung

Der Arbeitsbereich der Schwachstellenbewertung wurde für den Schwachstellenereignismanager zur Durchführung einer Bewertung des Gefahrenpotenzials und zur proaktiven Verwaltung kritischer Schwachstellenereignisse entwickelt, insbesondere während kritischer Schwachstellenereignisse wie Zero-Day-Ereignisse.

Nachdem eine kritische Schwachstelle identifiziert wurde, können Manager für Schwachstellenereignisse die potenziellen Auswirkungen und Risiken bewerten, die mit der Schwachstelle verbunden sind. Die Analysten können die betroffenen Systeme, Anwendungen oder Netzwerkkomponenten analysieren, um den Schweregrad und mögliche Angriffsvektoren innerhalb der Organisation zu verstehen.

Der Arbeitsbereich der Schwachstellenbewertung enthält:

Seite „Bewertung des Gefahrenpotenzials“.

Bietet detaillierte Einblicke in die Assets, die Schwachstellen und angreifbare Software ausgesetzt sind. Die Funktionalität zur Bewertung des Gefahrenpotenzials bietet:

- Einblick in betroffene Assets für Schwachstelle und betroffene Software
- Fähigkeit, eigenständige Bewertungen für ein einzelnes CVE oder eine angreifbare Software durchzuführen
- Sichtbarkeit für betroffene Assets für bekanntermaßen ausgenutzte Schwachstellen-CISA-CVEs
- Sichtbarkeit des Risikos durch zusätzliches Discovery-Modell und zusätzliche Assets.
- Fähigkeit zum Erstellen angreifbarer Elemente

Seite „Schwachstellenbewertung“.

Seite „Schwachstellenbewertung“, auf der Sie mit dem Workflow „Schwachstellen-Krisenmanagement“ Schwachstellen-Krisenereignisse von der Bewertung bis zur Lösung behandeln können. Mit dem Workflow können Sie Schwachstellenereignisse von Interesse nachverfolgen, das damit verbundene Risiko analysieren, eine Bewertung des Gefahrenpotenzials für mehrere Bestände durchführen (z. B. Softwareinstallationsbestand) und sie als Krise für ein erhöhtes Reaktionsengagement deklarieren. Anschließend können Sie den Schwachstellenbewertungsdatensatz einem schwerwiegenden Security Incident zuordnen und das Security Incident Response-Team in die Lage versetzen, auf die Krise zu reagieren.

- Erstellen und ändern Sie Schwachstellenbewertungen für kritische Schwachstellenereignisse
- Zeichnen Sie die Schlüsselattribute der Schwachstelle auf, um das Risiko zu berechnen
- Führen Sie eine Schwachstellenbewertung durch, um das Ausmaß und die Priorität des Gefahrenpotenzials zu bestimmen
- Deklarieren Sie die Schwachstellenbewertung als kritisches Ereignis
- Ordnen Sie die Schwachstellenbewertung einem schwerwiegenden Security Incident zu, indem Sie die Schwachstellenbewertung mit einem schwerwiegenden Security Incident verknüpfen, vorschlagen oder heraufstufen.

Automatische Übersetzung

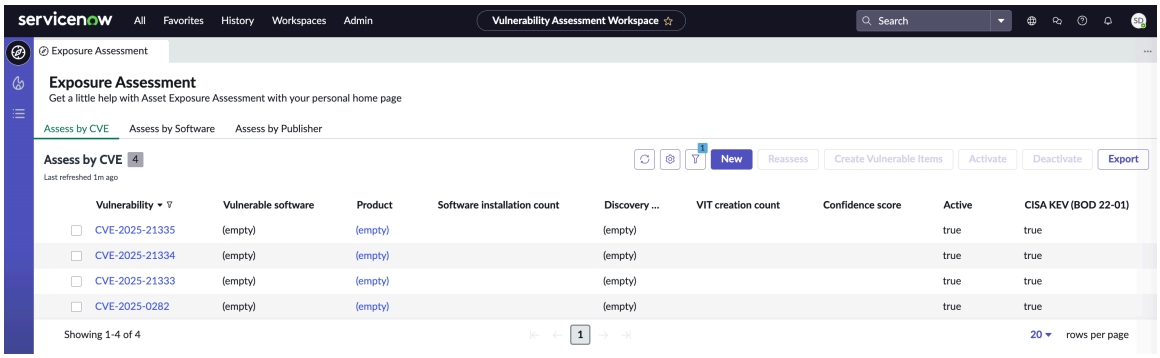
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen-Seite

Die Listenseite umfasst eine Bibliothek mit:

- CVEs
- TPEs
- CWEs

Die folgende Abbildung zeigt die Startseite des Arbeitsbereichs für die Schwachstellenbewertung.



Gefahrenbewertung erkunden

Die Bewertung des Gefahrenpotenzials verwendet das Framework der Common Platform Enumeration (CPE), das Teil des Common Vulnerabilities and Exposures-Systems (CVE) ist, um das Schwachstellenrisiko Ihrer Assets durch Schwachstellensoftware zu bewerten. Diese Bewertung wird mit einem Software-Discovery-Modell durchgeführt.

Durch die Verwendung eines Abgleichalgorithmus werden die relevanten CPEs verknüpft und dem Software-Discovery-Modell zugeordnet, wodurch potenzielle Risiken identifiziert werden können.

Sie können die Bewertung des Gefahrenpotenzials durch CVE oder Software verwenden, um das Risiko potenzieller Schwachstellen für die folgenden Szenarien zu identifizieren:

- Schwachstellen, die von herkömmlichen Scannern möglicherweise nicht identifiziert werden können
- Zero-Day-Schwachstellen vor dem Scanner stellen die Signatur für die Erkennung von Schwachstellen bereit

Eine Risikobewertung bietet eine Frühwarnung, um diese Schwachstellen zu beheben und die Reife des Schwachstellenmanagementprogramms zu verbessern.

Voraussetzungen für die Bewertung des Gefahrenpotenzials

Verfügbare Versionen

Anwendung	Version
Plugin „Schwachstellen-Krisenmanagement“.	1.0
Vulnerability Response	20.0
Vulnerability Response mit NVD	1.3
Vulnerability Response integration with CISA	1.2

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen (Fortsetzung)

Anwendung	Version
Vulnerability Response Integration with NVD **Hinweis:** Weitere Informationen finden Sie unter Grundlagen zu NVD-Integrationen.	1.3
Software Asset Management	Software Asset Management Foundation-Plugin oder Software Asset Management Professional Plugin

Anwendungsfälle

Beispiele dafür, wie die Organisation für Schwachstellenanalysten den Arbeitsbereich „Bewertung des Schwachstellenrisikos“ verwenden würde, finden Sie in den folgenden Anwendungsfällen.

Bewertungstyp	Verwenden
Nach CVE bewerten	Bewerten Sie Schwachstellen anhand von CVE, um ein vollständiges Verständnis der Auswirkungen und des Gefahrenpotenzials der betroffenen Systeme zu erhalten, indem Sie die Daten Software Asset Management von (SAM) und Discovery verwenden. Führen Sie sofortige Korrekturmaßnahmen durch, indem Sie manuelle VITs erstellen und den Korrekturbesitzern zuweisen. Die Bewertung durch CVEs ist vorteilhaft, da Scanner möglicherweise nicht alle betroffenen Systeme erkennen, während Discovery normalerweise den Großteil der Software auf der Angriffsoberfläche identifiziert.
Nach Software bewerten	Bewerten Sie die Auswirkungen auf die Software, wenn CVE nicht verfügbar ist, um die Anzahl der CIs zu ermitteln, auf denen die Software installiert ist. Durch die Bewertung nach Software können Sie proaktiv auf Zero-Day-Schwachstellen oder kritische Schwachstellen reagieren, indem Sie eine manuelle VIT erstellen und dem Korrekturverantwortlichen zuweisen, bevor sie offiziell veröffentlicht werden oder bevor Scanner sie identifizieren.
Nach Herausgeber bewerten	Bewerten Sie Schwachstellen durch einen Softwareanbieter, um die Auswirkungen und die Gefährdung betroffener Systeme für die vom Lieferanten innerhalb eines Zeitrahmens veröffentlichten CVEs zu verstehen. Die Bewertung nach Herausgeber hilft Ihnen, das Lieferantenrisiko und kritische Schwachstellen zu bewerten und ermöglicht so eine proaktive Korrektur.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kompatibilität und Systemanforderungen

Die Anwendung Vulnerability Response ist unter ServiceNow Storeverfügbar. Die Anwendung ITSM Software Asset Management (com.snc.asset_management) ist für das Modul „Risikobewertung“ erforderlich. Diese Anwendung verwaltet alle Ihre Assets und Softwarelizenzen, und die Version SAM Foundation dieser Anwendung ist Teil der Anwendung Vulnerability Response, die Sie von ServiceNow Storeherunterladen.

Wichtig:
Die Anwendung der Bewertung des Gefahrenpotenzials funktioniert mit den folgenden Plugins:

- Software Asset Management Foundation-Plugin (com.snc.sams)
- Software Asset Management Professional (com.snc.pa.samp)
- Software Asset Management-Plugin (com.snc.software_asset_management)

Um sicherzustellen, dass die Anwendung SAM Foundation auf Ihrer Instanz installiert ist, navigieren Sie zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie nach com.snc.asset_management. Wenn die Anwendung nicht installiert ist, wählen Sie **Installieren**aus. Da die Anwendung Schwachstellenbewertung Bewertung des Gefahrenpotenzials Zugriff auf die Asset-Daten in Ihrer Instanz Now Platform® erfordert, müssen die Asset-Verwaltungsanwendungen über Referenzdaten verfügen. Die Tabelle „Software-Discovery-Modelle“ (cmdb_sam_sw_discovery_model) und die Softwareinstallationen (cmdb_sam_sw_install) erfordern Daten.

Passende Algorithmusfelder für Software-Discovery-Modelle

Mit der Anwendung Software Asset Management Professional können Sie ein Software-Discovery-Modell bearbeiten, um erkannte Software, die nicht vollständig normalisiert wurde (teilweise normalisiert, vom Herausgeber normalisiert oder Übereinstimmung nicht gefunden), manuell im Formular „Software-Discovery-Modelle“ zu normalisieren, damit sie abgeglichen werden kann. Ab Version 20.0 von Vulnerability Response wird das normalisierte Discovery-Modell von Software Asset Management Professionalunterstützt. Die folgenden Felder werden für den Übereinstimmungsalgorithmus für Software-Discovery-Modelle verwendet.

CPE (Softwaremodell)	SAM – Grundlagen	SAM Professional
Lieferant	Primärer Schlüssel	Primärer Schlüssel
Produkt	Anzeigename	Anzeigename
Version	Erkannter Herausgeber	Erkannter Herausgeber
Edition	Erkanntes Produkt	Erkanntes Produkt
	Erkannte Version	Erkannte Version
		Normalisierter Herausgeber
		Normalisiertes Produkt
		Normalisierte Version

Hinweis:
Die Anwendung „SAM Professional“ ist nicht Teil des Kernprodukts Vulnerability Response von ServiceNow Store und erfordert ein separates Abonnement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaft

Um die von CISA ausgenutzten Schwachstellen automatisch für die Bewertung des Gefahrenpotenzials zu verarbeiten, legen Sie die Systemeigenschaft *sn_vul_analyst.enable_exposure_for_cisa* auf *true*fest. Der Standardwert ist *false*.

Geplante Aufgaben

Im Folgenden finden Sie die geplanten Aufgaben.

Name der geplanten Aufgabe	Beschreibung
Überprüfen Sie das potenzielle Schwachstellenrisiko	Verarbeitet die Delta-CVEs, die Software und die Delta-Installationen, um das Risiko zu erhalten. **Hinweis:** Diese regelmäßige Aufgabe wird alle 12 Stunden ausgeführt. Sie wird über einen längeren Zeitraum ausgeführt als die anderen geplanten Aufgaben.
Von CISA ausgenutztes CVE in Risikokonfiguration einfügen	Bei Bedarf Fügt die CISA-CVEs in die Risikokonfigurationstabelle ein, um das Risiko zu berechnen.
Führen Sie eine Bewertung des Gefahrenpotenzials für konfigurierte CVEs durch	Bei Bedarf Berechnet das Risiko für alle CVE-Datensätze in der Risikokonfigurationstabelle.
Führen Sie ein Softwarerisiko aus	Bei Bedarf Berechnet das Risiko für alle Softwaredatensätze in der Risikokonfigurationstabelle.

Wichtige Begriffe

- **Konfidenzpunktzahl:** Eine Konfidenzpunktzahl ist ein Maß für die Zuverlässigkeit der Bereitstellung einer Empfehlung für ein Feld. Je höher die Punktzahl, desto zuverlässiger ist die Empfehlung. Beispielberechnungen finden Sie unter Beispiel für die Berechnung der Konfidenzpunktzahl.
- **Anzahl Softwareinstallationen:** Anzahl der von der Schwachstelle betroffenen Software-Assets.
- **Softwaremodell:** Softwaremodell, das dem Produkt zugeordnet ist. Führen Sie einen Drilldown im Softwaremodell durch, um das Softwaremodellergebnis anzuzeigen. Weitere Informationen finden Sie unter Software Asset Management Foundation plugin discovery models and software installations .

Das Feld **Anzahl Softwareinstallationen** gibt die Gesamtzahl der Softwareinstallationen an, unabhängig von ihrem aktiven oder inaktiven Status im Discovery-Modell. Ab v22.0 von Vulnerability Responsewurde die neue Systemeigenschaft *sn_vul.filter_inactive_sw_installs*eingeführt, um zu bestimmen, ob inaktive Softwareinstallationen für die Bewertung des Gefahrenpotenzials[store-future: BEGIN review] oder für das Schwachstellen-Krisenmanagement (VCM)[End]herausgefiltert werden sollen. Standardmäßig ist die Eigenschaft im Basissystem aktiviert. Wenn der Filter aktiviert ist, werden nur aktive Installationen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Feld **Discovery-Modell** zeigt speziell die Anzahl der aktiven Softwareinstallationen an, da die inaktiven basierend auf dem Standardfilter active=true in der Tabelle „Software-Discovery-Modell“ herausgefiltert werden. Die Anzahl in diesem Feld muss mit der gefilterten Anzahl übereinstimmen, die im Feld **Anzahl der Softwareinstallationen** angezeigt wird. Die Anzahl im Feld **Softwareinstallation** wird beibehalten, auch wenn Sie die Systemeigenschaft aktualisieren. Um die aktualisierte Anzahl zu erhalten, müssen Sie die geplanten Aufgaben *`Run exposure assessment for configured CVEs`* und *`Run software exposure that updates the count`*ausführen.

Risikobewertung durch CVE

Die Bewertung des Gefahrenpotenzials verwendet Gemeinsame Schwachstellen und Risiken (Common Vulnerabilities and Exposures, CVEs), um das Risiko Ihrer Assets mithilfe des Software-Discovery-Modells zu bewerten. Sie können die Bewertung des Gefahrenpotenzials durch CVE verwenden, um das Risiko potenzieller Schwachstellen zu identifizieren.

Informationen zur Bewertung des Gefahrenpotenzials durch CVE finden Sie unter:

- CVEs hinzufügen, um das Gefahrenpotenzial zu bewerten
- Erstellen Sie VIs für CVEs für die Bewertung des Gefahrenpotenzials
- Aktivieren oder deaktivieren Sie CVEs für die Bewertung des Gefahrenpotenzials
- Exportieren Sie betroffene CIs für die Bewertung des Gefahrenpotenzials
- Beispiel für die Berechnung der Konfidenzpunktzahl

CVEs hinzufügen, um das Gefahrenpotenzial zu bewerten

Fügen Sie Common Vulnerabilities and Exposures (CVE) zur Risikokonfigurationsliste von CVEs in der Bewertung des Gefahrenpotenzials hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie **Hinzufügen**.
3. Wählen Sie im Dialogfeld „CVE hinzufügen“ die CVEs aus, die Sie der Liste hinzufügen möchten, und wählen Sie die Option **Hinzufügen** aus.
   CVEs, die bereits in der Liste enthalten sind, werden nicht erneut hinzugefügt. Die übrigen werden der Liste der CVEs hinzugefügt.

   Hinweis:
   Wählen Sie das Filtersymbol, um zur **Ansicht Erweitert** zu navigieren, und geben Sie die CVEs an, die Sie anzeigen möchten.

4. So bewerten Sie die Auswirkungen der bereits in der Liste enthaltenen CVEs:

   a. Aktivieren Sie die Checkbox der CVEs, die Sie neu bewerten möchten.

   b. Wählen Sie die Schaltfläche **Erneut bewerten** aus.
   Die aktualisierten Details werden in den entsprechenden Spalten angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie VIs für CVEs für die Bewertung des Gefahrenpotenzials

Erstellen Sie angreifbare Elemente (VIs) auf der Seite „Risikobewertung“. Manager für Schwachstellenereignisse analysieren dann diese Liste der VIs und empfehlen Lösungen und Patches, die dem IT-Team helfen, diese Schwachstellen zu patchen.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Warum und wann dieser Vorgang ausgeführt wird
Nachdem das Risiko bewertet wurde, wird die Liste für die potenzielle Bewertung im Datensatz der Risikobewertung mit der Anzahl der Konfigurationselemente (Configuration Items, CI) angezeigt. Sie können die Datensätze auswählen und in der Listenaktion **Angreifbare Elemente erstellen** wählen, um angreifbare Elemente (VIs) für die CIs zu erstellen, in denen sich die angreifbare Software befindet, und für Common Vulnerabilities and Exposures (CVEs). VIs werden im Hintergrund erstellt. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Nachdem die Elemente erstellt wurden, können Sie zur VI-Tabelle navigieren, um die erstellten Datensätze anzuzeigen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie die erforderlichen CVEs und anschließend die Option **Angreifbare Elemente erstellen** aus.
3. Wählen Sie im Dialogfeld „Angreifbare Elemente erstellen“ die Option **Angreifbare Elemente erstellen aus**.
4. Wählen Sie den Link **Status anzeigen** aus, um den Status des Hintergrundauftrags anzuzeigen, der zum Erstellen der AEs verwendet wird.

Aktivieren oder deaktivieren Sie CVEs für die Bewertung des Gefahrenpotenzials

Für die Delta-Verarbeitung eines CVE können Sie es aktivieren und so der aktiven Liste der CVEs hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Hinweis:
Ab Version 4.0.1 der Bewertung des Schwachstellenrisikos wird der Risikobewertungsdatensatz für dieses CVE automatisch als inaktiv markiert, wenn ein Common Vulnerability Eintrag (CVE) nicht aktualisiert wurde oder für das in den letzten 30 Tagen angreifbare Elemente (VITs) erstellt wurden. Sie können diese Datensätze jedoch manuell aktivieren oder deaktivieren. Darüber hinaus wird die regelmäßige Aufgabe `Check potential vulnerability exposure` kontinuierlich ausgeführt, um nach solchen CVEs zu suchen und sie als inaktiv zu kennzeichnen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie die erforderlichen aktiven CVEs aus, und wählen Sie die Option **Deaktivieren** aus.
   Die CVEs sind deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Um Software zu aktivieren, führen Sie den gleichen Vorgang aus und wählen Sie die Option **Aktivieren** aus.

3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte Aktiv anzuzeigen.

Exportieren Sie betroffene CIs für die Bewertung des Gefahrenpotenzials

Sie können die Liste der betroffenen Assets für ein neues CVE nachverfolgen, indem Sie die Configuration Items (CIs), die sich auf einen Datensatz der Offenlegungsbewertung beziehen, in eine Excel-Tabelle exportieren. Dieses Blatt kann verwendet werden, um die Details und Besitzer von Assets freizugeben und Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten.
   Die Registerkarte „Softwareinstallationen“ enthält die aktiven CIs, die sich auf den Softwaredatensatz beziehen. Diese CIs werden in der Spalte **Installiert auf** gespeichert.
3. Wählen Sie die Option **Exportieren**.
4. Wählen Sie im Dialogfeld „Exportieren“ Dateityp und Liefertyp aus, um die zugehörigen CIs zu exportieren.
5. Wählen Sie die Option **Exportieren**.

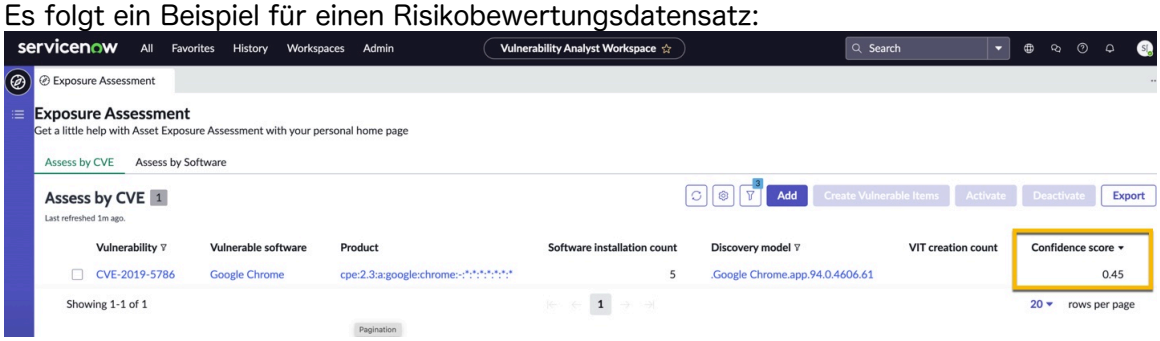
Beispiel für die Berechnung der Konfidenzpunktzahl

Beispiel für die Berechnung der Konfidenz für eine Zero-Day-Schwachstelle basierend auf den zugehörigen CVE-Informationen (Common Vulnerabilities and Exposures).

Im Folgenden finden Sie ein Beispiel für die Berechnung der Vertrauensbewertung aus den Informationen der Common Platform Enumeration (CPE) von **CVE-2019-5786**.

Hinweis:
Um die CPEs anzuzeigen, können Sie die Spalte „Schwachstelle“ nach Schwachstelle gruppieren. Weitere Informationen zum Anzeigen der Details zu angreifbarer Software finden Sie unter Zeigen Sie Details zu angreifbarer Software an.

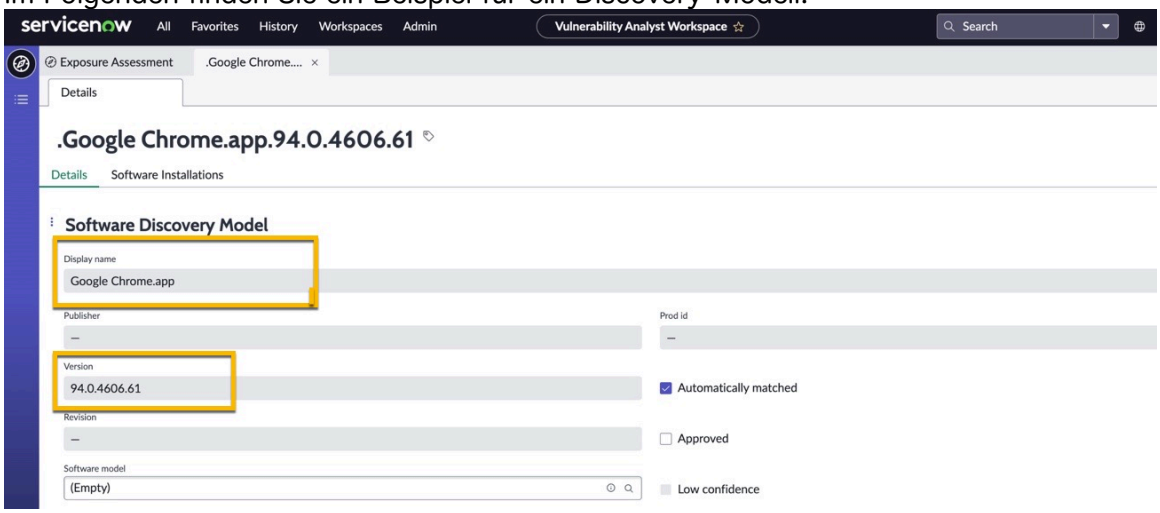
Es folgt ein Beispiel für einen Risikobewertungsdatensatz:



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden finden Sie ein Beispiel für ein Discovery-Modell:



Berechnung der Vertrauensbewertung

Der Konfidenzpunktzahlbereich ist 0–1. Basierend auf den CPE-Informationen wird die Vertrauensbewertung mit der folgenden Formel berechnet:

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

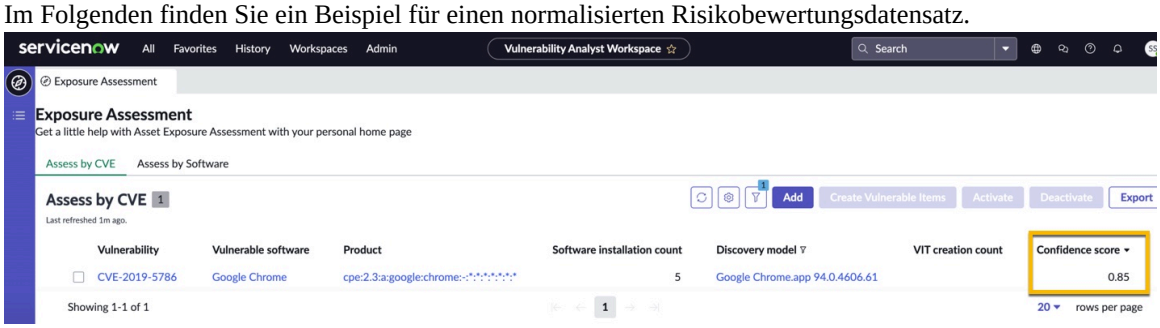
```
.45
```

> **Hinweis:**
> Informationen zu den zur Berechnung der Konfidenzpunktzahl verwendeten Werten finden Sie unter Referenztabellen der Konfidenzpunktzahl für die Bewertung des Gefahrenpotenzials.

Die Vertrauensbewertung wird berechnet, wenn das Softwaremodell mit dem normalisierten Discovery-Modell abgeglichen wird

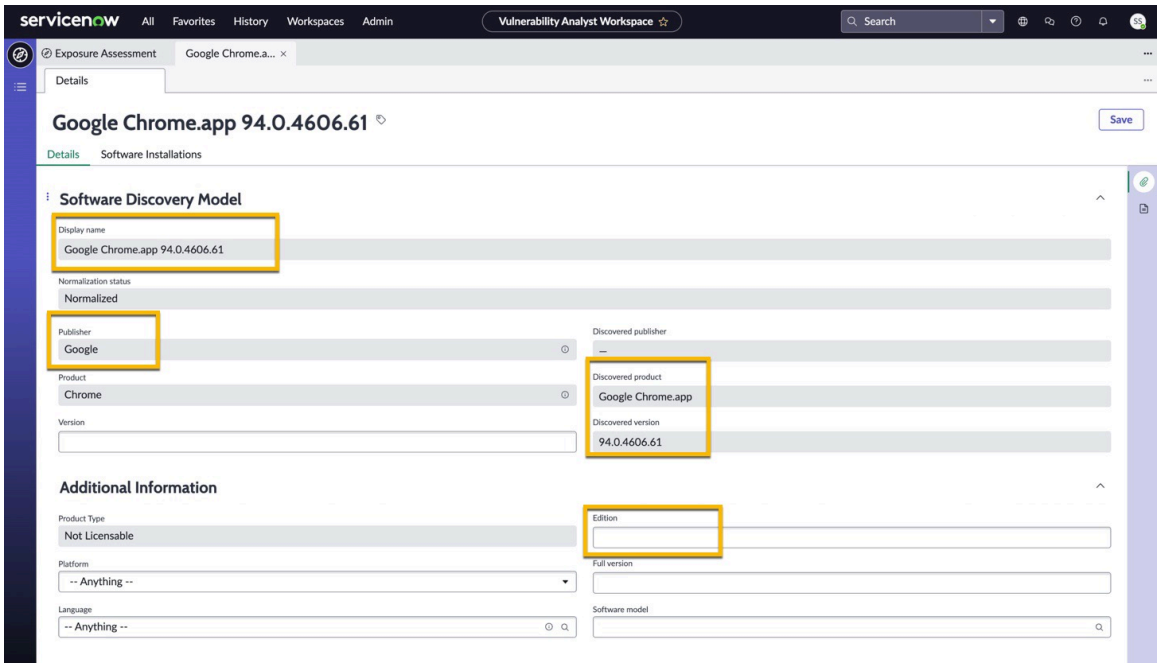
Wenn Sie das normalisierte Discovery-Modell verwenden, bieten die zusätzlichen für das Software-Discovery-Modell verfügbaren Informationen eine verbesserte Vertrauensbewertung. Es folgt die Beispielberechnung:

Im Folgenden finden Sie ein Beispiel für einen normalisierten Risikobewertungsdatensatz.



Im Folgenden finden Sie ein Beispiel für ein normalisiertes Discovery-Modell.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




```
((BASE SCORE) + (publisher score) + (product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

Hinweis:
Informationen zu den zur Berechnung der Konfidenzpunktzahl verwendeten Werten finden Sie unter Referenztabellen der Konfidenzpunktzahl für die Bewertung des Gefahrenpotenzials.

Zeigen Sie Details zu angreifbarer Software an

Zeigen Sie die Details der angreifbaren Software an, in diesem Fall Google Chrome. Es wird mit dem Discovery-Modell und der Common Platform Enumeration (CPE) abgeglichen. Diese CPE-Version wirkt sich auf alle Google Chrome-Versionen aus.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren Sie zu **Alle**, und geben Sie *sn_vul_software.LIST*ein.
2. Suchen Sie in der Liste der angreifbaren Software nach **cpe:2.3:a:google:Chrome:-:*:*:*:*:*:*:*,** um die Informationen anzuzeigen.

Referenztabellen der Konfidenzpunktzahl für die Bewertung des Gefahrenpotenzials

Zur Berechnung der Konfidenzpunktzahl verwendete Referenzwerte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenztabellen

Referenztabelle für die Berechnung der Konfidenzpunktzahl

Verwundbares Softwaresegment	Discovery-Modellsegment	Punktzahl	Segment für exakte Übereinstimmung des Discovery-Modells	Punktzahl für genaue Übereinstimmung
Herausgeber	Anzeigename	15	Herausgeber	5
Modell	Anzeigename	15	Modell	5
Version	Anzeigename	10	Version	5
Edition	Anzeigename	3	Normalisierte Edition	2
Anzeigename	Anzeigename	10	Anzeigename	5

Zusammenfassungstabelle der Vertrauensbewertung

Punktzahl	Wert
Summe aller Punktzahlen	75
Basispunktzahl **Hinweis:** Mindestpunktzahl, die allen übereinstimmenden Discovery-Modellen zugewiesen wird.	25
Gesamtpunktzahl	100

Bewertung des Gefahrenpotenzials durch Software

Bewertung des Gefahrenpotenzials für Zero-Day-Schwachstellen, wenn Common Vulnerabilities and Exposures (CVE) für das Asset oder Configuration Item nicht verfügbar ist. Es verwendet die Softwareinformationen, um das Gefahrenpotenzial mithilfe des Software-Discovery-Modells zu bewerten.

Informationen zur Bewertung des Gefahrenpotenzials mit Software finden Sie unter:

- Fügen Sie Software für die Bewertung des Gefahrenpotenzials hinzu
- Erstellen Sie VIs für Software für die Bewertung des Gefahrenpotenzials
- Aktivieren oder deaktivieren Sie Software für die Bewertung des Gefahrenpotenzials
- Exportieren Sie betroffene CIs für Software im Arbeitsbereich der Schwachstellenbewertung

Fügen Sie Software für die Bewertung des Gefahrenpotenzials hinzu

Fügen Sie dem Modul „Risikobewertung“ eine neue Software hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten** > **Hinzufügen**.
2. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Herausgeber	Herausgeber der Software.
Produkt	Produktname der Software.
Version	Version des Softwareprodukts.
Edition	Edition der Software.

Hinweis:
Wenn Sie versuchen, das Risiko für Software hinzuzufügen, die in der Tabelle mit dem Status „falsch“ vorhanden ist, wird kein doppelter Datensatz erstellt. Der Status der vorhandenen Software wird auf „wahr“ aktualisiert.

3. Wählen Sie die Option **Hinzufügen**.
4. So bewerten Sie die Auswirkungen der Software, die bereits in der Liste enthalten ist:
   a. Aktivieren Sie das Kontrollkästchen der Software, die Sie neu bewerten möchten.
   b. Wählen Sie die Schaltfläche **Erneut bewerten** aus.
   Die aktualisierten Details werden in den entsprechenden Spalten angezeigt.

Erstellen Sie VIs für Software für die Bewertung des Gefahrenpotenzials

Erstellen Sie angreifbare Elemente (VIs) auf der Seite „Risikobewertung“. Manager für Schwachstellenereignisse analysieren dann diese Liste der VIs und empfehlen Lösungen und Patches, die dem IT-Team helfen, diese Schwachstellen zu patchen.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**.
2. Wählen Sie die Datensätze aus, für die Sie AEs erstellen möchten.
3. Wählen Sie die Option **Angreifbare Elemente erstellen aus**.
4. Wählen Sie im Dialogfeld „Angreifbare Elemente erstellen“ aus:
   - Vorhandene Schwachstelle
   - Neue Schwachstelle
5. Wählen Sie die Option **Angreifbare Elemente erstellen aus**.

Aktivieren oder deaktivieren Sie Software für die Bewertung des Gefahrenpotenzials

Um die weitere Delta-Verarbeitung von Software zu stoppen, können Sie sie deaktivieren und so aus der aktiven Liste der Software entfernen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**.
2. Zum Deaktivieren wählen Sie die erforderliche aktive Software aus, und wählen Sie die Option **Deaktivieren** aus.
   Die Software ist deaktiviert.

   Hinweis:
   Um Software zu aktivieren, führen Sie den gleichen Vorgang aus und wählen Sie die Option **Aktivieren** aus.
3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte Aktiv anzuzeigen.

Exportieren Sie betroffene CIs für Software im Arbeitsbereich der Schwachstellenbewertung

Sie können die Liste der betroffenen Assets für neue Software nachverfolgen, indem Sie die Configuration Items (CIs), die sich auf einen Offenlegungsbewertungsdatensatz beziehen, in eine Excel-Tabelle exportieren. Dieses Blatt kann verwendet werden, um die Details und Besitzer von Assets freizugeben und Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten.
   Die Registerkarte „Softwareinstallationen“ enthält die aktiven CIs, die sich auf den Softwaredatensatz beziehen. Diese CIs werden in der Spalte **Installiert auf** gespeichert.
3. Wählen Sie die Option **Exportieren**.
4. Wählen Sie im Dialogfeld „Exportieren “ **Dateityp** und **Liefertyp** aus, um die zugehörigen CIs zu exportieren.
5. Wählen Sie die Option **Exportieren**.

Bewertung des Gefahrenpotenzials durch Herausgebersoftware

Bewerten Sie das Risiko für Zero-Day-Schwachstellen, wenn Common Vulnerabilities and Exposures (CVEs) für das Asset oder Configuration Item nicht verfügbar sind. Es verwendet die Softwareinformationen, um das Gefahrenpotenzial mithilfe des Software-Discovery-Modells zu bewerten.

Informationen zur Bewertung des Gefahrenpotenzials mit Software finden Sie unter:

- Fügen Sie Software eines Herausgebers für die Bewertung des Gefahrenpotenzials hinzu
- Erstellen Sie VIs für Software eines Herausgebers für die Bewertung des Gefahrenpotenzials
- Aktivieren oder deaktivieren Sie Software von einem Herausgeber für die Bewertung des Gefahrenpotenzials
- Exportieren Sie im Arbeitsbereich der Schwachstellenbewertung betroffene CIs für Software eines Herausgebers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Software eines Herausgebers für die Bewertung des Gefahrenpotenzials hinzu

Fügen Sie dem Risikobewertungsmodul Software von einem Herausgeber hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten** > **„Neu“**.
2. Wählen Sie im Fenster Neue Bewertung den Herausgeber aus, für den Sie die Bewertung durchführen möchten.
3. Wählen Sie ein Datum im Feld **CVE veröffentlicht von** aus.
   Wenn einer der Common Vulnerability-Einträge (CVE), die der Software zugeordnet sind, nach dem ausgewählten Datum geändert wird, wird diese Software für die Bewertung des Gefahrenpotenzials berücksichtigt.
4. Wählen Sie den Schweregrad des CVE im Abschnitt **„CVE-Schweregrad“** aus.
5. Wählen Sie **Bewertung starten aus**.
   Sobald der Auftrag abgeschlossen ist, werden die ausgewählten Datensätze erstellt.

Erstellen Sie VIs für Software eines Herausgebers für die Bewertung des Gefahrenpotenzials

Erstellen Sie angreifbare Elemente (VIs) auf der Seite „Bewertung des Gefahrenpotenzials“, um die Liste der VIs zu analysieren und Lösungen und Patches zu empfehlen, die dem IT-Team beim Patchen der Schwachstellen helfen können.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten**.
2. Wählen Sie die Datensätze aus, für die Sie AEs erstellen möchten.
3. Wählen Sie die Option **Angreifbare Elemente erstellen aus**.
4. Wählen Sie im Dialogfeld „Angreifbare Elemente erstellen“ aus:
   - Vorhandene Schwachstelle
   - Neue Schwachstelle
5. Wählen Sie die Option **Angreifbare Elemente erstellen aus**.

Aktivieren oder deaktivieren Sie Software von einem Herausgeber für die Bewertung des Gefahrenpotenzials

Aktivieren oder deaktivieren Sie Software von einem Herausgeber, um die Delta-Verarbeitung der Software zu stoppen und sie aus der Liste der aktiven Software zu entfernen.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten**.
2. Zum Deaktivieren wählen Sie die erforderliche aktive Software von einem Herausgeber aus, und wählen Sie die Option **Deaktivieren** unter der Schaltfläche **Erneut bewerten** aus.
   Der Herausgeber ist deaktiviert.

   Hinweis:
   Um die Software durch einen Herausgeber zu aktivieren, führen Sie den gleichen Vorgang aus und wählen Sie die Option **Aktivieren** aus.

3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte Aktiv anzuzeigen.

Exportieren Sie im Arbeitsbereich der Schwachstellenbewertung betroffene CIs für Software eines Herausgebers

Sie können die Liste der betroffenen Assets für neue Software nachverfolgen, indem Sie die Configuration Items (CIs), die sich auf einen Offenlegungsbewertungsdatensatz beziehen, in eine Excel-Tabelle exportieren. Dieses Blatt kann verwendet werden, um die Details und Besitzer von Assets freizugeben und Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten**.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten.
   Die Registerkarte „Softwareinstallationen“ enthält die aktiven CIs, die sich auf den Softwaredatensatz beziehen. Diese CIs werden in der Spalte **Installiert auf** gespeichert.
3. Wählen Sie die Option **Exportieren**.
4. Wählen Sie im Dialogfeld „Exportieren **“ Dateityp** und **Liefertyp** aus, um die zugehörigen CIs zu exportieren.
5. Wählen Sie die Option **Exportieren**.

Schwachstellenbewertung erkunden

Der Arbeitsbereich für die Schwachstellenbewertung wurde für den Schwachstellenereignismanager entwickelt, um ein Schwachstellenereignis zu erstellen und eine Schwachstellenbewertung durchzuführen, insbesondere während der Zero-Day-Schwachstellenanalyse.

Mit dem Schwachstellenbewertungs-Arbeitsbereich können Sie kritische Schwachstellen verwalten, z. B.:

- Zero-Day-Schwachstellen mit Schweregrad „Kritisch“ oder „Hoch“.
- Neue Bedrohungsinformationen für eine Schwachstelle identifiziert
- Schnelle Ausnutzung einer Schwachstelle mit Schweregrad „Kritisch“ oder „Hoch“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich für Schwachstellenbewertung und Krisenmanagement für Schwachstellen

Identifizieren und erstellen Sie als Schwachstellen-Ereignismanager einen Schwachstellen-Ereignisdatensatz für relevante Schwachstellen. Sobald Sie das angreifbare Ereignis erstellt haben, können Sie eine Risikobewertung durchführen, die Risikoattribute manuell aktualisieren und die Risikopunktzahl automatisch berechnen. Mit dem Schwachstellenbewertungs-Arbeitsbereich können Sie die folgenden Aktionen ausführen, um Schwachstellen-Krisenereignisse von der Grundlage bis zur Lösung zu behandeln.

- Erstellen Sie einen Schwachstellenbewertungsdatensatz
- Ändern Sie den Schwachstellenbewertungsdatensatz
- Führen Sie eine Schwachstellenbewertung durch
- Überprüfen Sie die Bewertungsdetails
- Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und eine Gefährdungsstufe zu
- Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu
- Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente
- Verknüpfen Sie den Schwachstellenbewertungsdatensatz mit einem schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidents

Voraussetzungen für die Schwachstellenbewertung

Verfügbare Versionen

Anwendung	Version
Plugin „Schwachstellen-Krisenmanagement“.	1.0
Vulnerability Response	20.0
Vulnerability Response mit NVD **Hinweis:** Weitere Informationen finden Sie unter Grundlagen zu NVD-Integrationen.	1.4.2
Vulnerability Response integration with CISA	1.2
Datenmodell für SBOM	1.1.2
Software Bill of Materials Zentral	2.0.2
Software Asset Management	Software Asset Management Foundation-Plugin oder Software Asset Management Professional Plugin
Management schwerwiegender Sicherheits-Incidents	2.2.5

Geplante Aufgaben

Im Folgenden finden Sie die geplanten Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name der geplanten Aufgabe	Beschreibung
Schwachstellenbewertung	Aktualisiert die Tabelle der betroffenen Konfigurationselemente und die Quelle des CI, wenn angreifbare Elemente (VITs oder AVITs) nach der Bewertung erstellt werden. **Hinweis:** Diese planmäßige Aufgabe wird täglich ausgeführt. Sie wird über einen längeren Zeitraum ausgeführt als die anderen geplanten Aufgaben.

Zugehörige Informationen

Schwachstellen-Krisenmanagement

Erstellen Sie einen Schwachstellenbewertungsdatensatz

Erstellen Sie Bewertungsdatensätze für Schwachstellen, die von Interesse sind. Nachdem Sie die Bewertung erstellt haben, können Sie eine erste Risikobewertung initiieren, den Datensatz manuell aktualisieren und die Risikopunktzahl automatisch berechnen.

Vorbereitungen

Sie müssen der Zuweisungsgruppe des Basissystem-Schwachstellenbewertungs-Ereignis-Managers angehören, um die mit der Schwachstellenbewertung verbundenen Aufgaben ausführen zu können. Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Schwachstellenbewertungsdatensatz für relevante Schwachstellen erstellen, indem Sie den Ereignisdatensatz entweder einem primären CVE oder einem betroffenen Produkt zuordnen.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie das Symbol **Schwachstellenbewertung**.
3. Wählen Sie **Neu**.
4. Geben Sie im Feld **Titel** einen entsprechenden Titel ein.
5. **Wahlweise:** Wählen Sie im Feld **Primäres CVE** ein primäres CVE aus, das dem neuen Bewertungsdatensatz zugeordnet werden soll.

   Hinweis:
   Alle vorläufigen Details im Bewertungsdatensatz werden basierend auf dem von Ihnen ausgewählten oder erstellten Produkt oder dem primären CVE, das Sie dem Datensatz zuordnen, ausgefüllt.

6. Wählen Sie **Absenden**.
   Der Schwachstellenbewertungsdatensatz mit dem von Ihnen eingegebenen Titel wird erstellt und auf einer neuen Registerkarte für Schwachstellenbewertungen angezeigt. Standardmäßig wird der Schwachstellenbewertungsdatensatz auf der Registerkarte **Details** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Standardmäßig werden die Details des zugeordneten/zugeordneten primären CVE angezeigt.

- Wenn während der Erstellung des Datensatzes für das Schwachstellenbewertungsereignis kein primäres CVE ausgewählt wird, wird ein Standarddatensatz erstellt.
- Wenn dem primären CVE CVEs zugeordnet sind, werden die zugehörigen CVEs auf der Registerkarte **„Schwachstelleneinträge“** eingetragen. Auf der Registerkarte **„Schwachstelleneinträge“** können Sie weitere zugeordnete CVEs hinzufügen.

7. Navigieren Sie zur Registerkarte **Betroffene Produkte**.

a. Wählen Sie **Neu**.

b. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Herausgeber	Herausgeber der Software. Das ist ein Pflichtfeld.
Produkt	Produktname der Software. Das ist ein Pflichtfeld.
Version	Version des Softwareprodukts.
Edition	Edition der Software.

Hinweis:
Wenn Sie versuchen, eine Schwachstelle für Software hinzuzufügen, die in der Tabelle mit dem Status „falsch“ vorhanden ist, wird kein doppelter Datensatz erstellt. Der Status der vorhandenen Software wird auf „wahr“ aktualisiert.

c. Wählen Sie **OK**.

8. Wählen Sie **Speichern**.

Aktualisieren Sie den Datensatz für das automatische Leeren der Schwachstellenbewertung

Aktualisieren Sie den Datensatz für das automatische Leeren der Schwachstellenbewertung.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Warum und wann dieser Vorgang ausgeführt wird
Im Basissystem ist der Aufbewahrungszeitraum für Schwachstellenbewertungsdatensätze auf 6 Monate festgelegt. Wenn ein Datensatz der Schwachstellenbewertung in den Status „Geschlossen“ versetzt wird, werden die Datensätze der Schwachstellenbewertung nur bis zum Ablauf des definierten Aufbewahrungszeitraums gespeichert. Die zugehörigen Datensätze dieser Bewertung werden nach 6 Monaten aus allen zugehörigen Tabellen entfernt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Automatisch entleeren**.
2. Öffnen Sie den Datensatz mit der Tabelle sn_vul_analyst_vulnerability_assessment.
3. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Option zum automatischen Leeren für den Schwachstellenbewertungsdatensatz zu aktivieren.
4. Klicken Sie auf **Aktualisieren**.

Ändern Sie den Schwachstellenbewertungsdatensatz

Aktualisiert den Datensatz der Schwachstellenbewertung nach seiner Erstellung. Basierend auf den Werten des Felds können Sie die Risikopunktzahlberechnen.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Warum und wann dieser Vorgang ausgeführt wird

Nachdem das primäre CVE zur Schwachstellenbewertung hinzugefügt wurde, wird der Datensatz in den Status Bewertung ausstehend verschoben. Sie können weitere zugehörige CVEs auf der Registerkarte **„Schwachstelleneinträge“**hinzufügen oder die von dieser Schwachstelle betroffenen Produkte auf der Registerkarte **„Betroffene Produkte“** hinzufügen. Sie können weitere Änderungen an den Feldern **Risikobewertung** vornehmen, und die **Risikopunktzahl** für den Bewertungsdatensatz wird automatisch entsprechend aktualisiert.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich der Schwachstellenbewertung** > **Schwachstellenbewertung**.
2. Aktualisieren Sie die Felder auf der Registerkarte **Details**.

Feld	Beschreibung
Titel	Titel, der den Datensatz des Schwachstellen-Ereignisses beschreibt.
Primäres CVE	Primäres CVE, das Sie dem Ereignisdatensatz zugeordnet haben.
Status	Aktueller Status des Ereignisdatensatzes.
Priorität	Priorität des Ereignisdatensatzes auf einer Skala von 1–5.
Warnungsquelle	Quelle des potenziellen Schwachstellen-Ereignisse.
Risikopunktzahl	Automatisch berechnete Risikopunktzahl. Standardmäßig nicht bearbeitbar.
Gefahrenpotenzial-Ebene	Die Gefährdungsstufe des Schwachstellenereignisses auf einer Skala von 1 bis 5.
Zuweisungsgruppe	Die Zuweisungsgruppe, der der Ereignisdatensatz zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugewiesen an	Der Benutzer, dem der Ereignisdatensatz zugewiesen ist.
Beschreibung	Detaillierte Beschreibung des Ereignisdatensatzes.

3. Navigieren Sie zur Registerkarte **Schwachstelleneinträge,** um zugeordnete oder zugehörige CVEs hinzuzufügen.
   a. Wählen Sie **Neu**.
   b. Suchen Sie im Feld **Schwachstelleneintrag** nach dem Datensatz.
   c. Wählen Sie den Schwachstellen-Datensatz aus, den Sie dem Bewertungsdatensatz zuordnen möchten.
   d. **Wahlweise:** Wählen Sie **Durchsuchen**, um eine Datei zu suchen und anzuhängen.
   e. Wählen Sie **Speichern**.
   Die von Ihnen ausgewählten Schwachstellen-Datensätze werden dem Bewertungsdatensatz hinzugefügt und auf der Registerkarte **Schwachstelleneinträge** angezeigt.
4. **Wahlweise:** Betroffene Produkte hinzufügen
5. Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu.
6. Ändern Sie die **Risikoattribute** für das primäre CVE, das dem Datensatz des Schwachstellenbewertungsereignisses zugeordnet ist.

Feld	Beschreibung
Speicherbeschädigung	Gibt an, ob dieser Ereignisdatensatz den Arbeitsspeicher beschädigen kann.
Ausführbarer Remotecode	Gibt an, ob die Remoteausführung von Code möglich ist.
Lokale Berechtigungsausweitung	Gibt an, ob eine lokale Schwachstelle bei der Berechtigungsausweitung vorhanden ist.
Nicht autorisierter Zugriff	Gibt an, ob eine Schwachstelle durch nicht autorisierten Zugriff vorhanden ist.
DDoS	Gibt an, ob das potenzielle Ereignis Distributed Denial of Service betreffen könnte.
Angriffskomplexität	Gibt die Komplexität des Anhangs an. Optionen sind Niedrig, Mittel oder Hoch.
Angriffsvektor	Gibt den potenziellen Pfad oder die Methode des Angriffs an. Optionen sind: Netzwerk, Angrenzendes Netzwerk, Lokal, Physisch, Keine.
Erforderliche Berechtigungen	Gibt die Berechtigungsebene an, die ein Angreifer zum Ausnutzen der Schwachstelle benötigt. Optionen sind Keine, Niedrig oder Hoch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwenderinteraktion	Gibt an, ob eine Benutzerinteraktion erforderlich ist, um die Schwachstelle auszunutzen.
Auswirkung auf die Vertraulichkeit	Gibt das Maß der potenziellen Auswirkung auf die Vertraulichkeit der Schwachstelle an. Optionen sind Keine, Niedrig oder Hoch
Umfangsänderung	Gibt an, ob sich der Umfang der Bewertung geändert hat.
Auswirkung auf die Verfügbarkeit	Gibt die potenziellen Auswirkungen auf die Verfügbarkeit einer erfolgreich ausgenutzten Missbrauchsschwachstelle an. Verfügbarkeit bezieht sich auf die Zugänglichkeit von Informationsressourcen. Optionen sind Keine, Niedrig oder Hoch
Auswirkung auf die Integrität	Gibt die potenziellen Auswirkungen auf die Integrität einer erfolgreich ausgenutzten Missbrauchsschwachstelle an. Integrität bezieht sich auf die Vertrauenswürdigkeit und garantierten Richtigkeit von Informationen. Optionen sind Keine, Niedrig oder Hoch
Korrekturstufe	Gibt den Status oder die Verfügbarkeit der Korrektur für die Schwachstelle an. Optionen sind Offizielle Korrektur, Temporäre Korrektur, Problemumgehung, Nicht verfügbar, Nicht definiert.
Reife des Exploit-Codes	Gibt die Wahrscheinlichkeit an, dass die Schwachstelle ausgenutzt wird, basierend auf dem aktuellen Status der Ausnutzungstechniken und der Codeverfügbarkeit. Optionen sind Nicht erprobt, Proof-of-Concept, Funktional, Hoch und Nicht definiert.
Berichtskonfidenz	Gibt an, wie sicher Sie sind, dass die Schwachstelle vorhanden ist.

Automatische Übersetzung

7. Geben Sie relevante Kommentare in das Feld **Verfassen** ein.
   - Geben Sie Ihre Arbeitsnotizen in das Feld **Arbeitsnotizen (privat)** ein.
   - Geben Sie Ihre Kommentare (für alle sichtbar) in das Feld **Kommentare** ein.
8. **Speichern Sie** den Bewertungsdatensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basierend auf den Aktualisierungen, die Sie an den **Risikoattributfeldern** für das primäre CVE oder das betroffene Produkt vorgenommen haben, das dem Bewertungsdatensatz zugeordnet ist, wird das Feld **Risikopunktzahl** automatisch aktualisiert.

Hinweis:
Um die Regeln oder Kriterien des Risikopunktzahl-Rechners des Basissystems zu ändern, navigieren Sie zu **Alle** > **Rechner für Schwachstellenbewertung** > **Risikorechner für Schwachstellenbewertung** > **Schwachstellenbewertung – Risikoregel**. Sie können Kriterien hinzufügen und die Gewichtung auf Feldebene bei Bedarf für vorhandene Kriterien ändern.

Nächste Maßnahme
Führen Sie eine erste Bewertung des Ereignisdatensatzes durch.

Löschen Sie zugeordnete CVEs oder betroffene Produkte aus dem Schwachstellenbewertungsdatensatz

Löschen Sie den Datensatz eines Schwachstellen-Ereignisses, wenn er nicht mehr benötigt wird.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Warum und wann dieser Vorgang ausgeführt wird
Sie können CVEs oder betroffene Produkte löschen, die dem Schwachstellenbewertungsdatensatz zugeordnet sind. Sie können Schwachstelleneinträge/zugehörige CVEs oder betroffene Produkte nur löschen, wenn sie sich im Status **„Neu“** oder **„Bewertung ausstehend“** befinden.

Prozedur
1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Schwachstellenbewertung**.
2. Wählen Sie den Schwachstellenbewertungsdatensatz aus.
3. Wählen Sie die Registerkarte **Schwachstelleneinträge** oder **Betroffene Produkte**.
4. Wählen Sie das zugeordnete CVE oder den betroffenen Produktdatensatz aus.
5. Wählen Sie **Löschen**.

Hinweis:
Die Schaltfläche **„Löschen“** wird für einen Bewertungsdatensatz nur angezeigt, wenn er sich im Status **„Neu“** oder **„Bewertung ausstehend“** befindet.

Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu

Fügen Sie zusätzliche Links und Informationen hinzu, die sich auf den Bewertungsdatensatz beziehen.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie den Bewertungsdatensatzeintrag aus.
3. Wählen Sie die Registerkarte **Zugehörige Links**.
4. Geben Sie eine relevante Beschreibung in das Feld **Beschreibung** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie die URL in das Feld **Link** ein.
6. Wählen Sie **OK**.
   Der zugehörige Link wird hinzugefügt und auf der Registerkarte Zugehörige Links aufgeführt.

Führen Sie eine Bewertung durch

Nachdem Sie den Schwachstellenbewertungsdatensatz erstellt und die Risikoattributfelder aktualisiert haben, führen Sie eine Bewertung des Ereignisdatensatzes aus.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Warum und wann dieser Vorgang ausgeführt wird
Führen Sie eine erste Bewertung durch, nachdem ein Ereignis für eine Schwachstelle von Interesse erstellt und festgestellt wurde, dass ein Risiko für Systeme und Daten darstellt. Der Zweck dieser Aktivität besteht darin, die Bedrohung weiter zu analysieren, indem die Risikobewertung mit einer eingehenden Bewertung des Gefahrenpotenzials aktualisiert wird.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Schwachstellenbewertung**.
2. Wählen Sie den relevanten Datensatz aus der Liste der Datensätze für Schwachstellenbewertungsereignisse aus.
3. Wählen Sie **Bewerten** aus, um die Schwachstellenbewertung auszuführen.
   Der Hintergrundauftrag Vulnerability Response – Schwachstellenbewertungsereignis verarbeiten wird initiiert, und es wird eine entsprechende Benachrichtigung angezeigt.
4. Wählen Sie in der Benachrichtigung **Status anzeigen,** um den Status des laufenden Auftrags anzuzeigen.
5. Wählen Sie **Speichern**.

   Auf der Registerkarte **Bewertungen** werden Bewertungsdetails angezeigt. Wenn die Bewertung verarbeitet wird, werden die VITs oder AVITs, die den angreifbaren Einträgen oder CVEs zugeordnet sind, auf der Registerkarte **Angreifbare Elemente** oder **Angreifbare Anwendungselemente** angezeigt.

Ergebnisse

- Angreifbare Elemente oder TPEs, die sich auf die zugeordneten CVEs beziehen, werden während der Bewertung abgerufen. Die CIs, die sich auf die angreifbaren Elemente beziehen, werden ebenfalls identifiziert und in der Tabelle Betroffene Konfigurationselemente angezeigt.
- Wenn die zugeordneten CIs in der betroffenen CI-Tabelle nicht vorhanden sind, werden die identifizierten CIs zur Tabelle hinzugefügt, und der Feldwert **Hat angreifbares Element** wird auf **true**festgelegt. Zudem wird der Wert des Felds **Quelle** auf Scanner festgelegt.
- Wenn das CI bereits in der betroffenen CI-Tabelle vorhanden ist, wird nur das Feld **Hat angreifbares Element** auf **Wahr** gesetzt, und der Wert des Felds **Quelle** für das CI bleibt derselbe wie bei der Erstellung des Bewertungsdatensatzes.
- Wenn angreifbare Elemente nach der Bewertung erstellt werden, wird eine geplante Aufgabe der Schwachstellenbewertung ausgeführt, um die Tabelle der betroffenen CIs und die Quelle des CI zu aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und eine Gefährdungsstufe zu
- Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu
- Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente
- Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu

Zugehörige Informationen

Registerkarte „Bewertung“.

Registerkarte „Übersicht“

Registerkarte „Bewertung“.

Überprüfen Sie die Bewertungsergebnisse auf der Registerkarte „Bewertung“. Nachdem Sie eine Bewertung des Schwachstellenereignisses durchgeführt haben, wird der Datensatz mit den Daten von Software Bill of Materials und Software Asset Management korreliert und Visualisierungen angezeigt.

Die Registerkarte „Bewertung“ füllt Daten (falls verfügbar) basierend auf dem von Ihnen erstellten Bewertungsdatensatz und korreliert die Details mit Bewertungen aus den Komponentendaten Software Asset Management und Software Bill of Materials in der CMDB.

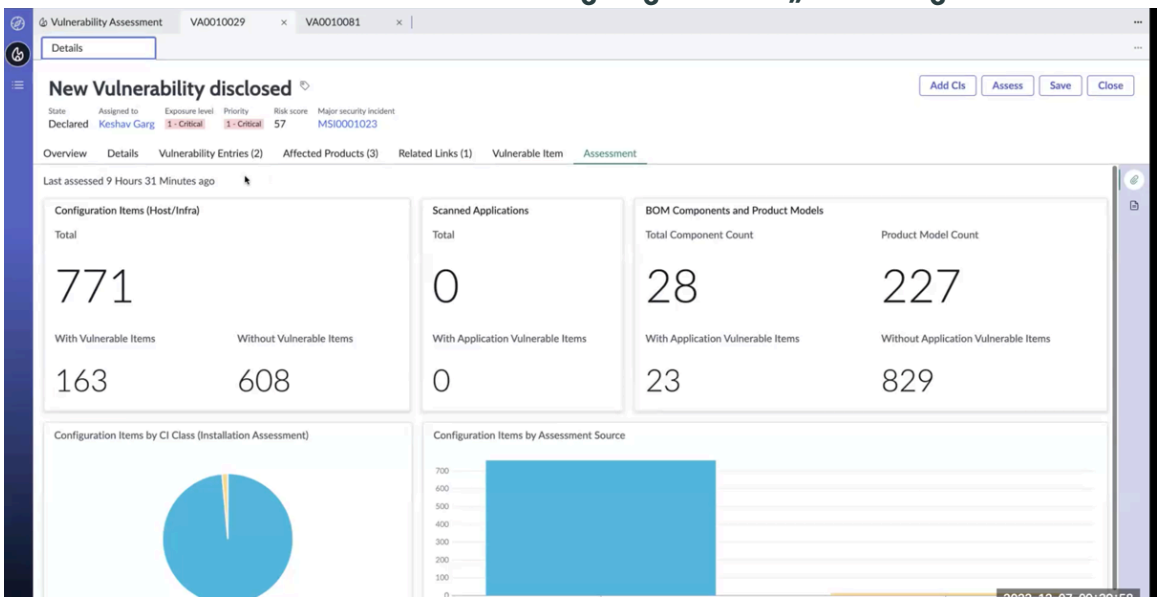
Funktionsweise der Bewertung

Wenn Sie auf die Schaltfläche **Bewerten** klicken, wird eine Bewertung für alle zugehörigen CVEs und betroffenen Produkte mit den Daten Software Asset Management und SBOM initiiert. Ein Hintergrundauftrag wird ausgelöst, und wenn die Bewertung verarbeitet wird, werden die VITs oder AVITs, die den angreifbaren Einträgen oder CVEs zugeordnet sind, auf den Registerkarten **Angreifbare Elemente** und **Angreifbare Anwendungselemente** angezeigt.

- Alle angreifbaren Elemente oder TPEs im Zusammenhang mit dem CVE werden identifiziert.
- Die Configuration Items (CIs), die zu den angreifbaren Elementen gehören, werden ebenfalls identifiziert und in der Tabelle der betroffenen Konfigurationselemente angezeigt.
- Wenn die CIs in der betroffenen CI-Tabelle nicht vorhanden sind, werden die identifizierten CIs zur Tabelle hinzugefügt, und die **Kennzeichnung Hat angreifbare Elemente** wird auf „Wahr“ gesetzt, und der Wert des Felds **Quelle** wird auf Scanner festgelegt.
- Wenn das CI bereits in der betroffenen Tabelle der Konfigurationselemente vorhanden ist, wird nur die Kennzeichnung **Hat angreifbares Element** auf wahr gesetzt, und die **Quelle** bleibt ab dem Zeitpunkt der Erstellung des Bewertungsdatensatzes unverändert.
- Wenn angreifbare Elemente nach der Bewertung erstellt werden, wird eine geplante Aufgabe der Schwachstellenbewertung ausgeführt, um die Tabelle der betroffenen CIs und die Quelle des CI zu aktualisieren.
- Im Bewertungsarbeitsbereich können Sie Zeitstempel anzeigen, um die letzte Bewertung der Ereignisse anzuzeigen. Die Registerkarte **Bewertung** ist nur sichtbar, wenn die neuen Bewertungen erstellt werden. Wenn die Bewertung den Status „In Bearbeitung“ hat, wird der letzte Bewertungsstatus angezeigt, da die Bewertung ausgeführt wird. Um den aktualisierten Bewertungsstatus anzuzeigen, müssen Sie die Seite aktualisieren. Sobald die Bewertung abgeschlossen ist, kann der Anwender alle zugehörigen Registerkarten für diese Bewertung sehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich der Schwachstellenbewertung: Registerkarte „Bewertung“.



Die Bewertungsdetails werden für die folgenden Widgets angezeigt.

- Konfigurationselemente (Host/Infra)
- Gescannte Anwendungen
- Stücklistenkomponenten und Produktmodelle
- Konfigurationselemente nach CI-Klasse (Installationsbewertung)
- Konfigurationselemente nach Bewertungsquelle: Zeigt die Liste der betroffenen Konfigurationselemente an.

Datenvisualisierungen

Name	Typ	Beschreibung
Konfigurationselemente (Host/Infra)	Einzelne Punktzahl	Zeigt die Anzahl der CIs mit und ohne VIs an. Das Widget Konfigurationselemente zeigt die Gesamtanzahl der CIs an, die dem Bewertungsdatensatz zugeordnet sind. Das Widget zeigt außerdem die Konfigurationselemente mit angreifbaren Elementen und ohne angreifbare Elemente an.
Gescannte Anwendungen	Anzahl	Gesamtanzahl der mit AVITs gescannten Anwendungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
		Hinweis: Sie können die Anzahl der gescannten Anwendungen für primäre und sekundäre CVEs anzeigen.
Stücklistenkomponenten und Produktmodelle	Einzelne Punktzahl	Gesamtanzahl der Komponenten, Anzahl der Produktmodelle, mit angreifbaren Anwendungselementen, ohne Anzahl angreifbarer Anwendungselemente.
Konfigurationselemente nach Bewertungsquelle	Gestapelter Balken	Betroffene Configuration Items gestapelt nach Bewertungsquelle.
Konfigurationselemente nach CI-Klasse (Installationsbewertung)	Kreisdiagramm	Konfigurationselemente gestapelt nach CI-Klasse.

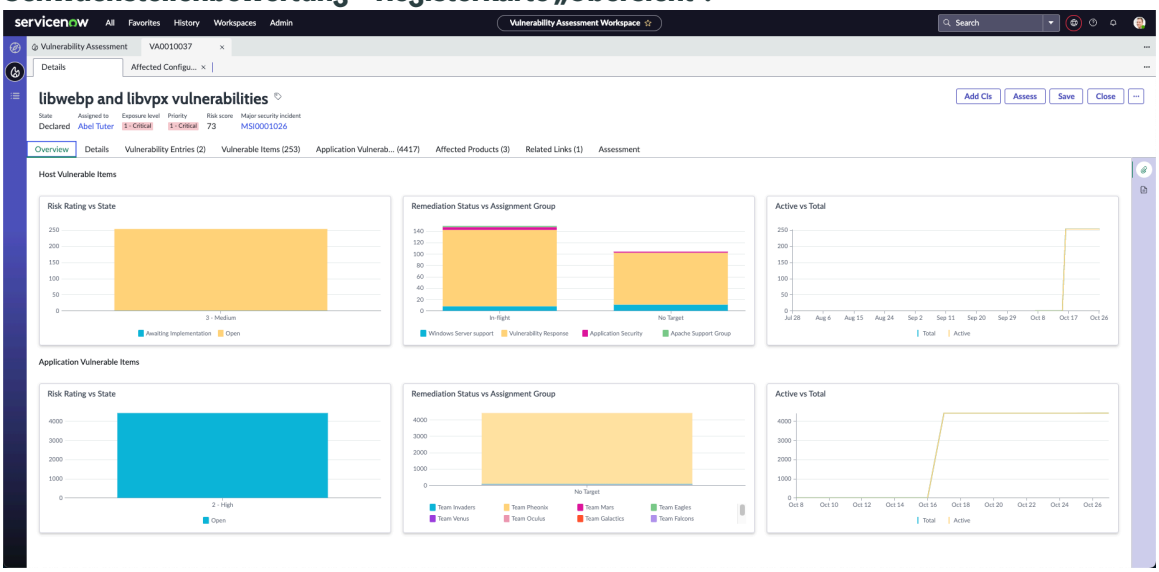
Registerkarte „Übersicht“

Auf der Registerkarte „Übersicht“ wird eine Übersicht über die Bewertungsdetails angezeigt. Nachdem Sie die erste Bewertung durchgeführt haben, wird der Datensatz mit den Daten von Software Bill of Materials und Software Asset Management korreliert und Visualisierungen angezeigt.

Registerkarte „Übersicht“

Die Registerkarte Übersicht füllt Daten (falls verfügbar) basierend auf dem von Ihnen erstellten Bewertungsdatensatz und korreliert die Details mit Bewertungen aus den Daten Software Asset Management und Software Bill of Materials in der CMDB. Die zugehörigen Listen namens

Schwachstellenbewertung – Registerkarte „Übersicht“.



Die Bewertungsdetails werden für die folgenden Widgets angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Angreifbare Host-Elemente (Host/Infra)
  - Risikobewertung vs. Status
  - Korrekturstatus vs. Zuweisungsgruppe
  - Aktiv vs. Gesamt
- Angreifbare Anwendungselemente
  - Risikobewertung vs. Status
  - Korrekturstatus vs. Zuweisungsgruppe
  - Aktiv vs. Gesamt

Datenvisualisierungen

Angreifbare Host-Elemente

Name	Typ	Beschreibung
Risikobewertung vs. Status	Gestapelter Balken	Status der angreifbaren Elemente, gestapelt nach ihrer Risikobewertung.
Korrekturstatus vs. Zuweisungsgruppe	Gestapelter Balken	Korrekturstatus des angreifbaren Elements, gestapelt nach seiner Zuweisungsgruppe.
Aktiv vs. Gesamt	Liste und Zeile	Gesamtzahl der diesem Eintrag zugeordneten angreifbaren Elemente im Vergleich zu den aktiven angreifbaren Elementen.

Angreifbare Anwendungselemente

Name	Typ	Beschreibung
Risikobewertung vs. Status	Gestapelter Balken	Status der angreifbaren Anwendungselemente, gestapelt nach Risikobewertung.
Korrekturstatus vs. Zuweisungsgruppe	Gestapelter Balken	Korrekturstatus des angreifbaren Anwendungselements, gestapelt nach seiner Zuweisungsgruppe.
Aktiv vs. Gesamt	Liste und Zeile	Gesamtzahl der diesem Eintrag zugeordneten angreifbaren Anwendungselemente im Vergleich zu aktiven angreifbaren Elementen.

Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und eine Gefährdungsstufe zu

Weisen Sie dem Schwachstellenbewertungsdatensatz manuell Priorität und Gefährdungsstufe zu.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie einen Schwachstellenbewertungsdatensatz aus.
3. Navigieren Sie auf der Registerkarte **Details** zu **Risikoattribute**.
4. Wählen Sie eine **Priorität** aus der Liste der Optionen aus.
5. Wählen Sie eine **Risikostufe** aus der Liste der Optionen aus.
6. Wählen Sie **Speichern**.

Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu

Fügen Sie manuell die CIs in Ihrer Organisation hinzu, die Ihrer Meinung nach mit dem Schwachstellenbewertungsdatensatz verknüpft werden sollten, aber nach der Erstbewertung nicht in den betroffenen CIs angezeigt werden.

Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie CIs hinzu, von denen Sie wissen, dass sie betroffen sind, aber nach der Bewertung nicht angezeigt werden. Sie können CIs nur hinzufügen, wenn sich der Bewertungsdatensatz im Status **„Deklariert“** oder **„Bewertung ausstehend“** befindet.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie den gewünschten Bewertungsdatensatz aus der Liste aus.
3. Wählen Sie **CIs hinzufügen**.
4. Wählen Sie die Konfigurationselemente im Dialogfeld Konfigurationselemente aus.
5. Wählen Sie **CIs hinzufügen**.
   Der Hintergrundauftrag Vulnerability Response – Konfigurationselemente zu Ereignis hinzufügen wird initiiert, und es wird eine entsprechende Benachrichtigung angezeigt.
6. Wählen Sie in der Benachrichtigung **Status anzeigen,** um den Status des laufenden Auftrags anzuzeigen.

Ergebnisse

Datensätze werden der Tabelle „Betroffene Konfigurationselemente“ mit *„Manuell“* als **Quelle**hinzugefügt.

Nächste Maßnahme

Navigieren Sie zur Registerkarte **Bewertung** und aktualisieren Sie das Widget **Konfigurationselemente (Host/Infra),** um die hinzugefügten CIs anzuzeigen.

Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente

Erstellen Sie angreifbare Elemente (VIs) oder angreifbare Elemente in der Anwendung (Application Vulnerable Items) im Arbeitsbereich der Schwachstellenbewertung. Schwachstellenanalysten analysieren die Liste der VIs und empfehlen Lösungen und Patches, die dem IT-Team helfen, diese Schwachstellen zu beheben.

Der Schwachstellen-Ereignismanager sollte in der Lage sein, eines, mehrere oder alle Suchergebnisse für das Gefahrenpotenzial auszuwählen, um angreifbare Elemente zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Angreifbares Anwendungselement für SBOM-Bewertungsergebnisse, denen keine AVITs zugeordnet sind
- Angreifbare Elemente für Konfigurationselemente, denen keine VITs zugeordnet sind
- Ordnen Sie den angreifbaren Elementen das primäre CVE zu.

Erstellen Sie VIs für Konfigurationselemente ohne zugeordnete angreifbare Elemente

Erstellen Sie VITs für angreifbare Elemente für Konfigurationselemente, die durch die Schwachstellenbewertung identifiziert wurden, aber dem Datensatz keine VITs zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertungen**.
2. Wählen Sie den Bewertungsdatensatz aus, für den Sie die VIT erstellen müssen.
3. Wählen Sie die Registerkarte **Bewertung**.
4. Wählen Sie im Widget **Konfigurationselemente (Host-Infra)** die Option **Ohne Konfigurationselemente** aus.
5. Wählen Sie aus der Liste **Betroffene Konfigurationselemente die Konfigurationselemente** aus, für die Sie VITs erstellen möchten.
6. Wählen Sie **Angreifbares Element erstellen aus**.
   Der Hintergrundauftrag „Vulnerability Response – Manuelle VITs Schwachstellenbewertung erstellen“ wird initiiert, und es wird eine entsprechende Benachrichtigung angezeigt.
7. Wählen Sie in der Benachrichtigung **Status anzeigen,** um den Status des laufenden Auftrags anzuzeigen.
   Angreifbare Elemente für die von Ihnen ausgewählten betroffenen Konfigurationselemente werden erstellt.

   Das Widget **Configuration Items (Host Infra)** zeigt jetzt dasselbe CI in der Anzahl **mit angreifbaren Elementen** an.

Erstellen Sie angreifbare Anwendungselemente (Application Vulnerable Items, AVITs) für betroffene Produktmodelle oder Komponenten ohne zugehörige angreifbare Anwendungselemente

Erstellen Sie angreifbare Elemente für die Anwendung (Application Vulnerable Items, AVITs) für betroffene Produkte oder Komponenten, die durch die Schwachstellenbewertung identifiziert wurden, aber dem Datensatz keine AVITs zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertungen**.
2. Wählen Sie den Bewertungsdatensatz aus, für den Sie die VIT erstellen müssen.
3. Wählen Sie die Registerkarte **Bewertung**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie im Widget für **Stücklistenkomponenten und Produktmodelle** die Option **Ohne Anzahl angreifbarer Anwendungselemente** aus.
5. Wählen Sie in der Liste Betroffene Produktmodelle die **betroffenen Produktmodelle** aus, für die Sie AVITs erstellen möchten.
6. Wählen Sie **Angreifbares Anwendungselement erstellen aus**.
   Der Hintergrundauftrag „Vulnerability Response – Manuelle VITs Schwachstellenbewertung erstellen“ wird initiiert, und es wird eine entsprechende Benachrichtigung angezeigt.
7. Wählen Sie in der Benachrichtigung **Status anzeigen,** um den Status des laufenden Auftrags anzuzeigen.
   Angreifbare Anwendungselemente für die von Ihnen ausgewählten betroffenen Produktmodelle werden erstellt. für das primäre CVE, das dem Datensatz zugeordnet ist.

   Das Widget **für Stücklistenkomponenten und Produktmodelle** zeigt jetzt dasselbe Produktmodell oder dieselbe Komponente in der Anzahl **mit angreifbaren Anwendungselementen** an.

Verknüpfen Sie den Schwachstellenbewertungsdatensatz mit einem schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidents

Sie können den Bewertungsdatensatz mit einem Major Security Incident verknüpfen, vorschlagen oder heraufstufen, sofern Sie Zugriff auf die Anwendung Management schwerwiegender Sicherheits-Incidents haben.

Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können den Bewertungsdatensatz so verschieben, dass er einem vorhandenen schwerwiegenden Security Incident zugeordnet wird, einen neuen MSI aus dem Bewertungsdatensatz erstellen oder den Schwachstellenbewertungsdatensatz zu einem schwerwiegenden Security Incident heraufstufen. Nutzen Sie die Funktionen Management schwerwiegender Sicherheits-Incidents von [], z. B. die Integrationen mit Microsoft Teams und Microsoft SharePoint.

Sie können auch den Link zu schwerwiegenden Security Incidents im Arbeitsbereich des Schwachstellenmanagers für angreifbare Elemente anzeigen. Der Link MSIM wird mit der Schwachstellenbewertung verknüpft, die in den Schwachstellen und in den anderen Arbeitsbereichen von Vulnerability Responseangezeigt wird.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie den Bewertungsdatensatz aus, den Sie mit einem schwerwiegenden Security Incident verknüpfen möchten.
3. Wählen Sie auf der Registerkarte **Details** das Symbol **Weitere Aktionen**.
4. Wählen Sie eine der folgenden Antworten aus.

Option	Bezeichnung
Mit schwerwiegendem Security Incident verknüpfen	Wählen Sie den vorhandenen MSI-Datensatz aus der Liste der schwerwiegenden Security Incidents aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Der Schwachstellenbewertungsdatensatz ist mit dem vorhandenen schwerwiegenden Security Incident verknüpft.
Als schwerwiegenden Security Incident vorschlagen	Geben Sie die folgenden Details ein, und wählen Sie **Vorschlagen**. ○ Erkennungsdatum ○ Begründung ○ Potenzieller Impact
Als schwerwiegendem Security Incident heraufstufen	Geben Sie die folgenden Details ein, und wählen Sie **Heraufstufen**. ○ Erkennungsdatum ○ Geschätztes Lösungsdatum ○ Begründung ○ Potenzieller Impact

5. Wählen Sie **Speichern**.

Nächste Maßnahme

Wählen Sie den MSI-Datensatz aus, um ihn in der Ansicht Management schwerwiegender Sicherheits-Incidents zu öffnen.

Zugehörige Informationen

Verknüpfen mit Major Security Incident

Vorschlagen als Major Security Incident

Heraufstufen zu einem Major Security Incident

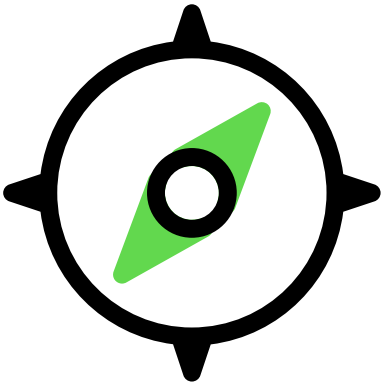
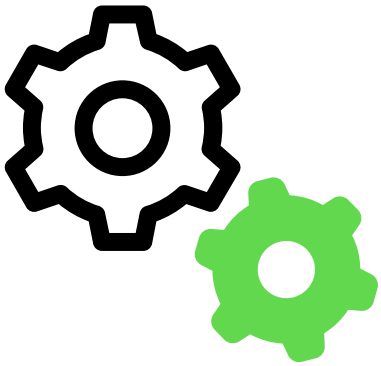
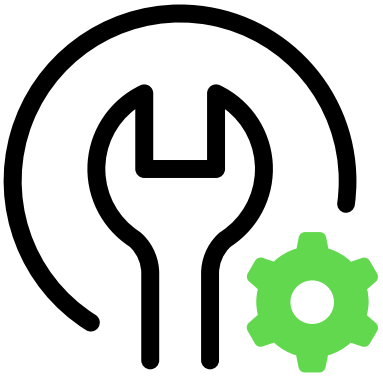
Software-Stückliste

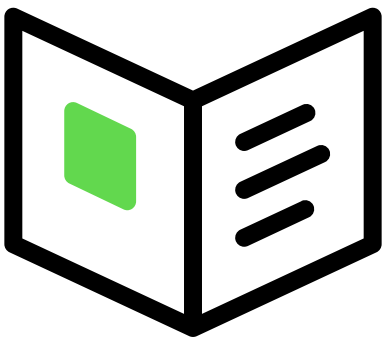
Zeigen Sie eine Liste der Open Source- und Drittanbieter-Softwarekomponenten an, die Sie in Ihrer Anwendungsentwicklung verwenden. Erhalten Sie Einblicke in Softwarelizenzen, Versionsinformationen und die bekannten Schwachstellen Ihrer Komponenten in den Dateien Software Bill of Materials (SBOM), die Sie in Ihre -Instanz hochladen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über die Konzepte und Funktionen SBOM von .	Konfigurieren Sie SBOM -Anwendungen.	Erfahren Sie, wie Sie SBOM -Komponenten importieren und Daten im -Arbeitsbereich anzeigen.

Referenz

Rufen Sie Details zu Formularen, Feldern, Tabellen und Eigenschaften SBOM von ab.

Problembehandlung und Hilfe

- Security Operations-Community
- CycleneDX – Software-Stückliste (Software Bill of Material, SBOM) .
- SPX .
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen .
- Kontakt Kundenservice und Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Software Bill of Materials erkunden

Identifizieren Sie die in den -Anwendungen Ihrer Organisation verwendeten -Komponenten anhand der -Dateien Software Bill of Materials (SBOM), die Sie in Ihre -Instanz hochladen. Machen Sie sich mit allen Risiken vertraut, die mit der Verwendung von Open Source-Software verbunden sind, um Ihr potenzielles Risiko zu ermitteln, die Lizenz-Compliance anzuzeigen und Schwachstellen zu beheben.

Software Bill of Materials – Übersicht

Open Source- und Drittpartei-Komponenten bieten Ihnen viele Vorteile für die schnelle Erstellung und Veröffentlichung Ihrer Softwareprojekte. In einigen Fällen sind jedoch mit der Verwendung öffentlich zugänglicher Komponenten Risiken verbunden, z. B.:

- Mangelnde Transparenz der Komponentenintegrität
- Schwachstellen in der Open Source-Software
- Package Intelligence für Open Source-Software
- Nicht konforme Softwarelizenzen

Sie können Ihre Software-Stücklistendateien über eine API oder manuell hochladen. Zeigen Sie die Dateien an, die Sie als Entitäten importieren. Hierbei handelt es sich um Bestände der in Ihrer Software verwendeten Komponentenbibliotheken von Drittparteien, einschließlich aller vorübergehenden Abhängigkeiten und verfügbaren Lizenzierungsinformationen.

Weitere Informationen dazu, was in den Softwarebeständen in den SBOMs „CycloneDX“ und „SPDPX“ enthalten ist, finden Sie unter CycleneDX – Software-Stückliste (Software Bill of Material, SBOM) und SPX.

Software Bill of Materials – Anwender

Anwender

Anwender	Beschreibung
Schwachstellenmanager und -analysten	Zeigen Sie hochgeladene Software-Stücklistendateien in Datensätzen, Datenvisualisierungen sowie erweiterte Schwachstelleninformationen im Arbeitsbereich Software Bill of Materials (SBOM) an. Schwachstellenmanager und Analysten verwenden diese Informationen, um die Compliance der Softwarelizenzierung und das potenzielle Risiko bei der Verwendung von Open Source-Software zu bestimmen.
Zu diesen Anwendern gehören unter anderem: • Anwälte für Technologie oder Software • IT-Manager • Auditoren • Software-Asset-Manager und -Teams	Zeigen Sie hochgeladene proprietäre und Open Source-Softwarelizenzen für Komponenten Ihrer hochgeladenen SBOM -Dateien an. Erstellen Sie eine Datenbank mit proprietären und Open Source-Softwarelizenzen für die Komponenten. Überprüfen und klassifizieren Sie Lizenzen mit fehlenden Informationen gemäß Ihren internen oder behördlichen Richtlinien. Ordnen Sie Ihre Komponenten Lizenzen zu, bestimmen Sie Ihre allgemeine Lizenz-Compliance und sehen Sie sich Ihr

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung
	potenzielles Risiko durch verbotene, eingeschränkte oder fehlende Lizenzen an.

Software Bill of Materials – Workflow

Mit den SBOM-Anwendungen können Sie Dateien hochladen und Details für Entitäten, Komponentenbestände, Schwachstellen und Softwarelizenzinformationen im Software-Bill-of-Materials-Arbeitsbereich (SBOM) anzeigen.

- Laden Sie SBOM -Dateien mit einer API oder manuell hoch.
- Überprüfen Sie die Komponenten in der Datei SBOM, die Sie in den Arbeitsbereich SBOM hochgeladen haben.
- Überprüfen Sie die Komponentenlizenzinformationen aus hochgeladenen SBOM -Dateien, und klassifizieren Sie sie, um Ihr Risiko für eingeschränkte oder gesperrte Lizenzen zu identifizieren.
- Bewerten Sie Ihre Gefährdung, und erstellen Sie angreifbare Elemente für Komponenten, denen Schwachstellen zugeordnet sind.
- Zeigen Sie Berichte und Dashboards sowie Ihre allgemeine Lizenz-Compliance für hochgeladene SBOM -Komponenten auf der Homepage im -Arbeitsbereich SBOM an.

Software Bill of Materials – Vorteile

Mit drei Software-Stücklisten-Anwendungen können Sie einen genauen Bestand Ihrer Softwarekomponenten und der zugehörigen Risiken anzeigen:

- Datenmodell für SBOM
- SBOM Zentral
- SBOM Antwort

Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen .

SBOM – Vorteile

Leistung	Anwendung	Unterstützte Versionen
Diese Anwendung stellt die Tabellen zum Speichern von Daten SBOM bereit. Diese Anwendung ist erforderlich. Sie enthält die Tabellen, ACLs und Rollen, die zum Lesen der Daten SBOM erforderlich sind.	Datenmodell für SBOM	v4.0, v3.0, v2.0
Diese Anwendung ist erforderlich. Enthält die API, die zum Hochladen von SBOM -Dokumenten erforderlich ist, und die Geschäftslogik, die zum Analysieren und Importieren der Daten aus diesen Dokumenten in Ihre -Instanz erforderlich ist. Sie können einen Bestand Ihrer Softwarekomponenten im SBOM -Arbeitsbereich anzeigen, aber Sie können	SBOM Zentral	v6.0, v5.0, v4.0 Ab Version 4.0 unterstützt SBOM Core:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SBOM – Vorteile (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen
die Datenvisualisierungen nicht auf der Zielseite anzeigen. Laden Sie Ihre Software-Stücklistendateien in den Standards „CycloneDX“ und „SPDPX“ hoch, analysieren und verarbeiten Sie sie. Die unterstützten Dateiformate und Versionen für diese Produkte finden Sie in der Spalte Unterstützte Versionen. Zeigen Sie Stücklistenentitäten (Stückliste) und einen Bestand Ihrer Softwarekomponenten an. Eine Stücklistenentität ist die Komponente der Stammebene in einer SBOM-Datei. Für ein Element mit dem Typ „CycloneDX SBOM“ wird beispielsweise die in den Metadaten aufgeführte Komponente als Stücklistenentität betrachtet.		• XML- und JSON-Versionen 1.0 bis 1.6 von Epic (CycloneDX) • JSON-Versionen 2.2 bis 2.3 von SPX.
• Die AntwortSBOM ist erforderlich, wenn Sie auf die Funktionen und Datenvisualisierungen auf der Zielseite im SBOM- Arbeitsbereich zugreifen möchten. • SBOM Response erfordert die Anwendung Vulnerability Response. • Zeigen Sie im Arbeitsbereich SBOM Ihren Komponentenbestand an, und bewerten Sie Ihr Risiko. Richten Sie Regeln ein, um automatisch angreifbare Elemente in der Anwendung (Application Vulnerable Items, AVITs) zu erstellen und sie mit dem Workflow Application Vulnerability Response zu korrigieren. • Zeigen Sie Komponentenlizenzinformationen an, die mit Ihren SBOM -Dateien im Lizenzverwaltungsmodulhochgeladen werden. Klassifizieren und lösen Sie die Komponenten, die Sie in Ihren Application Vulnerability Response -Dateien hochladen, in Lizenzen, um den Status Ihrer allgemeinen Lizenz-Compliance anzuzeigen. • Ab Version 4.0 von Application Vulnerability Response Response können Sie Komponenten, die als veraltet oder verworfen als „Nicht konform“ gekennzeichnet sind, in der Schnittstelle Policy as Code Engine (PaCE) anzeigen, die im Arbeitsbereich SBOM verfügbar ist.	SBOM Antwort	v6.0, v5.0, v4.0

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SBOM – Vorteile (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen
• Die OSV.dev- und Deps.dev-Integrationen sind in der Installation von SBOM Response enthalten. ◦ OSV.dev ist eine Open-Source-API, die Vulnerability Intelligence-Informationen für eine bestimmte Version eines Pakets oder einer bestimmten Bibliothek bereitstellt. ◦ Deps.dev ist eine Open-Source-API, die eine Versionsliste für ein bestimmtes Paket oder eine bestimmte Bibliothek bereitstellt und Komponenten identifiziert, die sich im Status **„Veraltet“** und **„Verworfen“** befinden. Weitere Informationen finden Sie unter Deps.dev-, OSV.dev- und PaCE-Integrationen für konfigurieren Software Bill of Materials. Weitere Informationen zu PaCE und PaCE-Richtlinien finden Sie unter Integrating PaCE with other applications .		
Generieren und laden Sie Software Bill of Materials (SBOM) Dateien für Software während der Entwicklungszyklen für kontinuierliche Integration und kontinuierliche Bereitstellung hoch.	SBOM Antwort	• Datenmodell für SBOM: v1.4 und höher. • SBOM Core: v3.0 und höher. • SBOM Antwort: v4.0 und höher.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Software Bill of Materials finden Sie unter:

- Unterstützte Anwendungen für erkunden Software Bill of Materials
- Software Bill of Materials konfigurieren
- Ihre SBOM -Dateien werden im SBOM -Arbeitsbereich hochgeladen und dort angezeigt
- Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials

Unterstützte Anwendungen für erkunden Software Bill of Materials

Schwachstellenanalysen von Drittparteien und andere Integrationen mit den -Anwendungen Software Bill of Materials können die Daten Ihrer hochgeladenen Dateien verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile unterstützter Anwendungen

Durch Schwachstellenanalysen von Drittparteien und andere Integrationen mit den Anwendungen Software Bill of Materials können Sie die Anzahl der Komponenten anzeigen, die als veraltet und verworfen gelten, sowie Informationen darüber, ob Sie Schwachstellen im Zusammenhang mit Komponenten beheben können.

Die in der folgenden Tabelle aufgeführten Anwendungen ServiceNow® und Drittanbieterintegrationen werden von den Anwendungen SBOM unterstützt. Diese Anwendungen liefern Ihnen angereicherte Schwachstellendaten, Schwachstelleninformationen und andere wichtige Informationen, mit denen Sie die mit SBOM-Dateien verbundenen Schwachstellen anzeigen und priorisieren können. Alle diese Anwendungen und Integrationen sind über den ServiceNow® Storeverfügbar.

Unterstützte Anwendungen und Drittanbieterintegrationen

Leistung	Anwendung	Unterstützte Versionen	Anwender
Vulnerability Response ist erforderlich, wenn Sie die Anwendung SBOM Response installieren. Installieren Sie die Anwendung Vulnerability Response, bevor Sie SBOM Response installieren. Die FunktionenApplication Vulnerability Response werden mit Vulnerability Responseinstalliert. Diese Funktionen ermöglichen den Zugriff auf den Arbeitsbereich des Schwachstellenmanagers in der Anwendung Vulnerability Response und den Schwachstellen-Workflow, um Sie bei der Korrektur von angreifbaren Elementen in der Anwendung (Application Vulnerable Items, AVIT) zu unterstützen.	Vulnerability Response	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen .	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Anwendungen und Drittanbieterintegrationen (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen	Anwender
Zeigen Sie erweiterte NVD-Schwachstellen- und -Schweregraddaten an. Zeigen Sie importierte Daten aus den NVD- und CWE-Integrationen an, um die in Ihren SBOM-Daten enthaltenen Schwachstellendaten zu ergänzen. Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittparteien.	Integration von Vulnerability Response mit NVD und SBOM Response	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen .	
Importieren Sie Software-Stücklistendateien mit Veracode Vulnerability Integration. Veracode Vulnerability Integration enthält die folgenden Erweiterungen mit SBOM-Dateien Veracode : • Wenn Sie SBOM Response installiert haben, können Sie von SBOM gefundene Schwachstellen für die von Ihnen hochgeladenen SBOM -Dateien einbeziehen. • SBOM wird dem Feld Quelle für Datensätze in der Stücklistentabelle [sn_sbom_doc] für die von Ihnen hochgeladenen SBOM SBOM -Dateien zugeordnet.	Veracode Vulnerability Integration und SBOM Response	Ab Version 4.3 von Veracode Vulnerability Integration. Wenn Veracode Vulnerability Integration bereits installiert ist, können Sie importierte Veracode SBOM -Daten ab Version v3.0 von SBOM Core auch in den Formaten Epic (JSON und XML) und SPX (XML) hochladen. Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen .	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Anwendungen und Drittanbieterintegrationen (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen	Anwender
Weitere Informationen finden Sie unter Veracode Vulnerability Integration.			
Laden Sie SBOM -Dateien aus Ihren GitHub-Repositorys auf die Now Platform hoch. Stellen Sie fest, ob SBOM Dateien, die in Ihren CI/CD-Pipelines (kontinuierliche Integration und kontinuierliche Bereitstellung/ Bereitstellung) generiert wurden, erfolgreich in der Warteschlange Ihrer Now Platform-Instanz platziert wurden. Schützen Sie Ihre Umgebungen während Softwareentwicklungszyklen mit GitHub-Aktionen, die Sie über Ihre GitHub-Umgebung initiieren, vor potenziell schädlichen Komponenten.	Rufen Sie alle erforderlichen GitHub-Aktionen für den Upload von SBOM im GitHub-Marketplace ab.	Ab Version 4.0 von SBOM Core.	

Software Bill of Materials konfigurieren

Laden Sie die erforderlichen Anwendungen für die Anwendung Software Bill of Materials (SBOM) herunter, und aktivieren Sie sie, bevor Sie SBOM -Dateien hochladen.

Konfiguration – Übersicht

1. Laden Sie die erforderlichen SBOM -Anwendungen und alle weiteren gewünschten unterstützten Anwendungen und Integrationen aus dem ServiceNow Store in Ihre ServiceNow-Instanz herunter. Weitere Informationen zu unterstützten Anwendungen finden Sie unter Software Bill of Materials erkunden und Laden Sie eine Anwendung zum ersten Mal von ServiceNow Store herunter.

   Die Anwendung Vulnerability Response ist für SBOM Response erforderlich. Installieren Sie die Anwendung Vulnerability Response, bevor Sie SBOM Response installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Suchen Sie die heruntergeladenen SBOM-Anwendungen, und wählen Sie Installieren, um sie zusammen mit ihren Abhängigkeiten in der folgenden Reihenfolge zu aktivieren. Weitere Informationen finden Sie unter Installieren Sie die unterstützten Anwendungen für Software Bill of Materials.

   - Vulnerability Response und ihre Abhängigkeiten
   - Vulnerability Response Integration with NVD
   - Datenmodell für SBOM
   - SBOM Zentral
   - SBOM Die Antwort umfasst die OSV.dev- und Deps.dev-Integrationen sowie Zugriff auf die Funktionen von Policy as Code Engine (PaCE) im SBOM-Arbeitsbereich.

3. Konfigurieren Sie die Deps.dev- und OSV.dev-Integrationen. Diese Integrationen sind in der Anwendung SBOM Response enthalten und werden automatisch installiert und aktiviert. Sie müssen OSV.dev Integration - Comprehensive bei Bedarf über den zugehörigen Integrationsdatensatz initiieren. Weitere Informationen finden Sie unter Deps.dev-, OSV.dev- und PaCE-Integrationen für konfigurieren Software Bill of Materials und Software Bill of Materials erkunden.

   Die Deps.dev-Integration bietet Ihnen Informationen zu Komponenten im Status **„Veraltet“** und „ **Verworfen“** für eine bestimmte Version eines Pakets oder einer Bibliothek, die Sie in Ihren Dateien SBOM hochladen.

   OSV.dev ruft Schwachstellendaten aus einer Open Source-Datenbank für eine Version eines Pakets oder einer Bibliothek ab, die Sie in Ihren Dateien SBOM hochladen.

4. Informationen zur Konfiguration zusätzlicher unterstützter Anwendungen und Integrationen, die Sie installiert haben, finden Sie in der Produktdokumentation. Siehe Vulnerability Response-Integrationen und Integration von Application Vulnerability Response mit anderen Anwendungen.

Installieren Sie die unterstützten Anwendungen für Software Bill of Materials

Laden Sie die erforderlichen Anwendungen für die Anwendung Software Bill of Materials (SBOM) herunter, und aktivieren Sie sie, bevor Sie Dateien hochladen.

Vorbereitungen

Erforderliche Rolle: admin für Download, Installation und Aktivierung aller Anwendungen und Rollenzuweisungen in Ihrer Instanz.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Laden Sie die erforderlichen SBOM -Anwendungen aus dem ServiceNow Store in Ihre ServiceNow -Instanz herunter.

   Mit diesen Anwendungen können Sie SBOM -Dateien in Ihre -Instanz hochladen und importieren. Sie können Stücklistenentitäten- und Komponentendaten im Arbeitsbereich SBOM anzeigen, wenn SBOM Core installiert ist.

   Sie können Stücklistenentitäten, Komponentendaten und Datenvisualisierungen im SBOM Workspace anzeigen, wenn Sie SBOM Response installiert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datenmodell für SBOM
- SBOM Zentral

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie unter:

- Install a ServiceNow Store application
- Install an update to a ServiceNow Store application

2. **Wahlweise:** Wenn Sie Ihre Daten SBOM im Arbeitsbereich SBOM anzeigen, importierte Schwachstelleninformationen von Drittparteien anzeigen, Ihre Gefährdung des Risikos bewerten und Schwachstellen mit den Workflows Application Vulnerability Response und Vulnerability Response beheben möchten, laden Sie die folgenden Anwendungen herunter:
   - Vulnerability Response und ihre Abhängigkeiten
   - Vulnerability Response Integration with NVD
   - SBOM Antwort

   Weitere Informationen zu diesen und anderen unterstützten SBOM -Anwendungen finden Sie unter Software Bill of Materials erkunden.
3. Nachdem Sie die Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
4. Suchen Sie die SBOM -Anwendungen, die Sie heruntergeladen haben, und wählen Sie **Installieren**, um sie zusammen mit ihren Abhängigkeiten zu aktivieren.

   Eine Meldung wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde. Aktivieren Sie die Anwendungen in der folgenden Reihenfolge:
   - Vulnerability Response und ihre Abhängigkeiten
   - Vulnerability Response Integration with NVD
   - Datenmodell für SBOM
   - SBOM Zentral
   - SBOM Antwort, die die OSV.dev- und Deps.dev-Integrationen enthält und die PaCE-Schnittstelle (Policy as Code Engine) im SBOM Workspace unterstützt.

   Unter Deps.dev-, OSV.dev- und PaCE-Integrationen für konfigurieren Software Bill of Materials finden Sie weitere Informationen zum Konfigurieren dieser Integrationsanwendungen, nachdem Sie SBOM Response installiert haben.
5. **Wahlweise:** Aktivieren Sie Integrationen, indem Sie zu navigieren **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und wählen Sie **Installieren**aus.

   (Optional) Weitere Informationen zu diesen Integrationen und den von ihnen bereitgestellten Funktionen finden Sie unter Software Bill of Materials erkunden.
   - Vulnerability Response Integration with Veracode. Weitere Informationen finden Sie unter ServiceNow Vulnerability Response Integration mit Veracodeinstallieren.
   - Vulnerability Response Integration with NVD (Integration von Vulnerability Response mit NVD) ist erforderlich, wenn Sie die erweiterten Daten für Schwachstellen anzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

möchten, die hochgeladenen Komponenten zugeordnet sind. Weitere Informationen finden Sie unter Grundlagen zu NVD-Integrationen.

- CWE Comprehensive 2000 Integration. Weitere Informationen zur Aktivierung dieser geplanten Aufgabe finden Sie unter Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus.

Eine Meldung wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

6. Weisen Sie Anwendern die folgenden Rollen zu.
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
   - sn_sbom_response.managelicense
   - sn_sbom_response.licenseresolver
7. **Wahlweise:** Weisen Sie der App-Sec-Manager-Gruppe Anwender zu, wenn Sie angreifbare Anwendungselemente für Schwachstellen in Ihren importierten SBOM -Daten erstellen.

   (Optional) Benutzer, die der App-Sec-Manager-Gruppe zugewiesen sind, priorisieren und verwalten angreifbare Anwendungselemente. Benutzer in dieser Gruppe erben viele der Rollen, die zum Lesen und Bearbeiten von Datensätzen und zum Konfigurieren der von der Anwendung Application Vulnerability Response unterstützten Anwendungen und ihrer Nachbesserungs-Workflows erforderlich sind.
8. **Wahlweise:** Deaktivieren Sie die Systemeigenschaft AVITs erneut öffnen, wenn erkannt (*sn_sbom_resp.reopen_avits_if_detected*), wenn **geschlossene** AVITs nicht automatisch in den Status **„Offen“** zurückkehren sollen.

   (Optional) Ein **geschlossenes** angreifbares Element in der Anwendung (Application Vulnerable Item, AVIT) für eine Komponente mit einer zugeordneten Schwachstelle wird automatisch erneut geöffnet (auf Offen **gesetzt**) und ist im SBOM-Arbeitsbereich sichtbar, wenn die folgenden Bedingungen vorliegen:

   - Das AVIT mit der zugehörigen Schwachstelle wird von den Schwachstellenscans einer Drittanbieterintegration erneut erkannt, oder die Komponente mit der Schwachstelle ist Teil eines nachfolgenden SBOM-Uploads.
   - Sie haben die Systemeigenschaft „AVITs erneut öffnen, wenn erkannt“ (*sn_sbom_resp.reopen_avits_if_detected*) nicht deaktiviert. Diese Systemeigenschaft ist standardmäßig aktiviert.
   - Der Substatus des **geschlossenen** AVIT ist keiner der folgenden: **Mitigationssteuerung vorhanden**, **Nicht betroffen**oder **Falsch positiv**. AVITs mit diesen Substatus werden von der Systemeigenschaft nicht erneut geöffnet.

Nächste Maßnahme

Laden Sie Ihre SBOM -Dateien hoch. Siehe Software Bill of Materials Dateien manuell hochladen und Software Bill of Materials -Dateien werden mit einer REST-API hochgeladen, um weitere Informationen zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Deps.dev-, OSV.dev- und PaCE-Integrationen für konfigurieren Software Bill of Materials

Sie können einige der Parameter für die Deps.dev- und OSV.dev-Integrationen bearbeiten. Es gibt auch zwei Codeauslöser-Versionen dieser Integrationen, die ausschließlich für interne Workflows verwendet werden. Sie sollten diese Integrationen nicht bei Bedarf initiieren. Darüber hinaus können Sie eine geplante Aufgabe aktivieren, um Richtlinien mit Policy as Code Engine (PaCE) zu erstellen.

Codeauslöser-Integrationen für interne Workflows

Ab v3.2 von SBOM Response umfassten die Leistungsverbesserungen das Hinzufügen von zwei OSV.dev- und Deps.dev -Codeauslöserintegrationen :

- OSV-Integration (Codeauslöser bei Bedarf)
- Deps.dev-Integration (Codeauslöser bei Bedarf)

Diese Integrationen werden automatisch durch interne Workflows initiiert und dienen nur zur internen Verwendung. Obwohl Sie sie finden können, dürfen Sie diese Integrationen bei Bedarf nicht über die Schaltfläche **Jetzt** ausführen in ihren Integrationsdatensätzen initiieren.

Ausführungszeitplan für Deps.dev-Integration konfigurieren

Um den Zeitplan zu ändern, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen** > **Deps.dev-Integration**. Die Rolle „sn_vul.app_configure_integrations“ ist erforderlich, um den Zeitplan dieser Integration zu bearbeiten.

Diese Deps.dev-Integration wird verwendet, um Komponenten zu identifizieren, die sich im Status **„Veraltet“** und **„Verworfen“** befinden. Die Version einer veralteten Komponente ist mehr als zwei Hauptversionen älter als die aktuelle Version und zwei Jahre älter als die aktuelle Version. Eine verworfene Komponente wurde seit mehr als zwei Jahren nicht mehr aktualisiert. Die Zwei-Jahres- und Zwei-Versions-Schwellenwerte können mit den Systemeigenschaften bearbeitet werden. Um diese Parameter zu bearbeiten, navigieren Sie zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** und suchen Sie die folgenden Datensätze:

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

Die Deps.dev-Integration wird mit der Antwort auf SBOM installiert. Die Integration ist standardmäßig aktiviert (Kontrollkästchen „Aktiv“ im Integrationsdatensatz aktiviert) und soll wöchentlich ausgeführt werden. Beachten Sie, dass dies nicht die bedarfsgesteuerte Deps.dev-Codeauslöserintegration ist. Sie können den Zeitplan bearbeiten und die geplante Aufgabe bei Bedarf über den zugehörigen Integrationsdatensatz initiieren. .

Die Schwellenwerte für „Verworfen“ und „Veraltet“ werden in Monaten angegeben. Der Schwellenwert für die Version ist numerisch.

Sie können importierte Daten auf der Homepage des -Arbeitsbereichs und im Modul „Stücklisten-Warteschlange“ anzeigen. Importierte Daten werden in der Tabelle „Paketgruppen“ [sn_sbom_pkg_group] gespeichert.

OSV.dev-Integration konfigurieren und initiieren – Umfassend

Die Integration „OSV.dev Integration - Comprehensive “ wird mit SBOM Response installiert. Die Integration ist standardmäßig aktiviert (Kontrollkästchen Aktiv im Integrationsdatensatz aktiviert). Beachten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie, dass dies nicht die bedarfsgesteuerte OSV.dev-Codeauslöser-Integration ist und Sie diese Integration bei Bedarf über den zugehörigen Integrationsdatensatz initiieren müssen.

Um diese Integration zu konfigurieren und zu initiieren, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen** > **OSV.dev-Integration – Umfassend**. Die Rolle sn_vul.app_configure_integrations ist erforderlich.

Sie können importierte Daten auf der Homepage des -Arbeitsbereichs auf der Registerkarte Schwachstelle in Datensätzen aus der Liste der Entitäten und im Modul Bibliotheken anzeigen. Importierte Daten werden in den Tabellen „Einträge für angreifbare Elemente in der Anwendung“ [sn_vul_app_vul_entry] und „Einträge in National Vulnerability Database“ [sn_vul_nvd_entry] gespeichert.

Hinweis:
Sie können den Integrationsparameter von OSV.dev `batchSize` auf der Registerkarte Integrationsparameter in der **Open Source-Schwachstelleninstanz** unter konfigurieren **Alle** > **Vulnerability Response** > **Administration** > **Integrationen** > **Schwachstellen-Integrationen** > **Open Source-Schwachstelleninstanz**. Der Standardwert ist 75 PURLs pro API-Aufruf.

Unter Umständen möchten Sie diesen Wert in der Standardeinstellung beibehalten. Das Ändern des Werts kann sich auf die Leistung auswirken.

PaCE wird aktiviert

Ab Version 4.0 von SBOM Response können Sie Komponenten, die als veraltet oder verworfen als „Nicht konform“ gekennzeichnet sind, in der Schnittstelle Policy as Code Engine (PaCE) anzeigen, die im Arbeitsbereich SBOM verfügbar ist.

- Ermitteln Sie mit der geplanten Aufgabe `Run PaCE policies for SBOM Response`, ob Komponenten veraltet oder verworfen sind. Diese geplante Aufgabe ist standardmäßig deaktiviert.
- Zeigen Sie Komponenten an, die in der PaCE-Schnittstelle, die im -Arbeitsbereich SBOM verfügbar ist und angezeigt wird, als veraltet oder als nicht konform eingestuft wurden.

Weitere Informationen zu PaCE und PaCE-Richtlinien finden Sie unter Integrating PaCE with other applications .

Ihre SBOM -Dateien werden im SBOM -Arbeitsbereich hochgeladen und dort angezeigt

Mit den SBOM -Anwendungen können Sie im Software-Stücklisten-Arbeitsbereich Dateien hochladen und Details für Entitäten, Komponentenbestände, Lizenzinformationen und andere Details anzeigen.

Übersicht über das Hochladen von SBOM Dateien

Sie können Ihre Software-Stücklistendateien über eine API oder manuell hochladen. Zeigen Sie die Dateien an, die Sie als Entitäten importieren. Hierbei handelt es sich um Bestände der in Ihrer Software verwendeten Komponentenbibliotheken von Drittparteien, einschließlich vorübergehender Abhängigkeiten.

- Software Bill of Materials -Dateien werden mit einer REST-API hochgeladen.

  Die Upload-API wird zum Hochladen und Erfassen einer SBOM -Datei (CycloneDX/SPDX) in Ihre -Instanz verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Software Bill of Materials Dateien manuell hochladen.

  Laden Sie Software-Stücklistendateien manuell hoch. Die Methode zum Hochladen Ihrer Dateien hängt davon ab, ob Sie die Anwendungen SBOM Core oder SBOM Response installiert haben.

- Software Bill of Materials für DevOps-Dateien SBOM werden hochgeladen.

  Generieren und laden Sie SBOM -Dateien für Software während der Entwicklungszyklen für kontinuierliche Integration und kontinuierliche Bereitstellung hoch.

- Klassifizieren und lösen Sie Komponentenlizenzen im Lizenzverwaltungsmodul.

  Überprüfen Sie die Klassifizierungund lösen Sie die Lizenzinformationen für die Komponenten, die Sie in Ihre Dateien SBOM hochladen, gemäß Ihren internen oder gesetzlichen Richtlinien auf. Sie können Ihre Komponenten Lizenzen zuordnen und Ihre allgemeine Lizenz-Compliance bestimmen, um Ihr potenzielles Risiko für verbotene, eingeschränkte oder fehlende Lizenzen anzuzeigen.

- Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials

  Schwachstellenanalysten und -manager können im -Arbeitsbereich Software Bill of Materials (SBOM) hochgeladene Software-Stücklistendateien und wichtige Daten in Datensätzen, Datenvisualisierungen sowie erweiterte Schwachstelleninformationen anzeigen.

  Hinweis:
  Sie müssen SBOM Response installieren, wenn Sie die Datenvisualisierungen auf der Zielseite (Homepage) des -Arbeitsbereichs anzeigen möchten.

Software Bill of Materials -Dateien werden mit einer REST-API hochgeladen

Lesen Sie sich die folgenden Informationen durch, bevor Sie Software Bill of Materials -Dateien mit einer API hochladen.

Mithilfe der REST API

Zum Hochladen einer SBOM-Datei mit einer API ist die Rolle sn_sbom_core.sbom_ingest erforderlich.

Upload-API.

Diese API wird zum Hochladen und Erfassen einer SBOM-Datei (CycloneDX/SPDX) in Ihre Instanz verwendet.

Version 4.0 von SBOM Core unterstützt:

- XML und JSON in CycloneDx (Versionen 1.0–1.6).
- JSON in SPX (Versionen 2.2–2.3)

- **Hinweis:**
  Dateien über 32 MB werden möglicherweise nicht ordnungsgemäß geladen.

HTTP-Methode: (POST)

API-URL:<host_name> `/api/sbom/core/upload`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
<host_name>ist Ihr Instanzname ServiceNow .

Alle folgenden Anforderungsparameter sind optional. Der Anforderungstext ist der Inhalt der SBOM-Datei. Wenn Sie DevOps als Teil Ihres Entwicklungsprozesses verwenden, sollte der Wert von „requestedBy“ „devops“ lauten. Allgemeine Informationen zu DevOps finden Sie unter Software Bill of Materials für DevOps-Dateien SBOM werden hochgeladen. Wenn der Wert für „requestedby“ „devops“ (Entwicklungsvorgänge) ist, sind die folgenden Parameter obligatorisch:

- buildId
- Lebenszyklusphase

Wenn „requestedBy“ auf „devops“ festgelegt ist, werden Daten für „fetchVulenrabilityInfo“ und „fetchPackageInfo“ eingeschlossen.

- buildId: Von Ihnen gesendete Zeichenfolge
- Lebenszyklusphase: Zwei Werte: „Produktion“ oder „Vorproduktion“.
- fetchVulenrabilityInfo: t/f
- fetchPackageInfo-t/f

Anforderungsparameter	Mögliche Werte	Beschreibung
Produktmodell-ID	Sys-ID	Sys-ID des Produktmodells, das der Stammanwendung des angegebenen SBOMzugeordnet werden soll.
businessApplicationId	Sys-ID	Sys-ID der Geschäftsanwendung, die der Stammanwendung des angegebenen SBOMzugeordnet werden soll.
businessApplicationName (veraltet)	Name Ihrer Geschäftsanwendung	Name der Geschäftsanwendung, die der Stammanwendung des angegebenen SBOMzugeordnet werden soll.
sbomSource	Ein Produkt wie beispielsweise Veracode	Die Quelle für Ihre SBOM -Datei.
requestedBy	Ein Tool oder Name einer Methode, Jenkins. Wenn Sie „devops“ verwenden, sind „buildId“ und „lifecycleStage“ obligatorisch.	Upload angefordert von
buildId	Eine anfordernde Person sendet eine Zeichenfolge.	Build-ID des SBOM -Builds.
Lebenszyklusphase	„Produktion“ oder „pre_produktion“.	Lebenszyklusphase der Entität.
abrufenVulenrabilityInfo	t/f	Bei „wahr“ wird die Vulnerability Intelligence-Integration ausgelöst.
abrufenPaketinformationen	t/f	Bei „wahr“ wird die Package Intelligence-Integration ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Antwort für Upload: „status“ erfolgreich/fehlgeschlagen, „message“ (Zeichenfolge), „bomRecordId“ (dies ist die Sys-ID des SBOM, die über die Upload-API für einen erfolgreichen SBOM-Upload zurückgegeben wird).

```
{

"result": {

"status": "success",

"message": "Queued for processing.",

"bomRecordId": "f207059b4393c290629aa597cbb8f247"

}

}
```

Status-API

Diese API ruft den Status und die Zusammenfassung einer SBOM ab, die sich in der Warteschlange zur Erfassung befindet.

- API-URL: `/api/sbom/core/upload/status`
- HTTP-Methode (GET)

Anforderungsparameter	Mögliche Werte	Beschreibung
Stücklistendatensatz-ID	Sys-ID	SBOM-Datensatz-ID, die über die Upload-API für einen erfolgreichen SBOM-Upload zurückgegeben wird.

Beispiel für die Standardantwort der Status-API.

```
{
  "result": {
    "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
    "uploadStatus": "processed",
    "additionalInfoStatus": "not_requested",
    "uploadSummary": {
      "components": {
        "added": 0,
        "removed": 0,
        "total": 70
      }
    }
  }
}
```

Beispiel für die Status-API-Antwort mit zusätzlichen Parametern. Wenn Sie fetchVulenrabilityInfo für diese SBOM angefordert haben, erhalten Sie die Schwachstellenaufgliederung als Teil der Antwort.

```
{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"result": {
 "bomRecordId": "93af349b4393c290629aa597cbb8f258",
 "uploadStatus": "processed",
 "additionalInfoStatus": "complete",
 "uploadSummary": {
  "components": {
   "added": 0,
   "removed": 0,
   "total": 3
  },
  "vulnerabilityInfo": {
   "critical": 0,
   "high": 0,
   "medium": 0,
   "low": 0,
   "none": 0
  }
 },
 "buildId": "1"
}
}
```


Wenn Sie fetchPackageInfo für diese SBOM angefordert haben, erhalten Sie als Teil der Antwort die Anzahl der veralteten und verworfenen Elemente.

Nachdem ein SBOM erfolgreich verarbeitet wurde, hängt es von den verwendeten Anwendungen ab, wo Sie die hochgeladenen Datensätze anzeigen.

- Wenn Sie SBOM die -Antwort verwenden, wird der Stücklistenentitätsdatensatz in der Liste SBOM Erfassungsstatus im Modul Stücklistenwarteschlange im Arbeitsbereich SBOM angezeigt.
- Wenn Sie SBOM Core verwenden, navigieren Sie zu **SBOM-Core** > **Stücklisten-Erfassungsstatus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterungen der unterstützten Standards SBOM und allgemeine Informationen zur Verwendung

Version 4.0 von SBOM Core unterstützt:

- XML und JSON in CycloneDx (Versionen 1.0–1.6).
- JSON in SPX (Versionen 2.2–2.3)

- **Hinweis:**
  Dateien über 32 MB werden möglicherweise nicht ordnungsgemäß geladen.

Ab v4.0 von SBOM Core wurden die folgenden Erweiterungen vorgenommen, um die CycleDx-Standards für die Versionen 1.0 bis 1.6 zu unterstützen:

- Importieren Sie mit der Eigenschaft (sn_sbom_core.collekt_properties) zusätzliche Informationen in Epic-SBOM-Dateien. Diese Eigenschaft ist standardmäßig deaktiviert. Aktivieren Sie die Eigenschaft, um Informationen zu importieren, die allgemein nicht unterstützt werden. Alle aus diesen Eigenschaften importierten Informationen werden in die Tabelle „SBOM-Komponenteneigenschaft“ [sn_sbom_comp_property] hochgeladen:
  - SBOM-Dateien hochgeladen
  - Metadaten
  - Individuelle Schwachstellen
  - Komponenten
- Zeigen Sie importierte Komponentendaten für deklarierte und abgeschlossene Lizenzen für SBOM-Dateien in den Versionen 1.4 und höher von CycleneDX in zwei neuen Lizenzfeldern an:
  - **Deklariert**
  - **Abgeschlossen**
- Die Unterstützung für SBOM-Analysen wird für die folgenden CycleneDX-Komponententypen erweitert:
  - Version 1.5: Plattform, Daten, Gerätetreiber, Modell für maschinelles Lernen
  - Version 1.6: Kryptografisch

Version 3.0 von SBOM Core unterstützt:

- XML und JSON in RobotDx (bis einschließlich Version 1.4).
- JSON in SPX (bis einschließlich v2.3).

Wenn der aufrufende Benutzer erfolgreich authentifiziert wurde und in Ihrer Instanz ServiceNow über die Rolle sn_sbom_core.sbom_ingest verfügt, können Sie von außerhalb Ihrer Instanz auf die API zugreifen, um die Daten SBOM hochzuladen.

Nachdem die Daten hochgeladen wurden, werden sie analysiert. Bevor Daten analysiert werden, werden die folgenden Anforderungen verifiziert:

- Bei eingehenden Daten wird geprüft, ob es sich um gültiges JSON oder XML handelt.
- Das Stücklistenformat wird unterstützt. Ab Version 2.1 von SBOM Core werden die Formate RobotX (JSON und XML) und SPX (XML) unterstützt.
- Es sind mindestens Felder verfügbar, damit Daten analysiert werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem diese Prüfungen verifiziert wurden, wird in der Stücklistentabelle [sn_sbom_doc] ein Eintrag mit eingehenden Daten SBOM als Anhang vorgenommen.

Die Geschäftsregel *Process BOM file* wird automatisch als Ergebnis der Datensatzeinfügung und der Datenanalyse ausgelöst.

Hinweis:
Diese Geschäftsregel wird standardmäßig während der Installation von SBOM Core aktiviert.

Alle in einem SBOM aufgeführten Komponenten haben einen definierten Typ.

- Komponenten, für die SBOM -Dateien hochgeladen wurden, gelten als Stücklistenentitäten.
- Komponenten, die als type=library aufgeführt sind, gelten als Komponenten von Drittparteien.

Zugehörige Informationen

Zeigen Sie den Upload-Status für Software Bill of Materials -Dateien an

Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials

Software Bill of Materials Dateien manuell hochladen

Software Bill of Materials (SBOM) Dateien manuell hochladen.

Vorbereitungen
Ab Version 4.0 unterstützt SBOM Core:

- XML und JSON in den Versionen 1.0 bis 1.6 von CycleneDX.
- JSON in den Versionen 2.2 bis 2.3 von SPX.

Erforderliche Rolle: sn_sbom_core.sbom_ingest

Prozedur

1. Lädt die Dateien manuell hoch.

   Die Methode zum Hochladen Ihrer Dateien hängt davon ab, ob Sie die Anwendungen SBOM Core oder SBOM Response installiert haben.

2. **Wahlweise:** Laden Sie SBOM -Dateien hoch, die von Veracode Vulnerability Integrationimportiert wurden.

   Hinweis:
   Sie können Veracode -Dateien nur in den Formaten Epic (JSON und XML) und SPX (XML) hochladen, wenn Sie die Integration Veracode mit Application Vulnerability Responseinstalliert und aktiviert haben. Weitere Informationen finden Sie unter Veracode Vulnerability Integration.

Ergebnisse
Nachdem ein SBOM erfolgreich verarbeitet wurde, hängt der Upload-Status von den verwendeten Anwendungen ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie SBOM die -Antwort verwenden, wird der Stücklistenentitätsdatensatz in der Liste SBOM Erfassungsstatus im Modul Stücklistenwarteschlange im Arbeitsbereich SBOM angezeigt.
- Wenn Sie SBOM Core verwenden, navigieren Sie zu **SBOM-Core** > **Stücklisten-Erfassungsstatus**.

Zugehörige Informationen

Software Bill of Materials -Dateien werden mit einer REST-API hochgeladen

Software Bill of Materials für DevOps-Dateien SBOM werden hochgeladen

Generieren und laden Sie Software Bill of Materials SBOM -Dateien für Software während der Entwicklungszyklen für kontinuierliche Integration und kontinuierliche Bereitstellung hoch.

DevOps- und SBOM -Dateien

SBOM -Dateien können in mehreren Phasen während des gesamten Entwicklungslebenszyklus der kontinuierlichen Integration und kontinuierlichen Bereitstellung (CI/CD) von Software generiert werden. Die meisten Softwareentwicklungsvorgänge (DevOps) in Organisationen verwenden eine Art von CI/CD-Prozess, um kostspielige Fehler zu identifizieren und zu vermeiden, die nach dem Release auftreten könnten. In der gesamten CI/CD-Pipeline kann DevOps SBOM-Dateien generieren und proaktiv nach Schwachstellen und gefährdeten Komponenten suchen. Diese Prüfungen können Unternehmen dabei unterstützen, eine bessere Softwarequalität zu erreichen und später kostspielige Wartungsarbeiten zu vermeiden. Das Generieren von SBOM -Dateien ist für die erfolgreiche Implementierung und Automatisierung genauer Build-Bewertungen während der CI/CD-Entwicklung von entscheidender Bedeutung.

Das Hochladen von SBOM-Dateien aus Entwicklungspipelines wird ab den folgenden Versionen der SBOM -Anwendungen unterstützt.

Unterstützte Versionen

Anwendung	Unterstützte Versionen
Datenmodell für SBOM	v3.0, v2.0
SBOM Zentral	v5.0, v4.0, v3.0
SBOM Antwort	v5.0, v4.0, v3.2, 3.1

Anwendungsfälle

Durch das Generieren von SBOM -Dateien und Senden über die SBOM-Upload-API als Teil der DevOps-Build-Pipeline können Sie Zählungen für Folgendes bereitstellen, um zu bestimmen, ob die Pipeline erfolgreich sein oder fehlschlagen sollte:

- Komponenten hinzugefügt
- entfernte Komponenten
- Informationen zu Schwachstellen
- Paketinformationen (verworfene/veraltete Komponenten)

DevOps-Richtlinien und -Regeln für den Erfolg oder Misserfolg einer Pipeline können durch die Anzahl der Schwachstellen sowie durch Schwellenwerte für die Anzahl veralteter und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verworfener Komponenten definiert werden, die von der SBOM Status-API empfangen werden.

Bei einer fehlgeschlagenen Pipeline können DevOps-Benutzer in ihrer Instanz ServiceNow® auf Informationen über den fehlgeschlagenen Build zugreifen, um die Ursache und den Ursprung der Schwachstellen besser zu verstehen.

Unter Software Bill of Materials -Dateien werden mit einer REST-API hochgeladen finden Sie weitere Informationen zu Parametern (POST) und (GET) sowie zu URLs für die Upload- und Status-APIs.

Domain Separation

Alle Tabellen in den SBOM-Anwendungen sind domänengetrennt.

Lizenzen werden klassifiziert und Komponentenlizenzen im Arbeitsbereich Software Bill of Materials aufgelöst

Klassifizieren Sie Lizenzen, und ordnen Sie sie Komponenten zu (ordnen Sie sie zu), oder erstellen Sie Lizenzen im Lizenzverwaltungsmodul im Arbeitsbereich SBOM. Durch die Klassifizierung und Zuordnung von Lizenzen zu Ihren Komponenten können Sie die Lizenz-Compliance für die proprietären, Open Source- und vom Lieferanten bereitgestellten Softwarekomponenten bestimmen, die Sie in Ihre Dateien SBOM hochladen.

Lizenzdaten und Software von Drittparteien

Wenn Unternehmen mehr eigene Softwareanwendungen erstellen, verwenden sie Open Source-Komponenten und von Lieferanten bereitgestellte Software. Die Verwendung von Drittanbieter- und Open-Source-Komponenten bietet Ihnen viele Vorteile für die schnelle Erstellung und Veröffentlichung Ihrer Softwareprojekte. Die Verwendung dieser Komponenten birgt jedoch Lizenzierungsrisiken:

- Open Source-Softwarekomponenten und vom Lieferanten bereitgestellte Softwarekomponenten sind zeitweise von anderen Komponenten abhängig, und für jede Komponente gelten möglicherweise eigene Lizenzierungsanforderungen.
- Wenn Sie die Bedingungen Ihrer Lizenzen für die Komponenten und die Software in Ihren Anwendungen nicht einhalten, versenden Sie möglicherweise versehentlich Code, der gegen Ihre internen Richtlinien und die gesetzlichen Lizenzierungsanforderungen verstößt.

Lizenzverwaltungsmodul

Mit dem Lizenzverwaltungsmodul im SBOM-Arbeitsbereich können Sie die folgenden Aufgaben ausführen.

- Klassifizieren Sie Lizenzen, die dies für die Komponenten erfordern, die Sie mit Ihren SBOM -Dateien hochladen.
- Lösen Sie jede Lizenz, die Sie für eine bestimmte Komponente klassifizieren, auf.
- Sehen Sie in einer Datenvisualisierung auf der Homepage, wie viel Prozent der von Ihnen verwendeten Komponenten nicht konform sind. Sie können diese Informationen verwenden, um Ihre allgemeine Sicherheitslage und Ihr potenzielles Risiko zu bestimmen.

Wenn die von Ihnen hochgeladenen Dateien SBOM Lizenzinformationen enthalten, wird die Lizenzdatenbank automatisch erweitert, da bei jedem SBOM-Upload eindeutige Lizenzen zu beachten sind. Bei jedem SBOM-Upload können Sie eine Datenbank der hochgeladenen Lizenzen erstellen und sie dann bei Bedarf mit dem Lizenzverwaltungsmodul im Arbeitsbereich SBOM klassifizieren. Sie erstellen einen Bestand von Lizenzen, damit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie sie Komponenten zuweisen können, nachdem Sie sie in eine der folgenden Kategorien klassifiziert haben:

- Zulässig
- Beschränkt
- Gesperrt
- Nicht klassifiziert

Juristisches Personal, Lizenzmanager, Compliance-Manager und Manager für regulatorische Angelegenheiten führen im Modul Lizenzverwaltung Aufgaben aus.

Hochgeladene Lizenzdaten werden angezeigt

Sie haben die folgenden Optionen, um alle Lizenzinformationen anzuzeigen, die Sie mit Ihren Komponenten in den SBOM-Arbeitsbereich hochgeladen haben.

- Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Komponenten**.

  Auf der Seite „Komponenten“ zeigt die Karte Lizenzklassifizierung von Komponenten eine Visualisierung Ihrer allgemeinen Lizenz-Compliance mit den folgenden Kategorien an.

Kategorie	Beschreibung
Gesperrt	Lizenzierte Nutzung ist nicht zulässig.
Klassifizierung erforderlich	Die Lizenz ist noch nicht klassifiziert und erfordert eine Überprüfung.
Zulässig	Die lizenzierte Nutzung ist ohne Einschränkung zulässig.
Beschränkt	Die lizenzierte Nutzung ist in bestimmten Anwendungsfällen nicht zulässig.

  Dieser Snapshot verwendet die Klassifizierungen und aufgelösten Lizenzinformationen, die Sie im Lizenzverwaltungsmodul eingeben, um Ihre allgemeine Lizenz-Compliance zu berechnen.

  Wenn Sie einen Komponentendatensatz aus dieser Liste auswählen, können Sie die Lizenzinformationen der Komponente zusammen mit anderen Informationen im Feld Status anzeigen.

- Alternativ navigieren Sie zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Lizenzverwaltung** > **Lizenzklassifizierung**.

  Auf dieser Seite wird die Gesamtzahl der eindeutigen Lizenzen nachverfolgt, die in den von Ihnen hochgeladenen SBOM-Dateien erkannt wurden. Außerdem werden sie in den Karten oben auf der Seite in den folgenden Kategorien gefiltert.
  - Nicht klassifiziert: Lizenz erfordert Überprüfung und Klassifizierung.
  - Gesperrt: Lizenznutzung ist nicht zulässig.
  - Eingeschränkt: Lizenz ist in bestimmten Anwendungsfällen nicht zulässig.
  - Zulässig: Die Lizenznutzung ist ohne Einschränkung zulässig.
  - Alle Lizenzen: Gesamtanzahl der Lizenzen.

  Alle Komponenten in Ihrer Organisation verwenden eine der auf dieser Seite aufgeführten Lizenzen. Wenn in einem SBOM-Upload eine neue Lizenz erkannt wird, wird ein Datensatz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellt, in der SBOM-Lizenztabelle [sn_sbom_license] gespeichert und dieser Liste hinzugefügt. Die standardmäßige Klassifizierung lautet **Klassifizierung erforderlich**. Lizenzdatensätze in diesem Status müssen überprüft und klassifiziert werden, bevor Sie sie auflösen (zuordnen) können, damit Ihre Lizenz-Compliance insgesamt genau berechnet wird.

Informationen zur Klassifizierung von Lizenzen finden Sie unter Klassifiziert importierte -Lizenzen im -Arbeitsbereich Software Bill of Materials ..

Rollen

Neue Lizenzen müssen von einem Benutzer mit der Rolle sn_sbom_response.managelicense klassifiziert werden. Dieser Anwender zeigt hochgeladene Lizenzinformationen an und bestimmt, welche Lizenzen zulässig und welche verboten sind. Benutzer mit dieser Rolle können das Modul „Komponentenlizenzauflösung“ nur anzeigen, wenn sie über die Rolle sn_sbom_response.licenseresolver verfügen.

Nach der Klassifizierung müssen Lizenzen von einem Benutzer mit der Rolle sn_sbom_response.licenseresolver gelöst werden, damit die allgemeine Lizenz-Compliance bestimmt werden kann. Dieser Anwender löst Lizenzen für Komponenten auf. Benutzer mit dieser Rolle können das Lizenzklassifizierungsmodul nur anzeigen, wenn sie über die Rolle sn_sbom_response.managelicense verfügen.

Die Klassifizierung neuer Lizenzinformationen ist ein fortlaufender Prozess. Möglicherweise möchten Sie die auf der Karte „Nicht klassifiziert“ angezeigte Gesamtzahl niedrig halten. Als Lizenzmanager möchten Sie möglicherweise alle paar Tage und nach dem Hochladen von SBOM-Dateien nach Lizenzen suchen, die klassifiziert werden müssen.

Als Lizenzlöser möchten Sie möglicherweise alle paar Tage nach aktualisierten klassifizierten Lizenzen suchen.

Klassifiziert importierte -Lizenzen im -Arbeitsbereich Software Bill of Materials .

Klassifizieren Sie die Komponentenlizenzen, die Sie mit Ihren SBOM -Dateien hochladen, mit der Lizenzklassifizierungsfunktion.

Vorbereitungen

Die Klassifizierung neuer Lizenzinformationen ist ein fortlaufender Prozess. Möglicherweise möchten Sie die auf der Karte „Nicht klassifiziert“ angezeigte Gesamtzahl niedrig halten. Als Lizenzmanager möchten Sie möglicherweise alle paar Tage und nach dem Hochladen von SBOM-Dateien nach Lizenzen suchen, die klassifiziert werden müssen.

Erforderliche Rolle: sn_sbom_response.managelicense

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Lizenzverwaltung** > **Lizenzklassifizierung**.

   Hinweis:
   Sofern Sie nicht auch über die Rolle sn_sbom_response.licenseresolver verfügen, ist nur die Registerkarte Lizenzklassifizierung sichtbar.

2. **Wahlweise:** Wählen Sie eine Karte aus, um Lizenzen anhand ihrer Klassifizierungen zu filtern.
3. Um Lizenzen zu klassifizieren, wählen Sie eine aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Nachdem Sie Lizenzen klassifiziert haben, können Sie Klassifizierte Lizenzen für Komponenten auflösen.

Lösen Sie Lizenzen für Komponenten im Arbeitsbereich Software Bill of Materials auf

Lösen Sie klassifizierte Lizenzen für bestimmte Komponenten mit der Funktion „Komponentenlizenzlösung“ auf (ordnen Sie sie zu). Weisen Sie Komponenten mit fehlenden oder falschen Lizenzinformationen Lizenzen zu, oder erstellen Sie neue Lizenzen, damit Ihre allgemeine Lizenz-Compliance berechnet werden kann.

Vorbereitungen
Erforderliche Rolle: sn_sbom_response.licenseresolver

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Lizenzverwaltung** > **Komponentenlizenzlösung**.

   Hinweis:
   Sofern Sie nicht auch über die Rolle sn_sbom_response.managelicense verfügen, ist nur die Registerkarte Komponentenlizenzlösung sichtbar.

   Diese Seite verfolgt die Gesamtzahl der eindeutigen Lizenzen und bietet eine Übersicht der Gesamtlizenzen, die in den von Ihnen hochgeladenen SBOM-Dateien erkannt wurden. Die auf dieser Seite angezeigten Lizenzen fallen unter zwei große Kategorien, je nachdem, wie sie sich auf Komponenten beziehen.

   - Alle Instanzen der Komponente stimmen einer Lizenz zu.
   - Es besteht eine Meinungsverschiedenheit bei einer einzelnen Lizenz, und für eine Komponente ist mehr als eine Lizenz vorhanden.

   Im zweiten Fall müssen Sie diese Lizenzen abgleichen, damit eine einzelne Lizenz für eine einzelne Komponente aufgelöst wird. Die Lizenz-Compliance wird basierend auf einer gelösten Lizenz pro Komponente berechnet.

   Die Lizenzen auf dieser Seite sind in die folgenden Kategorien gefiltert, um Ihnen bei der Lösung zu helfen.

Wert	Beschreibung
Komponenten mit nicht aufgelösten Lizenzen	Der Komponente ist keine Lizenz zugewiesen, und sie muss gelöst werden. (leer) wird in der Spalte Gelöste Lizenz für diese Komponenten angezeigt. Sowohl fehlende als auch mehrere Lizenzen insgesamt werden als Teil dieser Kategorie aufgeführt.
Komponenten mit fehlenden Lizenzen.	Komponenten mit fehlenden Lizenzinformationen, die gelöst werden müssen.
Komponenten mit mehreren Lizenzen	Komponenten, die für mehrere Entitäten mit unterschiedlichen Lizenzen sichtbar sind und eine Lösung erfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
Alle Komponenten	Gesamtliste der in Ihrer Organisation nachverfolgten Komponenten. Sie können Lizenzen in dieser gefilterten Liste ändern.

2. Wählen Sie eine Karte aus.
3. Wählen Sie eine aus, um eine Lizenz aufzulösen.

4. Navigieren Sie im SBOM-Arbeitsbereich zur Homepage, um zu sehen, wie viel Prozent der von Ihnen verwendeten Komponenten in der Visualisierung Lizenzklassifizierung von Komponenten nicht konform sind.
   Die Daten für diese Visualisierung werden täglich von der geplanten Aufgabe „Lizenzaufgliederung der Stücklistenkomponenten“ aktualisiert. Diese Aufgabe ist Teil der geplanten Aufgabe „SBOM-Berichte – Datensammler“, die täglich ausgeführt wird.

Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials

Schwachstellenanalysten zeigen hochgeladene Software-Stücklistendateien in Datensätzen, Datenvisualisierungen sowie erweiterte Schwachstelleninformationen im -Arbeitsbereich Software Bill of Materials (SBOM) an.

SBOM Zentral

Sie können Stücklistenentitäten und eine Liste der von Ihnen hochgeladenen Komponenten auf der Homepage (Zielseite) und im Modul Komponenten im Arbeitsbereich SBOM anzeigen.

SBOM Antwort

Die Anwendung SBOM Response bietet Ihnen Datenvisualisierungen mit detaillierten Informationen zu Stücklistenentitäten, Entitäten mit Schwachstellen und aktiven angreifbaren Anwendungselementen auf der Startseite (Zielseite) im Arbeitsbereich SBOM. Der -Arbeitsbereich mit der Antwort SBOM enthält die folgenden Module:

- Homepage – Datenvisualisierungen und erweiterte Schwachstellendetails.
- Komponenten: Versions- und Korrekturinformationen für Komponenten und Lizenzklassifizierung von Komponenten.
- Erstellungsregeln für AVIT (angreifbares Anwendungselement): Bedingungen für die Erstellung von angreifbaren Elementen in der Anwendung (Application Vulnerable Items, AVITs).
- Stücklistenwarteschlange: Status und Verlauf des Datei-Uploads.
- Liste: AVIT-Datensätze für Ihre angreifbaren Komponenten und Bibliotheken (NVD, CWE und Anwendungsschwachstellen).

Die folgenden Themen enthalten weitere Informationen dazu, wie Sie Details zu Ihren -Komponenten im -Arbeitsbereich Software Bill of Materials finden.

- Überprüfen Sie die Homepage im Arbeitsbereich Software Bill of Materials .
- Überprüfung des Komponentenmoduls im Arbeitsbereich Software Bill of Materials
- Zeigen Sie den Upload-Status für Software Bill of Materials -Dateien an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine Software Bill of Materials -Entität wird auf Schwachstellen überprüft
- Lizenzen werden klassifiziert und Komponentenlizenzen im Arbeitsbereich Software Bill of Materials aufgelöst

Überprüfen Sie die Homepage im Arbeitsbereich Software Bill of Materials .

Für hochgeladene Daten wird ein Rollup zu den Visualisierungen auf der Zielseite (Homepage) im Arbeitsbereich Software Bill of Materials (SBOM) durchgeführt. Daten werden geändert, nachdem Sie Dateien hochgeladen haben, sodass Schwachstellenanalysten Trends anzeigen und aktuelle Informationen zu Ihren Komponenten überprüfen können.

Vorbereitungen
Erforderliche Rolle: sn_sbom_resp.sbom_analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich**.
   Standardmäßig wird die Zielseite (Startseite) von angezeigt.

   Was Sie im Modul sehen können, hängt von den installierten Anwendungen ab.

   Importierte Daten werden nicht durch Live-Abfragen berechnet und ausgefüllt. Die Punktzahlen auf den Seiten „Homepage“ und „Komponenten“ werden einmal täglich mit Leistungsverbesserungen für die Berichterstellung aktualisiert. Diese Erweiterung ermöglicht Ihnen möglicherweise schnellere Ladezeiten für die Bewertungslisten in den Modulen Startseite und Komponenten im Arbeitsbereich SBOM.

   Diese Erweiterungen haben keine Auswirkungen darauf, wie oder wo Daten gespeichert werden.

Installierte Anwendung	Beschreibung
Wenn Sie SBOM Core installiert haben	Alle Stücklistenentitäten. Die Liste enthält den Namen, den Klassifizierer (Anwendung, Container, Bibliothek usw.) und die Komponentenanzahl für jede Entität. Eine Stücklistenentität bezieht sich auf die Komponente der Stammebene in einer Datei SBOM, für die ein Dokument SBOM generiert und hochgeladen wurde. Navigieren Sie im Arbeitsbereich zur Homepage, um die Liste der Stücklistenentitäten anzuzeigen.
Wenn Sie SBOM Response installiert haben	Die folgenden Datenvisualisierungen werden angezeigt. ○ Alle Stücklistenentitäten: Eine Aufgliederung der Stücklistenentitäten nach Typ: Anwendung, Container, Bibliothek und Andere. Eine Stücklistenentität bezieht sich auf die Komponente der Stammebene in einer Datei SBOM, für die ein Dokument SBOM generiert und hochgeladen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Anwendung	Beschreibung
	○ Stücklistenentitäten mit Schwachstellen: Entitäten, die eine Schwachstelle aufweisen, die einer Komponente zugeordnet ist, von der sie abhängig sind. Wenn eine Entitätsabhängigkeit eine **kritische** Schwachstelle aufweist, wird der Schweregrad der Entität als kritisch betrachtet. ○ Aktive AVIs: Der Trend für die Anzahl der pro Tag erstellten angreifbaren Elemente in der Anwendung. Die Datenvisualisierungen zeigen Daten für die letzten 30 Tage an. Der 30-Tage-Bereich kann nicht bearbeitet werden. Diese Daten sind verfügbar, nachdem Sie die Erstellungsregeln für angreifbare Anwendungselemente überprüft und eingerichtet haben. Weitere Informationen finden Sie unter Erstellen von Regeln für angreifbare Anwendungselemente im Arbeitsbereich Software Bill of Materials.

2. Wählen Sie eine Datenvisualisierungskarte aus, um die Liste der Datensätze anzuzeigen.
3. Wählen Sie die Registerkarte **Homepage** aus, um zur Zielseite zurückzukehren.
4. Alternativ können Sie einen Datensatz in der Liste **der Stücklistenentitäten** auswählen.

   Der Name und die Version der Entität werden oben im Datensatz angezeigt, z. B. SNC-SECOPS-SIR2.0.

   Hinweis:
   Mit dem Lizenzverwaltungsmodul wird die Entitäts-Lizenz-Beziehung in dieser Liste nicht angezeigt. Um die Entitäten anzuzeigen, in denen eine Komponente verwendet wird, navigieren Sie zum Komponentenmodul, und öffnen Sie einen Komponentendatensatz. Im Komponentendatensatz können Sie den Status anzeigen: „Ungelöst“ oder „Nicht klassifiziert“.

5. Wählen Sie die Registerkarten im Entitätsdatensatz aus, um die Daten zu überprüfen.

   a. Wenn dies nicht ausgewählt ist, wählen Sie die Registerkarte **Übersicht**.

   Überprüfen Sie die Daten. Wenn ein Feld in diesem Datensatz nicht ausgefüllt ist, wurden die Daten nicht in den von Ihnen hochgeladenen SBOM -Dateien enthalten.

Name	Beschreibung
Name	Entitätsname
Klassifizierung	Entitätstyp, z. B. eine Anwendung, Komponente oder Bibliothek.
Version	Versionsnummer der Entität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Lieferant	Produkt, das die Entität bereitgestellt hat.
Produktmodell	Wenn kein Produktmodell vorhanden ist oder Sie zum Zeitpunkt des SBOM -Uploads über die API keines hinzufügen, wird eines erstellt. Der Name der Entität wird für den Produktmodelldatensatz verwendet, z. B. SNC-SECOPS-SIR2.0.

b. Wählen Sie die Registerkarte **Abhängig von aus**.

Alle Abhängigkeiten dieser Entität werden zusammen mit Klassifizierern aufgelistet, z. B. Bibliothek. Die Versionsnummer, Lizenzenund andere Informationen werden angezeigt.

Durch Auswählen eines Links in dieser Liste wird ein Datensatz geöffnet. Die Registerkarte wird unter den Registerkarten Homepage und Entitätsdatensatz angezeigt. Der von Ihnen geöffnete Datensatz enthält möglicherweise die folgenden zugehörigen Listen, die Sie überprüfen können: Übersicht, Hashes, Stücklistenentitäten, Schwachstellenund angreifbare Elemente in der Anwendung (Application Vulnerabilities Items, AVITs).

In der zugehörigen Liste „Stücklistenentitäten“ werden alle Entitäten angezeigt, in denen dieses angezeigte Element verwendet wird.

c. Wählen Sie die Registerkarte **Schwachstellen** aus, um die Schwachstellen anzuzeigen, die einer Abhängigkeit dieser Entität zugeordnet sind.

Weitere Informationen zu den für eine Entität angezeigten Schwachstellen finden Sie unter Zeigen Sie den Upload-Status für Software Bill of Materials -Dateien an.

d. Wählen Sie die Registerkarte **AVIs** aus, um zu sehen, ob angreifbare Anwendungselemente für diese Entität vorhanden sind.

6. Wahlweise: Nachdem Sie Datensätze überprüft haben, können Sie einen oder mehrere Stücklistenentitäts-Datensätze löschen, wenn Sie feststellen, dass Sie sie nicht mehr benötigen.

Hinweis:
Durch das Löschen von Stücklisten-Entitätsdatensätzen werden sie und ihre Komponentenbeziehungen dauerhaft entfernt. Alle angreifbaren Elemente der Anwendung (Application Vulnerable Items, AVIT), die den Stücklistenentitäten zugeordnet sind, gehen in **den Status Geschlossen**über. Wenn Sie später entscheiden, dass die Datensätze und Komponentenbeziehungen, die Sie gelöscht haben, wieder in der Liste der Stücklistenentitäten angezeigt und im Arbeitsbereich verfügbar sein sollen, müssen Sie diese Stücklistenentitäten erneut hochladen.

a. Wenn Sie sich nicht auf der Homepage befinden, wählen Sie die Registerkarte **Homepage**, um dorthin zurückzukehren.

b. Wählen Sie in der Liste **„Stücklistenentitäten** “ die Datensätze aus, die Sie löschen möchten.

c. Wählen Sie **Löschen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfung des Komponentenmoduls im Arbeitsbereich Software Bill of Materials

Das Modul Komponenten im Arbeitsbereich Software Bill of Materials (SBOM) zeigt aktuelle Informationen über angreifbare, veraltete, verworfene und risikoreiche Kombinationen für die von Ihnen importierten Komponenten an.

Komponentenmodul anzeigen

Erforderliche Rolle: sn_sbom_resp.sbom_analyst

Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Komponenten**.

Was Sie im Modul sehen können, hängt von den installierten Anwendungen ab.

Importierte Daten werden nicht durch Live-Abfragen berechnet und ausgefüllt. Die Punktzahlen auf den Seiten „Homepage“ und „Komponenten“ werden einmal täglich mit Leistungsverbesserungen für die Berichterstellung aktualisiert. Diese Erweiterung ermöglicht Ihnen möglicherweise schnellere Ladezeiten für die Bewertungslisten in den Modulen Startseite und Komponenten im Arbeitsbereich SBOM.

Diese Erweiterungen haben keine Auswirkungen darauf, wie oder wo Daten gespeichert werden.

Installierte Anwendung	Beschreibung
Wenn Sie SBOM Core installiert haben	Ein Bestand aller hochgeladenen Komponenten mit den folgenden Informationen: • Name • Beschreibung • Version • Anzahl der Stücklistenentitäten
Wenn Sie SBOM Response installiert haben	Wählen Sie ein Diagramm oder eine Zahl im Diagramm aus, um eine Liste der zugehörigen Datensätze anzuzeigen. **Alle Komponenten** Liste der **veralteten** und **verworfenen** Komponenten sowie der Komponenten mit mindestens einer Schwachstelle in Ihrer Gesamtkomponentenanzahl. Diese Anzahlen können Ihnen helfen, Komponenten zu identifizieren, die Ihre Aufmerksamkeit erfordern. Diese Teilmengen von Komponenten stimmen möglicherweise nicht mit Ihrer Gesamtkomponentenanzahl überein, da möglicherweise nicht alle Ihre Komponenten in diese Kategorien passen. • Die Version einer veralteten Komponente ist mehr als zwei Hauptversionen älter als die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Anwendung	Beschreibung
	aktuelle Version und zwei Jahre älter als die aktuelle Version. • Eine verworfene Komponente wurde seit mehr als zwei Jahren nicht mehr aktualisiert. • Angreifbare Komponenten sind Komponenten, die Schwachstellen mit dem Schweregrad „ **Hoch“** oder höher aufweisen. **Kombinationen mit hohem Risiko** Komponenten mit hohem Risiko erfordern möglicherweise Ihre sofortige Aufmerksamkeit. Die Deps.dev-Integration, die bei der Installation der Anwendung SBOM Response installiert wird, stellt die Pakete Intelligence für Komponenten im Status „ **Veraltet“** und „ **Verworfen** “ bereit. Importierte Kombinationen mit hohem Risiko bestehen aus veralteten und verworfenen Komponenten mit mindestens einer schwerwiegenden Schwachstelle (**Kritisch** oder **Hoch**), die Sie durch Updates, Austausch oder eine andere Art der Reparatur beheben können. Der Status **„Vollständig reparierbar“** bedeutet, dass für eine Komponente eine Version verfügbar ist, mit der das Problem behoben werden kann. Der Prozentsatz der Gesamtzahl der Komponenten mit hohem Risiko, die über reparierbare Versionen verfügen, wird angegeben. **Behebbarkeit angreifbarer Komponenten** Gesamtsummen und Aufgliederungen der Komponenten mit Schwachstellen **vom Typ „Kritisch“**, **„Hoch“**, **„Mittel“**und **„Niedrig“**, und gibt an, ob einige oder alle ihrer Schwachstellen behoben werden können. Wenn eine Komponente mehr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Anwendung	Beschreibung
	als eine Schwachstelle aufweist, hat die kritischste Schwachstelle Vorrang. Der Behebbarkeitsstatus: • Abgeschlossen – Es gibt Korrekturversionen für alle Schwachstellen, die der aktuellen Version der Komponente zugeordnet sind. • Teilweise: Es gibt eine Korrekturversion für mindestens eine, aber nicht alle Schwachstellen, die der aktuellen Version der Komponente zugeordnet sind. **Lizenzklassifizierung von Komponenten** Gesamtsummen und Aufgliederungen der Komponenten nach Lizenzklassifizierung. In der Komponentenliste unter den Visualisierungen können Sie Name, Beschreibung, Version und Anzahl der Entitäten anzeigen. Im rechten Bereich können Sie einen Versionsverlauf anzeigen. Die aktuelle Version wird im Versionsverlauf hervorgehoben. Die Spalten Allgemeine Schwachstellen und Gefährdung (**CVE**) und **Behebbarkeit** werden ebenfalls angezeigt.

Risiko mit Vulnerability Intelligence bewerten

Weitere Informationen zum Überprüfen von Vulnerability Intelligence-Daten im -Arbeitsbereich finden Sie unter Eine Software Bill of Materials -Entität wird auf Schwachstellen überprüft.

Risiko mit Lizenz-Compliance bewerten

Unter Lizenzen werden klassifiziert und Komponentenlizenzen im Arbeitsbereich Software Bill of Materials aufgelöst finden Sie weitere Informationen zum Lizenzieren von Daten, die Sie mit Ihren Komponenten importiert haben, und zum Anzeigen Ihrer allgemeinen Lizenz-Compliance im -Arbeitsbereich.

Erstellen von Regeln für angreifbare Anwendungselemente im Arbeitsbereich Software Bill of Materials

Bevor Sie im Arbeitsbereich für Stücklistenelemente für Software (SBOM) angreifbare Elemente in der Anwendung anzeigen können, müssen Sie die Bedingungen einrichten, unter denen AVITs erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AVITs im Arbeitsbereich SBOM

Wenn Sie die Anwendung SBOM Response installiert und aktiviert haben, werden AVITs für SBOM -Dateien erstellt, wenn eine der importierten Daten den Bedingungen Ihrer vorhandenen AVIT-Erstellungsregeln entspricht.

Die Anwendungen SBOM Response und Vulnerability Response sind erforderlich, um Regeln für die automatische Erstellung von angreifbaren Elementen in der Anwendung (Application Vulnerable Items, AVITs) und deren Nachbesserung mit dem Workflow Application Vulnerability Response einzurichten. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Als Benutzer mit der Rolle sn_sbom_resp.manage_avi_rule müssen Sie im Arbeitsbereich SBOM AVIT-Erstellungsregeln hinzufügen, bevor Sie AVITs für die Schwachstellen erstellen können, die in Ihren erfassten Daten SBOM gefunden wurden. Mit AVITs können Sie die Integrität der Drittanbieterkomponenten in Ihren Anwendungen bewerten. Ein AVIT wird in Ihrer Instanz erstellt, wenn eine Anwendung mit einer Komponente abgeglichen wird, die eine zugeordnete Schwachstelle aufweist.

Im Arbeitsbereich SBOM können Sie nur SBOM-AVITs anzeigen. Sie können jedoch SBOM AVITs zusammen mit anderen Arten von angreifbaren Elementen im Arbeitsbereich des Schwachstellenmanagers in Vulnerability Responseanzeigen. Sie können alle AVITs anzeigen, die im SBOM-Arbeitsbereich im Listenmodul erstellt wurden. Das Listenmodul enthält auch alle NVD- und CWE-Einträge sowie Anwendungsschwachstellen.

Sie können AVITs auch zur Korrektur zuweisen, basierend auf Empfehlungen aus Listen bekannter Schwachstellen, z. B. der National Vulnerability Database (NVD). Eine geplante Aufgabe wird ausgelöst, und wenn die Bedingungen Ihrer Erstellungsregeln mit den erfassten Daten übereinstimmen, werden AVITs erstellt.

Sie können AVITs nachverfolgen und beheben, indem Sie anwenderdefinierte Regeln einrichten.

Informationen zum Erstellen von Regeln finden Sie unter Erstellen Sie im Software Bill of Materials -Arbeitsbereich eine Regel für angreifbare Anwendungselemente.

SBOM AVITs in Vulnerability Manager Workspace in Vulnerability Response

Sie können alle SBOM AVITs, die im Arbeitsbereich SBOM erstellt werden, im Vulnerability Manager Workspace anzeigen, wenn Sie Zugriff darauf haben.

Hinweis:
Um nur SBOM AVITs aus der Liste der angreifbaren Anwendungselemente in Vulnerability Manager Workspace und nicht alle AVITs anzuzeigen, legen Sie die Bedingung **[Quelle] [ist] [SBOM] UND [Scan-Typ] [ist] [SBOM-SCA]** für die Schwachstelle in der Anwendung fest Tabelle „Elemente“ [sn_vul_app_vulnerable_item]. Um die Tabelle anzuzeigen, navigieren Sie in Ihrer -Instanz zu **Alle**, und geben Sie im Filternavigator **sn_vul_app_vulnerable_item.list** ein.

Weitere Informationen zum Arbeitsbereich des Schwachstellenmanagers, zum Anzeigen von Überwachungsthemen, zu Maßnahmen zur Anwendungskorrektur und zu Regeln für Anwendungskorrekturaufgaben für AVITs, die über die Anwendung Vulnerability Response in Vulnerability Manager Workspacekonfiguriert werden, finden Sie unter Überwachungsthemen in Vulnerability Manager Workspaceverwenden.

Korrekturaufgaben (AVULs) werden aus AVITs erstellt und basierend auf Ihren Zuweisungsregeln automatisch Gruppen zur Korrektur zugewiesen. Weitere Informationen zum Erstellen dieser Regeln finden Sie in den folgenden Themen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen oder bearbeiten Sie Vulnerability Response -Zuweisungsregeln
- Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgabenund Erstellen Sie eine Korrekturmaßnahme in Vulnerability Manager Workspace.

Angreifbare Anwendungselemente in SBOM-Antwort werden erneut geöffnet

Ein **geschlossenes** angreifbares Anwendungselement (Application Vulnerable Item, AVIT) für eine Komponente mit einer zugeordneten Schwachstelle wird automatisch erneut geöffnet und ist im Arbeitsbereich SBOM sichtbar, wenn die folgenden Bedingungen vorliegen:

- Das AVIT mit der zugehörigen Schwachstelle wird von den Schwachstellenscans einer Drittanbieterintegration erneut erkannt, oder die Komponente mit der Schwachstelle ist Teil eines nachfolgenden SBOM -Uploads.
- Sie haben die Systemeigenschaft „AVITs erneut öffnen, wenn erkannt“ (*sn_sbom_resp.reopen_avits_if_detected*) nicht deaktiviert. Diese Systemeigenschaft ist standardmäßig aktiviert.
- Der Substatus des **geschlossenen** AVIT ist keiner der folgenden: **Mitigationssteuerung vorhanden**, **Nicht betroffen**oder **Falsch positiv**. AVITs mit diesen Substatus werden von der Systemeigenschaft nicht erneut geöffnet.

Deaktivieren Sie diese Systemeigenschaft nur, wenn **geschlossene** AVITs nicht automatisch erneut geöffnet werden sollen.

Zeigen Sie den Upload-Status für Software Bill of Materials -Dateien an

Überprüfen Sie den Upload-Status für die Software-Stücklistendateien (SBOM), die Sie in das Modul Stücklistenwarteschlange im Arbeitsbereich Software Bill of Materials (SBOM) hochladen. Verfolgen Sie die Dateien, die Sie erfolgreich hochladen, Ihren Upload-Verlauf und die Fehler.

Vorbereitungen

Erforderliche Rolle: sn_sbom_resp.sbom_analyst

Prozedur

1. Zeigen Sie Ihren Upload-Status an.

   Die Methode zum Anzeigen des Upload-Status hängt von den installierten Anwendungen ab.

Option	Beschreibung
SBOM Zentral	**a.** Navigieren zu **Alle** > **SBOM-Core** > **Stücklisten-Erfassungsstatus**. **b.** Überprüfen Sie in der Liste „Stückliste“ die Spalten „ **Status“**, **„Stücklisten-Generierungszeit“**und „ **Erstellt** “ auf Details.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
SBOM Antwort	**a.** Navigieren zu **Alle** > **SBOM-Arbeitsbereich** > **Stücklisten-Warteschlange**. **b.** Wählen Sie eine Visualisierungskarte aus, um die folgenden Details für die Kategorien Ihrer hochgeladenen Dateien zu überprüfen: ▪ Stücklistenaktualisierungen in den letzten 30 Tagen: Gesamtzahl der Stücklistenentitäten, die in den letzten 30 Tagen erfolgreich hochgeladen und analysiert wurden. ▪ Upload-Quelle: Gesamtzahl der erfolgreich hochgeladenen SBOM -Dateien und eine Aufgliederung der zu ihrer Erfassung verwendeten Methoden (API oder manuell). ▪ Upload-Fehler nach Kategorie: Die fünf häufigsten Kategorien von Upload-Fehlern. Wenn in dieser Visualisierung keine Daten angezeigt werden, wurden alle Ihre SBOM -Dateien erfolgreich hochgeladen.

Die Statusinformationen in der Stücklistentabelle [sn_sbom_doc_list] und im Stücklistenwarteschlangen-Modul enthalten jeweils Stücklistenformate, Erfassungsstatus und Stücklisten-Generierungszeit. Die Spalte „Status“ für die Stücklistenerfassung enthält die folgenden Status:

- In Warteschlange – SBOM Daten wurden hochgeladen.
- Verarbeitung – Die Komponentendaten werden als Teil des Imports verarbeitet.
- Verarbeitet – Datenerfassung wurde erfolgreich abgeschlossen.
- Fehler: Während der Verarbeitung ist ein Fehler aufgetreten.

Zusätzlich zum Status Ihrer hochgeladenen Dateien können Sie Listen der Komponenten anzeigen, die Sie erfasst haben, indem Sie einen Stücklistenentitätsdatensatz auswählen.

2. **Wahlweise:** Greifen Sie auf weitere Informationen zu Fehlern und Upload-Status zu, indem Sie das Zahnradsymbol auswählen und Felder wie **Fehlerkategorie** und **Fehlerdetail**hinzufügen.

Eine Software Bill of Materials -Entität wird auf Schwachstellen überprüft

Ermitteln Sie, ob den Komponenten in einer hochgeladenen Datei Software Bill of Materials (SBOM) Schwachstellen zugeordnet sind.

Die folgenden Anwendungen müssen installiert und aktiviert werden, bevor Sie die Schwachstellen und erweiterten Schwachstellendaten anzeigen können:

- SBOM Antwort
- Integration von Vulnerability Response mit NVD- und CWE-Aufträgen
- Vulnerability Response

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Erforderliche Rolle: sn_sbom_resp.sbom_analyst

1. Navigieren zu **Alle** > **SBOM-Arbeitsbereich** > **Komponenten**.
2. können Sie Schwachstelleninformationen entweder über eine Visualisierung oder einen Komponentendatensatz anzeigen.

Methode	Aktionen
Visualisierung von Stücklistenentitäten mit Schwachstellen	Wählen Sie das Visualisierungsdiagramm **Stücklistenentitäten mit Schwachstellen** aus. ○ Wenn dieser Komponente Schwachstellen zugeordnet sind, werden die Gesamtzahlen in den Spalten CVE und CWE in der Liste angezeigt. Eine Komponente kann mehr als eine Schwachstelle aufweisen. Wenn verfügbar, können Sie die Spalte „Behebbarkeit“ in dieser Liste auf Einträge überprüfen. ○ Wenn dieser Komponente keine Schwachstellen zugeordnet sind, zeigen diese Spalten 0 oder keine Werte für die Komponente an. Wenn die Spalten CVE, CWE und Fixability nicht angezeigt werden, können Sie sie der Seite hinzufügen, indem Sie das Zahnradsymbol oben rechts auf der Seite auswählen und **Spalten bearbeiten auswählen**. Wählen Sie sie in der Spaltenliste Verfügbar aus, und wählen Sie **OK**.
Komponentendatensatz	**a.** Wählen Sie in der Liste unter den Visualisierungen einen Datensatz aus. **b.** Wählen Sie die Registerkarte **Schwachstellen** im Datensatz aus. **i.** Wenn keine Daten angezeigt werden, sind dem Datensatz keine gemeldeten Schwachstellen zugeordnet. **ii.** Wenn -Daten angezeigt werden, rufen Sie Überprüfung des Komponentenmoduls im Arbeitsbereich Software Bill of Materials auf und befolgen Sie die Schritte im Nachbesserungs-Workflow für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode	Aktionen
	Application Vulnerability Response, um die Schwachstelle zu beheben. Weitere Informationen finden Sie unter Application Vulnerability Response Schwachstellen werden behoben.

Risiko mit Vulnerability Intelligence bewerten

Zeigen Sie erweiterte Schwachstellendaten mit der Antwort SBOM für Komponentendatensätze an. Die Anwendung SBOM Response, Vulnerability Response, Integration der National Vulnerability Database (NVD) und Common Weakness Enumeration (CWE), die unter Unterstützte Anwendungen beschrieben werden, müssen installiert und aktiviert sein.

1. Wählen Sie die Visualisierung **Alle Komponenten** aus, um die Liste der zugehörigen Datensätze anzuzeigen.
2. Wählen Sie einen Link in der Spalte **Name** aus, um einen Datensatz zu öffnen.

   Die Status, **Veraltet**, **Verworfen**und **Angreifbar** werden unter dem Komponentennamen angezeigt. Eine Komponente kann eine beliebige Kombination dieser Status aufweisen. Wenn kein Status angezeigt wird, ist die Komponente nicht veraltet, verworfen oder angreifbar.

   Überprüfen Sie die aktuelle Version und die zuletzt veröffentlichte Version. Im rechten Bereich können Sie einen Versionsverlauf anzeigen. Die aktuelle Version wird im Versionsverlauf hervorgehoben, und ihre Position in der Liste gibt Ihnen möglicherweise Aufschluss darüber, warum eine Komponente **veraltet**, **verworfen**und **angreifbar**ist. Beispielsweise könnten Sie eine ältere Version einer Komponente verwenden.
3. Wählen Sie im Datensatz die zugehörigen Registerkarten **Übersicht**, **Hashes**, **Stücklistenentitäten**, **Schwachstellen**und **AVIs** aus.
   - Übersicht: Eine Zusammenfassung der Komponentendetails.
   - Stücklistenentitäten: Eine Liste der Entitäten, die dieser Komponente zugeordnet sind.
   - Hashes: Bei Import werden Hashes angezeigt.
   - Schwachstellen: Informationen zu bekannten Schwachstellen, die dieser Komponente zugeordnet sind. Wenn diese Liste leer ist, sind keine Schwachstellen bekannt.

     Wenn die Liste ausgefüllt ist, wählen Sie die Registerkarte aus, um Schwachstellen-IDs, Zusammenfassungen und andere Schwachstelleninformationen für Common Vulnerabilities and Exposures-Daten (CVE) und Common Weakness Enumeration-Daten (CWE) anzuzeigen, die diesem Datensatz zugeordnet sind. CVEs werden nach Schweregrad aufgeschlüsselt, CWEs werden danach aufgeschlüsselt, wie wahrscheinlich es ist, dass die Komponente ausgenutzt wird. Sie können die erweiterten Schwachstellen-Datensätze in den Anwendungen Vulnerability Response oder Application Vulnerability Response anzeigen, indem Sie den Link Schwachstellen-ID wählen.
   - AVIs (AVITs): Angreifbare Anwendungselemente, die dieser Komponente zugeordnet sind, wenn Sie AVIT-Erstellungsregeln erstellt haben, die die Komponente mit einer bekannten Schwachstelle abgleichen. Die Anwendung Application Vulnerability

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Response (AVR) verknüpft eine Schwachstelle mit einer Anwendung, um einen AVI-Datensatz zu erstellen. Weitere Informationen finden Sie unter Erstellen von Regeln für angreifbare Anwendungselemente im Arbeitsbereich Software Bill of Materials.

Mit den -Anwendungen Software Bill of Materials installierte Komponenten

Bei der Aktivierung der Software Bill of Materials -Anwendungen werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen, Anwenderrollen und geplanten Aufgaben.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_sbom_response.managelicense	Diese Rolle wird mit der Anwendung SBOM Response installiert. Mit dieser Rolle können Sie Lizenzen für Komponenten auflösen.	Keine
sn_sbom_response.licenseresolver	Diese Rolle wird mit der Anwendung SBOM Response installiert. Mit dieser Rolle können Sie hochgeladene Lizenzinformationen anzeigen und bestimmen, welche Lizenzen zulässig und welche verboten sind.	Keine
SBOM schreiben [sn_sbom_dm.app_write], SBOM erstellen [sn_sbom_dm.app_create], SBOM lesen [sbom_dm.app_read]	Diese Rollen werden mit der Anwendung „Datenmodell für SBOM “ installiert. Sie ermöglichen Ihnen das Lesen, Erstellen und Bearbeiten von Datensätzen in Tabellen SBOM.	Keine
SBOM Cores erfasst [sn_sbom_core.sbom_ingest] und SBOM Core-Administrator [sn_sbom_core.admin]	Diese Rollen werden mit der Anwendung SBOM Core installiert. Mit der Rolle sn_sbom_core.sbom_ingest können Sie SBOMs manuell und über die REST API hochladen. Mit der	• sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_sbom_dm.app_read

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Rolle sn_sbom_core.admin können Sie SBOMs erstellen, lesen, Daten bearbeiten und hochladen. Mit dieser Rolle erhalten Sie auch Zugriff auf die SBOM Core-Module in Ihrer -Instanz. Sie erbt die Rollen von der Anwendung „Datenmodell für SBOM “ .	
SBOM-Analyst [sn_sbom_resp.sbom_analyst]	Diese Rolle wird mit der Anwendung SBOM Response installiert. Es erbt die Rolle sn_sbom_core.admin und ermöglicht Ihnen den Zugriff auf den -Arbeitsbereich SBOM.	• sn_sbom_core.admin • sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • Tabelle sn_sbom_config_rule

Mit den -Anwendungen SBOM installierte Tabellen

Die in der folgenden Tabelle aufgeführten Tabellen werden mit der Anwendung „Datenmodell für SBOM “ installiert.

Datenmodell für SBOM -Tabellen

Tabelle	Beschreibung
SBOM Dokument [sn_sbom_doc]	Enthält die Stücklistenentitäten, die Sie hochgeladen haben.
SBOM Komponente [sn_sbom_component]	Enthält importierte SBOM Komponenten, Klassifizierer und Versionen, die in der übergeordneten Komponente enthalten sind.
SBOM Komponentenbeziehung sn_sbom_comp_relationship	Enthält Komponenten und ihre Abhängigkeiten.
SBOM m2m-Stücklistenkomponente [sn_sbom_m2m_bom_comp]	Enthält die Stücklistenkomponentenzuordnungen.
SBOM-Lizenz	Enthält die Open Source-Lizenz-IDs, die für Komponenten verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenmodell für SBOM -Tabellen (Fortsetzung)

Tabelle	Beschreibung
sn_sbom_license	
SBOM Lieferant [sn_sbom_supplier]	Enthält die Organisation, die die Komponente geliefert hat. Dies kann ein Hersteller, Händler oder Umpacker sein.
SBOM Komponenten-ID [sn_sbom_comp_id]	Enthält die Komponentenbezeichner.
SBOM Komponenteneigenschaften [sn_sbom_comp_property]	Enthält die Name-Wert-Eigenschaften der Komponente.
SBOM Hash sn_sbom_hash	Enthält Komponenten-Hashing-Algorithmen.
SBOM Kontakt [sn_sbom_contact]	Enthält Kontaktinformationen des Lieferanten.
SBOM externe Referenzen [sn_sbom_comp_external_ref]	Enthält Komponenten, Komponententypen und externe URLs, die Systeme, Sites und Informationen dokumentieren, die relevant sein könnten, aber nicht in SBOMenthalten sind.
SBOM Paketgruppe [sn_sbom_pkg_group]	Enthält die Paketgruppeninformationen für jede Komponente. Mehrere Versionen von Bibliotheken können anwendungsübergreifend verwendet werden. Versionen derselben Komponenten werden gruppiert und dieser Tabelle hinzugefügt, um zu vermeiden, dass dieselben Daten mehrmals abgerufen werden.

Die in der folgenden Tabelle aufgeführten Tabellen werden mit der Anwendung SBOM Response installiert

SBOM Antworttabellen

Tabelle	Beschreibung
SBOM Konfiguration der Erstellungsregel sn_sbom_config_rule	Enthält AVIT-Erstellungsregeln, die im Arbeitsbereich SBOM verwendet werden.
SBOM Schwachstellen bei m2m-Komponenten	Enthält die Komponenten und zugehörigen Schwachstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SBOM Antworttabellen (Fortsetzung)

Tabelle	Beschreibung
[sn_sbom_m2m_comp_vuln]	
Informationen zur Korrektur von Komponentenschwachstellen [sn_sbom_comp_vuln_fix_info]	Enthält die Korrekturversionen für jede Drittpartei-Schwachstelle, die einer Version der Komponente zugeordnet ist.
Komponentenberichtseinblicke [sn_sbom_comp_report_insight]	Enthält Einblicke in veraltete, verworfene und Behebbarkeitsdaten für Komponenten.
Deps-Integrationsimporte sn_sbom_deps_integration_import	Enthält importierte Versionslisteninformationen für ein bestimmtes Paket oder eine bestimmte Bibliothek.
OSV-Integrationsimporte [sn_sbom_osv_integration_import]	Enthält Vulnerability Intelligence-Informationen für eine bestimmte Version eines Pakets oder einer bestimmten Bibliothek.
Komponentenversionslisten [sn_sbom_st_version_list]	Enthält Versionsinformationen und Veröffentlichungsdaten für Komponenten.

Geplante Aufgaben

Auftrag	Beschreibung
Berechnet die Behebbarkeit und Schwachstelle von Komponenten	Berechnet Informationen darüber, wie Komponenten mit Schwachstellen behoben werden können und wie wahrscheinlich es ist, dass Komponenten behoben werden können.
Neue OSV-Integrationskomponenten	Ruft alle öffentlich bekannten Schwachstellen ab, die Paketen (Bibliotheken) zugeordnet sind, die nach der letzten Integrationsausführung importiert wurden.
OSV Integration Comprehensive	Ruft alle öffentlich bekannten Schwachstellen ab, die allen importierten Paketen zugeordnet sind.
Deps.dev-Integration	Ruft alle öffentlich bekannten Versionen für Pakete ab und wird mit zum Identifizieren von Komponenten im Status **„Veraltet“** und „ **Verworfen“** verwendet.
Aktualisieren Sie „uln_based_criticality“ für Stücklistenkomponenten	Aktualisiert die Relevanz für Komponenten mit Schwachstellen.

Erstellen Sie im Software Bill of Materials -Arbeitsbereich eine Regel für angreifbare Anwendungselemente

Richten Sie die Bedingungen ein, unter denen im Modul „AVI-Erstellungsregeln“ im Arbeitsbereich Software Bill of Materials (SBOM) automatisch AVITs (Application Vulnerable Items) erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Anwendung SBOM Response ist erforderlich, wenn Sie angreifbare Anwendungselemente erstellen möchten. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Erforderliche Rolle: sn_sbom_resp.manage_avi_rule.

Prozedur

1. Navigieren zu **SBOM-Arbeitsbereich** > **AVI-Erstellungsregeln**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Regel.
Aktiv	Gibt an, ob die Erstellungsregel aktiviert ist.
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Die Regel mit dem niedrigsten numerischen Wert wird zuerst ausgeführt. Beispielsweise können Sie Regeln mit höherer Priorität für Elemente erstellen, die eine besondere Behandlung erfordern oder bei denen das Risiko kritisch ist, sodass sie zuerst ausgeführt werden. Als Nächstes erstellen Sie allgemeine Regeln für Elemente, die keine besondere Behandlung erfordern. Erstellen Sie abschließend eine Standardregel, um alle Komponenten zu erfassen, die Schwachstellen aufweisen.
Beschreibung	Beschreibung der Regel, damit Sie sie von anderen Regeln unterscheiden können.
Bedingungen	Erstellen Sie die Bedingungen, unter denen angreifbare Anwendungselemente (Application Vulnerable Items, AVIs) erstellt werden. Sie können beispielsweise **[Schwachstelle > Schweregrad][ist][1-Kritisch]** auswählen, um AVITs für Komponenten zu erstellen, die Schwachstellen aufweisen, die ein hohes Risiko darstellen und schwerwiegende Auswirkungen auf Sie haben könnten. Beachten Sie, dass Sie weitere Bedingungen hinzufügen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Speichern**.
   Ihre Erstellungsregel wird nach dem nächsten Upload automatisch ausgeführt und erstellt AVIs für Komponenten, die Ihren Bedingungen entsprechen. Sie können die Regel auch bei Bedarf über das Modul „AVI-Erstellungsregeln“ ausführen, indem Sie **Jetzt ausführen**auswählen.

Ergebnisse

Nach der Erstellung können Sie überprüfen, ob eine AVIT speziell für SBOM -Daten erstellt wurde, indem Sie die Werte in den Feldern **Quelle** und **Scan-Typ** in einem AVI-Datensatz überprüfen.

Feld	Wert
Quelle	SBOM
Überprüfungstyp	SBOM-SCA

Anwendungen zur Verwaltung von Sicherheitsfällen im Unternehmen

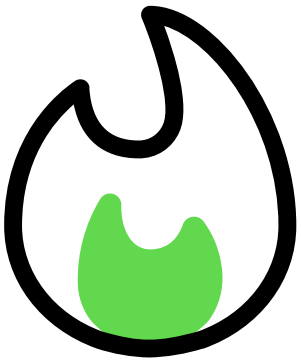
Zu den Anwendungen für die Verwaltung von Sicherheitsfällen im Unternehmen gehört Security Incident Response, eine SOAR-Lösung (Security Orchestration and Automation Response), mit der Sie schnell auf sich entwickelnde Bedrohungen reagieren und gleichzeitig die Sicherheitsabläufe des Unternehmens optimieren und orchestrieren können. Es eliminiert die Fehler und die Komplexität, die bei manuellen Übergaben zwischen Systemen, Teams und Zuständigkeiten auftreten.

Erste Schritte

Die folgenden Security Incident Response -Anwendungen sind mit separaten Abonnements von ServiceNow® Storeverfügbar. Unter Security Operations und ServiceNow Store finden Sie weitere Informationen zum Suchen von, zum Abrufen von Berechtigungen und zum Herunterladen von Apps in Ihre Instanz von.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response



Erfahren Sie mehr über die Anwendung Security Incident Response

Management schwerwiegender Sicherheits-Incidents

Erfahren Sie mehr über die Anwendung „Major Security Incident Management“.

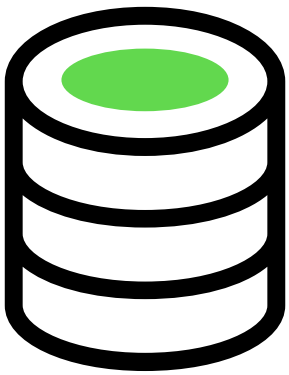
Threat Intelligence

Erfahren Sie mehr über die Anwendung Threat Intelligence

Threat Intelligence-Sicherheitszentrum

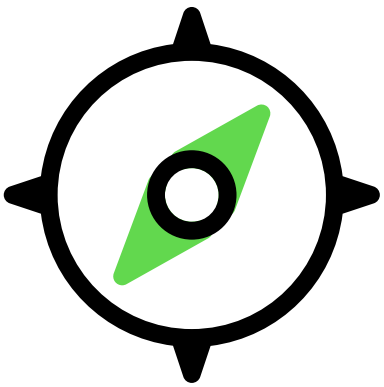
Erfahren Sie mehr über die Anwendung Threat Intelligence Security Center

Reaktion auf Incident zur Vermeidung von Datenverlust



Erfahren Sie mehr über die Anwendung Data Loss Prevention

Gemeinsam genutzte Funktionen von Security Incident Response-Anwendungen



Erfahren Sie mehr über die Funktionen, die von Security Incident Response-Anwendungen gemeinsam verwendet werden

Automatische Übersetzung

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

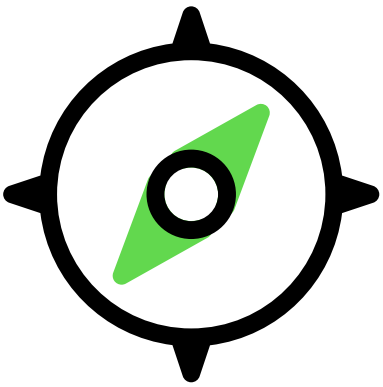
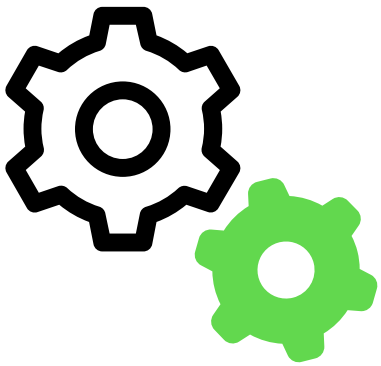
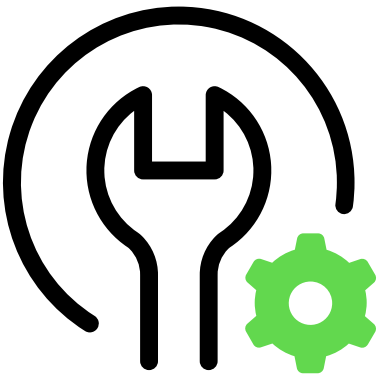
Security Incident Response

Die Anwendung ServiceNow® Security Incident Response verfolgt den Fortschritt von Security Incidents von der Discovery und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur abschließenden Überprüfung nach dem Incident, der Erstellung von Knowledge Base-Artikeln und dem Abschluss.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Security Incident Response

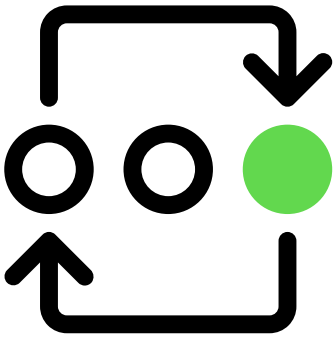
Untersuchen	Einrichten und konfigurieren	Verwalten
		
Erfahren Sie mehr über die Funktionen von Security Incident Response	Installieren Sie Ihre Security Incident Response-Anwendung, und richten Sie sie ein	Verwalten Sie Ihre -Security Incidents, und passen Sie sie an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response (Fortsetzung)

integrieren



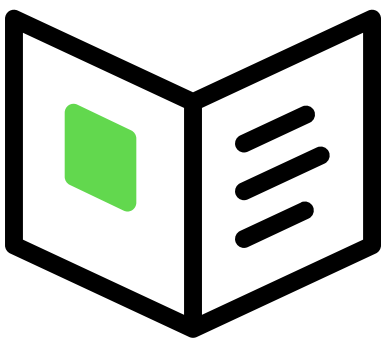
Erweitern Sie Security Incident Response durch die Integration mit anderen Anwendungen

Verwenden Sie den Arbeitsbereich für Security Incident Response

Erfahren Sie, wie Sie die Arbeitsbereiche für Security Incident Response und IT-Korrektur verwenden

Analytics und Reporting

Überwachen Sie den Korrekturfortschritt



Rufen Sie zusätzliche Informationen über Security Incident Response ab

Automatische Übersetzung

Security Operations-Apps im Store anfordern

Wenn Sie ein neuer Security Operations -Kunde mit London Patch 6 oder höher sind, besuchen Sie den ServiceNow Store auf der Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Security Incident Response verstehen

Verwalten Sie mit Security Incident Response (SIR) den Lebenszyklus Ihrer Security Incidents von der ersten Analyse bis zur Eindämmung, Beseitigung und Wiederherstellung. Mit Security Incident Response können Sie sich ein umfassendes Bild von den von Ihren Analysten durchgeführten Verfahren zur Reaktion auf Incidents machen und mithilfe analysegesteuerter Dashboards und Berichte Trends und Engpässe in diesen Verfahren nachvollziehen.

Eine Einführung in Security Incident Response, die die ersten Schritte bei der Verwendung der Anwendung zeigt.

Sehen Sie sich dieses neunminütige Video an, um mehr über den SIR-Prozess zu erfahren. Erfahren Sie mehr über den Einsatz von Security Incident Response zur Verhinderung von Angriffen und das Anzeigen von Sicherheitsaktivitäten im Security Incident Response -Explorer.

Integrierte Integrationen mit Cybersicherheitslösungen von Drittanbietern und von Partnern entwickelte Integrationen aus dem ServiceNow Store ermöglichen die Automatisierung und Orchestrierung der Sicherheit, um eine effiziente und genaue Reaktion auf Incidents zu ermöglichen.

Um Ihre Untersuchungen zu schützen und Security Incidents privat zu halten, bietet Security Incident Response die Möglichkeit, den Zugriff auf das System auf bestimmte sicherheitsbezogene Rollen und ACLs zu beschränken. Nicht-Sicherheitsadministratoren können vom Zugriff ausgeschlossen werden, es sei denn, Sie gewähren ihnen ausdrücklich Zugriff.

Hinweis:
IT-Systemadministratoren [admin] können die Identität von ServiceNow-Benutzern annehmen. Wenn die Identität eines Benutzers mit einer Anwendungsadministratorrolle für Security Incident Response angenommen wird, kann ein Administrator jedoch nicht auf die von dieser Rolle gewährten Funktionen zugreifen, einschließlich Security Incidents und Profilinformationen. Der Zugriff auf Module und Anwendungen in der Navigationsleiste ist ebenfalls eingeschränkt. Außerdem kann der Administrator das Passwort von Anwendern mit der Rolle „Anwendungsadministrator“ für Security Incident Response ändern.

Informations-Flow für Security Incident Response

Security Incident Response verwendet den folgenden Informationsfluss, von der Integration über die Untersuchung bis hin zur Lösung und Überprüfung.

Hinweis:
Dies ist eine interaktive Infografik. Sie können also versuchen, auf eines der Symbole oder Schritte im Bild zu klicken, um mehr über diesen Prozess oder diese Aufgabe zu erfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Klicken Sie auf diese Abbildung, um mehr über SIR-Integrationen zu erfahren
2. Klicken Sie auf diese Abbildung, um mehr über die Erstellung von Security Incidents zu erfahren
3. Klicken Sie auf diese Abbildung, um mehr über Threat Intelligence zu erfahren
4. Klicken Sie auf diese Abbildung, um mehr über den SIR-Arbeitsbereich zu erfahren
5. Klicken Sie auf diese Abbildung, um mehr über die Funktionen von MITRE Attack zu erfahren
6. Klicken Sie auf diese Abbildung, um mehr über Aktivitäten zur Überprüfung nach Incidents zu erfahren

Discovery

Security Incidents können auf folgende Weise protokolliert oder erstellt werden.

- Über das Formular „Security Incident“.
- Aus Ereignissen, die intern erzeugt oder von externen Überwachungs- oder Schwachstellennachverfolgungssystemen über Warnungsregeln oder manuell erstellt werden
- Aus externen Überwachungs- oder Nachverfolgungssystemen
- Aus dem Servicekatalog

Analyse

Abhängig von der ausgewählten Ansicht, die Sie verwenden (Standard, Nicht-IT-Sicherheit, Sicherheits-ITIL usw.) kann das Formular „Security Incident“ eine beliebige Kombination aus Schwachstellen, Incidents, Changes, Problemen, Aufgaben für das betroffene CI und das betroffene CI anzeigen Gruppen. Das System kann Malware, Viren und andere Schwachstellenbereiche durch Querverweise auf die Datenbanken des National Institute of Standards and Technology (NIST) oder andere Erkennungssoftware von Drittparteien identifizieren. Wenn Security Incidents gelöst werden, können Sie jeden Incident verwenden, um einen Knowledge Base-Artikel zur Sicherheit zu erstellen, um später darauf zurückgreifen zu können.

Führen Sie weitere Analysen mithilfe einer Business Service-Zuordnung durch, um andere betroffene Systeme oder Business Services zu finden, die infiziert sein können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eindämmung, Beseitigung und Wiederherstellung

Während Sie Schwachstellen überwachen und analysieren, können Sie Aufgaben erstellen und anderen Abteilungen zuweisen. Sie können eine Business Service-Zuordnung verwenden, um Aufgaben, Probleme oder Changes für alle betroffenen Systeme, Dokumente, Aktivitäten, SMS-Nachrichten, Brückenanrufe usw. zu erstellen.

Prüfung

Nachdem der Incident gelöst wurde, können vor dem Abschluss weitere Schritte ausgeführt werden. Sie können eine Überprüfung nach Incident durchführen. Das Erstellen von Knowledge Base-Artikeln kann bei zukünftigen ähnlichen Incidents hilfreich sein. Bedeutende Incidents erfordern möglicherweise eine Überprüfung der Lösung nach Incident. Diese Überprüfung kann verschiedene Formen annehmen. Zum Beispiel:

- Führen Sie eine Besprechung durch, um den Incident zu besprechen und Antworten zu sammeln.
- Schreiben Sie eine Liste mit Fragen zur Lösungsüberprüfung, die für jede Kategorie oder Priorität des incident erstellt wurden, und verteilen Sie sie an die Teams, die an einem Incident gearbeitet haben.
- Incident-Manager können den Bericht schreiben und selbst Informationen sammeln.

Es kann automatisch ein Bericht zur Überprüfung der Incident-Lösung generiert werden, der Folgendes enthält:

1. Eine Zusammenfassung dessen, was getan wurde
2. der Zeitleiste
3. Der Typ des aufgetretenen Security Incidents
4. alle zugehörigen Incidents, Changes, Probleme, Aufgaben, CI-Gruppen
5. Detailinformationen zu der Lösung

Darüber hinaus ist ein automatisiertes Umfragensystem zur Überprüfung der Lösung von Security Incidents verfügbar. Erfasst die Namen aller Benutzer, die einem Security Incident zugewiesen sind, und sendet eine anwenderdefinierte Umfrage, um Daten zur Behandlung des Incidents zu sammeln. Diese Daten können dann in einem generierten Bericht zur Überprüfung eines Security Incidents verfügbar gemacht werden, den Sie zu einem endgültigen Entwurf bearbeiten können. Ähnliche Daten können einem Knowledge Base-Artikel hinzugefügt werden, um gelernte Lektionen und Schritte zur Lösung ähnlicher Probleme in der Zukunft zu enthalten.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Security Incident Response-Terminologie

Die folgenden Begriffe werden in Security Incident Responseverwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benennung	Definition
Aktiv	Jeder Security Incident, der sich nicht im Status „Geschlossen“ oder „Abgebrochen“ befindet.
Administratorsperre	Die Möglichkeit, den Zugriff Security Incident Response auf Mitarbeiter mit sicherheitsbezogenen Rollen und ACLs zu beschränken.
Eingehende Sicherheitsanforderungen	Anforderungen, die für Sicherheitsanforderungen mit geringen Auswirkungen übermittelt werden, z. B. die Anforderung eines neuen elektronischen Abzeichens.
Verwalten Sie Aktivitäten nach Incidents	Eine Überprüfung der Herkunft und Behandlung eines Security Incidents. Das Endprodukt ist ein Nachfolgebericht zum Incident, in dem alle durchgeführten Aktionen und die Gründe dafür dokumentiert werden.
Antwortaufgaben	Aufgaben, die einem Security Incident zur Nachverfolgung von Aktionen als Reaktion auf die Bedrohung zugewiesen werden.
Informationen zu Security Incident-Rechnern	Rechner, die zum Aktualisieren von Datensatzwerten verwendet werden, wenn vorkonfigurierte Bedingungen erfüllt sind.
Verzeichnisübersichten zu Security Incidents	Diagrammtyp, der Security Incident-Daten hierarchisch in Form von geschachtelten Rechtecken anzeigt.
Bedrohungssuche	Eine aus dem Security Incident-Katalog übermittelte Anforderung zum Scannen von Dateien, URLs und IP-Adressen auf Malware.
Schwachstellen-Scan	Eine Anforderung, die über das Security Incident-Formular initiiert wird, um betroffene Ressourcen (Server, Computer und andere Configuration Items) auf Schwachstellen zu scannen.

Domain Separation und Security Incident Response

Die Domänentrennung wird in Security Incident Response unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Umfasst alle Aspekte des **Basis** -Supports.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht

In der Anwendung Security Incident Response können Service Provider (SPs) durch Domänentrennung SOC- (Security Operations Center) und Security Incident Response-Verfahren (SIR) im gesamten Kundenstamm standardisieren, was zu niedrigeren Betriebskosten und höherer Servicequalität führt. Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt und niemals für andere Clients verfügbar sind.

Unterstützung für Domänentrennung in Security Incident Response nach Versionsreleases

Release	Support-Stufe	Notizen
Genf, Helsinki	Kein Support	Initiierung der Domänentrennung auf Datenebene
Istanbul	Nur Daten	
Jakarta	Ebene 2 (Daten, Anforderer, Erfüller)	**Neue Funktionen**: Unterstützung für Integrationen von Drittparteien mit Domänentrennung der Ebene 2 unter einer einzigen Integrationsinstanz, einschließlich Threat Intelligence-Integrationen
Kingston	Ebene 2 (Daten, Anforderer, Erfüller)	**Neue Funktionen**: Die Integration der Sichtungssuche für SIR ist mit mehreren Instanzen aktiviert, aber alle Instanzen befinden sich weiterhin unter einer einzigen Domäne. Beispiel: Wenn zwei Instanzen einer Splunk-Integration konfiguriert sind (SplunkCLOUD und SplunkCORP), werden beide weiterhin für Aktivitäten zur Reaktion auf Incidents in einer einzelnen Domäne genutzt, in der die Implementierung ursprünglich konfiguriert wurde.
London	Ebene 2 (Daten, Anforderer, Erfüller)	**Neue Funktionen**: Alle Integrationen befinden sich in mehreren Domänen
Madrid	Ebene 2 (Daten, Anforderer, Erfüller)	Alle Integrationen können sich jetzt über mehrere Domänen hinweg befinden. Im obigen Beispiel kann „splunkCloud“ „domain1“ und „splunkCORP“ domain2 sein.
New York	Ebene 2 (Daten, Anforderer, Erfüller)	Alle Integrationen befinden sich in mehreren Domänen.
Orlando	Standard	Alle Integrationen befinden sich in mehreren Domänen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützung für Domänentrennung in Security Incident Response nach Versionsreleases (Fortsetzung)

Release	Support-Stufe	Notizen
Paris	Standard	Alle Integrationen befinden sich in mehreren Domänen.

Die Domänentrennung für die Anwendung Security Incident Response deckt die folgenden Produktfunktionen ab:

- Sicherheitswarnungen werden an die entsprechende Domäne des Benutzers weitergeleitet, dessen ID/Anmeldeinformationen/Umfang den Incident generiert und als Security Incident registriert ist.
- Warnungen generieren „observables“ – zustandsbehaftete Eigenschaften oder messbare Ereignisse: Sicherheits-Workflows in der Domäne des Security Incident werden verwendet, um die Reaktion zu orchestrieren.
- Integrationen werden in der Domäne des Security Incident für die Reaktionsautomatisierung konfiguriert.
- Fähigkeiten werden in der Domäne des Security Incident für die Reaktionsautomatisierung konfiguriert. Diese Fähigkeiten (ab dem Kingston-Release) umfassen:
  - Bedrohungssuche
  - Erkennbares Element ergänzen
  - Configuration Item ergänzen
  - Laufenden Prozess abrufen
  - Netzwerkstatistiken abrufen
  - Anforderung blockieren
  - Host isolieren
  - Sichtungssuche
  - E-Mails suchen und löschen
  - In Beobachtungsliste veröffentlichen
- Ergebnisse aus der automatisierten Reaktion (z. B. Bedrohungssuche oder Sichtungssuche) werden in der Domäne des Security Incidents gespeichert.
- Andere Security Incidents werden in derselben Domäne wie der Security Incident anhand eines gemeinsam genutzten Satzes von erkennbaren Elementen miteinander verknüpft.
- Es wird auf andere Benutzer in der Domäne des Security Incident verwiesen.
- Auf Konfigurationselemente wird in derselben Domäne wie der Security Incident verwiesen.
- Der Domäne des Security Incident werden manuelle Antwortaufgaben hinzugefügt.
- In der Domäne des Security Incident wird auf Knowledge Base-Artikel und Runbooks verwiesen.
- Security Incident Response-Metriken, die für Incidents in der Domäne relevant sind, werden sowohl in Dashboards als auch in Berichten angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In den obigen Fällen gelten die übergeordneten Prinzipien der Transparenz in getrennten Domänen in der NOW Platform. Wie immer kann ein Incident in der übergeordneten Domäne auf Artefakte in der untergeordneten Domäne verweisen, aber nicht umgekehrt.

So funktioniert Domain Separation in Security Incident Response

Die Anwendung Security Incident Response verwaltet den Lebenszyklus eines -Security Incidents durchgängig. Die folgenden Anwendungsfälle berücksichtigen die Domänentrennung:

- **Erfassung von Ereignissen und Warnungen,** um Security Incidents zu erstellen, auf die der Analyst im SOC des Kunden oder im MSP reagieren kann:
  - E-Mail-Parser (plattformbasiert, von Anwendern gemeldetes Phishing, anwenderdefiniert)
  - Deduplizierungsereignisse/-warnungen vor der Incident-Erstellung
  - Automatische Extraktion von erkennbaren Elementen
  - Anwendungen im SIEM-Store einer Drittpartei
- **Ergänzung** von Artefakten, die an den Incidents beteiligt sind (IP, URLs, Domänen, Datei-Hashes):
  - Asset-Ergänzung (CMDB)
  - Anwender (Plattform)
  - Automatisierung: Ergänzung erkennbarer Elemente (Beispiel: WhoIs)
- **Untersuchen Sie** die Incidents mithilfe der Artefakte und ihrer Reputation oder ihrer Zuordnung zu bekannten Bedrohungen
  - Orchestrieren: Playbooks und Knowledge Base-Artikel
  - Automatisierung: Bedrohungssuche (z. B. VirusTotal), Sichtungssuche (z. B. Splunk), Laufende Prozesse abrufen (z. B. Carbon Black)
- **Beseitigen Sie** die am Incident beteiligten Bedrohungsartefakte basierend auf der durchgeführten Untersuchung
  - Orchestrieren: Playbooks und Knowledge Base-Artikel
  - Automatisierung: E-Mails suchen und löschen (Beispiel: Microsoft Exchange), IP blockieren (Beispiel: Palo Alto Firewall)
- Effizienz von Vorgängen bei der Reaktion auf Incidents**messen**
  - Performance Analytics-Dashboards: Produktivitäts- und Incident-Trends
  - Rekonstruktion von Incident-Untersuchungsschritten aus Arbeitsnotizen
  - Überprüfung nach Incident

Domänentrennung – Einrichtung

Das Einrichten von Domain Separation für Security Incident Response erfordert keine zusätzlichen Schritte. Alle Security Incident Response -Tabellen erwerben die Spalte „Domäne“, nachdem die Instanz domänengetrennt wurde.

Domänengetrennte Daten

Daten können domänengetrennt sein. Das bedeutet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Incidents in einer Domäne können nicht in anderen Domänen angezeigt werden.
- Aus dem Security Incident extrahierte erkennbare Elemente werden in derselben Domäne platziert und können nicht in anderen Domänen angezeigt werden.
- Bis zum Kingston-Release sind konfigurierte Drittanbieterintegrationen in der globalen Domäne vorhanden, und sind für alle anderen Domänen in der Instanz zugänglich.
- Im Madrid-Release können Drittanbieterintegrationen für einzelne Domänen einzeln konfiguriert und aktiviert werden. Dies bedeutet, dass die in einer Domäne aktivierte und konfigurierte Integration nicht in einer anderen Domäne genutzt werden kann.
- Automatisierungen, die mithilfe von Drittanbieterintegrationen (für Bedrohungsuntersuchung, Eindämmung oder Beseitigung) für erkennbare Elemente ausgeführt werden, platzieren ihre Ergebnisse in der Domäne des Security Incidents, und die Ergebnisse können nicht in einer anderen Domäne angezeigt werden.
- In einer Domäne erstellte Orchestration-Workflows sind in einer anderen Domäne nicht sichtbar.
- Fähigkeiten (wie in der Funktionsliste der vorangegangenen Fähigkeiten beschrieben), die aufgerufen werden, bleiben domänenübergreifend generisch, mit einer domänenspezifischen Implementierung der aufgerufenen Fähigkeit. Beispielsweise kann eine Sichtungssuche auf einer IP eine Splunk-Implementierung in einer Domäne und eine QRadar-Implementierung in einer anderen Domäne aufrufen.

Konfiguration

Alle Aspekte der Produktkonfiguration sind in einer domänengetrennten Umgebung eigenständig. Das Setup kann für einzelne Domänen angepasst werden.

Hinweis:
Geschäftslogik und die Prozesse in Nr. 2 bis 5 können innerhalb der Mandantendomäne verwaltet werden.

Die folgenden Aufgaben müssen konfiguriert werden:

1. Systemverwaltung
   - Weisen Sie Anwendern und Gruppen von Anwendern Rollen zu: Mit Security Incident Response installierte Anwenderrollen
   - Installieren Sie ein oder mehrere Plugins für Drittanbieterintegrationen für die Verwendung mit Security Incident Response: Security Incident Response-Integrationen
2. Security Incident Response -Administration
   - Rollen hinzufügen oder überprüfen: Mit Security Incident Response installierte Komponenten
   - Konfigurieren Sie Gruppen und Anwender: Erstellen Sie eine Security Incident-Gruppe
   - Richten Sie Incident-Eskalationen ein: Eskalieren Sie einen Security Incident
   - Richten Sie Rechner für Risikopunktzahl für Security Incidents ein: Informationen zu Security Incident-Rechnern
   - Servicelevel-Vereinbarungen einrichten: Erstellen Sie ein Security Incident Response -SLA
   - Richten Sie Prozessdefinitionen für Security Incidents ein: Informationen zum Prozessdefinition von Security Incident Response
   - Richten Sie Prozesse für die Überprüfung nach Incidents ein: Verwalten Sie Aktivitäten nach Incidents
3. E-Mail-Einstellungen für Security Incidents

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie den Posteingang zur Analyse von E-Mails fest: Security Operations E-Mail-Analyse
- Richten Sie E-Mail-Parser für die Warnungserfassung ein: Erstellen Sie E-Mail-Parser in Security Operations
- Richten Sie E-Mail-Abgleichregeln für von Anwendern gemeldetes Phishing ein: Erstellen Sie Regeln, um von Anwendern gemeldete Phishing-Angriffe zu validieren
- Richten Sie Aktionen für eingehende E-Mails ein:Aktionen für eingehende E-Mails

4. Playbook-Einstellungen für Security Incidents
   - Überprüfen und Einrichten von Runbook-Dokumenten: Erstellt ein Security Incident Response-Runbook
   - Richten Sie Workflows für Security Incidents ein: Security Operations allgemeine Funktionalität
5. Fähigkeitskonfigurationen
   - Anforderung blockieren: Security Operations-Integration: Blockierungsanforderungsfunktion
   - E-Mail suchen und löschen: Security Operations-Integration – Funktion zum Suchen und Löschen von E-Mails
   - Configuration Item ergänzen: Security Operations-Integration: CI-Fähigkeit ergänzen
   - Erkennbares Element ergänzen: Security Operations-Integration: Fähigkeit „Erkennbares Element ergänzen“.
   - Netzwerkstatistiken abrufen: Security Operations-Integration: Funktion zum Abrufen von Netzwerkstatistiken
   - Laufende Prozesse abrufen: Security Operations-Integration: Fähigkeit zum Abrufen laufender Prozesse
   - Host isolieren: Security Operations-Integration: Fähigkeit „Host isolieren“.
   - In Beobachtungsliste veröffentlichen: Security Operations-Integration: Fähigkeit „In Beobachtungsliste veröffentlichen“.
   - Sichtungssuche: Security Operations-Integration – Fähigkeit zur Sichtungssuche
   - Bedrohungssuche: Security Operations-Integration – Funktionalität zur Bedrohungssuche

Wie Mandantendomänen ihre eigenen Anwendungsdaten verwalten

- Besitzer der Mandantendomäne erstellen ihre eigenen E-Mail-Analyseregeln für die Erfassung von Security Incidents.
- Besitzer der Mandantendomäne können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Besitzer der Mandantendomäne können ihre eigenen Workflows zur Reaktion auf Incidents erstellen.
- Domänenbesitzer des Mandanten können ihre eigenen Incident-Kategorien, Knowledge Base-Artikel zur Reaktion auf Incidents und Runbooks erstellen, die Incident Response-Workflows zugeordnet werden.
- Benutzer der Mandantendomäne erstellen und schließen ihre eigenen Security Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geschäftslogik und Prozesse, die nach Instanzbesitzer domänengetrennt werden können

- Security Incident Response Benutzer und Gruppen
- Security Incident Response -Integrationen (ab Madrid-Release)
- E-Mail-Analyseregeln für die Incident-Erstellung
- Geschäftsregeln, um mehrere Ereignisse oder Warnungen in einem Security Incident zu konsolidieren
- Workflows für die Orchestration der Reaktion auf Incidents
- Rechner für Risikopunktzahl von Security Incidents
- Eskalationspfad für Security Incidents
- Security Incident-SLAs
- Prozessdefinitionen für Security Incidents
- Nachfolgeprüfungen von Security Incidents

Zugehörige Informationen

Domänentrennung für Service Provider

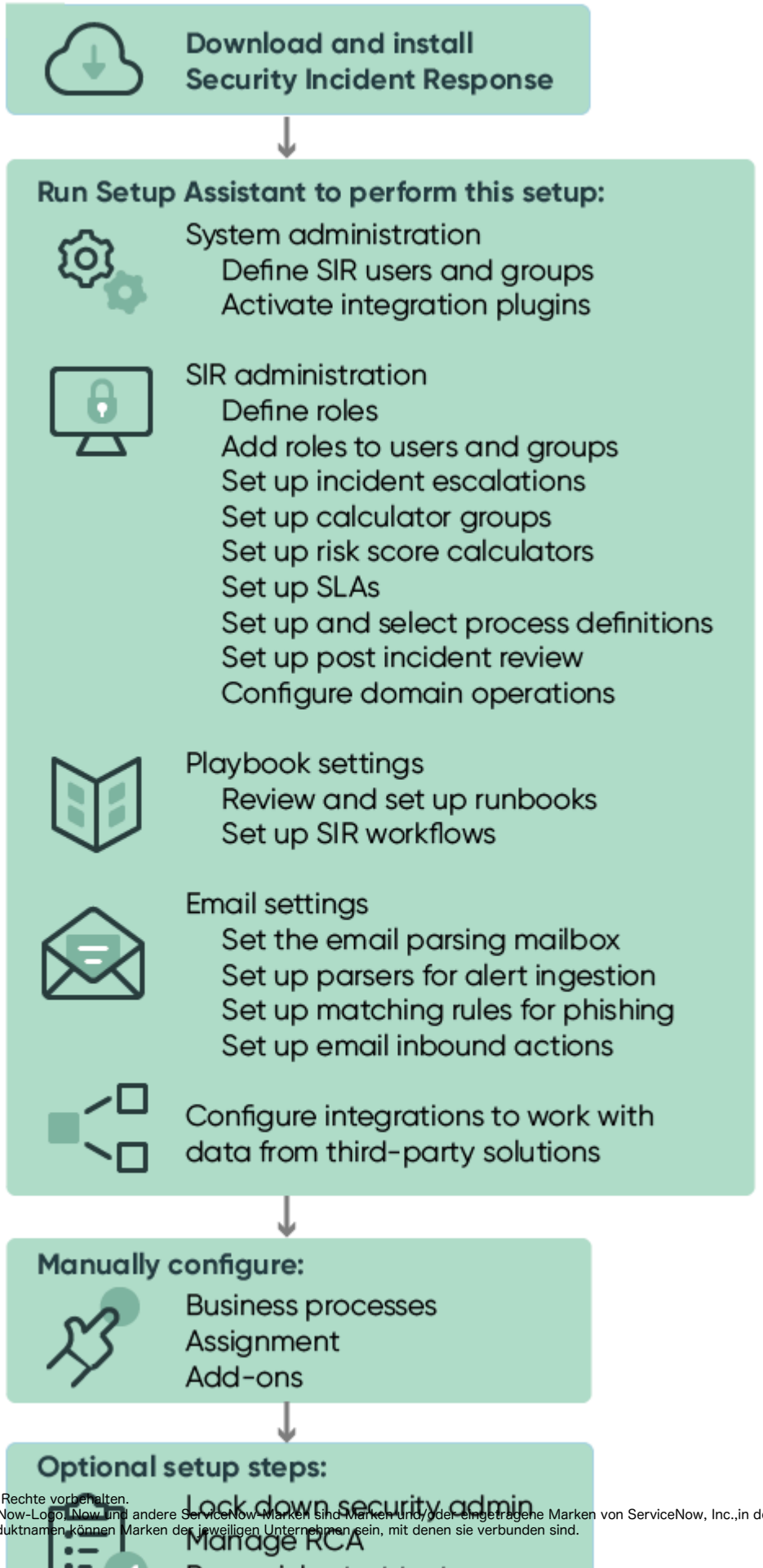
Setup von Security Incident Response

Das Setup für Security Incident Response umfasst einige obligatorische und mehrere optionale Schritte, abhängig von Ihren spezifischen Anforderungen. Nachdem Sie Security Incident Response aus ServiceNow Store heruntergeladen und installiert haben, können Sie den Setup-Assistenten ausführen, um eine grundlegende Konfiguration für Security Incident Response und Drittanbieterintegrationen durchzuführen.

Der Setup-Prozess Security Incident Response für [].

Das folgende Diagramm veranschaulicht den Setup-Prozess. Er ist in zwei Teilprozesse unterteilt, die die Anwendung Security Incident Response herunterladen und konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der erste Setup-Schritt führt zu laden Sie die herunter Security Incident Response Anwendung aus dem ServiceNow Store. Wenn der Download abgeschlossen ist, werden mehrere abhängige Anwendungen, einschließlich des Setup-Assistenten, geladen und können zur Konfiguration von Security Incident Responseverwendet werden.

Setup-Assistent

Der Security Incident Response Setup-Assistent ist eine assistentenähnliche Anwendung, die Sie Schritt für Schritt durch das Setup Ihrer Basisinstanz Security Incident Response führt.

Die Setup-Schritte sind ziemlich selbsterklärend. Wenn Sie jedoch zusätzliche Erklärungen benötigen, finden Sie zusätzliche Unterstützung in der Referenz des Setup-Assistenten. Nachdem Sie das Setup mit dem Setup-Assistenten abgeschlossen haben, können Sie bei Bedarf weitere optionale Setup-Verfahrendurchführen. Diese Verfahren umfassen Optionen für:

- Richten Sie den Anforderungslebenszyklus ein
- Erstellen von Katalogen und Anforderungen
- Benachrichtigungen werden konfiguriert
- Einrichten der manuellen und automatischen Zuweisung
- Aktivieren der Knowledge Base, verwalteter Dokumente und von Aufgabenaktivitäten

Ein neuer und verbesserter Arbeitsbereich für Security Incident Response ist verfügbar. Weitere Informationen finden Sie unter Arbeitsbereich für Security Incident Response.

Security Incident Response installieren und konfigurieren

Bevor Sie Security Incident Response in Ihrer -Instanz ausführen, müssen Sie es von ServiceNow Store herunterladen und die Konfigurationsschritte abschließen.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

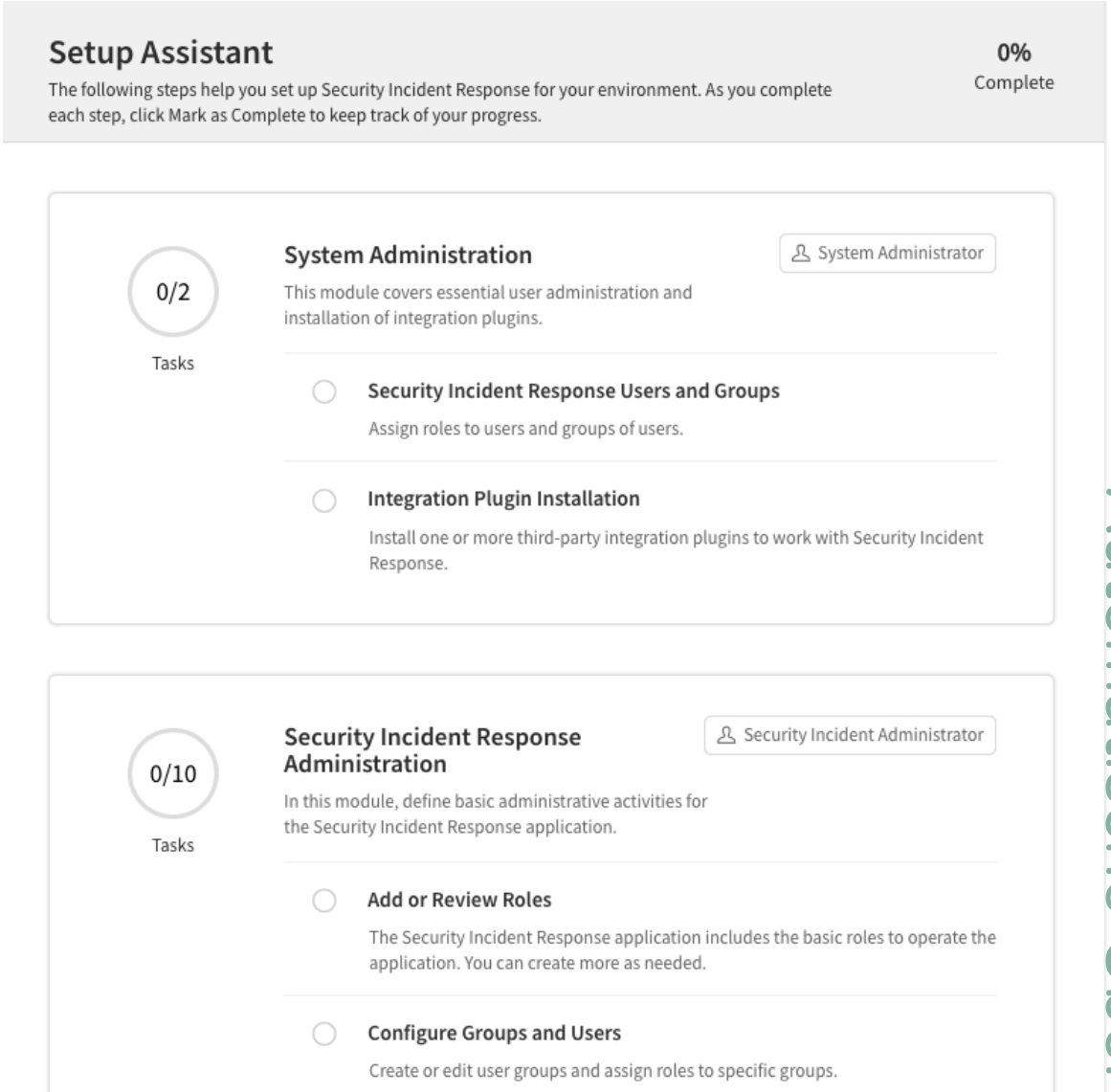
Wichtig:

- Wenn Sie Security Incident Response Version 13.4.5 oder höher aus ServiceNow Store installieren, wird standardmäßig automatisch die Version Arbeitsbereich für Security Incident Response (sn_si_aw) Version 1.5.1 oder höher installiert. Weitere Informationen zu den abhängigen Anwendungen finden Sie im Abschnitt SIR Workspace Plugins und Rollen.
- Beachten Sie, dass Version 1.5.1 und höher von Security Incident Response Workspace nur durch eine Installation/ein Upgrade von Security Incident Response installiert/aktualisiert und nicht unabhängig installiert werden kann.
- Die neuesten Funktionen in Security Incident Response sind ausschließlich in Arbeitsbereich für Security Incident Responseverfügbar. Installieren oder aktualisieren Sie auf die neueste Version Security Incident Response oder Arbeitsbereich für Security Incident Response, um auf Funktionen wie Schichtübergabe, Risikobewertungsrechner usw. zuzugreifen und sie zu nutzen.

Prozedur

1. Befolgen Sie die Anweisungen für Herunterladen einer Anwendung aus dem ServiceNow Store.
2. Nachdem Sie die Anwendung Security Incident Response und alle zugehörigen Anwendungen heruntergeladen haben, navigieren Sie zu **Security Incident** > **Setup von Analyst Workspace** > **Setup-Assistent**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Befolgen Sie die Anweisungen in den Formularen, um das -Basissystem Security Incident Response zu konfigurieren.
   Weitere Informationen zu einigen der komplexeren Setupaufgaben finden Sie bei Bedarf unter Referenz des Setup-Assistenten.

Laden Sie den Arbeitsbereich für Sicherheitsanalysten herunter, und installieren Sie ihn

Bevor Sie die neue UI Security Incident Response in Ihrer -Instanz ausführen, müssen Sie sie von ServiceNow® Store herunterladen und installieren.

Vorbereitungen

Um eine reibungslose Installation zu gewährleisten, vergewissern Sie sich, dass Sie über die erforderlichen ServiceNow -Rollen für Ihre Instanz von verfügen. Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:

- Wenn sie noch nicht zugewiesen wurden, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle „Security Incident Response-Administrator“ [sn_si.admin] zu.
- Der Security Incident Response-Administrator [sn_si.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

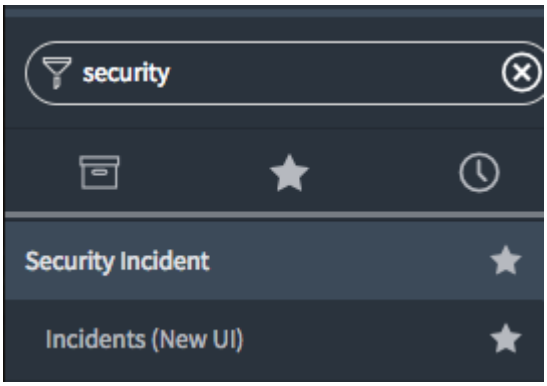
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Administrator

Prozedur

1. Befolgen Sie die Anweisungen für Herunterladen einer Anwendung aus dem ServiceNow Store und installieren Sie die Anwendung **Security Incident Response UI**.
2. Nach Abschluss der Installation können Sie den Arbeitsbereich für Sicherheitsanalysten öffnen, indem Sie zu navigieren **Security Incident** > **Incidents (neue UI)**



Mit Security Incident Response installierte Komponenten

Wenn Sie die Anwendung Security Incident Response herunterladen und aktivieren, werden verschiedene Arten von Komponenten installiert, einschließlich Anwenderrollen, Tabellen, Eigenschaften und geplante Aufgaben.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Installierte Eigenschaften

Benutzer mit der Rolle „Systemadministrator“ [admin] können die Eigenschaften von anzeigen. Benutzer mit der Rolle „Sicherheitsadministrator“ [sn_si.admin] können sie ändern.

Eigenschaft	Monatlich
Die Standardkategorieknoten, die auf der Registerkarte Beziehungsdiagramm im -Arbeitsbereich angezeigt werden. Die Standardwerte stellen die Tabellennamen dar, die den zugehörigen Datensätzen entsprechen. sn_si_aw.defaultCategories	• **Typ**: Zeichenfolge • **Standardwert**: sn_ti_m2m_task_observables,sn_si_m2m_task_affected_user,s
Standardmäßige Startzeit für alle Mitarbeiter, wenn kein Zeitplan festgelegt ist, formatiert als 08:00 sn_si.default.start.time	• **Typ**: Zeichenfolge • **Standardwert**: 08:00 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Standardmäßige Endzeit für alle Mitarbeiter, wenn kein Zeitplan festgelegt ist, im Format 17:00 sn_si.default.end.time	• **Typ**: Zeichenfolge • **Standardwert**: 17:00 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Erkennbare Elemente vom Typ Ziel zusammen mit anderen erkennbaren Elementen vom Typ Kontext in die Security Incident-Anwender- und -CI-Beziehungen einschließen sn_si.link_dest_ip	Bestimmt, ob ein erkennbares Element für einen Security Incident mit dem K „Ziel“ unter den **Registerkarten Konfigurationselemente** oder **Betrof Anwender** angezeigt wird. Standardmäßig werden erkennbare Elemente mi Zielkontexttyp ausgeschlossen. Um die erkennbaren Elemente einzubeziehen,
Erlauben Sie Anpassungen beim Erstellen eines Problems oder einer Change-Anforderung aus einem Security Incident sn_si.popup	Wenn ein Problem oder ein Change erstellt wird, öffnet diese Ei ein Popup-Fenster, in dem Sie die Anforderung ändern können. Wenn diese Eigenschaften auf **false**festgelegt sind, weist das P oder die Change-Anforderung dieselbe Priorität, Kurzbeschreib Beschreibung wie der Security Incident auf, ohne dass diese Fe hinzugefügt oder bearbeitet werden können. • **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Ordnen Sie Ergebnisse der Sichtungssuche CIs in der CMDB zu. sn_si.associate_ci_with_sighting_search	Bei Festlegung auf true enthalten die Ergebnisse der Sichtungssuche zugehöri Configuration Items, die sich in Ihrer CMDB befinden. • **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Risikopunktzahlen im Bereich werden grün hervorgehoben und im Format 0–49 angegeben sn_si.risk.score.green	In der Liste „Security Incidents“ werden Security Incidents mit einer Risikop zwischen 0 und 49 mit einem grünen Punkt markiert.
Risikopunktzahlen im Bereich werden orange hervorgehoben und im Format 50–79 angegeben sn_si.risk.score.orange	In der Liste der Security Incidents werden Security Incidents mit einer Risiko zwischen 50 und 79 mit einem orangefarbenen Punkt markiert.
Risikopunktzahlen im Bereich werden rot hervorgehoben und im Format 80–100 angegeben sn_si.risk.score.red	In der Liste „Security Incidents“ werden Security Incidents mit einer Risikop zwischen 80 und 100 mit einem roten Punkt markiert.
Dieser Parameter aktiviert oder deaktiviert Sichtungssuchkonfigurationen, die diese Funktion implementiert haben.	Bei Festlegung auf „true“ können Sichtungssuchen für aktivierte Integrationen werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
sn_si.enable_sighting_search	• **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Die Anzahl der Zeilen mit Rohdaten, die gespeichert werden, wenn eine Sichtungssuche ausgeführt wird. Bereich 0–100 sn_si.sighting_search_raw_data_rows	Diese Eigenschaft ist standardmäßig auf 50 Zeilen Rohdaten festgelegt. Die H Ergebniszeilen wird ab dem Beginn des Suchzeitraums und die andere Hälfte des Suchzeitraums gemeldet. Wenn Sie also 50 Zeilen auswählen, stammen 2 des Suchzeitraums und 25 vom Ende des Suchzeitraums.
Incident-Status automatisch auf „Eindämmen“ erhöhen, wenn eine Antwortaufgabe auf „In Arbeit“ gesetzt wird sn_si.rollup_task_state	Erwägen Sie bei der Verwendung von Flows oder Workflows, diese Eigensch **false**zu setzen. Auf diese Weise können Sie den Incident-Status innerhalb vo Workflows steuern. Außerdem vermeiden sie potenzielle Konflikte beim Übe einem Incident-Status zu einem anderen. • **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Zuweisungseigenschaften für Security Incident Response	
Standortgewichtung sn_si.location.gewichtung	Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Z eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise der Standort Aufgabe berücksichtigt wird, wird der Standortgewichtungswert zur Bewertu Sicherheitsanalysten hinzugefügt. • **Typ**: Ganzzahl • **Standardwert**: 10 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Gewichtung der Kompetenzen sn_si.skills.gewichtung	Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Z Sicherheitsanalysten verwendet wird. Wenn beispielsweise Kompetenzen für berücksichtigt werden, wird der Gewichtungswert der Kompetenzen zur Bew Sicherheitsanalysten hinzugefügt. • **Typ**: Ganzzahl • **Standardwert**: 10 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Legen Sie die maximale Anzahl von Sicherheitsanalysten fest, die durch die automatische Zuweisung gleichzeitig verarbeitet werden sollen sn_si.max.agents.processed	Das System hat ein absolutes Limit von 300 Sicherheitsanalysten. Wenn Sie 300 angeben, wird der Wert auf diese Ebene festgelegt. Das System kann eine nicht automatisch für eine Versandgruppe senden, die mehr Sicherheitsanalys konfigurierten Wert enthält. • **Typ**: Ganzzahl • **Standardwert**: 100 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Gewichtung Zeitzone sn_si.timezone.gewichtung	Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Z eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise die Zeitzone Sicherheitsanalysten für eine Aufgabe berücksichtigt wird, wird der Gewichtu Zeitzone zur Bewertung des Sicherheitsanalysten hinzugefügt. • **Typ**: Ganzzahl • **Standardwert**: 10 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Zwischen Ende einer Aufgabe und dem Reistestart der nächsten hinzuzufügende Dauer (in Minuten). sn_si.work.sacing	Ein Beispiel für einen gültigen Zeitwert ist 10. • **Typ**: Ganzzahl • **Standardwert**: 0 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Angegebene Journalfelder, `die Code` -Tags enthalten, die den Inhalt als HTML rendern. sn_si.journal_field.html_enabled	• **Typ**: Zeichenfolge • **Standardwert**: work_notes, Kommentare • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Berechnen Sie die betroffenen Services im Hintergrund. sn_si.refresh_impacted.event	Die zugehörige Liste „Betroffene Services/CIs“ wird durch Ereignisse generi Option aktiviert ist, wird die Aktualisierung im Hintergrund ausgeführt, und werden Sicherheits-Tags hinzugefügt. Legen Sie den Wert auf **„wahr“** fest, um den Vorgang im Hinter auszuführen. • **Typ**: true | false • **Standardwert**: false • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Rufen Sie den kritischen Service aus vorab berechneten Daten ab. sn_si.critical_service.calculator.use_cache	Ermöglicht es dem Rechner für kritische Services, vorab berech von Configuration Items zu verwenden. Legen Sie den Wert auf **„wahr“** fest, um in vorberechneten Dat suchen • **Typ**: true | false • **Standardwert**: false • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Security Incident-Administrator [sn_si.admin]	Vollständige Kontrolle über alle Security Incident Response -Daten. Verwaltet bei Bedarf auch Gebiete und Kompetenzen. **Hinweis:** Im Basissystem hat der Administrator auch Zugriff auf sn_si.admin. Security Incident Response kann vom Administrator eingeschränkt werden, solange mindestens einem anderen Anwender die Sicherheitsadministratorrolle zugewiesen ist.	• assessment_admin • catalog_admin • decision_table_admin • decision_table_reader • filter_admin • flow_designer • pd_author • pd_content_author • pd_operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manager • sn_si.spezial_access_read_manager • sn_si.spezial_access_write_manager • sn_ti.malicius_attachment_access • sn_ti.observable.admin • Tags_Administrator • template_admin • territory_admin • baumkarte_admin • user_admin
Security Incident-Analyst [sn_si.analyst]	Verwalten Sie Security Incidents. Zugrunde liegende Rolle für grundlegenden Sicherheitszugriff. Benutzer mit dieser Rolle können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.	• pd_operator • snc_platform_rest_api_access • sn_msi.promoter • sn_msi.proposer • sn_si.basic • sn_ti.malicius_attachment_access

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
Security Incident – Standard [sn_si.basic]	Zugrunde liegende Rolle für grundlegenden Sicherheitszugriff. Benutzer mit dieser Rolle können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.	• canvas_user • document_management_user • email_composer • flow_operator • inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.read • task_activity_writer • task_editor • Treemap_user
Chief Information Security Officer (CISO) [sn_si.cso]	Zeigen Sie das CISO-Dashboard an, und bearbeiten Sie es. Wenn das Plugin Vulnerability Response aktiviert ist, können Benutzer mit dieser Rolle dem Dashboard außerdem Schwachstellen-Definitionen für Bedeutungsdefinitionen hinzufügen. Dasselbe können Sie auch mit dem Plugin Security Incident Response tun.	• pa_viewer • sn_si.basic • sn_si.read
Security Incident Extern sn_si.external	Alle Security Incidents anzeigen, die zu ihrer jeweiligen Gruppe gehören.	service_fulfiller

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Hinweis: Die folgenden beiden Regeln gelten im gesamten ServiceNow unabhängig vom Bereichsadministrator oder der Bereichs-App. • Wenn Sie einer Gruppe einen Benutzer hinzufügen, weisen Sie dieser Gruppe auch Rollen zu. Wenn Sie einen Anwender aus einer Gruppe entfernen, werden auch die geerbten Rollen entfernt. • Jede Rolle kann von einer Rolle mit höherer Priorität zugewiesen werden.	
Benutzer für Security Incident-Integration [sn_si.integration_user]	Externe Tools können neue Security Incident-Datensätze bereitstellen und Security Incident-Datensätze aktualisieren.	import_transformer
Security Incident Knowledge-Administrator [sn_si.knowledge_admin]	Verwalten, aktualisieren und löschen Sie die Informationen in der Knowledge Base für Security Incidents.	• knowledge_admin • sn_si.read
Sicherheitsvorfallmanager [sn_si.manager]	Gleicher Zugriff wie für Sicherheitsanalysten.	• pd_author • pd_operator • sn_si.basic
Lesen des Security Incidents [sn_si.read]	Lesen Sie Security Incidents.	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snippet_reader • sn_ti.observable.read • workspace_user
Zugriffsmanager für Sicherheitsbeschränkungen [sn_si.restriction_access_manager]	Ermöglicht Anwendern oder Gruppen, „Beschränkungen“ für Security Incidents zu erzwingen. Dies gilt nur für Feldänderungen.	N/V

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
Spezieller Zugriff auf Security Incidents sn_si.spezial_access	Bietet Zugriff auf bestimmte Security Incidents für Benutzer außerhalb der Security Operations-Organisation.	N/V
Aktiver für Sicherheitssonderzugriff [sn_si.sonder_zugriff_aktivieren]	Gewährt einem Benutzer außerhalb der Security Operations-Organisation eine spezielle Zugriffsrolle für bestimmte Security Incidents.	N/V
Manager für spezielle Zugriffsrechte für Security Incidents [sn_si. special_access_read_manager]	Verwalten Sie die Rolle „Spezialzugriff für Security Incidents“ [sn_si.sonder_zugriff]. Verwenden Sie diese Rolle, um das Feld **„Lesezugriff“** im Formular „Security Incident“ zu ändern. Diese Rolle kann von sn_si.admin zugewiesen werden.	sn_si. special_access_enabler
Manager für Security Incident Special Access Writer [sn_si. special_access_write_manager]	Verwalten Sie die Rolle „Spezialzugriff für Security Incidents“ [sn_si.sonder_zugriff]. Verwenden Sie diese Rolle, um das Feld **Privilegierter Zugriff** im Formular „Security Incident“ zu ändern. Diese Rolle kann von sn_si.admin zugewiesen werden.	sn_si. special_access_enabler

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Suchen Sie nach erkennbaren Elementen des Security Incidents	Sucht nach erkennbaren Elementen nach einem anwenderdefinierten Zeitplan.

Installierte Tabellen

Tabelle	Beschreibung
Nachrichtenfeed-Konfiguration [sn_si_feed_configuration]	Konfigurationsdatensätze, die zum Definieren des Inhalts verwendet werden, der im Nachrichtenfeed für Security Incidents angezeigt wird.
Zuweisungsregel für die Überprüfung nach Incidents sn_si_vir_condition]	Automatisiert die Auswahl von Teilnehmern einer Umfrage zur Überprüfung nach Incident, wenn ein Security Incident geschlossen wird.
Security Incident sn_si_incident	Speichert einen Security Incident, die Antworten darauf, alle verknüpften Aufgaben, Changes, Probleme und Incidents im Zusammenhang mit diesem Security Incident.
Security Incident-Angriffsvektoren	Angriffsvektoroptionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_si_attack_vector	
Auditprotokoll für Security Incidents sn_si_audit_log	Speichert Audit-Protokolle zur Ergänzung von Security Incidents.
Security Incident-Rechner sn_si_calculator]	Ein Rechner zum Festlegen bestimmter Felder für Security Incidents, wenn bestimmte Bedingungen erfüllt sind.
Security Incident-Rechnergruppe sn_si_calculator_group]	Eine Gruppierung von Security Incident-Rechnern Die Reihenfolge der Rechnergruppe bestimmt, welche Gruppe zuerst ausgewertet wird, und in jeder Gruppe wird höchstens ein Rechner verwendet.
Security Incident Enrichment Firewall sn_si_enrichment_firewall	Wird aus der Basistabelle (sn_sec_cmn_enrichment_data_base) erweitert und enthält alle für die Palo Alto Networks-Firewall spezifischen Ergänzungsdatensätze.
Malware-Ergebnisse für die Ergänzung von Security Incidents [sn_si_enrichment_malware]	Wird aus der Basistabelle (sn_sec_cmn_enrichment_data_base) erweitert und enthält alle für Malware spezifischen Ergänzungsdatensätze.
Netzwerkstatistiken zur Ergänzung von Security Incidents sn_si_enrichment_network_statistiken	Wird aus der Basistabelle (sn_sec_cmn_enrichment_data_base) erweitert und enthält alle für Netzwerkstatistiken spezifischen Ergänzungsdatensätze.
Laufende Prozesse zur Ergänzung von Security Incidents [sn_si_enrichment_running_processes]	Wird aus der Basistabelle (sn_sec_cmn_enrichment_data_base) erweitert und enthält alle Ergänzungsdatensätze, die für laufende Prozesse spezifisch sind.
Laufende Services zur Ergänzung von Security Incidents sn_si_enrichment_running_service	Wird aus der Basistabelle (sn_sec_cmn_enrichment_data_base) erweitert und enthält alle Ergänzungsdatensätze, die für laufende Services spezifisch sind.
E-Mail-Suche für Security Incidents [sn_si_m2m_incident_email_search]	Ordnet E-Mail-Suchdatensätze Security Incidents zu.
Security Incident-Import sn_si_incident_import	Importieren Sie die -Tabelle für Security Incidents. Wird verwendet, um Security Incidents aus externen Systemen zu erstellen.
Prozessdefinition für Security Incidents sn_si_process_definition	Speichert die Konfiguration für Security Incident-Prozess-Flows.
Prozessdefinitionsauswahl für Security Incidents sn_si_process_definition_selector]	Speichert die Prozessdefinition für Security Incidents, die für Security Incidents verwendet werden soll.
Mit Security Incident verbundener Kundenservicefall	Ordnet Kundenservicefälle und Security Incidents zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_si_m2m_incident_customerservice_case]	
Mit Security Incident verbundene Ergänzungsdaten sn_si_m2m_incident_enrichment	Ordnet Security Incidents und zugehörige Ergänzungsdatensätze zu.
Security Incident Response Aufgabe sn_si_task	Verwaltet Teilaufgaben im Zusammenhang mit der Bearbeitung eines Security Incidents. Diese Aufgaben können Sicherheitspersonal oder Personen in anderen Abteilungen zugewiesen werden, um die abteilungsübergreifende Kommunikation und die Aufgabennachverfolgung zu verwalten.
Security Incident Response Aufgabenvorlage sn_si_task_template]	Wird zum Erstellen einer Security Incident Response -Aufgabe verwendet. Diese Vorlagen werden häufig in Katalogeinträgen verwendet, um automatisch einen Satz geeigneter Teilaufgaben für einen bestimmten Typ von Security Incident zu erstellen.
Security Incident Runbook-Dokument [sn_si_runbook_document]	Ordnet Bedingungen oder Filter für Security Incidents einem Wissensartikel zu. Wird verwendet, um Runbook-Verfahren für die Nachbesserung von Security Incidents anzugeben.
Vorlage für Security Incidents sn_si_incident_template]	Wird zum Erstellen eines Security Incident verwendet. Diese Vorlagen werden häufig in Katalogeinträgen verwendet, um einen vordefinierten Security Incident zu erstellen.
Sicherheitsanfrage sn_si_request	Eine sicherheitsbezogene Anforderung an das Sicherheitsteam.
Anforderung für Sicherheitsprüfung sn_si_scan_request	Eine Anforderung für eine Bedrohungssuche.
Schweregradrechner sn_si_severity_calculator	Definiert die Werte für Schweregrad, Auswirkung, Risiko und Kritikalität für einen Security Incident.
Von Aufgabe betroffener Anwender [sn_si_m2m_task_affected_user]	Eine 1:n-Tabelle, die Security Incidents den betroffenen Anwendern zuordnet.
Vorlagen-Workflow-Aktivität – Ergebnisauswertung [sn_si_wf_activity_outcome_evaluator]	Ordnet eine Fähigkeit einem Bewertungsskript zu. Ein neuer Subflow kann einem Vorlagen-Workflow hinzugefügt werden, um ein Antwortaufgabenergebnis festzulegen, anstatt dass ein Analyst es manuell festlegen muss.

Andere zusätzliche Setup-Aufgaben für Security Incident Response .

Als Administrator in der globalen Domäne konfigurieren Sie, wie Security Incident Response tägliche Vorgänge handhabt.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Diese Optionen sind für viele Servicemanagement-Anwendungen Standard und verwenden als solche Servicemanagement-Terminologie. Beispielsweise wird Anforderung für die Hauptaufgabe (den Security Incident) und Aufgabe für Teilaufgaben oder Antwortaufgaben verwendet.

Wenn Sie Administrator in einer Domäne sind, die niedriger als die globale Domäne ist, können Sie den Bildschirm Konfigurationen anzeigen, aber die Einstellungen nicht ändern.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Konfiguration**.
   Die Optionen zum Konfigurieren der Anwendungen sind unter den folgenden Registerkarten organisiert:
   - Die Registerkarte **Geschäftsprozess** enthält Optionen für das Einrichten des Anforderungslebenszyklus, das Erstellen von Katalogen und Anforderungen und das Konfigurieren von Benachrichtigungen.
   - Die Registerkarte **Zuweisung** enthält Optionen für die Einrichtung der manuellen und automatischen Zuweisung.
   - Die Registerkarte **Add-Ons** enthält Optionen zum Aktivieren der Wissensdatenbank, verwalteter Dokumente und von Aufgabenaktivitäten.
2. Füllen Sie die Felder auf der Registerkarte **Geschäftsprozess** aus.

Konfigurationsbildschirm – Registerkarte „Geschäftsprozess“.

Feld	Beschreibung
Lebenszyklus	
Zum Schließen oder Abbrechen einer Anforderung oder Aufgabe sind Arbeitsnotizen erforderlich.	Aktivieren Sie diese Option, damit der Anwender Arbeitsnotizen eingeben kann, bevor ein Security Incident oder eine Reaktionsaufgabe geschlossen oder abgebrochen werden kann.
Arbeitsnotizen zur Aufgabe in die Anforderung kopieren	Aktivieren Sie diese Option, um Arbeitsnotizen zur Antwortaufgabe mit den Arbeitsnotizen im Security Incident zu synchronisieren. Wenn also Arbeitsnotizen in der Aufgabe hinzugefügt werden, werden dieselben Arbeitsnotizen auch im übergeordneten Security Incident angezeigt.
Katalog- und Anforderungserstellung	
Anforderungen per eingehender E-Mail erstellen und aktualisieren	Aktivieren Sie diese Option, um Security Incidents aus eingehenden E-Mails zu erstellen oder zu aktualisieren.
Anforderungen werden erstellt mit	Wählen Sie **Katalog oder das reguläre Formular** aus, um den Katalog zu aktivieren und die automatische Veröffentlichung von Vorlagen für Security Incidents im Katalog zu ermöglichen. Wählen Sie **nur das reguläre Formular** aus, um den Katalog zu deaktivieren und die automatische Veröffentlichung von Vorlagen für Security Incidents im Katalog zu deaktivieren.
Mit Vorlagen wird ein eigenes Katalogelement erstellt.	Aktivieren Sie diese Option, um die automatische Veröffentlichung von Katalogelementen für die Anwendung zu aktivieren.
Benachrichtigungen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wenn sich für eine Anforderung oder Aufgabe das ausgewählte Feld ändert, wird eine Benachrichtigung an die Empfänger gesendet	Sie können Benachrichtigungen konfigurieren, die an bestimmte Empfänger gesendet werden, wenn sich ausgewählte Felder in Security Incidents und Antwortaufgaben ändern. **a.** Wählen Sie unter **Tabelledie Option Anforderung (Security Incident)** oder **Aufgabe (Antwortaufgabe)**aus. **b.** Wählen Sie unter **Feld** das Feld zum Generieren von Benachrichtigungen aus. Wenn am ausgewählten Feld eine Änderung vorgenommen wird, wird eine Benachrichtigung an die identifizierten Empfänger gesendet. **c.** Wählen Sie unter **Empfänger**einen oder mehrere Empfänger aus. **d.** Wenn **ein bestimmter Benutzer** oder **eine bestimmte Gruppe** ausgewählt ist, werden Sie aufgefordert, einen Benutzer oder eine Gruppe auszuwählen. **e.** Um weitere Benachrichtigungen mit anderen Feldern oder Empfängern zu definieren, wiederholen Sie die vorherigen Schritte für den nächsten Satz von Benachrichtigungseinstellungen. **f.** Um eine Benachrichtigung zu entfernen, klicken Sie auf das ⊖ rechts neben der Benachrichtigung.

3. Klicken Sie auf die Registerkarte **Zuweisung**, und füllen Sie die Felder aus.

Konfigurationsbildschirm – Registerkarte „Zuweisung“.

Feld	Beschreibung
Zuweisungsmethode für Anforderungen	Wählen Sie die Methode für die Zuweisung von Security Incidents aus: ○ **automatische Zuweisung verwenden**: Security Incidents werden automatisch zugewiesen. ○ **Workflow verwenden**: Security Incidents werden vom ausgewählten Workflow zugewiesen. ○ **manuell**: Security Incidents werden manuell zugewiesen.
Diesen Workflow zur Zuweisung von Anforderungen verwenden	Wählen Sie den Workflow für die Verteilung von Security Incidents aus. Dieses Feld wird angezeigt, wenn in der Liste **Zuweisungsmethode für Anforderungendie Verwendung eines Workflows** ausgewählt wird.
Zuweisungsmethode für Aufgaben	Wählen Sie die Methode für die Zuweisung von Antwortaufgaben aus: ○ **automatische Zuweisung verwenden**: Antwortaufgaben werden automatisch zugewiesen. ○ **Workflow verwenden**: Antwortaufgaben werden vom ausgewählten Workflow zugewiesen. ○ **manuell**: Antwortaufgaben werden manuell zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verwenden Sie diesen Workflow, um Aufgaben zuzuweisen	Wählen Sie den Workflow für die Zuweisung von Antwortaufgaben aus. Dieses Feld wird angezeigt, wenn in der Liste **Zuweisungsmethode für Aufgabenein Workflow verwendet wird**.
Anforderungen oder Aufgaben basierend auf Abdeckungsgebieten von Zuweisungsgruppen zuweisen	Aktivieren Sie diese Option, um die Zuweisung von Security Incidents und Antwortaufgaben an Gruppen zu beschränken, die den Standort der Aufgabe abdecken.
Zeitplanung	
Bei der automatischen Auswahl von Service Desk-Mitarbeitern wird die Zeitzone für Aufgaben berücksichtigt	Aktivieren Sie diese Option, um die Zeitzone des Mitarbeiters zu berücksichtigen, wenn Sie eine Aufgabe zuweisen. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Antwortaufgaben ausgewählt ist.
Zusätzliche Faktoren	
Bei der automatischen Auswahl von Mitarbeitern wird der Standort der Mitarbeiter berücksichtigt	Aktivieren Sie diese Option, um Mitarbeitern, die sich näher am Aufgabenstandort befinden, bei der Zuweisung von Aufgaben den Vorzug zu geben. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Antwortaufgaben ausgewählt ist.
Bei der automatischen Auswahl von Mitarbeitern für Aufgaben werden bestimmte Kompetenzen vorausgesetzt.	Wählen Sie aus, inwieweit die Kompetenzen von Service Desk-Mitarbeitern mit einer Aufgabe übereinstimmen müssen, wenn die automatische Zuweisung bestimmt wird. ○ Wählen Sie **alle** aus, um festzulegen, dass ein zugewiesener Service Desk-Mitarbeiter alle Kompetenzen zum Ausführen der Aufgabe haben muss. Ein Service Desk-Mitarbeiter, dem auch nur eine Kompetenz fehlt, wird ausgeschlossen. ○ Wählen Sie **einige** aus, wenn Sie möchten, dass Service Desk-Mitarbeiter über die meisten der zum Ausführen der Aufgabe erforderlichen Kompetenzen verfügen. ○ Wählen Sie **„Keine“** aus, wenn Sie bei der automatischen Zuweisung von Service Desk-Mitarbeitern Kompetenzen nicht berücksichtigen möchten. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Antwortaufgaben ausgewählt ist.
Bei der automatischen Auswahl wird versucht, allen Aufgaben in einer Anforderung denselben Service Desk-Mitarbeiter zuzuweisen	Aktivieren Sie diese Option, um alle Antwortaufgaben für einen Security Incident automatisch demselben Service Desk-Mitarbeiter zuzuweisen.

4. Klicken Sie auf die Registerkarte **Add-ons**, und füllen Sie die Felder aus.

Konfigurationsbildschirm – Registerkarte „Add-Ons“.

Feld	Beschreibung
Dokumentation	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Eigene Knowledge Base aktivieren	Aktivieren Sie diese Option, um die Knowledge Base für Security Incident Responsezu aktivieren.
Verwaltete Dokumente aktivieren	Aktivieren Sie diese Option, um eine zugehörige Liste zu den verwalteten Dokumenten hinzuzufügen.
Aufgabenaktivitäten aktivieren	Aktivieren Sie diese Option, um Aufgabeninteraktionen und Kommunikation wie Telefonanrufe und E-Mail-Nachrichten zu protokollieren.

5. Klicken Sie auf **Speichern**.

Sperren Sie die Sicherheitsadministration

Um Untersuchungen zu schützen und Security Incidents privat zu halten, können Sie den Zugriff Security Incident Response von auf sicherheitsspezifische Rollen und ACLs beschränken. Nicht-Sicherheitsadministratoren können vom Zugriff ausgeschlossen werden, es sei denn, Sie gewähren ihnen ausdrücklich Zugriff.

Vorbereitungen

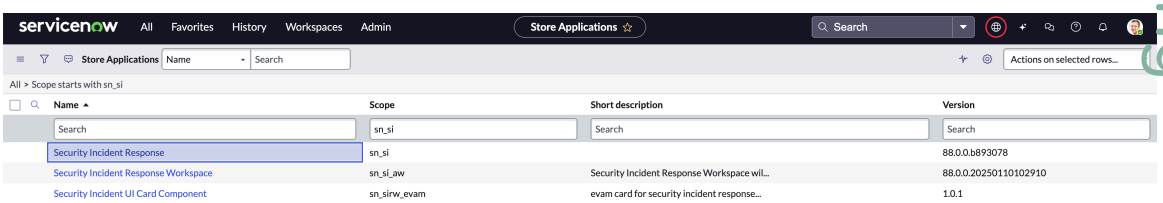
Wenn die Anwendung Security Incident Response aktiviert ist, wird dem Systemadministrator standardmäßig die Rolle sn_si.admin gewährt. Der Systemadministrator ist der einzige Administrator, der Sicherheitsgruppen und Benutzer einrichten kann.

Für den Zugriff auf die Funktionen und Datensätze Security Incident Response von ist eine Sicherheitsrolle erforderlich.

Erforderliche Rolle: sn_si.admin

Prozedur

1. Nachdem das Plugin Security Incident Response aktiviert wurde, weist ein Benutzer mit der Administratorrolle die Rolle „Bereichsbezogener Administrator“ (sn_si.admin) mindestens einem Benutzer zu.
2. Der Benutzer mit der Administratorrolle wechselt zum Bereich „Security Incident“.
3. Navigieren zu **Alle** > **sys_store_app.list**.
4. Geben Sie **sn_si** in das Feld **Umfang ein**.



5. Klicken Sie auf **Security Incident Response**.
6. Scrollen Sie nach unten zu den **zugehörigen Links**, und klicken Sie **in der Rolle admin auf Entfernen**.
7. Melden Sie sich ab und wieder an.
   Der Administratorbenutzer kann nicht auf die Anwendung Security Incident Response zugreifen.

Zugehörige Informationen

Anwendungsverwaltung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie den eingeschränkten Anruferzugriff

Mit der Funktion „Restricted Caller Access (RCA)“ kann ein Administrator den bereichsübergreifenden Zugriff auf eine Anwendung oder Anwendungsressource definieren und Zugriffsanforderungen zulassen oder ablehnen. Diese Funktion ist standardmäßig in Security Incident Response aktiviert, damit Sicherheitsanalysten vertrauliche sicherheitsbezogene Informationen schützen können.

Ein Feld namens **Anruferzugriff** wurde allen Tabellen und Skripteinbindungen in Security Incident Responsehinzugefügt, und das Feld ist standardmäßig auf **Anruferverfolgung**festgelegt. Diese Einstellung bedeutet, dass Anwendungsbereiche Zugriff auf Tabellen und Skripteinbindungen Security Incident Response haben. Es wird jedoch für jeden Datensatz ein Nachverfolgungsdatensatz erstellt und in der Tabelle für eingeschränkte Anruferzugriffsberechtigungen [sys_restricted_caller_access] gespeichert.

Hinweis:
Seien Sie vorsichtig, wenn Sie Datensätze von **„Anruferverfolgung“** in **„Anruferbeschränkung“**ändern. Auf Datensätze mit diesem Status kann erst zugegriffen werden, wenn ein Administrator manuell den Zugriff gewährt. Der Administrator muss zu navigieren **Systemanwendungen** > **Anwendung – Eingeschränkter Aufruferzugriff**, suchen Sie die Tabelle oder Skripteinbindung, für die Zugriff angefordert wurde, und ändern Sie das Feld **Status** von **Angefordert** in **Zulässig**.

Zugehörige Informationen

Einstellungen für eingeschränkte Anruferzugriffsberechtigungen

Legen Sie den Anwendungsbereich, die Anwendungsressource und den Ereigniszugriff fest

Schnellstarttests für Security Incident Response ausführen

Überprüfen Sie, ob Security Incident Response noch funktioniert, nachdem Sie Konfigurationsänderungen vorgenommen haben, z. B. durch Anwendung eines Upgrades oder durch die Weiterentwicklung einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Security Incident Response-Schnellstarttests erfordern die Aktivierung des Plugins „Security Incident Response“ (com.snc.security_incident) und das Laden der Demodaten.

Security Incident Response-Tests

Test	Beschreibung	Release-Version
SIR: Sicherheitsincident erstellen	Ermittelt, ob ein Benutzer einen Sicherheitsincident erfolgreich aus dem Sicherheitsincident-Formular erstellen kann.	Yokohama
SIR: Sicherheitsincident über den Sicherheitsincident-Katalog erstellen	Ermittelt, ob ein Benutzer einen Sicherheitsincident erfolgreich aus dem Katalog erstellen kann.	Yokohama
SIR: Lebenszyklus des Sicherheitsincident	Validiert die Antwortaufgaben des Richtlinienverletzungs-Workflows.	Yokohama
SIR: Bedrohungssuche	Validiert die Funktion der Bedrohungssuche.	Yokohama
SIR: PIR Assessments OOTB configuration (SIR: PIR-	Mit diesem Test können Sie PIR-Bewertungen und	Yokohama

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
Bewertungen – OOTB-Konfiguration)	Basissystemkonfigurationen validieren.	
SIR: PIR Assessments conditional configuration (SIR: PIR-Bewertungen – Bedingte Konfiguration)	Verifiziert, dass Security Incidents, die der obligatorischen bedingten Regel entsprechen, erst geschlossen werden, wenn die Bewertung nach dem Incident abgeschlossen ist. Verifiziert, dass Security Incidents, die der optionalen bedingten Regel entsprechen, geschlossen werden können, wenn die Bewertung nach dem Incident abgeschlossen ist. Verifiziert, dass für Security Incidents, die keiner Regel entsprechen, keine Bewertungen generiert werden.	Yokohama
SIR: PIR-Laufzeitverifizierung	Überprüft, ob PIR-Berichte gemäß dem neuen Design konfiguriert und an Sicherheits-Incidents angehängt werden.	Yokohama
SIR: Setupverifizierung der PIR-Designzeit	Überprüft, ob der Sicherheit-Incident je nach Administratorkonfiguration der Berichtsvorlage zugeordnet wird.	Yokohama
SIR: Security Incident mit einem vorhandenen schwerwiegenden Security Incident verknüpfen	Verknüpfen Sie einen Security Incident mit einem vorhandenen schwerwiegenden Security Incident, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden.	Yokohama
SIR: Security Incident als schwerwiegenden Security Incident hochstufen	Stufen Sie einen Security Incident zu einem schwerwiegenden Security Incident hoch, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden.	Yokohama
SIR: Security Incident als schwerwiegenden Security Incident vorschlagen	Schlagen Sie einen Security Incident als einen schwerwiegenden Security Incident	Yokohama

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
	vor, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden.	
Verifiziert, dass nur zulässige Mitglieder auf den Security Incident zugreifen können, wenn „Beschränkung erzwingen“ aktiviert ist	Verifiziert, dass nur die zulässigen Mitglieder auf den Security Incident zugreifen können, wenn „Beschränkung erzwingen“ aktiviert ist.	Yokohama
Verifiziert, dass nur zulässige Gruppen auf den Security Incident zugreifen können, wenn „Beschränkung erzwingen“ aktiviert ist	Verifiziert, dass nur die zulässigen Gruppen auf den Security Incident zugreifen können, wenn „Beschränkung erzwingen“ aktiviert ist.	Yokohama
Lesezugriff validieren	Validieren Sie den Anzeigezugriff.	Yokohama
Schreibzugriff validieren	Validieren Sie den Bearbeitungszugriff.	Yokohama
SIR-Arbeitsbereich: Lesezugriff	Verifiziert, ob ein Anwender mit Lesezugriff den Security Incident anzeigen kann, ohne über Sicherheitsrollen zu verfügen, auch im Arbeitsbereich	Yokohama
SIR-Arbeitsbereich: Schreibzugriff	Verifiziert, ob ein Anwender mit Schreibzugriff den Security Incident aktualisieren kann, ohne über Sicherheitsrollen zu verfügen	Yokohama
SIR-Arbeitsbereich: Neuen Security Incident erstellen	Erstellen Sie im Arbeitsbereich einen neuen Security Incident	Yokohama
SIR-Arbeitsbereich: Antwortaufgabe erstellen	Erstellen Sie eine neue Antwortaufgabe aus einem vorhandenen Security Incident	Yokohama

Zugehörige Informationen

Schnellstarttests

Referenz des Setup-Assistenten

Der Setup-Assistent führt Sie durch die Schritte, die Sie zum Einrichten des Basissystems Security Incident Response ausführen müssen. Dieser Abschnitt enthält zusätzliche Informationen zu den komplizierten Schritten, für die Sie möglicherweise weitere Erklärungen benötigen.

Erstellen Sie eine Security Incident Response -Prozessdefinition

Sie können eine Prozessdefinition erstellen, um zu definieren, wie Security Incidents von einem Status in den nächsten übergehen. Prozessdefinitionen helfen Service Desks und Endanwendern, das Problem während des gesamten Lebenszyklus nachzuverfolgen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn.si_admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Prozessdefinition**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Prozessdefinitionen werden erstellt

Feld	Beschreibung
Name	Name des Datensatzes, der den in der Skripteinbindungsdatei codierten Prozess beschreibt. Der Name wird als Auswahl in der Liste **Prozessdefinitionsauswahl** angezeigt.
Skripteinbindung	Der Name (einschließlich des Präfix `sn_si.`) der Skripteinbindung, die die Definition des Prozesses enthält. Das Skript muss sich im Anwendungsbereich „Security Incident“ (`sn_si`) befinden. Weitere Informationen finden Sie unter Erstellen Sie eine anwenderdefinierte Security Incident Response Prozessdefinitions-Skripteinbindung. Wenn dieses Feld keinen gültigen Skripteinbindungsnamen enthält, wird die Standarddefinition ProcessDefinition_NIST_Stateful verwendet.
Beschreibung	Hilfreiche Informationen zur Skripteinbindung.
Bestellung	Bestimmt die Position in der Liste der Prozessdefinitionen.
Aktiv	Wenn diese Option aktiviert ist, kann diese Prozessdefinition auf der Seite **„Auswahl für Prozessdefinition“** ausgewählt werden.

4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Prozessauswahl für Security Incident Response

Informationen zum Prozessdefinition von Security Incident Response

Informationen zum Prozessdefinition von Security Incident Response

Security Incident Response Prozessdefinition ersetzt Status-Flows und stellt Endanwendern und Service Desks den Status eines Problems bereit. Eine Prozessdefinition hilft, das Problem während seines Lebenszyklus nachzuverfolgen. Security Incident Response ist eine Servicemanagement-Anwendung (Service Management, SM) mit eigenen Status. Ungültige Status werden als Teil von Prozessauswahlgemeldet.

Prozessdefinition für Security Incident Response

Die Standardprozessdefinition (NIST Stateful) definiert die folgenden Incident-Status:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die verfügbaren Status variieren je nach aktuellem Status des incident.

Status der Prozessdefinition für Security Incidents

Status	Beschreibung
Entwurf	Der Initiator der Anforderung fügt Informationen zum Security Incident hinzu, er ist jedoch noch nicht zur Bearbeitung bereit.
Analyse	Der Incident wurde zugewiesen, und das Problem wird analysiert.
Begrenzen	Das Problem wurde identifiziert, und das Sicherheitspersonal arbeitet daran, es einzudämmen und Schadenskontrolle durchzuführen. Diese Aktionen können das Offline-Schalten von Servern, das Trennen von Geräten vom Internet und das Überprüfen des Vorhandenseins von Sicherungen umfassen.
Beseitigen	Das Problem wurde eingedämmt, und das Sicherheitspersonal unternimmt Schritte, um das Problem zu beheben.
Wiederherstellen	Das Problem ist behoben, und die Betriebsbereitschaft der betroffenen Systeme wird überprüft.
Prüfung	Der Security Incident ist abgeschlossen, und alle Systeme funktionieren wieder normal, es ist jedoch noch eine Überprüfung nach dem Incident erforderlich.
Abgeschlossen	Der Incident ist abgeschlossen, aber bevor ein Security Incident geschlossen werden kann, müssen Sie die Informationen auf der Registerkarte **Abschlussinformationen** ausfüllen.

Prozessdefinitionen für Security Incident-Aufgaben

Die folgenden Prozessdefinitionen werden für Security Incident-Aufgaben verwendet.

Status der Aufgabenprozessdefinition

Status	Beschreibung
Bereit	Die Aufgabe ist zur Bearbeitung bereit, nachdem sie einem Service Desk-Mitarbeiter zugewiesen wurde.
Zugewiesen	Die Aufgabe ist einem Service Desk-Mitarbeiter zugewiesen.
In Bearbeitung	Der zugewiesene Service Desk-Mitarbeiter arbeitet an der Aufgabe.
Abgeschlossen	Die Aufgabe ist abgeschlossen.
Abgebrochen	Die Aufgabe wurde abgebrochen.

NIST unterstützt die folgenden beiden Modelle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **NIST Stateful**

  Mit dieser Prozessdefinition können Analysten in einer sequenziellen Reihenfolge von einem Status in einen anderen wechseln, ohne einen Schritt zu überspringen. Wenn der Analyst beispielsweise mit dem Status **Entwurf** beginnt, lautet die sequenzielle Reihenfolge dieser Prozessdefinition **Entwurf**>**Analyse**>**Eindämmen**>**Löschen**>**Wiederherstellen**. Daher ist die Definition des NIST Stateful-Prozesses unidirektional und ermöglicht es Analysten, nur zu den Vorwärtsstatus zu gelangen.

  Hier sehen Sie ein weiteres Beispiel: Wenn der Analyst mit dem Status Analyse beginnt, lautet die sequenzielle Reihenfolge dieser Prozessdefinition **Analyse**>**Eindämmen**>**Beseitigen**>**Wiederherstellen**.

- **NIST Open**

  Mit dieser Prozessdefinition können Analysten von einem Status in einen anderen wechseln, entweder vorwärts oder rückwärts. Wenn der Analyst beispielsweise mit dem Status **Analyse** beginnt, kann die Reihenfolge der Prozessdefinition entweder **Analyse**>**Eindämmen**>**Beseitigen**>**Wiederherstellen** oder **Analyse**>**Entwurf lauten**. Die Prozessdefinition von NIST Open ist also bidirektional und ermöglicht es Analysten, je nach Anforderungen in den Status „Vorwärts“ oder „Rückwärts“ zu wechseln.

Prozessauswahl für Security Incident Response

Security Incident Response Die Prozessauswahl listet Prozesse mit ungültigen Status für Security Incidents und Antwortaufgaben auf.

Ein Administrator kann den Incident oder die Aufgabe entweder manuell oder mithilfe eines Skripts auf gültige Status zurücksetzen. Eine leere zugehörige Liste (keine Incidents, keine Aufgaben) gibt an, dass jede aktive Aufgabe einen gültigen Status aufweist. Die verfügbaren Status variieren je nach aktuellem Status des incident. Weitere Informationen finden Sie unter Korrektur ungültiger Status von Security Incidents oder Aufgaben mit Prozessdefinitionen.

Wählen Sie eine Security Incident Response -Prozessdefinition aus

Sie können die Prozessdefinition auswählen, die für die entsprechenden Status der Security Incidents und Reaktionsaufgaben Ihres Unternehmens verwendet werden soll.

Vorbereitungen

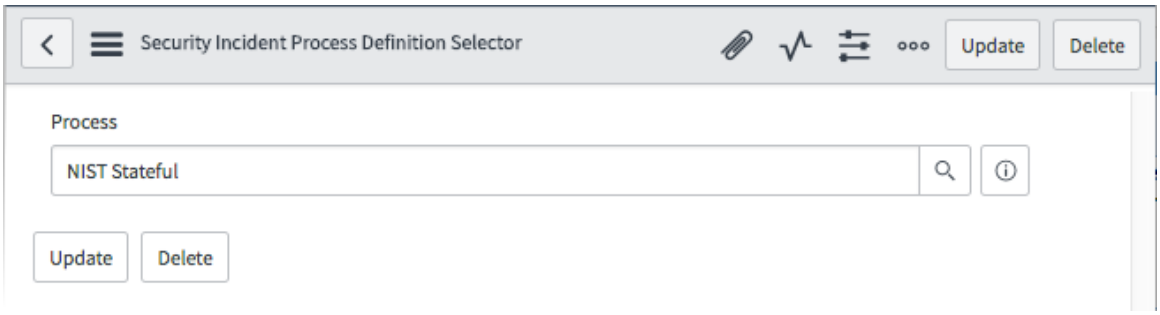
Erforderliche Rolle: admin und sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Security Incident Response** > **Administration** > **Prozessauswahl**.
2. Klicken Sie auf das Suchsymbol, um die verfügbaren Prozessdefinitionen aufzulisten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie eine Prozessdefinition aus.
4. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine anwenderdefinierte Security Incident Response Prozessdefinitions-Skripteinbindung

Erstellen Sie ein anwenderdefiniertes Prozessdefinitionsskript für die entsprechenden Status für Security Incidents und Antwortaufgaben Ihres Unternehmens.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Die Hauptskripteinbindung sn_si.ProcessDefinition steuert Prozessdefinitionen. **Die Prozessdefinition** bestimmt, welche Definition verwendet wird (mithilfe **der Prozessauswahl**). Sie ruft die entsprechende Skripteinbindungsdatei auf, um die Anfangsstatus und Übergänge für Security Incidents und Antwortaufgaben zu bestimmen.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

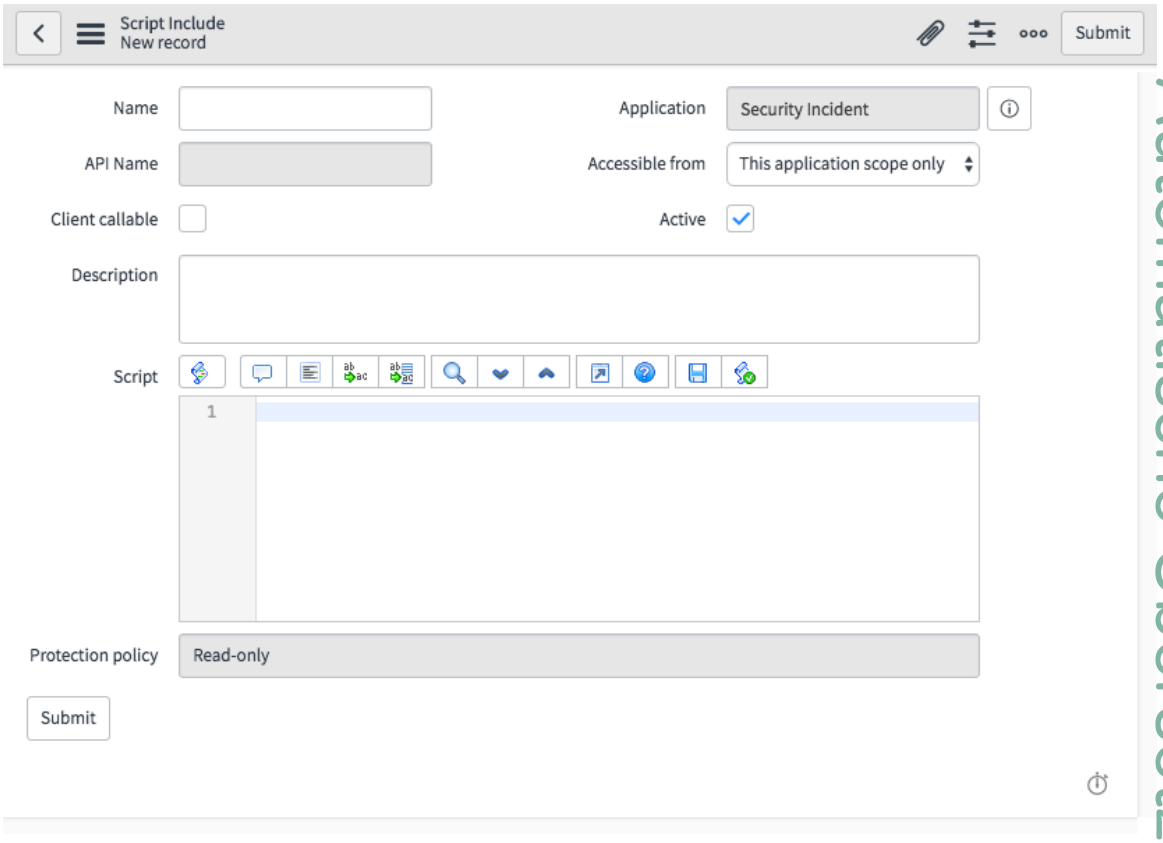
Prozessdefinitionen werden erstellt

Feld	Beschreibung
Name	Name dieser Skripteinbindung.
API-Name	Wird basierend auf dem Namen der Skripteinbindung erstellt.
Vom Client aufrufbar	Stellt die Skripteinbindung für Client-Skripts, Listen- und Berichtsfilter, Referenzqualifizierer oder,, falls angegeben, als Teil der URL bereit.
Anwendung	Security Incident
Zugänglich von	Wählen Sie **Nur dieser Anwendungsbereich** aus.
Aktiv	Wenn diese Option aktiviert ist, kann diese Skripteinbindung auf der Seite **„Prozessdefinition“** ausgewählt werden.
Beschreibung	Hilfreiche Informationen zur Skripteinbindung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Skript	Definiert das serverseitige Skript, das bei Aufruf von anderen Skripts ausgeführt werden soll. Das Skript muss eine einzelne JavaScript-Klasse oder eine globale Funktion definieren. Der Klassen- oder Funktionsname muss mit dem Wert im Feld Name übereinstimmen. Informationen zu Skriptinhalten finden Sie unter Skripteinbindung für Prozessdefinition.



4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Skripteinbindung für Prozessdefinition

Skripteinbindung für Prozessdefinition

Die Skripteinbindung für die Prozessdefinition stellt Methoden zum Definieren einer Prozessdefinition bereit.

Implementieren Sie die hier beschriebenen Konstanten, Attribute, Arrays und Methodenaufrufe, um eine Skripteinbindung für eine Prozessdefinition anzupassen.

Verwendungszweck

Verwenden Sie diese Skripteinbindung, um eine Prozessdefinition zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skripteinbindungstext

Der Textkörper der Skripteinbindung besteht aus drei Abschnitten:

- Konstanten: Definitionen des Anfangsstatus
- Security Incident und Antwortaufgabe: Prozessdefinitions-Arrays
- Methodenaufrufe: Abrufen von Informationen

Konstanten

Konstanten werden verwendet, um die Anfangsstatus von Security Incidents und Antwortaufgaben zu definieren.

Die Verwendung von Konstanten ist optional, wird jedoch aus Gründen der Lesbarkeit empfohlen. Zum Beispiel:

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Welche werden später von den folgenden Methoden verwendet:

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

Der nächste Satz von Konstanten definiert die Status für Security Incidents und Antwortaufgaben.

Jedes Array enthält auch die Definition, welche Status verfügbar sind, wenn sich der Incident oder die Aufgabe in einem bestimmten Status befindet.

Zum Beispiel:

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

Das Beispiel ist ein Array von Objekten. Jedes Objekt definiert einen Status und mögliche Übergangsstatus.

Die Reihenfolge des Statusobjekts bestimmt die gewünschte Reihenfolge für den Flow.

Wenn sich die Aufgabe im Status „Entwurf“ (Wert 1) befindet, sind folgende Status möglich: 1 (Entwurf, keine Änderung) und 10 (Bereit, nächster Schritt im Prozess).

Es gibt keine Begrenzung für die Anzahl der Übergänge aus einem Status. Die Status „Abschließen“ und „Abgebrochen“ sind Endstatus und weisen daher keine möglichen Statusübergänge auf.

Die Reihenfolge der Attribute im Objekt ist nicht wichtig. Wenn dies die Definition klarer macht, setzen Sie die Bezeichnung zuerst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute

Erforderliche Attribute in einem Statusdefinitionsobjekt:

- state: Numerischer Wert des Status
- label: visuell lesbarer Text, der dem Status zugeordnet ist
- Auswahl: Ein Array von Statuswerten, in die der Status übergehen kann (bestimmt den Inhalt der Status-Dropdownliste)

Optionale Attribute:

- obligatorisch: Liste der Feld-IDs, die in diesem Status obligatorisch werden
- schreibgeschützt: Liste der Feld-IDs, die in diesem Status schreibgeschützt werden
- sichtbar: Liste der Feld-IDs, die in diesem Status sichtbar werden
- nicht obligatorisch: Liste der Feld-IDs, die in diesem Status nicht obligatorisch werden
- notvisible: Liste der Feld-IDs, die in diesem Status nicht mehr sichtbar sind

Hinweis:

Wenn optionale Attribute verwendet werden, liegt es in der Verantwortung des Autors, sicherzustellen, dass Felder zwischen den Status entsprechend sichtbar/unsichtbar, obligatorisch/nicht obligatorisch, sichtbar/ausgeblendet oder schreibgeschützt sind.

Wenn Sie beispielsweise ein Feld in einem Status ausblenden, wird es später in einem anderen Status sichtbar, es sei denn, das Attribut „sichtbar“ wird verwendet.

Arrays für Prozess-Flow-Definitionen

Um die im Formatierer für Prozess-Flows angezeigten Informationen (der Balken oben auf den Formularen für Security Incident- und Response-Aufgaben) zu definieren, benötigt das System Informationen darüber, was für den jeweiligen Status angezeigt werden soll.

Zum Beispiel:

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>"},
{label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>"},
{label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>"},
{label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>"},
{label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>"},
],
```

Das Array TASK_PF ist eine Sammlung von Bezeichnungen, Bedingungen und Beschreibungen, die verwendet werden, um den Text zu bestimmen, der in der Prozessformatierer-Leiste angezeigt wird (einschließlich Reihenfolge und Aktivität).

Im Beispiel wird der Text „Bereit“ als zweites Element angezeigt. Sie wird hervorgehoben, wenn die Aufgabe die Bedingung „state=10^EQ“ erfüllt.

Wenn der Mauszeiger über den Text bewegt wird, wird die Beschreibung „Security Incident Response-Aufgabe ist bereit für die Zuweisung“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Status können zu einem einzelnen Formatiererstatus kombiniert werden.

Im Beispiel werden die Status „Abschließen – vollständig“ und „Abgebrochen“ in der oberen Leiste als „Geschlossen“ angezeigt.

Methodenaufrufe

Die folgenden Methoden müssen in der Skripteinbindung vorhanden sein, da sie von sn_si.ProcessDefinition verwendet werden:

Rückgabetyp	Methodenübersicht	Beschreibung
Zeichenfolge	getInitialIncidentState: Funktion ()	Gibt den numerischen Wert des anfänglichen Incident-Status zurück
Zeichenfolge	getInitialTaskState: Funktion():	Gibt den numerischen Wert der anfänglichen Aufgabe zurück
Array von Zeichenfolgen	getIncidentStates: Funktion():	gibt das Array des Incident-Status zurück
Array von Zeichenfolgen	getTaskStates: Funktion():	gibt das Array des Aufgabenstatus zurück
Array von Objekten	getIncidentProcessFlows: Funktion():	Geben Sie das Array der Definitionen des Incident-Prozess-Flows zurück
Array von Objekten	getTaskProcessFlows: Funktion():	Geben Sie das Array der Definitionen des Prozess-Flows für die Aufgabe zurück

Der nächste Satz von Methoden wird immer dann aufgerufen, wenn ein Incident oder eine Aufgabe aktualisiert wird, und ermöglicht Aktionen für bestimmte Change-Übergänge.

Rückgabetyp	Methodenübersicht	Beschreibung
void	durchführenIncidentStateChange: Funktion (aktuell, vorher)	In den Beispielen wird diese Methode verwendet, um SM-bezogene Werte festzulegen und sicherzustellen, dass ein Incident aus „Entwurf“ fortschreitet, nachdem ihm jemand zugewiesen wurde.
void	durchführenTaskStateChange: Funktion (aktuell, vorherige)	Im Beispiel wird diese Methode verwendet, um Zeitstempel zu aktualisieren (bei Zuweisung und Abschluss) und die Aufgabe von „Bereit“ auf „Zugewiesen“ zu ändern, sobald das Feld assigned_to ausgefüllt ist.

Die gleichen Aktionen, die durch diese beiden Methoden ausgeführt werden, können mit einer Geschäftsregel durchgeführt werden. Durch die Definition in der Skripteinbindung wird der Wechsel der Prozessdefinitionen erleichtert.

Korrektur ungültiger Status von Security Incidents oder Aufgaben mit Prozessdefinitionen

Ein Administrator kann den Security Incident oder die Aufgabe manuell oder mithilfe eines Skripts auf gültige Status zurücksetzen. Die verfügbaren Status variieren je nach aktuellem Status des incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

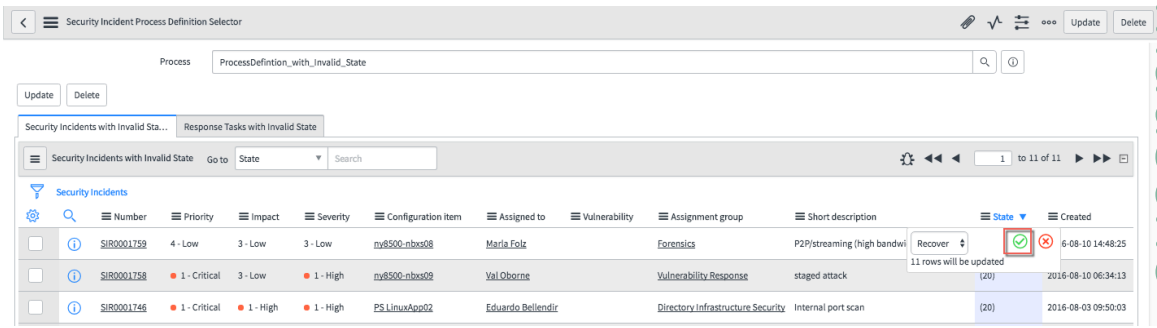
Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie die Prozessdefinitionen gewechselt haben, unterstützt die neue Definition möglicherweise einige der alten Status nicht. Um die Status verwaister Incidents oder Aufgaben zu korrigieren, können Sie Ihre Prozessdefinition ändern, Ihre Skripteinbindung bearbeitenoder die einzelnen Incidents und Aufgaben manuell öffnen, um den Status zu aktualisieren. Im Allgemeinen ist das Aktualisieren des Status (das Massenaktualisieren kann) die einfachste Lösung.

Um Status in einem Massenvorgang zu ändern, gehen Sie wie folgt vor:

Prozedur

1. Navigieren zu **Alle** > **Prozessauswahl**.
2. Markieren Sie das Feld **Status** für die Incidents oder Aufgaben, die Sie ändern möchten.
3. Doppelklicken Sieauf das Feld **Status** im ersten Datensatz, wählen Sie den neuen **Status aus,** und klicken Sie auf das grüne Häkchen ( ), um die Änderung abzuschließen.



4. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine Security Incident-Gruppe

Richten Sie eine Security Incident-Gruppe ein, und weisen Sie der Gruppe die entsprechenden Rollen und Anwender zu.

Vorbereitungen

Erforderliche Rollen:

- Mit der Rolle user_admin können Sie Security Incident-Zuweisungsgruppen erstellen.
- Mit der Rolle sn_si.admin können Sie Zuweisungsgruppen für Security Incidents erstellen und bearbeiten.

Warum und wann dieser Vorgang ausgeführt wird

Benutzer in einer Gruppe erben die Rollen der Gruppe, sodass Sie nicht jedem Benutzer einzeln Rollen zuweisen müssen.

Es empfiehlt sich, in Ihrer Organisation so viele Gruppen wie nötig zu erstellen. Es wird auch empfohlen, eine Gruppe für Administratoren zu erstellen und nur diese Gruppe die Administratorrolle zuzuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen** oder **Security Incident** > **Setup** > **Gruppen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Hinweis:

Weitere Informationen finden Sie unter Benutzergruppen erstellen .

4. Stellen Sie sicher, dass Sie den **Security Incident** -Typ für diese Gruppe auswählen.
   a. Wenn das Feld **Typ** nicht sichtbar ist, konfigurieren Sie das Formular zum Hinzufügen.
   b. Klicken Sie auf das Schlosssymbol neben dem Feld **Typ**.
   c. Klicken Sie auf das Referenz-Suchsymbol ( )
   d. Suchen Sie nach dem Typ **des Security Incident**, und wählen Sie ihn aus.
5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Fügen Sie in der zugehörigen Liste **„Rollen“** die Rollen hinzu, die jedes Mitglied dieser Gruppe erhält. Wenn Sie beispielsweise eine Gruppe für Security Incident Response Teammitglieder erstellen, fügen Sie sn_si.analyst hinzu. Wenn Sie eine Gruppe für Security Incident Response -Administratoren erstellen, fügen Sie sn_si.admin hinzu.
7. Fügen Sie dieser Gruppe in der zugehörigen Liste **Gruppenmitglieder** Anwender hinzu.
8. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine Rechnergruppe für Security Incidents

Security Incident-Rechnergruppen werden verwendet, um Rechner zu gruppieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Security Incident-Rechnergruppen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name des Rechners für Security Incidents.
Anwendung	Die Anwendung, die diesen Datensatz enthält.
Bestellung	Reihenfolge, in der der Security Incident-Rechner ausgeführt wird. Ein Rechner mit einem Reihenfolgeneintrag von 100 wird vor einem Rechner mit einem Reihenfolgeneintrag von 200 ausgeführt.
Beschreibung	Eine Beschreibung dieser Rechnergruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellt von	Geben Sie den Namen des Benutzers ein, der erstellt hat

4. Klicken Sie auf **Absenden**.

Erstellen Sie einen Security Incident-Rechner

Mit Security Incident-Rechnern können Sie den Schweregrad eines Security Incidents basierend auf vordefinierten Formeln berechnen. Sie können nach Bedarf eigene Rechner für Security Incidents definieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Security Incident-Rechnergruppen**.
2. Klicken Sie auf den Namen der Gruppe, für die Sie einen Rechner erstellen möchten, oder erstellen Sie eine Rechnergruppe.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name des Rechners für Security Incidents.
Rechnergruppe	Name der Gruppe, zu der dieser Rechner gehört. **Hinweis:** Das Erstellen oder Ändern der Rechnergruppe wird erst möglich, nachdem Sie einen **Namen** und **eine Tabelle**eingegeben haben.
Tabelle	Wählen Sie die Tabelle aus, die für diesen Rechner verwendet werden soll. Wenn Sie Rechner zu anderen Tabellen als „Schwachstelle“ [sn_vul_vulnerability] und „Angreifbares Element“ [sn_vul_vulnerable_item] hinzufügen, müssen Sie diesen Tabellen Business-Regeln und UI-Aktionen hinzufügen. So zeigen Sie Beispiele an: ○ Navigieren zu **Systemdefinition** > **Business-Regeln**, und suchen Sie die Geschäftsregel **Schweregrad berechnen** in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item]. ○ Navigieren zu **System-UI** > **UI-Aktionen**, und suchen Sie in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item] nach der UI-Aktion **Schweregrad berechnen**. Außerdem müssen der Schwachstellen-Administratorrolle für jede Tabelle, die von einem Rechner verwendet wird, vollständige Lese-, Schreib- (oder save_as_template) Funktionen gewährt werden, damit die auf die Vorlage anzuwendenden Werte ordnungsgemäß angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Die bereichsbezogene Anwendung, zu der der Rechner gehört.
Bestellung	Reihenfolge, in der der Security Incident-Rechner ausgeführt wird. Ein Rechner mit einem Reihenfolgeneintrag von 100 wird vor einem Rechner mit einem Reihenfolgeneintrag von 200 ausgeführt.
Aktiv	Rechner ein- oder ausschalten.
Beschreibung	Eine Beschreibung dieses Rechners.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Registerkarten **Bedingungen** und **Anzuwendende Werte** werden angezeigt.
6. Füllen Sie die Felder auf der Registerkarte **Bedingungen** entsprechend aus.

Feld	Beschreibung
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine vordefinierte Filtergruppe zu verwenden oder eine neue Filtergruppe zu erstellen, um die Rechnerkriterien zu definieren.
Filtergruppe	Wählen Sie die Filtergruppe aus, die zum Definieren eines Rechners verwendet werden soll. Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Filtergruppen verwenden** aktiviert haben.
Erweiterte Bedingung verwenden	Aktivieren Sie dieses Kontrollkästchen, um anzugeben, dass eine Skriptbedingung verwendet wird, um zu bestimmen, wann dieser Rechner angewendet wird. Wenn Sie das Kontrollkästchen aktivieren, wird das Skriptfeld **Erweiterte Bedingung** angezeigt. Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert haben, wird dieses Feld ausgeblendet. **Hinweis:** Bevor Sie erweiterte Bedingungen definieren und Skripts schreiben, um zu bestimmen, wann die Rechner für Security Incidents angewendet werden, kehren Sie zur Liste der Rechner für Security Incidents zurück. Erkunden Sie die im Lieferumfang des Basissystems enthaltenen Rechnerdatensätze.
Bedingung	Definiert grundlegende Filterbedingungen, um zu bestimmen, ob der Rechner verwendet wird. Wenn Sie eines der Kontrollkästchen **Filtergruppe verwenden** oder **Erweiterte Bedingungen verwenden** aktiviert haben, wird dieses Feld ausgeblendet.

7. Klicken Sie auf die Registerkarte **Anzuwendende Werte**, und füllen Sie die Felder im Formular entsprechend aus.
   Sie können ein Skript zum Definieren der Werte erstellen, die auf die Berechnung angewendet werden sollen, oder eine Vorlage basierend auf Feldern in der ausgewählten Tabelle definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Skriptwerte verwenden	Aktivieren Sie dieses Kontrollkästchen, um Feldwerte mit einem Skript zu definieren.
Skriptwerte	Definiert, auf welche Werte die Berechnungen angewendet werden sollen. Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Skriptwerte verwenden** aktiviert haben.
Vorlage	Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**. Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten.

8. Wenn Sie alle Eingaben abgeschlossen haben, klicken Sie auf **Absenden**.

Informationen zu Security Incident-Rechnern

Security Incident-Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner sind nach den Kriterien gruppiert, mit denen bestimmt wird, wie die Datensätze aktualisiert werden.

Das -Basissystem Security Incident Response enthält die folgenden Rechnergruppen und Rechner für Security Incidents. In jeder Gruppe wird der erste Rechner ausgeführt, der den Bedingungen entspricht.

Security Incident-Rechner im Basissystem

Rechnergruppenna für Security Incident	Rechner in Gruppe enthalten	Beschreibung
Geschäftsauswirkung	Aus Schweregradrechnern zusammenfassen	Dieser Rechner wird an den Sicherheitsrelevanz-Rechner delegiert, der die Relevanz durch Gewichtung der Werte anderer Felder bestimmt.
Schweregrad	Geschäft betroffen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators.
	Wichtiger Service betroffen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe einer erweiterten Bedingung. Wenn das Configuration Item im Security Incident einem äußerst wichtigen Business-Service zugeordnet ist, werden die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** entsprechend der Definition im Rechner erhöht.
	Kritische Serviceänderungen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe einer erweiterten Bedingung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-Rechner im Basissystem (Fortsetzung)

Rechnergruppennar für Security Incident	Rechner in Gruppe enthalten	Beschreibung
		Wenn der Security Incident die Bedingungen erfüllt, wird ein Skript ausgeführt, um zu definieren, auf welche Ebenen die Felder erhöht werden. Wenn das Configuration Item im Security Incident mit einem sehr kritischen oder kritischsten Business-Service verknüpft ist, werden die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** entsprechend der Definition im Rechner erhöht.
	Vektoren für Mehrfachangriffe	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators. Wenn das Konfigurationselement im Security Incident mit Web-, E-Mail- und Identitätswechsel-Angriffsvektoren verknüpft ist, werden die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** entsprechend der Definition im Rechner erhöht.
	Priorität mit Kategorie und Services festlegen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators. Die Priorität des Security Incidents wird auf **1 - Kritisch** festgelegt, wenn die folgenden Bedingungen erfüllt sind: • Dem Security Incident sind betroffene Services zugeordnet, von denen einer kritisch ist. • Der Security Incident ist eine der folgenden Kategorien: ○ Denial of Service ○ Spear-Phishing ○ Böswillige Code-Aktivität **Hinweis:** Dieser Rechner ist im Basissystem verfügbar, wenn Sie die Preisstufe Starter Security Operation haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-Rechner im Basissystem (Fortsetzung)

Rechnergruppennar für Security Incident	Rechner in Gruppe enthalten	Beschreibung

	Priorität für erkennbare Elemente festlegen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators.
		
		Die Priorität des Security Incidents wird auf **1 - Kritisch** festgelegt, wenn die folgenden Bedingungen erfüllt sind:
		• Dem Security Incident sind betroffene Services zugeordnet, von denen einer kritisch ist.
		• Der Security Incident ist eine der folgenden Kategorien:
		  ○ Denial of Service
		  ○ Spear-Phishing
		  ○ Böswillige Code-Aktivität
		• Eines der zugeordneten erkennbaren Elemente oder Indikatoren hat eine Sichtungsanzahl, die zwei Sichtungen mit aktiven Indikatoren überschreitet (d. h., die erkennbaren Elemente oder Indikatoren werden von mehreren Quellen als schlecht bestätigt).
		
		Hinweis:
		Dieser Rechner ist im Basissystem verfügbar, wenn Sie die Preisstufe „Erweiterter Sicherheitsvorgang“ haben und das Plugin „Bedrohungsfeeds“ aktivieren.

Anwenderrelevanz	Anwenderrelevanz abrufen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators. Dieser Schweregradrechner bewirkt, dass die Geschäftsrelevanz des Benutzers in **1 – Kritisch** geändert wird, wenn das Feld **Abteilung** in **Finanzwesen**geändert wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-Rechner im Basissystem (Fortsetzung)

Rechnergruppenname für Security Incident	Rechner in Gruppe enthalten	Beschreibung
	Anwendergruppenrelevanz abrufen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators. Dieser Schweregrad-Rechner ist ein Beispiel für einen Rechner, der für Daten in einer zugehörigen Liste ausgeführt wird.

Schweregrad-Rechner

Wenn Sie einen Security Incident erstellen, enthalten die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** Standardwerte. Wenn Sie den Incident speichern, validiert eine Geschäftsregel automatisch die Informationen im Security Incident anhand der Bedingungen, die in jedem Ihrer aktiven Schweregradrechner definiert sind. Sie werden jeweils mit einem Sicherheitsrechner in der durch das Feld **„Reihenfolge“** in jedem Rechner definierten Reihenfolge validiert. Wenn Informationen im Security Incident den in einem der Rechner definierten Bedingungen entsprechen, werden die Feldwerte für den Schweregrad entsprechend den im Rechner eingerichteten Regeln aktualisiert.

Angenommen, Sie erstellen einen Security Incident für ein betroffenes CI, und das CI ist äußerst kritisch. Beim Speichern des Security Incident werden die CI-Informationen mit den in den Schweregradrechnern definierten Bedingungen verglichen. Wenn der Security Incident anhand des Rechners für den Schweregrad **des betroffenen Service „Kritisch“** validiert wird, werden die Felder für den Schweregrad automatisch aktualisiert, und es wird oben im Security Incident eine Meldung ähnlich der folgenden angezeigt.

Severity Calculation applied: Critical service changes; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High

Sie können diese Schweregradrechner unverändert verwenden oder sie bearbeiten, um sie den Anforderungen Ihres Unternehmens besser zu entsprechen. Wenn Sie beispielsweise Web- und E-Mail-Bedrohungen identifizieren möchten, die für den Geschäftsbereich Finanzen spezifisch sind, können Sie die Bedingungen des Rechners **für Mehrfachangriffsvektoren** ändern:

- [Angriffsvektor] [enthält] [Web]
- [Angriffsvektor] [enthält] [E-Mail]
- [Geschäftsbereich] [enthält] [Finanz]

Sie können die Schweregradwerte in einem vorhandenen Security Incident auch jederzeit aktualisieren, indem Sie den Datensatz öffnen und auf den zugehörigen Link **Schweregrad berechnen** klicken.

Rechner für Risikopunktzahl von Security Incidents

Die Rechner **„Priorität mit Kategorie und Services festlegen“** und **„Priorität mit erkennbaren Elementen festlegen“** werden verwendet, um eine Risikopunktzahl für einen Security Incident zu berechnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rechner für Benutzerrelevanz

Die beiden Rechner in der **Benutzerrelevanzgruppe** (**Anwenderkritikalität abrufen** und **Anwendergruppenkritikalität abrufen**) zeigen, wie Sie die Relevanz anhand von Kriterien steuern können, die in einem Benutzerdatensatz oder anhand der Gruppe, zu der ein Benutzer gehört, definiert sind.

Sie können nach Bedarf bearbeitet werden, oder es können neue Benutzerrelevanzrechner erstellt werden.

Mit dem Rechner **für Anwenderrelevanz** abrufen ändert sich die Geschäftskritikalität des Anwenders in **1 – Kritisch,** wenn das Feld **Abteilung** in **Finanzwesen**geändert wird.

Mit dem Rechner **für die Kritikalität von Anwendergruppen** abrufen ändert sich die Geschäftsrelevanz des Anwenders in **1 - Kritisch,** wenn der Anwender zur Gruppe **Datenbank** hinzugefügt wird.

Hinweis:
„Benutzergruppenrelevanz abrufen“ ist ein Beispiel für einen Rechner, der für Daten in einer zugehörigen Liste ausgeführt wird. Wenn Sie weitere Gruppen hinzufügen möchten, um eine Kritikalitätsänderung zu initiieren, fügen Sie in der ersten Zeile des Skripts eine durch Kommas getrennte Liste mit Gruppen-sys_ids hinzu. Beispiel: `var CRITISCH_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id]`.

Berechnung der Risikopunktzahl des Security Incidents

Die Risikopunktzahl wird als arithmetischer Mittelwert berechnet, der das Risiko basierend auf der Priorität eines Security Incidents, dem Typ des Security Incidents (Denial of Service, Spear-Phishing oder böswillige Code-Aktivität) und der Anzahl der Quellen darstellt, die einen fehlgeschlagenen Incident ausgelöst haben Reputationspunktzahl für einen Indikator.

Die Risikopunktzahl hilft Analysten, die Arbeit mit Security Incidents zu priorisieren.

Wichtig:
Wenn Sie den neuen Risikobewertungsrechner verwenden möchten, lesen Sie unter Definieren Sie die neuen Regeln des Risikobewertungsrechnersnach.

Die Security Incident-Rechner „ **Priorität mit Kategorie und Services festlegen“** und **„Priorität mit erkennbaren Elementen festlegen“** werden verwendet, um eine Risikopunktzahl für einen Security Incident zu berechnen. Darüber hinaus lösen die folgenden Geschäftsregeln die automatische Berechnung von Risikopunktzahlen aus:

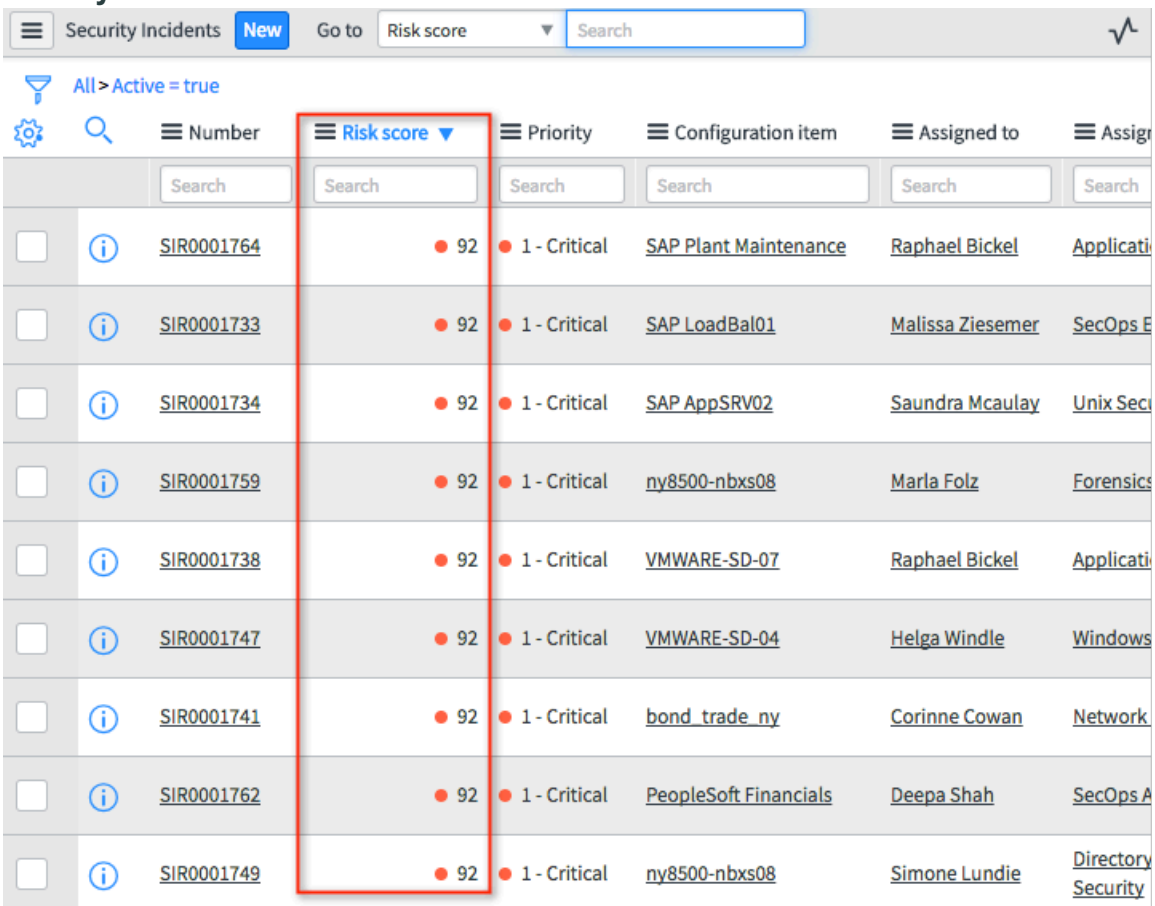
- Schweregrad berechnen
- Aktualisieren Sie die Risikopunktzahl
- SI-Risikopunktzahl aktualisieren

Hinweis:
Der im Basissystem verfügbare Risikorechner hängt von Ihrer Security Operations-Preisstufe ab.

Wenn Sie sich eine Liste von Security Incidents im Basissystem ansehen, beachten Sie die Spalte **Risikopunktzahl**.

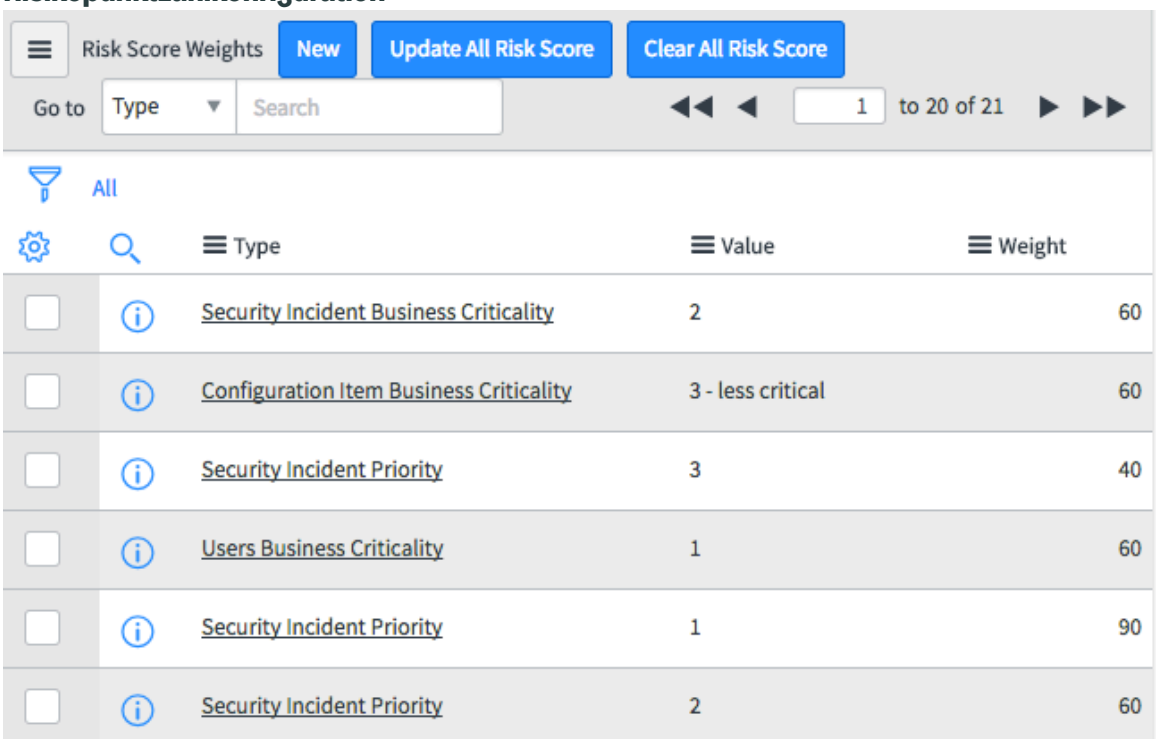
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incidents



Die Risikopunktzahl wird mit Gewichtungen berechnet, die in **der Konfiguration der Risikopunktzahl**definiert sind.

Risikopunktzahlkonfiguration



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn beispielsweise für einen Security Incident die **Geschäftsauswirkung** auf **2 Hoch** und die **Priorität** auf **3 – Mittel**festgelegt ist, werden die entsprechenden Gewichtungen in der Tabelle Risikopunktzahlgewichtungen wie folgt gesucht und berechnet:

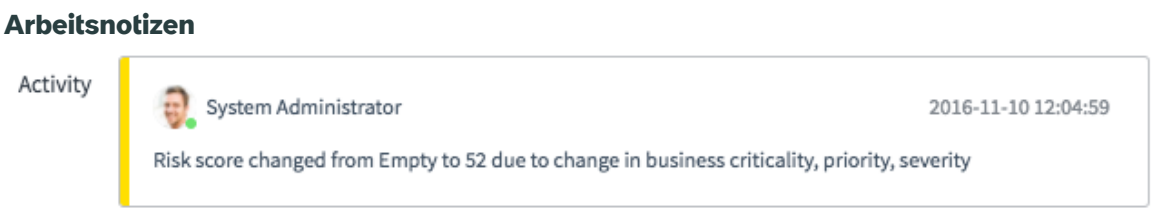
Security Incident – Geschäftsauswirkung mit einem Wert von 2 = einer Gewichtung von 60.

Security Incident-Priorität mit einem Wert von 3 = einer Gewichtung von 40.

(60 + 40)/2 = Risikopunktzahl 50.

Die Position des Security Incidents in der Liste der Security Incidents wird dann auf Grundlage der aktualisierten Risikopunktzahl neu geordnet.

Wenn im obigen Beispiel die **Geschäftsauswirkung** oder **die Priorität** des Security Incidents geändert werden, wird die Risikopunktzahl neu berechnet, und die Änderungen werden in den Arbeitsnotizen berücksichtigt.



Die Arbeitsnotizen werden aktualisiert, wenn die folgenden Felder geändert werden (wodurch die Risikopunktzahl aktualisiert wird):

- **Geschäftsauswirkung** auf dem Formular „Security Incident“.
- **Priorität** im Formular „Security Incident“.
- **Schweregrad** im Formular „Security Incident“ (standardmäßig ausgeblendet)
- **Geschäftsauswirkung** auf die zugehörige Liste **„Betroffene Benutzer“.**
- **Geschäftsauswirkung** auf die zugehörige Liste **„Betroffene Services“.**
- **Geschäftsauswirkung** auf Schwachstellen in der zugehörigen Liste **„Angreifbare Elemente“.**

Darüber hinaus werden die Arbeitsnotizen in den folgenden Situationen aktualisiert:

- Wenn eine Zuordnung zwischen betroffenen Benutzern und einem Security Incident erstellt oder geändert wird
- Wenn eine Zuordnung zwischen betroffenen Services und einem Security Incident erstellt oder geändert wird
- Wenn eine Zuordnung zwischen angreifbaren Elementen und einem Security Incident erstellt oder geändert wird

Arbeitsnotizen werden auch aktualisiert, wenn im Formular „Gewichtungen der Risikopunktzahl“ auf **Alle Risikopunktzahlen aktualisieren** und **Alle Risikopunktzahlen löschen** geklickt wird.

Gewichtungen der Risikopunktzahl verwalten

Die Gewichtungen der Risikopunktzahl, die zur Berechnung der Risikopunktzahlen in Security Incidents verwendet werden, können einzeln entfernt oder aktualisiert werden. Sie können auch für alle Security Incidents entfernt oder aktualisiert werden. Die Möglichkeit, sie aus Security Incidents zu entfernen, ist beim Ändern der Gewichtungswerte nützlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Hinweis:
Benutzer mit der Rolle sn_si.read können die Konfiguration der Risikopunktzahl in Security Incident Responseanzeigen.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Konfiguration der Risikopunktzahl**.

   Hinweis:
   Benutzer mit der Rolle sn_si.read können die Konfiguration der Risikopunktzahl anzeigen, indem sie zu navigieren **Security Incident** > **Warnungen und Ereignisse** > **Risikopunktzahlkonfiguration**.

2. Um eine neue Gewichtung der Risikopunktzahl hinzuzufügen, klicken Sie auf **Neu**, und geben Sie Informationen in die Felder ein.

Feld	Beschreibung
Typ	Wählen Sie den Typ der Risikopunktzahl aus, die Sie definieren.
Wert	Geben Sie den Wert an, der dem ausgewählten Typ zugeordnet ist. Wenn für den Typ mehrere Werte verfügbar sind, können Sie mehrere Datensätze für die Gewichtung der Risikopunktzahl definieren. Beispiel: Security Incident-Priorität mit einem Wert von 1, Security Incident-Priorität mit einem Wert von 2 usw.
Gewichtung	Die Gewichtung, die dem ausgewählten Typ-Wert-Paar zugeordnet ist. Gültige Einträge liegen zwischen 0 und 100, wobei 0 für die niedrigste und 100 für die höchste Gewichtung steht.

3. Klicken Sie auf **Absenden**.
4. Führen Sie bei Bedarf einen dieser Schritte aus.
   - Um einen Risikopunktzahl-Gewichtungsdatensatz zu löschen, öffnen Sie ihn in der Liste und klicken Sie auf **Löschen**.
   - Um alle Risikopunktzahl-Gewichtungsdatensätze zu löschen, klicken Sie auf **Alle Risikopunktzahlen löschen**.
   - Um alle Risikopunktzahl-Gewichtungsdatensätze zu aktualisieren, klicken Sie auf **Alle Risikopunktzahlen aktualisieren**.

Erstellen Sie ein Security Incident Response -SLA

Sie können eine Servicelevel-Vereinbarung (Service Level Agreement, SLA) für Security Incident Responsedefinieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **SLAs**.
2. Klicken Sie auf **Neu**.
   Feldbeschreibungen und detaillierte Anweisungen finden Sie unter Create an SLA definition .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-SLAs reparieren

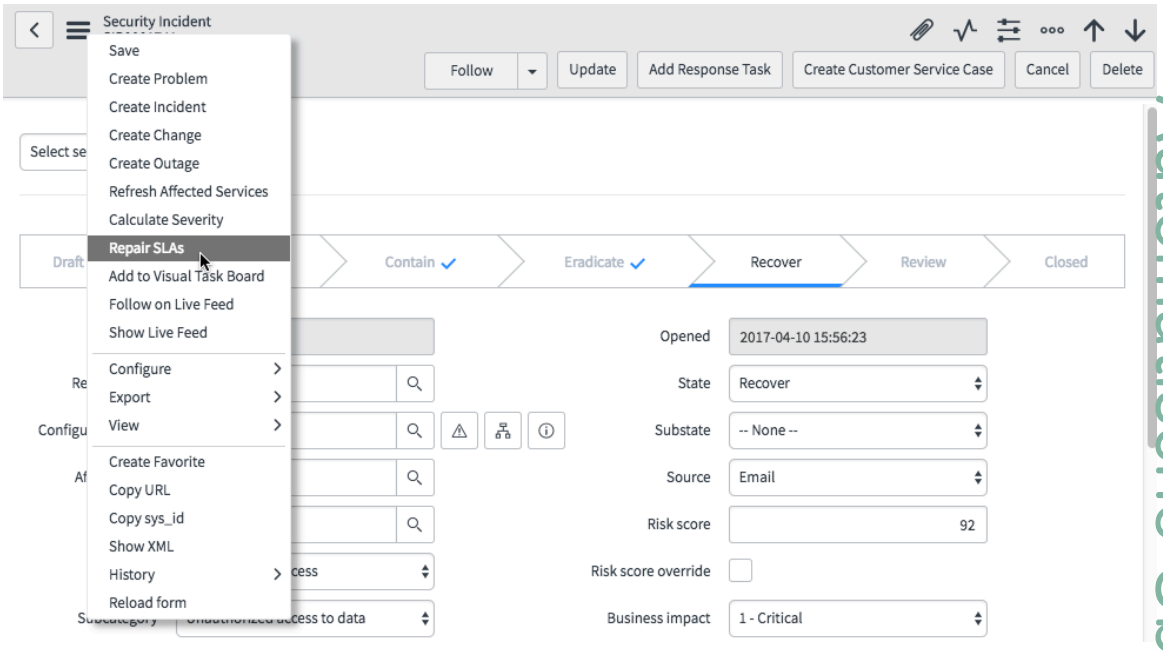
Sie können SLA-Datensätze reparieren, um sicherzustellen, dass die Informationen zu SLA-Timing und -Dauer korrekt sind.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie SLAs reparieren möchten.
2. Klicken Sie auf das Kontextmenü des Formular-Headers, und wählen Sie **SLAs neu berechnen**aus:



3. Klicken Sie im Bestätigungsfeld Warnung **auf OK**.
   Weitere Informationen finden Sie unter SLAs neu berechnen .

Erstellt ein Security Incident Response-Runbook

Ein Runbook ist eine Zuordnung zwischen einem veröffentlichten Wissensartikel und einer bestimmten Aufgabe. Während Sie die Aufgabe ausführen, wird automatisch ein Wissensartikel im Runbook geöffnet, der Informationen enthält, die für die Aufgabe relevant sind.

Vorbereitungen

In der Security Incident Response Runbook-Knowledge Base müssen Wissensartikel vorhanden sein. Wenn Sie einen Wissensartikel zu einem Security Incident erstellen, müssen Sie im Feld **Knowledge Base** unbedingt **Security Incident Response-Runbook** auswählen. Nachdem Sie den Artikel veröffentlicht haben, können Sie auf die Schaltfläche **Runbook erstellen** klicken.

Erforderliche Rolle: sn.si.knowledge_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Runbooks während der Erstellung von Security Incidents oder Antwortaufgaben verwenden oder die Knowledge Base-Artikel in einem Runbook Aufgaben im Playbook zuordnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Manuelles Runbook** > **Neues Runbook erstellen**.
2. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Wissensartikel	Wählen Sie einen Wissensartikel aus, der in das Runbook aufgenommen werden soll.
Aktiv	Aktivieren Sie das Kontrollkästchen, um das Runbook im **Filternavigator**verfügbar zu machen.
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine vordefinierte Filtergruppe zu verwenden oder eine neue Filtergruppe zu erstellen, um die Runbook-Kriterien zu definieren.
Filtergruppe	Wählen Sie die Filtergruppe aus, die zum Definieren eines Runbooks verwendet werden soll. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Filtergruppen verwenden** aktiviert ist.
Tabelle	Wählen Sie entweder „Security Incident“ [sn_si_incident] oder Security Incident Response „ Aufgabe [sn_si_task] aus. Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert und eine Filtergruppe ausgewählt haben, wird in diesem Feld standardmäßig die Tabelle verwendet, die der ausgewählten Filtergruppe zugeordnet ist.
Bedingung	Legen Sie die Bedingungen fest, die dieses Runbook mit dem Incident oder der Aufgabe verbinden. Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** und eine Filtergruppe ausgewählt haben, werden die Felder **Bedingung** nicht angezeigt.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Es werden die Registerkarte Details zu Wissensartikeln und eine Reihe von Schaltflächen angezeigt.
4. Um die Details des Runbooks anzuzeigen, klicken Sie auf die Registerkarte **Knowledge Base-Details**.
5. Um den Wissensartikel so anzuzeigen, wie er dem Benutzer angezeigt wird, klicken Sie auf **Artikel anzeigen**.
6. An Um die Details des Wissensartikels zu bearbeiten , klicken Sie auf **Artikel bearbeiten**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Regeln, um von Anwendern gemeldete Phishing-Angriffe zu validieren

Wenn Ihre Mitarbeiter E-Mails erhalten, die wie Phishing-Angriffe aussehen, können sie Ihnen diese mit einer Phishing-E-Mail-Adresse melden. Die verdächtige E-Mail wird anhand von von Ihrer Organisation definierten Regeln validiert.

Vorbereitungen
Bevor E-Mail-Abgleichregeln zur Identifizierung potenzieller Phishing-Angriffe verwendet werden können, definieren Sie eine E-Mail-Adresse, an die von Ihren Mitarbeitern weitergeleitete E-Mails zur Verarbeitung gesendet werden. Sie haben die folgenden Möglichkeiten, diese E-Mail-Adresse zu definieren (vorausgesetzt, die E-Mail-Domäne Ihres Unternehmens lautet acme.com):

- Definieren Sie eine E-Mail-Adresse wie **acme+phishing@service-now.com**. Das Tag **+phishing** wird von SMTP unterstützt, um die Filterung zu aktivieren, und Ihre -Instanz kann an sie gesendete E-Mails empfangen.
- Definieren Sie eine E-Mail-Adresse, z. B. **phishing@acme.com** (Ihr Exchange-Postfach), die sie wiederum an **acme+phishing@service-now.com** (Ihr Instanzpostfach, das durch eine E-Mail-Weiterleitungsregel definiert wird) weiterleitet.

Erforderliche Rolle: sn_sec_cmn.write

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Mitarbeiter auf eine verdächtige E-Mail stößt, sollte er diese als Anhang an Ihre Phishing-E-Mail-Adresse weiterleiten. Wenn die angehängte E-Mail mit einer Regel übereinstimmt, die eine Bedrohung definiert, wird ein Security Incident erstellt.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Vom Anwender gemeldetes Phishing**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder nach Bedarf aus.

Formular „E-Mail-Übereinstimmungsregeln“.

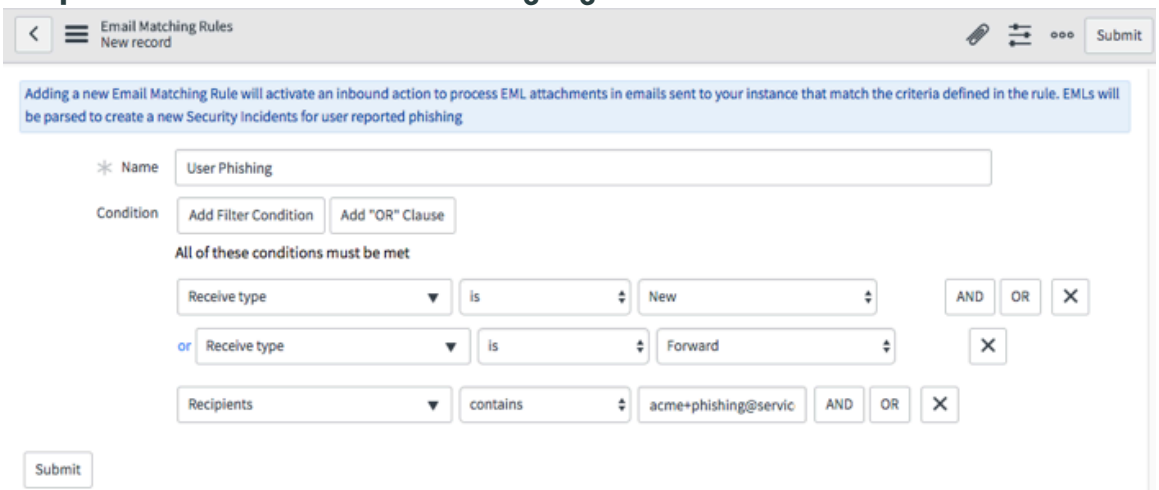
Feld	Beschreibung
Name	Name für diese E-Mail-Übereinstimmungsregel. Beispiel: Vom Anwender gemeldetes Phishing.
Bedingungen	Verwenden Sie den Mit dem Bedingungsgenerator können Sie überprüfen, ob eine E-Mail, die an die Phishing-E-Mail-Adresse Ihres Unternehmens gesendet wird, einen Phishing-Angriff darstellt. Siehe folgendes Beispiel.

4. Klicken Sie auf **Absenden**.

Example:
Dieses Beispiel zeigt eine Übereinstimmungsregel für die Verarbeitung von von Benutzern gemeldetem Phishing.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine E-Mail-Übereinstimmungsregel



Konfigurieren Sie die Eigenschaften Security Analyst Workspace

Konfigurieren Sie die Anwenderoberfläche des Incident-Datensatzes in Security Analyst Workspace, um die Felder anzugeben, die Sie anzeigen möchten.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Geben Sie die Felder an, die in Ihrem Incident-Datensatz angezeigt werden sollen, und geben Sie die Reihenfolge an, in der die Felder im Formular „Security Incident“ und im Formular „Antwortaufgabe“ angezeigt werden sollen. Sie können auch einen Grenzwert für die Anzahl der Felder festlegen, die angezeigt werden sollen.

Hinweis:

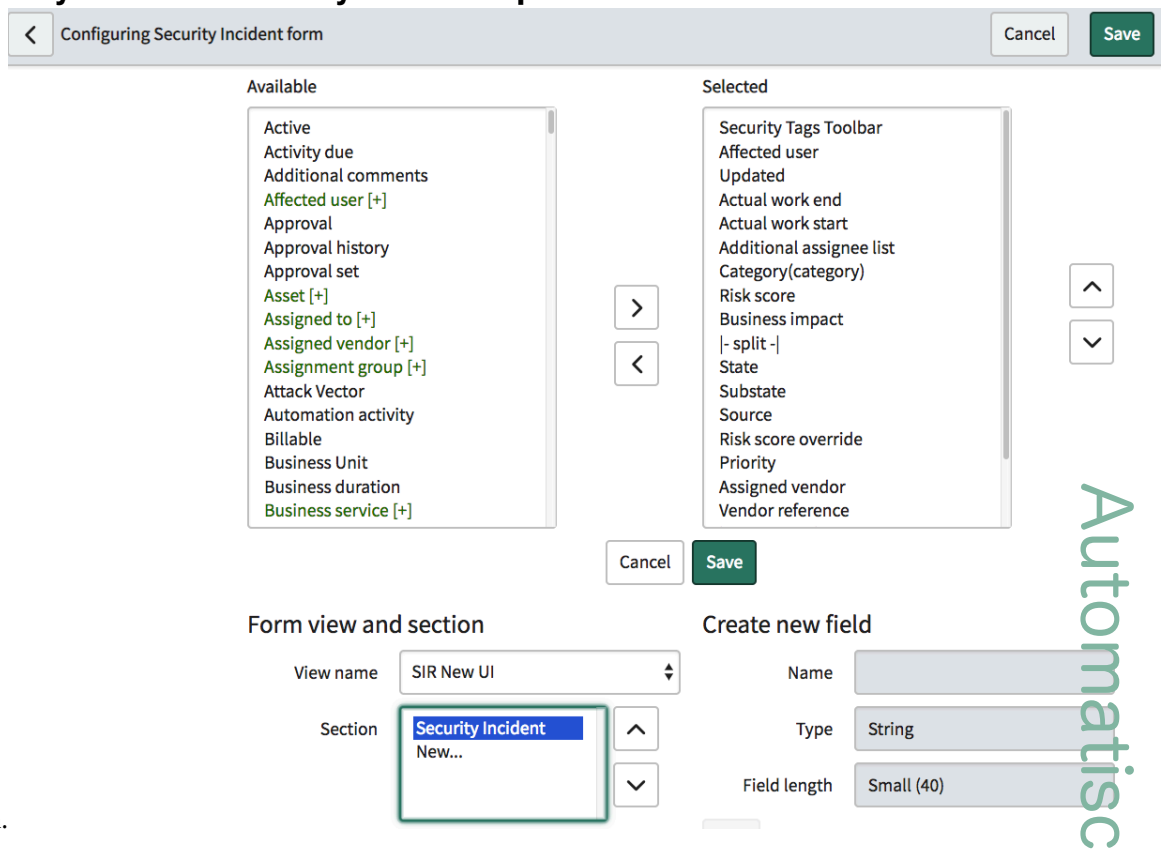
Sie können Regeln erstellen, um zu bestimmen, welche Ansicht für ein bestimmtes Formular verwendet werden soll. Das Basissystem enthält mehrere Ansichten, einschließlich der Ansichten Standard und Neue UI für SIR. Mehrere Ansichtsregeln sind ebenfalls im Lieferumfang des Basissystems enthalten, einschließlich der Regel Alle anderen Antwortaufgaben. Diese Regel erzwingt die Ansicht Standard im Antwortaufgabenformular, wenn die in der Ansichtsregel angegebene Bedingung erfüllt ist. Security Analyst Workspace verwendet die Ansicht „Neue SIR-UI“. Wenn die in Security Analyst Workspace angezeigten Formularfelder nicht mit den Formularfeldern in der klassischen Umgebung übereinstimmen, wird höchstwahrscheinlich eine Ansichtsregel erzwungen. Um die Ansicht **„Neue SIR-UI“** für das Formular zu verwenden, müssen Sie die Ansichtsregel deaktivieren. Details finden Sie unter Steuern, wenn das System eine Ansicht anzeigt .

Prozedur

1. Navigieren Sie zu einer beliebigen Liste der Security Incidents (z. B. **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**) an.
2. Klicken Sie auf einen Security Incident-Link, um den Security Incident-Datensatz zu öffnen.
3. Um zur Formularseite „Security Incident konfigurieren“ zu navigieren, klicken Sie auf das ☰ -Symbol, und wählen Sie **Konfigurieren** > **Formularlayout**.
4. Wählen Sie in der Liste **der Ansichtsnamendie Option SIR – Neue UI**aus.
5. Wählen Sie im Feld **Abschnitt** den entsprechenden Abschnitt aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies kann **Security Incident** oder **Security Incident Response-**



Aufgabesein.

6. Wählen Sie die Felder und die Reihenfolge aus, in der sie im Incident-Banner in der neuen Anwenderoberfläche angezeigt werden sollen.
7. Klicken Sie auf **Speichern**.

Hinweis:

- Bestimmte Felder werden in den Incident- und Antwortaufgaben-Bannern standardmäßig ausgeblendet. Ändern Sie die Felder, die ausgeblendet oder angezeigt werden, indem Sie die Eigenschaften `sn_app_secops_ui.form.excluded_fields.incident` und `sn_app_secops_ui.form.excluded_fields.response_task` ändern (siehe Eigenschaften des Security Analyst Workspace) .
- Geben Sie die Anzahl der Felder an, die in den Bannern für Incidents und Antwortaufgaben sowie in der ersten Zeile des Incident-Banners angezeigt werden können, indem Sie die folgenden Eigenschaften festlegen:
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

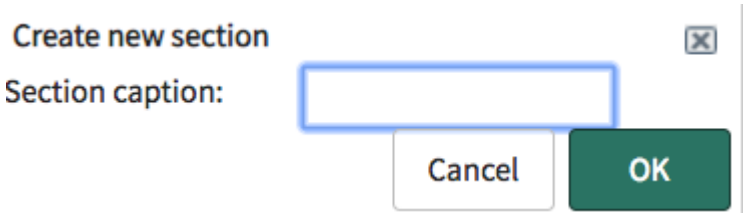
8. Um die Stile der gepunkteten Kreise zu konfigurieren, die neben einem Feldwert im Incident-Datensatz angezeigt werden, z. B. navigieren zu **System-UI** > **Feldstile** und ändern oder erstellen Sie einen neuen Stildatensatz für den spezifischen Tabellen- und Feldnamen.
   Die Eigenschaft „background-color“ im Feld Stil des Stildatensatzes bestimmt die Farbe des gepunkteten Kreises.
9. Klicken Sie auf, um das aktualisierte Incident-Banner anzuzeigen **Security Incidents** > **Incidents (neue UI)** um zum Incident-Datensatz in Security Analyst Workspace zu navigieren und die Seite zu aktualisieren, um das aktualisierte Incident-Banner anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Um das Banner für die Antwortaufgabe im Incident-Datensatz zu konfigurieren, navigieren Sie zu **Security Incidents** > **Antwortaufgaben** > **Alle Aufgaben anzeigen** und wiederholen Sie die Schritte.
11. Wenn Sie eine neue Aufgabentabelle als Erweiterung der Basistabelle „Security Incident Response-Aufgabe“ erstellen, müssen Sie der Tabelle auch die Ansicht „Neue SIR-UI“ hinzufügen.

    a. Wählen Sie in der Liste **„Name der Ansicht“Neu**aus.



    b. Geben Sie im Fenster Neue Ansicht erstellen **den Wert SIR New UI** (Groß-/Kleinschreibung beachten) ein, und klicken Sie auf **OK**.

Ergebnisse

Die Banner für Security Incidents und Reaktionsaufgaben werden unter Security Analyst Workspace (Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace) aktualisiert.

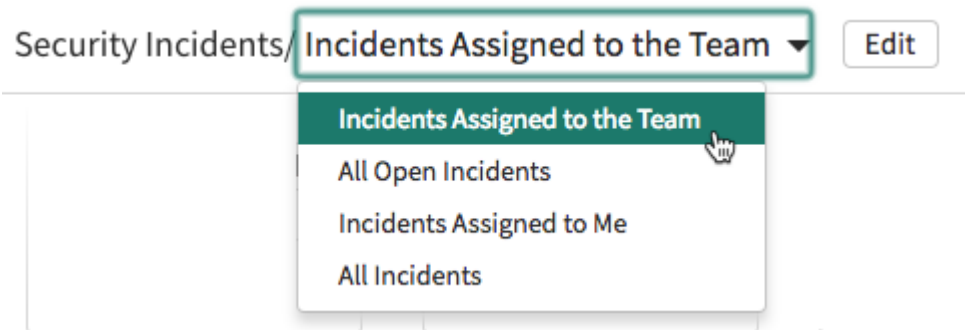
Richten Sie primäre und sekundäre Filter für ein Security Analyst Workspace

Das Basissystem Security Analyst Workspace enthält eine Reihe von primären Filtern zum Eingrenzen der Liste der zu analysierenden Security Incidents (für Ihnen zugewiesene Security Incidents, alle offenen Incidents usw.) sowie eine Reihe von Schnellfiltern (oder sekundären Filtern) zur Eingrenzung die Liste noch weiter erweitern (nach neuen Incidents, offenen Incidents, nur kritischen Incidents usw.).

Vorbereitungen

In der klassischen Umgebung können Sie zusätzliche primäre und sekundäre Filter definieren.

Bei der Definition von Filtern, die in Security Analyst Workspaceverwendet werden sollen, können Sie Tags zuweisen, um anzugeben, ob sie als primäre oder sekundäre Filter verwendet werden können. Primäre Filter werden oben in der Liste der Security Incidents angezeigt.



Klicken Sie neben der Option Schnellfilter **auf Bearbeiten**, um sekundäre Filter (oder Schnellfilter) auszuwählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin oder sn_sec_cmn.write

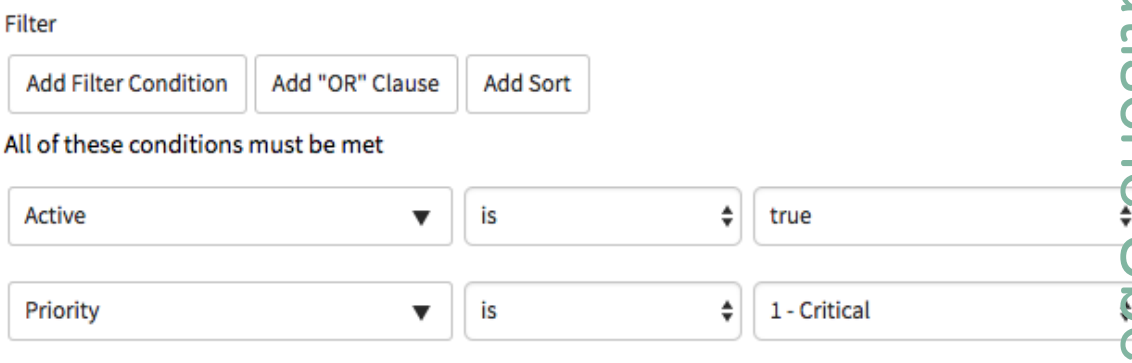
Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Filter**.
2. Klicken Sie auf **Neu**, und führen Sie die folgenden Schritte aus.

   a. Geben Sie einen **Titel**ein.

   b. Wählen Sie in der Auswahlliste **Tabelledie Option Security Incident [sn_si_incident]** aus.

   c. Fügen Sie Ihre Filterbedingungen hinzu.
   Beispielsweise verwendet der Filter **Offene Incidents mit Priorität = Kritisch** diese Bedingungen.



   d. Klicken Sie auf **Absenden**.

3. Wenn die Spalte **„Tags“** in der Filterliste nicht sichtbar ist, klicken Sie auf das Zahnradsymbol und personalisieren Sie die Ansicht, um sie hinzuzufügen.
4. Suchen Sie den von Ihnen erstellten Filter, und fügen Sie eines der folgenden Tags hinzu, um anzugeben, wie der Filter im Security Analyst Workspaceangezeigt werden soll.
   - **SN_SI_Primary**: Wenn dieses Tag ausgewählt ist, kann der Filter aus dem primären Filter-Slushbucket in Security Analyst Workspaceausgewählt werden.
   - **SN_SI_Primary_OOB**: Wenn dieses Tag ausgewählt ist, wird der Filter standardmäßig auf der Seite **„Ausgewählt“** des Slushbuckets des primären Filters angezeigt.
   - **SN_SI_Secondary**: Wenn dieses Tag ausgewählt ist, kann der Filter aus dem sekundären (Schnell-)Filter-Slushbucket ausgewählt werden.
   - **SN_SI_Secondary_OOB**: Wenn dieses Tag ausgewählt ist, wird der Filter standardmäßig auf der Seite **„Ausgewählt“** des Slushbuckets des primären Filters angezeigt.

Zugehörige Informationen

Erstellen und bearbeiten Sie Filter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Security Analyst Workspace

Diese Systemeigenschaften werden zum Konfigurieren des Arbeitsbereichs für Sicherheitsanalysten verwendet.

Es gibt zwei Arten von Eigenschaften:

- Eigenschaften, die normalerweise nicht geändert werden, wie sys_ids und Produktschlüssel.
- Eigenschaften, die nach Bedarf geändert werden, wie z. B. lange Abfrageintervalle und Konfigurationen der Anwenderoberfläche.

Hinweis:
Die Eigenschaften des Security Analyst Workspace befinden sich an folgender Stelle: **Security Incident** > **Setup von Analyst Workspace** > **Eigenschaften des Analystenarbeitsbereichs**.

Eigenschaften des Security Analyst Workspace

Eigenschaftsname	Beschreibung
Felder, die im Antwortaufgabenbanner standardmäßig ausgeblendet sind. sn_app_secops_ui.form.excluded_fields.response_task	• **Typ**: Zeichenfolge • **Standardwert**: ◦ Nummer ◦ Kurzbeschreibung ◦ Kommentare ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity
Felder, die im Incident-Banner standardmäßig ausgeblendet sind. sn_app_secops_ui.form.excluded_fields.incident	• **Typ**: Zeichenfolge • **Standardwert**: ◦ Nummer ◦ Kurzbeschreibung ◦ Kommentare ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity ◦ security_tags
Der Hintergrundfarbstil wird auf die hier aufgeführten Felder angewendet.	• **Typ**: Zeichenfolge • **Standardwert**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Security Analyst Workspace (Fortsetzung)

Eigenschaftsname	Beschreibung
sn_app_secops_ui.form.color_coded_fields	○ Geschäftsrelevanz ○ impact ○ Priorität ○ risk_score ○ Schweregrad
Bei „wahr“ haben Tabellen, die aus der Basis-Antwortaufgabentabelle „sn_si_task“ erweitert wurden, auch Zugriff auf E-Mail-Vorlagen, die für die Basis-Antwortaufgabentabelle erstellt wurden. sn_app_secops_ui.extend.base.response_task.email_templates	• **Typ**: true | false • **Standardwert**: true
Legt die Breite jedes Zusammenfassungsfelds in jedem Antwortaufgabenbanner fest. sn_app_secops_ui.task_summary.single_summary.width.response_task	• **Typ**: Ganzzahl • **Standardwert**: 10
Legt die Breite jedes Zusammenfassungsfelds in jedem Incident-Banner fest. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Typ**: Ganzzahl • **Standardwert**: 15
Legt einen Grenzwert für die Anzahl der im Incident-Banner zulässigen Zusammenfassungsfelder fest. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Typ**: Ganzzahl • **Standardwert**: 12
Legt einen Grenzwert für die Anzahl der Zusammenfassungsfelder fest, die im Antwortaufgabenbanner zulässig sind. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• **Typ**: Ganzzahl • **Standardwert**: 12
Legt einen Grenzwert für die Anzahl der Zusammenfassungsfelder fest, die in der ersten Zeile des Incident-Banners zulässig sind. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Typ**: Ganzzahl • **Standardwert**: 3

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Security Analyst Workspace (Fortsetzung)

Eigenschaftsname	Beschreibung
Kommagetrennte Liste von Feldern, die Anwenderfotos enthalten können. sn_app_secops_ui.form.user_fields	• **Typ**: Zeichenfolge • **Standardwert**: ◦ impacted_user ◦ caller ◦ sys_updated_by ◦ sys_created_by ◦ opened_by ◦ closed_by ◦ Übermittelt_von
Legt die Breite jedes Zusammenfassungsfelds in jeder Incident-Vorschauansicht fest. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Typ**: Ganzzahl • **Standardwert**: 13,5
Kommagetrennte Liste von Feldern, die die Zeit anzeigen. sn_app_secops_ui.form.time_fields	• **Typ**: Zeichenfolge • **Standardwert**: ◦ opened_at ◦ sys_created_on ◦ sys_updated_on
Steuert die Häufigkeit (in Millisekunden), mit der die Ergebnisse der Sichtungssuche aktualisiert werden. sn_app_secops_ui.poller_interval.search_action	• **Typ**: Ganzzahl • **Standardwert**: 30.000 **Mindestens**15.000
Steuert die Häufigkeit (in Millisekunden), mit der die Anzahl oder Abfragedaten aktualisiert werden. sn_app_secops_ui.poller_interval.related_list	• **Typ**: Ganzzahl • **Standardwert**: 30.000 **Mindestens**15.000
Steuert die Häufigkeit (in Millisekunden), mit der die Ergebnisdaten aktualisiert werden (für das Playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Typ**: Ganzzahl • **Standardwert**: 30.000 **Mindestens**15.000

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Security Analyst Workspace (Fortsetzung)

Eigenschaftsname	Beschreibung
ID für den Workflow „Security Operations Integration – Host isolieren“. sn_app_secops_ui.workflow.id.isolate_host	• **Typ**: Zeichenfolge • **Standardwert**: d72041f1ff203200c68c84648e94fa5e
ID für den Workflow „Security Operations Integration – Beobachtungsliste“. sn_app_secops_ui.workflow.id.publish_to_watchlist	• **Typ**: Zeichenfolge • **Standardwert**: 35800c0eff343200c68c84648e94fa85
ID für den Workflow „Security Operations Integration – Anforderung blockieren“. sn_app_secops_ui.workflow.id.block_request	• **Typ**: Zeichenfolge • **Standardwert**: 11a6a5270b9032008f9108e3c5673a24
ID für die Anwenderrolle „sn_si_analyst“. sn_app_secops_ui.roles.id.sn_si.write	• **Typ**: Zeichenfolge • **Standardwert**: 66878663ff123100158bffffffffff8d
ID für die Anwenderrolle sn_si_read. sn_app_secops_ui.roles.id.sn_si.read	• **Typ**: Zeichenfolge • **Standardwert**: ae878663ff123100158bffffffffff8e
ID für die Anwenderrolle „sn_si_admin“. sn_app_secops_ui.roles.id.sn_si.admin	• **Typ**: Zeichenfolge • **Standardwert**: 22878663ff123100158bffffffffff8d
ID für den Workflow „Microsoft Exchange – E-Mail-Suche und -Löschung durchführen“. sn_app_secops_ui.email.phishing.manual.workflow	• **Typ**: Zeichenfolge • **Standardwert**: ed9f289cc310220031fbdccdf3d3aeb4
ID für die anwenderdefinierte Aktion Zur Deny-Liste hinzufügen auf der Registerkarte „Untersuchen“ in Security Analyst Workspace. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Typ**: Zeichenfolge • **Standardwert**: DENY_e9bd0ac50b632200263a089b37673a0b
ID für die anwenderdefinierte Aktion „Zur Allow-Liste hinzufügen“ auf der Registerkarte „Untersuchen“ in der Security Analyst Workspace	• **Typ**: Zeichenfolge • **Standardwert**: ALLOWLIST_e9bd0ac50b632200263a089b37673a0b

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Security Analyst Workspace (Fortsetzung)

Eigenschaftsname	Beschreibung
sn_app_secops_ui.explore.action.direct.id.allow_list	
ID für die UI-Aktion „Bedrohungssuche ausführen“. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Typ**: Zeichenfolge • **Standardwert**: da5ff4420b540300263a089b37673ae7
ID für die Integrationsfunktionalität der Bedrohungssuche. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Typ**: Zeichenfolge • **Standardwert**: 39344d4f0b273200263a089b37673ab1
ID für die anwenderdefinierte Aktion „Anreicherung erkennbarer Elemente“ auf der Registerkarte „Untersuchen“ in Security Analyst Workspace. sn_app_secops_ui.explore.action.id.observable_enrichment	• **Typ**: Zeichenfolge • **Standardwert**: OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673
ID für die Fähigkeit „Erkennbares Element anreichern“. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Typ**: Zeichenfolge • **Standardwert**: 9ad183640b1003009f66e94685673af4
ID für die UI-Aktion „In Beobachtungsliste veröffentlichen“. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• **Typ**: Zeichenfolge • **Standardwert**: 8ee94002ff743200c68c84648e94faf9
ID für die UI-Aktion „Sperranforderung“. sn_app_secops_ui.explore.action.id.block_request	• **Typ**: Zeichenfolge • **Standardwert**: 7158f6e40b2032008f9108e3c5673adf
ID für die UI-Aktion „Sichtungssuche ausführen“. sn_app_secops_ui.explore.action.id.sightings_search	• **Typ**: Zeichenfolge • **Standardwert**: 43f91a6f0b032200b97c67d985673a2c
ID für die UI-Aktion „Untergeordneten Security Incident erstellen“. sn_app_secops_ui.explore.action.id.create_child_incident	• **Typ**: Zeichenfolge • **Standardwert**: 5a6882645363530099d5ddeeff7b1272

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Security Analyst Workspace (Fortsetzung)

Eigenschaftsname	Beschreibung
ID für die UI-Aktion „Sicherheitsanmerkung hinzufügen“. sn_app_secops_ui.explore.action.id.add_security_annotation	• **Typ**: Zeichenfolge • **Standardwert**: 1e3a3e723b5332005a9149a4d2efc4eb
ID für die anwenderdefinierte CI-Ergänzungsaktion auf der Registerkarte „Untersuchen“ in Security Analyst Workspace. sn_app_secops_ui.explore.action.id.ci_enrichment	• **Typ**: Zeichenfolge • **Standardwert**: CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1
ID für die UI-Aktion „Host isolieren“. sn_app_secops_ui.explore.action.id.isolate_host	• **Typ**: Zeichenfolge • **Standardwert**: d6244e0aff203200c68c84648e94fad3
ID für die UI-Aktion „Mehrere erkennbare Elemente hinzufügen“. sn_app_secops_ui.explore.action.id.multiple_observable	• **Typ**: Zeichenfolge • **Standardwert**: 138de478d78322007a6de294de6103aa
Produktschlüssel für ag-Grid-Enterprise. sn_app_secops_ui.ag-grid-license	• **Typ**: Zeichenfolge • **Standardwert**: ServiceNow_ServiceNow_5Devs2_August_2018_MTUzM

Zusätzliche Konfiguration des Security Analyst Workspace

Konfigurieren Sie Security Analyst Workspace, und definieren Sie Filter, UI-Aktionen und zugehörige Listen.

- Konfiguration des Zielseitenfilters
- UI-Aktionen aktivieren
- Formular-UI-Aktionen
- Konfiguration der zugehörigen Liste
- UI-Aktionen für zugehörige Liste
- Systemeigenschaften für Formularkonfigurationen
- Aktivieren Sie Playbooks für die Analystenauswahl

Konfiguration des Zielseitenfilters

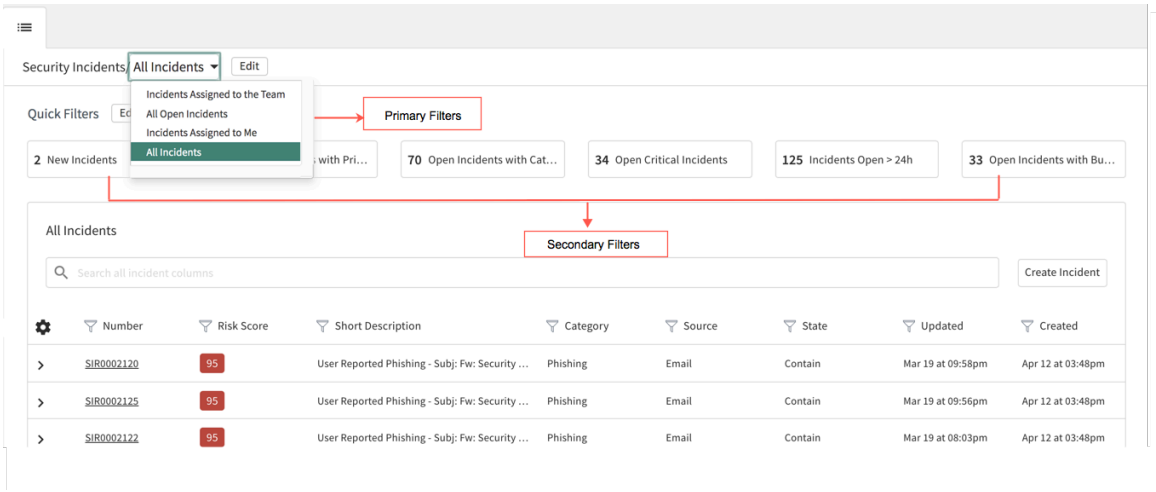
Sie können neue Filter hinzufügen oder vorhandene Filter ändern, die in Security Analyst Workspaceangezeigt werden.

Security Analyst Workspace verfügt über primäre und sekundäre Filter, mit denen Sie die Liste der Security Incidents filtern können, um die zu analysierenden Security Incidents schnell zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden. Weitere Informationen finden Sie unter Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace.



Erstellen Sie einen neuen Filter

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **Konfiguration der Zielseitenfilter**.
2. Klicken Sie auf **Neu**.
3. Geben Sie einen Titel für den Filter ein, legen Sie die Filterbedingung fest, und klicken Sie auf **Absenden**, um zur vorherigen Seite zurückzukehren.

   Der neu hinzugefügte Filter wird auf der Seite aufgelistet.
4. Fügen Sie ein Tag für diesen Filter hinzu, um anzugeben, ob dies ein primärer oder sekundärer Filter ist. Die folgenden Tags sind verfügbar:
   - SN_SI_Primär
   - SN_SI_Secondary

Bearbeiten Sie vorhandene Filter

Sie können auch Folgendes tun:

- Zum Ändern vorhandener Filter klicken Sie auf den Titel eines vorhandenen Filters. Ändern Sie den Titel und die Filterbedingung, und klicken Sie auf **Aktualisieren**.
- Tags ändern: Wählen Sie einen Filter aus, und klicken Sie auf die Spalte Tag in der Konfiguration des Zielseitenfilters. Sie können das vorhandene Tag löschen oder ein neues Tag für den Filter hinzufügen.

UI-Aktionen aktivieren

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind.

Hinweis:
Um die UI-Aktionen zu ändern, melden Sie sich als Benutzer mit den folgenden Rollen an:

- ui_action_admin
- ui_page_admin
- web_service_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt zwei Arten von UI-Aktionen, die für Security Analyst Workspacekonfiguriert werden können:

- Dialogbasierte UI-Aktion
- Serverseitige UI-Aktion

Dialogbasierte UI-Aktion

Um Dialogfeld-basierte UI-Aktionen in Security Analyst Workspacezu aktivieren, nehmen Sie die folgenden Änderungen an den UI-Seiten vor, die den entsprechenden Standard-UI-Aktionen zugeordnet sind.

1. **HTML-Abschnitt**: Ändern Sie den HTML-Abschnitt so, dass er das *`Reaktionseingabe`* -Tag enthält. Der Tag-Wert *`der Reaktionseingabe`* wird im Client-Skriptabschnitt verwendet, um zu ermitteln, ob die UI-Seite über Security Analyst Workspacegestartet wurde. Ein Beispiel ist unten dargestellt:

   ```
   <input id="react" name="react" type="hidden"
   value="${JS,HTML:sysparm_react}" />
   ```

2. **Client-Skript**: Zusätzliche Logik muss in das Client-Skript geschrieben werden, wenn die *`Reaktionskennzeichnung`* „wahr“ ist. Dies ist erforderlich, um die Schaltflächenereignisse **„Absenden“** und **„Abbrechen“** zu verarbeiten, die als Teil des Dialogfelds angezeigt werden.

   a. Der Ereignishandler für onCancel () muss das Ereignis „SIR_WORKBENCH_POPUP_CANCEL“ von senden Security Analyst Workspace

   b. Der Ereignishandler für onSubmit () muss das Ereignis „SIR_WORKCH_POPUP_SUBMIT“ von senden Security Analyst Workspace

3. Die Ausführung des Verarbeitungsskripts wird im Kontext Security Analyst Workspace übersprungen, da die Aktion „onSubmit“ so geändert wurde, dass „falsch“ zurückgegeben wird, wenn der *`Reaktionseingabe`* -Tag-Wert „wahr“ ist. Die Logik des Verarbeitungsskripts muss entweder über ein vom Client aufrufbares Skript (aufgerufen über die GlideAjax-API) oder einen REST-Ressourcenendpunkt gehandhabt werden.

Weitere Informationen finden Sie auf den folgenden UI-Beispielseiten:

- Beispiel für UI-Aktion „Zugehörige Liste“: In Beobachtungsliste veröffentlichen (Name der UI-Seite: Publisher_to_watchlist)
- Beispiel für UI-Aktion Formular: Problem erstellen (UI-Seitenname: create_prb_change_inc)

Serverseitige UI-Aktion

Um serverseitige UI-Aktionen zu aktivieren, müssen Sie wie folgt vorgehen:

Die Logik des Standard-UI-Aktionsskripts muss als Teil einer geskripteten REST-Ressource behandelt werden.

Weitere Informationen finden Sie in den folgenden UI-Beispielaktionen für „Formular“:

- Ausfall erstellen
- Abbrechen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular-UI-Aktionen

Sie können die UI-Aktionen konfigurieren, die unter Security Analyst Workspaceangezeigt werden.

Voraussetzungen:

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren.

Um eine UI-Aktion „Formular“ für Security Analyst Workspacezu konfigurieren, gehen Sie wie folgt vor:

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **Formular-UI-Aktionen**.
2. Geben Sie die folgenden Details ein:

Feldname	Beschreibung
Aktion	Wählen Sie eine UI-Aktion aus der Auswahlliste aus.
Typ	Wählen Sie den Aktionstyp aus. Kann sein: ○ Dialogbasierte Aktion: Dieser Aktionstyp wird verwendet, wenn Benutzerinteraktionen oder -eingaben zum Ausführen einer bestimmten Geschäftslogik erforderlich sind. ○ Serverseitige Aktion: Diese Aktion führt die erforderliche Geschäftslogik ohne zusätzliche Benutzereingabe aus. **Hinweis:** Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren.
Anwendung	Der Name des Anwendungsbereichs (Security Incident Response UI), in dem die UI-Aktion hinzugefügt wird, wird hier angezeigt.
Dialogbasierte Aktion Wenn Sie Dialogbasierte Aktion im Feld Typ auswählen, geben Sie die folgenden Details ein:	
UI-Seite	Wählen Sie die UI-Seite aus, die der Aktion zugeordnet ist.
Dialogfeldtitel	Geben Sie einen Titel für die Dialogaktion ein.
Breite und Höhe des Dialogfelds	Geben Sie die Höhe und Breite des Dialogfelds in Pixel ein.
Skript	Für die ausgewählte UI-Seite können Sie hier zusätzliche Abfrageparameter angeben. Die mit dem Basissystem bereitgestellte Vorlage erstellt und gibt nur den Parameter „`sysparm_sys_id`“ zurück. Sie können dies überschreiben, indem Sie hier andere Parameter angeben.
Serverseitige Aktion	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

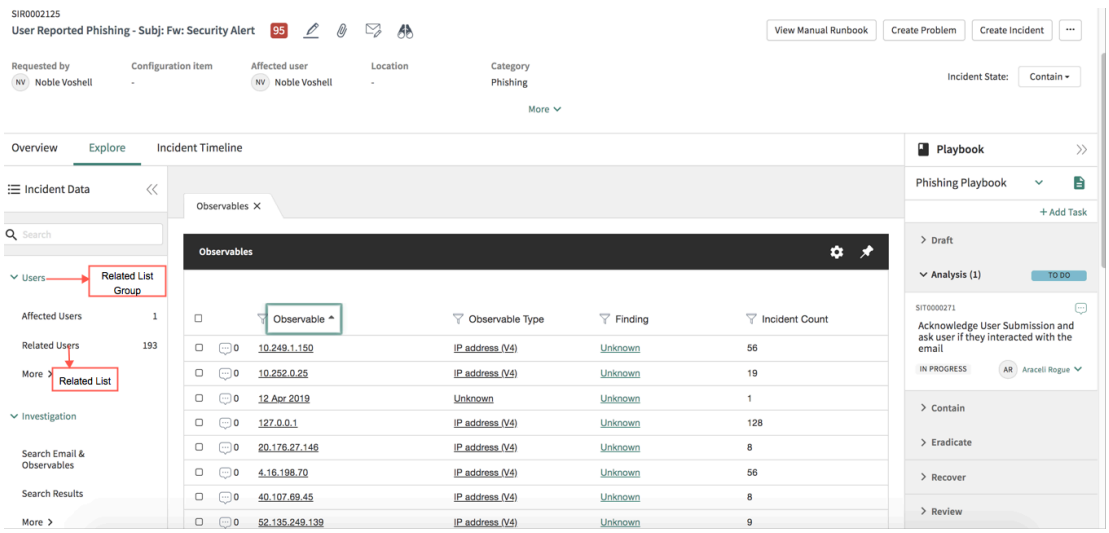
Feldname	Beschreibung
Wenn Sie Serverseitige Aktion im Feld Typ auswählen, geben Sie die folgenden Details ein:	
Geskriptete REST-Ressource	Wählen Sie die Scripted REST-Ressource aus, die die Aktion definiert. **Hinweis:** Die **SIR-UI-Analysten** -ACL muss der REST-Ressource hinzugefügt werden.

3. Klicken Sie auf **Absenden**.
4. Navigieren zu **Security Incidents** > **Incidents (neue UI)** Seite.
5. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Sie können die neue UI-Aktion oben auf der Seite sehen.

Klicken Sie zum Ändern einer vorhandenen Formular-UI-Aktion auf den Aktionsnamen, um zur Seite „Formular-UI-Aktionen“ zu navigieren. Sie können den Aktionsnamen, den Typ und die restlichen Felder basierend auf dem ausgewählten Typ ändern.

Konfiguration der zugehörigen Liste

Sie können neue zugehörige Listen oder neue zugehörige Listengruppen hinzufügen und vorhandene Gruppen oder zugehörige Listen ändern, die in Security Analyst Workspaceangezeigt werden.



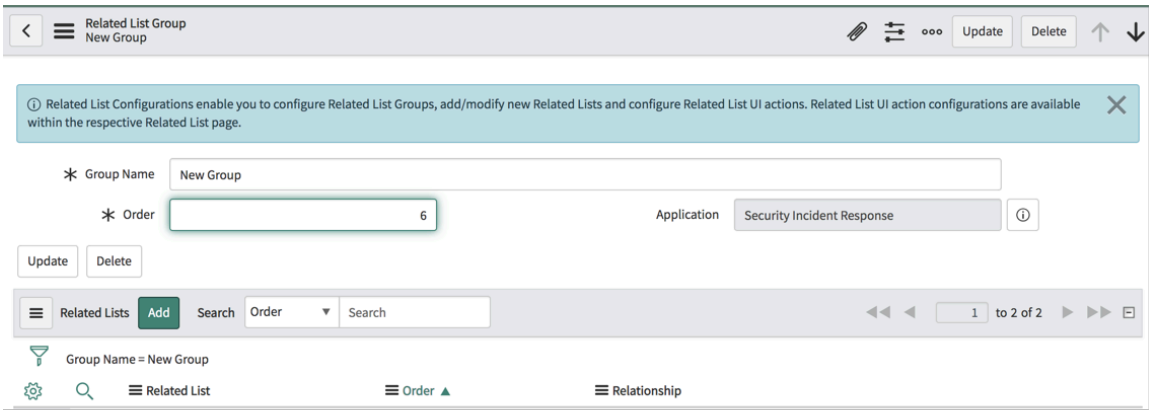
Fügen Sie eine zugehörige Listengruppe hinzu

Führen Sie die folgenden Schritte aus, um eine zugehörige Listengruppe hinzuzufügen:

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **Konfigurationen zugehöriger Listen**.
2. Klicken Sie auf **Neu**, um eine neue zugehörige Listengruppe hinzuzufügen. Geben Sie den Gruppennamen und die Reihenfolge ein, in der er auf der Seite Incidents (neue UI) angezeigt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Absenden**. Die neu hinzugefügte Gruppe wird auf der Seite „Zugehörige Listengruppen“ angezeigt.



Fügen Sie eine zugehörige Liste hinzu

Führen Sie die folgenden Schritte aus, um eine neue zugehörige Liste hinzuzufügen:

1. Klicken Sie auf den Link einer zugehörigen Listengruppe.
2. Klicken Sie im Abschnitt „Zugehörige Listen“ **auf Hinzufügen**, um eine neue zugehörige Liste hinzuzufügen.

   Wenn die Schaltfläche **„Hinzufügen“** nicht angezeigt wird, überprüfen Sie, ob Sie sich im selben Anwendungsbereich wie die zugehörige Listengruppe befinden.
3. Wählen Sie die zugehörige Liste aus, die in die Gruppe aufgenommen werden soll.

   Hinweis:
   Wenn eine bestimmte zugehörige Liste nicht angezeigt wird, gehen Sie wie folgt vor:

   a. Navigieren zu **System-UI** > **Zugehörige Listen** und suchen Sie nach zugehörigen Listen in der Tabelle `sn_si_incident`.

   b. Klicken Sie auf die Tabelle `sn_si_incident`, die der Ansicht **„Neue SIR-UI“**zugeordnet ist.

   c. Klicken Sie im Abschnitt „Zugehörige Listeneinträge“ auf **Neu**, um die zugehörige Liste der Ansicht **„Neue SIR-UI“** hinzuzufügen.
4. Geben Sie die Reihenfolge an, in der sie angezeigt werden sollen, und klicken Sie auf **Absenden**.

   Die von Ihnen hinzugefügte zugehörige Liste wird unter Security Analyst Workspaceangezeigt.

Um eine vorhandene zugehörige Listengruppe zu ändern, klicken Sie auf den Gruppennamen, um zur Seite „Zugehörige Listengruppe“ zu navigieren. Sie können den Gruppennamen und die Reihenfolge ändern und zugehörige Listen zur Gruppe hinzufügen oder daraus löschen.

UI-Aktionen für zugehörige Liste

Sie können den zugehörigen Listen unter Security Analyst Workspaceneue UI-Aktionen hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen:

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren.

Führen Sie die folgenden Schritte aus, um eine neue UI-Aktion „Zugehörige Liste“ hinzuzufügen:

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **Konfigurationen zugehöriger Listen**.
2. Klicken Sie auf den Gruppennamen. Die Konfigurationsseite „Zugehörige Listengruppe“ wird angezeigt.
3. Klicken Sie auf die zugehörige Liste, für die Sie eine UI-Aktion hinzufügen möchten.
4. Klicken Sie im Abschnitt „UI-Aktionen der zugehörigen Liste“ **auf Hinzufügen**.
5. Geben Sie die folgenden Details ein:

Feldname	Beschreibung
Aktion	Wählen Sie eine UI-Aktion aus der Auswahlliste aus.
Typ	Wählen Sie den Aktionstyp aus. Kann sein: ○ Dialogbasierte Aktion: Dieser Aktionstyp wird verwendet, wenn Benutzerinteraktionen oder -eingaben zum Ausführen einer bestimmten Geschäftslogik erforderlich sind. ○ Serverseitige Aktion: Diese Aktion führt die erforderliche Geschäftslogik ohne zusätzliche Benutzereingabe aus. **Hinweis:** Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren.
Anwendung	Der Name des Anwendungsbereichs (Security Incident Response UI), in dem die UI-Aktion hinzugefügt wird, wird hier angezeigt.
Dialogbasierte Aktion Wenn Sie Dialogbasierte Aktion im Feld Typ auswählen, geben Sie die folgenden Details ein:	
UI-Seite	Wählen Sie die UI-Seite aus, die der Aktion zugeordnet ist.
Dialogfeldtitel	Geben Sie einen Titel für die Dialogaktion ein.
Breite und Höhe des Dialogfelds	Geben Sie die Höhe und Breite des Dialogfelds in Pixel ein.
Skript	Für die ausgewählte UI-Seite können Sie hier zusätzliche Abfrageparameter angeben. Die mit dem Basissystem bereitgestellte Vorlage erstellt und gibt nur die Parameter `sysparm_incident_id`, `sysparm_record_table`und `sysparm_related_sys_ids` zurück. Sie können sie überschreiben, indem Sie hier andere Parameter angeben.
Serverseitige Aktion	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
Wenn Sie Serverseitige Aktion im Feld Typ auswählen, geben Sie Folgendes an:	
Geskriptete REST-Ressource	Wählen Sie die Scripted REST-Ressource aus, die die Aktion definiert. **Hinweis:** Die **SIR-UI-Analysten** -ACL muss der REST-Ressource hinzugefügt werden.

6. Klicken Sie auf **Absenden**.
7. Navigieren zu **Security Incidents** > **Incidents (neue UI)** Seite.
8. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Starten Sie die entsprechende zugehörige Liste, um die neue UI-Aktion anzuzeigen.

Systemeigenschaften für Formularkonfigurationen

Diese Systemeigenschaften definieren die Formularaktualisierungsintervalle für die Playbook-Aufgaben.

Um diese Eigenschaften zu konfigurieren, navigieren Sie zu **Setup von Analyst Workspace (neue UI)** > **Eigenschaften des Analystenarbeitsbereichs**.

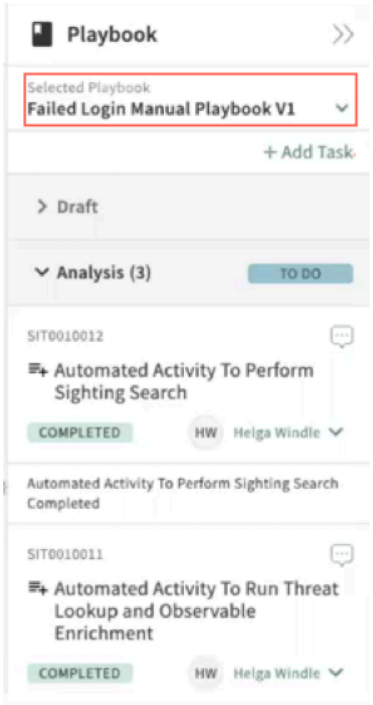
Eigenschaft	Standardwert	Beschreibung
sn_app_secops_ui.poller_interval.playbook_tasks	10000 ms	Die Intervallzeit, die von der Playbook-Komponente verwendet wird, um ihre Antwortaufgaben für jede konfigurierte Intervallzeit zu aktualisieren.
sn_app_secops_ui.poller_interval_count.playbook_tasks	9	Die Anzahl der Abfragen der Playbook-Komponente für Antwortaufgaben.
sn_app_secops_ui.poller_interval.related_lists	30000 ms	Diese Intervallzeit wird von der Komponente „Untersuchen“ verwendet, um die Anzahl der zugehörigen Listen für jede konfigurierte Intervallzeit zu aktualisieren.

Aktivieren Sie Playbooks für die Analystenauswahl

Fügen Sie der Playbook-Auswahlliste neue Playbooks hinzu.

Sie können ein geeignetes Playbook auswählen, um Security Incidents in Security Analyst Workspace (Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace) zu untersuchen. Die Playbook-Auswahloption unterstützt nur Playbooks, die mit Flow Designer entworfen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem Sie ein Playbook mit Flow Designer erstellt haben, gehen Sie wie folgt vor, um es in die Auswahlliste Selected Playbook (Ausgewähltes Playbook) aufzunehmen:

1. Navigieren Sie zur Tabelle *sys_hub_flow*.
2. Suchen Sie nach dem neuen, mit dem Flow Designer erstellten Playbook.
3. Fügen Sie den Playbooks, die Sie in die Auswahlliste Selected Playbook (Ausgewähltes Playbook) aufnehmen möchten, das Tag **sir_playbook** hinzu.

Hinweis:
Wenn Sie alte Playbooks haben, die nicht von Workflows zu Flow Designer migriert wurden, werden sie nicht in der Liste angezeigt. Wenn jedoch ein mit Workflows erstelltes Playbook einem Security Incident zugewiesen wird, entweder durch eine Auslöserbedingung oder durch manuelle Auswahl (mit der Option **Orchestration ausführen** in der klassischen Umgebung), wird dieses Playbook gestartet, wenn Sie den Security Incident in Security Analyst Workspaceöffnen.

Problembehandlung bei Security Incident Response

In diesem Abschnitt finden Sie wichtige Tipps zur Problembehandlung und häufig gestellte Fragen im Zusammenhang mit Security Incident Response.

Probleme mit Zugriffssteuerungsregeln

Zugriffssteuerungsregeln ermöglichen Zugriff auf die angegebene Ressource, wenn alle der folgenden drei Bedingungen erfüllt sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Anwender hat eine der in der **Rollenliste** angegebenen Rollen, oder die Liste ist leer.
- Die Bedingungen im Feld **Bedingung** ergeben bei Auswertung „wahr“, oder die Bedingungen sind leer.
- Das Skript im Feld **Skript** (erweitert) ergibt als „true“ ausgewertet oder legt die **Variablenantwort** auf „true“ fest oder ist leer.

Weitere Informationen zu Zugriffssteuerungsregeln finden Sie unter Exploring Access Control Lists.

Wichtig:
Wenn die Option **Administratorüberschreibungen** für eine Security Incident-Tabelle deaktiviert ist und der Administrator auf die Security Incident-Tabelle zugreifen kann, finden Sie weitere Informationen unter KB1444673.

Security Incident Response Platform Analytics-Lösungen

Platform Analytics-Lösungen enthalten vorkonfigurierte Dashboards. Die -Dashboards enthalten wichtige Metriken für die Analyse des Prozesses Security Incident Response, z. B. neue Security Incidents oder das durchschnittliche Alter offener Security Incidents.

Platform Analytics Datenvisualisierungen verwenden Performance Analytics *Indikatordaten*, um Daten im Zeitverlauf anzuzeigen, sodass Sie Ihre Geschäftsprozesse analysieren und Verbesserungsbereiche identifizieren können. Mit Platform Analytics-Lösungen können Sie mit einem minimalen Setup den Mehrwert von Performance Analytics für Ihre Anwendung nutzen. Sie können auch jederzeit eigene Objekte erstellen.

Wichtig:
Richten Sie Platform Analytics-Lösungen in einer Instanz außerhalb der Produktion ein, und testen Sie die Lösung, bevor Sie sie in der Produktion aktivieren.

Die Lösung Security Incident Response Performance Analytics ist über den ServiceNow Storeverfügbar. Informationen zum Herunterladen und Installieren dieser Anwendung finden Sie unter Security Operations und ServiceNow Store.

Hinweis:
Um die Funktionalität zu bewerten, können Sie Performance Analytics-Lösungen und formularinterne Analysen für nicht lizenzierte Instanzen aktivieren Performance Analytics. Sie haben jedoch die folgenden Einschränkungen:

- Sie können keine neuen Indikatoren erstellen.
- Sie können keine Daten sammeln, die älter als 180 Tage sind.

Lizenzieren Sie Performance Analytics für vollständige Funktionalität. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

Wichtig:
Standardmäßig ist das Datensammlungslimit für die Eigenschaft `(com.snc.pa.dc.max_records)` in Performance Analytics auf 5.000 Datensätze festgelegt. Sie können dieses Limit jedoch entsprechend Ihren Anforderungen erhöhen, z. B. auf 50.000 Datensätze. Eine Erhöhung dieses Grenzwerts kann sich jedoch auf die Leistung während der Datenerfassung oder bei Vorgängen in der Snapshot-Tabelle auswirken. Weitere Informationen zu den Performance Analytics-Eigenschaften finden Sie unter Performance Analytics properties .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

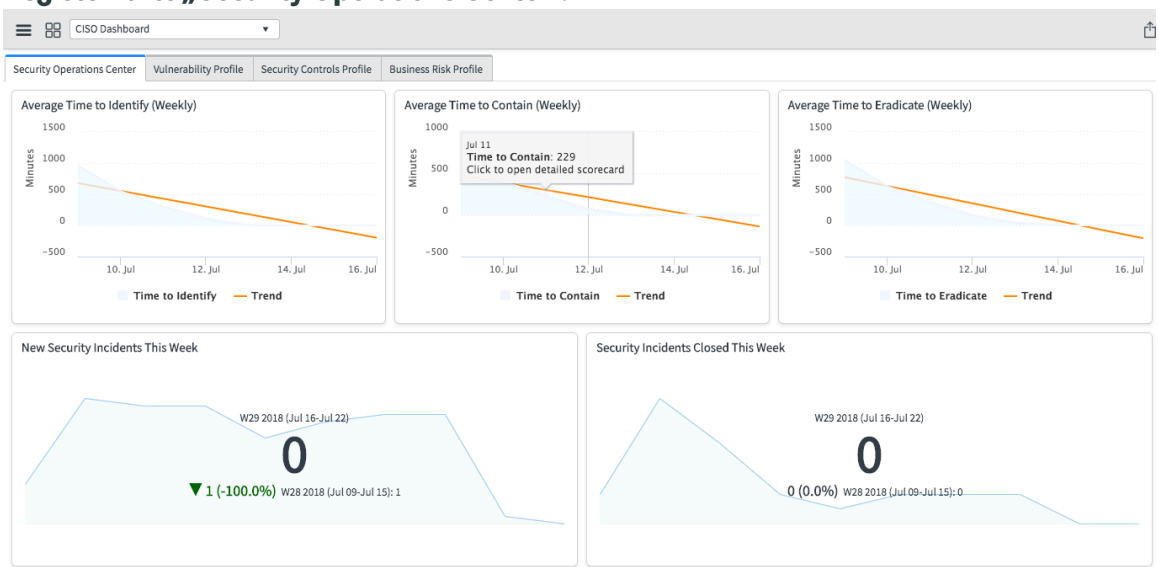
Platform Analytics-Lösungen

Performance Analytics-Abonnement aktivieren

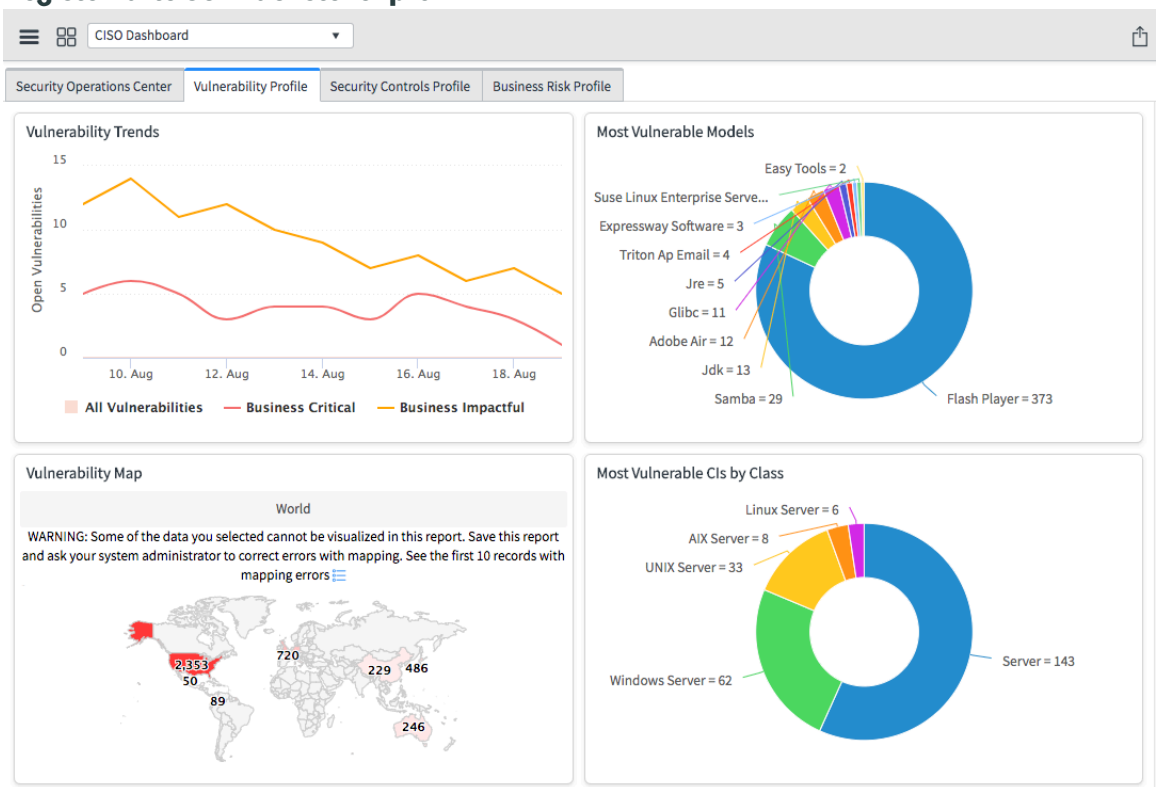
CISO-Dashboard

Dieses Dashboard zeigt die allgemeine Sicherheitslage Ihrer Organisation, einschließlich Sicherheitsschwachstellen und Incidents.

Registerkarte „Security Operations Center“.



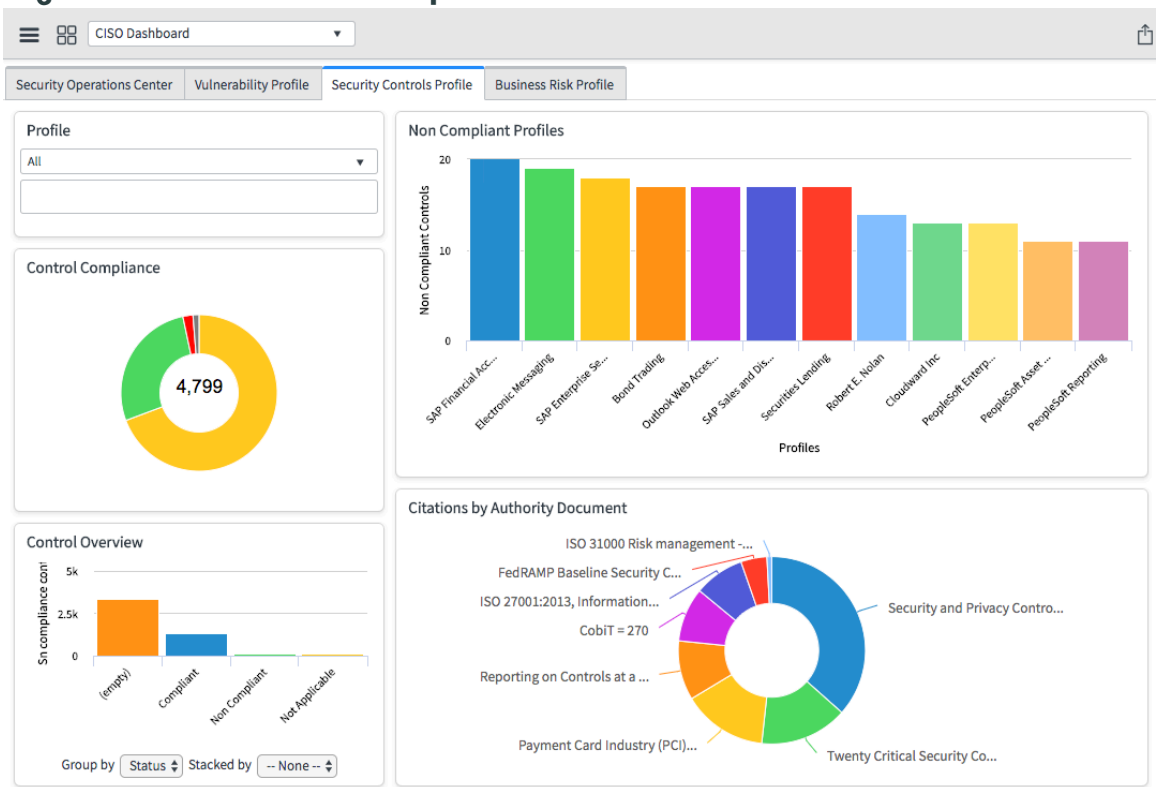
Registerkarte Schwachstellenprofil



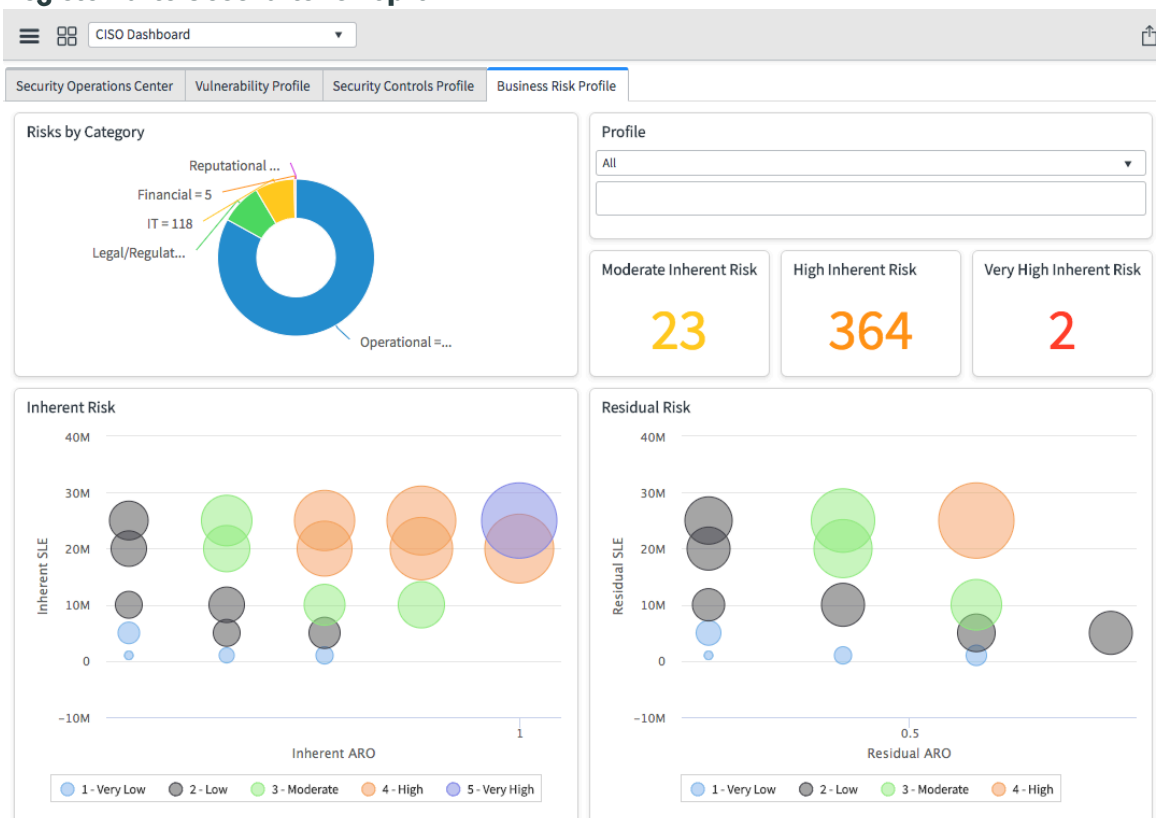
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte Sicherheitskontrollprofil



Registerkarte Geschäftsrisikoprofil



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle
CISO: Benötigt klare Transparenz über die aktuelle Sicherheitslage der gesamten Organisation	sn_si.cISO

CISO-Dashboard-Indikatoren

Das CISO-Dashboard enthält die folgenden Leistungskennzahlen:

SI: Durchschnittliche Zeit für Identifizierung

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die zur Identifizierung eines Security Incident benötigt wird, täglich berechnet.

Durchschnittliche Zeit bis zur Eindämmung

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die benötigt wird, um einen Security Incident einzudämmen, täglich berechnet.

Durchschnittliche Zeit bis Beseitigung

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die zur Beseitigung eines Security Incident benötigt wird, täglich berechnet. Sowohl „Durchschnittliche Zeit bis zur Eindämmung“ als auch „Durchschnittliche Zeit bis zur Beseitigung“ basieren auf dem Indikator „SI – Durchschnittliche Dauer aufgegliedert nach Status des Security Incident“.

Neue Security Incidents diese Woche

Die wöchentliche Summe der Punktzahl für den täglichen Indikator Anzahl neuer Security Incidents.

Geschlossene Security Incidents (wöchentlich)

Laufende Summe des täglichen Indikators Anzahl der geschlossenen Security Incidents über 7 Tage.

Neue Security Incidents nach Priorität

Tägliche Aufgliederung des Indikators „Anzahl neuer Security Incidents“ nach Priorität.

Volumen neuer vs. geschlossener Security Incidents (wöchentlich).

Die über 7 Tage laufende Summenzeitreihe des Indikators „Anzahl neuer Incidents“ im Diagramm mit der über 7 Tage laufenden Summenzeitreihe des Indikators „Anzahl geschlossener Incidents“ dargestellt.

Heatmap des Security Incidents

Eine globale Karte, die die Anzahl der offenen Security Incidents in jedem Land zeigt.

Strukturzuordnung für Security Incidents

Eine interaktive Verzeichnisübersicht, in der Sie Folgendes auswählen können:

- Security Incidents pro Business-Service, aufgeschlüsselt nach Geschäftsrelevanz
- Security Incidents, aufgeschlüsselt nach Kategorie oder Unterkategorie des Incidents
- Security Incidents pro Zuweisungsgruppe oder pro Beauftragtem
- „Opferstatistiken“ des Security Incident pro betroffener Ressource oder betroffenem Anwender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

- Business-Relevanz
- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Lösungscode für Security Incident
- Priorität von Security Incident
- Status des Security Incidents
- SI – Business-Service
- Schwachstelle

Datenvisualisierungen

Das Dashboard enthält die folgenden Visualisierungen:

Titel	Typ	Beschreibung
Security Incidents, die mehr als 30 Tage offen sind, nach Zuweisungsgruppe und Status	Heatmap	Zeigt Modelle mit den angreifbarsten Elementen an.
Risiken nach Kategorie	Ring	Listet das Alter der erneut geöffneten angreifbaren Elemente auf.
Zitate nach Berechtigungsdokument	Ring	Anzahl der aktiven Schwachstellen
Security Incidents mit Beauftragtem, der nicht aktiv ist	Heatmap	Zeigt die Anzahl der offenen angreifbaren Elemente an, die Schwachstellen zugeordnet sind (CVE-Datensätze (Common Vulnerability Enumeration)), von der höchsten zur niedrigsten.
Security Incidents, die seit mehr als 30 Tagen nicht aktualisiert wurden, nach Zuweisungsgruppe und Status	Heatmap	Zeigt die Herausgeber mit den angreifbarsten Elementen an.
Schwachstellenübersicht	Karte	Eine Weltkarte, die Schwachstellen nach Standort zeigt
Modelle mit den meisten Schwachstellen	Ring	Anwendungen, die die meisten Schwachstellen enthalten
CIs mit den meisten Schwachstellen nach Klasse	Ring	CIs nach Servertyp
Services mit kritisch signifikanten Schwachstellen	Liste	
Nicht konforme Profile	Balken	Nicht konforme Steuerungen nach Profil
Kontrollübersicht	Balken	Anzahl der konformen und nicht konformen Steuerungen
Richtlinienausnahmen	Liste	Richtlinienausnahmen mit Priorität, Besitzer und Kurzbeschreibung

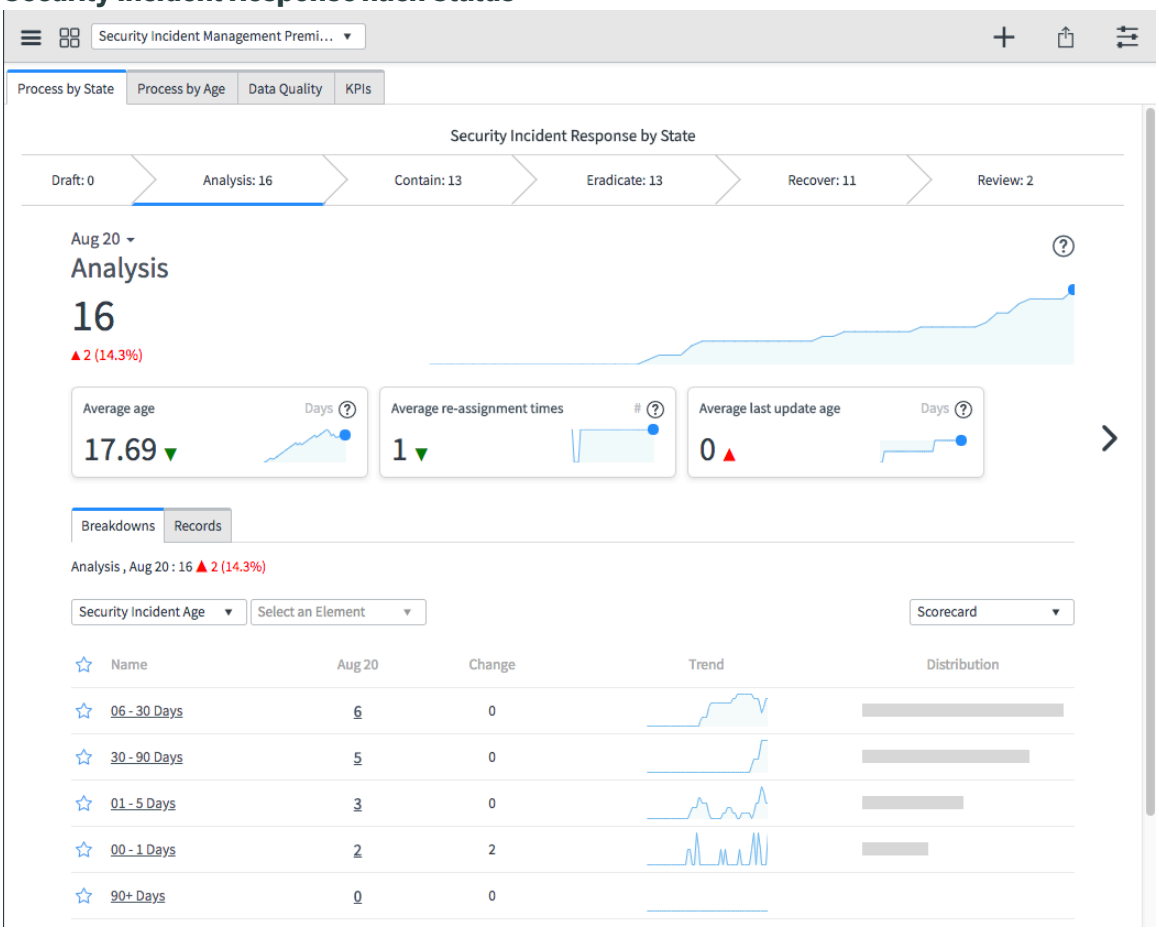
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
Risiken nach Kategorie	Ring	Die Anzahl der Risiken in jeder Risikokategorie
Inhärentes Risiko		Inhärente SLE im Vgl. zu inhärenter ARO
Restrisiko		Rest-SLE vs. Rest-ARO
Moderate, hohe und sehr hohe Risiken	Punktzahlen	Die Anzahl der moderaten, hohen und sehr hohen Risiken
Risiko nach Profil	Gestapelter Balken	Risikoanzahl, in der Sie auswählen können, nach welchen Elementen gruppiert und gestapelt werden soll

Dashboard „Security Incident Management Premium“.

Dieses Dashboard nutzt erweiterte Visualisierungen Platform Analytics, um Sicherheitsmanagern dabei zu helfen, das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung nachzuverfolgen. Die lizenzierte Version von Performance Analytics ist daher erforderlich.

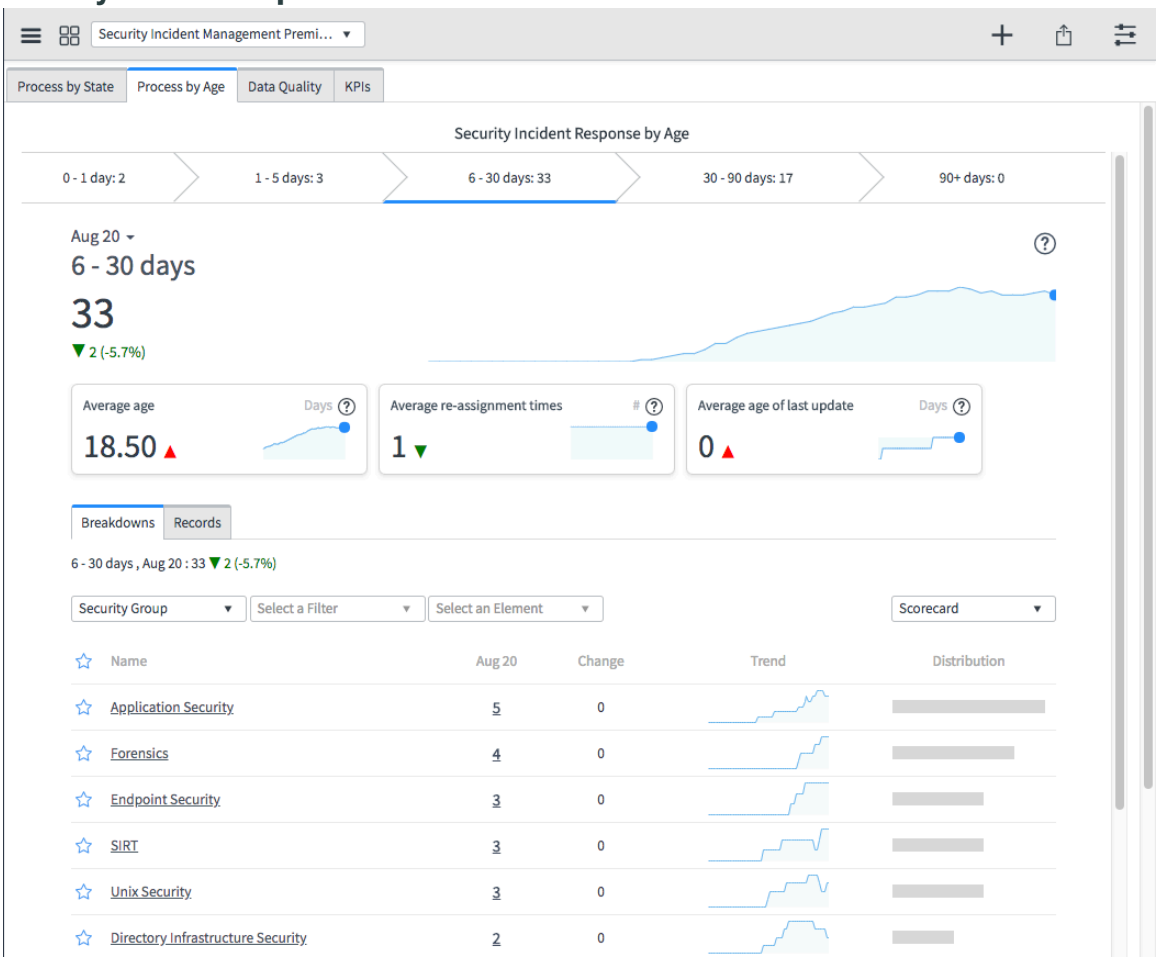
Security Incident Response nach Status



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response nach Alter



Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
Security Response Manager: Benötigt klare Einblicke in den Gesamtstatus und das Volumen der Security Incidents, die Anwendungen und Services zugeordnet sind.	sn_si.manager	Kann die allgemeine Sicherheitslage überprüfen und dabei die Mitglieder von Zuweisungsgruppen anpassen.
Security Response-Administrator: Muss Problembereiche schnell identifizieren und vollständige Kontrolle über alle Security Incident Response-Daten haben, während nach Bedarf Gebiete und Kompetenzen verwaltet werden.	sn_si.admin	Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden.
Security Response-Analysten: Sie müssen schnell priorisieren, auf welche Schwachstellen der Schwerpunkt gelegt werden soll, je nach Relevanz für das Unternehmen.	sn_si.analyst	Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
		Zusammenhang mit ihren Incidents erstellen und aktualisieren.

Indikatoren von Security Incident Management Premium

Die Registerkarten Nach Status verarbeiten und Nach Alter verarbeiten enthalten Workbench-Widgets mit den folgenden Indikatoren:

Durchschnittliches Alter

Der Indikator „Durchschnittliches Alter der offenen Security Incidents“ verwendet die Formel [[Summe des Alters offener Security Incidents]]/[[Anzahl offener Security Incidents]]/24, um ein Ergebnis in Tagen anzugeben.

Durchschnittliche Anzahl der Neuzuweisungen

Der Indikator Durchschnittliche Neuzuweisung offener Security Incidents verwendet die Formel Summierte Neuzuweisung offener Security Incidents/Anzahl der offenen Security Incidents.

Durchschnittliches Alter der letzten Aktualisierung

Der Indikator „Durchschnittliches Alter der letzten Aktualisierung offener Security Incidents“ verwendet die Formel Summiertes Alter der letzten Aktualisierung offener Security Incidents/Anzahl der offenen Security Incidents/24, um ein Ergebnis in Tagen zu erhalten.

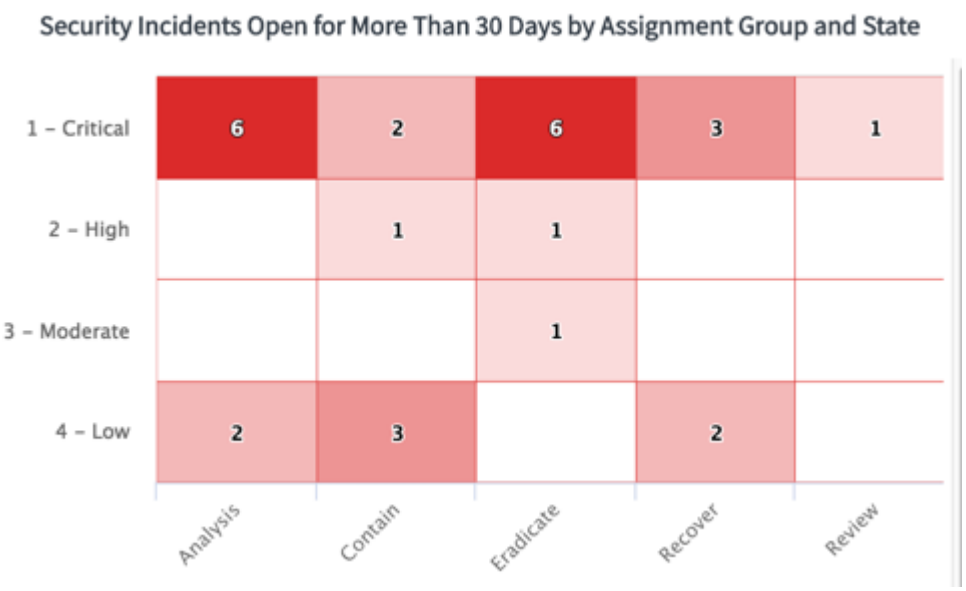
% seit 5 Tagen nicht aktualisiert

Der Indikator für den Prozentsatz offener Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden, verwendet die Formel ([[Anzahl der offenen Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden]] / [[Anzahl der offenen Security Incidents]]) * 100.

Die Registerkarte „Datenqualität“ enthält interaktive Filter für die Kategorie des Security Incident und die Stufen Risiko, Priorität und Schweregrad. Diese Filter werden gleichzeitig auf die folgenden Indikatoren angewendet:

Security Incidents, die mehr als 30 Tage offen sind, nach Zuweisungsgruppe und Status

Die Anzahl der offenen Security Incidents, gefiltert nach einem Alter von 30 Tagen und aufgeschlüsselt nach Zuweisungsgruppe und Status.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incidents mit Beauftragtem, der nicht aktiv ist

Anzahl der offenen Security Incidents ohne Beauftragten oder mit einem Beauftragten, der nicht aktiv ist.

Security Incidents, die mehr als 30 Tage offen sind, nach Zuweisungsgruppe und Status

Der Indikator Anzahl der offenen Security Incidents, die in den letzten 30 Tagen nicht aktualisiert wurden, aufgeschlüsselt nach Zuweisungsgruppe und Status.

Die Registerkarte „KPI“ enthält die folgenden zusätzlichen Indikatoren:

- % der neuen kritischen Security Incidents
- Durchschnittliches Alter der offenen Security Incidents
- Durchschnittliche Abschlusszeit von Security Incidents
- % der Security Incidents, die neu zugewiesen wurden
- % der Security Incidents, die bei der ersten Zuweisung geschlossen wurden
- % der per Selfservice geschlossenen Security Incidents
- % der nicht gelösten Security Incidents
- Durchschnittliche Abschlusszeit von Aufgaben von Security Incidents

Aufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

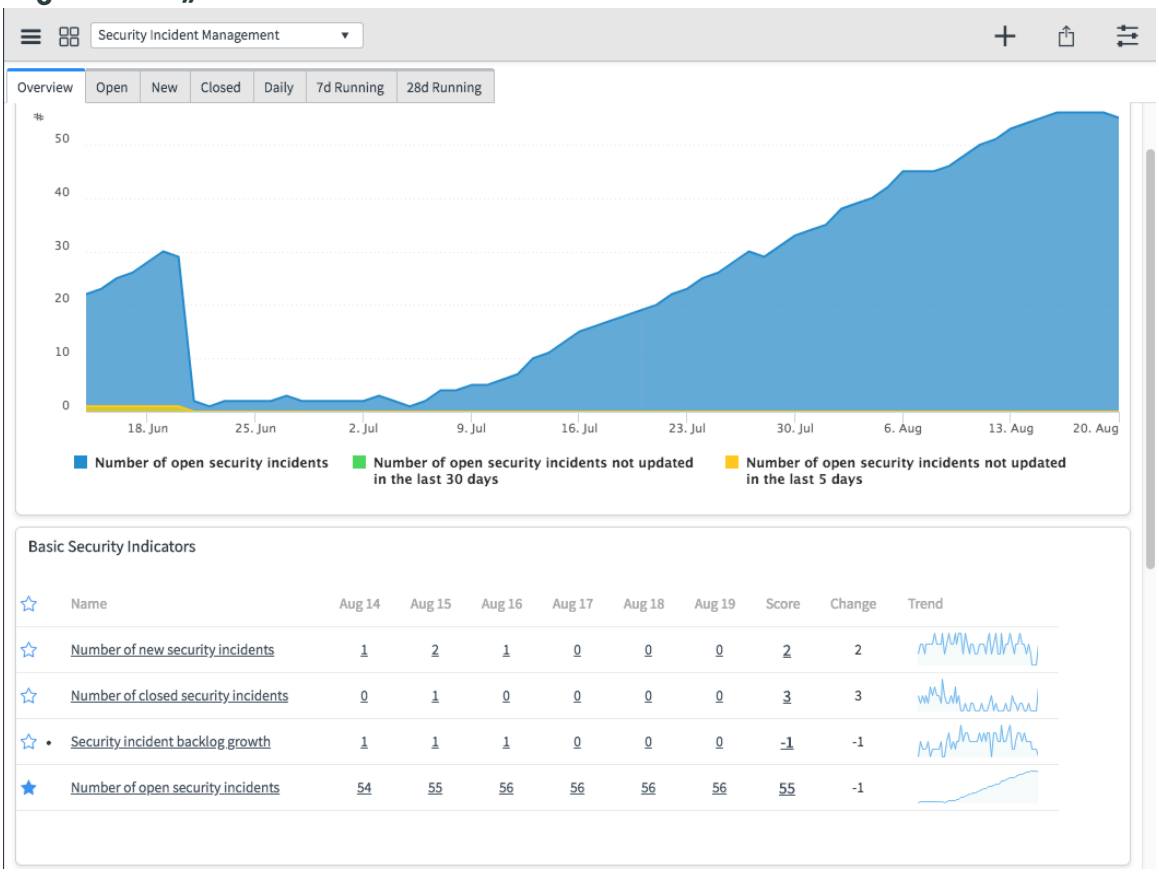
- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Priorität von Security Incident
- Status des Security Incidents

Dashboard „Security Incident Management“.

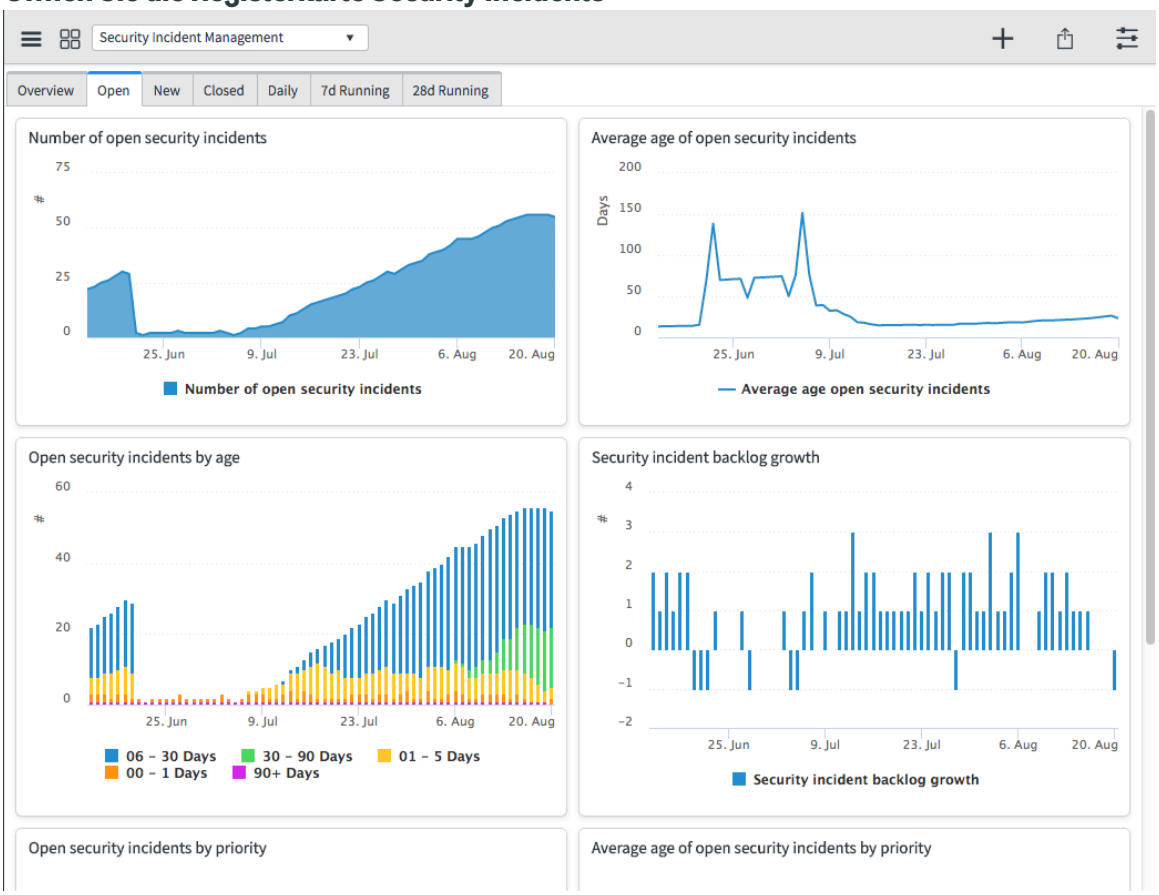
Mit diesem Dashboard können Sicherheitsmanager auf einfache Weise das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung verfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Übersicht“



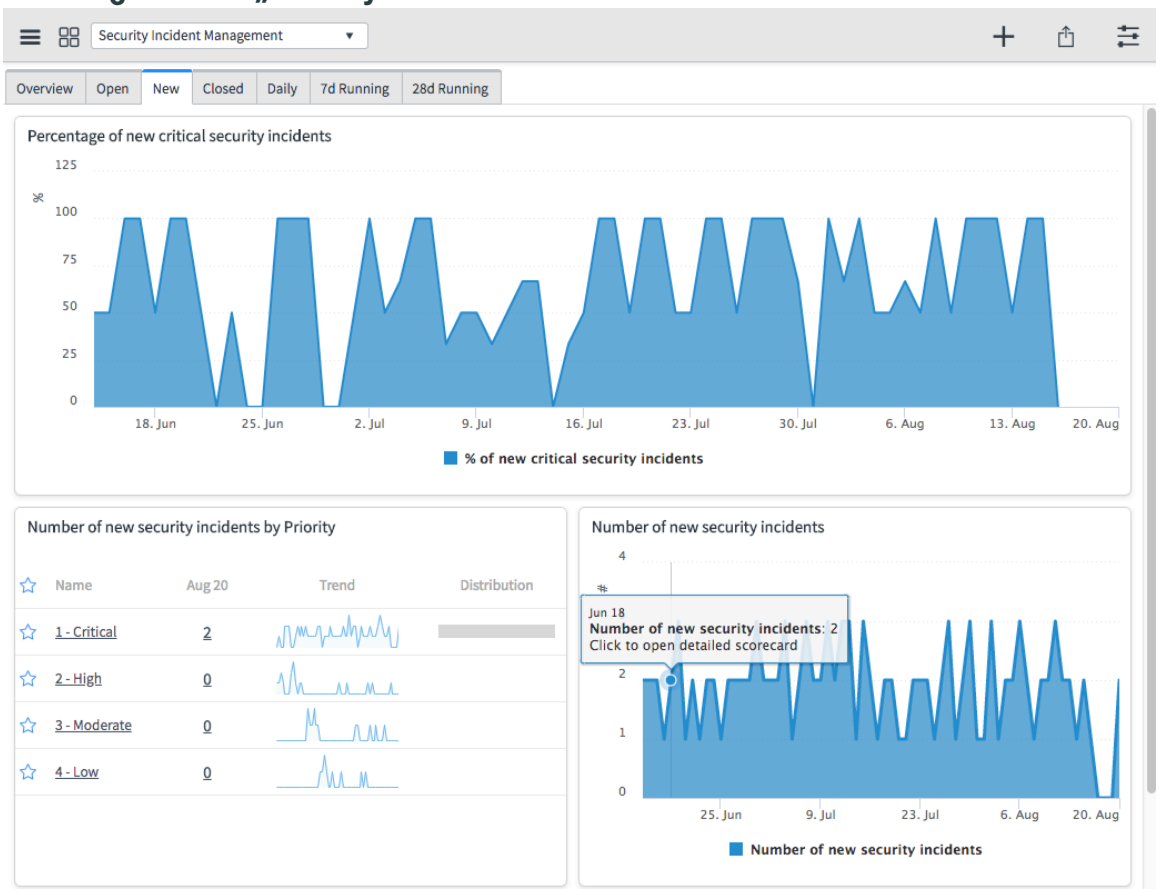
Öffnen Sie die Registerkarte Security Incidents



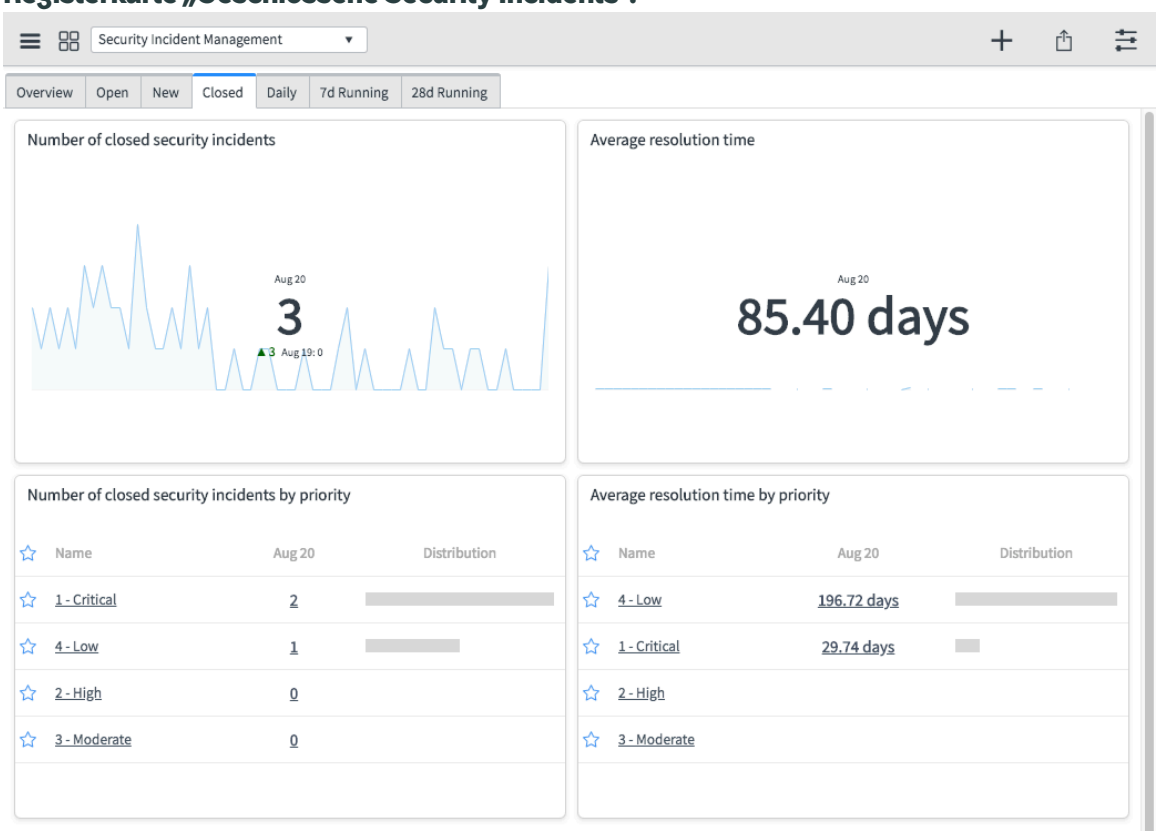
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Registerkarte „Security Incident“.



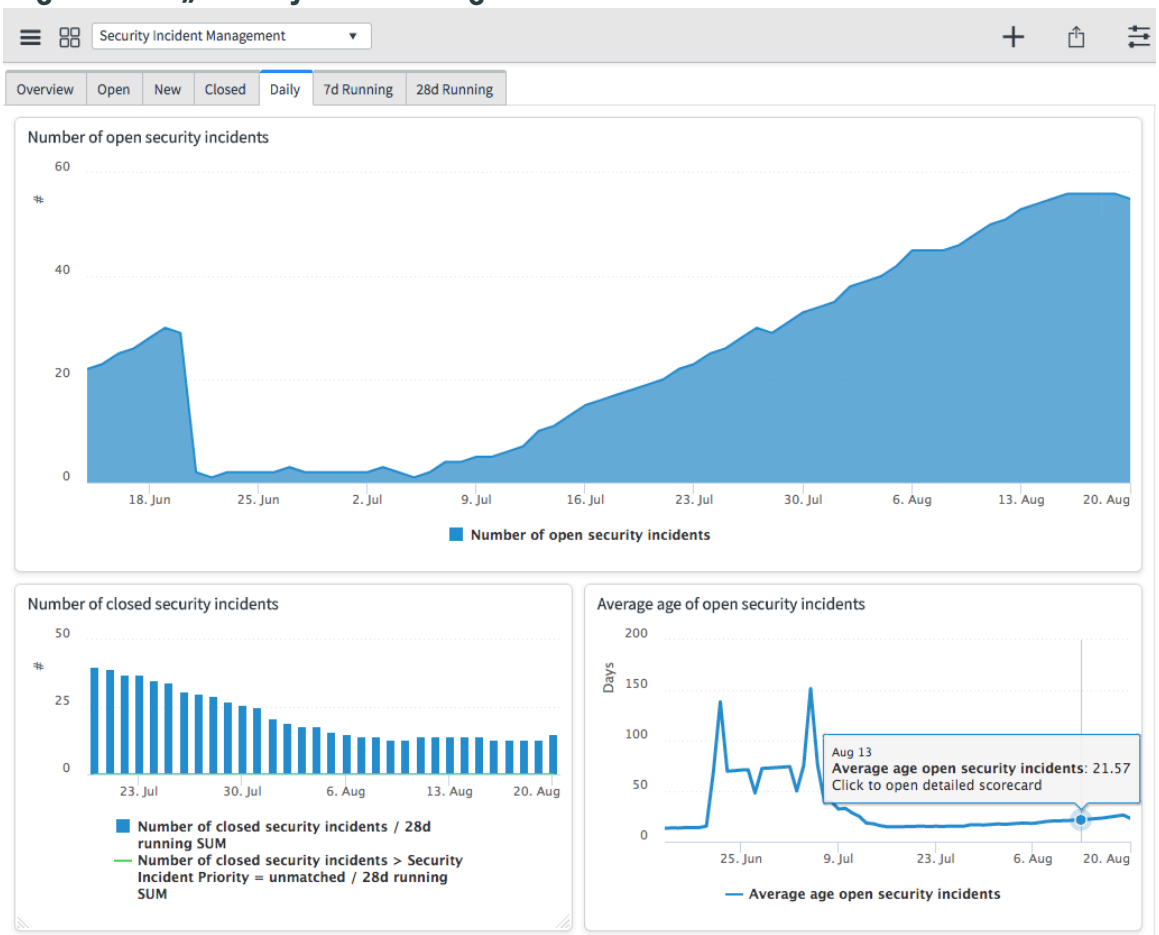
Registerkarte „Geschlossene Security Incidents“.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Security Incidents Täglich“.



Die Registerkarten **„7 Tage laufend“** und **„28 Tage laufend“** folgen dem Format der Registerkarte **Täglich**.

Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
Security Response Manager: Benötigt klare Einblicke in den Gesamtstatus und das Volumen der Security Incidents, die Anwendungen und Services zugeordnet sind.	sn_si.manager	Kann die allgemeine Sicherheitslage überprüfen und dabei die Mitglieder von Zuweisungsgruppen anpassen.
Security Response-Administrator: Muss Problembereiche schnell identifizieren und vollständige Kontrolle über alle Security Incident Response-Daten haben, während nach Bedarf Gebiete und Kompetenzen verwaltet werden.	sn_si.admin	Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden.
Security Response-Analysten: Sie müssen schnell priorisieren, auf welche Schwachstellen der Schwerpunkt gelegt werden	sn_si.analyst	Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
soll, je nach Relevanz für das Unternehmen.		Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.

Indikatoren für Security Incident-Management

Das Dashboard „Security Incident Management“ enthält die folgenden Leistungskennzahlen:

Neue Security Incidents

Ein Diagramm der Anzahl der neuen Security Incidents.

Offene Security Incidents

Ein Diagramm, in dem Sie die Anzahl der offenen Security Incidents, die Anzahl der offenen Security Incidents, die in den letzten 30 Tagen nicht aktualisiert wurden, und die Anzahl der offenen Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden, vergleichen können.

Indikatoren für einfache Sicherheit

Die letzten 6 Tage mit Punktzahlen für die Anzahl der Indikatoren „Anzahl neuer Security Incidents“, „Anzahl der geschlossenen Security Incidents“, „Wachstum des Security Incident-Backlogs“ und „Anzahl der offenen Security Incidents“.

Neue Security Incidents nach Priorität

Die Anzahl der neuen Security Incidents, aufgeschlüsselt nach Priorität.

Aufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

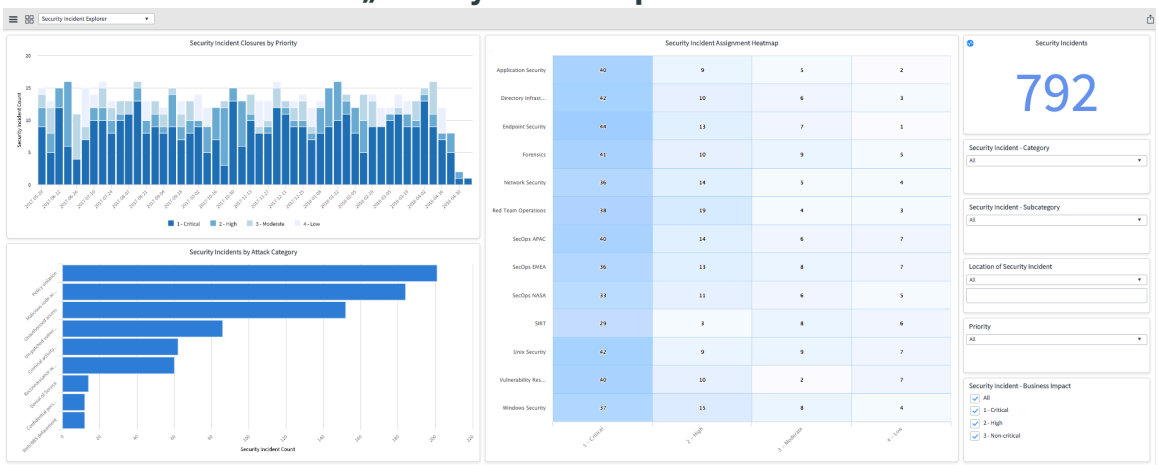
- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Priorität von Security Incident
- Status des Security Incidents

Security Incident Explorer-Dashboard

Mit diesem Dashboard können Sicherheitsmanager Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkung gruppiert anzeigen. Mit diesen Ansichten können Manager schnell Einblicke in die Häufigkeit von Angriffen und die betroffenen Business Services erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Teilansicht des Dashboards „Security Incident Explorer“.



Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
Security Response Manager: Benötigt klare Einblicke in den Gesamtstatus und das Volumen der Security Incidents, die Anwendungen und Services zugeordnet sind.	sn_si.manager	Kann die allgemeine Sicherheitslage überprüfen und dabei die Mitglieder von Zuweisungsgruppen anpassen.
Security Response-Administrator: Muss Problembereiche schnell identifizieren und vollständige Kontrolle über alle Security Incident Response-Daten haben, während nach Bedarf Gebiete und Kompetenzen verwaltet werden.	sn_si.admin	Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden.
Security Response-Analysten: Sie müssen schnell priorisieren, auf welche Schwachstellen der Schwerpunkt gelegt werden soll, je nach Relevanz für das Unternehmen.	sn_si.analyst	Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.

Indikatoren des Security Incident Explorers

Das Security Incident Explorer-Dashboard enthält die folgenden Leistungskennzahlen:

Security Incidents

Gesamtvolumen offener und ausstehender Security Incidents

Security Incident-Abschlüsse nach Priorität

Die Anzahl der geschlossenen Security Incidents, aufgeschlüsselt nach Priorität.

Security Incidents nach Angriffskategorie

Die Anzahl der offenen Security Incidents, aufgeschlüsselt nach Kategorie.

Heatmap für Security Incident-Zuweisung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Aufgliederung der Anzahl offener Security Incidents nach Zuweisungsgruppe und Priorität in zwei Ebenen.

Heatmap des Security Incidents

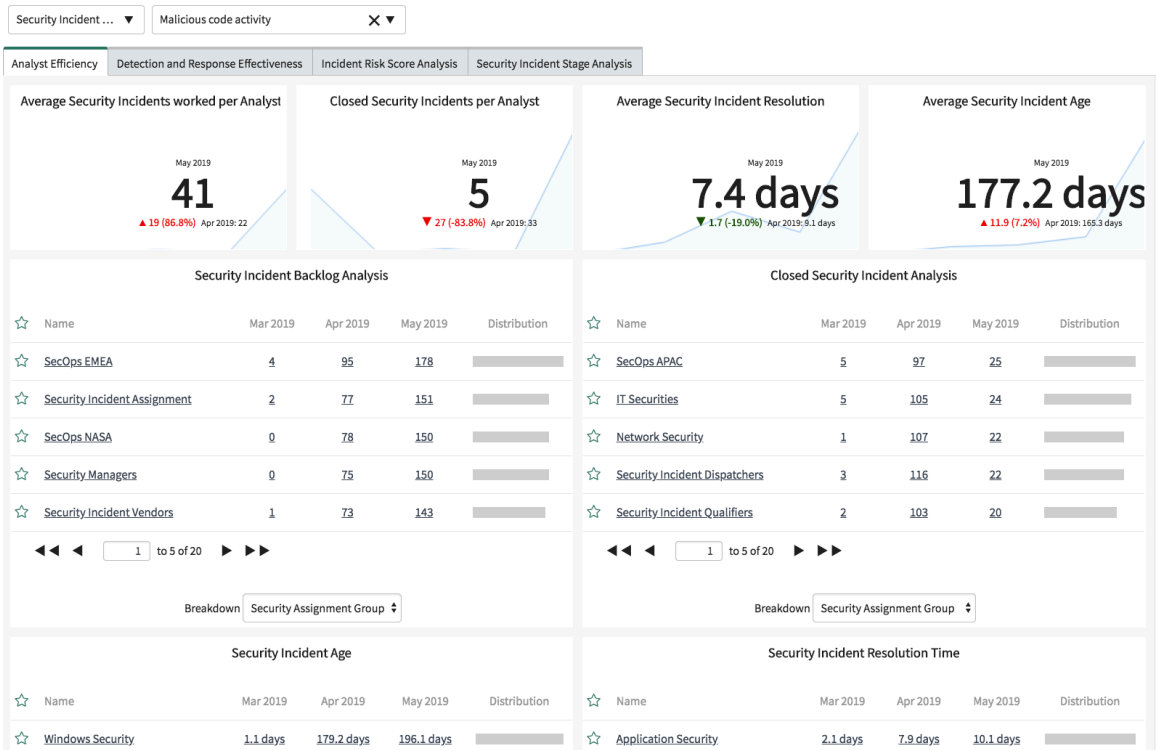
Eine globale Karte, die die Anzahl der offenen Security Incidents in jedem Land zeigt.

Effizienz von Security Operations-Dashboard

SOC-Manager (Security Operations Center) können allgemeine Effizienzmetriken anzeigen und die individuelle Leistung der SOC-Teammitglieder in der Organisation messen.

Der SOC-Manager kann das Performance Analytics-Dashboard verwenden, um die Effizienz zu verbessern und sich ein Bild von der Leistung von SOC in allgemeinen und spezifischen Bereichen im Laufe der Zeit zu machen.

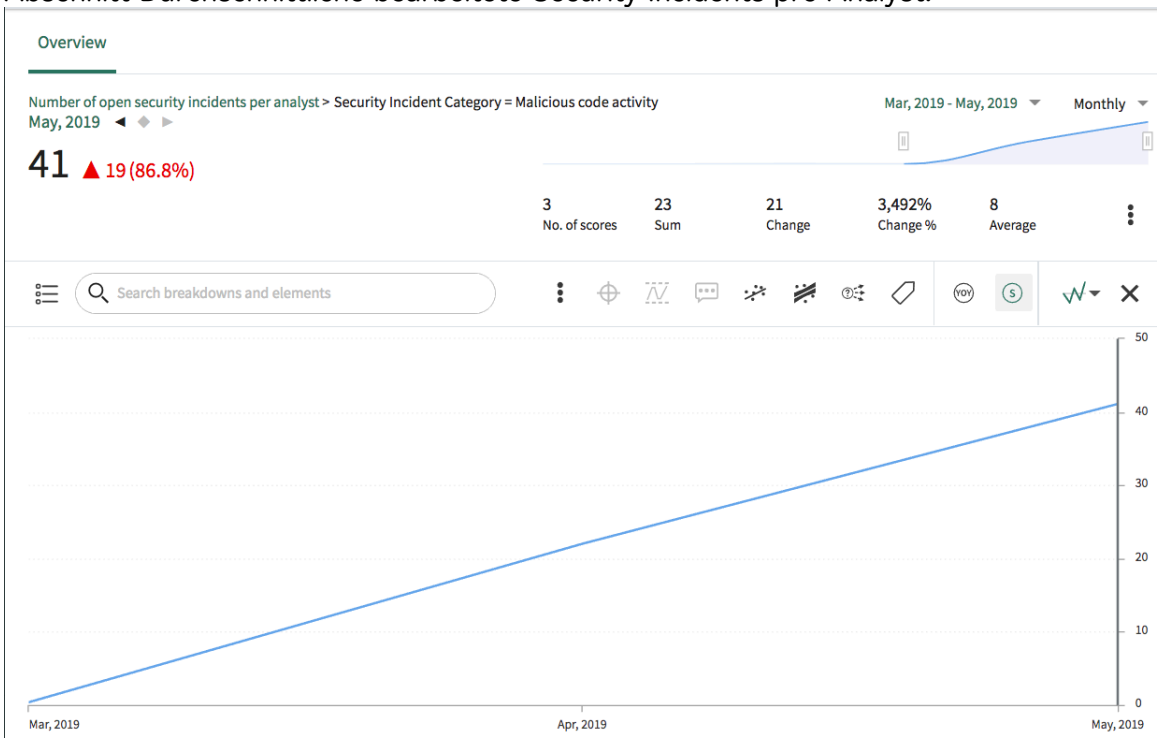
Registerkarte „Analyseneffizienz“.



Klicken Sie auf einen der Indikatoren, um einen Drilldown für weitere Details durchzuführen. Klicken Sie beispielsweise auf den Indikator im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt Durchschnittliche bearbeitete Security Incidents pro Analyst.



Das Diagramm zeigt, dass die Anzahl der offenen Security Incidents von 0 im März auf über 40 im Mai gestiegen ist. Beachten Sie die im Header angezeigten Daten:

- Trendindikator: Zeigt die Änderung der Anzahl der offenen Incidents im letzten Zeitraum an, für den die Daten gesammelt wurden. Dieses Diagramm zeigt Daten für den Zeitraum März 2019 bis Mai 2019, wobei die Anzahl der offenen Incidents im Monat Mai um 19 gestiegen ist. Die Effizienz der Analysten ist besser, wenn die Anzahl der offenen Incidents im Laufe der Zeit abgenommen hat.
- Anzahl der Punktzahlen: Der Zeitraum, für den die Daten gesammelt wurden (März bis Mai 2019).
- Summe: Anzahl der neuen offenen Incidents für den Zeitraum zwischen März und Mai.
- Change: Anzahl der neuen offenen Incidents zwischen März und April
- Durchschnitt: Die durchschnittliche Anzahl der offenen Incidents pro Analyst für den ausgewählten Zeitraum.

Registerkarte „Analyseneffizienz“.

Indikator	Beschreibung
Durchschnittliche bearbeitete Security Incidents pro Analyst	Durchschnittliche Anzahl der offenen Security Incidents pro Analyst für den angegebenen Zeitraum. Die verwendete Formel lautet [[Anzahl der offenen Security Incidents / Pro Monat - Durchschnitt +]]/[[Anzahl der Sicherheitsmitarbeiter]]
Geschlossene Security Incidents pro Analyst	Gesamtzahl der Incidents, die von jedem Analysten in der ausgewählten Kategorie im angegebenen Zeitraum geschlossen wurden. Die verwendete Formel lautet [Anzahl der geschlossenen Security Incidents > Kategorie des Security Incidents =“.<category_name> /Pro Monat - Summe +]]/[[Anzahl der Sicherheitsmitarbeiter/Pro Monat - Durchschnitt +]]
Durchschnittliche Lösung von Security Incidents	Die durchschnittliche Zeit, die jeder Analyst benötigt, um Security Incidents im angegebenen Zeitraum zu schließen. Die Formel für die Anzeige des

Automatische Übersetzung

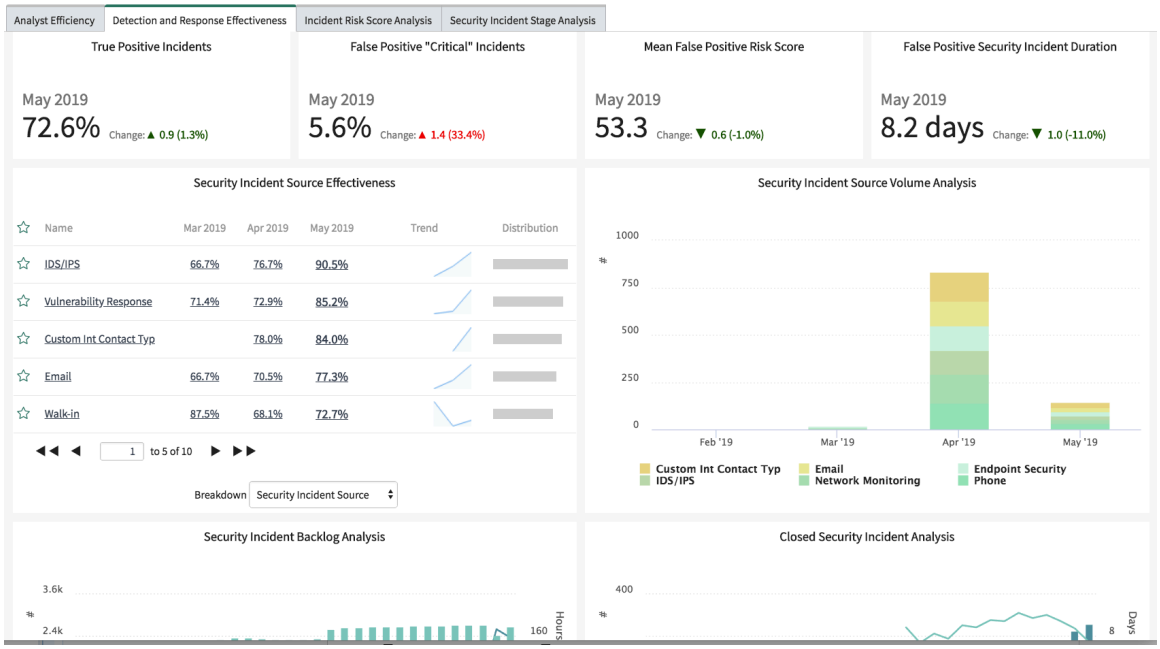
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Analyseneffizienz“. (Fortsetzung)

Indikator	Beschreibung
	Ergebnisses in Tagen lautet ([[Summierte Dauer der geschlossenen Security Incidents > Kategorie des Security Incident =<category_name> / Pro Monat - Durchschnitt +]] / [[Anzahl geschlossener Security Incidents > Security Incident-Kategorie = / Pro Monat - Durchschnitt +]]) / 24
Durchschnittliches Alter der Security Incidents	Die durchschnittliche Anzahl von Tagen, für die Security Incidents für jeden Analysten offen bleiben. Die Formel für die Anzeige des Ergebnisses in Tagen lautet ([[Summiertes Alter der offenen Security Incidents > Security Incident-Kategorie =<category_name> / Pro Monat - Durchschnitt +]]/ [[Anzahl der offenen Security Incidents > Kategorie von Security Incidents = / Pro Monat - Durchschnitt +]]) / 24
Analyse des Security Incident-Backlogs	Gesamtzahl der offenen Security Incidents im angegebenen Zeitraum. Wählen Sie eine Option aus der Liste „Aufgliederung“ aus, um das Backlog für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Sie können auch die Anzahl der offenen Security Incidents zwischen zwei ausgewählten Monaten vergleichen.
Analyse eines geschlossenen Security Incidents	Gesamtzahl der Security Incidents, die im angegebenen Zeitraum geschlossen wurden. Wählen Sie eine Option aus der Liste „Aufgliederung“ aus, um die Anzahl für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Sie können auch die Anzahl der Security Incidents vergleichen, die zwischen zwei ausgewählten Monaten geschlossen wurden.
Alter des Security Incidents	Die durchschnittliche Anzahl der Tage, an denen Security Incidents im angegebenen Zeitraum offen bleiben. Wählen Sie eine Option aus der Liste „Aufgliederung“ aus, um das Alter der Security Incidents für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Die Formel für die Anzeige des Ergebnisses in Tagen lautet ([[Summiertes Alter der offenen Security Incidents > Security Incident-Kategorie =<category_name> > Sicherheitszuweisungsgruppe =<group_name> / Pro Monat - Durchschnitt +]]/ [[Anzahl der offenen Security Incidents > Kategorie von Security Incidents = > Sicherheitszuweisungsgruppe = / Pro Monat - Durchschnitt +]]) / 24
Lösungszeit für Security Incident	Die durchschnittliche Anzahl von Tagen, die für die Lösung von Security Incidents im angegebenen Zeitraum benötigt wurden. Wählen Sie eine Option aus der Liste „Aufgliederung“ aus, um die Lösungszeit für Security Incidents für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Die Formel zum Anzeigen des Ergebnisses in Tagen lautet ([[Summierte Dauer der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Code-Aktivität > Sicherheit zugewiesen = John Asby / Pro Monat - Durchschnitt +]] / [[Anzahl geschlossener Security Incidents >). Kategorie des Security Incidents = Böswillige Code-Aktivität > Sicherheit zugewiesen an = John Asby / Pro Monat - Durchschnitt +]]) / 24

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erkennung und Antworteffektivität“.



Registerkarte „Erkennung und Antworteffektivität“.

Indikator	Beschreibung
Richtig positive Incidents	Prozentsatz der wirklich positiven Security Incidents in der ausgewählten Kategorie für den angegebenen Zeitraum. Die verwendete Formel lautet (1-([[Anzahl der falsch positiven Security Incidents > Kategorie des Security Incident = Böswillige Codeaktivität / Pro Monat - Summe +]] / [[Anzahl der geschlossenen Security Incidents > Kategorie des Security Incident = Böswillige Codeaktivität / Pro Monat Summe +]])) * 100
Falsch positive kritische Incidents	Prozentsatz der falsch positiven kritischen Security Incidents in der ausgewählten Kategorie für den angegebenen Zeitraum. Die verwendete Formel lautet ([[Anzahl der falsch positiven Security Incidents > Risikopunktzahl des Security Incident = Kritisches Risiko > Kategorie des Security Incident = Böswillige Codeaktivität / Pro Monat - Summe +]] / [[Anzahl der geschlossenen Security Incidents > Kategorie des Security Incident = Böswillig Codeaktivität / Pro Monat - Summe +]]) * 100 **Hinweis:** Jeder Security Incident, bei dem der geschlossene Code = Ungültige Schwachstelle oder Falsch positiv ist, wird als falsch positiver Incident behandelt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erkennung und Antworteffektivität“. (Fortsetzung)

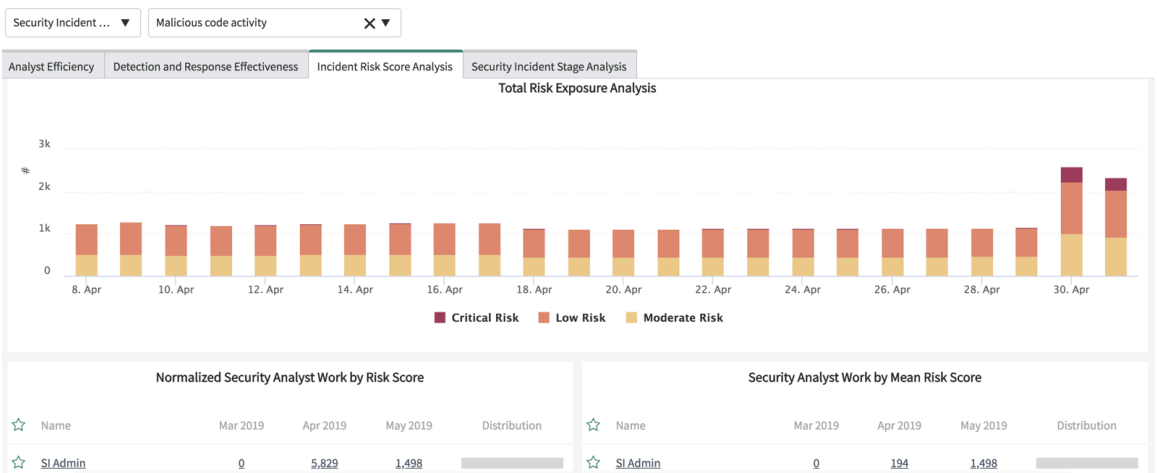
Indikator	Beschreibung
Mittlere falsch positive Risikopunktzahl	Durchschnittliche monatliche Risikopunktzahl der geschlossenen Security Incidents, die als falsch positive Incidents identifiziert wurden. Eine niedrigere Risikopunktzahl zeigt an, dass die Sicherheitsanalysten weniger Zeit für die Analyse falsch positiver Incidents aufgewendet haben. Die verwendete Formel lautet ([[Anzahl der falsch positiven Security Incidents > Risikopunktzahl des Security Incident = Kritisches Risiko > Kategorie des Security Incident = Böswillige Codeaktivität / Pro Monat - Summe +]] / [[Anzahl der geschlossenen Security Incidents > Kategorie des Security Incident = Böswillig Codeaktivität / Pro Monat - Summe +]]) * 100
Dauer der falsch positiven Security Incidents	Durchschnittliche Anzahl der Tage, die Sicherheitsanalysten mit der Untersuchung falsch positiver Incidents verbracht haben. Die verwendete Formel lautet ([[Summierte Dauer der falsch positiven Security Incidents]]/[[Anzahl der falsch positiven Security Incidents]])/24
Effektivität der Security Incident-Quelle	Prozentsatz der wirklich positiven Security Incidents, die von einer bestimmten Quelle für den angegebenen Zeitraum identifiziert wurden. Die Quelle kann E-Mail, Netzwerkaktivität,Kundensupport usw. sein. Mit diesen Daten kann die Effektivität der Quelle des Security Incident gemessen werden. Die verwendete Formel lautet (1-([[Anzahl der falsch positiven Security Incidents > Kategorie des Security Incidents = Böswillige Codeaktivität > Quelle des Security Incidents = IDS/ IPS / Pro Monat - Summe +]] / [[Anzahl der geschlossenen Security Incidents > Security Incident Kategorie = Böswillige Code-Aktivität > Quelle des Security Incidents = IDS/IPS / Pro Monat - Summe +]])) * 100
Analyse des Quellvolumens des Security Incidents	Anzahl der geschlossenen Security Incidents für den aktuellen Monat für jede Security Incident-Quelle. Sie können auch die Anzahl der Security Incidents für jeden Quelltyp zwischen zwei ausgewählten Monaten vergleichen.
Analyse des Security Incident-Backlogs	Die Gesamtzahl der offenen Security Incidents im angegebenen Zeitraum und die durchschnittliche Anzahl der Tage, für die die Incidents offen bleiben. Sie können auch die Anzahl der offenen Security Incidents zwischen zwei ausgewählten Monaten vergleichen. Die zur Berechnung des durchschnittlichen Backlog-Zeitraums verwendete Formel lautet ([[Summiertes Alter der offenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erkennung und Antworteffektivität“. (Fortsetzung)

Indikator	Beschreibung
	Security Incidents > Kategorie des Security Incident = Böswillige Codeaktivität]]/[[Anzahl der offenen Security Incidents > Kategorie des Security Incident = Böswillige Codeaktivität]])/ 24
Analyse eines geschlossenen Security Incidents	Die Gesamtzahl der geschlossenen Security Incidents im angegebenen Zeitraum sowie die durchschnittliche Lösungszeit für diese Incidents. Die zur Berechnung der durchschnittlichen Lösungszeit verwendete Formel lautet ([[Summierte Dauer der geschlossenen Security Incidents > Kategorie des Security Incident = Böswillige Codeaktivität]] / [[Anzahl der geschlossenen Security Incidents > Kategorie des Security Incident = Böswillige Codeaktivität]]) / 24

Registerkarte „Analyse der Incident-Risikopunktzahl“



Registerkarte „Analyse der Incident-Risikopunktzahl“

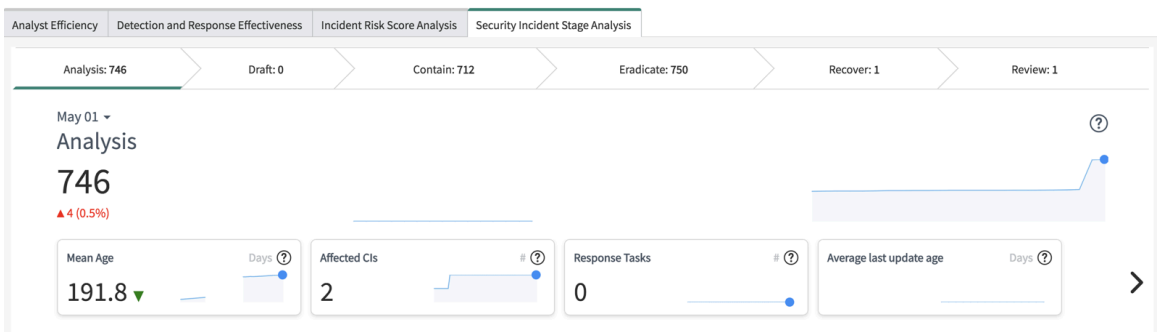
Indikator	Beschreibung
Analyse des Gesamtrisikos des Gefahrenpotenzials	Gesamtzahl der offenen Incidents in jeder Risikokategorie (niedrig, mittel und kritisch) im angegebenen Zeitraum. Sie können auch die Anzahl der Incidents in den verschiedenen Risikokategorien zwischen zwei Monaten vergleichen.
Normalisierte Sicherheitsanalystenarbeit nach Risikopunktzahl	Gesamtrisikopunktzahl für jeden Sicherheitsanalysten für den angegebenen Zeitraum. Dies wird basierend auf der Anzahl der richtig positiven Security Incidents berechnet, die der Sicherheitsanalyst geschlossen hat. Die verwendete Formel lautet [[Summierte Risikopunktzahl der geschlossenen Security Incidents > Kategorie des Security Incident = Böswillige Code-Aktivität > Sicherheit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Analyse der Incident-Risikopunktzahl“ (Fortsetzung)

Indikator	Beschreibung
	zugewiesen = SI-Administrator / Pro Monat SUMME +]] - [[Summierte Risikopunktzahl der falsch-positiven Security Incidents > Kategorie des Security Incidents“. = Böswillige Code-Aktivität > Sicherheit zugewiesen = SI-Administrator / Pro Monat - Summe +]]
Sicherheitsanalysten arbeiten nach durchschnittlicher Risikopunktzahl	Die durchschnittliche Risikopunktzahl für jeden Sicherheitsanalysten für den angegebenen Zeitraum. Die verwendete Formel lautet [[Summierte Risikopunktzahl der geschlossenen Security Incidents > Kategorie des Security Incidents = Böswillige Code-Aktivität > Sicherheit zugewiesen = SI-Administrator / Pro Monat - Durchschnitt +]] - [[Summierte Risikopunktzahl der falsch-positiven Security Incidents > Kategorie des Security Incidents“. = Böswillige Code-Aktivität > Sicherheit zugewiesen an = SI-Administrator / Pro Monat - Durchschnitt +]]

Registerkarte „Phasenanalyse des Security Incidents“.



Sie können die Anzahl der offenen Incidents an einem bestimmten Tag und den Status (Analyse, Entwurf, Eindämmen, Löschen, Wiederherstellen oder Überprüfen) dieser Incidents anzeigen. In jeder Phase können Sie das Durchschnittsalter, betroffene CIs, Antwortaufgaben usw. anzeigen. Klicken Sie auf einen Link, um zusätzliche Details oder die Aufgliederung dieser Incidents anzuzeigen.

Arbeitsbereich für Security Incident Response

ServiceNow® Arbeitsbereich für Security Incident Response ist eine neu gestaltete Schnittstelle, die Sicherheitsanalysten und SOC-Managern eine Anwender-Experience der nächsten Generation bietet. Sicherheitsanalysten können hiermit den Lebenszyklus von Security Incidents verwalten, von der ersten Analyse bis zur Eindämmung, Beseitigung und Wiederherstellung.

Erste Schritte mit SIR Workspace

Wählen Sie eine Kachel aus, um mit den ersten Schritten zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich erkunden

Erfahren Sie mehr über die Konzepte und Funktionen des SIR-Arbeitsbereichs

Administratoren, die Workspace verwenden

Konfigurieren Sie den SIR-Arbeitsbereich und die Funktionen

Analysten, die Workspace verwenden

Erfahren Sie, wie Analysten den SIR-Arbeitsbereich verwenden

Zeigen Sie SIR-Dashboards an

Zeigen Sie Dashboards des SIR-Arbeitsbereichs an

Automatische Übersetzung

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- Wenn Sie Security Incident Response Version 13.4.5 oder höher aus ServiceNow Store installieren, wird standardmäßig automatisch die Version Arbeitsbereich für Security Incident Response (sn_si_aw) Version 1.5.1 oder höher installiert. Weitere Informationen zu den abhängigen Anwendungen finden Sie im Abschnitt SIR Workspace Plugins und Rollen.
- Beachten Sie, dass Security Incident Response Workspace, Version 1.5.1 und höher, nur durch eine Installation/ein Upgrade von Security Incident Response installiert/aktualisiert werden kann und nicht unabhängig installiert werden kann.

Weitere Ressourcen

Besuchen Sie das Security Incident Response Forum unter ServiceNow Community.

SIR Workspace erkunden

Erkunden Sie Arbeitsbereich für Security Incident Response, um zu verstehen, wie Sicherheitsanalysten und -manager ihre täglichen Vorgänge mit einer verbesserten Anwender-Experience durchführen, führen Sie eine vollständige Untersuchung von Incidents durch, und erhalten Sie einen Überblick über die Security Incidents, Antwortaufgaben und SLAs, die dem Sicherheitsanalysten und zugewiesen sind Team

In diesem Abschnitt wird Folgendes beschrieben:

- SIR Workspace Plugins und erforderlichen Rollen.
- Schlüsselfunktionen von SIR Workspace.

SIR Workspace Plugins und Rollen

Im Folgenden finden Sie die Anwendungen, die für die Verwendung mit dem Plugin Arbeitsbereich für Security Incident Response (sn_si_aw) erforderlich sind.

Anwendungen

Durch die Installation der Anwendung Security Incident Response, Version 13.4.5 oder höher, werden Arbeitsbereich für Security Incident Response und die folgenden Apps automatisch installiert.

- Enterprise Security Case Management PAD Common [sn_escm_pad_cmn]
- Gemeinsamer Arbeitsbereich für Security Operations [sn_escm_ws_cmn]
- Security Incident UI Card Component [sn_sirw_ema]
- Security Operations-Spoke [sn_sec_spoke]

Wichtig:

- Wenn Sie Security Incident Response Version 13.4.5 oder höher aus ServiceNow Store installieren, wird standardmäßig automatisch die Version Arbeitsbereich für Security Incident Response (sn_si_aw) Version 1.5.1 oder höher installiert. Weitere Informationen zu den abhängigen Anwendungen finden Sie im Abschnitt SIR Workspace Plugins und Rollen.
- Beachten Sie, dass Version 1.5.1 und höher von Security Incident Response Workspace nur durch eine Installation/ein Upgrade von Security Incident Response installiert/aktualisiert und nicht unabhängig installiert werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enterprise Security Case Management PAD Common erfordert das Plugin „Playbook-Experience“ [playbook_experience].

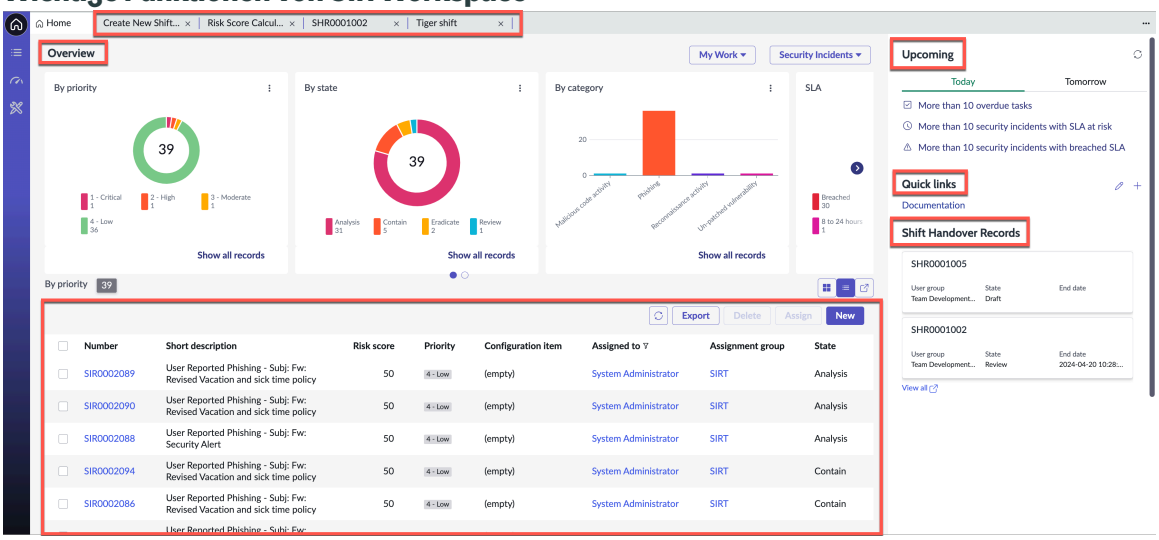
Informationen zu den Rollen, Tabellen, Eigenschaften und geplanten Aufgaben Security Incident Response] finden Sie unter Mit Security Incident Response installierte Komponenten

SIR Workspace-Funktionen

Arbeitsbereich für Security Incident Response besteht aus den folgenden Schlüsselfunktionen.

- Übersichtsbereich
- Abschnitt „Bevorstehend“
- Abschnitt „Quick-Links“.
- Abschnitt „Datensätze der Schichtübergabe“.
- Listenansicht
- Schnittstelle mit mehreren Registerkarten, die das Öffnen mehrerer Security Incidents unterstützt

Wichtige Funktionen von SIR Workspace



SIR Workspace Übersicht über die -Schnittstelle

Die Übersichtsseite SIR Workspace enthält die Details zu Security Incidents und Antwortaufgaben, die sich unter Sicherheitsanalysten und ihrem Team befinden.

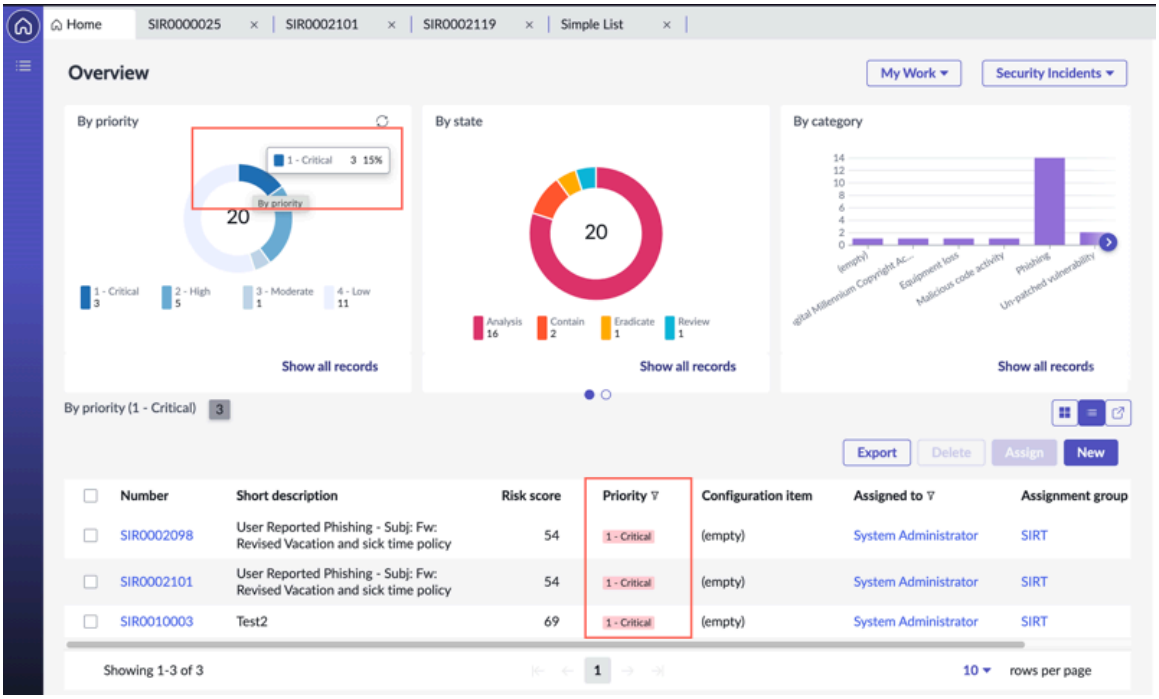
Unter jedem Filter sind verschiedene Widgets vorhanden, die nach Priorität, Kategorie, Status und SLA gruppiert sind und sich in den Warteschlangen der Sicherheitsanalysten und in der Warteschlange des Sicherheitsanalystenteams befinden.

Wenn Filter auf die Widgets angewendet werden, wird die untere Hälfte der Übersichtsseite mit den entsprechenden Security Incidents oder Antwortaufgaben gefüllt, die als Karten oder Listenelemente dargestellt werden. Der Analyst kann nach Belieben zwischen der Kartenansicht und der Listenansicht wechseln.

Wenn Sie beispielsweise im **Prioritäts** -Widget alle kritischen Incidents oder Antwortaufgaben auswählen möchten, klicken Sie auf das Segment **„Kritisch“** (Beispiel-Screenshot unten) des Widgets. Die kritischen Incidents oder Antwortaufgaben werden in der Liste oder Karte angezeigt Ansicht.

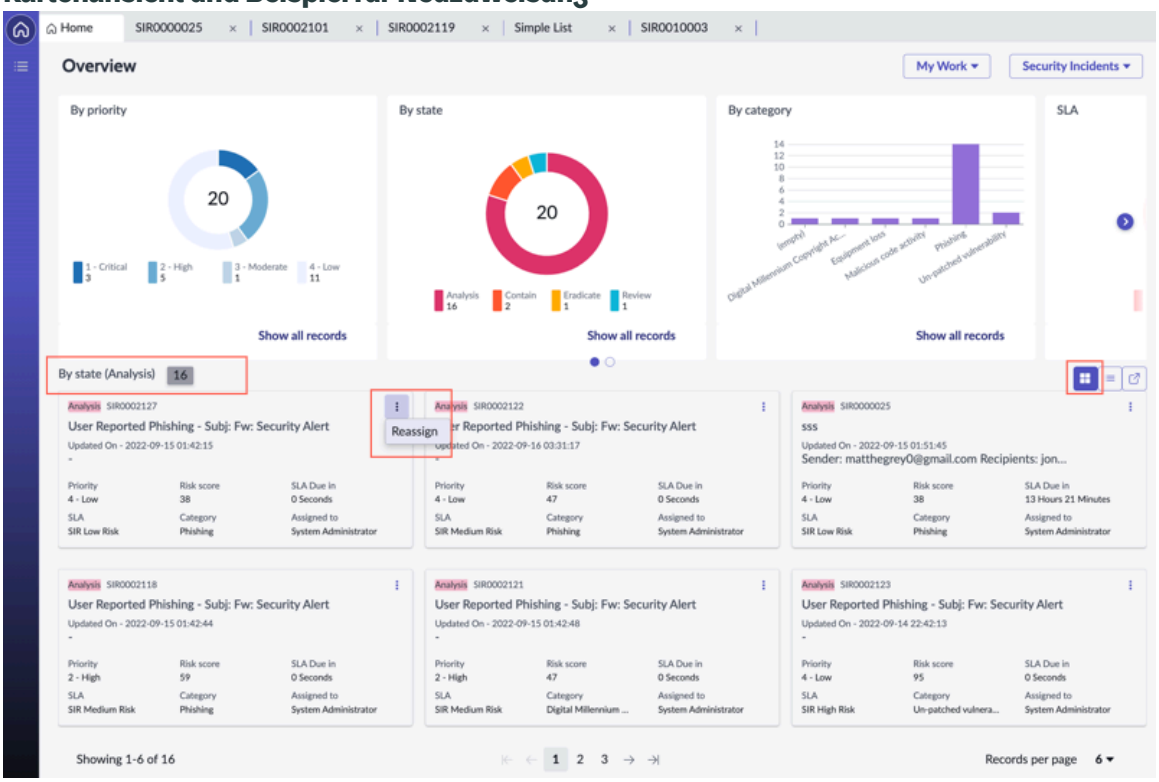
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichtsbereich



Sie können die Security Incidents oder Antwortaufgaben direkt aus dieser Ansicht zuweisen oder erneut zuweisen, indem Sie auf das Symbol mit den Auslassungspunkten klicken und **Zuweisen** (Option in Kartenansicht) oder direkt die Schaltfläche **Zuweisen** (Option in Listenansicht) auswählen, um einen Incident zuzuweisen.

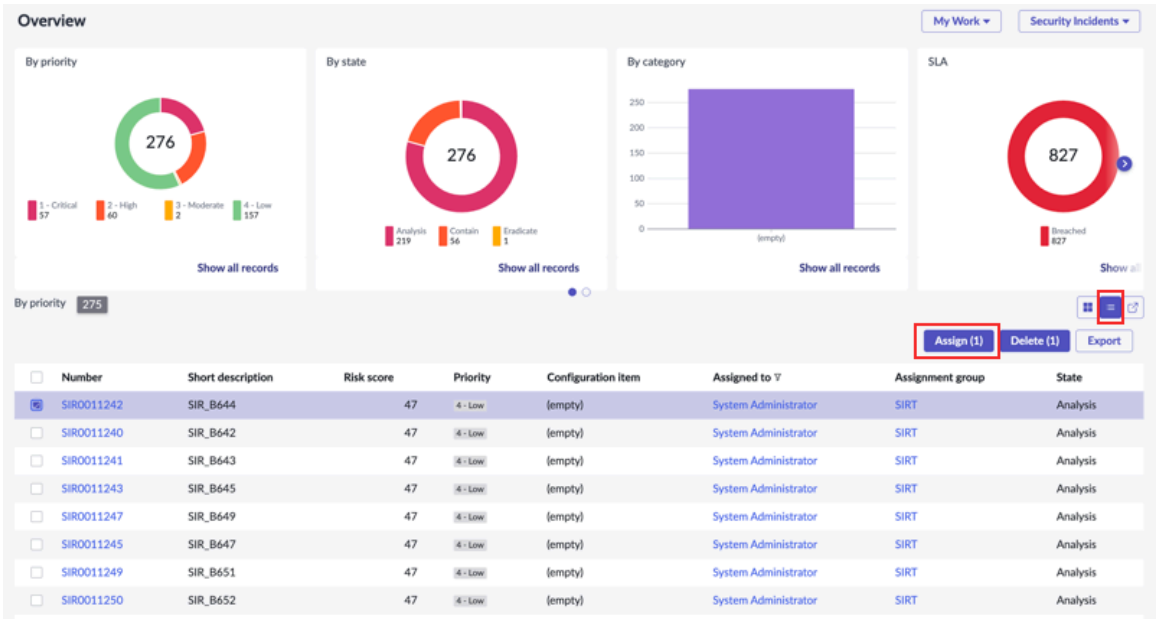
Kartenansicht und Beispiel für Neuzuweisung



Automatische Übersetzung

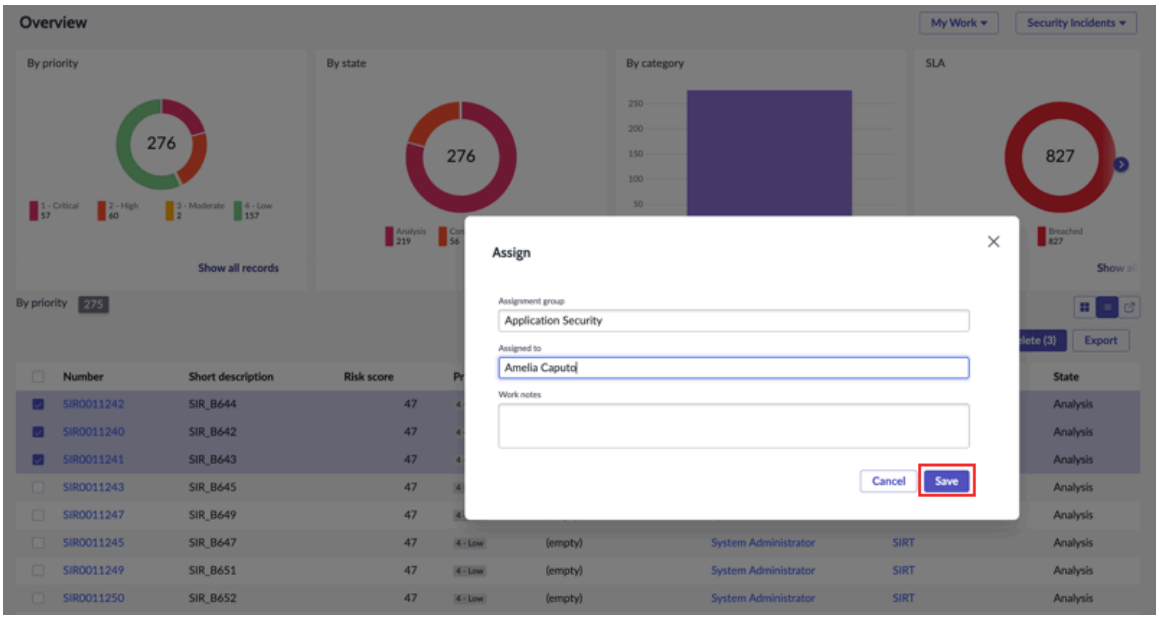
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incident zuweisen



Hier ist ein Beispiel für die Listenansicht. Der Benutzer kann Incidents auch in der Listenansicht zuweisen.

Incident zuweisen



Fügen Sie die Beauftragtendetails wie Zuweisungsgruppe und Zugewiesen an hinzu, oder ändern Sie sie, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.

Hinweis:

Sie können den Zuweisungsgruppen einen oder mehrere Security Incidents oder Antwortaufgaben zuweisen. Die ausgewählte Nummer wird auf der **Schaltfläche** Zuweisen angezeigt.

Der Benutzer kann Security Incidents aus dieser Ansicht löschen. Klicken Sie auf die Schaltfläche **„Löschen“**, um den Security Incident zu löschen. Der Datensatz wird aus der Listenansicht gelöscht.

Der Anwender kann den Listeninhalt auch exportieren. Klicken Sie auf die Schaltfläche **Exportieren**, um die Liste im gewünschten Format zu exportieren.

Automatische Übersetzung

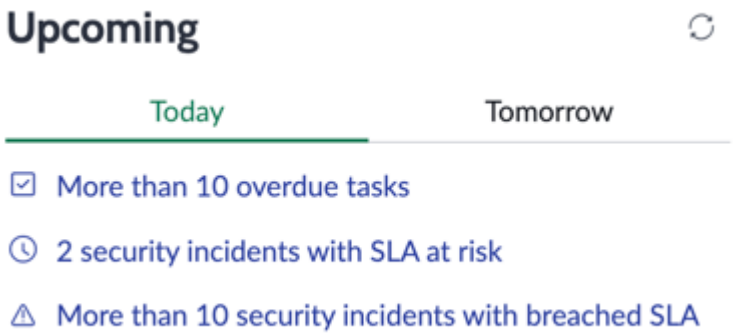
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Bevorstehend“

In diesem Abschnitt werden die bevorstehenden Aufgaben angezeigt, z. B. Security Incidents und Antwortaufgaben, die am selben Tag und am nächsten Tag fällig sind.

Die Liste mit Security Incidents und Antwortaufgaben, die angezeigt wird, basiert auf dem Feld für das Fälligkeitsdatum und der für diese Datensätze definierten SLA-Definition.

Wenn dieser Abschnitt mehr als einen Security Incident oder eine Antwortaufgabe enthält, werden durch den Incident oder die Datensätze alle diese Datensätze in einer neuen Registerkarte geöffnet.



Zeigen Sie bevorstehende Aufgaben an

Der Sicherheitsanalyst kann die bevorstehenden Aufgaben im Zusammenhang mit Security Incidents und Antwortaufgaben anzeigen, die fällig oder überfällig sind oder bei denen das definierte SLA verletzt wurde.

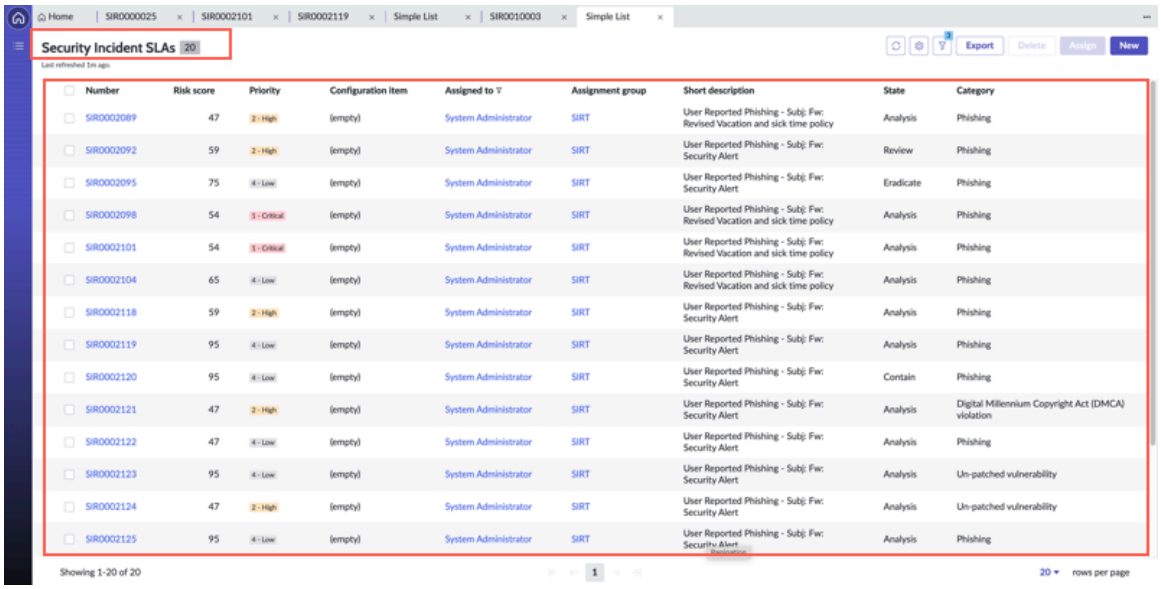
Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Bevorstehend**.
2. Klicken Sie auf die Registerkarte **Heute**, um die Aufgaben anzuzeigen, die am selben Tag fällig sind.
3. Wählen Sie die Registerkarte **Morgen**, um die Aufgaben anzuzeigen, die am nächsten Tag überfällig sind. Im nächsten Abschnitt werden die Security Incidents oder Antwortaufgaben aufgelistet, die basierend auf dem Fälligkeitsdatum überfällig sind und gegen die SLA-Definition verstoßen haben.
4. Klicken Sie auf **das Aktualisieren** -Symbol, um die Liste der bevorstehenden Abschnitte zu aktualisieren. Wenn Sie beispielsweise auf den Link **Mehr als 10 Security Incidents mit nicht eingehaltenem SLA** klicken, wird die Liste der Incidents mit SLA-Verstoß auf einer neuen Registerkarte im Arbeitsbereich angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Sie können in jeder Listenansicht Neu-, Zuweisungs-, Export- und Löschvorgänge ausführen.

Abschnitt „Quick-Links“

Quick-Links funktionieren wie Lesezeichen-Links. Sie können externe URLs hinzufügen und vom Arbeitsbereich aus schnell darauf zugreifen.

Arbeiten mit Quick-Links

Fügen Sie Quick-Links hinzu, um die Referenz zu erleichtern.

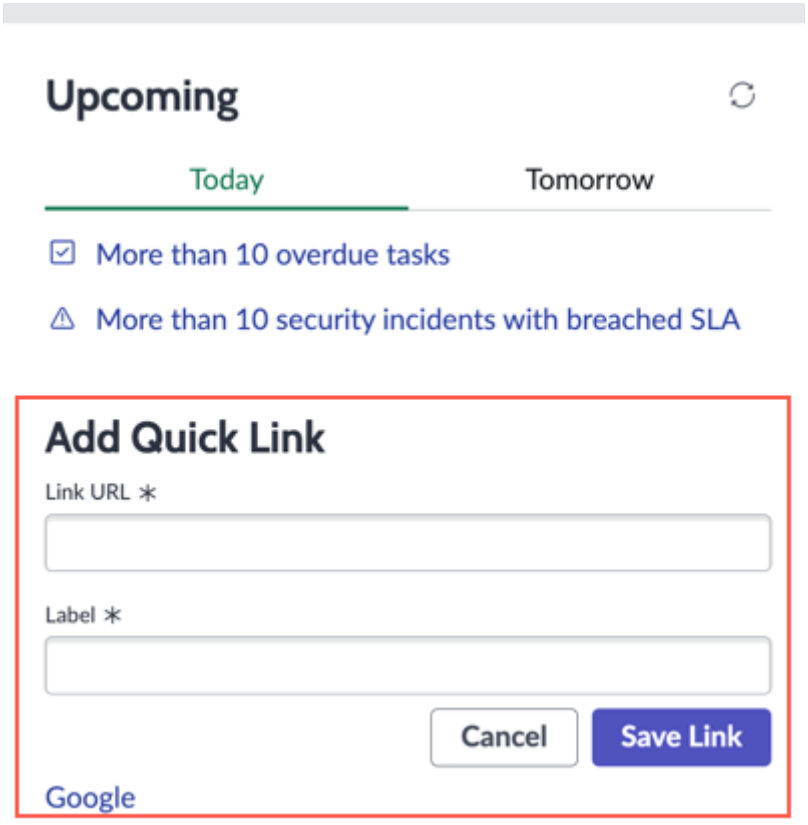
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Sie können nützliche Quick-Links hinzufügen und ändern und diese Links mit Lesezeichen versehen, um bei der Lösung von Incidents zu helfen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Quick-Links**.
2. Klicken Sie auf das Symbol **Quick-Link hinzufügen,** um die Links hinzuzufügen.
3. Geben Sie den Link zur URL und zur Bezeichnung ein.
4. Klicken Sie auf **Link speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der neue Link wird unter dem Abschnitt „Quick-Links“ hinzugefügt.

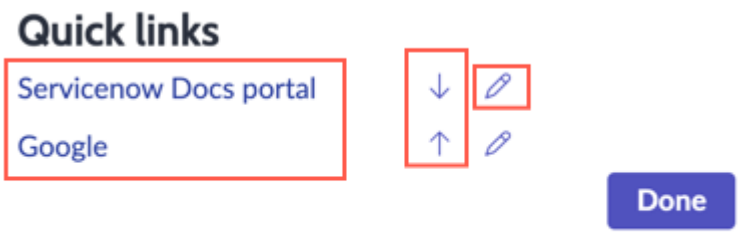
5. So ändern oder löschen Sie die Links:

a. Klicken Sie auf das Symbol **„Link bearbeiten“**.

b. Ändern Sie den gewünschten Link oder zeigen Sie den Text an, der die Bezeichnung der URL ist.

c. Klicken Sie auf **Speichern**.

d. Klicken Sie auf **Erledigt**.



e. Verwenden Sie die Aufwärts- und Abwärtspfeile, um die Position der Links zu verschieben.

f. Klicken Sie auf **Löschen**, um die mit Lesezeichen versehenen Links während der Bearbeitung zu löschen.

Automatische Übersetzung

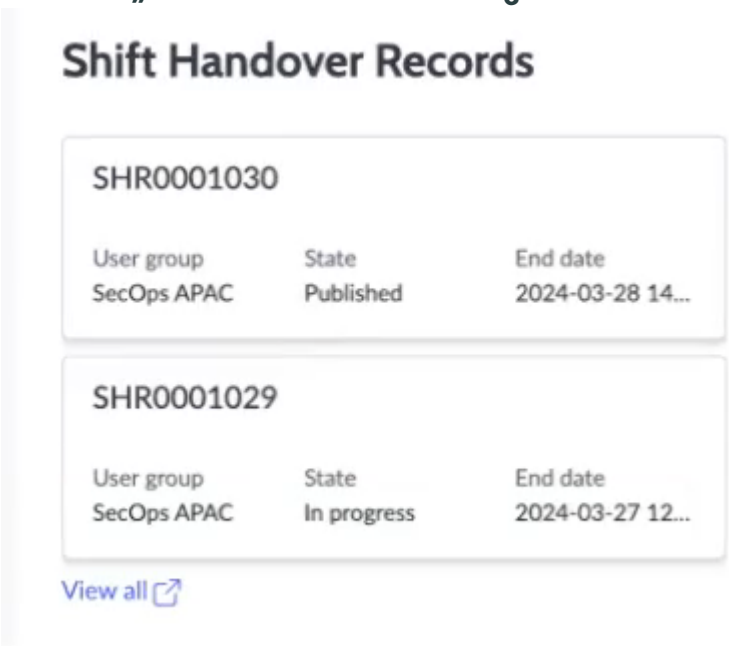
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Datensätze der Schichtübergabe“.

In diesem Abschnitt wird die Liste der Schichtübergabe-Datensätze im Security Incident Response-Arbeitsbereich angezeigt.

Im Abschnitt „Schichtübergabe-Datensätze“ im Security Incident Response-Arbeitsbereich werden die letzten beiden Schichtübergabe-Datensätze basierend auf den für diese Datensätze definierten Feldern „Enddatum“, „Status“ und „Anwendergruppe“ angezeigt. Um alle Schichtübergabedatensätze anzuzeigen, wählen Sie **Alle anzeigen**aus.

Abschnitt „Datensätze der Schichtübergabe“.



Listenansicht in SIR Workspace

Die Listenansicht besteht aus Security Incidents, Antwortaufgaben, Phishing-E-Mails und Bewertungen.

Auf die Listenansicht wurden bereits Filter angewendet, z. B. Mir zugewiesen, Dem Team zugewiesen, Nicht zugewiesen, Alle Offen, Alle usw.

Mit diesen Listenkategorien und gefilterten Listen können Analysten schnell die erforderlichen Datensätze zu Security Incidents und Reaktionsaufgaben finden, die sie bearbeiten müssen.

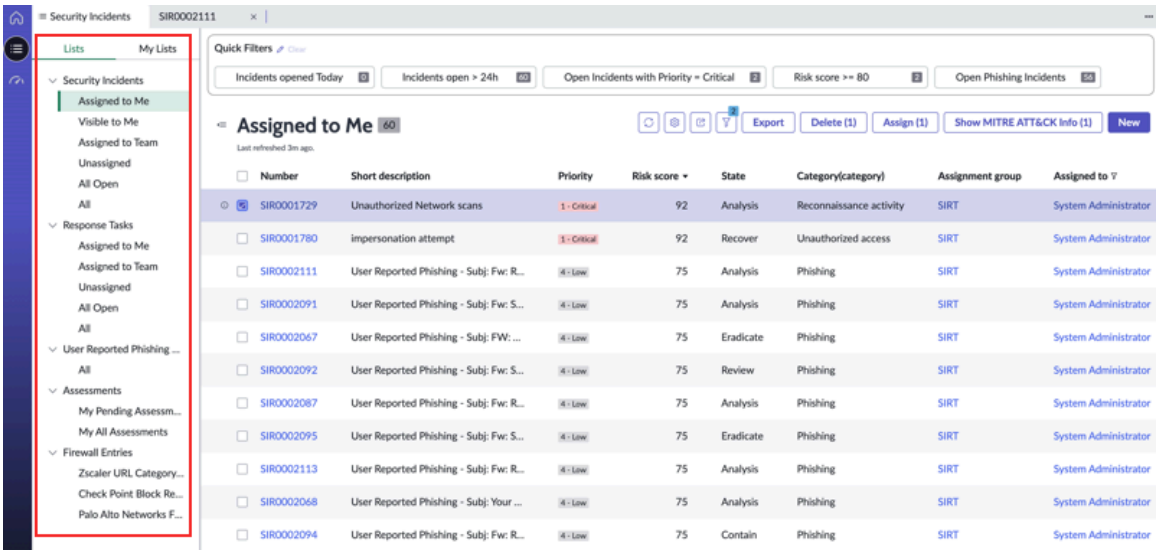
Um zur Listenansicht zu gelangen, müssen Sie auf das Listensymbol ( ) klicken. Wenn Sie in einer Listenansicht auf einen Datensatz klicken, wird der Datensatz in einer neuen Registerkarte geöffnet.

Listentypen

Im Folgenden finden Sie eine Beispielansicht der -Listen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Listenbereich enthält die folgenden Abschnitte:

Listen

Listenelement	Beschreibung	Fähigkeit
Security Incidents	Zeigen Sie die Liste der Security Incidents an, und navigieren Sie zum gewünschten Incident, um mit der Bearbeitung zu beginnen. Die folgenden Listen sind verfügbar: • **Für mich sichtbar**: Security Incidents, die für den angemeldeten Benutzer sichtbar sind. • **Mir zugewiesen**: Security Incidents, die dem Analysten zugewiesen sind. • **Dem Team zugewiesen**: Security Incidents, die allen Teams zugewiesen sind, denen der Analyst angehört. • **Nicht zugewiesen**: Liste der nicht zugewiesenen Security Incidents. • **Alle offenen**: Liste aller offenen Security Incidents. • **Alle**: Liste aller Security Incidents.	• In der Listenansicht kann der Analyst die Liste der Spalten konfigurieren, indem er auf das Zahnradsymbol klickt, das über den Incident-Spalten verfügbar ist. • Der Analyst kann einen oder mehrere Security Incidents auswählen und diese Incidents den anderen Benutzern zuweisen. • Der Analyst kann die Security Incidents löschen. • Der Analyst kann einen neuen Security Incident erstellen. • Der Analyst kann die Schnellfilter anwenden. Wenden Sie die Filter an, indem Sie auf die Option **„Schnellfilter“** klicken, anstatt die Option „Erweiterter **Filter“** zu verwenden. Mit den Schnellfiltern können Sie die Liste der Security Incidents, die sofortige Aufmerksamkeit erfordern, schnell filtern. Weitere

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Fähigkeit
		Informationen finden Sie unter Arbeiten mit Schnellfiltern. • Die Analysten können die Liste der Incidents aktualisieren. • Der Analyst kann die Listenansicht in die Formate Excel, CSV, JSON und PDF exportieren.
Schichtübergabedatensätze	Zeigen Sie die Liste der Schichtübergabe-Datensätze an. Die folgenden Listen sind verfügbar: • **Dem Team zugewiesen**: Schichtübergabe-Datensätze, die allen Teams/Anwendergruppen zugewiesen sind, denen die Analysten angehören. • **Alle**: Liste aller Security Incidents.	Die Schichtübergabe unterstützt die folgenden drei Rollen: • Administrator: Schichtbesitzerrolle • Sicherheitsanalyst: Analystenrolle für Schichten • Sicherheitsmanager: Schichtbesitzerrolle, hat jedoch keinen Zugriff auf die Anwendergruppe, der der Datensatz „Schichtübergabe“ zugewiesen ist. • Benutzer mit der Rolle „Schichtbesitzer/ Analyst“, die Teil der Benutzergruppe in der aktiven Schicht sind, können in den Schichtübergabedatensätzen im Entwurfsstatus Inhalte hinzufügen oder ändern. • Benutzer, die nicht über die Rolle „Schichtbesitzer/ -Analyst“ verfügen oder nicht Teil der Benutzergruppe in der aktiven Schicht sind, können nur den Inhalt in den Schichtübergabe-Datensätzen anzeigen.
Antwortaufgaben	Zeigen Sie die Liste der Antwortaufgaben an, und navigieren Sie zur gewünschten Antwortaufgabe, um mit der	• In der Listenansicht kann der Analyst die Liste der Spalten konfigurieren, indem er auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Fähigkeit
	Bearbeitung zu beginnen. Die Listenansicht enthält: • **Mir zugewiesen**: Antwortaufgaben, die dem Analysten zugewiesen sind. • **Dem Team zugewiesen**: Antwortaufgaben, die den Teams zugewiesen sind, zu denen die Analysten gehören. • **Nicht zugewiesen**: Liste der nicht zugewiesenen Antwortaufgaben. • **Alle offenen**: Liste aller offenen Antwortaufgaben. • **Alle**: Liste aller Antwortaufgaben.	das Zahnradsymbol klickt, das über den Incident-Spalten verfügbar ist. • Der Analyst kann eine oder mehrere Antwortaufgaben auswählen und diese Aufgaben anderen Benutzern zuweisen. • Der Analyst kann eine neue Antwortaufgabe erstellen. • Der Analyst kann die Schnellfilter anwenden. Wenden Sie die Filter an, indem Sie auf die Option **„Schnellfilter“** klicken, anstatt die Option „Erweiterter **Filter“** zu verwenden. Mit den Schnellfiltern können Sie die Liste der Antwortaufgaben, die sofortige Aufmerksamkeit erfordern, schnell filtern. • Die Analysten können die Liste der Antwortaufgaben aktualisieren. • Der Analyst kann die Listenansicht in die Formate Excel, CSV, JSON und PDF exportieren. Weitere Informationen finden Sie unter Exportieren Sie Security Incidents oder Antwortaufgaben.
Phishing-E-Mails	Zeigen Sie die Liste aller Phishing-E-Mails an. Die Listenansicht wird basierend auf der letzten Aktualisierung sortiert.	• Phishing-E-Mail melden. Weitere Informationen zum Melden einer Phishing-E-Mail finden Sie unter Phishing-E-Mail melden. • Löschen Sie Phishing-E-Mails. • Exportieren Sie die Listenansicht der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Fähigkeit
		Phishing-E-Mails in die Formate Excel, CSV, JSON und PDF.
Bewertungen	Zeigen Sie die Liste der Bewertungen an, die für die Überprüfung nach Incidents erforderlich sind. • **Meine ausstehenden Bewertungen**: Liste der ausstehenden Bewertungen. • **Meine alle Bewertungen**: Liste aller Bewertungen.	Nehmen Sie Bewertungen vor.

Personalisieren Sie eine Liste

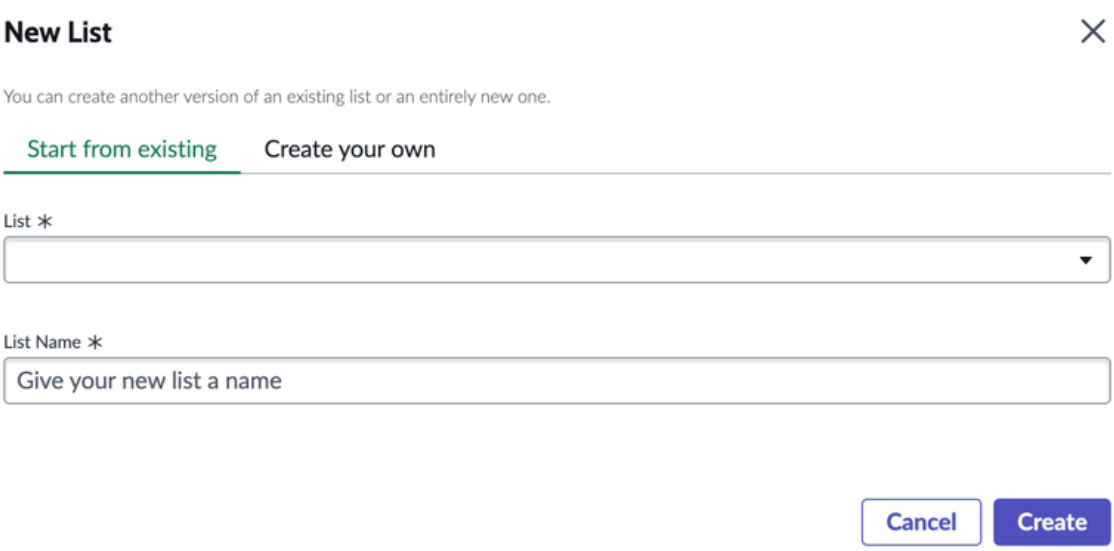
Sicherheitsanalysten oder -manager können die anwenderdefinierte Listenansicht für Security Incidents, Antwortaufgaben oder Phishing-E-Mails basierend auf ihren individuellen Einstellungen personalisieren.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf **Listenansicht**.
3. Klicken **Meine Listen**.
4. Klicken Sie auf **Neue Liste hinzufügen**, verfügbar unten in der Ansicht **Meine Listen**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsanalysten können entweder eine andere Version einer vorhandenen Liste oder eine komplett neue anwenderdefinierte Liste erstellen.

5. **So erstellen Sie aus einer vorhandenen Listenansicht:**

   a. Klicken Sie auf den Link **Von vorhandener beginnen**.

   b. Wählen Sie die **Liste** aus der Dropdown-Liste aus.

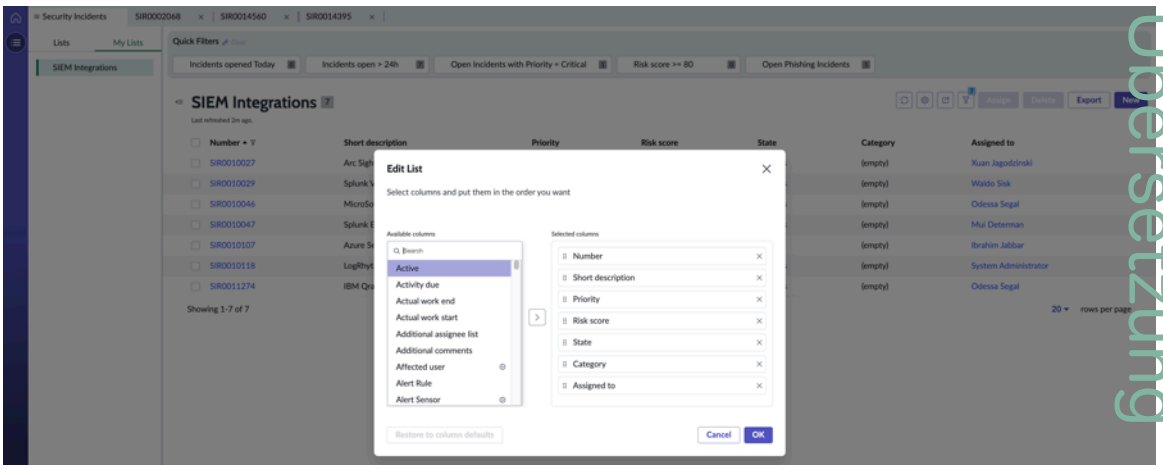
   > **Hinweis:**
   > Welche Liste Sie auch immer aus der Dropdown-Liste auswählen, der Listenname ist die Kopie Ihrer Hauptliste. Wenn Sie beispielsweise im Abschnitt „Security Incidents“ **Mir zugewiesen** auswählen, wird der Listenname „ **Mir zugewiesen“ Kopie** des Abschnitts „Security Incidents“.

   c. Wählen Sie die zu personalisierenden Spalten aus, und fügen Sie Filter hinzu.
   Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und (einen) Wert/e enthalten.

   d. Klicken Sie auf **Erstellen**.

   > **Hinweis:**
   > Um Ihre eigene Listenansicht anzupassen, können Sie anwenderdefinierte Spalten und Filter hinzufügen, Bedingungen festlegen und nach Bedarf nach Reihenfolge sortieren.

   e. Nachdem eine personalisierte Listenansicht erstellt wurde, klicken Sie auf das Zahnradsymbol, und passen Sie die Listenspalten an, indem Sie die Option **Spalten bearbeiten** wählen, um die Spalten zu bearbeiten und in die gewünschte Reihenfolge zu bringen.



Sie haben auch die folgenden Möglichkeiten:

- **Benennen Sie** die personalisierte Listenansicht um.
- **Löschen Sie** die personalisierte Listenansicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Speichern Sie die personalisierte Listenansicht wie gewünscht mit der Option **Speichern unter**.
- **Setzen Sie die Breite der Listenansicht zurück**.

Hinweis:
Sie können diese Vorgänge auch direkt über die anderen bereitgestellten Listenaktionen-Schaltflächen wie Zuweisen, Löschen und Exportieren der Listenansicht ausführen.

6. So erstellen Sie eine eigene Liste:

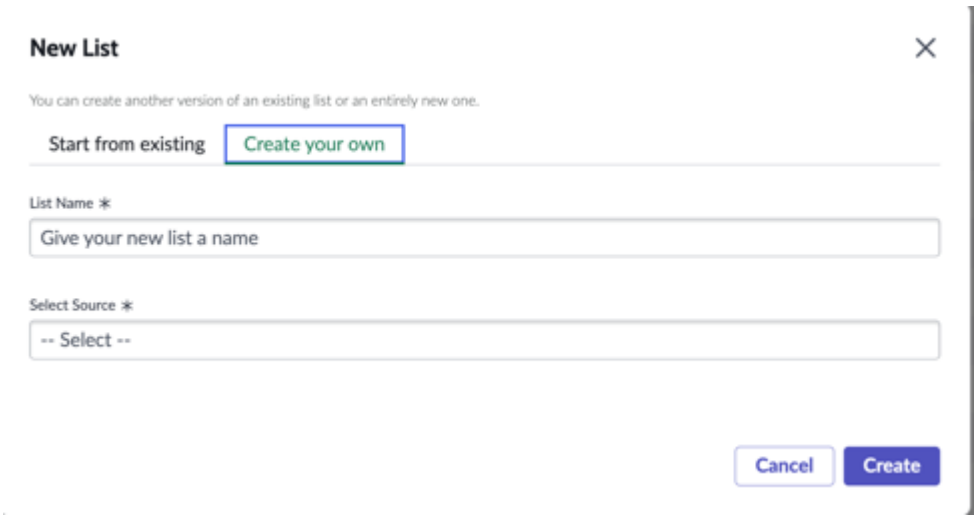
a. Klicken Sie auf den Link **Selbst erstellen**.

b. Geben Sie einen **Listennamen**an.

c. Wählen Sie die **Quelle** und **die Spalten**aus.

d. Fügen Sie Filter hinzu.
Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, und geben Sie die Reihenfolge an, in der die Liste angezeigt werden soll.

e. Klicken Sie auf **Erstellen**.



Eine neue Liste wird entsprechend Ihrer Definition und Anpassung im Abschnitt **„My Lists“** (Meine Listen) erstellt.

Hinweis:
können Sie Ihre personalisierte Ansicht **neu anordnen,** indem Sie ihre Positionen verschieben.

Security Incidents zuweisen

Security Incidents zuweisen.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Prozedur

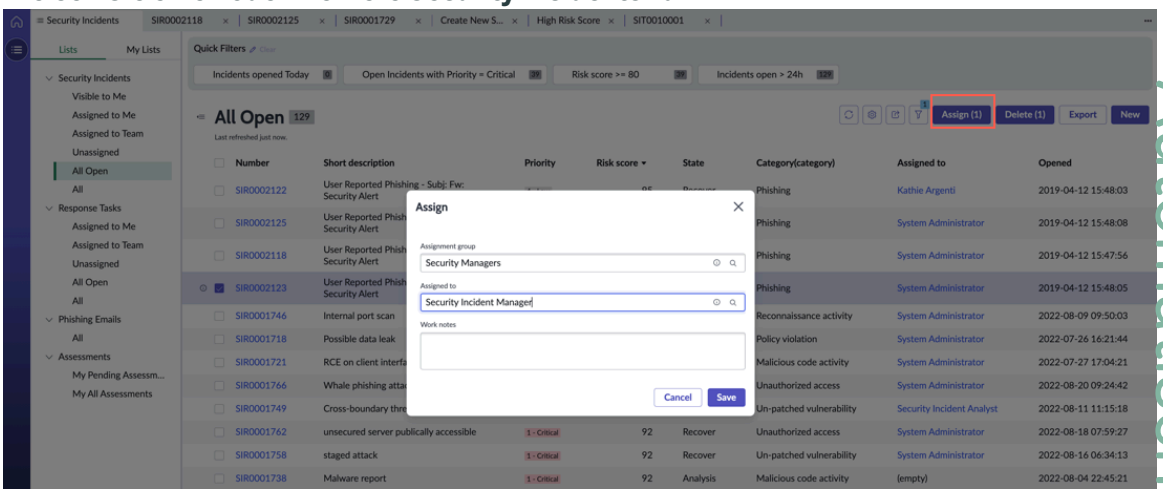
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.

2. Klicken Sie auf das Listensymbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Listen**.
4. Wechseln Sie beispielsweise zu **Security Incidents** > **Alle offen**.
5. Wählen Sie einen oder mehrere Security Incidents aus.
6. Klicken Sie auf **Zuweisen**.
7. Füllen Sie die Details wie Zuweisungsgruppe, Zugewiesen an aus, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.
   Der Incident wird dann dem Benutzer zugewiesen.
8. Klicken Sie auf **Speichern**.

Weisen Sie einen oder mehrere Security Incidents zu



Antwortaufgaben zuweisen

Weisen Sie Antwortaufgaben für ein Sicherheitsproblem zu.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

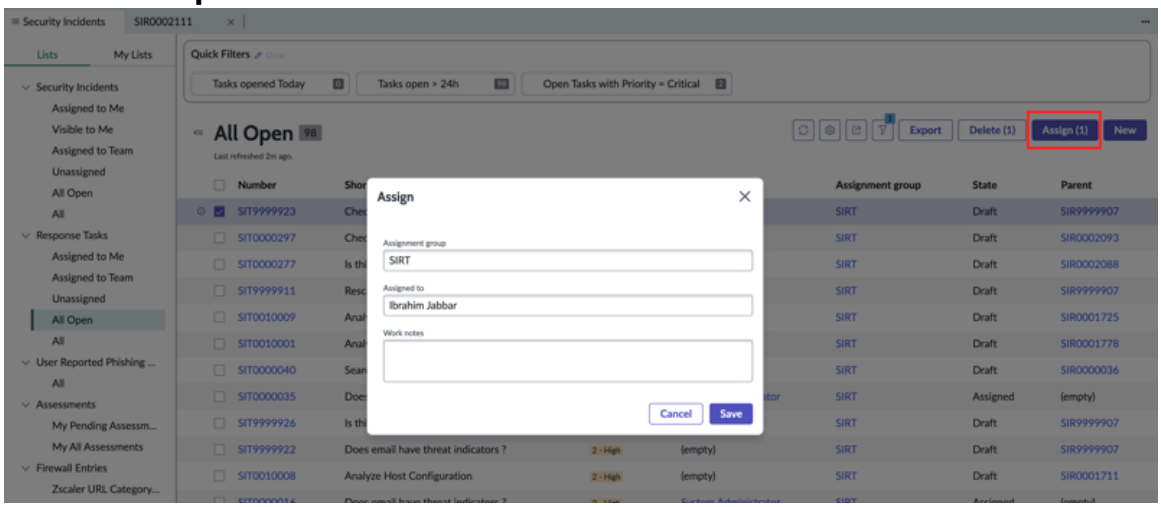
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol ( ).
3. Klicken Sie auf **Listen**.
   Wechseln Sie beispielsweise zu **Antwortaufgaben** > **Alle offen**.
4. Wählen Sie eine oder mehrere Antwortaufgaben aus.
5. Klicken Sie auf **Zuweisen**.
6. Füllen Sie die Details wie Zuweisungsgruppe, Zugewiesen an aus, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.
   Der Incident wird dann dem Benutzer zugewiesen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Speichern**.



Phishing-E-Mail melden

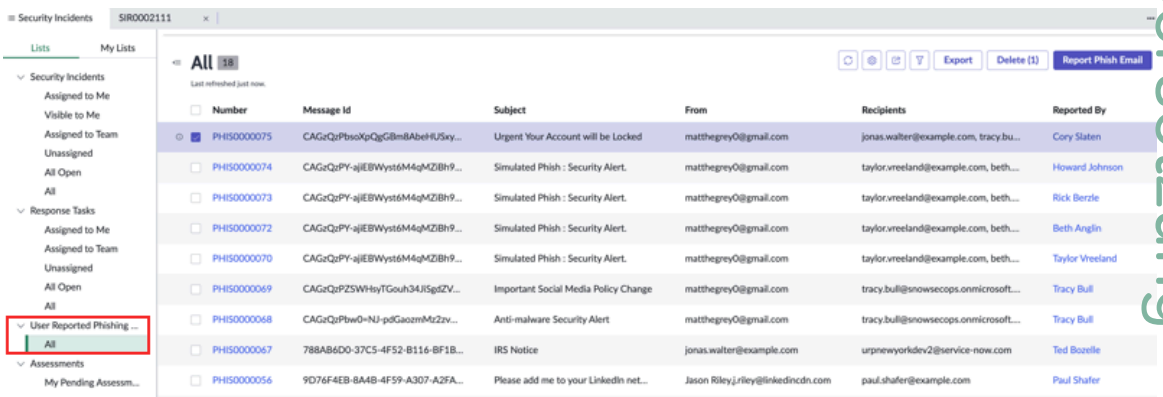
Melden Sie Phishing-E-Mails aus der Listenansicht.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol ( ).
3. Gehe zu **Vom Anwender gemeldete Phishing-E-Mails** > **Alle**.
   Die Liste der vom Anwender gemeldeten Phishing-E-Mails wird angezeigt.



4. Klicken Sie auf die Schaltfläche **Phishing-E-Mail melden**.
   Melden Sie eine Phishing-E-Mail, indem Sie sie hochladen.
5. Klicken Sie auf **Datei hinzufügen**, um Anhänge hinzuzufügen.
6. Klicken Sie auf **Hochladen**.

Hinweis:
Melden Sie eine Phishing-E-Mail, indem Sie die Anhänge hochladen. Sie können jeweils nur eine Phishing-E-Mail hochladen. Diese muss im EML-Format vorliegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Absenden**.
   Die Phishing-E-Mail zum Protokollieren eines Security Incident wird erstellt.

Arbeiten mit Schnellfiltern

Schnellfilter sind leicht zugängliche Filter, die in den Listen, Security Incidents und Reaktionsaufgaben verfügbar sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

SIR Workspace bietet eine Schnellfilterfunktion, mit der Sie die Liste der Security Incidents oder Antwortaufgaben einfach filtern können.

Sie können Schnellfilter verwenden, um neue Filter zu konfigurieren oder vorhandene Filter zu ändern, die in diesen Listen angezeigt werden. Das Basissystem bietet die folgenden Schnellfilter für jeden Security Incident:

- **Heute geöffnete Incidents**
- **Offene Incidents > 24 Stunden**
- **Offene Incidents mit Priorität = Kritisch**
- **Risiko >= 80**
- **Offene Phishing-Incidents**

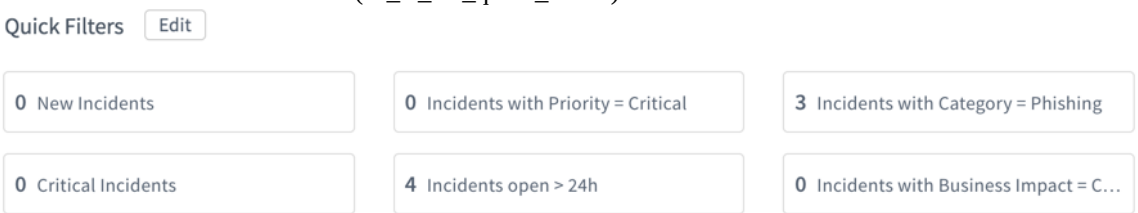
Das Basissystem bietet die folgenden Schnellfilter für jede Antwortaufgabe:

- **Aufgaben offen > 24 Stunden**
- **Offene Aufgaben mit Priorität = kritisch**

Hinweis:
Ein Administrator kann die erforderliche Liste von Schnellfiltern entsprechend den Organisationsanforderungen konfigurieren.

Prozedur

1. Navigieren zu **Systemdefinition** > **Tabellen**.
2. Suchen Sie nach **Schnellfiltern** (sn_si_aw_quick_filters).



3. Gehe zu **Zugehörige Links** > **Liste anzeigen** Abschnitt.
   Die Listenseite **„Schnellfilter“** wird angezeigt. OOTB, im Folgenden finden Sie die Liste der mit der Anwendung gelieferten Schnellfilter.

Name	Tabelle	Wert
Heute geöffnete Aufgaben	Security Incident-Aufgabe [sn_si_task]	wahr
Heute geöffnete Incidents	Security Incident [sn_si_incident]	wahr

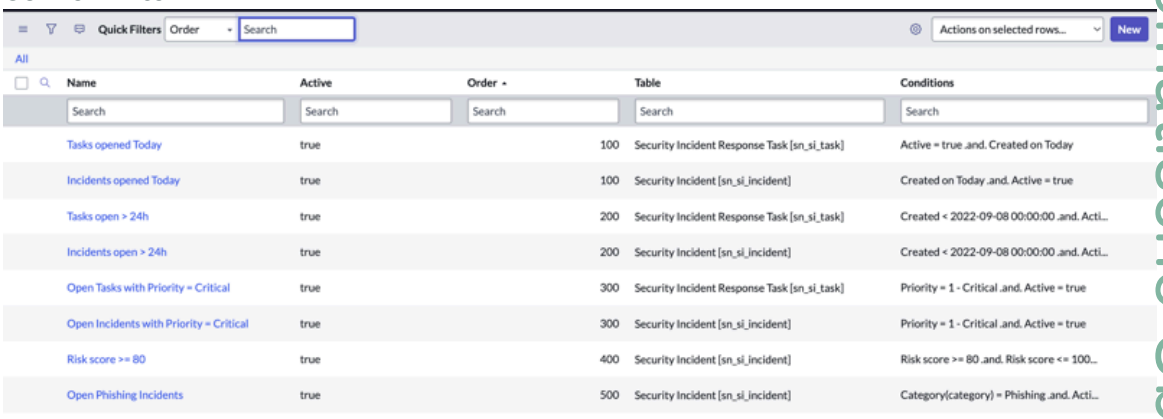
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

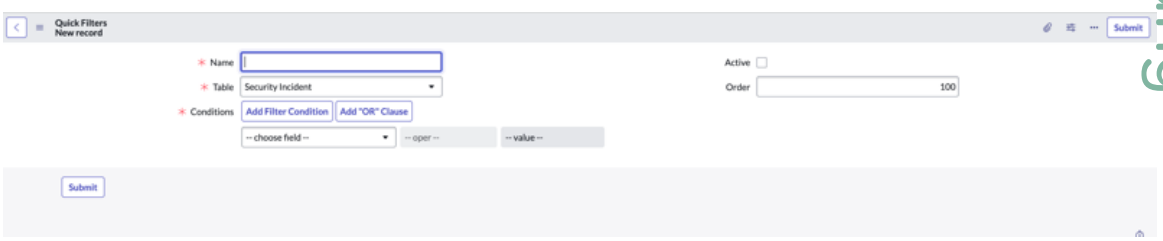
Name	Tabelle	Wert
Aufgaben offen > 24 Stunden	Security Incident Response-Aufgabe [sn_si_task]	wahr
Offene Incidents > 24 Stunden	Security Incident [sn_si_incident]	wahr
Offene Aufgaben mit Priorität = kritisch	Security Incident Response-Aufgabe [sn_si_incident]	wahr
Offene Incidents mit Priorität = kritisch	Security Incident [sn_si_incident]	wahr
Risikopunktzahl >= 80	Security Incident [sn_si_incident]	wahr
Offene Phishing-Incidents	Security Incident [sn_si_incident]	wahr

Hinweis:
Der Sicherheitsadministrator kann diese Schnellfilter konfigurieren. Je nach Geschäftsbedürfnis kann der Administrator den vorhandenen Wert in „false“ ändern und einen neuen Schnellfilter erstellen.

Schnell-Filter



4. Klicken Sie auf **Neu**, um einen neuen Filter zu erstellen.
5. Geben Sie einen Namen für den Filter ein, wählen Sie die Tabelle aus, und geben Sie die Filterbedingung an.
6. Klicken Sie auf **Senden**, um zur vorherigen Listenseite zurückzukehren.
   Der neu hinzugefügte Filter wird auf der Seite aufgelistet.



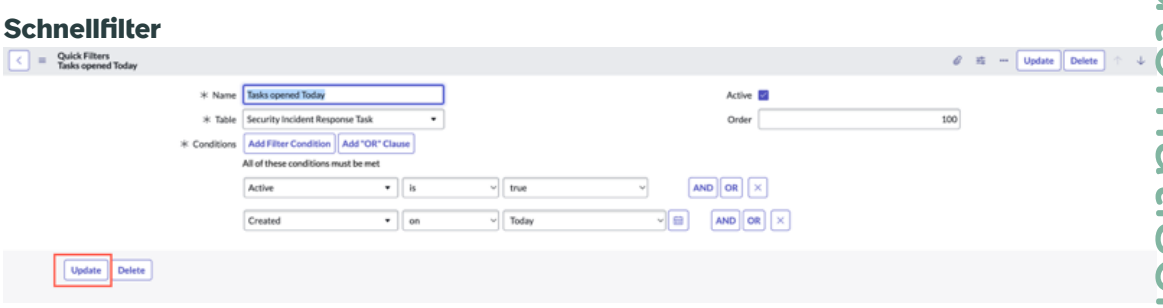
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Der Schnellfilter ist nur anwendbar, wenn das Kontrollkästchen **Aktiv** aktiviert ist.
- Im Arbeitsbereich kann jeder angemeldete Benutzer die in der Anwendung verfügbaren aktiven Schnellfilter personalisieren. Benutzer können die neu erstellten Schnellfilter ein- oder ausblenden. Diese Funktion basiert auf ihren Anwendereinstellungen.
- Wenn ein Benutzer die Einstellungen für Schnellfilter geändert hat und danach ein neuer Schnellfilter erstellt wird und der Schnellfilter auf aktiv festgelegt ist, gilt er nicht für die Einstellung des Benutzers. Der Benutzer muss die Einstellungen in der personalisierten Ansicht manuell ändern.

7. Wählen Sie einen vorhandenen Filterdatensatz aus, um die vorhandenen Schnellfilter zu ändern.
8. Ändern Sie den Namen und die Filterbedingung.
9. Klicken Sie auf **Aktualisieren**.



Schnellfilter hinzufügen oder ändern

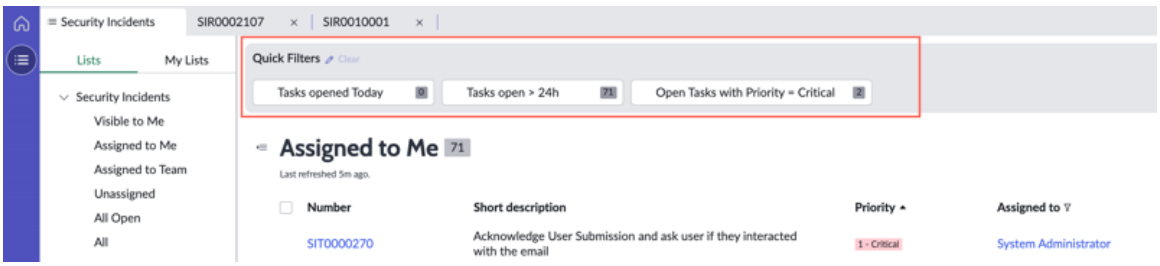
Fügen Sie in der Listenansicht Schnellfilter für Security Incidents oder Antwortaufgaben hinzu, oder ändern Sie sie.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol ( ).
3. Wechseln Sie beispielsweise zu **Listen** > **Security Incidents** > **Schnell-Filter** Abschnitt.

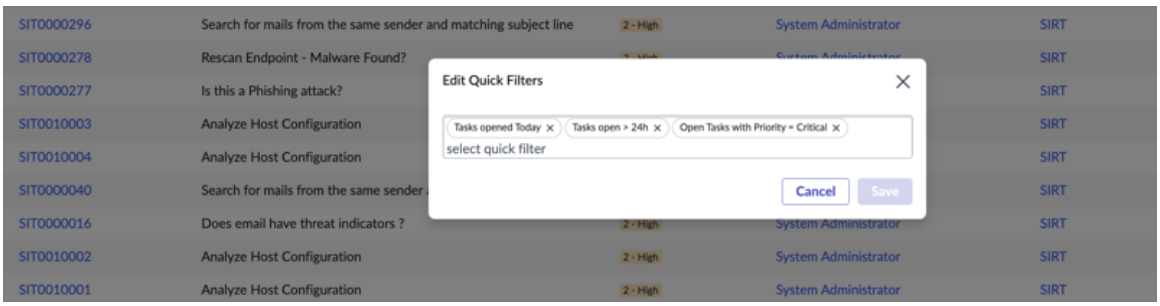


4. Klicken Sie auf das **Bearbeitungssymbol**, um die Änderungen vorzunehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die von Ihnen vorgenommene Änderung wird beibehalten. Wenn der Anwender das nächste Mal zu dieser Seite zurückkehrt, wird die beibehaltene Einstellung angezeigt.



5. Klicken Sie auf **Speichern**.

Exportieren Sie Security Incidents oder Antwortaufgaben

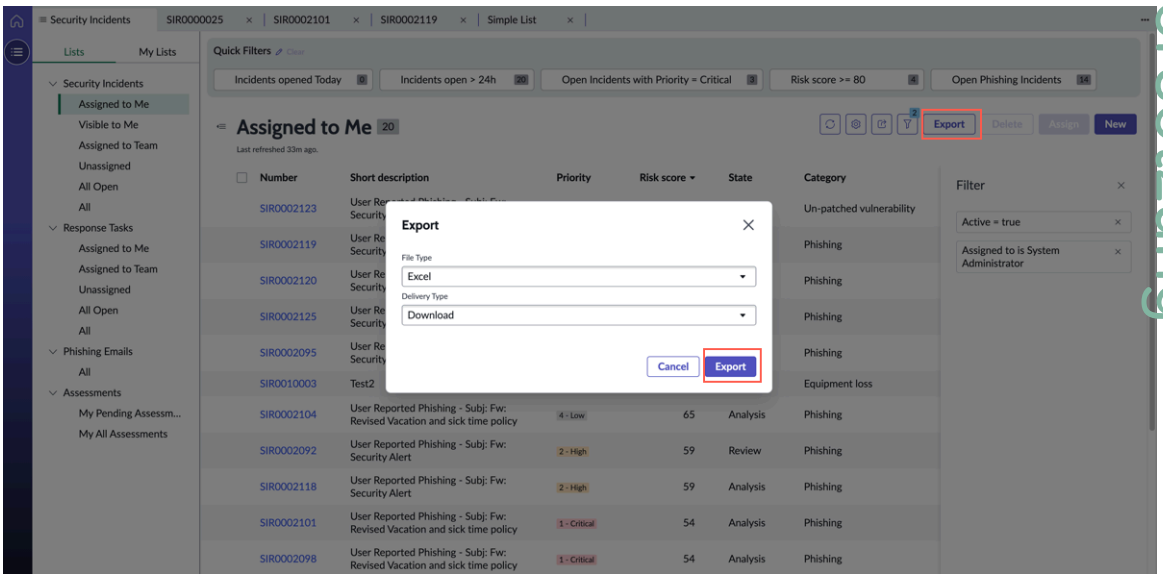
Exportieren Sie die Security Incidents oder Antwortaufgaben aus der Listenansicht.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol .
3. Klicken Sie auf **Listen**.
4. Gehe zu **Security Incidents oder Antwortaufgaben** > **Alle offen**.
5. Zeigen Sie die Liste an, und klicken Sie auf **Exportieren**.



6. Wählen Sie den **Dateityp** und **den Bereitstellungstyp**aus.
   Beispiel: **Excel** und **Download** oder **E-Mail senden** der Liste.
7. Klicken Sie auf **Exportieren**.
   Die Datei wird je nach gewählter Option heruntergeladen oder per E-Mail gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Schichtübergabe-Datensätze

Verwenden Sie die Listenansicht der Schichtübergabe-Datensätze zum Erstellen, Bearbeiten, Kopieren oder Löschen von Schichtübergabe-Datensätzen. Jeder Schichtübergabedatensatz ist einer Vorlage für den Schichtübergabebericht zugeordnet.

Vorbereitungen
Erforderliche Rolle:

- sn_escm_sh.shift_analyst: Mindestanforderung für den Zugriff auf die Schichtübergabe-Datensätze.
- sn_escm_sh.shift_owner: Übergabeprotokolldatensätze in den Anwendergruppen erstellen, bearbeiten und löschen, denen der Schichtbesitzer angehört. Diese Rolle erbt die Rolle sn_escm_sh.shift_analyst.
- sn_escm_sh.shift_analyst: Zeigt alle Protokolldatensätze der Schichtübergabe an, kann jedoch nur zu laufenden Schichtübergabedatensätzen beitragen, die der Gruppe des Schichtanalysten zugewiesen sind.
- sn_si.analyst: Erbt die Rolle sn_escm_sh.shift_analyst.
- sn_si.admin: Erbt die Rolle sn_escm_sh.shift_admin.
- sn_escm_sh.shift_admin: Erbt die Rolle sn_escm_sh.shift_owner

Wichtig:
Wie Sie als Administrator die Schichtübergabe-Vorlage konfigurieren, erfahren Sie unter Konfigurieren Sie Schichtübergabevorlagen.

Warum und wann dieser Vorgang ausgeführt wird
Der Schichtbesitzer und das entsprechende Team bzw. die entsprechende Benutzergruppe erstellen die Protokolldatensätze für die Schichtübergabe. Der Schichtbesitzer muss die Schichtübergabevorlage und die Anwendergruppe auswählen, die am Schichtübergabebericht arbeiten soll. Nachdem der Schichtübergabebericht abgeschlossen ist, wird er für den nächsten aktiven Schichtbesitzer und das nächste aktive Team freigegeben.

Wichtige Punkte der Vorlage „Schichtübergabe“:

- Wenn ein anderer Analyst aus dem aktiven Schichtteam den Bericht bereits vor Ihnen aktualisiert hat und Änderungen verarbeitet werden, wird möglicherweise eine Fehlermeldung angezeigt, dass Inhaltsaktualisierungen ausstehen. Sie müssen 30 Sekunden warten und dann **Change zu Status „Überprüfen“** erneut auswählen. Im rechten Bereich können Sie sehen, wie der konsolidierte Bericht mit den aktualisierten Inhalten anderer Analysten aktualisiert wird.
- Wenn der Schichtbesitzer den Inhalt in einem Abschnitt im Status Überprüfung geändert hat, wird derselbe Inhalt für den Analysten übernommen, wenn der Datensatz zurück in den Status In Bearbeitung wechselt.
- Der Schichtbesitzer muss beim Bearbeiten des Inhalts im Überprüfungsstatus und beim Ausführen von Aktionen wie dem Zusammenführen von zwei Zeilen, dem Zusammenführen von zwei Abschnitten oder dem Entfernen eines Abschnitts vorsichtig sein, da dies Auswirkungen auf den Schichtübergabebericht der anderen Analysten hat.
- Nach der Veröffentlichung des Schichtübergabeberichts kann der Schichtbesitzer den Inhalt ändern, aber nicht den Datensatzstatus ändern.

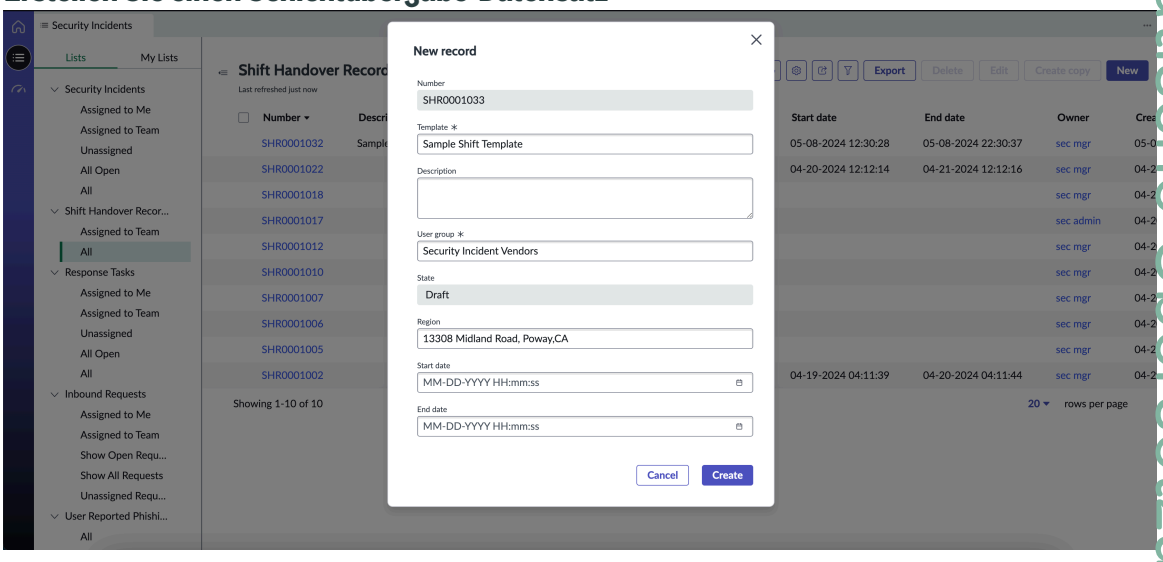
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn jemand den Inhalt ändert und während dieser Zeit der Datensatzstatus von In Bearbeitung in Überprüfung geändert wird, werden die nicht gespeicherten Inhaltsänderungen verworfen.
- Der Schichtadministrator hat unabhängig von den Anwendergruppen Schreibzugriff auf alle Datensätze der Schichtübergabeprotokolle.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen Sie das Listensymbol Security Incident- .
3. Wählen Sie auf der **Registerkarte Listendie Option Schichtübergabe-Datensätze**aus.
4. Wählen Sie **Alle Datensätze** aus, um die Liste aller Schichtübergabe-Datensätze anzuzeigen.
5. Wählen Sie **Dem Team zugewiesen aus,** um die Liste der Schichtübergabe-Datensätze anzuzeigen, die allen Teams/Benutzergruppen zugewiesen sind, denen die Analysten angehören.
6. Um einen neuen Schichtübergabe-Datensatz zu erstellen, wählen Sie **Neu**.
7. Füllen Sie die Felder im Formular aus.

Erstellen Sie einen Schichtübergabe-Datensatz

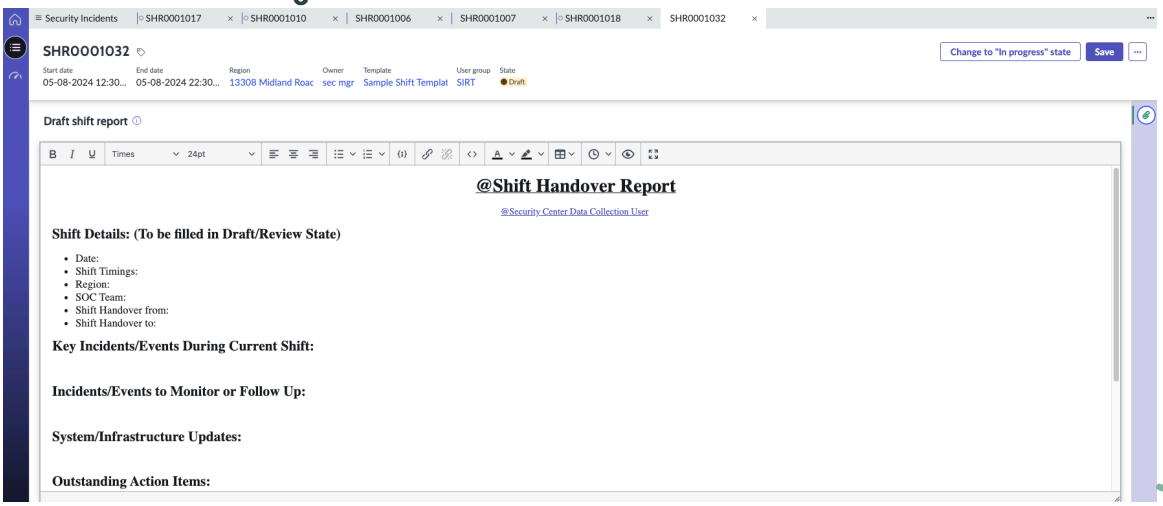


8. Wählen Sie **Erstellen** aus.
   Ein neuer Schichtübergabe-Datensatz wird basierend auf der Vorlage erstellt, die Sie ausgewählt und der Listenansicht hinzugefügt haben.
9. Öffnen Sie den neuen Schichtübergabe-Datensatz, um den Status und die Details der Security Incidents im Schichtübergabe-Bericht zu aktualisieren.
   Standardmäßig befindet sich der Schichtübergabe-Datensatz im Status **Entwurf**.

Hinweis:
Nur der Schichtbesitzer kann den Inhalt ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhalt des Schichtübergabeberichts



10. Verwenden Sie im Editor für Schichtberichte-Entwürfe die Abschnitte mit den Berichtsvorlagen für Schichtübergaben, um die Details der Security Incidents und Benutzer zu aktualisieren.

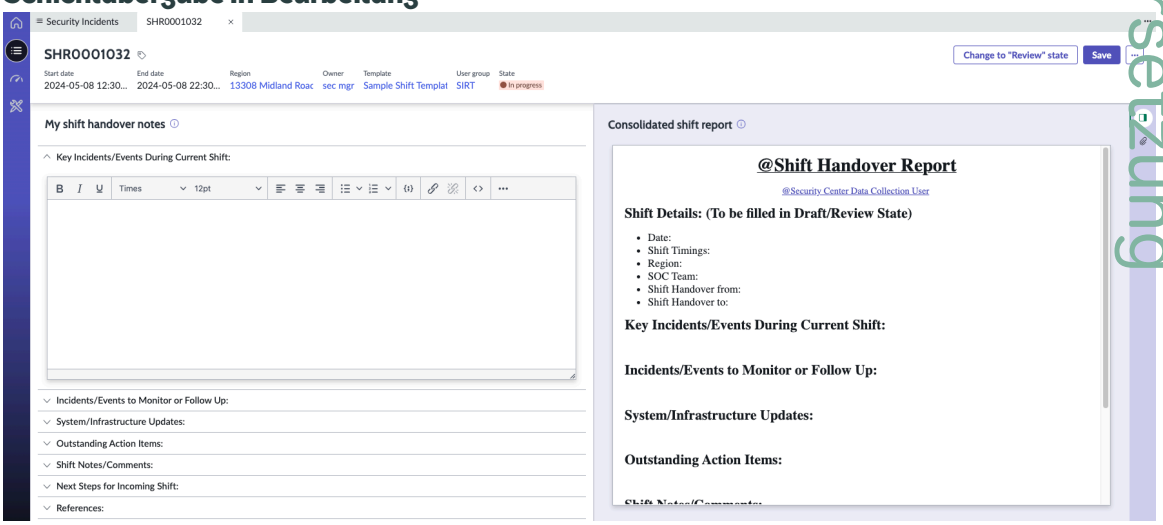
Sie können Ihren Bericht mit allen Optionen des Editors formatieren, z. B. Schriftarten, Farben, Aufzählungszeichen, Links und Anhänge.

Hinweis:
Sowohl der Schichtbesitzer als auch der Schichtanalyst können den Inhalt ändern.

a. Nachdem Sie die erforderlichen Änderungen am Schichtübergabebericht vorgenommen haben, wählen Sie **Speichern**aus.

b. Wählen Sie die Aktion **„Zu Status „In Bearbeitung“ ändern“**, um den Datensatz der Schichtübergabe in den Status „In Bearbeitung“ zu versetzen.

Schichtübergabe in Bearbeitung



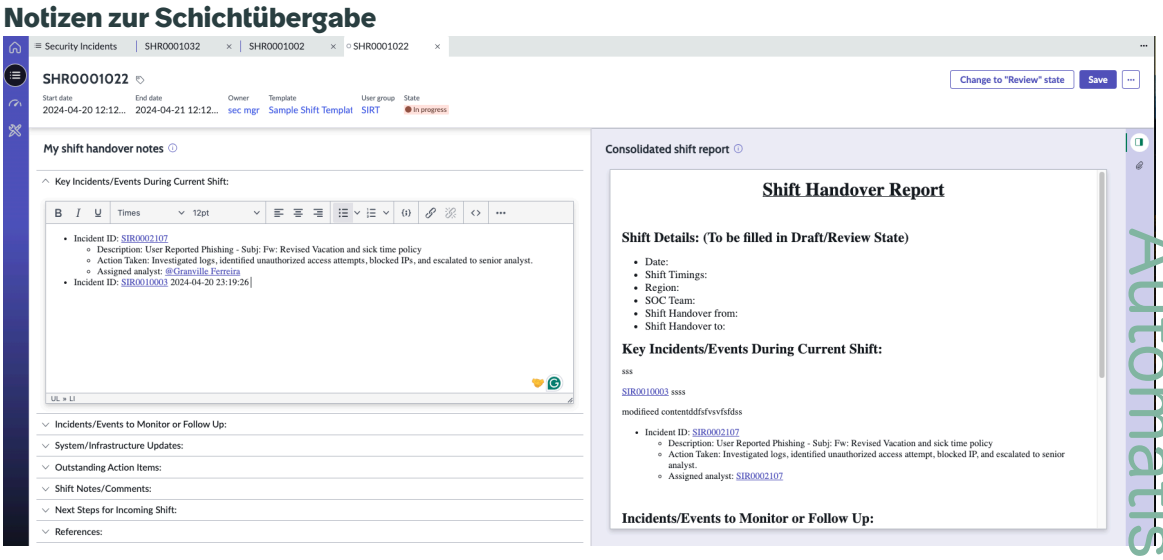
11. Aktualisieren Sie im Editor „Meine Schichtübergabenotizen“ die erforderlichen Details für alle Abschnitte wie Security Incident und Benutzerdetails.

Hinweis:
Sowohl der Schichtbesitzer als auch der Schichtanalyst können den Inhalt ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um einen bestimmten Datensatz im Editor zu erwähnen, verwenden Sie **/**, wählen Sie **Datensatz auswählen**und wählen Sie dann einen Datensatz aus der Liste der angezeigten Tabellen aus.
Wenn Sie beispielsweise den Datensatz **Security Incidents** auswählen, wird eine Liste mit Security Incidents angezeigt. Wählen Sie einen Security Incident (**SIR0010025**) aus der Liste aus, und aktualisieren Sie die erforderlichen Details zur Schichtübergabe. Sie können auch die Felder angeben, die dem Security Incident zugeordnet sind, z. B. „Kurzbeschreibung“, „Beobachtung“, indem Sie **„/“** nach der Nummer des Security Incidents verwenden.



b. Um einen bestimmten Benutzer im Editor zu erwähnen, verwenden Sie **/**, wählen Sie **Benutzer auswählen**und wählen Sie dann einen Benutzer aus der angezeigten Liste aus.

c. Sie können Ihren Bericht mit allen Optionen des Editors formatieren, z. B. Schriftarten, Farben, Aufzählungszeichen, Links und Anhänge.

d. Nachdem Sie die erforderlichen Änderungen an den Schichtübergabenotizen vorgenommen haben, wählen Sie **Speichern**aus.

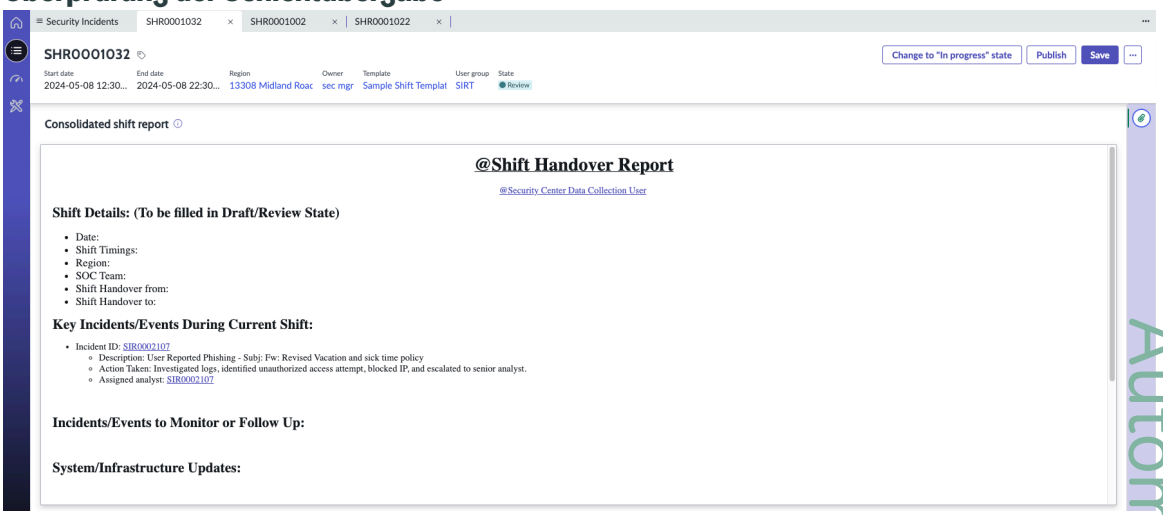
e. Wählen Sie die Aktion **„In Status „Überprüfen“ ändern“**, um den Schichtübergabe-Datensatz in den Status „Überprüfen“ zu verschieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn ein anderer Analyst aus dem aktiven Schichtteam den Bericht vor Ihnen bereits aktualisiert hat und Änderungen verarbeitet werden, wird möglicherweise eine Fehlermeldung angezeigt. Sie müssen einige Sekunden warten und dann **Change zu Status „Überprüfen“** erneut auswählen.

Überprüfung der Schichtübergabe



12. Überprüfen Sie im Bericht Konsolidierte Schicht den Bericht zur Schichtübergabe, und nehmen Sie die erforderlichen Änderungen vor.

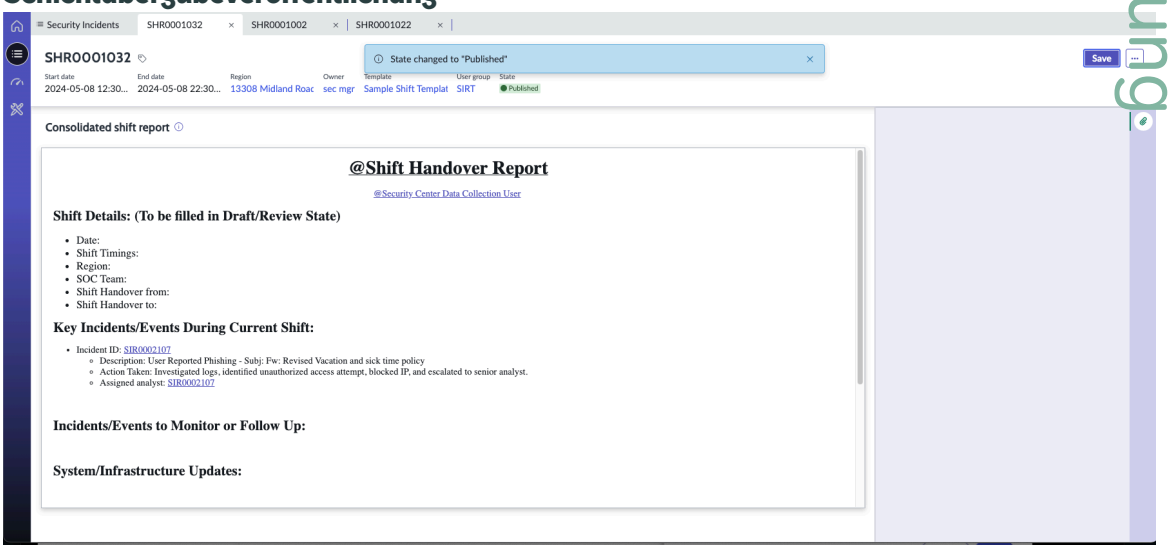
Hinweis:
Nur der Schichtbesitzer kann den Inhalt ändern.

a. Nachdem Sie die erforderlichen Änderungen an den Schichtübergabenotizen vorgenommen haben, wählen Sie **Speichern**aus.

b. Wenn der Schichtübergabebericht weitere Updates von den Analysten erfordert, können Sie **den Status „In Bearbeitung“ ändern**.

c. Wählen Sie die Aktion **Veröffentlichen** aus, um den Bericht zur Schichtübergabe zu veröffentlichen.

Schichtübergabeveröffentlichung



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Wählen Sie **Speichern** aus, um den Bericht zur Schichtübergabe zu speichern.
    Nach dem Speichern wird im Vorschaufenster eine Vorschau des Schichtübergabeberichts mit den neuesten Aktualisierungen angezeigt.

    Hinweis:
    Sie können zwar sofort eine Vorschau der Aktualisierungen anzeigen, die Sie am Schichtübergabebericht vorgenommen haben, es kann jedoch einige Sekunden dauern, bis die anderen Analysten die Änderungen sehen.

14. Als Schichtbesitzer können Sie in der Listenansicht „Schichtübergabe“ auch die folgenden Aktionen ausführen.

    a. Um einen vorhandenen Schichtübergabe-Datensatz zu bearbeiten, wählen Sie den Datensatz aus, und wählen Sie die Aktion **Bearbeiten** aus.
    Sie können nur Startzeit, Endzeit, Beschreibung und Region ändern.

    b. Um eine Kopie eines Schichtübergabe-Datensatzes zu erstellen, wählen Sie den Datensatz aus, und wählen Sie die Aktion **Kopie erstellen aus**.

    c. Um einen vorhandenen Schichtübergabe-Datensatz zu löschen, wählen Sie den Datensatz aus, und wählen Sie die Aktion **Löschen** aus.

SIR Workspace konfigurieren

In diesem Abschnitt werden die Konfigurationen beschrieben, die für die Verwendung mit Arbeitsbereich für Security Incident Responseerforderlich sind.

Richten Sie die Ansicht von SIR-Datensätzen ein

In diesem Abschnitt wird beschrieben, wie die zugehörigen Listen gruppiert und auf der Registerkarte „Zugehörige SIR-Datensätze“ dargestellt werden, um die Navigation zu erleichtern.

Benutzer des Arbeitsbereichs können die zugehörige Liste auch einfach nach Namen durchsuchen.

Konfigurieren Sie die SI-Entwurfszeituntersuchung

Verwenden Sie diesen Abschnitt, um die Untersuchungsseite für die Designzeit von Security Incidents zu konfigurieren und mehrere Einstiegspunkte und die zugehörigen Datensätze innerhalb von Arbeitsbereich für Security Incident Responsehinzuzufügen.

Erforderliche Rolle: sn_si.admin.

Im Folgenden werden die Schritte beschrieben, die bei der Konfiguration der Untersuchungsseite unter Arbeitsbereich für Security Incident Responseauszuführen sind.

- Ansicht für zugeordnete Infotabellen wird erstellt
- Hinzufügen einer Einstiegspunktliste
- Zuordnungsansicht der Liste „Informationen zuordnen zur Einstiegspunktliste“.
- Konfigurieren Sie jede zugeordnete Liste aus der Ansicht für das Rendern von Laufzeitdaten

Zugehörige Informationen

Untersuchungs-Canvas erkunden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht für zugeordnete Infotabellen wird erstellt

Der Untersuchungsbildschirm nutzt die zugehörigen Listenansichten, die für einen Security Incident erstellt wurden, um zugehörige Listen zu konfigurieren.

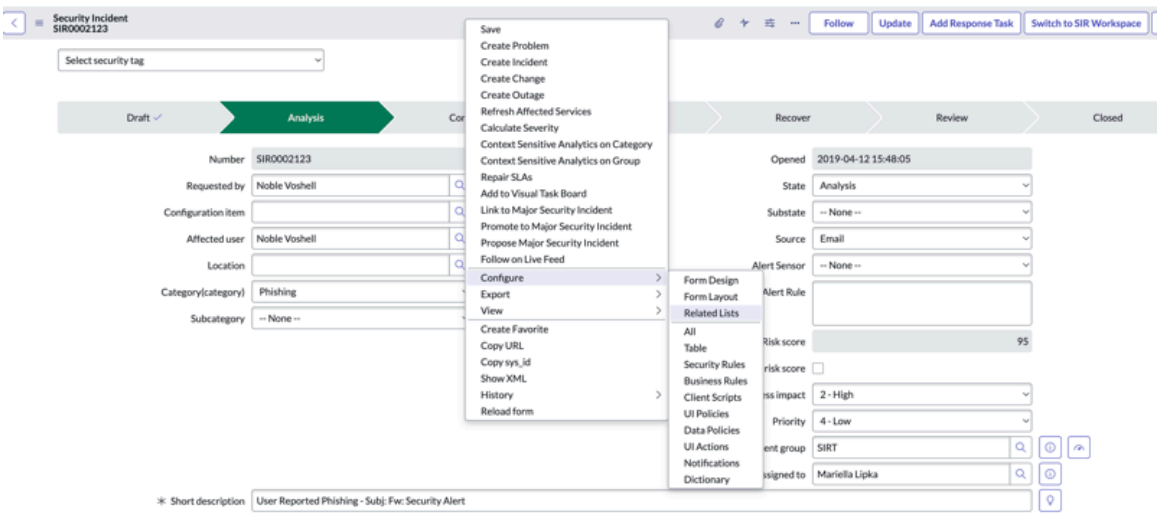
Vorbereitungen

Erforderliche Rolle: sn_si.admin

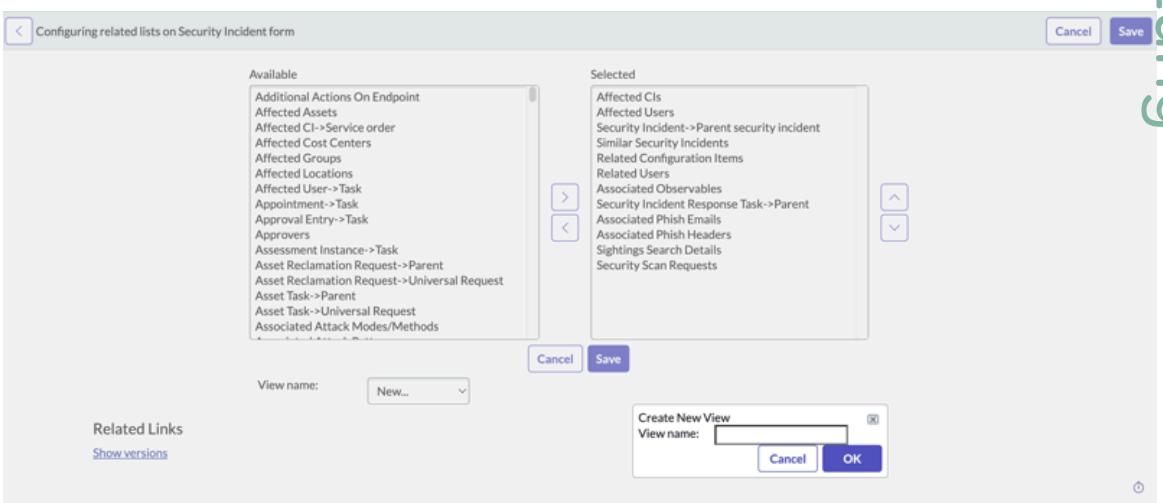
Im Folgenden finden Sie ein Verfahren zum Erstellen einer Ansicht und zum Hinzufügen zugehöriger Listen.

Prozedur

1. Navigieren Sie zu **Security Incident** Liste.
2. Öffnen Sie einen beliebigen -Security Incident in der klassischen Anwenderoberfläche.
3. Navigieren Sie über das Kontextmenü des Formulars zu **Konfigurieren** > **Zugehörige Listen**.
   Das Slushbucket-Fenster wird angezeigt.



4. Wechseln Sie zur Dropdown-Liste **Ansichtsname**, und klicken Sie auf **Neu,** um eine neue Ansicht zu erstellen.
   Sie müssen der Ansicht einen Namen hinzufügen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Fügen Sie die gewünschten zugehörigen Listen dem rechten Bucket unter der neu erstellten Ansicht hinzu, und speichern Sie die Ansicht.
   Diese Ansicht wird verwendet, um die zugehörigen Informationen auf der Registerkarte „Ermittlung“ darzustellen.

Hinzufügen einer Einstiegspunktliste

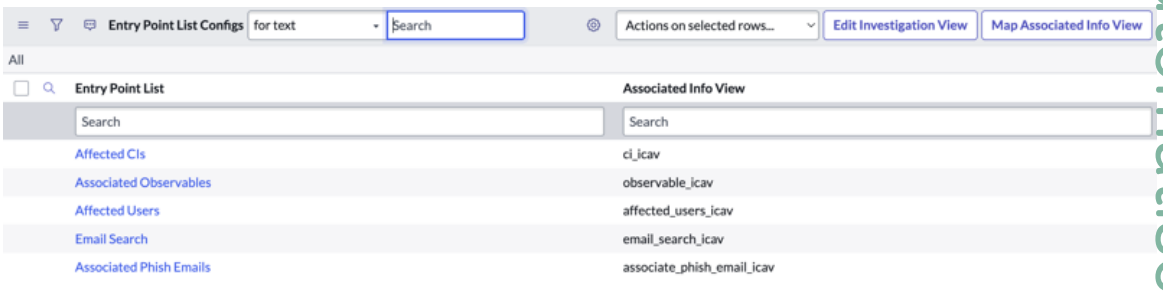
Konfigurieren Sie die neue Einstiegspunktliste, um sie der Untersuchungsseite hinzuzufügen.

Vorbereitungen

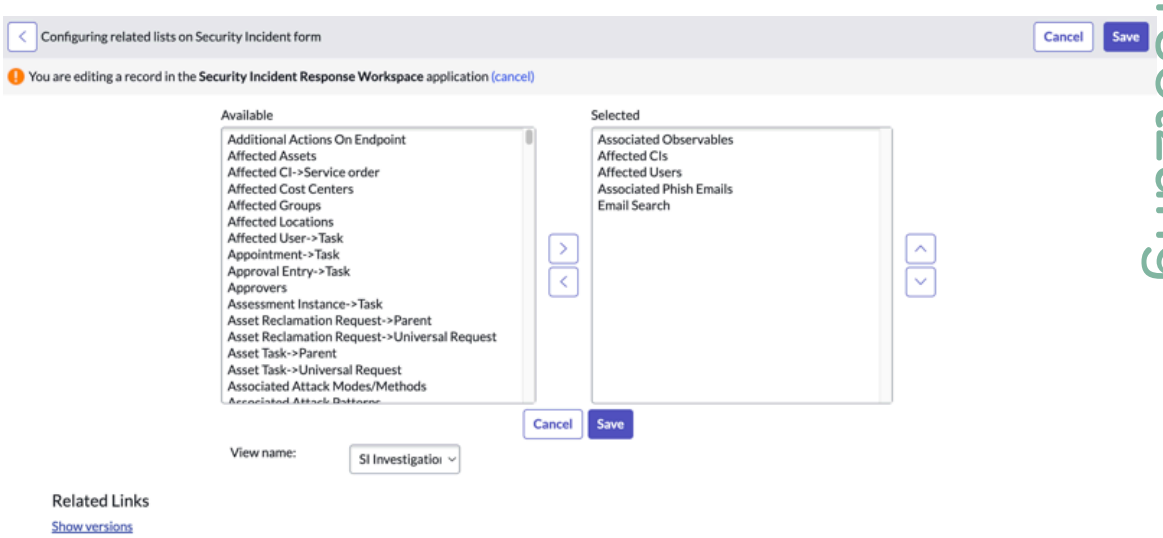
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **sn_si_aw_entry_point_config.list**.
   Die Seite **„Einstiegspunkt-Listenkonfigurationen“** wird angezeigt.



2. Klicken Sie auf die Schaltfläche **Untersuchungsansicht bearbeiten,** um dem Untersuchungsbildschirm eine Einstiegspunktliste hinzuzufügen.
   Das **Formular „Zugehörige Listen werden konfiguriert“ im Formular „Security Incident“** wird angezeigt.



3. Fügen Sie die Liste der Einstiegspunkte in der Slushbucket-Ansicht hinzu, oder entfernen Sie sie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Speichern**.

> **Hinweis:**
> Die Ansicht, die dem Untersuchungsbildschirm mit den Einstiegspunktlisten entspricht, wird als **SI-Untersuchungsansicht** bezeichnet und ist standardmäßig ausgewählt, wenn Sie zur Seite **„Untersuchungsansicht bearbeiten“** navigieren.
>
> Die Reihenfolge, in der die Einstiegspunktlisten im Untersuchungs-Canvas angezeigt werden, hängt von der Reihenfolge in der ausgewählten Ansicht des Slushbuckets ab.

Zuordnungsansicht der Liste „Informationen zuordnen zur Einstiegspunktliste“.

Ordnen Sie die zugehörige Infoansicht der neu hinzugefügten Einstiegspunktliste zu, indem Sie die Aktion „Zugeordnete Infoansicht zuordnen“ verwenden.

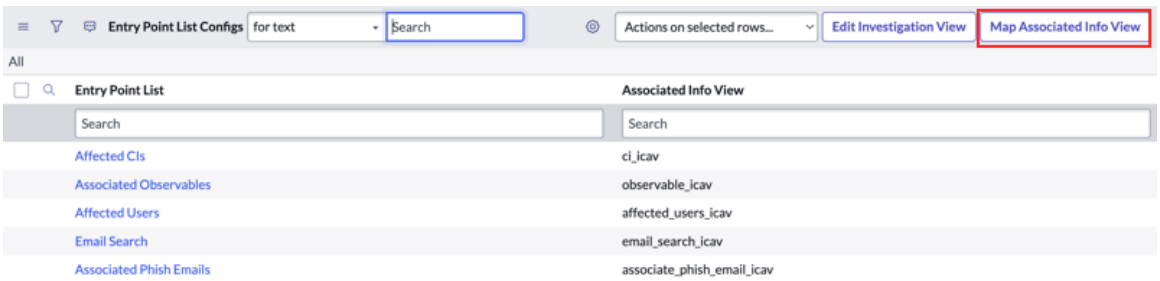
Vorbereitungen

> **Hinweis:**
> Dieser Schritt ist erforderlich, damit die Einstiegspunktliste auf der Untersuchungsseite sichtbar ist. Auch wenn unter einem Einstiegspunkt keine Listen mit zugehörigen Informationen angezeigt werden sollen, müssen Sie dennoch eine Dummy-Ansicht erstellen und diese zuordnen.

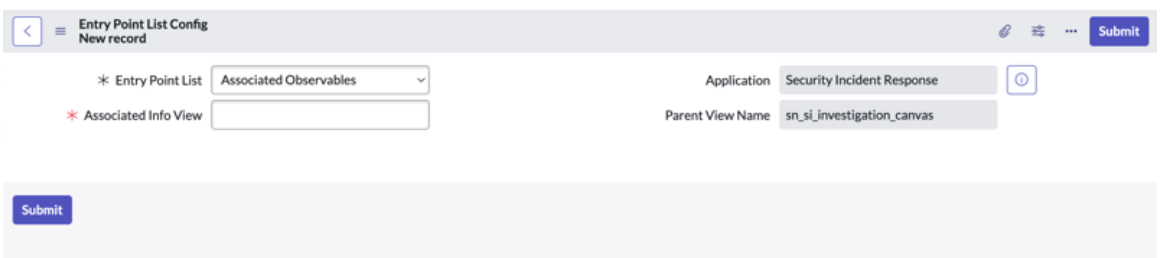
Erforderliche Rolle: Administrator

Prozedur

1. Klicken Sie auf die Schaltfläche **Zugeordnete Infoansicht zuordnen** auf der Seite **„Einstiegspunktkonfigurationen“**.



2. Wählen Sie die neu hinzugefügte Einstiegspunktliste aus der **Dropdown-Liste Einstiegspunktliste** aus.
3. Geben Sie im Feld **Zugeordnete Informationsansicht** den Namen der Ansicht ein, die die zugehörigen Listen mit zugehörigen Informationen enthält.
   Informationen zum Erstellen einer Ansicht für die zugehörigen Informationslisten finden Sie unter Ansicht für zugeordnete Infotabellen wird erstellt.



4. **Speichern** Sie das Formular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Darüber hinaus können Sie bei Bedarf mithilfe der **Ansicht „Zugeordnete Informationen bearbeiten“**weitere zugeordnete Listen hinzufügen oder entfernen.
   Sie können das Layout der Einstiegspunktliste auch mit der Aktion **„Layout Einstiegspunktliste bearbeiten“** konfigurieren. Fügen Sie dem Slushbucket nach Bedarf Spalten hinzu, oder entfernen Sie sie, und speichern Sie das Formular.

Konfigurieren Sie jede zugeordnete Liste aus der Ansicht für das Rendern von Laufzeitdaten

Konfigurieren Sie jede zugeordnete Liste aus der Ansicht für das Rendern von Laufzeitdaten.

Vorbereitungen

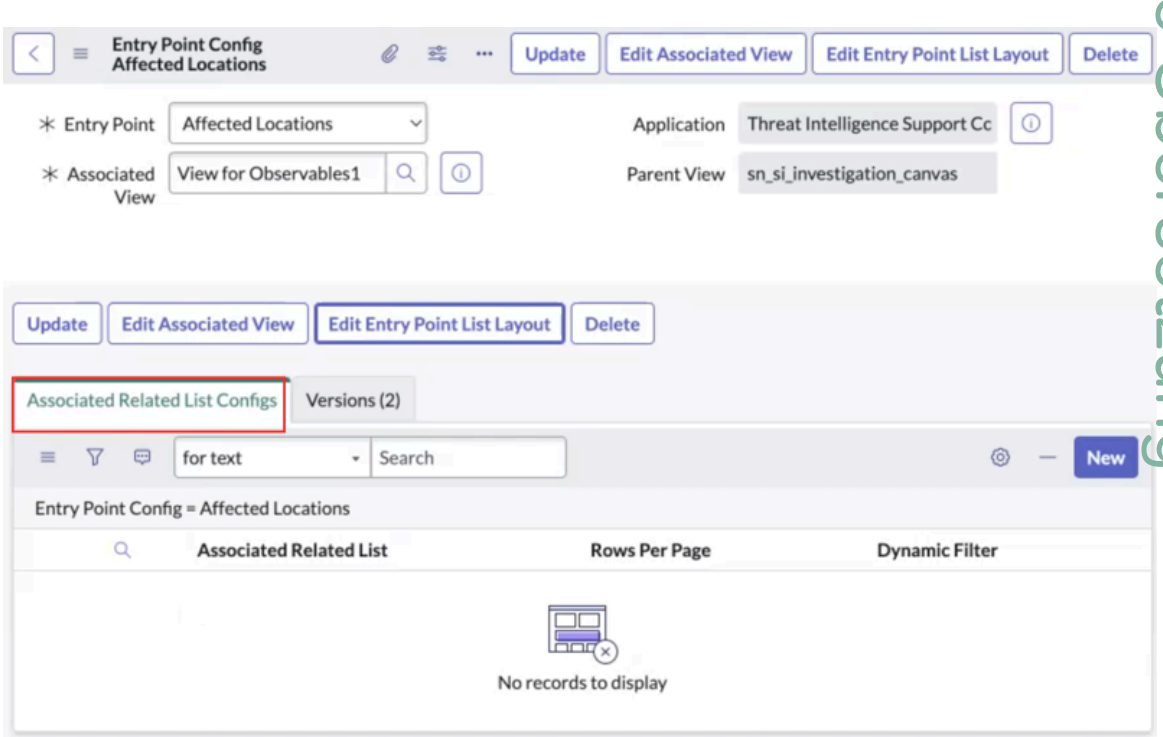
Hinweis:
Dieser Schritt ist für jede zugeordnete Liste obligatorisch, die in der zugehörigen Informationsansicht konfiguriert ist. Andernfalls ist die zugehörige Liste auf der Untersuchungsseite nicht verfügbar.

Jede der aus der zugehörigen Liste hinzugefügten Daten (beim Zuordnen einer zugeordneten Infoansicht zu einer Einstiegspunktliste) Zuordnungsansicht der Liste „Informationen zuordnen zur Einstiegspunktliste“. (oder direkt aus der Ansicht) benötigt eine zusätzliche Konfiguration, um die Daten im Hinblick auf die Auswahl des Laufzeitdatensatzes und der Filterauswahl zu filtern.

Erforderliche Rolle: Administrator

Prozedur

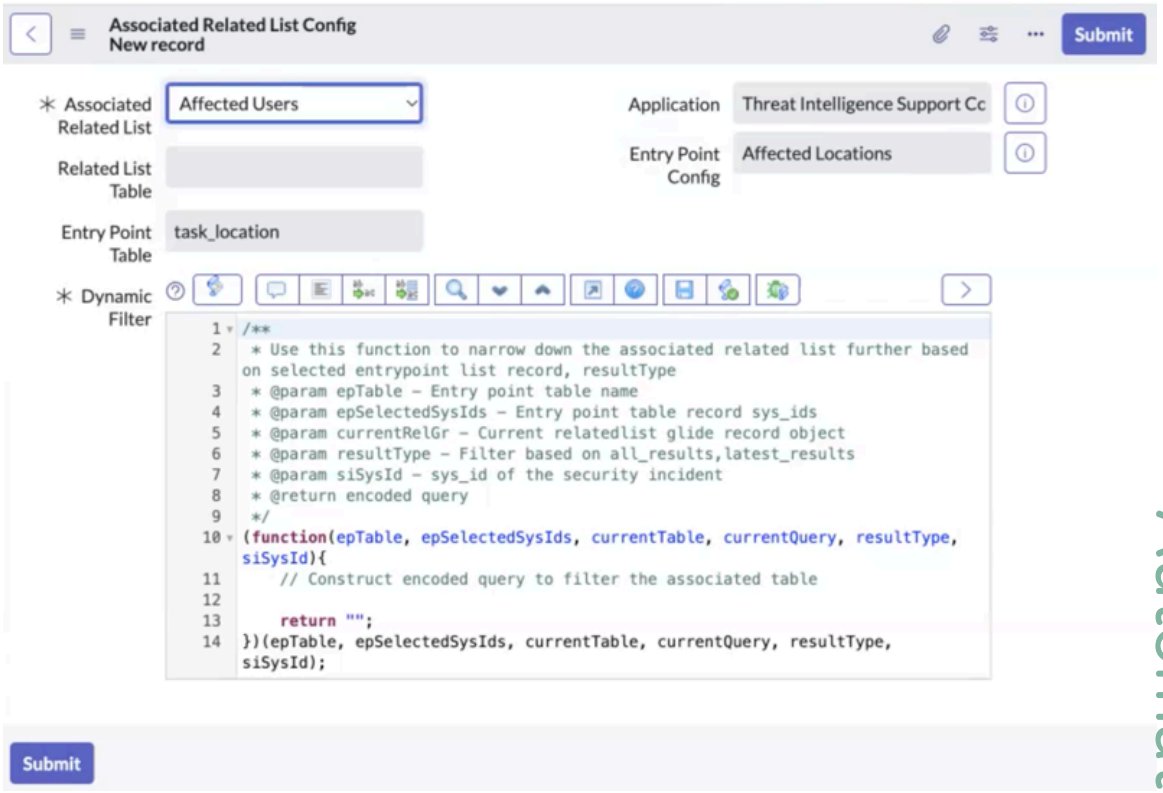
1. Klicken Sie unter **Zugeordnete Listenkonfigurationen** auf **Neu**.



2. Wählen Sie den Feldwert **der zugeordneten Liste** aus.
3. Verwenden Sie die Spalte **Dynamischer Filter**, um die zugeordnete Liste basierend auf den ausgewählten Einstiegspunkt-Listendatensätzen und dem Ergebnistyp (neueste Ergebnisse aus jeder Lieferantenimplementierung, alle Ergebnisse) weiter zu filtern.
   Sehen Sie sich die vorhandenen Beispiele an, die im Lieferumfang des Produkts enthalten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Außerdem können Sie das Layout der zugehörigen Liste mit der Aktion **„Layout der zugeordneten Liste bearbeiten“** konfigurieren.
   Fügen Sie im Slushbucket-Fenster nach Bedarf Spalten hinzu, oder entfernen Sie sie.

SIR Workspace Zugehörige Datensätze

Dieser Abschnitt besteht aus den zugehörigen Listenelementen, die in Abschnitte wie zugehörige erkennbare Elemente und Konfigurationselemente gruppiert sind.

In den folgenden zugehörigen Listen sind Gruppen aufgeführt, die als Teil des Basissystems verfügbar sind. Sie können diese Gruppen ändern oder Gruppen innerhalb der Anwendung und ihrer jeweiligen Aktionen erstellen.

Sie können diese Gruppen ändern oder neue Gruppen erstellen. Weitere Informationen zum Konfigurieren und Gruppieren der zugehörigen Liste für Security Incidents und Antwortaufgaben finden Sie unter Konfigurieren Sie die zugehörige Liste „Security Incident“.. Alle zugehörigen Listen sind innerhalb von SIR Workspacevoll funktionsfähig.

Zugehörige Liste	Gruppiertes Element
Geschäftsauswirkung	• Konfigurationselemente • Betroffene Anwender • Zugehörige Configuration Items • Zugehörige Anwender • Betroffene Services

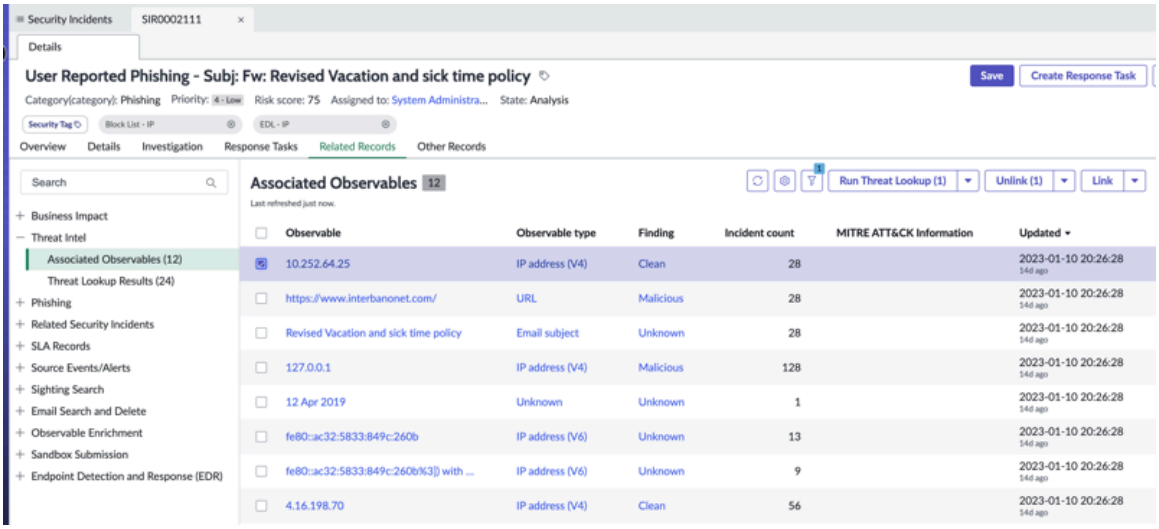
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Gruppiertes Element
Bedrohungsinformationen	• Zugehörige erkennbare Elemente • Bedrohungssuche – Ergebnisse
Phishing	• Zugeordnete Phishing-E-Mails • Zugehörige Phishing-Header
Zugehörige Security Incidents	• Übergeordneter Security Incident • Untergeordneter Security Incident • Ähnlicher Security Incident
SLA-Datensätze	Aufgaben-SLAs
Quell-Ereignisse/-warnungen	Quellereignisse oder -warnungen sind die SIEM-Integrations-fähige zugehörige Liste, z. B. Quell-E-Mail, LogRhythm-Drilldown-Protokolle, LogRhythm-Ereignisse, aggregierter IBM QRadar-Angriff usw. **Hinweis:** Diese Liste ist vollständig abhängig von der Integration, die Sie in Ihrer Instanz von haben. Um die relevante zugehörige Liste für die SIEM-Integration anzuzeigen, müssen Sie die neueste Version installieren.
Sichtungssuche	• Ergebnisse der Sichtungssuche • Details einer Sichtungssuche • Sichtung
Ergänzung erkennbarer Elemente	• Erkennbare Elemente – Datenanreicherungs-Ergebnisse • Zugeordnete MISP-Ereignisse • MISP-Datenanreicherungs-Ergebnisse
Endpoint Detection and Response (EDR	• Hostdetails • Laufende Prozesse • Laufende Services • Angemeldete Anwender • Netzwerkstatistiken • Datei abrufen • Hosteinträge isolieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Gruppiertes Element
	• Zusätzliche Aktion für Endpunkt • Microsoft Defender für Endpunkt-bezogene Computer – Details



Hinweis:
Im Allgemeinen können Sie neue Datensätze erstellen, vorhandene Datensätze verknüpfen oder neue Datensätze mit der zugehörigen Listengruppe verknüpfen oder die Verknüpfung aufheben.

Zugehörige Informationen

Konfigurieren Sie die zugehörige Liste „Security Incident“.

Konfigurieren Sie die zugehörige Liste „Security Incident“.

Sie können neue zugehörige Listen oder neue zugehörige Listengruppen hinzufügen und vorhandene Gruppen oder zugehörige Listen ändern, die in SIR Workspaceangezeigt werden.

Vorbereitungen

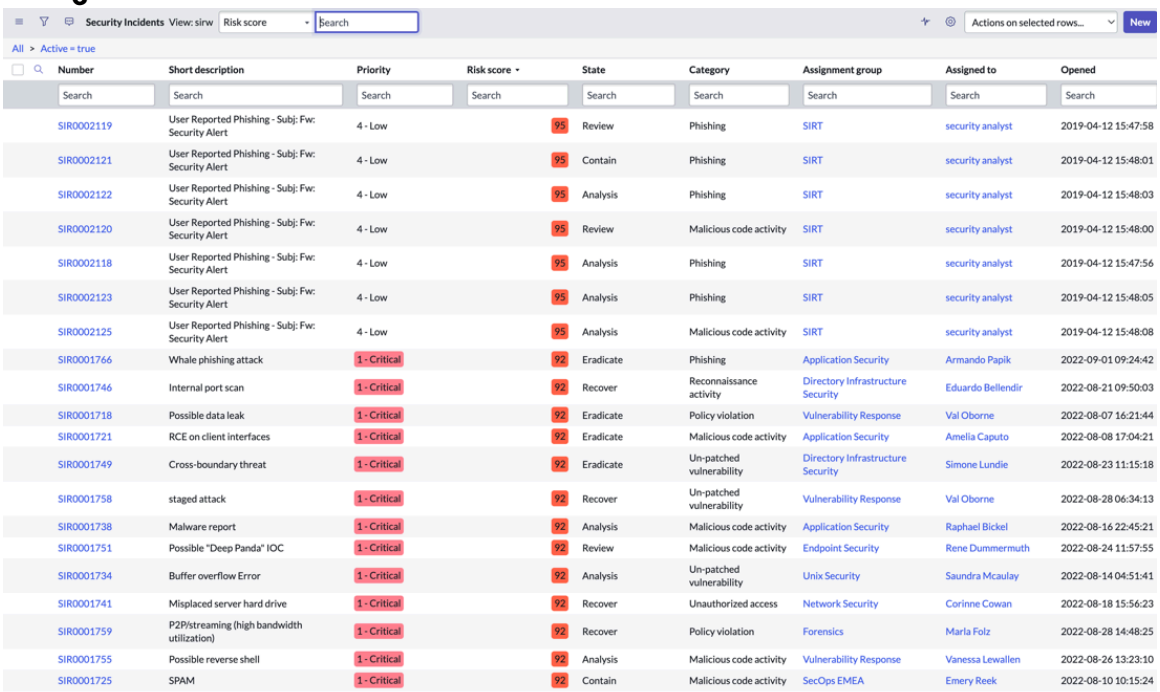
Die zugehörige Liste „Security Incident“ wird gruppiert und als zugehörige Gruppenlistenelemente auf der **Registerkarte Zugehörige** Datensätze im Arbeitsbereich angezeigt.

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

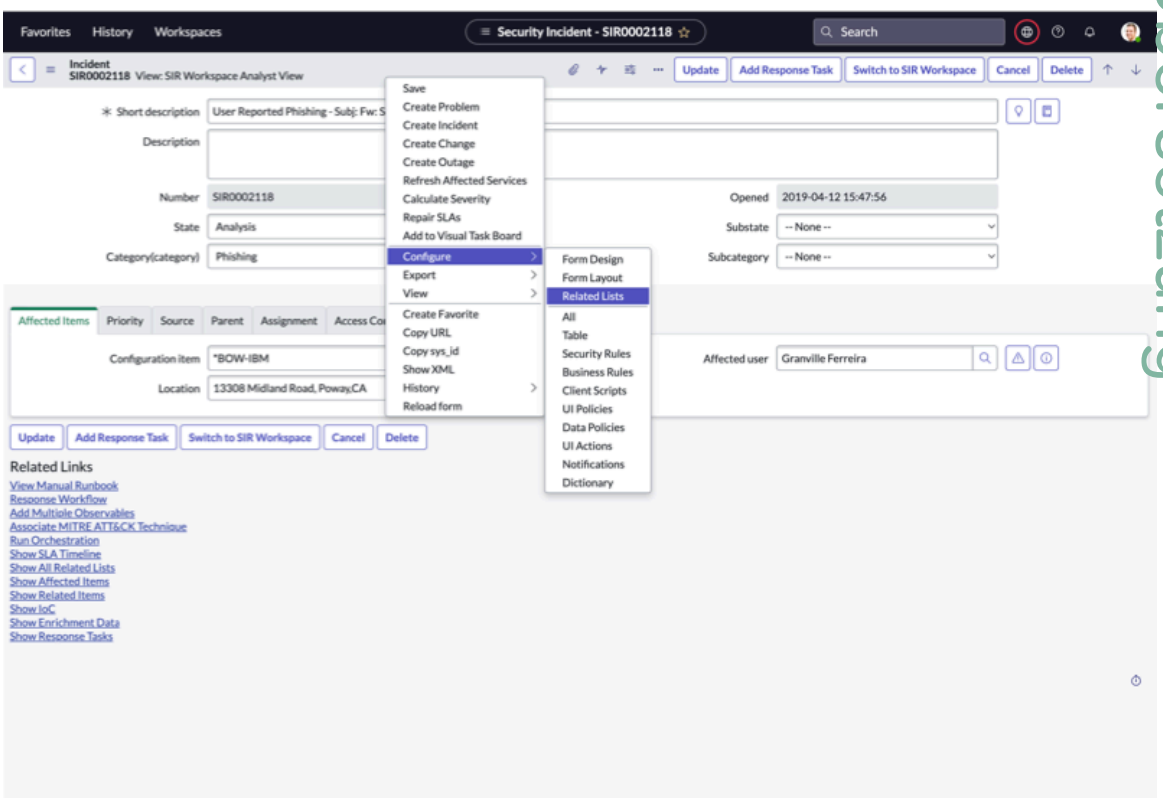
Prozedur

1. Navigieren Sie in der klassischen Anwenderoberfläche zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.



Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. Wählen Sie einen beliebigen Incident-Datensatz aus.
3. Klicken Sie mit der rechten Maustaste auf das Incident-Kontextmenü.
4. Gehe zu **Konfigurieren** > **Zugehörige Liste**.

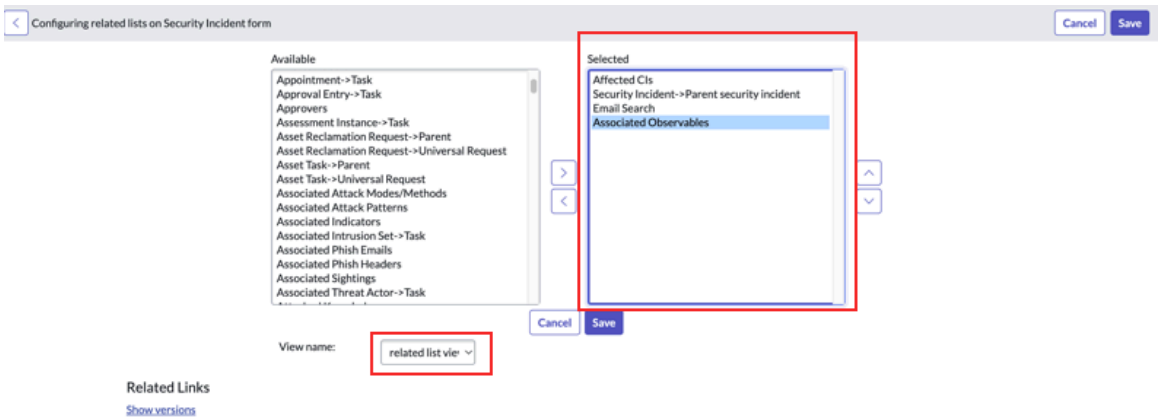


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

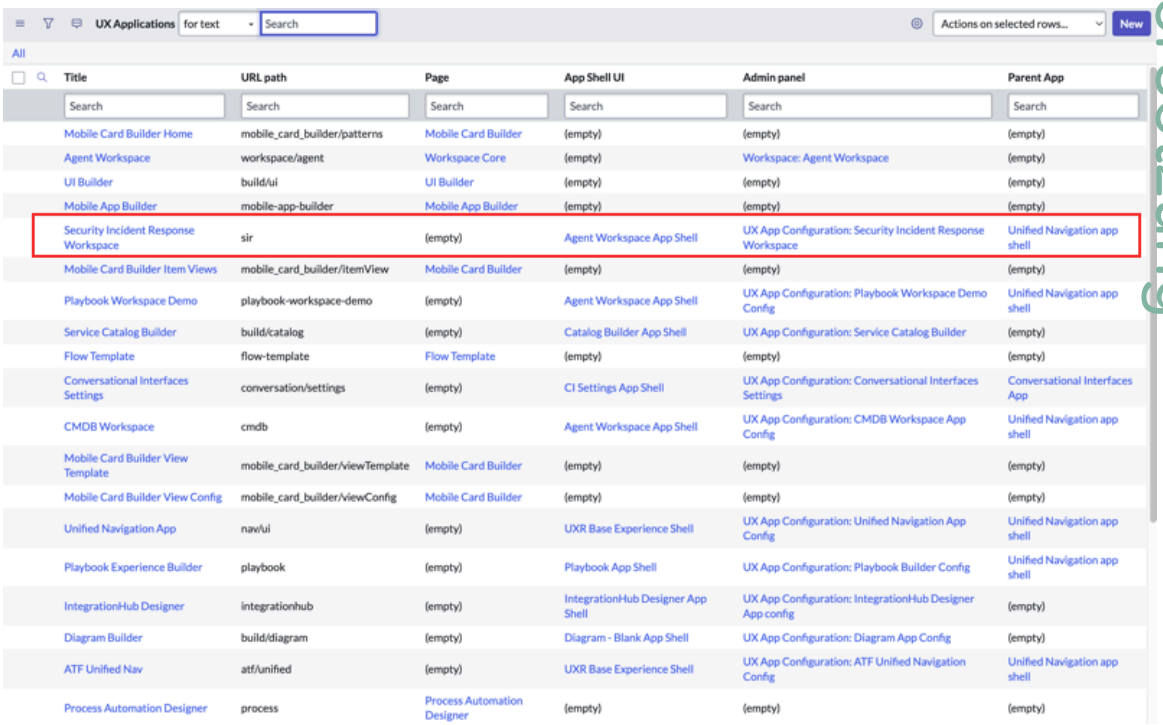
Das **Formular „Zugehörige Listen werden konfiguriert“ im Formular „Security Incident“** wird angezeigt.

5. Wechseln Sie zu **Ansichtsname**, und wählen Sie **Neu**.
6. Geben Sie einen Namen für die Ansicht ein.
7. Wählen Sie die neu erstellte Ansicht aus.
   Nachdem Sie die Ansicht ausgewählt haben, wählen Sie die erforderlichen zugehörigen Listenfelder aus dem Slushbucket aus.



Hinweis:
Wenn Sie etwas ändern möchten, wählen Sie die Ansicht aus, und entfernen Sie die Elemente oder fügen Sie sie hinzu.

8. Klicken Sie auf **Speichern**.
9. Navigieren Sie im linken Navigationsbereich zu **Alle** > **Now-Experience-Framework** > **Erfahrungen**.
10. Wählen Sie **Arbeitsbereich für Security Incident Response**aus.

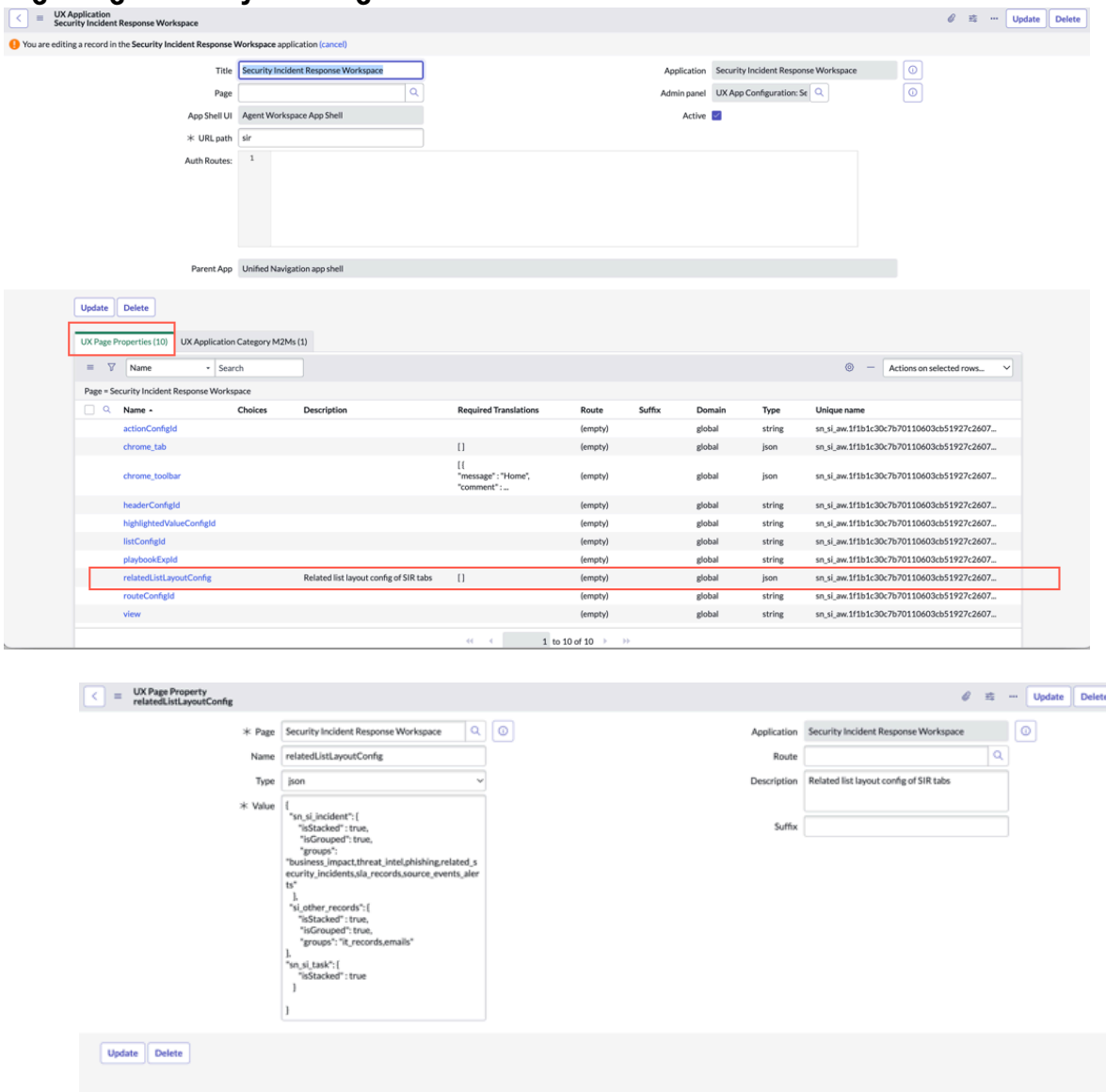


Die Seite **„Arbeitsbereich für UX Application Security Incident Response“** wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

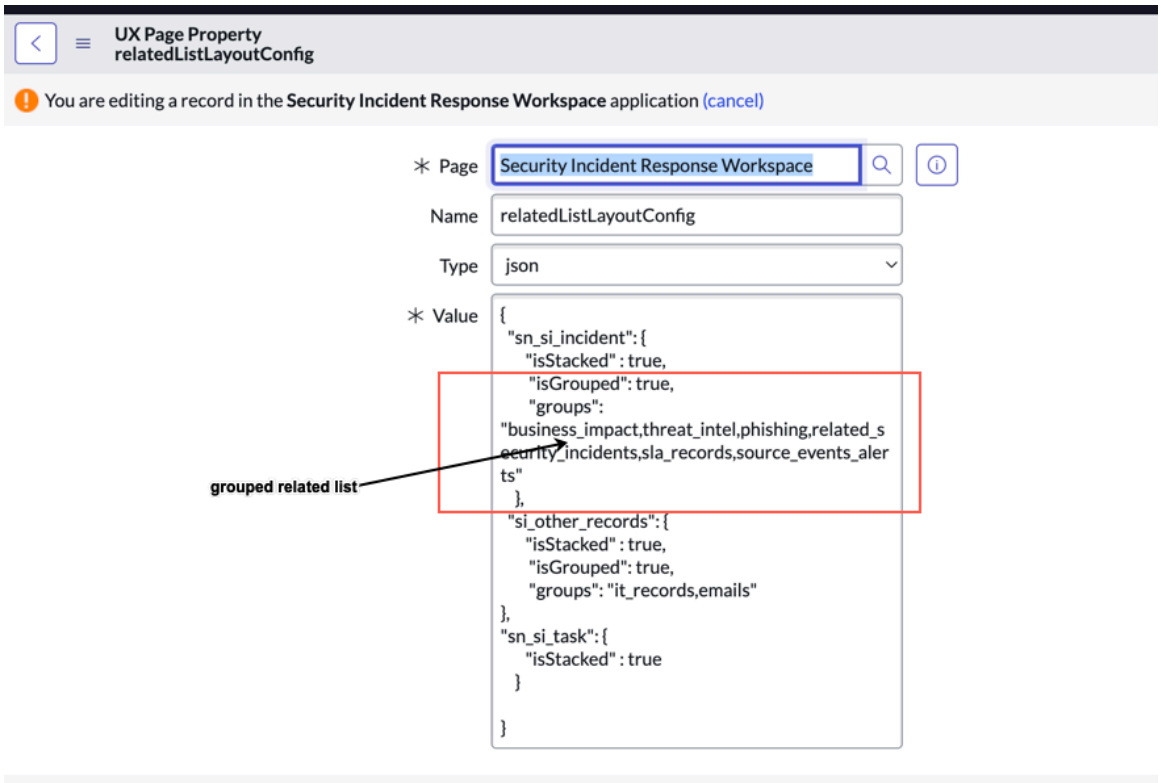
11. Wechseln Sie zur Registerkarte **UX-Seiteneigenschaften**, und wählen Sie in der Listenansicht die Option **zugehörige Listenlayoutkonfiguration** aus.



12. Fügen Sie den neu erstellten Ansichtsnamen, getrennt durch ein Komma, einer bereits vorhandenen Liste von Werten im Textfeld **Wert** unter dem Feld **sn_si_incident.viewsUsedForGrouping** hinzu.
Wenn Sie beispielsweise einen neuen Ansichtsnamen mit der Bezeichnung **Geschäftsauswirkung** erstellt haben, müssen Sie ihn im Textfeld **Wert** als **business_impact** (durch Unterstrich innerhalb des Ansichtsnamens und getrennt durch ein Komma nach einem vorhandenen Wert) unter sn_si_incident angeben Feld :groups.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

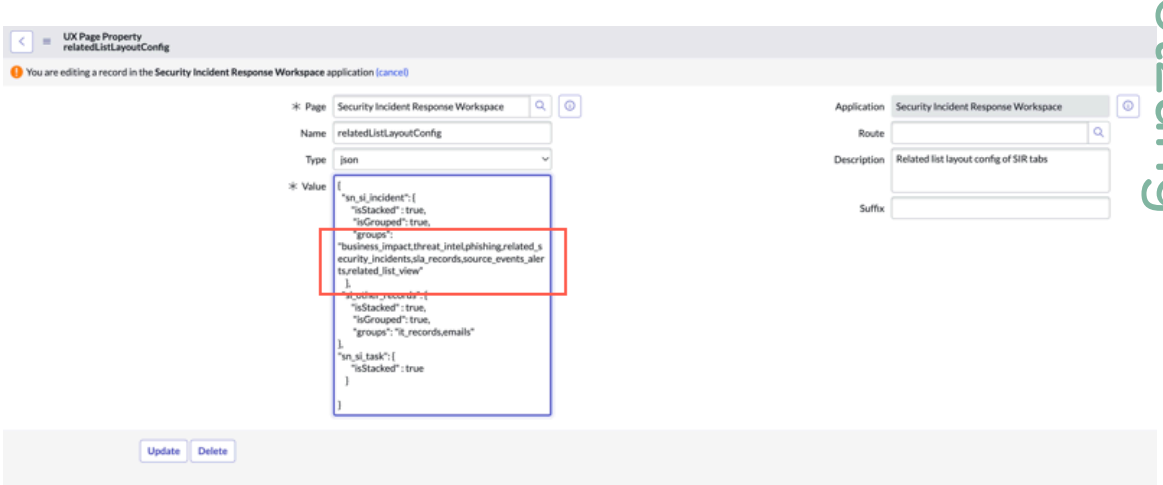


Hinweis:

Wenn Sie den neuen Ansichtsnamen unter dem Feld **sn_si_incident.viewsUsedForGrouping** hinzufügen, wird der Eintrag auf der Registerkarte **Zugehörige Datensätze** des Arbeitsbereichs erstellt.

Wenn Sie den Eintrag für den Ansichtsnamen in **„si_other_records.viewsUsedForGrouping“** aktualisieren, wird die zugehörige Listengruppe auf der Registerkarte **„Andere Datensätze“** des Arbeitsbereichs hinzugefügt.

Nachfolgend finden Sie eine Beispielansicht, in der die neu erstellten Ansichten hinzugefügt werden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
„requiredRolesForGrouping“ enthält kommagetrennte sys_user_role-Datensatznamen. Der SIR Workspace-Anwender muss mindestens eine dieser Rollen haben, um die gruppierten zugehörigen Listen zu verwenden. Wenn ein Anwender über keine dieser Rollen verfügt, wird die zugehörige Listenansicht, die für die aktuelle Anwenderrolle mithilfe der Ansichtsregelkonfiguration konfiguriert wurde, vertikal ohne Gruppierung dargestellt. Diese Eigenschaft wird ignoriert, wenn die Eigenschaft **„isGrouped“** auf „falsch“ festgelegt ist. Wenn diese Eigenschaft leer ist, kann jeder Anwender auf die gruppierten zugehörigen Listen zugreifen.

13. Klicken Sie auf **Speichern**.
14. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
15. Wählen Sie einen bestimmten Security Incident aus.
16. Wechseln Sie zur Registerkarte **Zugehörige Datensätze** des Arbeitsbereichs.
    Die gruppierten zugehörigen Listen werden angezeigt.

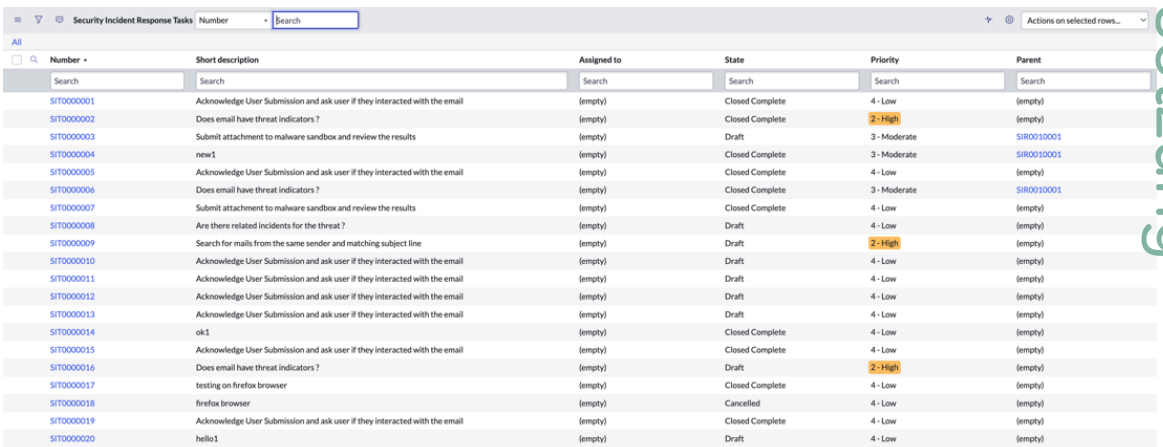
Konfigurieren Sie die zugehörige Liste „Antwortaufgabe“.

Verwenden Sie diesen Abschnitt, um neue zugehörige Listen für Antwortaufgaben zu konfigurieren, die in der Anwendung Security Incident Response angezeigt werden.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die zugehörige Liste der Antwortaufgaben ist nicht gruppiert, sondern wird als einzelne zugehörige Listenelemente angezeigt, da einige Standardlisten vorhanden sind. Zeigen Sie die zugehörigen Elemente zu Antwortaufgaben auf der Registerkarte **Antwortaufgaben** des Security Incident-Datensatzes des -Arbeitsbereichs an.

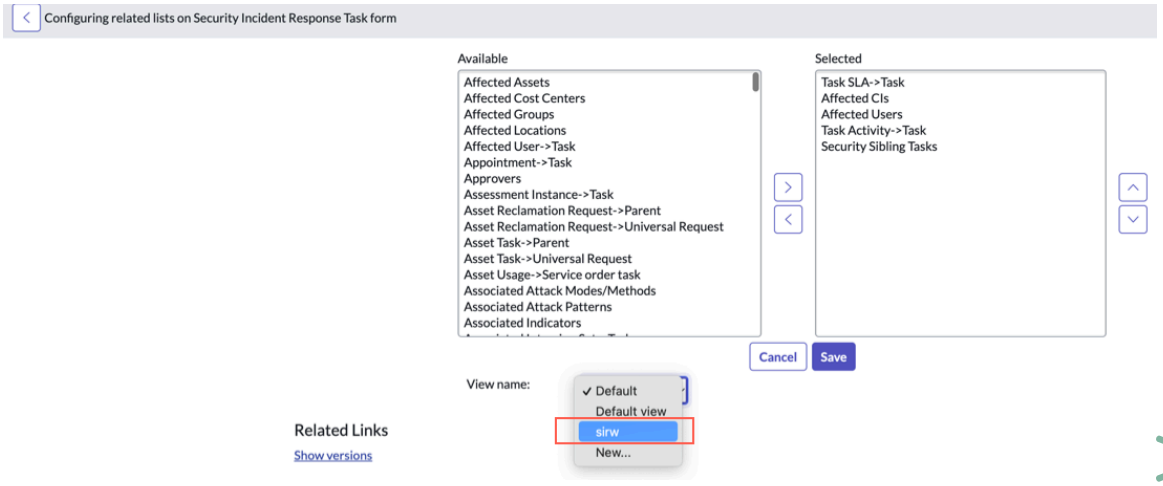
Prozedur
1. Navigieren zu **Alle** > **Security Incident** > **Antwortaufgaben** > **Alle Aufgaben anzeigen**.



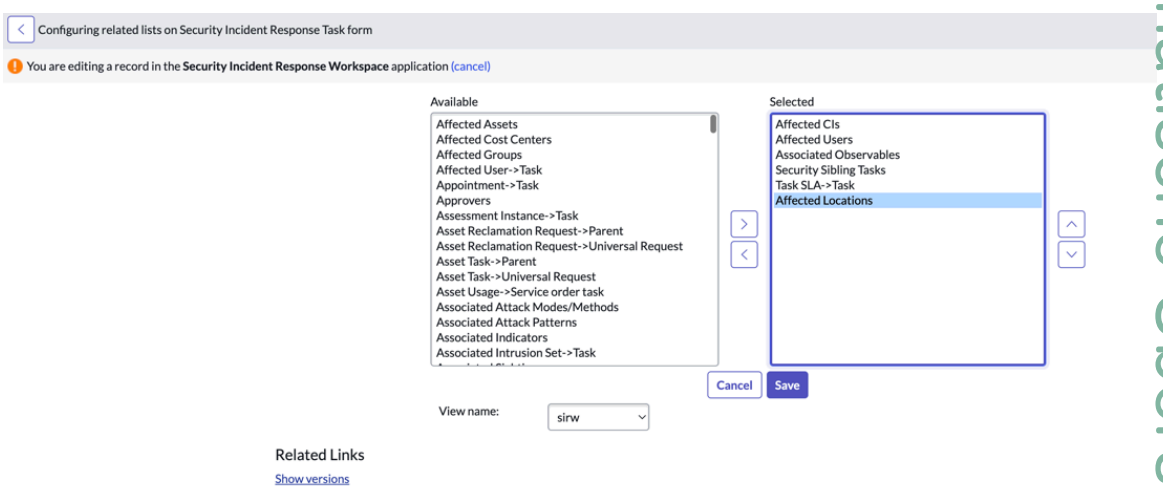
2. Wählen Sie einen beliebigen Antwortaufgaben-Datensatz aus.
3. Klicken Sie mit der rechten Maustaste auf das Kontextmenü Security Incident Response-Aufgabe.
4. Navigieren zu **Konfigurieren** > **Zugehörige Liste**.
   Das **Konfigurationszugehörige Listen im Formular „Sicherheitsantwortaufgabe“** wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wechseln Sie zu **Ansichtsname**, und wählen Sie die Ansicht **„Sirw-** Ansicht“ aus.



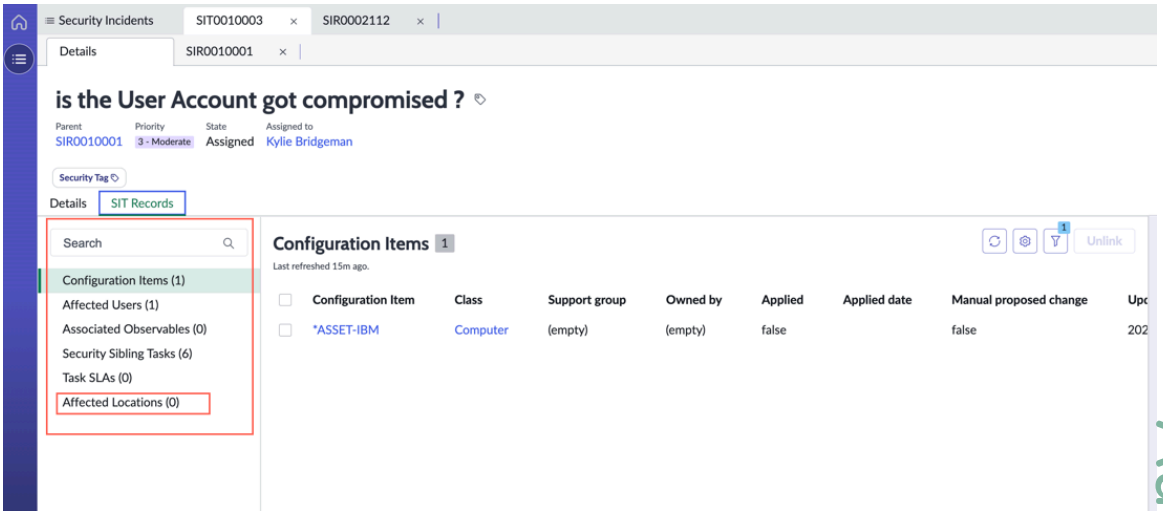
6. Wählen Sie die gewünschten zugehörigen Listenfelder aus dem Slushbucket aus.
   Beispiel: Betroffene Standorte.



7. Klicken Sie auf **Speichern**.
8. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Antwortaufgaben** > **SIT-Datensätze**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die konfigurierten zugehörigen Listen (z. B. „Betroffene Standorte als ausgewählt“) werden in der Liste der SIT-Datensätze aufgeführt.



Definieren Sie die neuen Regeln des Risikobewertungsrechners

Verwenden Sie den neuen Risikobewertungsrechner, um die Risikopunktzahl von Security Incidents basierend auf den anwenderdefinierten Kriterien zu definieren und zu berechnen, die eine transparente Intelligenzbewertung von Security Incidents ermöglichen. Die Risikopunktzahl wird für die Security Incident-Datensätze automatisch berechnet.

Vorbereitungen

Erforderliche Rolle: sn_si.admin.

Aktivieren Sie den neuen Risikobewertungsrechner, indem Sie die Systemeigenschaft sn_si_aw.activate_new_risk_score_calculator auf wahr setzen.

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie eine Risikopunktzahl für die Security Incident-Datensätze, die basierend auf den anwenderdefinierten Parametern generiert werden. Das Basissystem wird mit einer Risikobewertungsregel bereitgestellt, die entsprechend angepasst und aktiviert werden kann.

Hinweis:

- Standardmäßig ist die neue Regel des Risikobewertungsrechners inaktiv. Sie müssen die Regel aktivieren, um die Risikopunktzahl der Security Incidents anzuzeigen.
- Informationen zur Berechnung der Risikopunktzahl für zusätzliche zugehörige Tabellen, die nicht im Basissystem verfügbar sind, finden Sie unter Risikobewertungsrechner für zusätzliche zugehörige Tabellen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Administration**.
2. Navigieren zu **Regel-Engine** > **Regel des Risikobewertungsrechners**.
   Die Seite Regel des Risikobewertungsrechners wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Als Teil des Basissystems erhalten Sie eine vordefinierte Vorlage für Risikobewertungsregeln zum Anzeigen, Bearbeiten oder Ändern der Risikopunktzahl. Sie können die vordefinierte Regelvorlage für die Risikopunktzahl jedoch nicht erstellen oder löschen.
- Die von Ihnen vorgenommenen Änderungen gelten für alle neuen Security Incidents oder Updates für die vorhandenen Security Incidents. Um historische Punktzahlen neu zu formulieren, verwenden Sie die Aktion **Punktzahl neu berechnen**.

3. Wählen Sie die Regel **Risikobewertungsrechner** aus.
4. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Name des Risikopunktzahlwerts. Beispiel: Risikobewertungsrechner.
Gesamtgewichtung (gilt für den Kriteriengenerator)	Gewichtung dieses Feldes innerhalb der Risikoregel. Dieses Feld kann nicht bearbeitet werden und zeigt die vom System berechnete Gesamtgewichtung basierend auf der Gewichtung an, die den aktivierten Kriterien entspricht. Die Gesamtgewichtung muss immer 100 % betragen.
Beschreibung	Beschreibung des Risikopunktzahl-Datensatzes. Beispielsweise berechnet die Risikopunktzahl basierend auf der gewichteten Summe vordefinierter Kriterien.
Bewertungskriterien	Gibt die Bewertungskriterien für einen Security Incident an. Sie können die **Risikobewertungskriterien** mithilfe der folgenden Optionen definieren: ○ **Kriteriengenerator**: Verwenden Sie diese Option, um Kriterien hinzuzufügen, zu bearbeiten oder zu entfernen sowie Kriterien zu aktivieren und zu deaktivieren, die zur Berechnung der Risikopunktzahl beitragen, und um sicherzustellen, dass die aggregierte Gesamtgewichtung 100 % beträgt. ○ **Skript verwenden (erweitert)**: Die Skripterstellungsfunktion ist eine erweiterte Funktion zum Erstellen eines anwenderdefinierten Skripts, das die Risikopunktzahl im Bereich von 0 bis 100 zurückgeben soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Um die **Bewertungskriterien** mit dem **Kriteriengenerator**zu definieren, gehen Sie wie folgt vor:

> **Hinweis:**
> Sie können die vorhandenen Kriterien bearbeiten oder ändern oder neue Kriterien hinzufügen.

a. Um ein neues Kriterium hinzuzufügen, wählen Sie die Aktion **+Neue Kriterien**.

b. Wählen Sie die **Tabelle** aus, für die Sie die Kriterien festlegen möchten.

> **Hinweis:**
> - Wenn es sich bei der ausgewählten Tabelle um einen Security Incident handelt, wird die Bedingung auf den Security Incident-Datensatz angewendet, für den die Risikopunktzahl berechnet wird. Wenn die ausgewählte Tabelle kein Security Incident ist, wird die Bedingung nur angewendet, wenn sich die Datensätze auf den Security Incident beziehen, für den die Risikopunktzahl berechnet wird.
> - Ein zusätzlicher Zusammenfassungstyp wird hinzugefügt, um die Punktzahlen basierend auf der Anzahl der Beziehungen zu definieren, die den Security Incidents zugeordnet sind.

c. Wählen Sie die **Typkriterien** für die ausgewählte Tabelle aus.
Der Typwert kann je nach gewählter Tabelle entweder **Feld** oder **Aggregat** sein.

d. Wählen Sie die **Feldkriterien** für die ausgewählte Tabelle aus.
Wenn Sie den Wert Typ als **Feld**ausgewählt haben, zeigen die Feldkriterien die Feldwerte an, die sich auf die Tabelle beziehen. Wenn Sie den Wert Typ als **Aggregat**ausgewählt haben, zeigen die Feldkriterien die Aggregatwerte an, die sich auf die Tabelle beziehen.

> **Hinweis:**
> Der Aggregattyp unterstützt nur Anzahlwerte.

Wenn Sie beispielsweise als Tabellenkriterium **Security Incident**auswählen, zeigt das Kriterium Typ nur die Option **Feld** an. Die Feldkriterien zeigen alle Feldwerte an, die sich auf die Tabelle beziehen. Dies können „Schweregrad“, „Aktiv“ usw. sein. Wenn Sie für das Tabellenkriterium „ **Betroffene Anwender“**auswählen, zeigen die Typkriterien sowohl die Option **„Feld“** als auch **„Aggregat“** an. Wenn Sie als Typ Aggregat auswählen, zeigen die Feldkriterien die Aggregatwerte an, die sich auf die Tabelle beziehen **(Anzahl)**.

e. Geben Sie die **Gewichtung** der Kriterien zwischen 0 und 100 ein.
Die Gesamtgewichtung aller Kriterien muss 100 % betragen.

f. Geben Sie den Namen und eine Kurzbeschreibung der Kriterien ein.

g. Aktivieren Sie das Kontrollkästchen **Bewertungskriterien aktivieren**, um die Bewertungskriterien zu aktivieren.

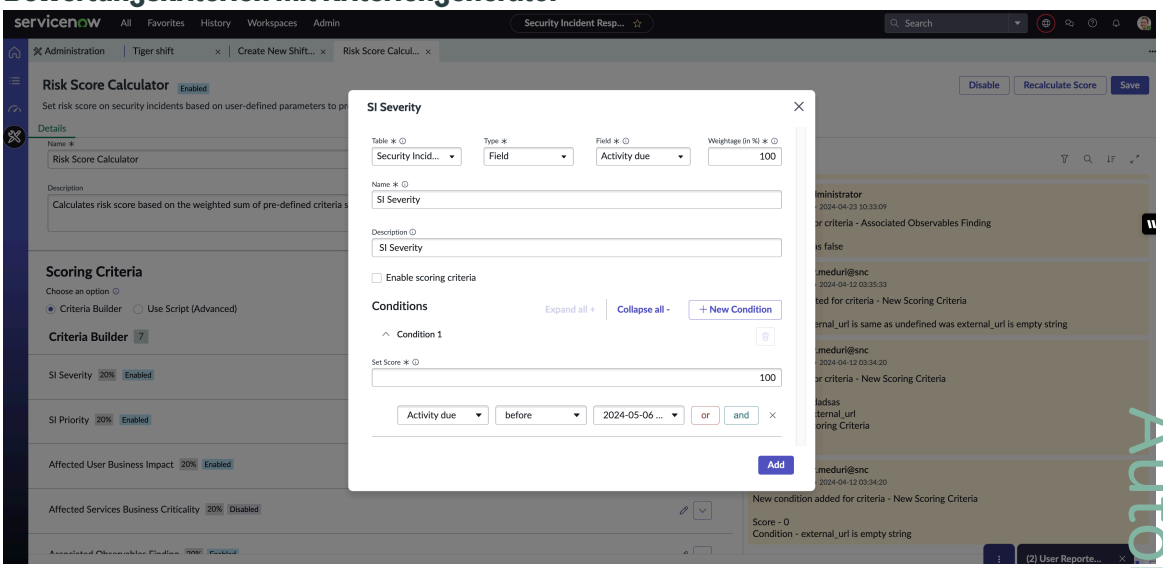
h. Definieren Sie die **Bedingungen**, und legen Sie die Punktzahl für die Bedingungen fest.

i. Sie können auch neue Bedingungen mit der Option **Neue Bedingung** hinzufügen und vorhandene Bedingungen mit dem Symbol **Kriterien** löschen löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

j. Wählen Sie **Hinzufügen**, um die konfigurierten Kriterien hinzuzufügen.

Bewertungskriterien mit Kriteriengenerator



6. Wählen Sie die Option **Punktzahl neu berechnen** aus, um die Risikopunktzahl neu zu berechnen.

Zum Beispiel, wenn Änderungen an der Regel für Risikopunktzahlen vorgenommen wurden. In diesem Fall müssen Sie die Bewertungsregel erneut auf die Security Incidents anwenden, bei denen die Risikopunktzahl bereits in der Vergangenheit berechnet wurde. Verwenden Sie die Aktion **Punktzahl neu berechnen**, um den Neuberechnungsauftrag auszulösen.

7. Wählen Sie **Bestätigen** aus.

Hinweis:
Sobald Sie diese Aktion ausgelöst haben, wird der Prozess im Hintergrund ausgeführt und dauert einige Minuten. Sie können bis zum Abschluss keine Änderungen vornehmen.

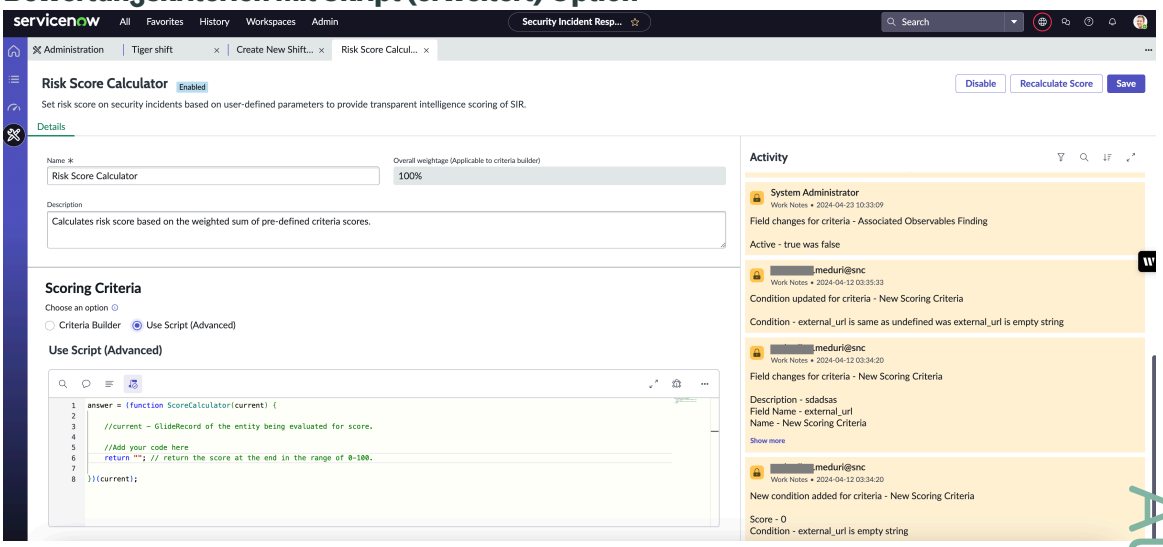
8. Um die **Bewertungskriterien** mit der Option **Skript verwenden (erweitert)** zu definieren, gehen Sie wie folgt vor:

a. Verwenden Sie dieses vordefinierte Skript, um ein anwenderdefiniertes Skript zu erstellen, das die Risikopunktzahl im Bereich von 0 bis 100 zurückgeben soll.
Das Feld „Erweitertes Skript“ wird automatisch mit einer Funktion ausgefüllt, die die Parameter **current** annimmt. Diese Funktion sollte die Risikopunktzahl im Bereich von 0 bis 100 zurückgeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertungskriterien mit Skript (erweitert) Option



Hier ist der aktuelle Parameter das GlideRecord-Objekt der Entität (Security Incident), für die die Risikopunktzahl berechnet wird. Bei Security Incidents entspricht sie dem GlideRecord für die Tabelle sn_si_incident.

9. Um den Risikobewertungsrechner zu deaktivieren, wählen Sie **Deaktivieren aus**.
10. Wählen Sie **Speichern**.

Risikobewertungsrechner für zusätzliche zugehörige Tabellen

Der Risikobewertungsrechner wird mit einer Risikobewertungsregel als Teil des Basissystems bereitgestellt, um die Risikopunktzahl von Security Incidents basierend auf anwenderdefinierten Kriterien zu berechnen. Sie können jedoch zusätzliche zugehörige Tabellen anpassen und einfügen, um die Risikopunktzahl zu berechnen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie einen beliebigen Security Incident-Datensatz aus.
3. Wählen Sie die Option **Zusätzliche Aktionen** neben der Nummer des Security Incidents aus.
4. Gehe zu **Konfigurieren** > **Zugehörige Listen**.
5. Wechseln Sie zum Namen der Ansicht, und wählen Sie **Risikobewertungsrechner**aus.
   Nachdem Sie die Ansicht ausgewählt haben, wählen Sie aus dem Slushbucket die erforderliche zugehörige Liste aus, die Sie hinzufügen möchten. Beispiel: Zugeordnete Sichtungen.
6. Wählen Sie **Speichern**.
   Sie haben die neuen zugehörigen Listen oder Tabellen, für die Sie die Risikopunktzahl berechnen möchten, erfolgreich hinzugefügt.

> **Wichtig:**
> Um die Risikopunktzahl für Security Incidents mit neuen Kriterien für die neu erstellten zugehörigen Listen zu berechnen, müssen Sie in der Basistabelle der zugehörigen Liste Business-Regeln definieren.

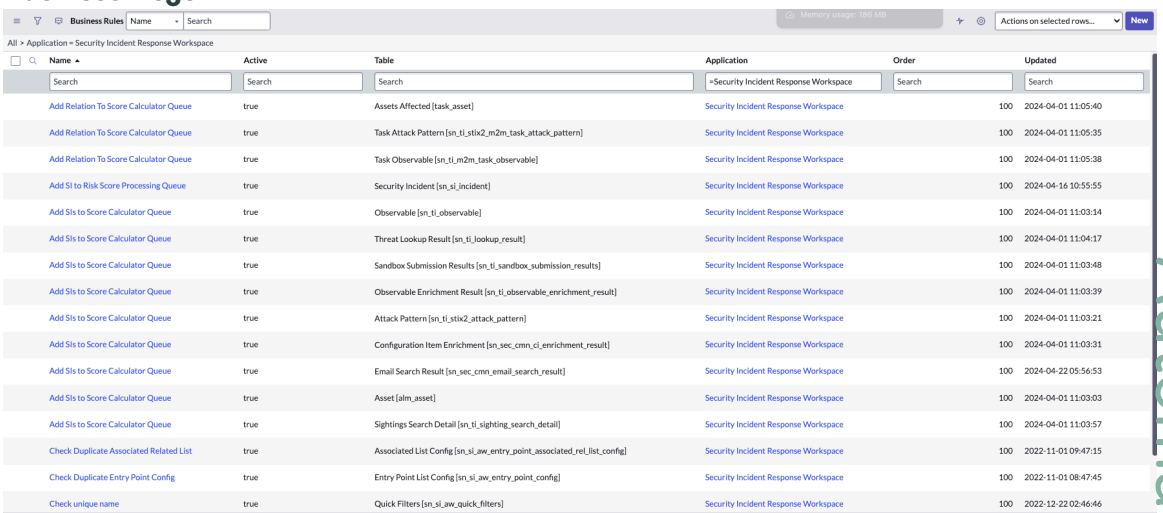
7. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die folgenden beiden Geschäftsregeln als Referenz für die Erstellung eigener Geschäftsregeln verwenden:

- Fügen Sie der Warteschlange des Bewertungsrechners Security Incidents (SIs) hinzu
- Beziehung zur Warteschlange des Punktzahlrechners hinzufügen (gilt für m2m-Tabellen)

Business-Regeln



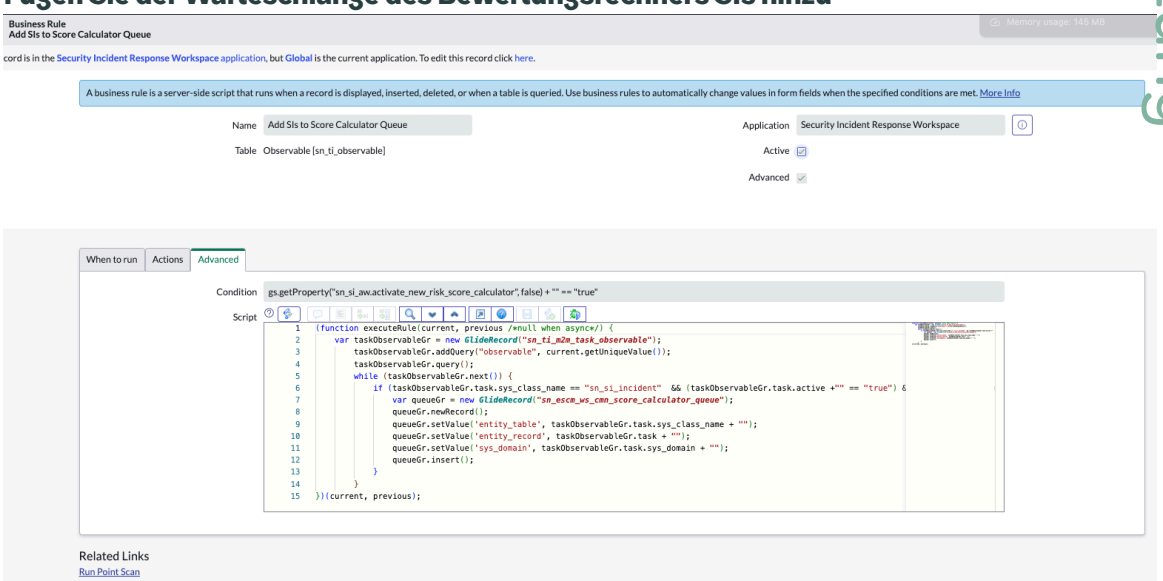
Name	Active	Table	Application	Order	Updated
Add Relation To Score Calculator Queue	true	Assets Affected [task_asset]	Security Incident Response Workspace	100	2024-04-01 11:05:40
Add Relation To Score Calculator Queue	true	Task Attack Pattern [sn_ti_stix2_m2m_task_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:05:35
Add Relation To Score Calculator Queue	true	Task Observable [sn_ti_m2m_task_observable]	Security Incident Response Workspace	100	2024-04-01 11:05:38
Add SI to Risk Score Processing Queue	true	Security Incident [sn_si_incident]	Security Incident Response Workspace	100	2024-04-16 10:55:55
Add SIs to Score Calculator Queue	true	Observable [sn_ti_observable]	Security Incident Response Workspace	100	2024-04-01 11:03:14
Add SIs to Score Calculator Queue	true	Threat Lookup Result [sn_ti_lookup_result]	Security Incident Response Workspace	100	2024-04-01 11:04:17
Add SIs to Score Calculator Queue	true	Sandbox Submission Results [sn_ti_sandbox_submission_results]	Security Incident Response Workspace	100	2024-04-01 11:03:48
Add SIs to Score Calculator Queue	true	Observable Enrichment Result [sn_ti_observable_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:39
Add SIs to Score Calculator Queue	true	Attack Pattern [sn_ti_stix2_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:03:21
Add SIs to Score Calculator Queue	true	Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:31
Add SIs to Score Calculator Queue	true	Email Search Result [sn_sec_cmn_email_search_result]	Security Incident Response Workspace	100	2024-04-22 05:56:53
Add SIs to Score Calculator Queue	true	Asset [alm_asset]	Security Incident Response Workspace	100	2024-04-01 11:03:03
Add SIs to Score Calculator Queue	true	Sightings Search Detail [sn_ti_sighting_search_detail]	Security Incident Response Workspace	100	2024-04-01 11:03:57
Check Duplicate Associated Related List	true	Associated List Config [sn_si_aw_entry_point_associated_rel_list_config]	Security Incident Response Workspace	100	2022-11-01 09:47:15
Check Duplicate Entry Point Config	true	Entry Point List Config [sn_si_aw_entry_point_config]	Security Incident Response Workspace	100	2022-11-01 08:47:45
Check unique name	true	Quick Filters [sn_si_aw_quick_filters]	Security Incident Response Workspace	100	2022-12-22 02:46:46

8. Damit beispielsweise die zugehörigen Kriterien für erkennbare Elemente funktionieren, haben wir zwei Geschäftsregeln definiert.

   Die erste ist die Geschäftsregel **„SIs zu Warteschlange des Bewertungsrechners hinzufügen“**.

   Beispielsweise wird ein neuer Security Incident erstellt und einer Tabelle erkennbarer Elemente (Observables[sn_ti_observable]) zugeordnet. Nach der Bedrohungssuche wird das erkennbare Element als schädlich erkannt. Anschließend müssen Sie alle Security Incidents, die diesem schädlichen erkennbaren Element zugeordnet sind, der Warteschlange hinzufügen, um die Risikopunktzahl der Security Incidents neu zu berechnen.

Fügen Sie der Warteschlange des Bewertungsrechners SIs hinzu

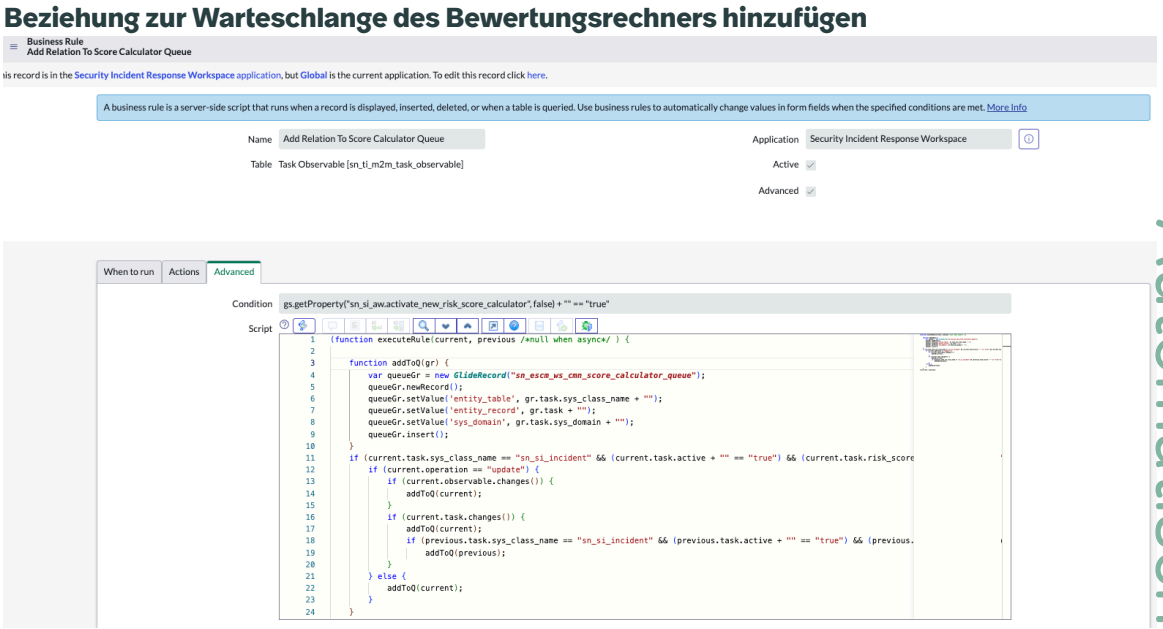


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die zweite Option ist die Geschäftsregel **„Beziehung zu Warteschlange des Bewertungsrechners hinzufügen“**.

Beispielsweise wird ein neuer Security Incident erstellt oder gelöscht und einer Tabelle erkennbarer Elemente (Task Observables[sn_ti_m2m_task_observable]) zugeordnet. Daher ändert sich die Zuordnung des Security Incident. Anschließend müssen Sie diesen Security Incident der Warteschlange hinzufügen, um die Risikopunktzahl für den Security Incident neu zu berechnen.



Konfigurieren Sie Schichtübergabevorlagen

Der Administrator kann verschiedene Schichtübergabevorlagen für den Schichtbesitzer definieren und konfigurieren, um Schichtübergabedatensätze zu erstellen und sie an das nächste Schichtteam zu übergeben.

Vorbereitungen

Erforderliche Rolle:

- sn_escm_sh.shift_admin
- sn_si.admin erbt die Rolle sn_escm_sh.shift_admin

Warum und wann dieser Vorgang ausgeführt wird

Zum Konfigurieren einer Schichtübergabevorlage erstellt der Administrator entweder eine neue Schichtübergabevorlage oder öffnet im Basissystem eine vorhandene Vorlage mit dem Namen **Beispiel-Schichtvorlage** und ändert die Details und Abschnitte entsprechend Ihren Anforderungen.

Der Schichtbesitzer kann die konfigurierte Vorlage verwenden, um Protokolldatensätze für die Schichtübergabe zu erstellen. Dann wird der Schichtübergabebericht für den nächsten aktiven Schichtbesitzer und das nächste aktive Team freigegeben.

Hinweis:
Nur die aktiven Schichtübergabevorlagen sind für den Schichtbesitzer sichtbar, um Übergabeprotokolldatensätze zu erstellen.

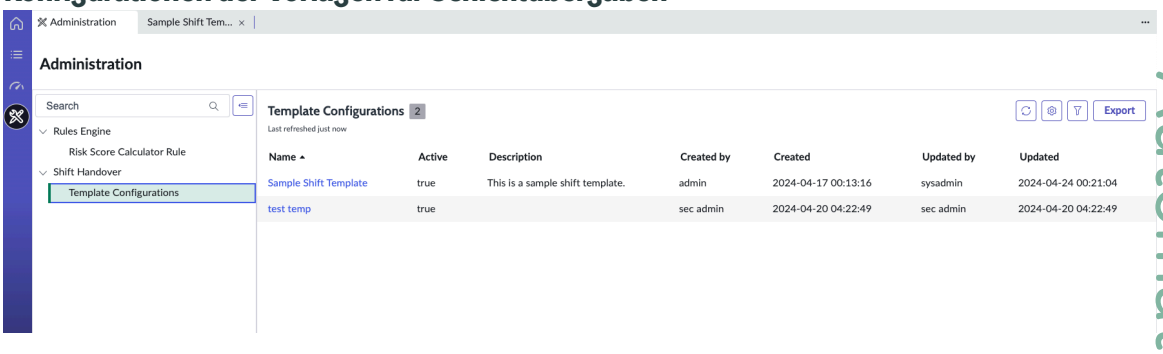
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Administration**.
2. Navigieren zu **Schichtübergabe** > **Vorlagenkonfigurationen**.
   Die Seite Vorlagenkonfigurationen wird angezeigt.

> **Hinweis:**
> Als Teil des Basissystems erhalten Sie eine vordefinierte Schichtübergabe-Vorlagenkonfiguration zum Anzeigen, Bearbeiten oder Ändern der Schichtübergabevorlage. Sie können die vordefinierte Konfiguration der Schichtübergabevorlage jedoch nicht erstellen oder löschen.

Konfigurationen der Vorlagen für Schichtübergaben



3. Um eine neue Schichtübergabe-Vorlage zu erstellen, wählen Sie **Neu**.
4. Füllen Sie die Felder im Detailformular aus.

Erstellen Sie eine neue Schichtübergabe-Vorlage

Feld	Beschreibung
Name	Name der Schichtübergabe-Vorlage. Beispiel: SIR-Vorlage.
Anwendung	Name der Anwendung, für die Sie die Schichtübergabevorlage erstellen. Beispiel: Arbeitsbereich für Security Incident Response.
Aktiv	Option, um anzugeben, ob die Vorlage „Schichtübergabe“ aktiv ist. Aktivieren Sie diese Option, um die Vorlage „Schichtübergabe“ zu aktivieren.
Beschreibung	Beschreibung der Schichtübergabe-Vorlage.
Konfiguration der Datensatzerwähnung	Verwenden Sie dieses Feld, um die Details zur Datensatzerwähnung des Rich-Text-Editors (RTE) zu konfigurieren. Die Eingabe ist ein Array von JSON-Objekten mit den folgenden Feldern: ○ `sourceTable`: Name der Quelltabelle. ○ `label`: Name der anzuzeigenden Bezeichnung. ○ `filterCondition`: Codierte Abfrage zum Filtern ○ `fields`: Wählen Sie die Felder aus, um das Muster abzufragen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

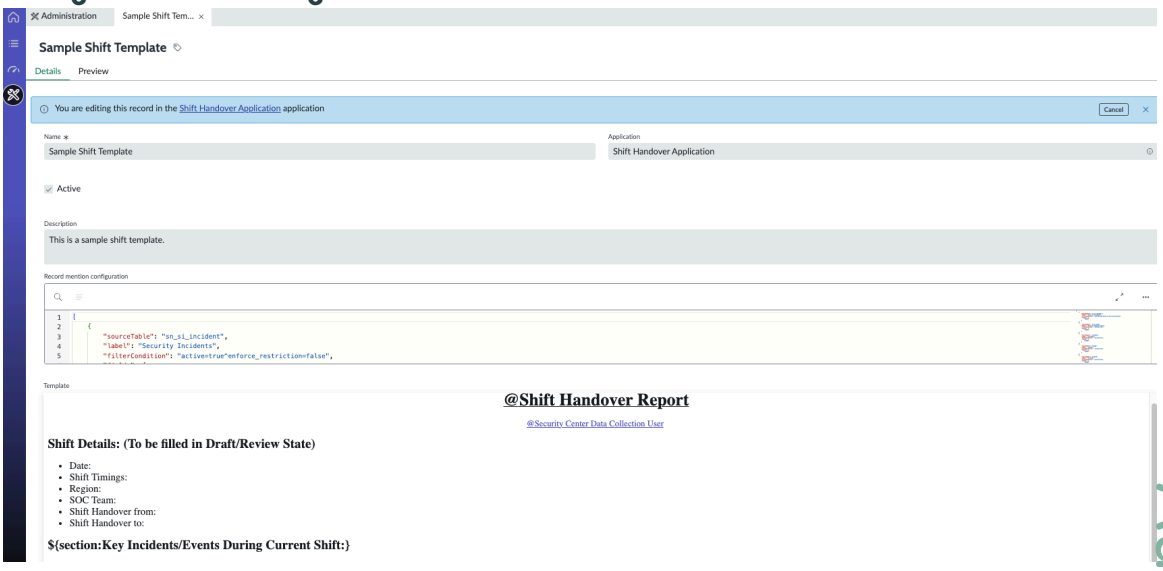
Feld	Beschreibung
	Beispielkonfiguration, die Sie kopieren und in das Feld „Konfiguration der Datensatzerwähnung“ einfügen können. `[ { "sourceTable": "incident", "label": "Incidents", "filterCondition": "active=true", "fields": [ "number" ] } ]` Um die Beispielkonfiguration zu kopieren, verwenden Sie die Aktion **In Zwischenablage kopieren** im Bereich Kontexthilfe. Anschließend können Sie basierend auf Ihren Anforderungen zusätzliche Änderungen vornehmen.

Vorlage	Erstellen Sie mithilfe von Abschnitten eine Schichtübergabevorlage. Stellen Sie sicher, dass es mindestens einen Abschnitt gibt, in dem Analysten basierend auf der Vorlage zu den Datensätzen der Schichtübergabeprotokolle beitragen können.
	Die Vorlage kann in den entsprechenden Abschnitten statischen Text, Bilder usw. enthalten. Sie können Bilder kopieren und direkt in das Feld Vorlage einfügen. Sie können Abschnitte in der Vorlage mit dem folgenden Code erstellen:
	`${section:Section Label}`
	Beispiel:
	`${section:Key Incidents/Events During Current Shift}`
	`${section:Incidents/Events to Monitor or Follow Up}`
	`${section:System/Infrastructure Updates}`
	`${section:Next Steps for Incoming Shift}`
	`${section:References}`
	Hinweis:
	Weitere Informationen finden Sie unter **Kontextbezogene Hilfe** im rechten Bereich.

5. Um eine vorhandene Schichtübergabevorlage zu verwenden und zu ändern, wählen Sie **Beispiel für Schichtvorlage**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

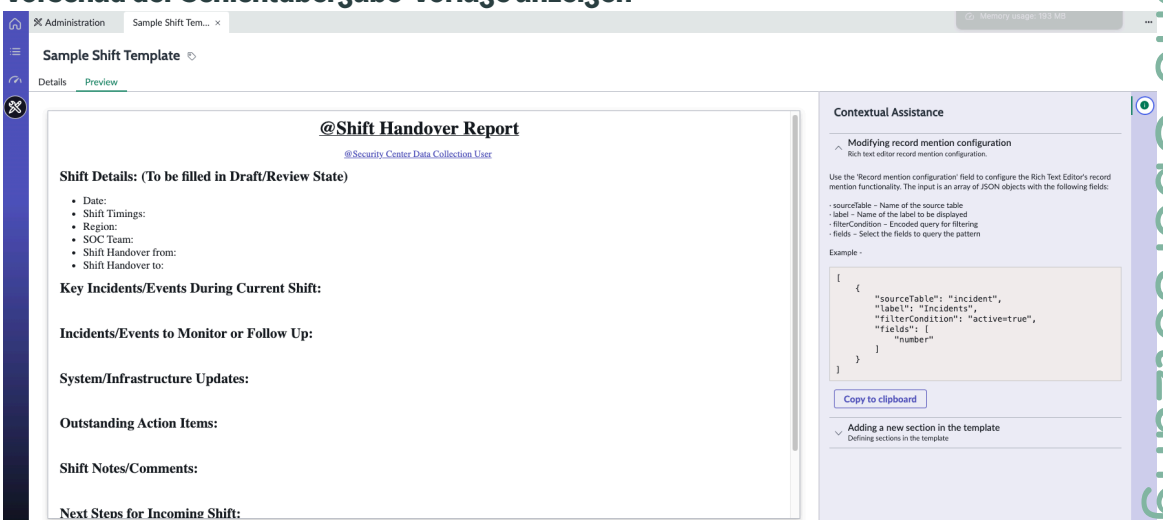
Vorlage für Schichtübergabe



6. Aktualisieren Sie die Schichtübergabe-Vorlage entsprechend Ihren Anforderungen.
7. Wählen Sie **Vorschau** aus, um die Laufzeitvorschau der Schichtübergabevorlage anzuzeigen.

   Der Bericht generiert eine Vorschau basierend auf der Konfiguration der Schichtübergabevorlage.

Vorschau der Schichtübergabe-Vorlage anzeigen



8. Wählen Sie **Speichern** aus, um die Vorlage für die Schichtübergabe zu speichern.

Nächste Maßnahme

Informationen zum Verwalten von Schichtübergabedatensätzen in der Listenansicht und zum Ausführen von Aktionen wie das Erstellen, Bearbeiten, Kopieren oder Löschen von Schichtübergabedatensätzen finden Sie unter Verwalten Sie Schichtübergabe-Datensätze.

Security Incident Response Telefonkonferenz

Mit der Security Incident Response Telefonkonferenz-Integration können Sie Telefonkonferenzen und Chats für Analysten, Manager und betroffene Benutzer verwalten und initiieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit der Telefonkonferenzfunktion Security Incident Response von können Sie mit Kunden und Kollegen zusammenarbeiten, um Security Incidents während eines Anrufs zu lösen. Sie können auch über einen Gruppenchat zusammenarbeiten.

Sie können Telefonkonferenzen über Kommunikationskanäle von Drittparteien wie Microsoft Teams, Cisco Webex oder Zoom-Meetings initiieren. Verwenden Sie für die Zusammenarbeit per Chat den Sidebar-Chat der SIR-Anwendung.

Schlüsselfunktionen

Die Zusammenarbeit beim Anrufen von Security Incident Response bietet die folgenden wichtigen Funktionen:

- SIR-Manager/-Analysten können eine Microsoft Teams-, Cisco Webex- oder Zoom-Telefonkonferenz direkt aus dem Security Incident initiieren.
- SIR-Manager/Analysten können einen Chat direkt in der Anwendung SIR initiieren.
- Laden Sie zusätzliche Teilnehmer zum Anruf oder Chat ein.
- Zeigen Sie Anrufaufzeichnungen und Chatdetails an.
- Senden Sie Einladungen per E-Mail und im Microsoft Teams-Chat an Teilnehmer.

Verwalten Sie Anwender und Gruppen für Telefonkonferenzen

Der Administrator kann Telefonkonferenzeinstellungen so konfigurieren, dass eine vordefinierte Liste von Benutzern und Gruppen angezeigt wird, die einem Anruf hinzugefügt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereiche für Security Incident Response** > **Administration**.
2. Wählen Sie **Telefonkonferenz**und dann **Anrufkonfiguration**aus.
3. Wählen Sie auf der Seite Anrufkonfigurationen **die Option Konferenzanrufkonfiguration**aus. Die Konfigurationsseite wird angezeigt, um eine vordefinierte Liste von Benutzern und Gruppen zu konfigurieren.
4. Füllen Sie die Felder im Detailformular aus.

Feld	Beschreibung
Name	Name der Konferenzanrufkonfiguration.
Anwender automatisch ausfüllen	Option zum automatischen Ausfüllen der konfigurierten Benutzer für eine Telefonkonferenz. Wenn Sie diese Option auswählen, werden die konfigurierten Benutzer und Gruppen einer Telefonkonferenz hinzugefügt. **Hinweis:** Sie können Anwender/Gruppen auch hinzufügen oder entfernen, wenn Sie einen Anruf einleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Betroffene Anwender anzeigen	Option zum Anzeigen der betroffenen Benutzer zum Hinzufügen zu einem Anruf.
Zuweisungsgruppenanwender anzeigen	Option zum Anzeigen der Zuweisungsgruppenanwender, die einem Anruf hinzugefügt werden sollen.
Standardgruppen	Option zum Hinzufügen von Standardgruppen, die zu einem Anruf hinzugefügt werden sollen.
Standardanwender	Option zum Hinzufügen von Standardbenutzern zum Hinzufügen zu einem Anruf.

5. Wählen Sie **Speichern** aus, um die Konferenzanrufkonfiguration zu speichern.

Integrieren Sie SIR in Kommunikationskanäle von Drittparteien

Die Integration der SIR-Telefonkonferenz mit Kommunikationskanälen von Drittanbietern wie Microsoft Teams, Zoom und Cisco Webex ermöglicht es Ihnen, einen Anruf direkt aus einem Security Incident heraus zu verwalten und zu initiieren.

Schlüsselfunktionen

- Starten und beenden Sie Telefonkonferenzen direkt von einem beliebigen Security Incident aus.
- Einer Telefonkonferenz Teilnehmer hinzufügen oder entfernen.
- Verfolgen und melden Sie Besprechungsdetails wie Besprechungsdauer und Teilnehmer zur weiteren Analyse.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Integration Hub-Plugins in Ihrer ServiceNow-Instanz installiert sind.

- Notify-Plugin (com.snc.notify). Weitere Informationen finden Sie unterConfiguring Notify
- Notify-UI-Komponenten für konfigurierbare Arbeitsbereiche
- So integrieren Sie Microsoft Teams als Kommunikationskanal:
  - Microsoft Teams Communications-Spoke-Plugin (sn_msteams_com_spk).
  - Azure Active Directory User Mapping-Plugin (sn_now_azure).
- So integrieren Sie Zoom als Kommunikationskanal:
  - Zoom-Spoke (sn_zoom_spoke)
  - Notify Zoom (sn_notify_zoom)
- So integrieren Sie Cisco Webex als Kommunikationskanal:
  - Notify Cisco Webex-Connector (sn_notify_webex)
  - Cisco Webex Teams-Spoke (sn_cisco_teams_spk)

Weitere Informationen finden Sie unter Request Integration Hub .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration

Führen Sie die folgende Konfiguration für die Kommunikationskanäle durch, die Sie verwenden möchten:

- Informationen zur Konfiguration der Cisco Webex-Integration für Telefonkonferenzen über den Notify-Kommunikationskanal finden Sie unter Configure Notify Cisco Webex Connector .
- Informationen zur Konfiguration der Zoom-Integration für Telefonkonferenzen über den Notify-Kommunikationskanal finden Sie unter Configure Notify Zoom connector in Notify .
- Informationen zur Konfiguration der Microsoft Teams-Integration für Telefonkonferenzen mit der vorkonfigurierten App finden Sie unter Integrate Notify connector pre-published app with Microsoft Teams .
- Informationen zur Konfiguration der Microsoft Teams-Integration für Telefonkonferenzen mit der selbstkonfigurierten App finden Sie unter Integrating Notify connector self-configured app with Microsoft Teams .

Konfigurieren Sie Berichtsvorlagen in Security Incident Response

Sie können Berichtsvorlagen erstellen, die zum Generieren einer Incident-Zusammenfassung oder einer Kurzübersicht zur Analyse und Freigabe verwendet werden können.

Verwenden Sie die Funktion Security Incident Response Berichtsvorlagen, um Berichtsvorlagen für die Generierung von Berichten zu erstellen, die eine Zusammenfassung eines incident auf Analyst- oder Führungsebene bereitstellen. Sie können den Bericht mithilfe verschiedener Incident-Felder entsprechend Ihren Anforderungen formatieren und konfigurieren.

In der folgenden Tabelle werden die Berichtsvorlagen erläutert, die im Basissystem bereitgestellt werden.

Berichtsvorlagen in Security Incident Response

Name	Beschreibung
Status-Reporting durch Analysten	Stellt vollständige Informationen zu einem Security Incident für einen Analysten bereit.
Kurzübersicht	Bietet eine Übersicht über den Status eines Security Incident für die -Verwaltung.

Hinweis:
Standardmäßig befinden sich diese Berichte im Entwurfsstatus und im schreibgeschützten Modus. Sie müssen diese Standardvorlagen wiederverwenden, um Berichtsvorlagen zu erstellen und zu veröffentlichen.

Erstellen Sie eine Berichtsvorlage in Security Incident Response

Erstellen Sie eine neue Berichtsvorlage für die Analystenzusammenfassung oder die Kurzübersicht für einen Incident.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereiche für Security Incident Response** > **Administration**.
2. Wählen Sie **Berichte**und dann **Berichtsvorlagen**aus.
   Die Seite „Berichtsvorlagen“ wird mit allen im Basissystem verfügbaren Vorlagen angezeigt.
3. Wählen Sie **Neu**.
   Zeigt die **Detailseite** der Vorlage an.
4. Geben Sie den Namen und die Beschreibung der Vorlage ein.
5. Wählen Sie **Speichern**.
6. Wählen Sie die Registerkarte **Inhalt**.
   Zeigt die Inhaltsseite der Vorlage mit einem leeren Bericht an.
7. Wählen Sie **Erweitern** aus, und fügen Sie die gewünschten Felder in den Vorlagentext ein.
   - **Allgemeine SIR-Felder**: Liste der am häufigsten verwendeten Felder für einen Incident.
   - **Alle SIR-Felder**: Alle Felder im Zusammenhang mit einem Incident. Wenn Sie beispielsweise einen Incident-Bericht generieren und ein Feld mit der Bezeichnung Kurzbeschreibung hinzufügen möchten, können Sie dieses Feld unter Alle SIR-Felder auswählen. Das Feld Kurzbeschreibung wird als Variable in der Berichtsvorlage hinzugefügt. Wenn Sie einen Bericht für den Analysten generieren, wird die Kurzbeschreibung des incident im Bericht angezeigt.
   - **Zugehörige Datensätze**: Die zugehörigen Datensätze eines bestimmten Incidents. Wenn Sie dem Bericht beispielsweise zugeordnete erkennbare Elemente hinzufügen möchten, können Sie diese Ihrer Berichtsvorlage hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt
   - **Skripts**: Um das Datum und die Uhrzeit des Berichts hinzuzufügen, können Sie Ihrer Berichtsvorlage das Skript „Aktuelles Datum/Uhrzeit“ hinzufügen. Dadurch werden das Datum und die Uhrzeit der Berichterstellung im Bericht hinzugefügt.
   -
8. Wählen Sie **Inhalt speichern** aus, um den Inhalt Ihrer Berichtsvorlage zu speichern.
9. Wählen Sie **Vorschau**, um eine Vorschau Ihres Berichtsformats anzuzeigen.

   Nachdem Sie Ihrer Berichtsvorlage alle erforderlichen Felder hinzugefügt haben, müssen Sie Ihre Berichtsvorlage veröffentlichen.
10. Wählen Sie **Veröffentlichen** aus, um die Vorlage zu veröffentlichen.

    Ob Sie die Berichtsvorlage veröffentlichen möchten oder nicht wird eine Bestätigungsmeldung angezeigt.
11. **Wahlweise:** Wählen Sie das Symbol „ **Weitere Aktionen“** und dann **Löschen**, um die Berichtsvorlage zu löschen.

Systemeigenschaften für Berichte

Die Systemeigenschaften für Security Incident Response -Berichte werden unten erläutert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften für Berichte

Eigenschaft	Beschreibung	Wert
sn_si.sn_si_incident.load_all_records	Lädt alle Datensätze für die Listen im Bericht, die aus einer Vorlage erstellt wurden. „true“ – lädt alle Datensätze; „false“ – lädt eine bestimmte Anzahl von Datensätzen, die durch die Eigenschaft „sn_si.sn_si_incident.reporting_list_records_count“ definiert ist.	falsch
sn_si.sn_si_incident.max_list_columns_allowed	Anzahl der Spalten beschränken, die beim Rendern von Listen in PDF-Berichten hinzugefügt werden können. Dadurch werden die Spalten vom Anfang der Ansicht bis zum zulässigen Grenzwert verwendet.	5
sn_si.sn_si_incident.report_default_style_object	Verwenden Sie diese Eigenschaft, um die CSS von freien Formfeldern, dem linken Bereich und der Berichtslisten zu steuern.	(JSON-Objekt)
sn_si.sn_si_incident.reporting_list_records_count	Lädt eine bestimmte Anzahl von Datensätzen im Berichtseditor.	200
sn_si_reporting_email_template_sn_si_incident	System-ID der E-Mail-Client-Vorlage für die SIR-Tabelle (sn_si_incident), die im freigegebenen Bericht verwendet wird.	9ce97ae643461210416896ed3ab8f258
sn_si.sn_si_incident.ctx_menu_field_header	Feldheader	sn_si_incident_report_field_header, sn_si_incident_report_list_header
sn_si.sn_si_incident.defang_record_list_urls	Steuern Sie, ob die URLs aus der Liste entsperrt sind oder nicht.	falsch
sn_si.sn_si_incident.reporting_punkt_walk_tables	Liste der Tabellen, die für Dot-Walking in Berichten verfügbar sind.	(JSON-Objekt)

Duplizieren Sie eine Berichtsvorlage in Security Incident Response

Duplizieren Sie eine Berichtsvorlage, um sie zu bearbeiten, oder verwenden Sie eine vorhandene Vorlage, um eine neue Vorlage zu erstellen.

Vorbereitungen

Hinweis:
Sie müssen eine Kopie der Vorlagen für die Zusammenfassung und das Analyst Status Reporting erstellen, um sie wiederzuverwenden.

Um die Kurzzusammenfassung und die Analystenstatusberichte wiederzuverwenden, müssen Sie eine Kopie dieser erstellen und dann

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereiche für Security Incident Response** > **Administration**.
2. Wählen Sie **Berichte**und dann **Berichtsvorlagen**aus.
   Die Seite „Berichtsvorlagen“ wird mit allen im Basissystem verfügbaren Vorlagen angezeigt.
3. Wählen Sie die Vorlage aus.
4. Wählen Sie **Duplikat**aus.

Ergebnisse

Der Inhalt der ausgewählten Vorlage wird dupliziert, und eine Kopie der ausgewählten Vorlage ist in der Liste der Vorlagen verfügbar. Die duplizierte Vorlage befindet sich im Status Entwurf. Sie können den Inhalt anpassen und die Vorlage dann bei Bedarf umbenennen.

Nächste Maßnahme

Bearbeiten Sie eine Berichtsvorlage in Security Incident Response

Bearbeiten Sie eine Berichtsvorlage in Security Incident Response

Bearbeiten Sie eine Berichtsvorlage, um eine vorhandene Vorlage wiederzuverwenden und eine neue Vorlage zu erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereiche für Security Incident Response** > **Administration**.
2. Wählen Sie **Berichte**und dann **Berichtsvorlagen**aus.
   Die Seite „Berichtsvorlagen“ wird mit allen im Basissystem verfügbaren Vorlagen angezeigt.
3. Wählen Sie die Vorlage aus.
   Zeigt die Registerkarte **Details** der Vorlage im Bearbeitungsmodus an.
4. Aktualisieren Sie den Namen und die Beschreibung der Vorlage.
5. Wählen Sie **Speichern**.
6. Wählen Sie die Registerkarte **Inhalt**.
   Zeigt die Inhaltsseite der Vorlage mit einem leeren Bericht an.
7. Wählen Sie **Erweitern** und fügen Sie die gewünschten Felder ein/entfernen Sie sie.
   - **Allgemeine SIR-Felder**: Liste der am häufigsten verwendeten Felder für einen Incident.
   - **Alle SIR-Felder**: Alle Felder im Zusammenhang mit einem Incident. Wenn Sie beispielsweise einen Incident-Bericht generieren und ein Feld mit der Bezeichnung Kurzbeschreibung hinzufügen möchten, können Sie dieses Feld unter Alle SIR-Felder auswählen. Das Feld Kurzbeschreibung wird als Variable in der Berichtsvorlage hinzugefügt. Wenn Sie einen Bericht für den Analysten generieren, wird die Kurzbeschreibung des incident im Bericht angezeigt.
   - **Zugehörige Datensätze**: Die zugehörigen Datensätze eines bestimmten Incidents. Wenn Sie dem Bericht beispielsweise zugeordnete erkennbare Elemente hinzufügen möchten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie diese Ihrer Berichtsvorlage hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt

- **Skripts**: Um das Datum und die Uhrzeit des Berichts hinzuzufügen, können Sie Ihrer Berichtsvorlage das Skript „Aktuelles Datum/Uhrzeit“ hinzufügen. Dadurch werden das Datum und die Uhrzeit der Berichterstellung im Bericht hinzugefügt.

8. Wählen Sie **Inhalt speichern** aus, um den Inhalt Ihrer Berichtsvorlage zu speichern.
9. Wählen Sie **Vorschau**, um eine Vorschau Ihres Berichtsformats anzuzeigen.

   Nachdem Sie Ihrer Berichtsvorlage alle erforderlichen Felder hinzugefügt haben, müssen Sie Ihre Berichtsvorlage veröffentlichen.

10. Wählen Sie **Veröffentlichen** aus, um die Vorlage zu veröffentlichen.

    Ob Sie die Berichtsvorlage veröffentlichen möchten oder nicht wird eine Bestätigungsmeldung angezeigt.

SIR Workspace verwenden

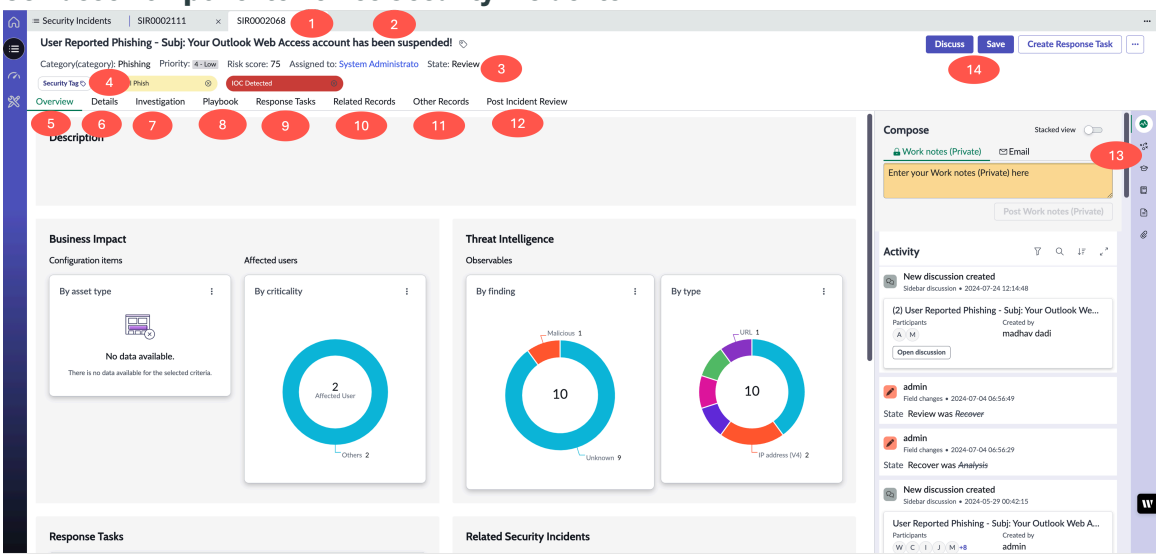
Sicherheitsanalysten und -manager verwenden SIR Workspace, um bei täglichen Vorgängen eine verbesserte Anwender-Experience zu bieten, Incident-Untersuchungen durchzuführen und sich einen Überblick zu verschaffen.

Arbeiten mit Security Incident-Datensätzen

Der Security Incident Record besteht aus folgenden Komponenten.

Wichtige Komponenten, die für einen Security Incident-Datensatz verfügbar sind:

Schlüsselkomponenten eines Security Incidents



Nummer	Name	Beschreibung
1	Nummer des Security Incidents	Die Nummer des Security Incidents ist gegen den Registerkartennamen verfügbar.
2	Kurzbeschreibung	Kurzbeschreibung des Security Incident, die über dem Formularbanner angezeigt wird.
3	Formularbanner	Dies ist ein schreibgeschützter Abschnitt, der die wichtigsten Felder wie Kategorie, Priorität,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nummer	Name	Beschreibung
		Risikopunktzahl, Status und die Details der Incident-Zuweisung enthält. **Hinweis:** Die regulären Plattform-Tags können auch hier angewendet werden.
4	Sicherheits-Tags	Zeigt die Sicherheits-Tags an, die einem Security Incident zugeordnet sind.
5	Übersicht	Bietet eine Snapshot-Übersicht über den Security Incident, z. B. Beschreibung, Geschäftsauswirkung mit Asset-Details nach Typ, betroffene Anwender nach Relevanz, Threat Intelligence-Elemente mit erkennbaren Elementen nach Ergebnis und Typ, Antwortaufgaben, zugehörige Security Incidents mit untergeordneten Security Incidents und ähnliche Security Incidents.
6	Details	Auf der Registerkarte „Details“ wird das Formular „Security Incident“ angezeigt.
7	Ermittlung	Auf der Registerkarte Ermittlung wird die Experience der Incident-Untersuchung angezeigt.
8	Playbook	Playbook wird über den Prozessautomatisierungs-Designer (PAD) ausgelöst. Ob ein Prozess erstellt wird und ob eine Auslöserbedingung festgelegt ist, um das Playbook für einen Security Incident auszulösen. Dann wird ein Playbook angezeigt.
9	Antwortaufgaben	Die Antwortaufgaben erfassen alle Antwortaufgaben, die einem Security Incident zugeordnet sind.
10	Zugehörige Datensätze	Die Registerkarte Zugehörige Datensätze besteht aus allen zugehörigen Listen aus der klassischen Anwenderoberfläche in diesem Abschnitt. Die zugehörigen Listen sind unter verschiedenen Abschnitten wie Geschäftsauswirkung, Bedrohungsinformationen usw. gruppiert, um die Navigation zu erleichtern.
11	Andere Datensätze	Die Registerkarte Andere Datensätze besteht aus IT-Datensätzen wie Change-Anforderungen, Incidents und E-Mails, die in diesem Abschnitt gruppiert und angezeigt werden.
12	Registerkarte Überprüfung nach Incident	Während der Security Incident in den Status Überprüfen übergeht, wird die Registerkarte Überprüfung nach Incident mit den Bewertungen und Berichten nach Incident angezeigt.
13	Kontextmenü	Bietet einfachen Zugriff auf Schnellaktionen und ist auf allen Registerkarten verfügbar, auf die Analysten bei Bedarf zugreifen können. Das Kontextmenü bietet eine einfache Navigation zu den verschiedenen Ressourcen, z. B.:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nummer	Name	Beschreibung
		1. Aktivitätenstrom **2.** Playbook **3.** Analyst Assist **4.** Ausführungsbuch **5.** Vorlagen **6.** Anhänge
14	Formular-UI-Aktionen	Die verschiedenen UI-Aktionen für Security Incident-Formulare werden oben rechts im Incident-Formular angezeigt. Die für Formulare verfügbaren UI-Aktionen sind: • Diskutieren • Speichern • Antwortaufgabe erstellen • E-Mail erstellen • Playbook hinzufügen • Verknüpfte(n) Workflow(s) öffnen • Incident erstellen • Problem erstellen • Change-Anforderung erstellen • Ausfall erstellen • Schweregrad berechnen • Verknüpfen mit Major Security Incident • Vorschlagen als Major Security Incident • Heraufstufen zu Major Security Incident • Zusätzliche Aktion(en) für Endpunkt ausführen • Ordnen Sie die MITRE ATT&CK-Technik zu • Zu klassischer UI wechseln • Dem Sicherheitsfall hinzufügen • Löschen Weitere Informationen finden Sie unter Arbeiten mit Formular-UI-Aktionen.

Abschnitt „Übersicht über Security Incident“.

Der Abschnitt Übersicht im -Arbeitsbereich enthält die wichtigsten Informationen, die dem Security Incident zugeordnet sind.

Die Ringdiagramme sind Drilldown-fähig. Wenn ein Analyst eines der Diagrammelemente auswählt, werden Sie zum jeweiligen Datensatz mit einer gefilterten Listenansicht von Elementen auf der entsprechenden Registerkarte navigiert. Wenn beispielsweise

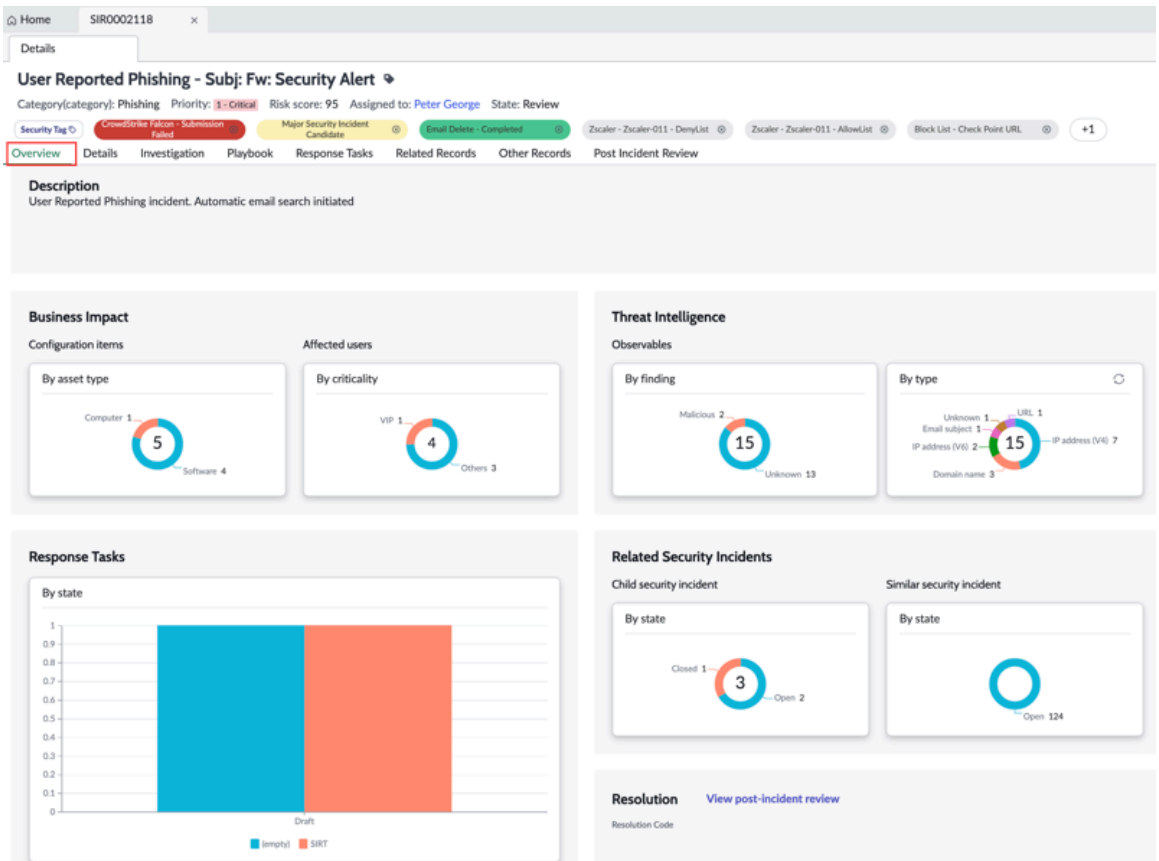
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Böswillige erkennbare Elemente “ ausgewählt ist, gelangen Sie zu den erkennbaren Elementen mit einer gefilterten Listenansicht der schädlichen erkennbaren Elemente auf der **Registerkarte Zugehörige** Datensätze.

Im Abschnitt Übersicht wird Folgendes angezeigt:

- Beschreibung des Security Incidents.
- Geschäftsauswirkungsdetails, z. B. Konfigurationselemente nach Asset-Typ und betroffene Benutzer nach Relevanz – VIP-Benutzer oder andere Benutzer.
- Threat Intelligence-Elemente wie erkennbare Elemente, indem ermittelt wird, ob die erkennbaren Elemente schädlich oder unbekannt sind, sowie nach Typ.
- Antwortaufgaben nach Status und Zuweisungsgruppe.
- Zugehörige Security Incidents, bestehend aus untergeordneten Security Incidents nach Status – offen oder geschlossen – und ähnlichen Security Incidents nach Status – offen oder geschlossen.
- Der Abschnitt „Lösung“ wird angezeigt, wenn ein Incident in den Status „Überprüfen“ wechselt. Anschließend wird der Abschnitt „Lösung“ im Abschnitt **„Übersicht“** angezeigt, mit der Möglichkeit, die Überprüfung nach Incident anzuzeigen.
- Lösung – Überprüfung nach Incident anzeigen: Wählen Sie den Link, um zur Seite **„Überprüfung nach Incident“** zu navigieren.
- Nachdem der Incident geschlossen wurde, werden im Abschnitt „Lösung“ der Lösungscode, Lösungshinweise und „Gelöst von (Benutzer)“ zusammen mit Details zur Überprüfung nach Incident angezeigt.

Übersichtsbereich



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Abschnitt „Details“.

In diesem Abschnitt werden die Felder des Security Incident-Formulars angezeigt, die von der klassischen Security Incident-UI gerendert werden.

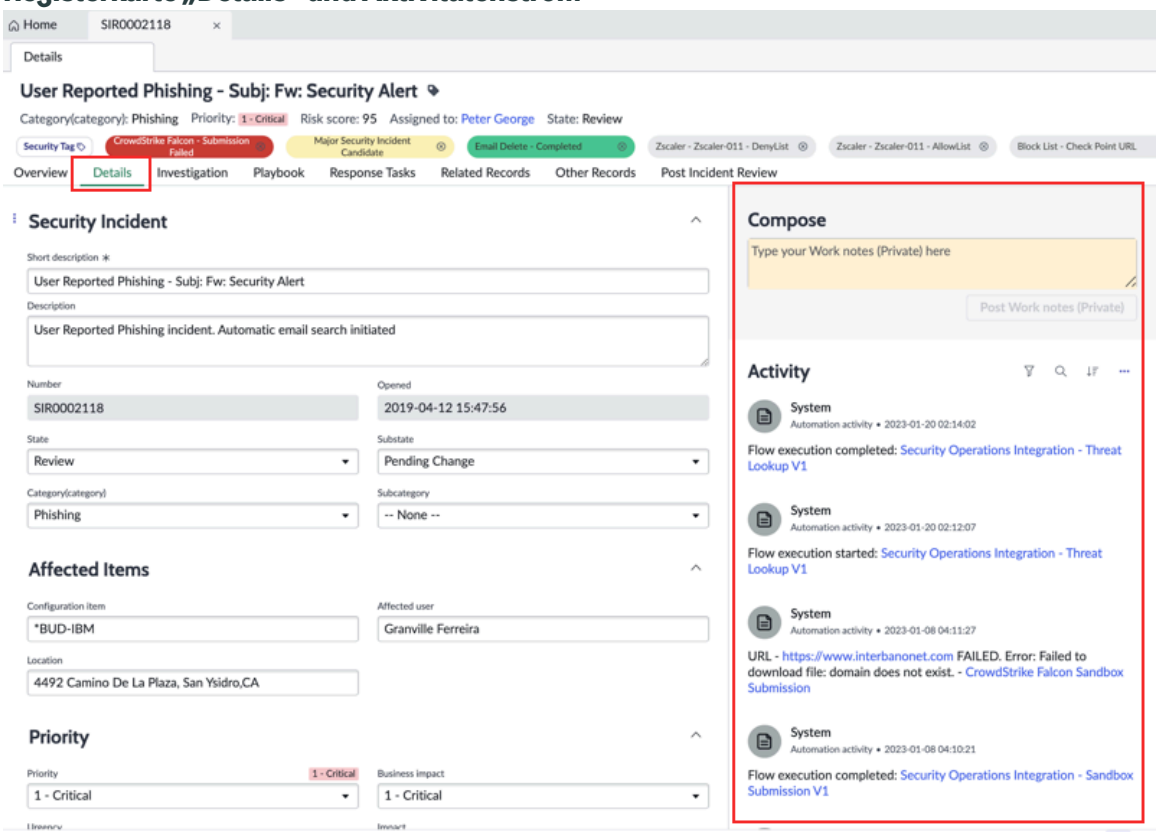
Für die klassische UI wurde eine Ansicht namens **„SIRW** -Ansicht“ erstellt. Diese Ansicht ist der Registerkarte **Details** im neuen Arbeitsbereich zugeordnet. Alle erforderlichen Anpassungen müssen in dieser Ansicht implementiert werden.

Die Formularfelder sind in die folgenden Abschnitte gruppiert und werden auf der Formularansicht der Registerkarte „Details“ angezeigt. Klicken Sie auf einen beliebigen Abschnitt, oder springen Sie zum entsprechenden Abschnitt im Formular:

- Security Incident
- Priorität
- Quelle
- Übergeordnet
- Zuweisung
- Zugriffssteuerungen
- Betroffene Elemente
- Lösung

Die Registerkarte **„Details“** enthält den Abschnitt „ **Aktivitätenstrom** “ innerhalb des Detailformulars selbst, über das die Sicherheitsanalysten schnell Kommentare hinzufügen und veröffentlichen können.

Registerkarte „Details“ und Aktivitätenstrom

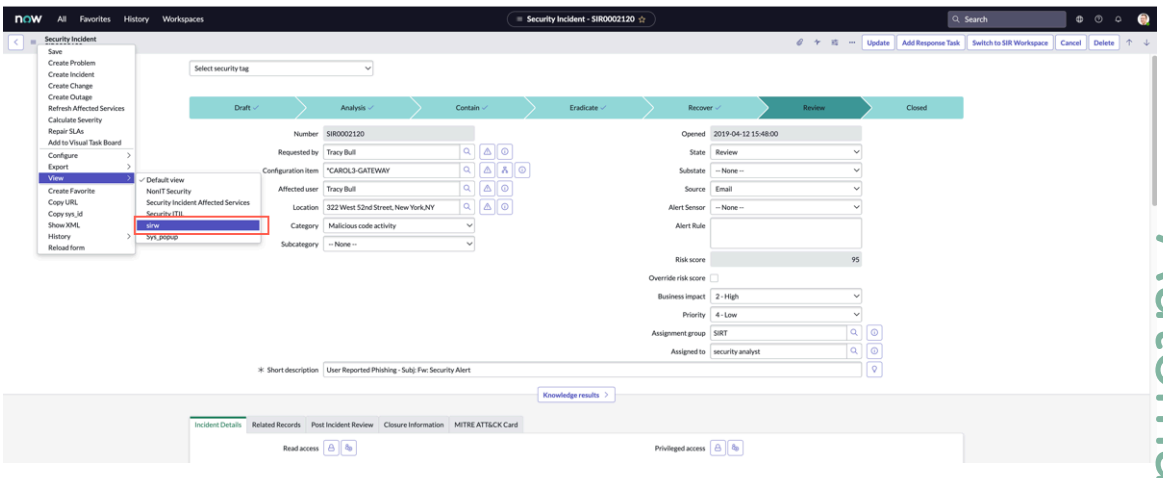


Wie rufen Sie die Ansicht „SIR-Analystenarbeitsbereich“ auf?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

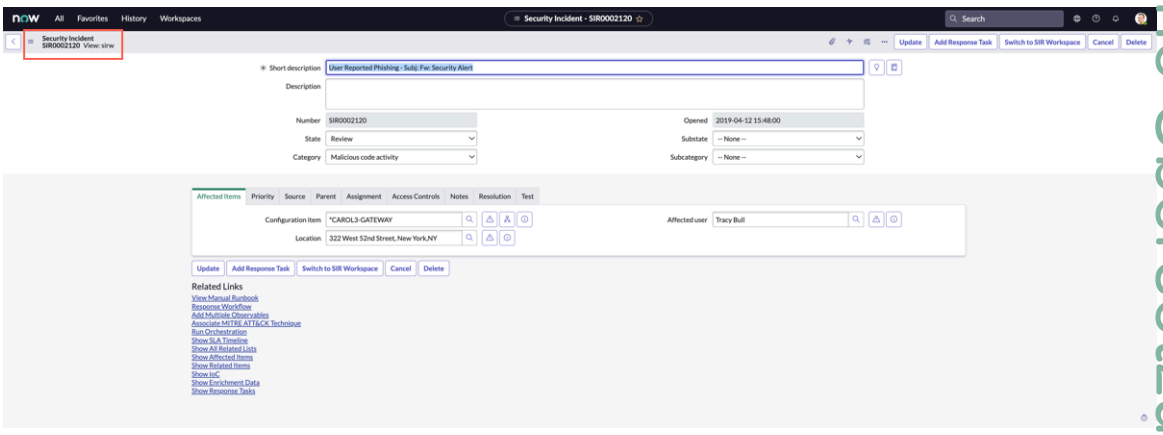
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Wählen Sie einen beliebigen Security Incident-Datensatz aus.
3. Klicken Sie auf das Kontextmenü, und wählen Sie **Ansicht** > **sirw**.

Hinweis:
Sie können die Ansicht **des Sirw** -Arbeitsbereichs im klassischen UI-Formular anpassen.



4. Die Ansicht des Security Incident-Arbeitsbereichs wird wie unten gezeigt gerendert.

Ansicht des SIR-Arbeitsbereichs

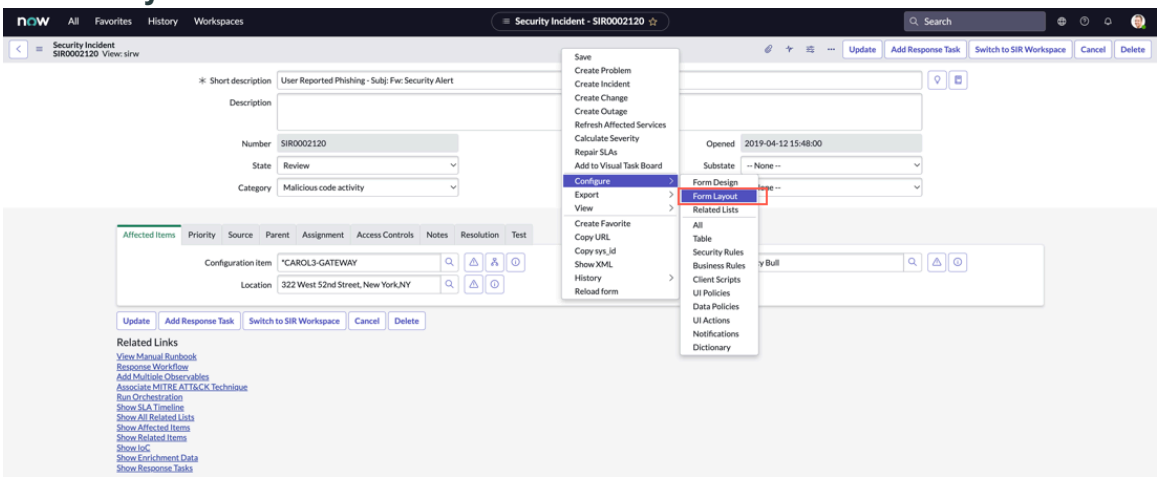


5. Klicken Sie im Datensatz des Security Incident mit der rechten Maustaste, und wechseln Sie zu **Konfigurieren** > **Formularlayout**.

Automatische Übersetzung

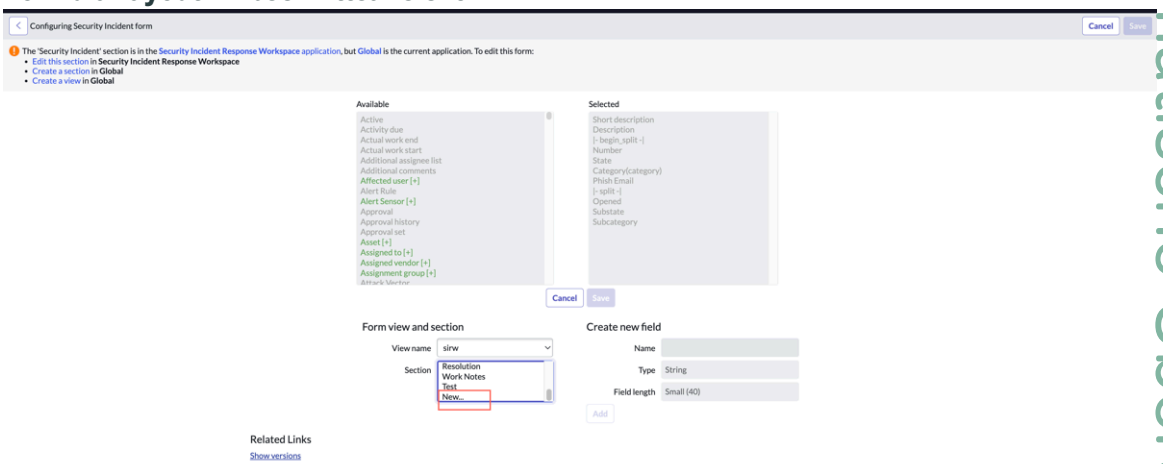
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularlayout



6. Führen Sie einen Drilldown zur **Formularansicht und zum Abschnitt** durch, und wählen Sie **Neu** aus **Abschnitt**, um einen neuen Abschnitt zu erstellen.

Formularlayout – Abschnittsansicht

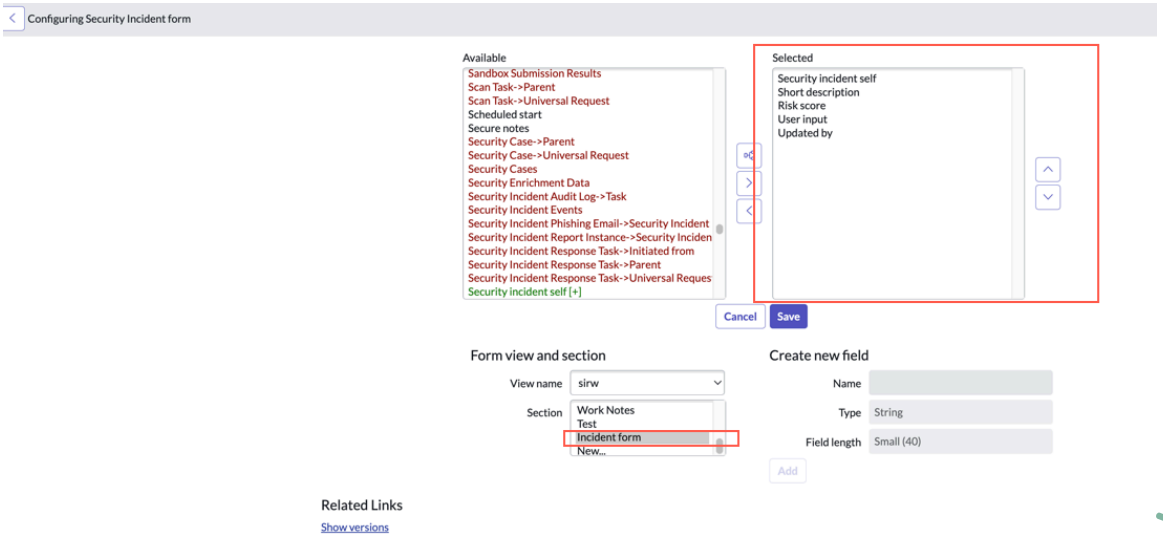


7. Geben Sie den Namen des neuen Abschnitts ein, und klicken Sie auf **OK**.

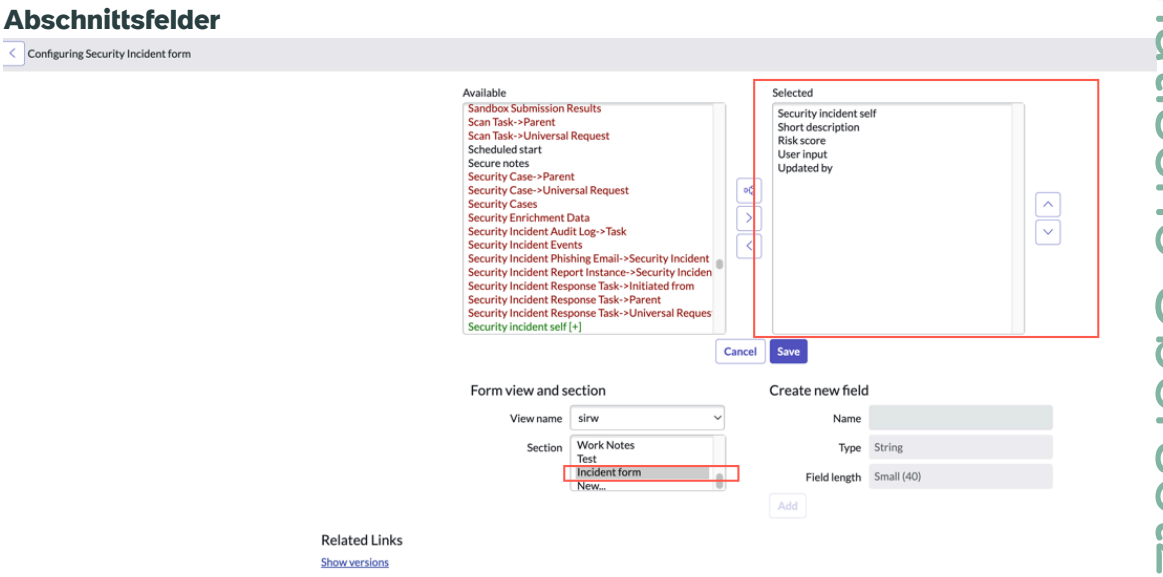
   Beispiel: Incident-Formular.

8. Der neue Abschnitt wird erstellt und dem **Abschnitt**hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

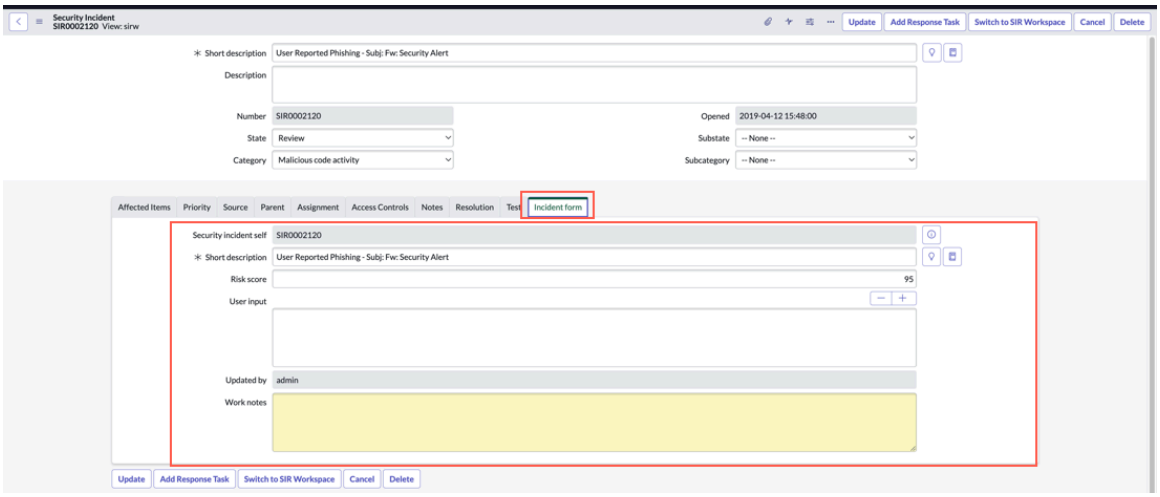


9. Wählen Sie Ihren neuen Abschnitt aus, fügen Sie dem Slushbucket die erforderlichen Abschnittsfelder hinzu, und klicken Sie auf **Speichern**.



10. Der neu hinzugefügte Abschnitt wird zusammen mit dem vorhandenen Abschnittslayout im Formular „Security Incident“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Klicken Sie nun **auf Zu SIR-Arbeitsbereich wechseln,** um zum Formular „Security Incident“ und zum anwenderdefinierten Abschnitt auf der Registerkarte **Details** des Arbeitsbereichs zu springen.

SIR Workspace Orchestration

Arbeitsbereich für Security Incident Response Orchestration-Aktivitäten helfen Sicherheitsanalysten, den Untersuchungs-Canvas anzuzeigen und verschiedene anwendbare Aktionen auszuführen.

SIR Workspace Untersuchungs-Canvas

Arbeitsbereich für Security Incident Response ermöglicht es den Sicherheitsanalysten, die wichtigsten Informationen anzuzeigen, die dem Security Incident während des Incident-Korrekturprozesses zugeordnet sind. Die Schlüsselinformationen enthalten auch die zugehörigen Listen wie „Erkennbare Elemente“, „Ergebnisse der Bedrohungssuche“, „Sichtungssuche“, „Anreicherung erkennbarer Elemente“ usw.

In der klassischen Anwenderoberfläche sind die meisten Orchestration-Aktionen, die den vordefinierten Integrationen zugeordnet sind, in den zugehörigen Listen verfügbar. Beispielsweise sind „Bedrohungssuche ausführen“, „Anreicherung erkennbarer Elemente ausführen“ usw. in der zugehörigen Liste „Zugeordnete erkennbare Elemente“ vorhanden. Ebenso sind „Hostdetails abrufen“, „Netzwerkstatistiken abrufen“ usw. für die zugehörige Liste „Konfigurationselemente“ verfügbar.

Wenn ein Sicherheitsanalyst diese Aktionen ausführt, werden die Ergebnisse in einer anderen zugehörigen Liste eingetragen. Wenn ein Benutzer beispielsweise die Bedrohungssuche ausführen ausführt, sind die Ergebnisse in der Tabelle „Ergebnisse der Bedrohungssuche“ verfügbar. Manchmal sind Ergebnisse in mehreren verschiedenen Tabellen verfügbar. Während dieses Prozesses machen die Sicherheitsanalysten eine unzusammenhängende und unorganisierte Anwender-Experience, wenn es darum geht, die Informationen von mehreren Stellen miteinander in Beziehung zu setzen.

In der überarbeiteten Version von SIR Workspacebietet die **Untersuchungs-** Canvas (Registerkarte) alle erforderlichen Informationen logisch gruppiert an einem Ort, damit der Analyst die Untersuchung durchführen kann.

Untersuchungs-Canvas erkunden

Das primäre Ziel des Untersuchungs-Canvas besteht darin, die erforderlichen Daten zu Security Incidents an einem zentralen Ort darzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Innerhalb von SIR Workspacegeht es bei der Untersuchung von Security Incidents hauptsächlich um einige wenige wichtige Einstiegspunkte.

Im Folgenden sind einige wichtige Einstiegspunkte aufgeführt, die für Sicherheitsanalysten im Basissystem bereitgestellt werden:

- Zugehörige erkennbare Elemente
- Konfigurationselemente
- Betroffene Anwender
- Zugeordnete Phishing-E-Mails
- E-Mail-Suche

Sie können die oben genannten Einstiegspunkte auch konfigurieren, indem Sie die Einstiegspunkte je nach Bedarf hinzufügen, ändern oder entfernen. Weitere Informationen finden Sie unter Konfigurieren Sie die SI-Entwurfszeituntersuchung.

Auf der Registerkarte **Ermittlung** fungiert die Einstiegspunkttabelle als übergeordnete Tabelle. Alle Tabellen, die die Ergebnisse einer für die übergeordnete Tabelle ausgeführten Orchestration-Aktion enthalten, werden als untergeordnete Tabellen innerhalb des Einstiegspunkts dargestellt.

Für den Einstiegspunkt **„Zugeordnete erkennbare Elemente“** ist beispielsweise die Tabelle **„Erkennbare Elemente zuordnen“** die übergeordnete Tabelle, und andere Tabellen wie Ergebnisse der Bedrohungssuche, Ergebnisse der Sandbox-Übermittlung usw. sind die untergeordneten Tabellen.

Der -Sicherheitsanalyst kann alle Orchestration-Aktionen in der Tabelle „Zugeordnete erkennbare Elemente“ ausführen und alle zugehörigen Informationen auf derselben Seite anzeigen, ohne an mehreren Stellen navigieren zu müssen.

Hinweis:
Wenn ein Anwender auf der Seite **„Übersicht“** auf die Interaktionsdiagramme klickt, z. B. auf schädliche erkennbare Elemente, wird er zur gefilterten Ansicht der schädlichen erkennbaren Elemente im Untersuchungs-Canvas navigiert. Alternativ kann der Benutzer die Untersuchung direkt starten, indem er zum Untersuchungs-Canvas navigiert, der alle Daten enthält.

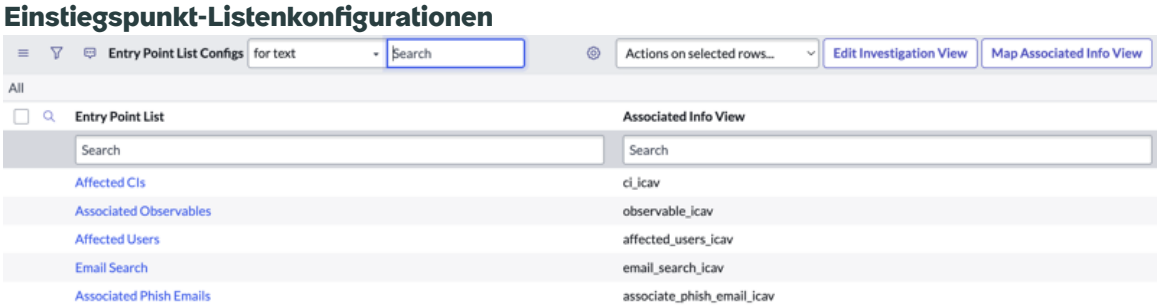
Die Liste der untergeordneten Tabellen unter einem Einstiegspunkt ist ebenfalls konfigurierbar. Weitere Informationen finden Sie unter Konfigurieren Sie die SI-Entwurfszeituntersuchung.

Im Folgenden finden Sie ein detailliertes Beispiel für einen Einstiegspunkt (zugeordnetes erkennbares Element), der im Basissystem konfiguriert und bereitgestellt wird:

1. Wählen Sie den Einstiegspunkt **„Zugeordnete erkennbare Elemente“** in der Dropdown-Liste aus.

   Hier ist die übergeordnete Tabelle auch **Zugeordnetes erkennbares Element**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Wählen Sie ein oder mehrere erkennbare Elemente aus der übergeordneten Tabelle aus.
3. Führen Sie die gewünschte Fähigkeit aus.

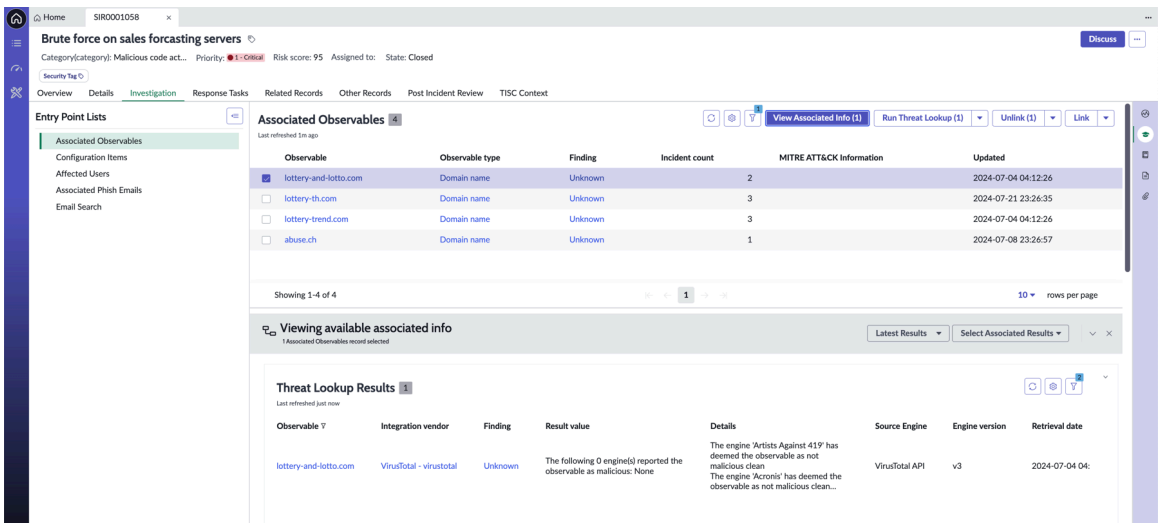
   Wählen Sie beispielsweise **Bedrohungssuche ausführen** aus, um die Ergebnisse der Bedrohungssuche für ein ausgewähltes erkennbares Element abzurufen.

   Hinweis:
   Wenn eine entsprechende Aktion für ein erkennbares Element ausgeführt wird, wird der Prozess im Back-End ausgeführt, und die Ergebnisse werden unter der Liste „Erkennbare Elemente“ angezeigt.

4. Klicken Sie auf **Zugehörige Informationen anzeigen,** um die Ergebnisse der erkennbaren Elemente anzuzeigen. Die Ergebnisse werden auf derselben Seite angezeigt.

   Hinweis:
   Sie können die Ergebnisse mithilfe von Filtern nach Ergebnissen anzeigen. Wählen Sie entweder **Alle Ergebnisse** oder **Neueste Ergebnisse**, je nachdem, welche Ansicht gewünscht ist. Standardmäßig werden die neuesten Ergebnisse angezeigt. Wenn mehrere Implementierungen (von Integrationen) vorhanden sind, werden die neuesten Ergebnisse pro Implementierung angezeigt.

   Darüber hinaus können Sie die Ergebnisse **nach zugehörigen zugehörigen Listen** filtern, bei denen es sich um die Ergebnisse der untergeordneten Tabelle handelt. Standardmäßig werden alle konfigurierten zugehörigen Listen für untergeordnete Tabellen angezeigt. Weitere Informationen finden Sie unter Konfigurieren Sie die SI-Entwurfszeituntersuchung. Sie können jedoch nur die untergeordneten Tabellen auswählen, die erforderlich sind.

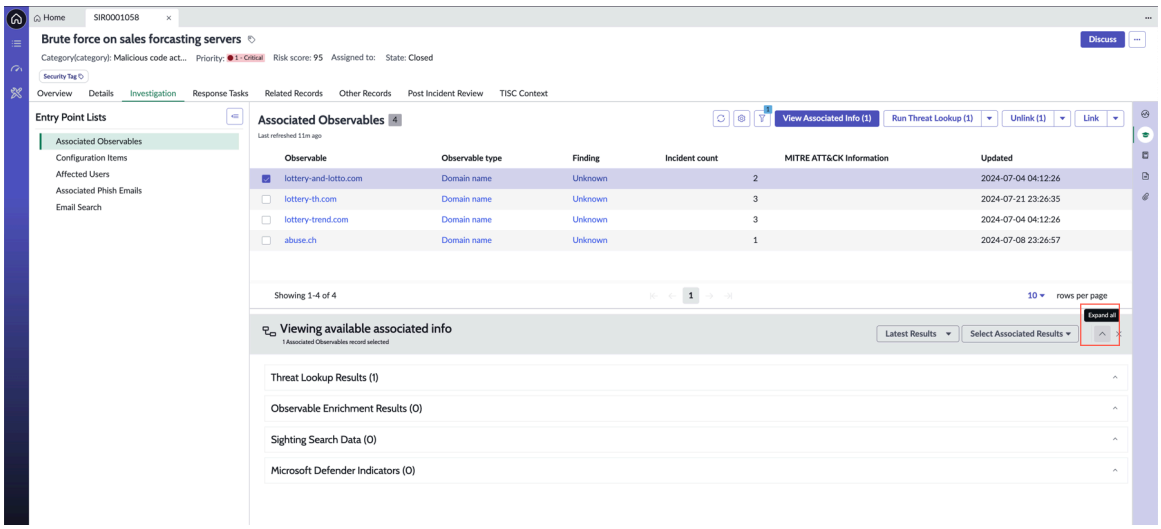


5. Wenn Sie auf **„Zugeordnete Informationen anzeigen“** klicken, können Sie alle zugehörigen untergeordneten Tabellendaten an einem Ort anzeigen. Sie können jedoch die Ansicht der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugehörigen Listen schließen, indem Sie auf die Schaltfläche **„Ansicht schließen“** klicken. Sobald Sie die Ansicht geschlossen haben, können Sie wie zuvor nur die übergeordnete Tabelle der erkennbaren Elemente anzeigen.

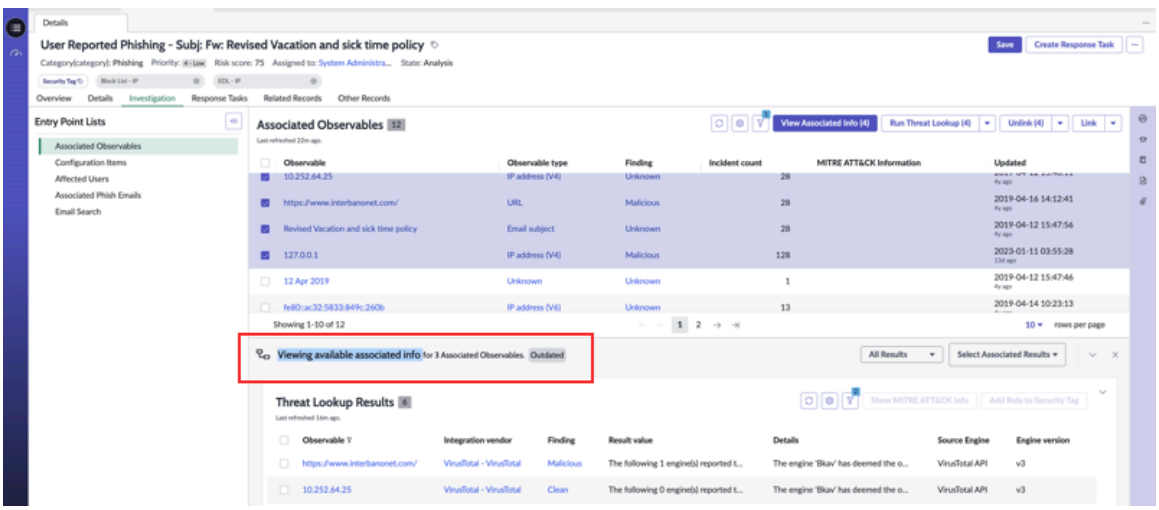
6. Klicken Sie auf das Symbol **Alle Aufwärtsrichtung erweitern** in der Tabelle Ergebnisse **der verfügbaren zugeordneten Informationen anzeigen,** um alle untergeordneten Tabellendaten der zugehörigen Listen zu erweitern.



7. Klicken Sie auf das Symbol **Alle Abwärtsrichtung reduzieren,** um alle Tabellendaten der untergeordneten zugehörigen Listen zu reduzieren.

Hinweis:

Das Banner über dem zugehörigen Infoabschnitt, der alle Daten der untergeordneten Tabelle enthält, zeigt an, wie viele Informationen zu erkennbaren Elementen dem Anwender angezeigt werden. Wenn Sie beispielsweise zunächst zwei erkennbare Elemente auswählen und **auf Zugehörige Informationen anzeigen**klicken, wird im Banner Folgendes angezeigt: **Verfügbare zugeordnete Informationen für 2 zugeordnete erkennbare Elemente werden angezeigt.**. Wenn Sie beispielsweise ein anderes erkennbares Element auswählen, wird im Banner angezeigt, dass die Informationen veraltet sind (Screenshot unten). Sie müssen erneut auf **„Zugeordnete Informationen anzeigen“** klicken, um die aktuellen Daten zu erhalten.



Wenn Sie zusätzlich zur obigen umfassenden Ansicht der zugehörigen Informationen zu erkennbaren Elementen weitere Informationen zu einem Datensatz in der übergeordneten Tabelle anzeigen möchten, klicken Sie auf das erkennbare Element. Das Datensatzformular der übergeordneten Tabelle wird auf einer anderen Registerkarte mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einer detaillierteren Ansicht von geöffnet ausgewählter Datensatz. Alle zugeordneten untergeordneten Tabellendaten dieses ausgewählten Datensatzes werden auch im Abschnitt **„Zugeordnete Informationen“** angezeigt.

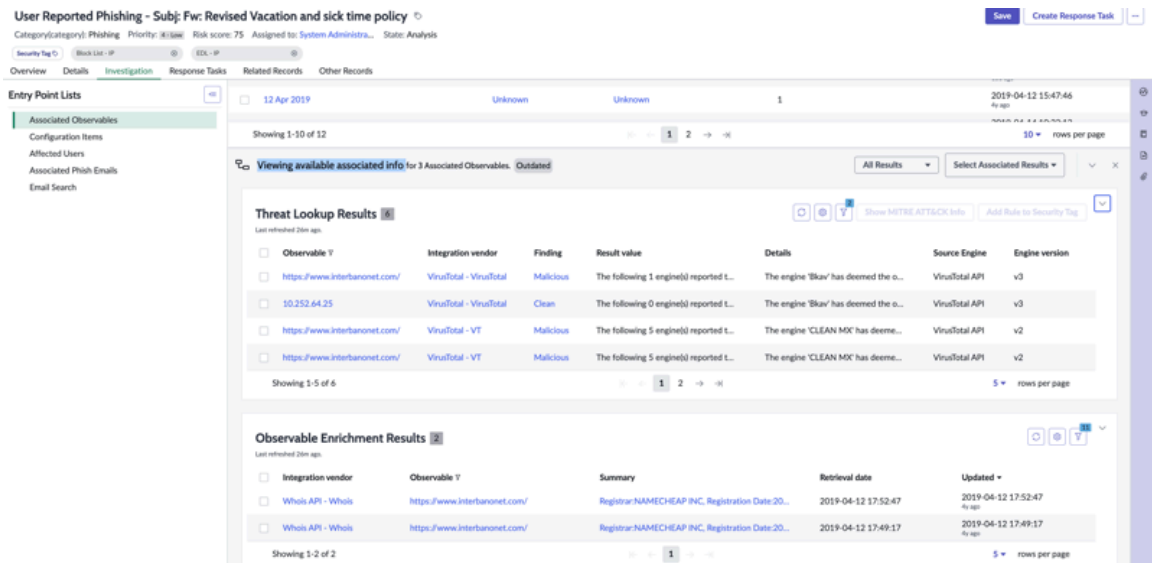
Im zugehörigen Infoabschnitt werden jedoch nur die neuesten Ergebnisse der untergeordneten Tabelle angezeigt, wie im Untersuchungs-Canvas im schreibgeschützten Modus zu sehen ist. In dieser Ansicht sind keine Aktionen möglich. Die Formularseite der untergeordneten Tabelle kann in einer neuen Registerkarte geöffnet werden, die die voll funktionsfähige Seite mit beliebigen Aktionen (falls vorhanden) bereitstellt.

Über die Dropdown-Liste können Sie zwischen den verschiedenen Tabellen wechseln. Sie können auch jedes Formular unter dem zugehörigen Infoabschnitt erweitern oder reduzieren.

Auf der Formularseite **für erkennbare Elemente** (übergeordnete Tabellendatensatz-Formularseite) können Sie je nach Verfügbarkeit bestimmte Aktionen ausführen. Wenn Sie eine Aktion ausführen, können Sie im zugehörigen Infobanner auf „Aktualisieren“ klicken, um die Daten zu aktualisieren.

8. Klicken Sie auf **Alle erweitern**, um alle untergeordneten Tabellen für zugehörige Listen zu erweitern. Standardmäßig werden alle untergeordneten Elemente erweitert.

Erweiterte Ansicht der erkennbaren Elemente



Zugehörige Informationen

Konfigurieren Sie die SI-Entwurfszeituntersuchung

Unified Experience Framework für Integrationen, die auf dem Fähigkeits-Framework basieren

In der klassischen Anwenderoberfläche wird die Experience bei der Durchführung von Orchestration-Aktivitäten wie dem Ausführen der Bedrohungssuche, der Sichtungssuche usw. getrennt. Jede Fähigkeit hat ihre eigene Experience bei der Ausführung. Der neue Arbeitsbereich bietet eine einheitliche Experience für alle Fähigkeiten.

Die einheitliche Experience gilt nur für die Integrationen und Orchestration-Aktivitäten, die unter das Fähigkeits-Framework fallen. Es kann spezifische Aktionen für die Integration geben, z. B. Indikatoren in Microsoft Defender erstellen. Diese Aktionen verfügen je nach Anwendungsfall über eine eigene Experience.

Das neue Framework besteht aus modalen Bildschirmen mit drei Schritten, wie unten erläutert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. **Implementierungen**: Der erste Schritt umfasst die Auswahl einer oder mehrerer Implementierungen, die für die ausgewählte Fähigkeit vorhanden sind.

   Wenn der Analyst beispielsweise auf **„Bedrohungssuche ausführen“**klickt, kann er eine oder mehrere Implementierungen auswählen, die für **die Fähigkeit „Bedrohungssuche ausführen“**vorhanden sind.

   Jede Implementierung enthält die Details der Integrationsquelle. Weitere Informationen finden Sie in der folgenden Tabelle. Zusätzliche Informationen werden auch für jede Implementierung angezeigt.

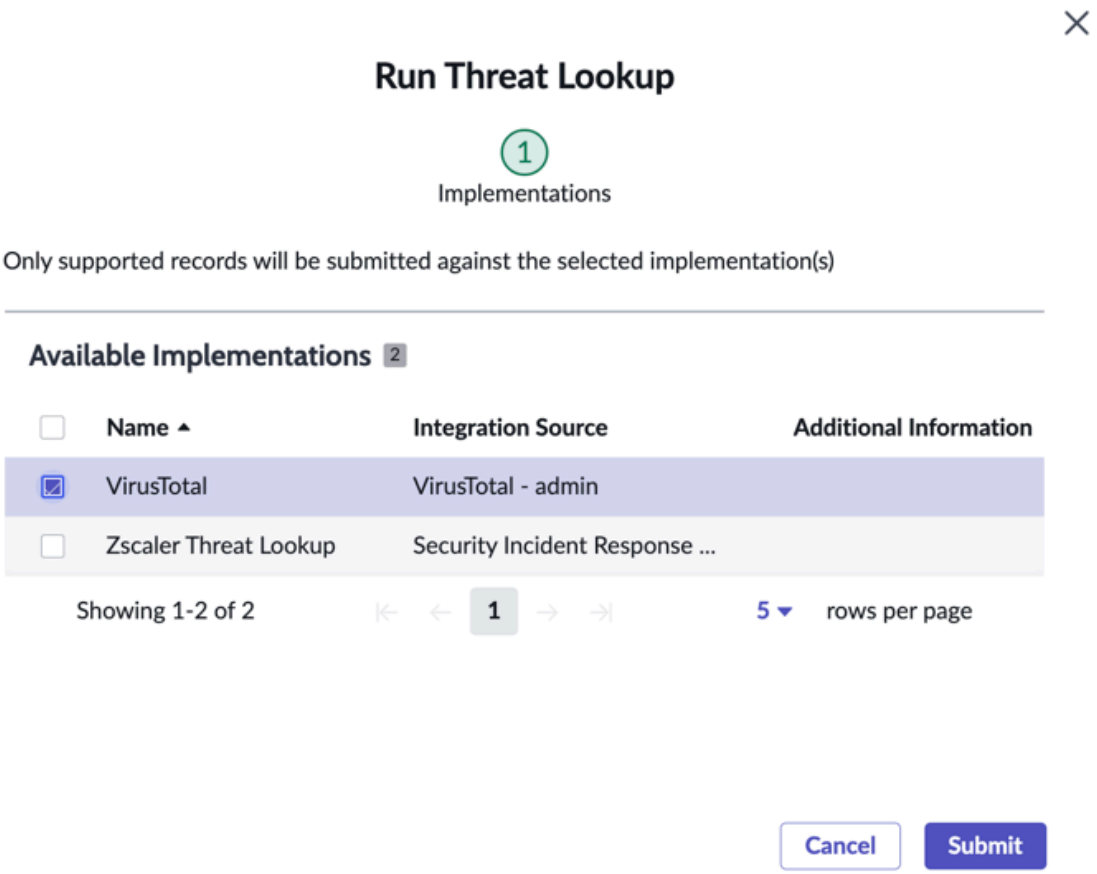
   Zusätzliche Informationen können beispielsweise Informationen zu Filtern, Typen der unterstützten erkennbaren Elemente usw. enthalten. Die Zusatzinformationen können nach Belieben konfiguriert werden. Weitere Informationen finden Sie unter Verfahren zur technischen Konfiguration des UX-Frameworks.

Unified Implementation Framework Modal

Implementierung	Beschreibung
Name	Name der -Implementierung
Integrationsquelle	Die Quelle der Implementierung, z. B. die verwendete Konfiguration.
Zusätzliche Informationen	Diese Spalte erfasst die statischen Informationen, die dem Sicherheitsanalysten mehr Kontext für die ausgewählten Implementierungen hinzufügen, um mit einer Aktion fortzufahren. Zum Beispiel Supportfähigkeit oder gefilterte Informationen. Wenn eine Implementierung nur einen bestimmten Typ von erkennbaren Elementen unterstützt, z. B. Domäne oder URL, können Sie diese zusätzlichen Informationen hier in dieser Spalte hinzufügen, um dem Benutzer den Kontext bereitzustellen. **Hinweis:** Das UI-Framework ermöglicht im Grunde die Auswahl jeder Art von Implementierung und jeder Art von erkennbaren Elementen. Während der Übermittlung übernehmen die im Lieferumfang enthaltenen vorhandenen Basissystemintegrationen die Filterung im Back-End und übermitteln nur den unterstützten Typ von erkennbaren Elementen. Der Rest der Datensätze, die nicht mit der Supportfähigkeit übereinstimmen, wird ignoriert. Daher wird eine UI-Informationsmeldung angezeigt, während Sie die Fähigkeit auswählen: **Nur unterstützte Datensätze werden für die ausgewählte(n) Implementierung(en) übermittelt.**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bildschirm 1: Implementierung(en)

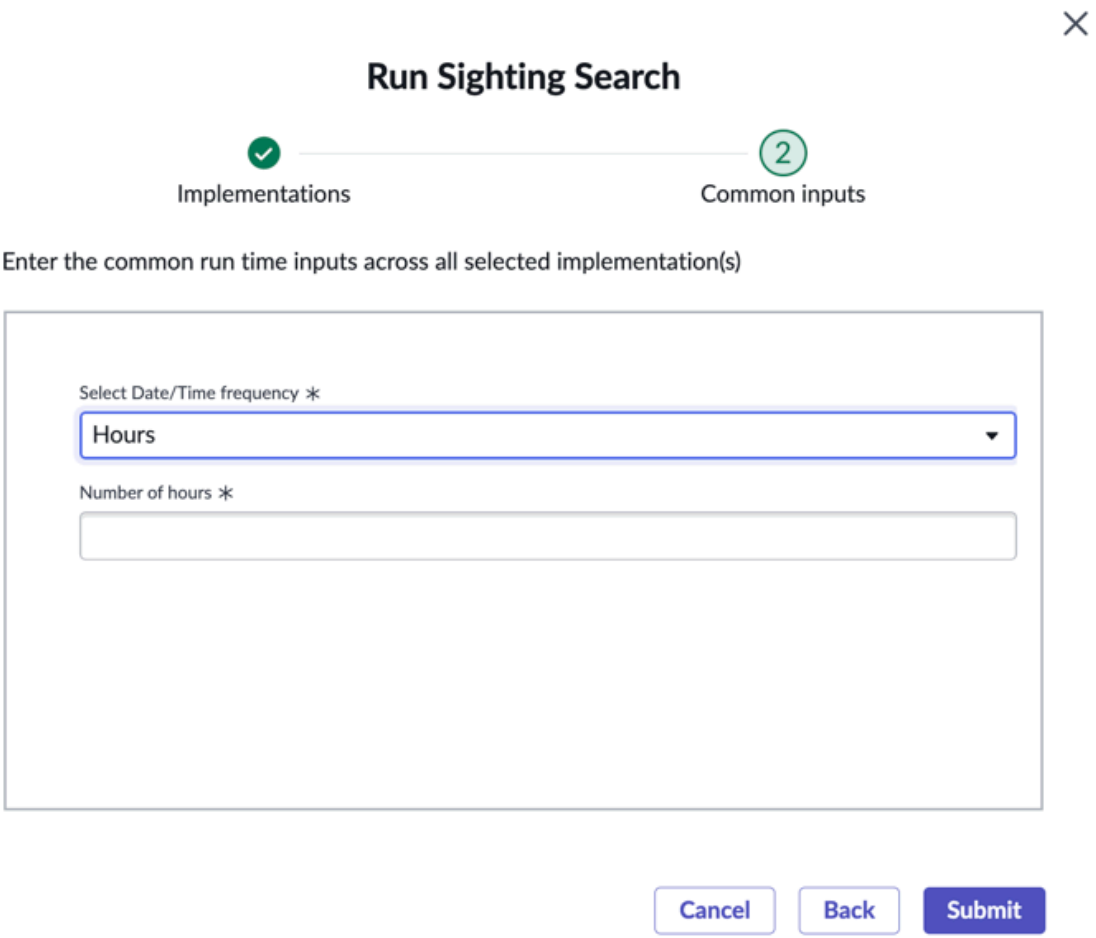


2. **Allgemeine Eingaben**: Fügen Sie allgemeine Eingaben für die ausgewählten Implementierungen oder für alle ausgewählten anwendbaren Implementierungen hinzu. Dies ist der Bildschirm 2 Ihrer Implementierung. Beispielsweise verfügt ab jetzt nur die **Sichtungssuche** über den allgemeinen Eingabebildschirm. Diese Implementierung ist eine Kombination aus Bildschirm 1 (Implementierungen) und Bildschirm 2 (allgemeine Eingaben).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bildschirm 1 + Bildschirm 2



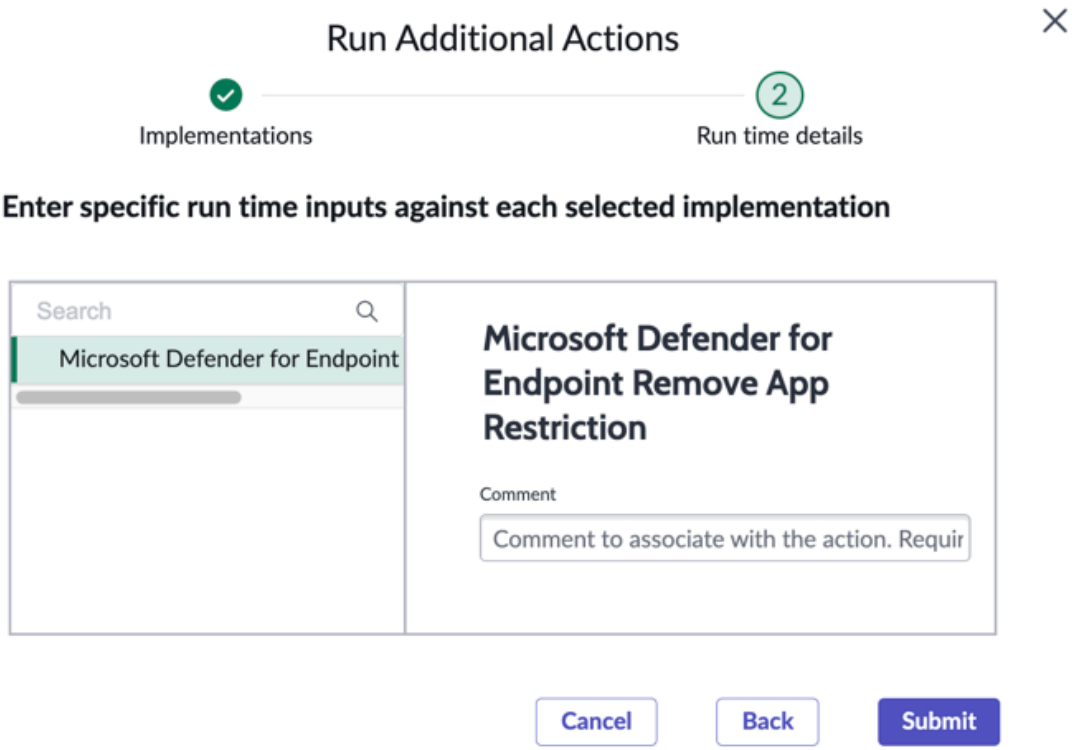
3. **Laufzeitdetails**: Fügen Sie spezifische Laufzeiteingaben für die ausgewählten Implementierungen hinzu, die sich von den anderen Implementierungen unterscheiden. Dies ist der Bildschirm 3 Ihrer Implementierung. Diese Implementierung ist eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kombination aus Bildschirm 1 (Implementierungen) und Bildschirm 3 (spezifische Laufzeiteingaben).

Bestimmte Eingaben



Hinweis:
Nicht immer sind alle drei Schritte erforderlich. Abhängig von der Fähigkeit und der Art der erforderlichen Eingaben sind der Schritt „Laufzeitdetails“ und der Schritt „Allgemeine Eingaben“ sichtbar.

Einheitliche Experience-Fähigkeiten und modale Bildschirme

In der folgenden Tabelle werden die Funktionen und entsprechenden Bildschirme beschrieben.

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
Bedrohungssuche durchführen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder Implementierungsspezifischen Eingaben, die für die Ausführung der Bedrohungssuche gelten. Daher wird dem Sicherheitsanalysten nur	• Viren insgesamt • Hybrid Analysis • Security Incident Response Integration with Zscaler • Phistanker • Metadefender • Bedrohungsmenge

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
	Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• Wurde ich verpfändet? • CrowdStrike Falcon Intelligence
Anreicherung erkennbarer Elemente durchführen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar Es gibt keine allgemeinen oder Implementierungsspezifischen Eingaben, die für die Ausführung der Anreicherung erkennbarer Elemente gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• MISP • Microsoft Defender-Endpunkt • Shodan • RiskIQ • WHOIS • WHOIS umkehren
Sichtungssuche/Web-Sichtungssuche/E-Mail-Sichtungssuche ausführen	Bildschirm 1 – **Implementierungen auswählen** und Bildschirm 2 – **Allgemeine Eingaben** sind anwendbar. Die Sichtungssuche verwendet Datum und Uhrzeit (Häufigkeit) als allgemeine Eingaben für mehrere Implementierungen von Splunk und anderen Integrationen. Dieser Bildschirm wird dem Sicherheitsanalysten angezeigt, um Datums- und Uhrzeithäufigkeiten zu erfassen. Bei Integrationen, die diese Eingaben nicht erfordern, z. B. FireEye	• Splunk-Incident-Ergänzung • Carbon Black • Elasticsearch • FireEye HX • McaFee ESM • MSFT Defender für Endpunkt • Splunk-Sichtung • Qradar-Sichtungssuche • MISP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
	HX, werden sie ignoriert. Nachdem er eine oder mehrere Implementierungen ausgewählt und allgemeine Eingaben gemacht hat, kann der Sicherheitsanalyst die Aktion übermitteln.	
An die Sandbox übermitteln	Bildschirm 1 – Implementierungen auswählen und Bildschirm 3 – Implementierungsspezifische Eingaben sind anwendbar. „An die Sandbox übermitteln“ benötigt unterschiedliche Eingaben für unterschiedliche Implementierungen. Für diese Fähigkeit sind derzeit keine allgemeinen Eingaben vorhanden. Wenn der Analyst beispielsweise Crowdstrike Falcon X Quick Scan, Crowdstrike Falcon X Windows 64, Crowdstrike Falcon X Linux und Zscaler auswählt, variieren die Eingaben. Crowdstrike Falcon X Quick Scan und Zscaler benötigen keine weiteren Laufzeiteingaben. Crowdstrike Falcon X Windows 64 akzeptiert optionale Laufzeiteingaben, die sich von Crowdstrike Falcon X Linux unterscheiden. Daher können diese in Bildschirm 3 gegebenenfalls speziell für einzelne ausgewählte Implementierungen bereitgestellt werden.	• CrowdStrike Falcon X Sandbox-Integration • Security Incident Response Integration with Zscaler
In Beobachtungsliste veröffentlichen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder Implementierungsspezifischen	Crowdstrike Falcon-Host

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
	Eingaben, die für **In Beobachtungsliste veröffentlichen**gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	
Anforderung zulassen/blockieren	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen Eingaben oder Implementierungsspezifischen Eingaben, die für **die Zulassungs-/ Blockierungsanforderung**gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• Palo Alto Network NGFW • Prüfpunkt NGFW • Security Incident Response Integration with Zscaler
Hostdetails abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder Implementierungsspezifischen Eingaben für „Hostdetails abrufen“. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann	• FireEye HX • Microsoft Defender für Endpunkt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
	der Sicherheitsanalyst die Aktion übermitteln.	
Datei abrufen	Bildschirm 1 – Implementierungen auswählen und Bildschirm 2 – Allgemeine Eingaben sind anwendbar. „Datei abrufen“ verwendet Dateiname und Pfad als allgemeine Eingaben. Nachdem er eine oder mehrere Implementierungen ausgewählt und allgemeine Eingaben gemacht hat, kann der Sicherheitsanalyst die Aktion übermitteln.	FireEye HX
Netzwerkstatistiken abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder Implementierungsspezifischen Eingaben für „Netzwerkstatistiken abrufen“. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• FireEye HX • NetStat
Laufende Prozesse abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder Implementierungsspezifischen Eingaben, die für „Laufende Prozesse abrufen“ gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl	• FireEye HX • Carbon Black • Systembefehl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
	der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	
Laufende Services abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder implementieren spezifischen Eingaben, die für „Laufende Services abrufen“ gelten. Daher wird dem Analysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Analyst die Aktion übermitteln.	FireEye HX
Host isolieren/Isolierung des Hosts aufheben	Bildschirm 1 – Implementierungen auswählen und Bildschirm 3 – Implementierungsspezifische Eingaben sind anwendbar. „Host isolieren“/„Isolierung des Hosts aufheben“ akzeptiert unterschiedliche Eingaben für verschiedene Implementierungen. Für diese Fähigkeit sind derzeit keine allgemeinen Eingaben vorhanden. Wenn der Analyst beispielsweise FireEye HX und Microsoft Defender für Endpunkt auswählt, variieren die Eingaben. FireEye HX benötigt keine Laufzeiteingaben. Microsoft Defender hingegen akzeptiert Eingaben wie Isolationstyp und Kommentare. Daher können diese in Bildschirm 3 gegebenenfalls speziell	• FireEye HX • Microsoft Defender-Endpunkt • Carbon Black

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
	für einzelne ausgewählte Implementierungen bereitgestellt werden.	
Zusätzliche Aktionen ausführen	Bildschirm 1 – Implementierungen auswählen und Bildschirm 3 – Implementierungsspezifische Eingaben sind anwendbar. Der Host „Zusätzliche Aktionen ausführen“ akzeptiert unterschiedliche Eingaben für unterschiedliche Implementierungen. Für diese Fähigkeit sind derzeit keine allgemeinen Eingaben vorhanden. Wenn der Analyst beispielsweise „FireEye HX Standard Untersuchungsdetailskript“, „FireEye HX Triage Acquisition“ und „Crowdstrike Falcon Insight reg. unload“ auswählt, variieren die Eingaben. Das FireEye HX-Standardskript für Untersuchungsdetails und die FireEye HX-Selektierungsakquisition verwenden Kommentare als Eingabe, die für beide unterschiedlich sein können. Das reguläre Entladen von Crowdstrike Falcon Insight verwendet Unterschlüssel als Eingabe. Daher können diese in Bildschirm 3 gegebenenfalls speziell für einzelne ausgewählte Implementierungen bereitgestellt werden.	• FireEye HX • Microsoft Defender für Endpunkt • Crowdstrike Falcon Insight

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen unterstützt
	Hinweis: Unterstützt derzeit nur die Einzelauswahl von Implementierungen. In zukünftigen Versionen wird die Mehrfachauswahl für Implementierungen unterstützt.	

Beispiel für einheitliche Experience

In diesem Beispiel werden die Fähigkeiten des Unified Experience Framework demonstriert.

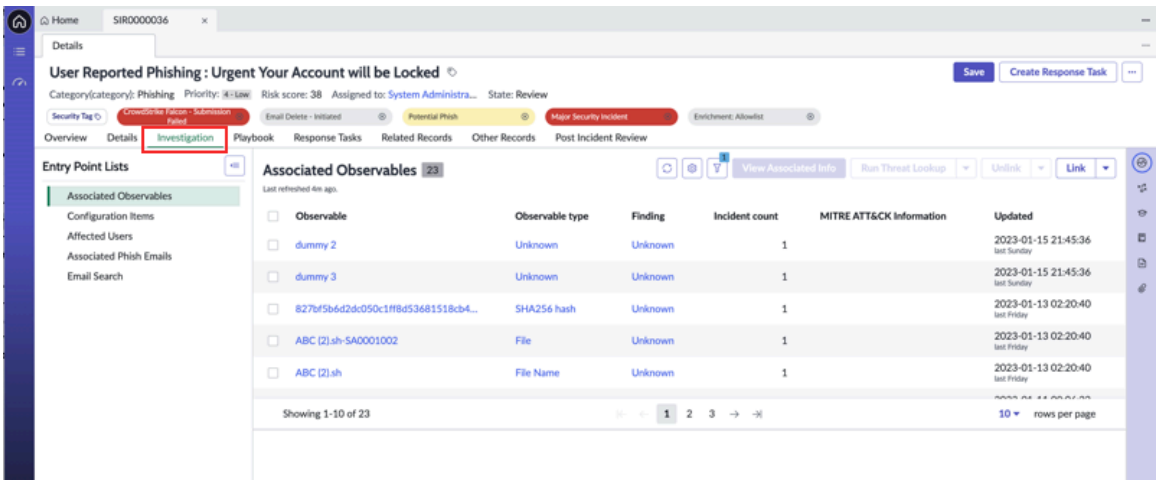
Beispiel 1: Implementierungen auswählen: Bedrohungssuche

Das folgende Beispiel veranschaulicht die Implementierung(en).

Beispiel 1: Nur Bildschirm 1: Bedrohungssuche

Auf der Registerkarte **Ermittlung** unter SIR Workspacekönnen Sie die Aktion **„Bedrohungssuche ausführen“** für Integrationsfunktionen ausführen.

1. Navigieren Sie auf der Registerkarte **Ermittlung** zum Abschnitt **Einstiegspunktlisten**, der auf der linken Seite angezeigt wird.
2. Wählen Sie einen beliebigen Einstiegspunkt aus, und führen Sie die Aktion für die Integrationsfähigkeit aus.



Hinweis:
Sie können auch im Arbeitsbereich zur **Registerkarte Zugehörige Datensätze** navigieren, um die Aktion „Integrationsfunktionen“ auszuführen.

Die Bedrohungssuche ist eines der Beispiele, in dem die Durchführung der Integrationen ausführlich beschrieben wird.

Wählen Sie Implementierungen aus

Wählen Sie je nach Bedarf mindestens eine Implementierung aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

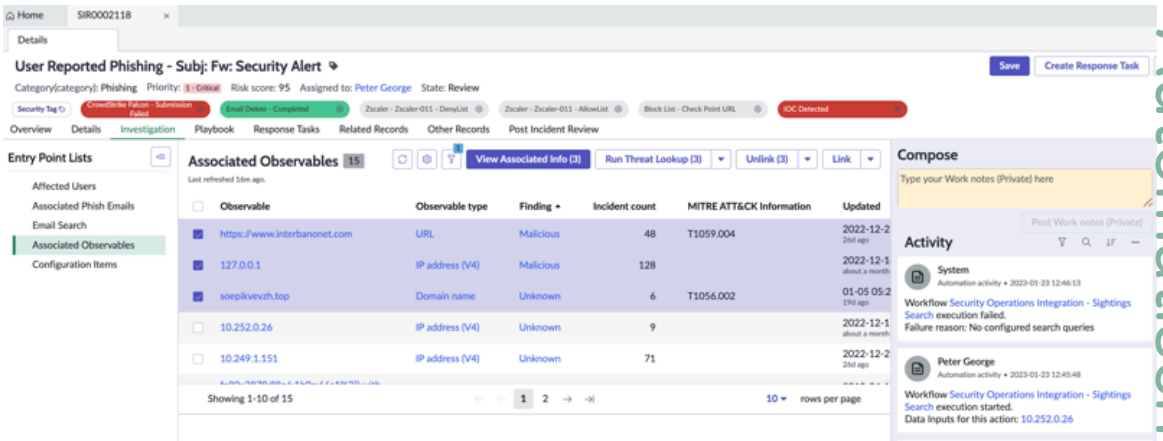
Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nachdem Sie sie ausgewählt haben, werden nur die unterstützten Datensätze für die ausgewählten Implementierungen übermittelt.

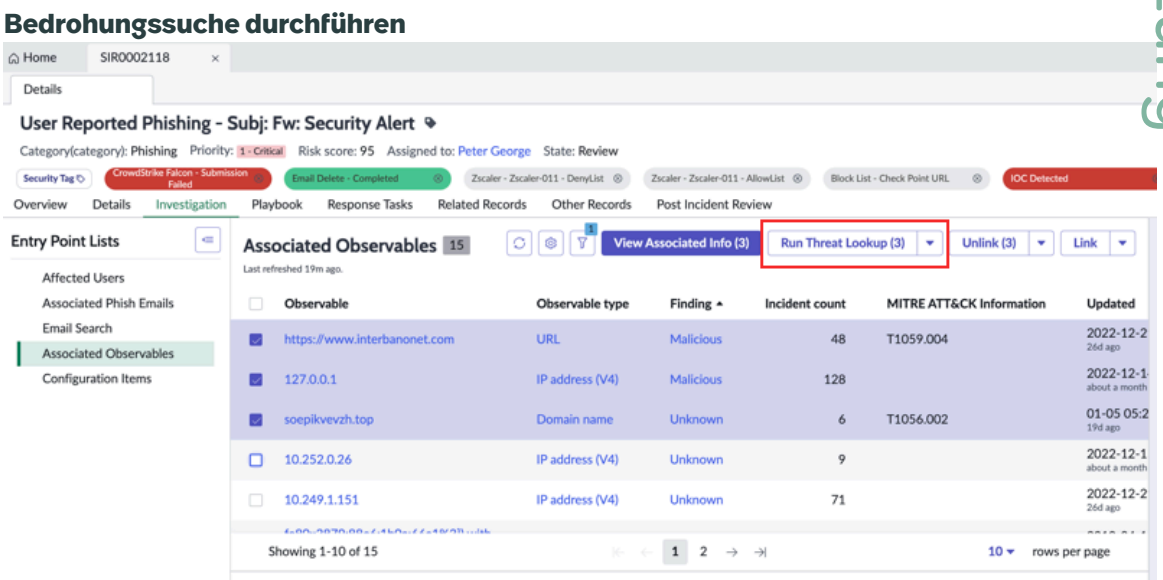
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Wechseln Sie zur Registerkarte **Ermittlung** des Arbeitsbereichs.
   Die Registerkarte Ermittlung mit den Einstiegspunktlisten wird angezeigt.



4. Wählen Sie das zugeordnete erkennbare Element aus den Einstiegspunktlisten aus.
   Wählen Sie beispielsweise aus **Zugehörige erkennbare Elemente** Zugehörige Liste. Die entsprechenden Datensätze für erkennbare Elemente werden angezeigt.

Hinweis:
Sie können eine Implementierung auswählen, um eine Suche für die ausgewählten erkennbaren Elemente durchzuführen, oder Sie können die Suche durchführen, indem Sie alle Implementierungen auswählen.



Automatische Übersetzung

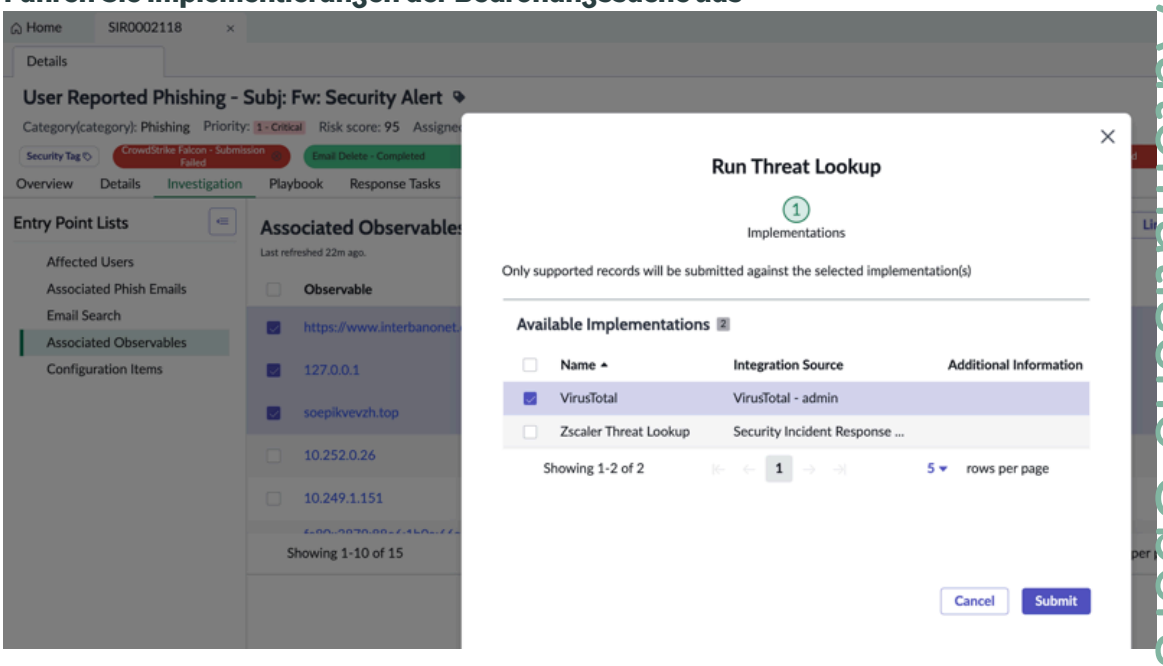
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Aktivieren Sie das Kontrollkästchen für ein erkennbares Element, für das Sie die Bedrohungssuche durchführen möchten.
6. Navigieren Sie zu der Dropdown-Liste Aktionen für zugehörige Listen, die oben auf der Seite mit zugehörigen Listen angezeigt wird.
7. Wählen Sie **„Bedrohungssuche ausführen“**, um die Aktion für Integrationsfähigkeiten im Zusammenhang mit Bedrohungsinformationen auszuführen.

   Hinweis:
   Die Fähigkeit „Bedrohungssuchen ausführen“ führt Threat Intelligence-Suchen durch, um zu bestimmen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsrisiken zugeordnet sind.

   Der modale Bildschirm **„Implementierungen der Bedrohungssuche ausführen“** wird angezeigt.

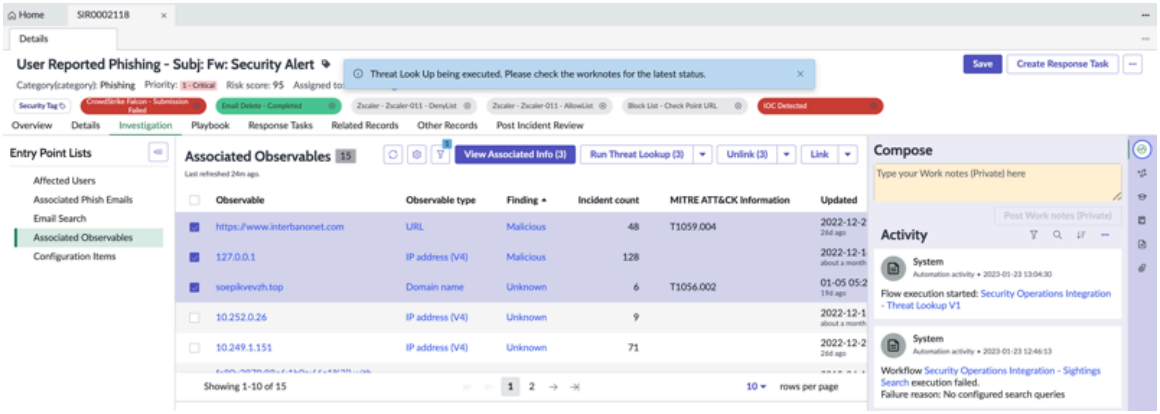
Führen Sie Implementierungen der Bedrohungssuche aus



8. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.
9. Klicken Sie auf **Absenden**.
   Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Suche ausgeführt wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im zugehörigen Listenabschnitt **„Ergebnisse der Bedrohungssuche“** angezeigt. Außerdem wird die entsprechende Implementierungsaktivität im Abschnitt **„Aktivität“** angezeigt. Es werden zwei Aktivitäten angezeigt: eine, wenn die Implementierungsausführung gestartet wird, und eine zweite, wenn sie abgeschlossen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die zugehörigen Listen **für Bedrohungsinformationen** wie die zugehörigen Listen für erkennbare Elemente werden im Abschnitt „ **Ergebnisse der Bedrohungssuche“** angezeigt, und die zugehörigen Listen **der Sichtungssuche** werden im Abschnitt „ **Ergebnisse der Sichtungssuche“** unter „Zugehörige Datensätze“ angezeigt.

Beispiel 2: Allgemeine Eingaben: Sichtungssuche

Das folgende Beispiel zeigt die Fähigkeitsaktion für allgemeine Eingaben.

Sie können die Aktion **„Sichtungssuche ausführen“** für die zugehörigen Integrationsfähigkeiten auf der Registerkarte **Ermittlung** in SIR Workspaceausführen.

1. Navigieren Sie auf der Registerkarte **Ermittlung** zum Abschnitt **Einstiegspunktlisten**, der auf der linken Seite angezeigt wird.
2. Wählen Sie den entsprechenden Einstiegspunkt aus, und führen Sie die Aktion für die Integrationsfähigkeit aus.

Hinweis:
Sie können auch im Arbeitsbereich zur **Registerkarte Zugehörige Datensätze** navigieren, um die Aktion „Integrationsfunktionen“ auszuführen.

Fügen Sie einer Implementierung allgemeine Eingaben hinzu

Fügen Sie allgemeine Laufzeiteingaben hinzu, die für alle ausgewählten Implementierungen gelten.

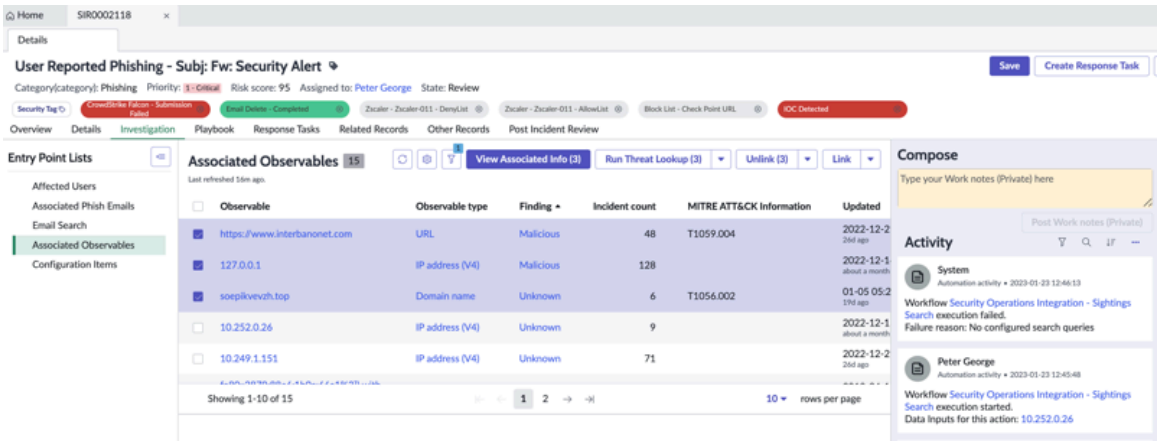
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nachdem Sie sie ausgewählt haben, werden nur die unterstützten Datensätze für die ausgewählten Implementierungen übermittelt.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Wechseln Sie zur Registerkarte **Ermittlung** des Arbeitsbereichs.
   Die Registerkarte Ermittlung mit den Einstiegspunktlisten wird angezeigt.

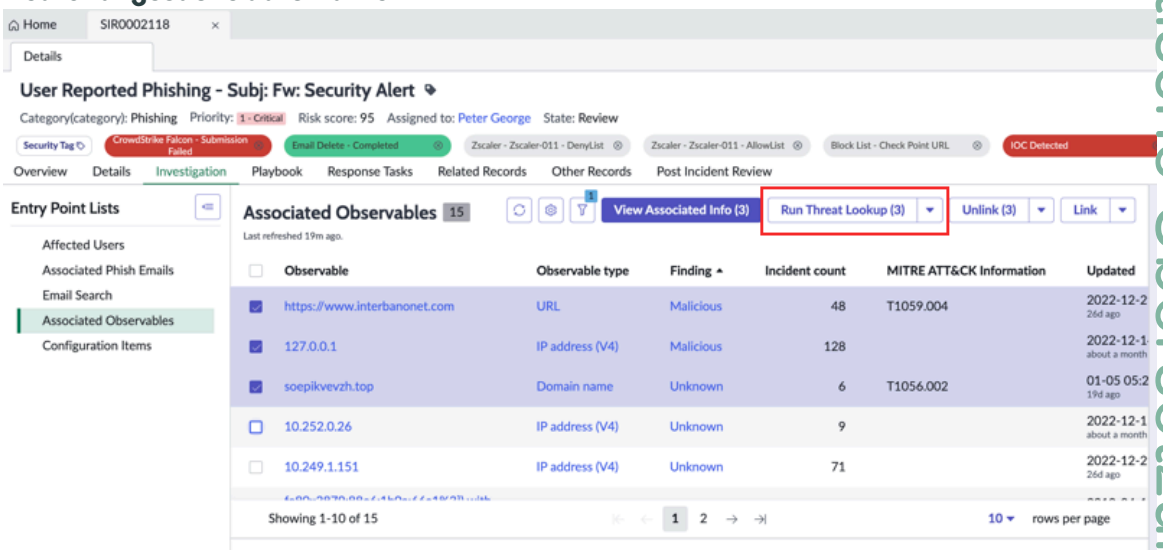
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie das zugeordnete erkennbare Element aus den Einstiegspunktlisten aus.
   Wählen Sie beispielsweise aus **Zugehörige erkennbare Elemente** Zugehörige Liste. Die entsprechenden Datensätze für erkennbare Elemente werden angezeigt.

> **Hinweis:**
> Sie können eine Implementierung auswählen, um eine Sichtungssuche für die ausgewählten erkennbaren Elemente durchzuführen, oder mehrere Implementierungen auswählen.

Bedrohungssuche durchführen

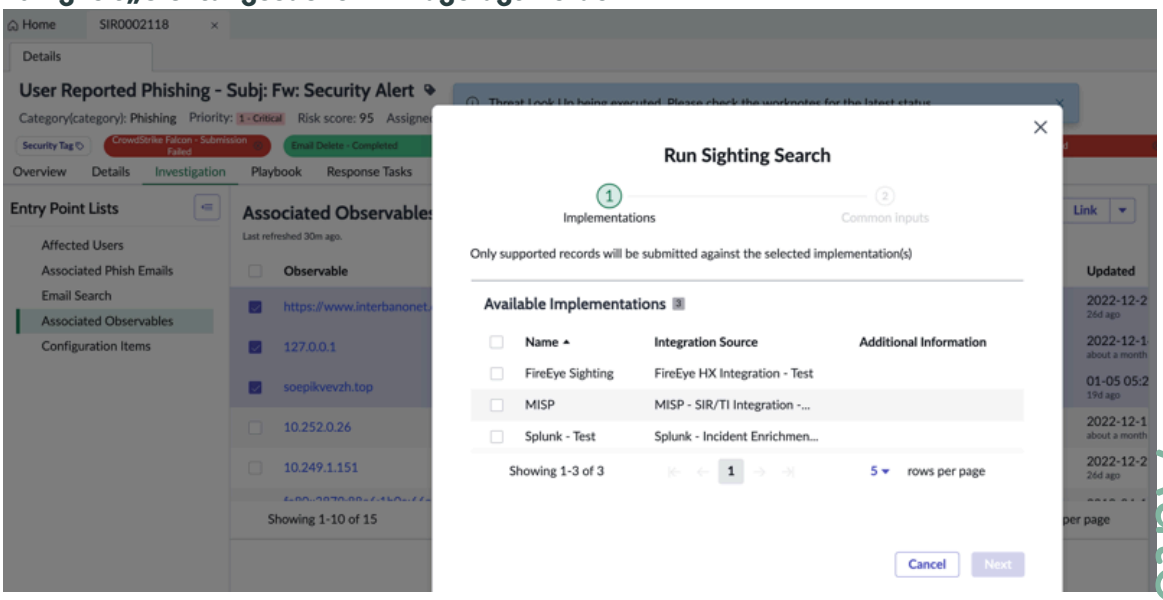


5. Aktivieren Sie das Kontrollkästchen für ein erkennbares Element, für das Sie die Bedrohungssuche durchführen möchten.
6. Wählen Sie **Sichtungssuche ausführen aus,** um eine E-Mail-Suche durchzuführen.
   Das modale Dialogfeld „Implementierungen der Sichtungssuche ausführen“ wird angezeigt.

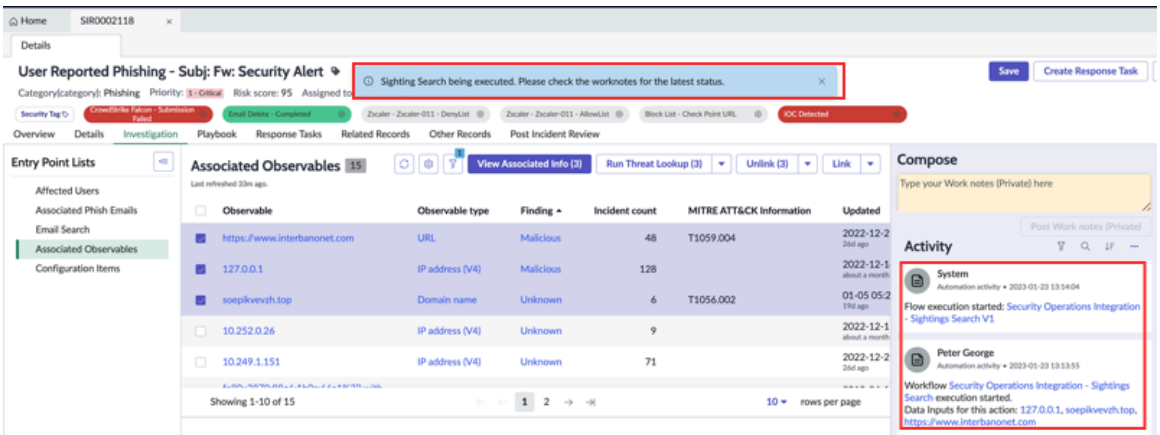
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Beispiel, das zeigt, wie allgemeine Laufzeiteingaben durch Auswahl der Fähigkeit „Sichtungssuche“ hinzugefügt werden



7. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.
8. Klicken Sie auf **Next (Weiter)**.
   Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Sichtungssuche angefordert wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im zugehörigen Listenabschnitt **„Sichtungssuche“** angezeigt. Außerdem wird die entsprechende Implementierungsaktivität im Abschnitt „Aktivität“ angezeigt. Es werden zwei Aktivitäten angezeigt: eine, wenn die Implementierungsausführung gestartet wird, und eine zweite, wenn sie abgeschlossen wird.
9. Wählen Sie den allgemeinen Laufzeit-Eingabewert aus.
10. Klicken Sie auf **Absenden**.



Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Sichtungssuche angefordert wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im zugehörigen Listenabschnitt **„Sichtungssuchergebnisse“** angezeigt. Außerdem wird im Abschnitt **„Aktivität“** der jeweilige Verarbeitungsstatus der Implementierungsaktivität angezeigt.

Beispiel 3: Hinzufügen spezifischer Laufzeitdetaileingaben zu einer Implementierung: Zusätzliche Aktionen ausführen

Fügen Sie einer Implementierung spezifische Laufzeitdetaileingaben hinzu, und führen Sie zusätzliche Aktionen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können auf der Registerkarte **Ermittlung** von SIR Workspacedie Aktion **„Zusätzliche Aktionen ausführen“** für Integrationsfähigkeiten ausführen.

1. Navigieren Sie auf der Registerkarte **Ermittlung** zum Abschnitt **Einstiegspunktlisten**, der auf der linken Seite angezeigt wird.
2. Wählen Sie den entsprechenden Einstiegspunkt aus, und führen Sie die Aktion für die Integrationsfähigkeit aus.

Hinweis:
Sie können auch im Arbeitsbereich zur **Registerkarte Zugehörige Datensätze** navigieren, um die Aktion „Integrationsfunktionen“ auszuführen.

Fügen Sie einer Implementierung bestimmte Eingaben hinzu

Fügen Sie nach Bedarf spezifische Laufzeiteingaben für jede der ausgewählten Implementierungen hinzu.

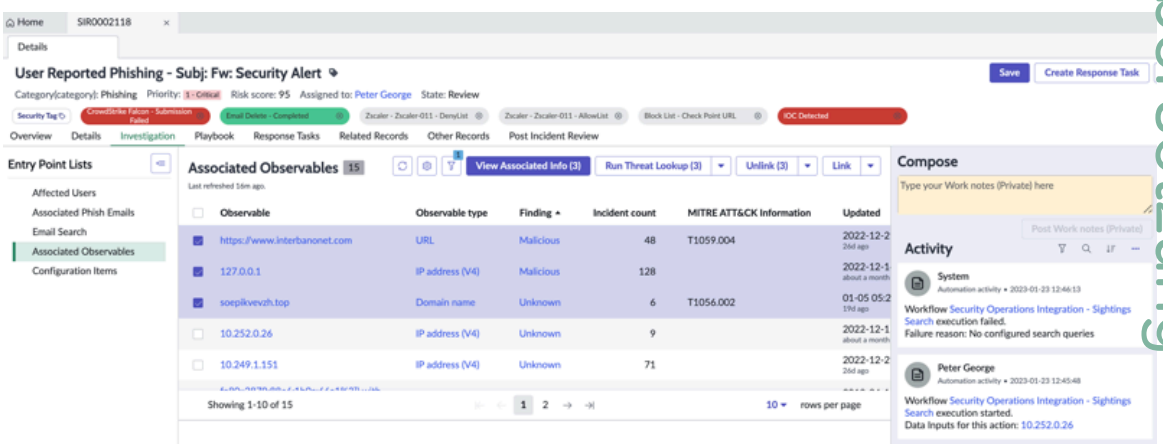
Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nachdem Sie sie ausgewählt haben, werden nur die unterstützten Datensätze für die ausgewählten Implementierungen übermittelt.

Prozedur

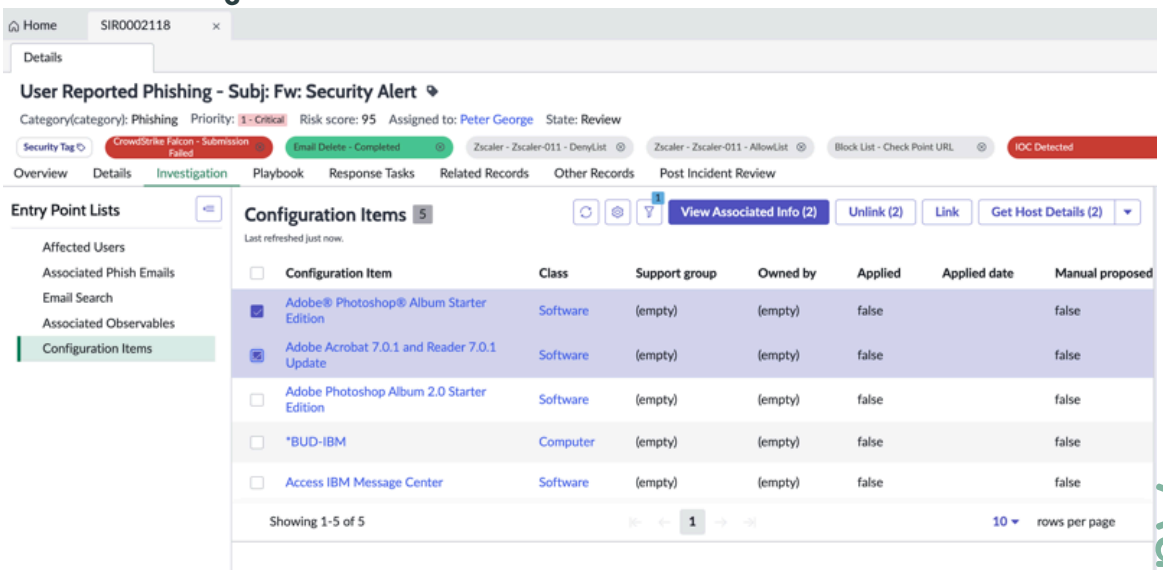
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Wechseln Sie zur Registerkarte **Ermittlung** des Arbeitsbereichs.
   Die Registerkarte Ermittlung mit den Einstiegspunktlisten wird angezeigt.



4. Wählen Sie das Configuration Item aus der Liste der Einstiegspunkte aus.
   Wählen Sie beispielsweise die Liste **der Konfigurationselement** -Einstiegspunkte aus. Die entsprechenden Datensätze für Configuration Items werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

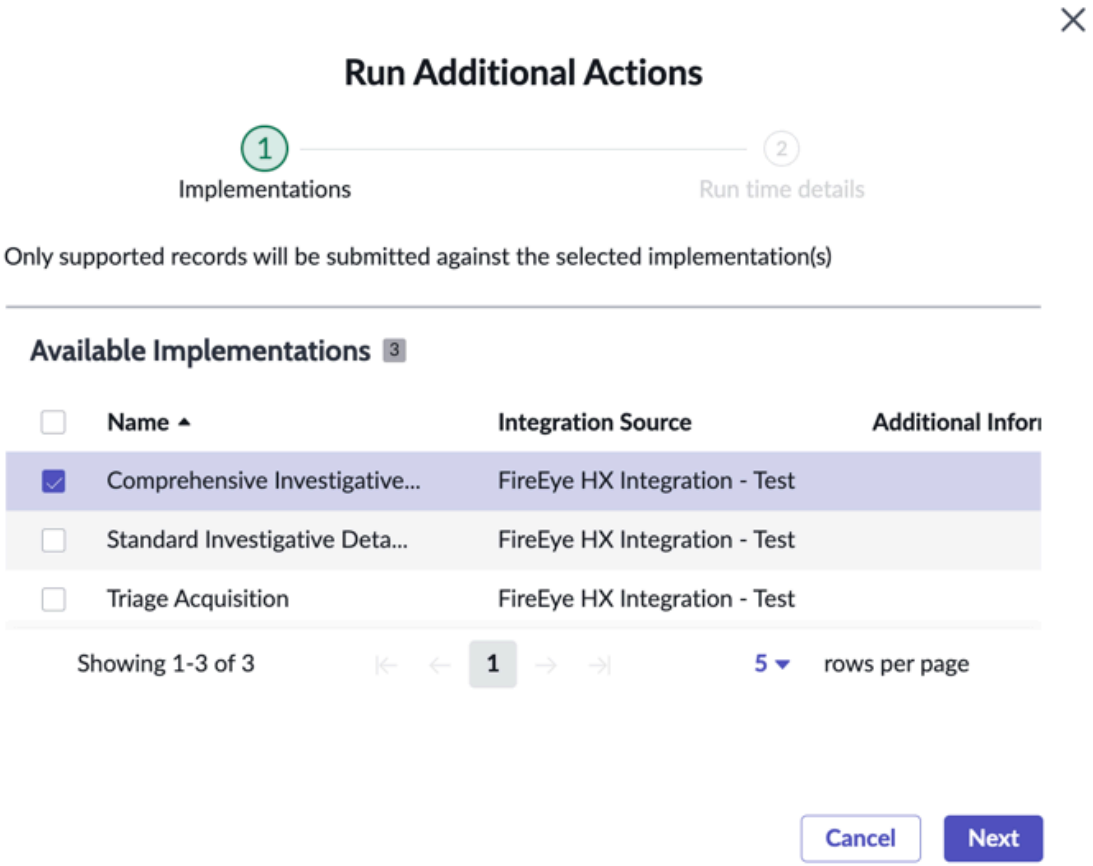
Wählen Sie Configuration Item aus



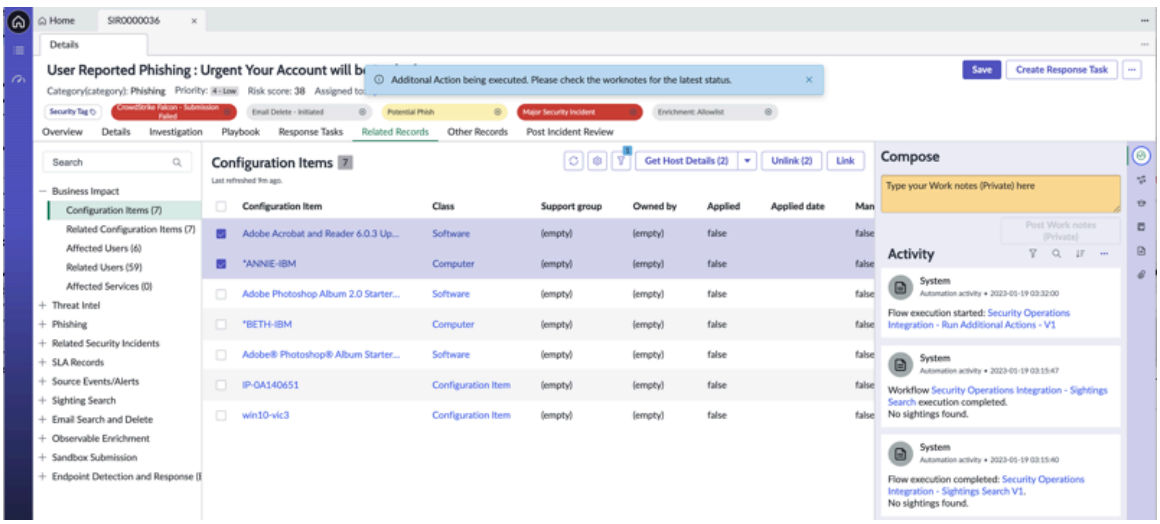
5. Wählen Sie ein beliebiges **Configuration Item**aus.
6. Navigieren Sie zu den zugehörigen Listen, die oben auf der Seite angezeigt werden.
   Für Security Incident Configuration Item (CI) enthalten die Dropdown-Listen die folgende Liste von Fähigkeitsaktionen. Die aufgeführten CI-Aktionen erfassen die Ergebnisse und speichern sie als Ergänzungsdaten zu einem Security Incident:
   - Datei abrufen: Diese Fähigkeit führt die Aktion aus, um Dateien mit einem bestimmten Hash-Wert oder einem Dateinamen abzurufen.
   - Host isolieren: Diese Fähigkeit schränkt Systemverbindungen mit anderen Geräten ein.
   - Hostdetails abrufen: Diese Fähigkeit ruft die Hostdetails, Details angemeldeter Benutzer und andere Ergänzungsfunktionen ab.
   - Zusätzliche Aktionen ausführen: Diese Fähigkeit führt zusätzliche Aktionen aus, die über die Standardaktionen hinausgehen.
   - Netzwerkstatistiken abrufen: Diese Fähigkeit ruft die Netzwerkstatistiken für eine betroffene Ressource ab.
   - Laufenden Prozess abrufen: Diese Fähigkeit ruft eine Liste der laufenden Prozesse für ein Configuration Item (CI) von einem Host ab.
   - Angemeldete Anwender abrufen: Diese Funktion sammelt die Daten angemeldeter Anwender und bezieht sie auf den Security Incident.
7. Wählen Sie **„Zusätzliche Aktionen ausführen“** aus, um die Aktion für Integrationsfähigkeiten im Zusammenhang mit Bedrohungsinformationen auszuführen.
   Das modale Dialogfeld Zusätzliche Implementierungen ausführen wird angezeigt.
8. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie auf **Next (Weiter)**.
   Sie werden jetzt zum nächsten Schritt weitergeleitet, um die Laufzeitdetails hinzuzufügen.
10. Geben Sie einen Kommentar ein, der der Aktion zugeordnet werden soll.
11. Klicken Sie auf **Absenden**.



Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Anforderung „Zusätzliche Aktion“ ausgeführt wird. Außerdem wird im Abschnitt **„Aktivität“** der jeweilige Fortschritt der Implementierungsaktion angezeigt.

12. Zeigen Sie die Ergebnisse aus dem Abschnitt mit der zugehörigen Liste für EDR an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

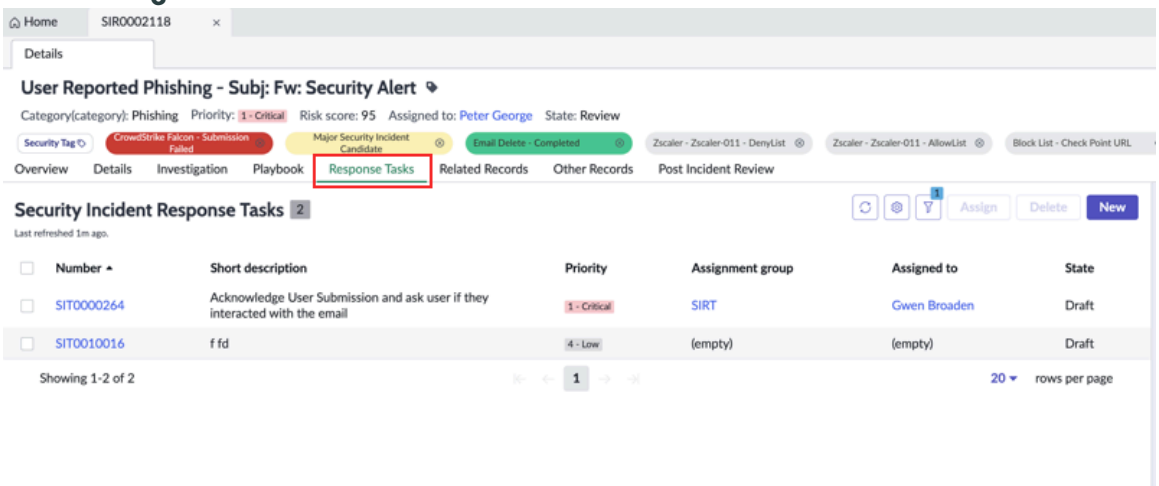
Security Incident Response-Aufgaben

Alle mit einem Security Incident verknüpften Antwortaufgaben werden im Abschnitt „Antwortaufgaben“ angezeigt.

Der Analyst kann:

- eine neue Antwortaufgabe erstellen
- sich selbst oder anderen Antwortaufgaben zuweisen
- Antwortaufgaben löschen

Antwortaufgaben im -Arbeitsbereich



Hinweis:
Dient zur schnellen Bearbeitung der Antwortaufgaben. Wählen Sie die Antwortaufgabe aus. Eine Liste mit Antwortaufgaben wird angezeigt. Wählen Sie den Datensatz aus, nehmen Sie Änderungen vor, und speichern Sie die Antwortaufgabe.

Erstellt eine Antwortaufgabe

Erstellen Sie Antwortaufgaben, um einzelne Aktionen nachzuverfolgen, die als Reaktion auf das Sicherheitsproblem auszuführen sind.

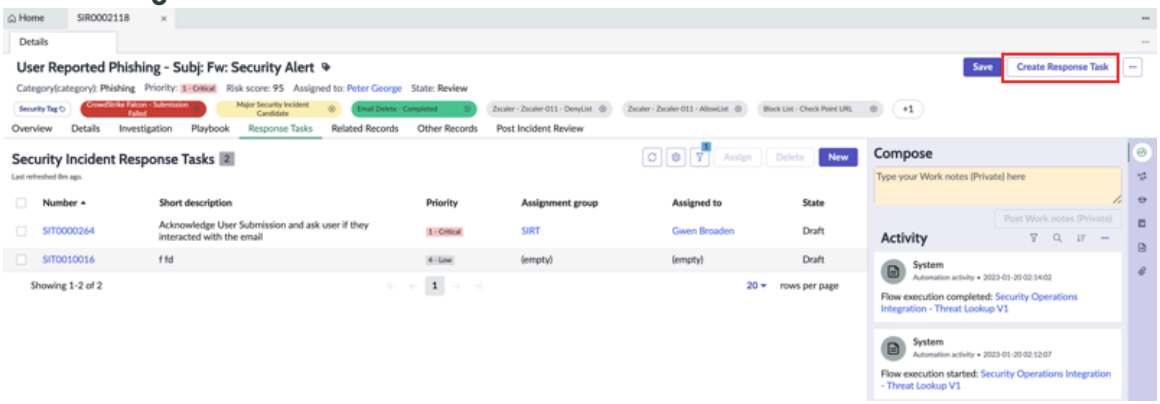
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf die **Option Antwortaufgabe erstellen** aus den UI-Aktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe erstellen



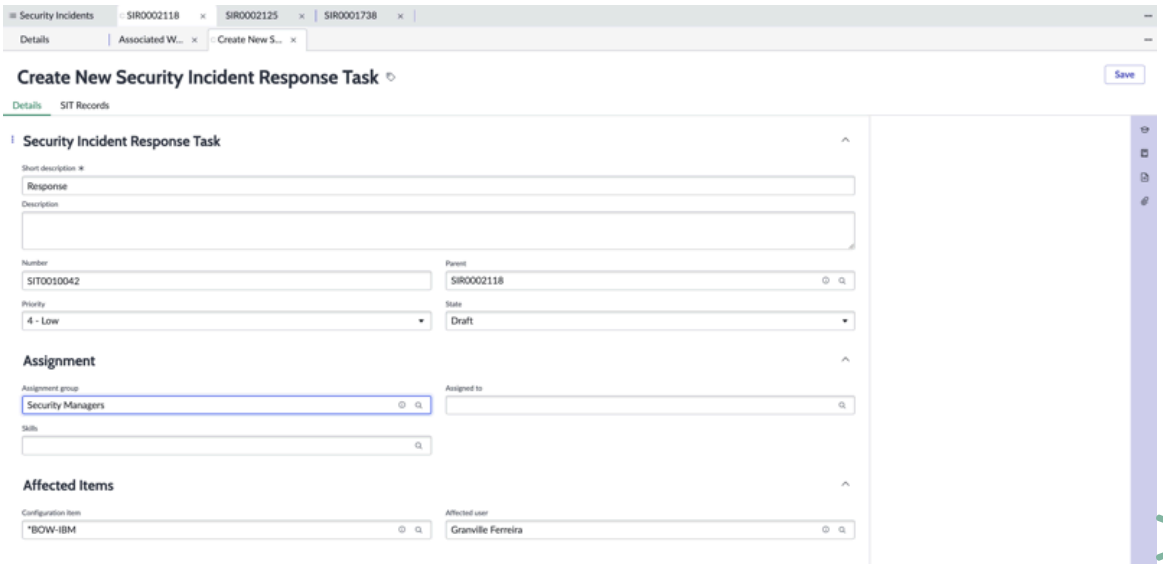
3. Füllen Sie die entsprechenden Felder im Formular aus.

Security Incident

Feld	Beschreibung
Kurzbeschreibung	Eine Beschreibung der Aufgabe Security Incident Response.
Beschreibung	Eine Beschreibung für die ausgewählte Aufgabe.
Nummer	Eindeutige Nummer, die automatisch für einen Security Incident generiert wird.
Übergeordnet	Die Nummer des zugehörigen Security Incidents.
Priorität	Die Priorität, mit der bestimmt wird, wann diese Aufgabe ausgeführt wird.
Status	Der aktuelle Status der Sicherheitsantwortaufgabe. Standardmäßig lautet der Anfangsstatus **Entwurf**.
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Person, der die Ausführung der Aufgabe zugewiesen ist.
Kompetenzen	Die für die Ausführung dieser Aufgabe erforderliche Kompetenz. Suchen Sie über die Suche, und wählen Sie die erforderliche Kompetenz aus.
Betroffene Elemente	Die von dem Sicherheitsproblem betroffenen Elemente.
Konfigurationselement	Das Configuration Item, das von dem Sicherheitsproblem betroffen ist.
Betroffener Anwender	Die von dem Sicherheitsproblem betroffene Person.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



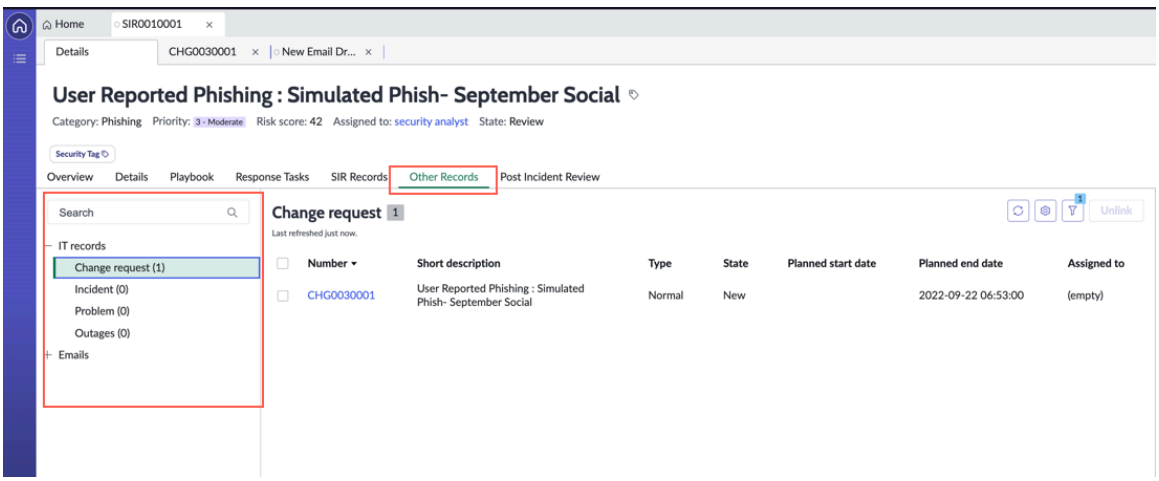
4. Klicken Sie auf **Speichern**.
   Die neue Antwortaufgabe (SIT) wird erstellt.

Security Incident Response – Andere Datensätze

In diesem Abschnitt werden die anderen Datensätze angezeigt, z. B. IT-bezogene Datensätze und E-Mail-Datensätze. Unter IT-Datensätze werden Incident, Change-Anforderung, Problem und Ausfälle angezeigt.

Unter E-Mail werden Entwürfe, Gesendete E-Mails und Empfangene E-Mails angezeigt.

Andere Datensätze



Incident erstellen

Erstellt einen Incident in einem Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst.

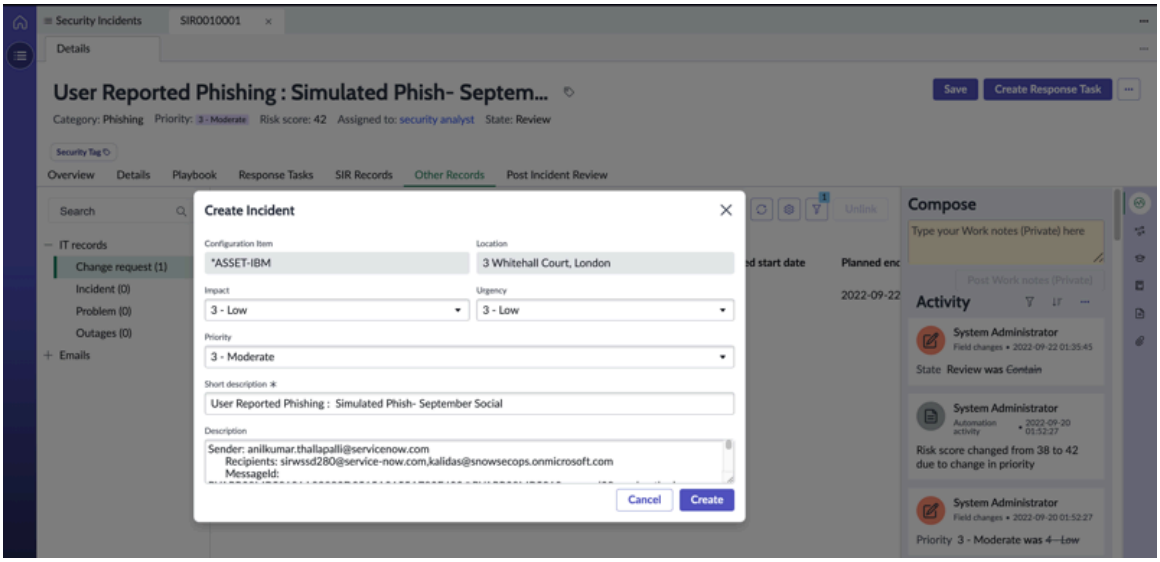
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.

Automatische Übersetzung

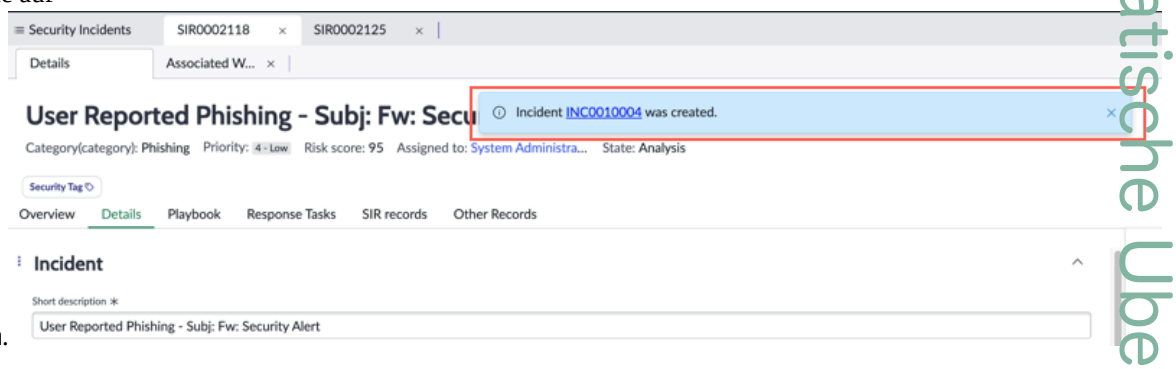
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Incident erstellen**.



4. Geben Sie die Details wie Konfigurationselement, Auswirkung, Dringlichkeit, Standort, Priorität und Kurzbeschreibung ein.

5. Klicken Sie auf **Erstellen**.



6. Ein Incident wird erstellt.

Problemaufgaben erstellen

Erstellen Sie eine Problemaufgabe.

Vorbereitungen

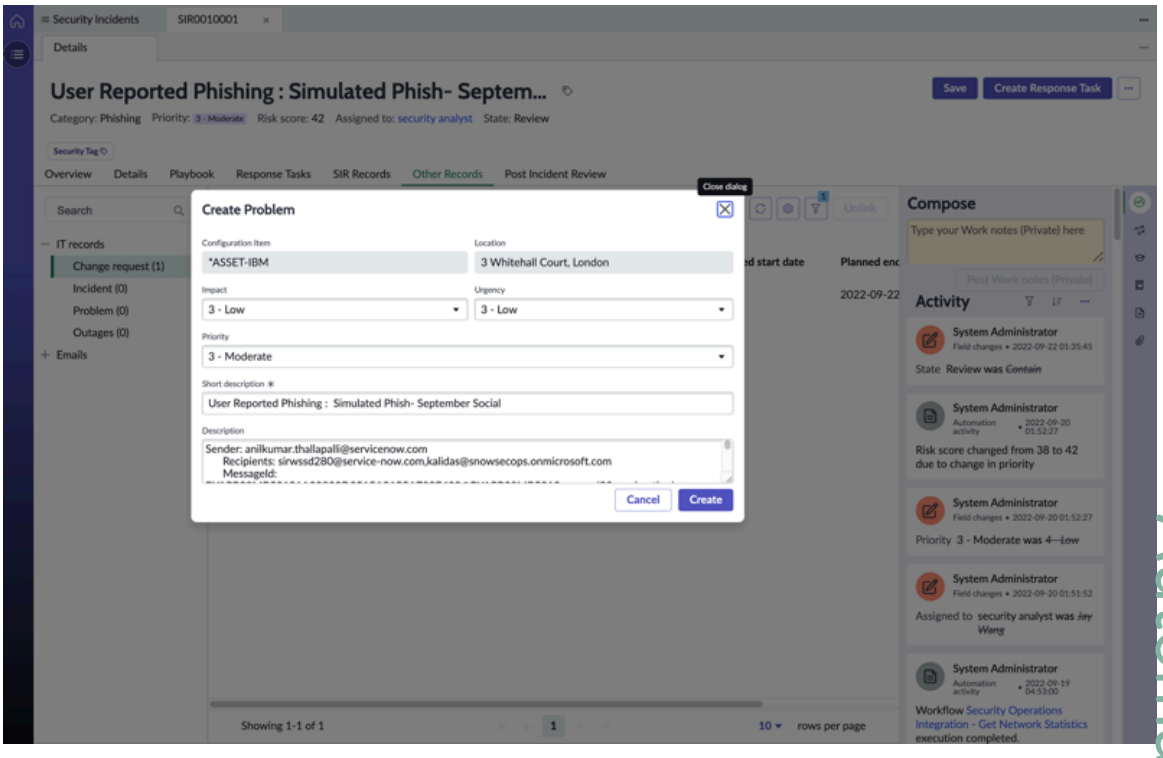
Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.
3. Klicken Sie auf **Problem erstellen**.

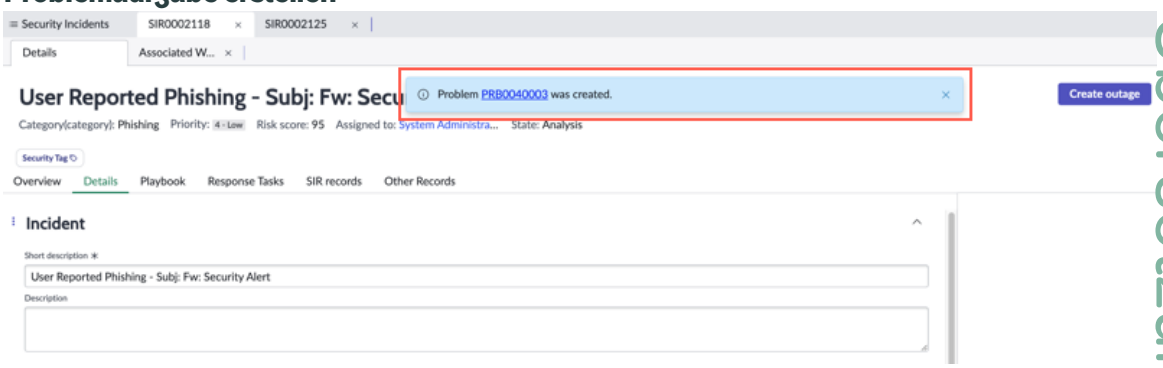
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Details wie Konfigurationselement, Ort, Auswirkung, Dringlichkeit, Priorität und Kurzbeschreibung aus.
5. Klicken Sie auf **Erstellen**.

Problemaufgabe erstellen



6. Eine Problemaufgabe wird erstellt.

Change-Anforderungen erstellen

Erstellen Sie eine Change-Anforderung.

Vorbereitungen

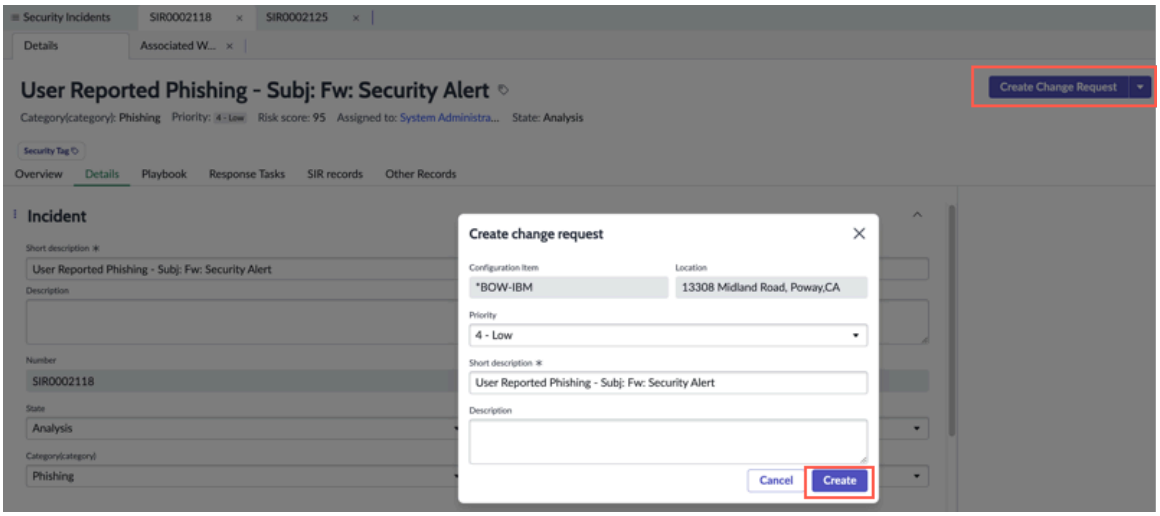
Erforderliche Rolle: sn_si.analyst.

Prozedur

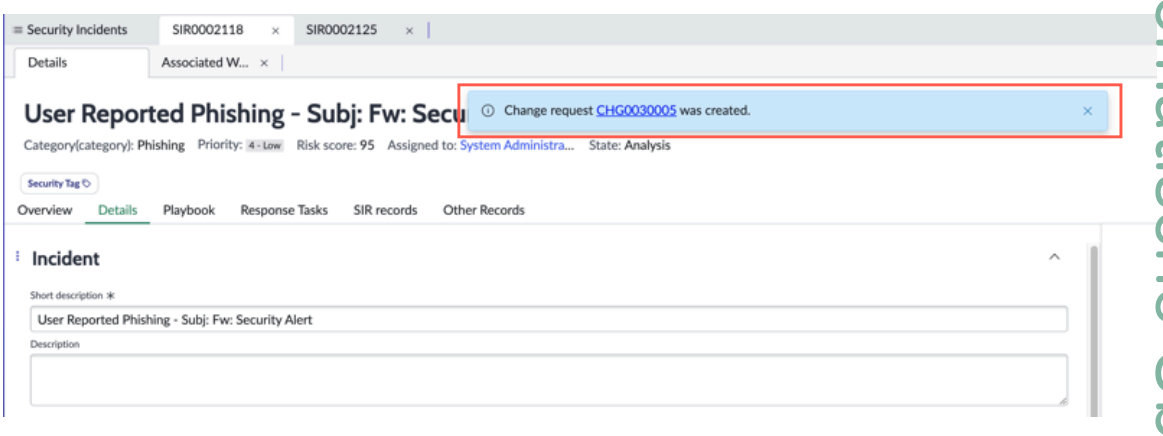
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.
3. Klicken Sie auf **Change-Anforderung erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie die Details wie Configuration Item, Standort, Priorität und Kurzbeschreibung ein.
5. Klicken Sie auf **Erstellen**.



6. Eine Change-Anforderung wird erstellt.

Ausfall erstellen

Erstellen Sie einen Ausfall aus einem Incident, um die Ausfallzeit eines Konfigurationselements nachzuverfolgen.

Vorbereitungen

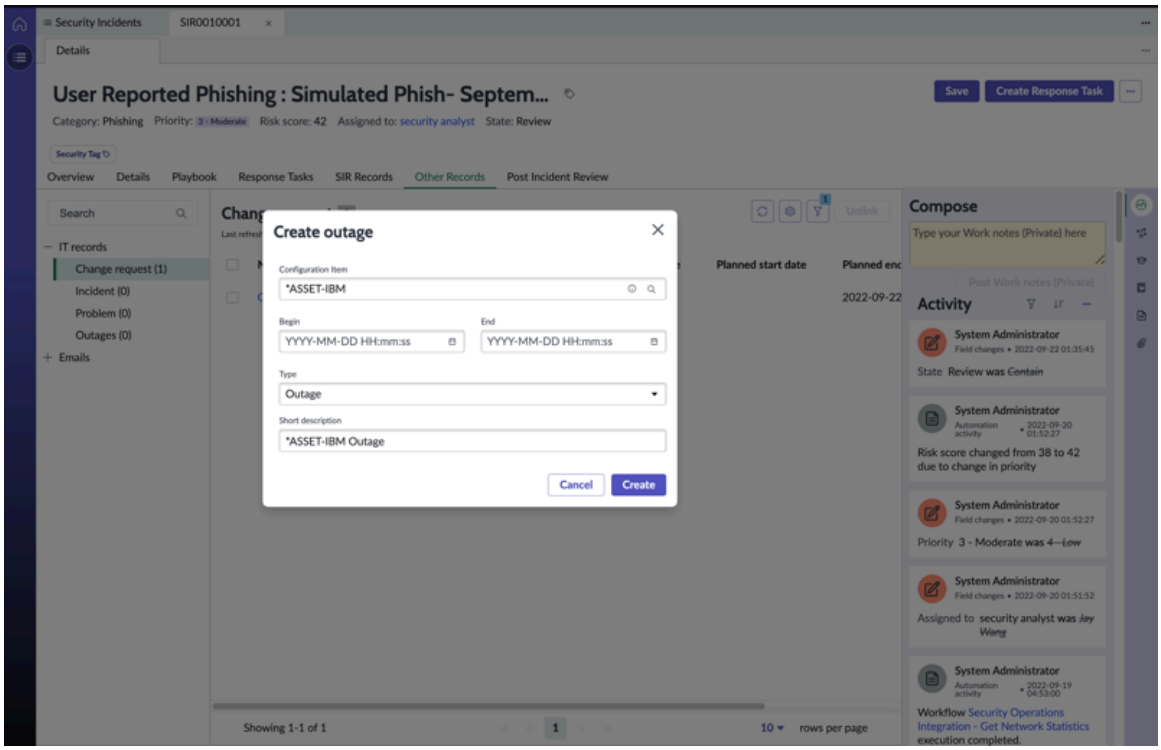
Erforderliche Rolle: sn_si.analyst

Prozedur

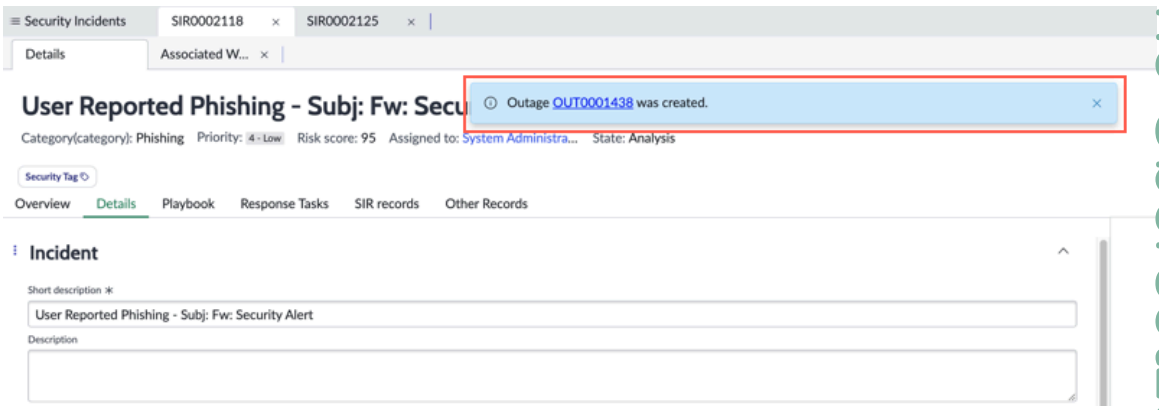
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.
3. Klicken Sie auf **Ausfall erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie die Details wie Konfigurationselement, Startdatum, Enddatum, Typ und Kurzbeschreibung ein.
5. Klicken Sie auf **Erstellen**.



E-Mails verfassen

Als Analyst können Sie E-Mails direkt aus Security Incidents verfassen.

Vorbereitungen

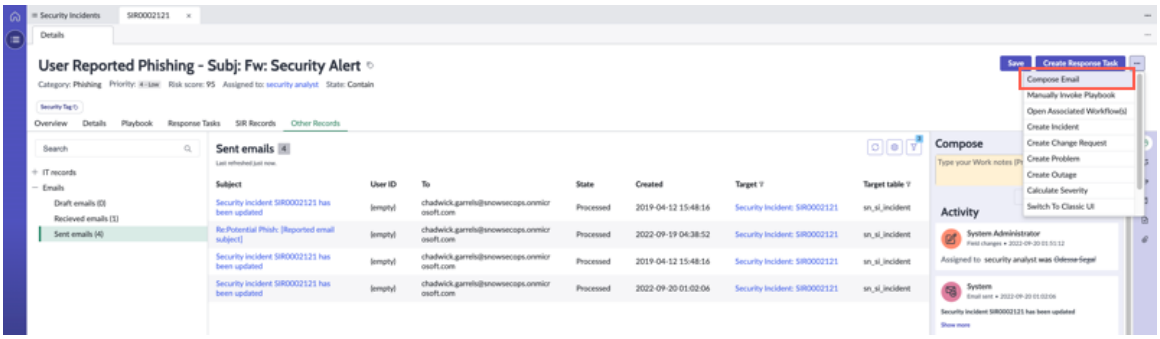
Erforderliche Rolle: sn_si.analyst

Prozedur

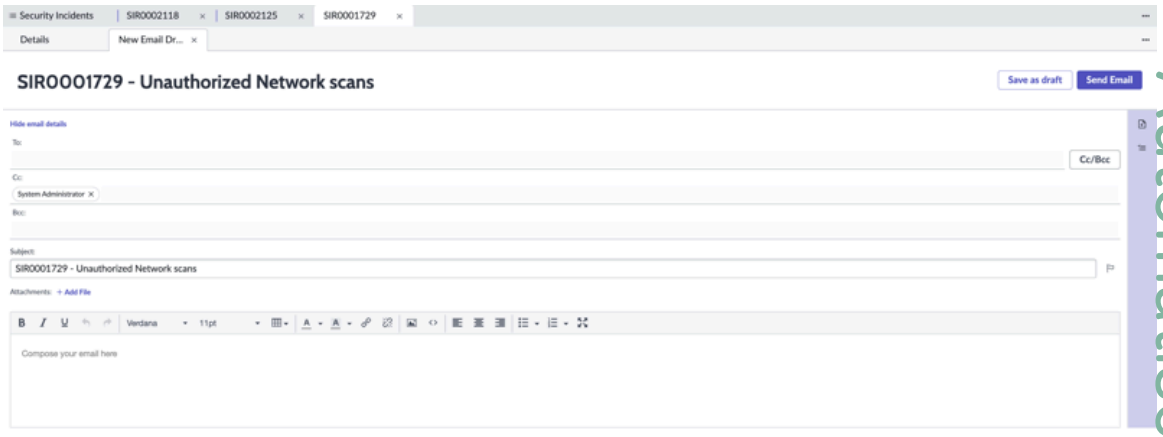
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen Sie den Incident aus, für den Sie eine E-Mail verfassen möchten, und öffnen Sie ihn.
3. Klicken Sie auf den Überlauf, und wählen Sie **E-Mail erstellen**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

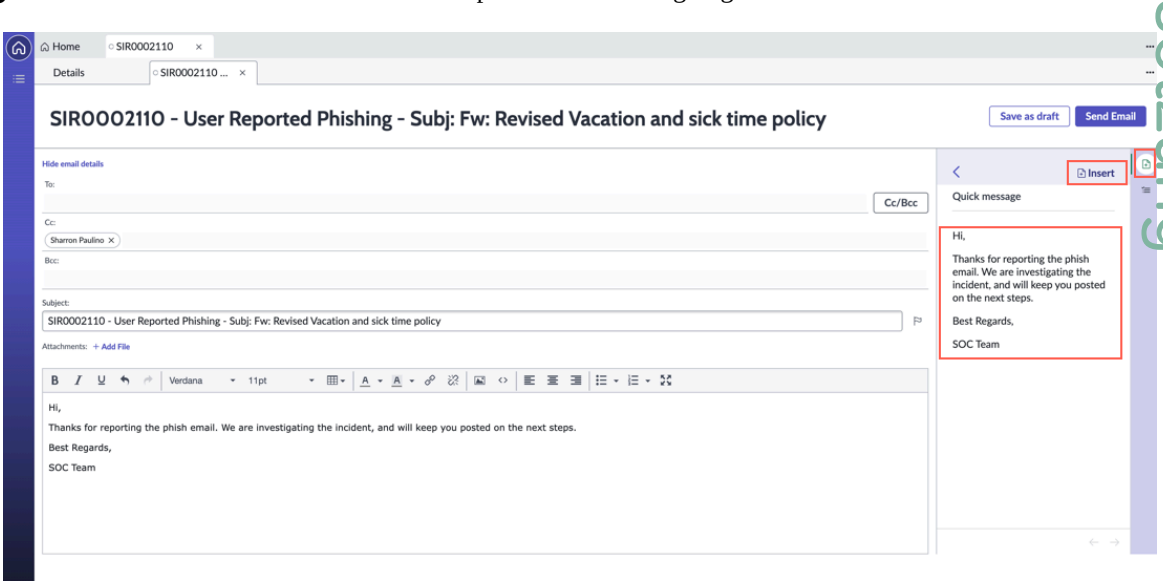


4. Geben Sie die Felder **An** und **CC** ein.



5. **Fügen Sie** ggf. Anhänge hinzu.

6. Klicken Sie im E-Mail-Formular **auf Textbausteine**, um die Textbausteine anzuzeigen, die auf der rechten Seite im Abschnitt **E-Mails erstellen** angezeigt werden.
   Die verfügbaren Textbausteine werden angezeigt. Wählen Sie die Nachricht aus, und klicken Sie auf **Einfügen**. Die Nachrichten werden in den Textkörper der E-Mail eingefügt.



7. Verfassen Sie Ihre E-Mail, und klicken Sie auf **E-Mail senden**.

Automatische Übersetzung

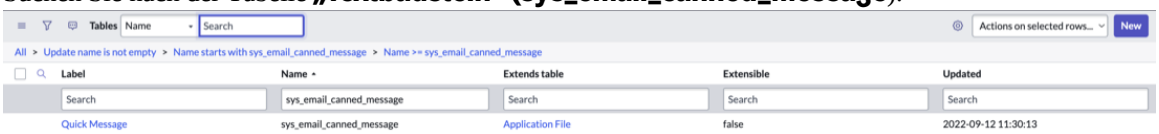
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können eine E-Mail als Entwurf speichern. Diese E-Mail-Entwürfe sind unter der Registerkarte „Andere Datensätze“ verfügbar.

So konfigurieren Sie Textbausteine:

a. Navigieren zu **Systemdefinitionen** > **Tabellen**.

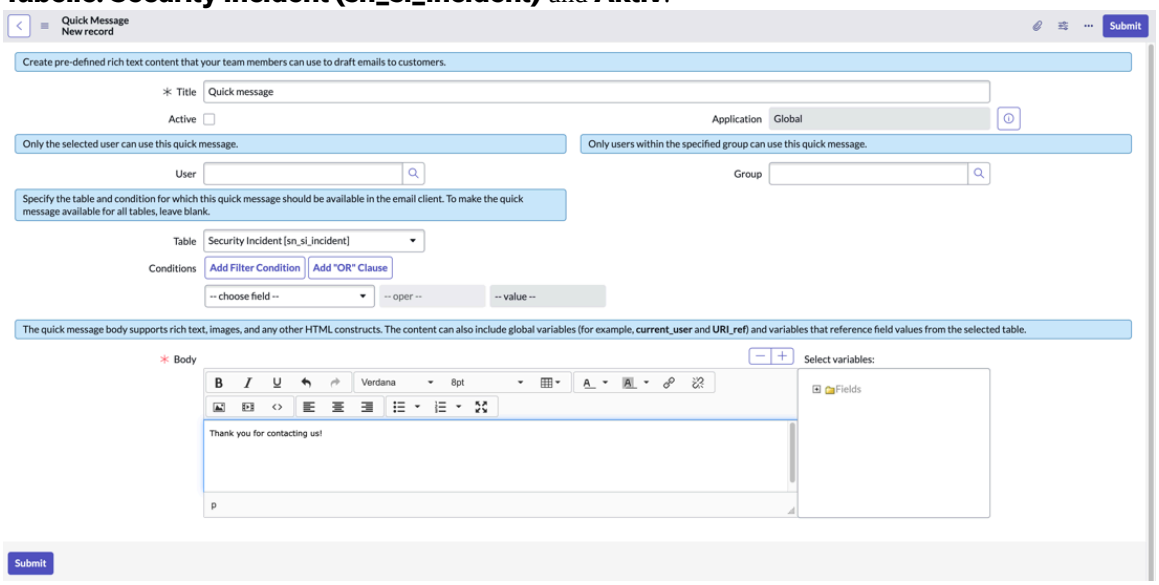
b. Suchen Sie nach der Tabelle **„Textbaustein“ (sys_email_canned_message**).



c. Gehe zu **Zugehörige Links** > **Liste anzeigen**.

d. **Neu**erstellen .

e. Geben Sie den **Titel**und **den Textkörper der Nachricht**ein, und aktivieren Sie die Kontrollkästchen **Tabelle: Security Incident (sn_si_incident)** und **Aktiv**.



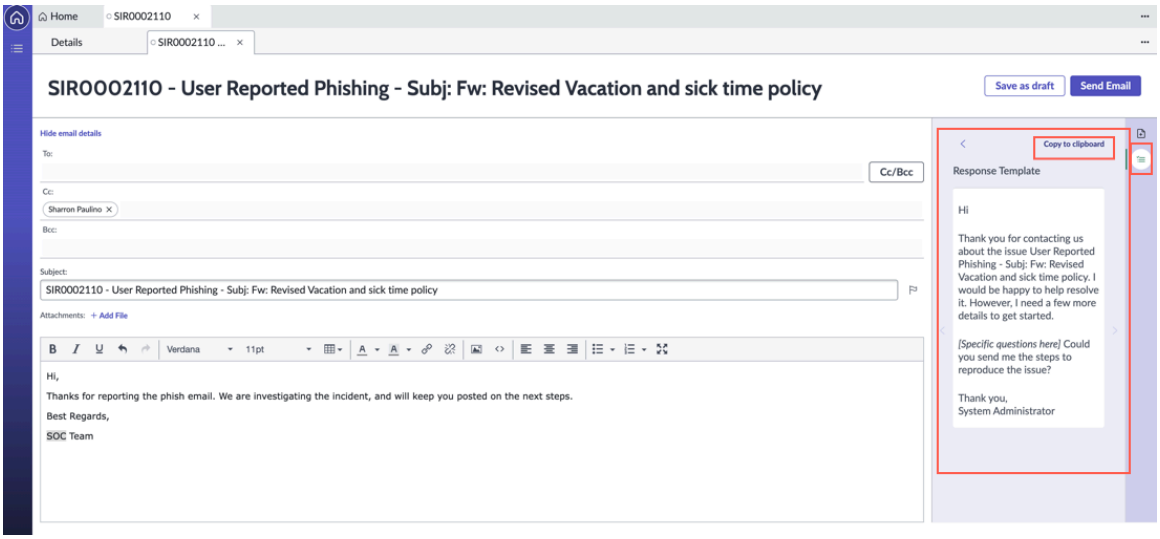
f. Klicken Sie auf **Absenden**.
Nachdem in der Tabelle ein neuer Eintrag erstellt wurde, wird die Textbaustein im Kontextmenü angezeigt.

8. Klicken Sie auf **Vorlagen**, um bei Bedarf eine Vorlage hinzuzufügen.

9. Wählen Sie die **Antwortvorlage** aus, und klicken Sie auf **In Zwischenablage kopieren** und wenden Sie die Vorlage an, falls erforderlich.

Automatische Übersetzung

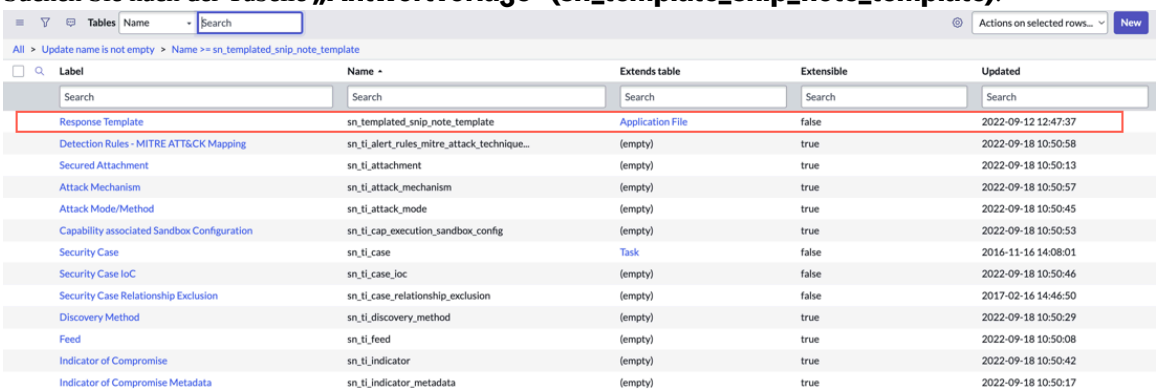
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



So konfigurieren Sie Antwortvorlagen:

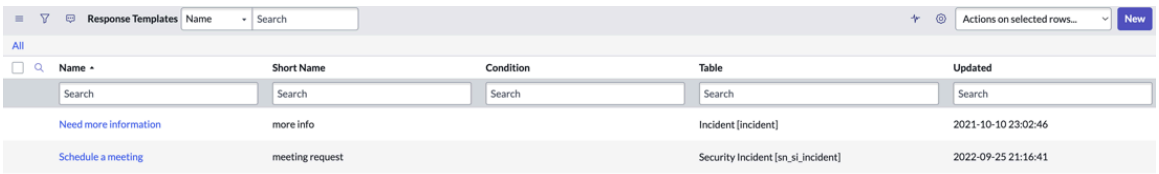
a. Navigieren zu **Systemdefinitionen** > **Tabellen**.

b. Suchen Sie nach der Tabelle **„Antwortvorlage" (sn_template_snip_note_template)**.



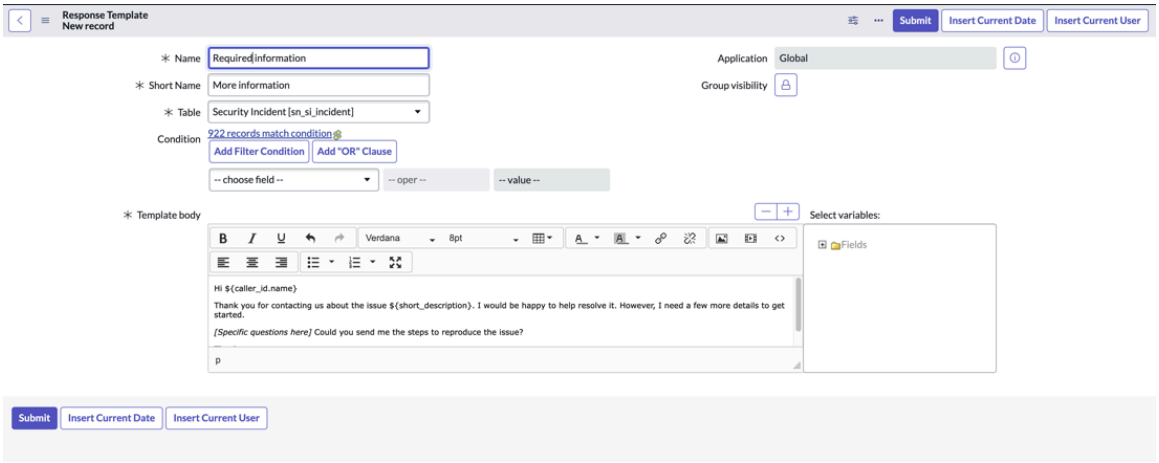
c. Gehe zu **Zugehörige Links** > **Liste anzeigen**.

d. Neuerstellen .



e. Geben Sie den **Namen**und **den Kurznamen**ein, und wählen Sie die **Tabelle: Security Incident (sn_si_incident)** und **den Vorlagentext**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



f. Klicken Sie auf **Absenden**.
Nachdem in der Tabelle ein neuer Eintrag erstellt wurde, wird die neue Vorlage im Kontextmenü angezeigt.

Security Incident Response – Überprüfung nach Incident

Die Überprüfung nach Incident wird angezeigt, wenn ein Incident in den Status Überprüfen versetzt wird.

Ausführlichere Informationen zur Durchführung von Aktivitäten nach Incidents finden Sie unter Bericht zur Überprüfung nach Incident

Die Überprüfung nach Incident besteht aus den folgenden Abschnitten:

1. Bewertungen
2. Berichte

Im Arbeitsbereich für Security Incident Response können Sie mit diesen beiden neuen UI-Aktionen Bewertungen anfordern und durchführen.

Name	Beschreibung
Bewertungen	Bewertung zeigt alle Bewertungen an, die dem Security Incident zugeordnet sind. Der Analyst kann Bewertungen vornehmen und Bewertungen anfordern. • **Assessments durchführen**: Klicken Sie auf **Assessments durchführen,** um (falls zutreffend) die Assessments durchzuführen und das Assessment abzuschließen. Vor Abschluss der Bewertung wird der Status des Security Incidents als Bereit zur Abnahme angegeben, und das Fälligkeitsdatum des Incidents wird rot angezeigt. • Bewertungen anfordern: Klicken Sie auf **Bewertung anfordern**, um zusätzliche Bewertungen anzufordern. Fügen Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	dann die neuen Benutzer hinzu, die Sie anfordern möchten. **Hinweis:** Anwender, die bereits angefordert haben, werden in diesem Abschnitt nicht angezeigt. Jede Bewertung für diesen Incident wurde auf Grundlage der in der Überprüfung nach Incident festgelegten Bedingungen konfiguriert; entweder obligatorisch oder optional.
Berichte	Ändern Sie die Laufzeitkonfigurationen, und generieren Sie den Bericht. Wählen Sie die Berichtsinstanz aus, ändern Sie die Filter, und speichern Sie den Bericht. Analysten können den PIR-Bericht in der Vorschau anzeigen und herunterladen.

TISC-Integration in SIR-Arbeitsbereich

Der folgende Abschnitt enthält Informationen zur Integration des Threat Intelligence-Sicherheitszentrums aus dem SIR-Arbeitsbereichskontext.

Senden Sie Daten aus dem SIR-Arbeitsbereich an TISC

Erfahren Sie, wie die Daten zwischen den Arbeitsbereichen Threat Intelligence Security Center (TISC) und Security Incident Response (SIR) zusammenarbeiten und geteilt werden, indem Sie die in den folgenden Abschnitten erläuterten Verfahren anwenden.

Systemeigenschaften zum Senden von Daten

Überprüfen Sie die Systemeigenschaften für TISC-Integrationen für die Kombination mit SIRW. Sie können diese Eigenschaften konfigurieren, um zu steuern, wie beide Anwendungen die Integrationen verwalten.

Wichtige Überlegungen

Die Systemeigenschaften für TISC-Integrationen bieten erweiterte Konfigurationsoptionen für den Umgang der Anwendung mit erkennbaren Elementen und Ergänzungen.

1. Zum Festlegen der Systemeigenschaften für TISC-Integrationen in SIRW navigieren Sie zu den **Systemeigenschaften** für Threat Intelligence, und greifen Sie auf die Tabelle [sys_properties] zu.
2. Die Systemeigenschaften steuern und verarbeiten das Verhalten jedes einzelnen Daten-Push-Vorgangs.
3. Wenn die Eigenschaft aktiviert ist, werden die Daten automatisch übertragen, wenn die erkennbaren Elemente oder Ergänzungsdaten im SIR-Arbeitsbereich generiert werden.
4. Wenn die Eigenschaft deaktiviert ist, werden die Daten manuell übertragen. Anwender können Daten mithilfe der UI-Aktionen aus dem SIR-Arbeitsbereich übertragen.

Die folgende Liste zeigt die Systemeigenschaften für die TISC-SIR-Integration:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Daten von erkennbaren Elementen automatisch und manuell aus SIR pushen: Aktivieren Sie die Eigenschaft sn_ti.allow_observable_and_enrichment_records_push, um die Daten entweder automatisch oder manuell zu pushen. Wenn diese Eigenschaft deaktiviert ist, deaktiviert sie den automatischen und manuellen Modus für alle Daten-Push-Übertragungen von SIR.
- Ergebnisse der Bedrohungssuche pushen: Aktivieren Sie die Systemeigenschaft sn_ti.automatic_push_threat_lookup_results, um Daten der Bedrohungssuche automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Bedrohungssuchedaten weiterhin manuell veröffentlichen.
- Sichtungssuchergebnisse an TISC weiterleiten: Aktivieren Sie diese Systemeigenschaft sn_ti.automatic_push_sighting_results_to_tisc, um Sichtungssuchdaten automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Sichtungssuchdaten weiterhin manuell pushen.
- Erkennbare Elemente pushen: Aktivieren Sie diese Systemeigenschaft sn_ti.automatic_push_observable_to_tisc, um Daten erkennbarer Elemente automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Daten erkennbarer Elemente weiterhin manuell veröffentlichen.
- Ergänzungsergebnisse veröffentlichen: Aktivieren Sie diese Systemeigenschaft sn_ti.automatic_push_enichment_results, um Daten zu Ergänzungsergebnissen automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Daten der Ergänzungsergebnisse weiterhin manuell veröffentlichen.

Fügen Sie dem TISC-Fall einen Security Incident hinzu

Fügen Sie TISC-Falldatensätzen Security Incidents hinzu.

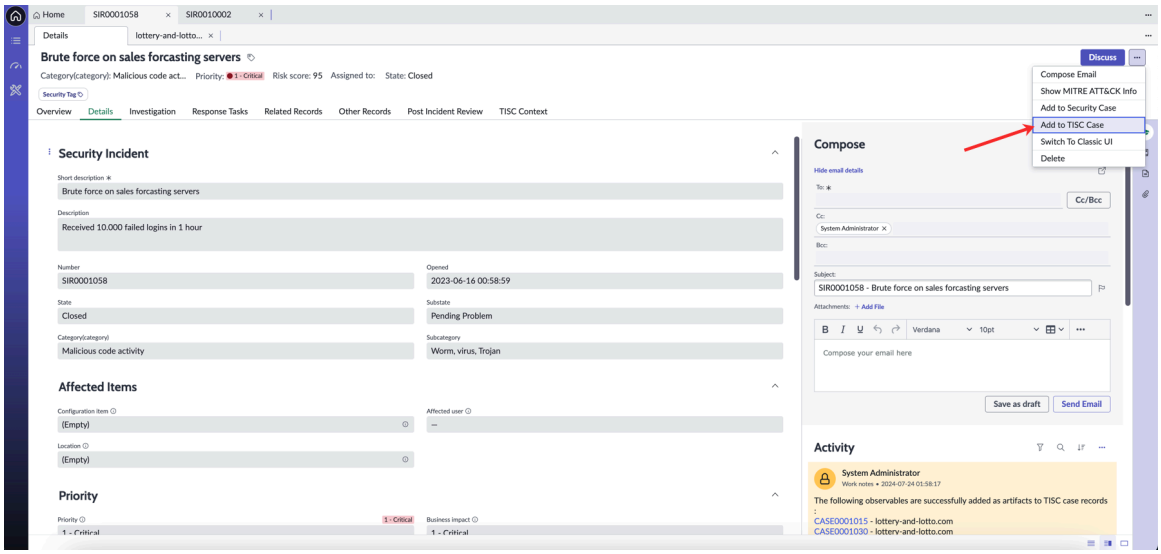
Vorbereitungen

Erforderliche Rolle: sn_si.analyst, sn_sec_tisc.case_write

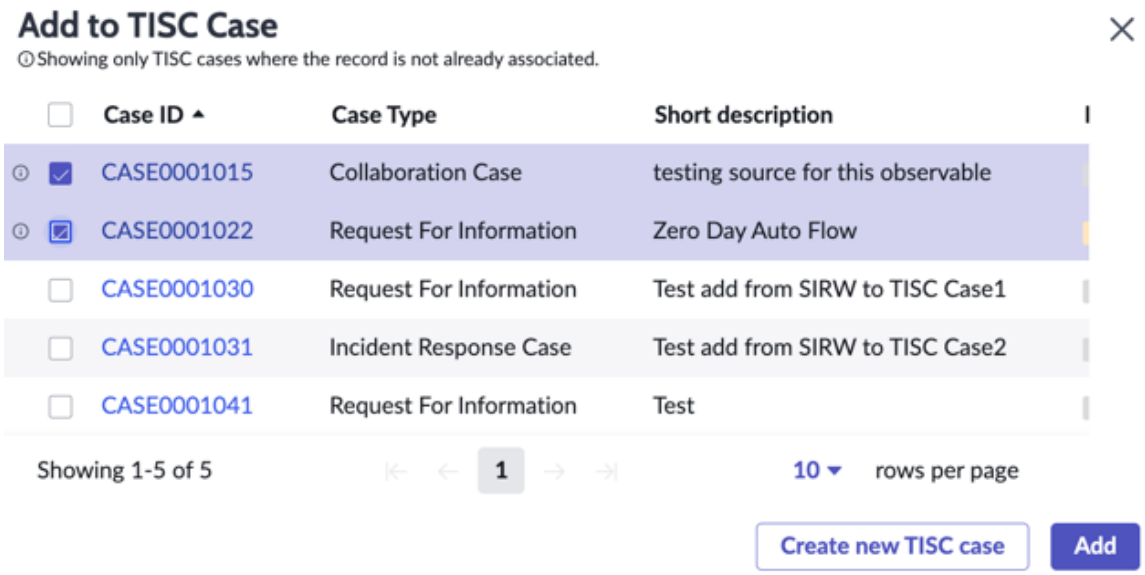
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**.
2. Suchen und öffnen Sie einen bestimmten Security Incident, den Sie untersuchen.
   Sie können dazu auch nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder nach dem Incident-Status filtern.
3. Klicken Sie auf das Symbol **„Weitere Aktionen“**.
4. Klicken Sie auf die Aktion **Zu TISC-Fall hinzufügen**.
   Das Dialogfeld „Zu TISC-Fall hinzufügen“ wird angezeigt, und zeigt nur die TISC-Fälle an, denen der Incident noch nicht zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



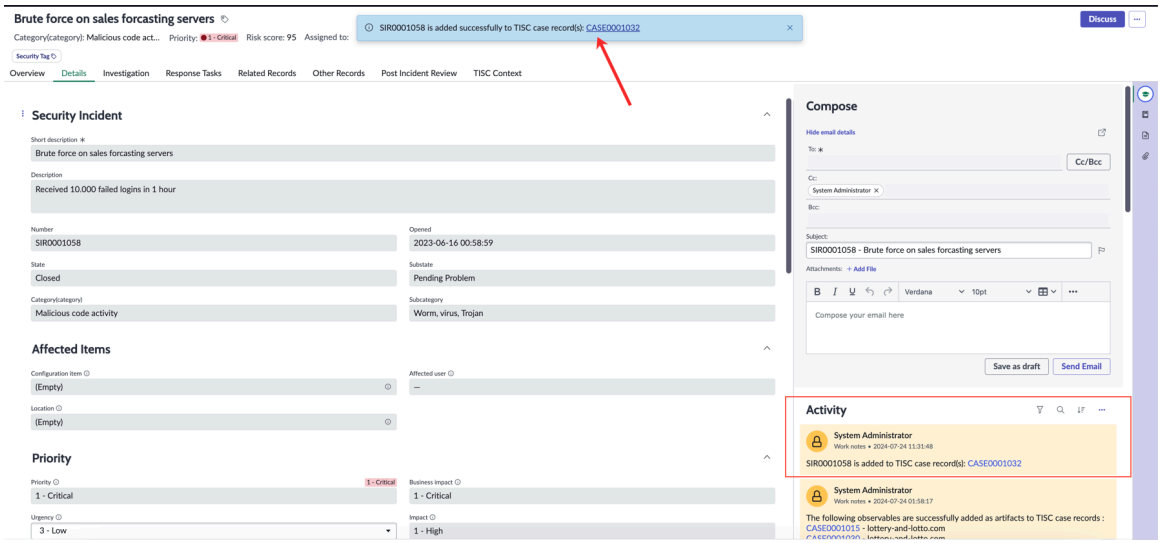
5. Wählen Sie den/die Fall(e) im Dialogfeld **„Zu Fall hinzufügen“** aus.



Hinweis:
Neuen TISC-Fall erstellen, wenn keine Falldatensätze vorhanden sind. Weitere Informationen zum Erstellen von Fällen finden Sie unter Erstellen von Fällen mit der Workbench für Bedrohungsanalysten.

6. Klicken Sie auf **Hinzufügen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf den Falldatensatz, um den Fall in TISC aus der angezeigten Informationsnachricht oder aus dem **Aktivitätenstrom** anzuzeigen.

> **Hinweis:**
> Um die verknüpften Security Incidents anzuzeigen, klicken Sie auf den jeweiligen Falldatensatz im **Aktivitätenstrom** des Security Incidents. Wenn Sie auf klicken, gelangen Sie zum Falldatensatz im TISC-Arbeitsbereich, und die Security Incidents werden auf der Registerkarte **Artefakte** des Moduls Fallverwaltung hinzugefügt.

Fügen Sie dem TISC-Fall erkennbare Elemente hinzu

Fügen Sie TISC-Falldatensätzen erkennbare Elemente hinzu.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst, sn_sec_tisc.case_write

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**.
2. Suchen und öffnen Sie einen bestimmten Security Incident, den Sie untersuchen.
   Sie können dazu auch nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder nach dem Incident-Status filtern.
3. Klicken Sie im Arbeitsbereich auf die Registerkarte **Zugehörige Datensätze**.
   Sie können auf verschiedenen Registerkarten im Arbeitsbereich für Security Incident Response erkennbare Elemente zu TISC-Fällen hinzufügen.

> **Hinweis:**
> Sie können zu folgendem Ort navigieren:
>
> - Detailseite für erkennbare Elemente auf der Registerkarte „Zugehörige Datensätze“.
> - Registerkarte**Ermittlung**, navigieren Sie zum Abschnitt **„Einstiegspunktlisten“**, der auf der linken Seite angezeigt wird, und wählen Sie **Zugeordnete erkennbare Elemente**, um dem TISC-Fall erkennbare Elemente hinzuzufügen.

4. Wählen Sie beispielsweise aus **Bedrohungsinformationen** > **Zugehörige erkennbare Elemente**.

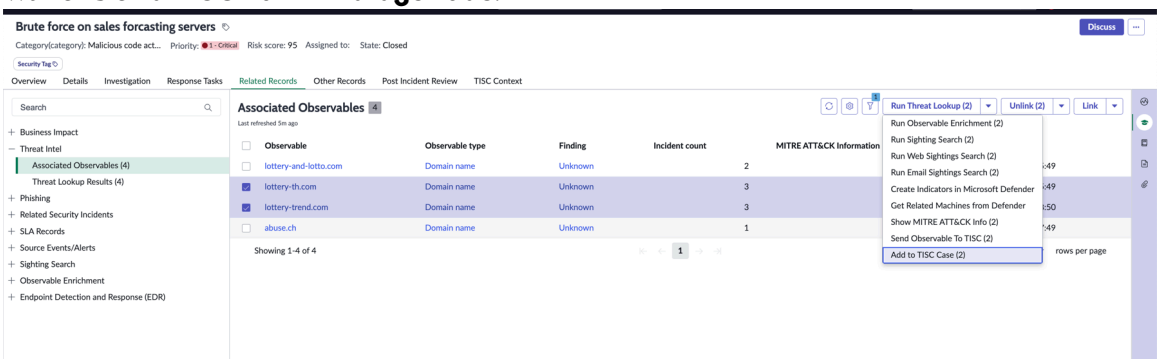
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

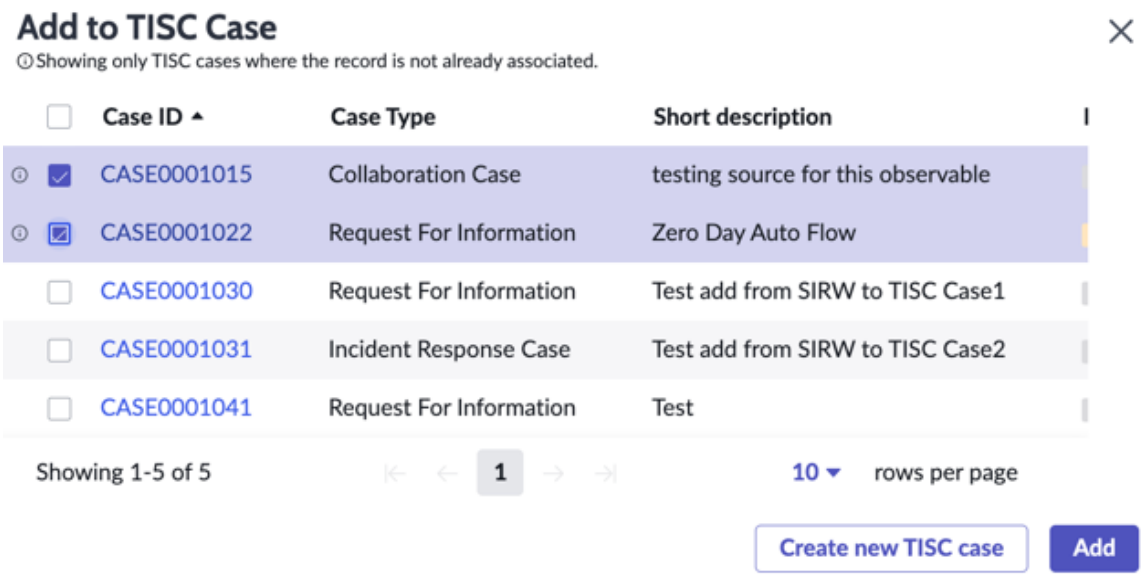
5. Wählen Sie ein oder mehrere erkennbare Elemente aus, um die ausgewählten erkennbaren Elemente den Falldatensätzen hinzuzufügen.

Hinweis:
Sie können auch auf einen beliebigen Datensatz für erkennbare Elemente klicken. Dadurch wird die Detailseite für erkennbare Elemente auf einer anderen Registerkarte geöffnet. Sie können auch Falldatensätze von hier hinzufügen, indem Sie auf „Zu TISC-Fall hinzufügen“ klicken.

6. Klicken Sie auf die Schaltfläche zum Teilen **von Fähigkeitsaktionen**.
7. Wählen Sie **Zu TISC-Fall hinzufügen aus**.



8. Wählen Sie den/die Fall(e) im Dialogfeld **„Zu Fall hinzufügen“** aus.



Hinweis:
Neuen TISC-Fall erstellen, wenn keine Falldatensätze vorhanden sind. Weitere Informationen zum Erstellen von Fällen finden Sie unter Erstellen von Fällen mit der Workbench für Bedrohungsanalysten.

9. Klicken Sie auf **Hinzufügen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf den Falldatensatz, um den Fall in TISC aus der angezeigten Informationsnachricht oder aus dem **Aktivitätenstrom** anzuzeigen.

Hinweis:
Wenn das erkennbare Element kein entsprechendes TISC-Erkennbares Element hat, wird das im SIR-Arbeitsbereich ausgewählte erkennbare Element automatisch an TISC gesendet und anschließend den ausgewählten TISC-Falldatensätzen hinzugefügt. Um die verknüpften erkennbaren Elemente anzuzeigen, klicken Sie im **Aktivitätenstrom** auf den jeweiligen Falldatensatz. Wenn Sie auf klicken, gelangen Sie zum Falldatensatz im TISC-Arbeitsbereich, und die erkennbaren Elemente werden auf der Registerkarte **„Artefakte“** des Moduls „Fallverwaltung“ hinzugefügt.

Ergebnisse
Sie haben die Daten der erkennbaren Elemente erfolgreich an die Fallverwaltung für das Threat Intelligence-Sicherheitszentrum gesendet.

Erkennbare Elemente an TISC senden

Mit dieser Funktion kann der Sicherheitsanalyst die Daten erkennbarer Elemente von SIR zu TISC übertragen. Mithilfe des TISC-Kontexts können Sie überprüfen, ob die erkennbaren Elemente in TISC vorhanden sind. Andernfalls kann der Sicherheitsanalyst die Daten bei Bedarf veröffentlichen.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Prozedur

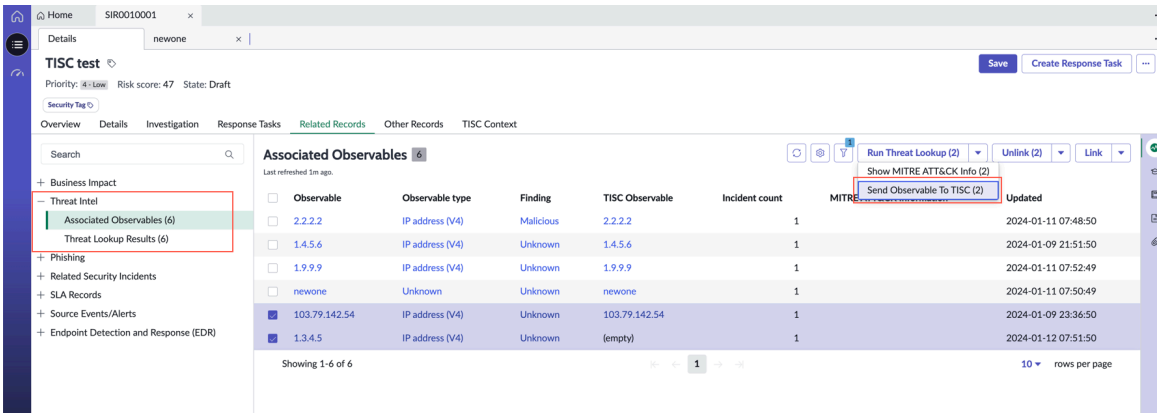
1. Navigieren Sie im SIR-Arbeitsbereich zur Registerkarte **Zugehörige Datensätze,** um die Aktion für die TISC-Integrationsfunktion auszuführen.

Hinweis:

- Sie können auch zur Registerkarte **Ermittlung** und dann zum Abschnitt **Einstiegspunktlisten** navigieren, der auf der linken Seite angezeigt wird, und **Zugehörige erkennbare Elemente** auswählen, um den Veröffentlichungsvorgang auszuführen.
- Klicken Sie auf der Registerkarte **Ermittlungauf Zugehörige Informationen anzeigen**, um alle zugehörigen Daten für die Bedrohungssuche, die Sichtungssuche und die Ergänzungsdaten für das ausgewählte erkennbare Element anzuzeigen. Weitere Informationen finden Sie unter Untersuchungs-Canvas erkunden.

2. Wählen Sie beispielsweise aus **Bedrohungsinformationen** > **Zugehörige erkennbare Elemente** um den Veröffentlichungsvorgang auszuführen und die Daten manuell in TISC zu übertragen.
3. Wählen Sie einen oder mehrere erkennbare Elemente aus, um den Vorgang **„Erkennbares Element an TISC senden“** auszuführen, um die Daten zu übertragen.

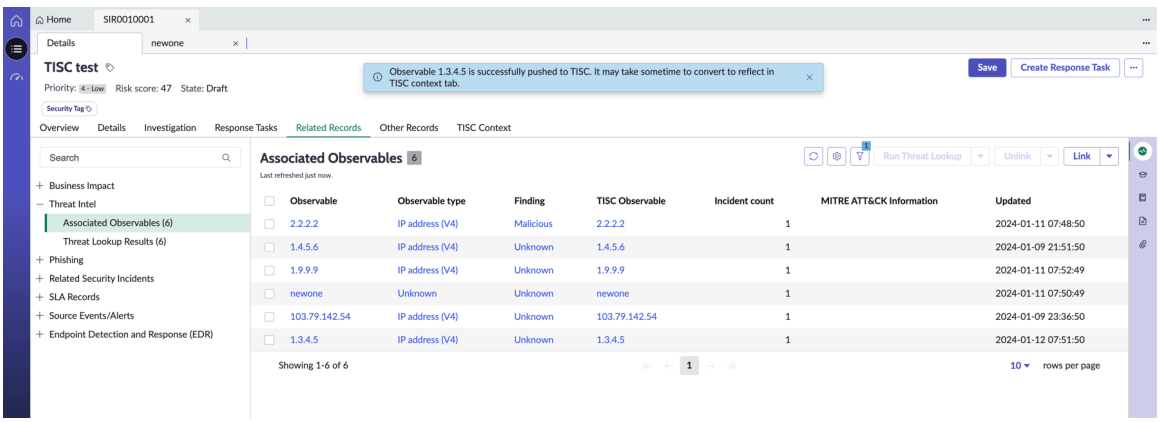
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Erkennbares Element an TISC senden**.

Hinweis:

- Wenn das ausgewählte erkennbare Element nicht in TISC vorhanden ist, wird es zuerst als erkennbare Quelle erstellt. Sobald das erkennbare Quellelement einen TISC-Datensatz für erkennbare Elemente erstellt, wird der erkennbare Datensatz automatisch dem neu erstellten erkennbaren Element zugeordnet.
- Sobald der Push-Vorgang für erkennbare Elemente ausgeführt wurde, wird eine Informationsmeldung angezeigt, dass Observable 0.0.0.0 erfolgreich an TISC übertragen wurde. Es kann einige Zeit dauern, bis die Konvertierung in der TISC-Kontextregisterkarteenthalten ist.

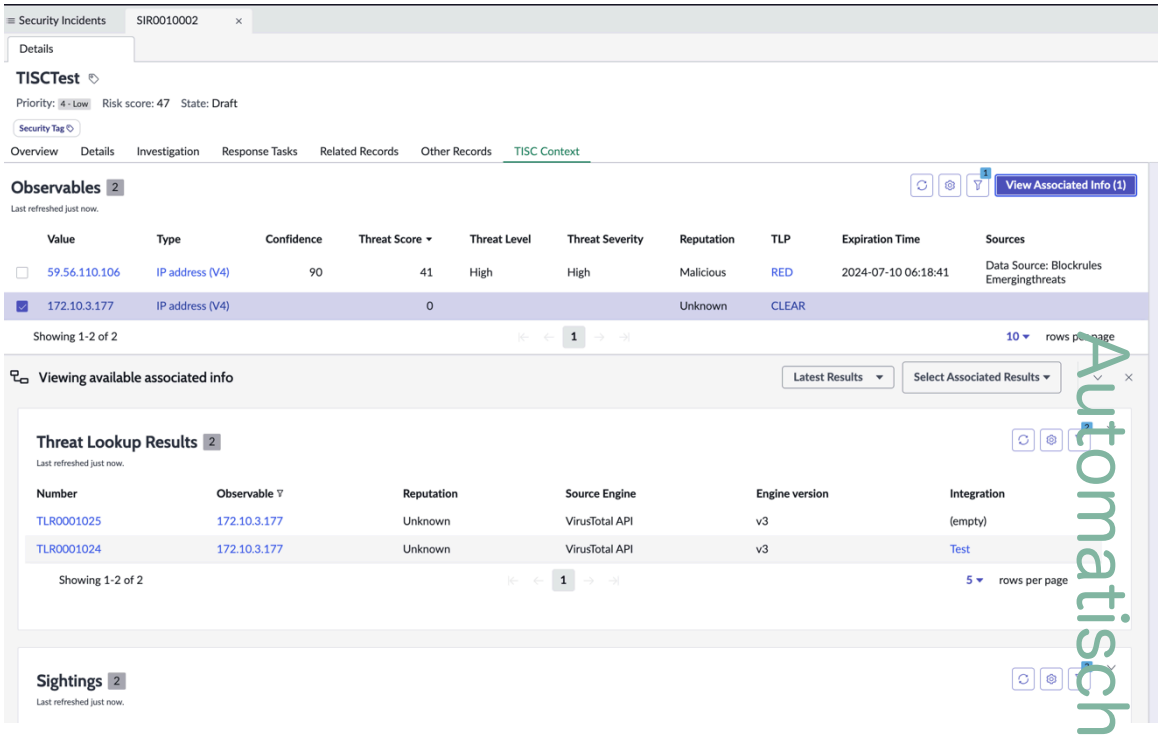


5. Wählen Sie **TISC-Kontext**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
:

- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.



- **Bei einem manuellen Veröffentlichungsvorgang**: Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element aus SIR übertragen wurde, können diese Daten mithilfe von Quellen identifiziert werden, die einen Verweis auf den mit dem erkennbaren Element verknüpften Security Incident enthalten.
- **Bei einem automatischen Push-Vorgang**: Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.
- **TISC-Kontext** zeigt alle dem SIR zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Über den TISC-Kontext können SIR-Analysten alle TISC-Ergänzungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuchen und Daten der Ergänzung erkennbarer Elemente.
- **„Zugeordnete Informationen anzeigen“** zeigt alle zugeordneten Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

6. Zeigen Sie die Ergebnisse an.

Senden Sie die Bedrohungssuche an TISC

Mit dieser Funktion kann der Sicherheitsanalyst die Bedrohungssuchdaten von SIR an TISC übertragen. Mithilfe des TISC-Kontexts können Sie überprüfen, ob die Ergebnisse der Bedrohungssuche in TISC vorhanden sind. Andernfalls kann der Sicherheitsanalyst die Daten bei Bedarf veröffentlichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

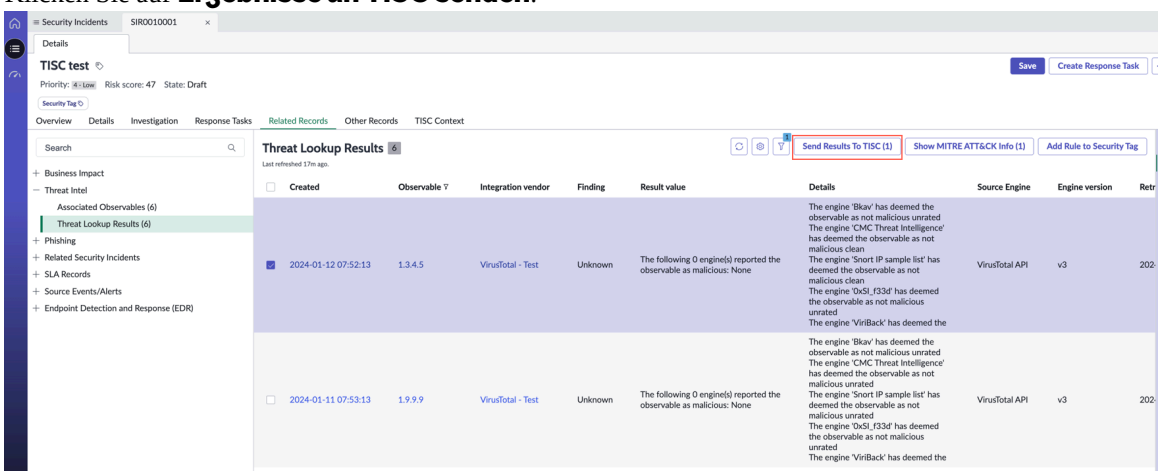
Prozedur

1. Navigieren Sie im SIR-Arbeitsbereich zur Registerkarte **Zugehörige Datensätze,** um die Aktion für die TISC-Integrationsfunktion auszuführen.

Hinweis:

- Sie können auch zur Registerkarte **Ermittlung** und dann zum Abschnitt **Einstiegspunktlisten** navigieren, der auf der linken Seite angezeigt wird, und **Zugehörige erkennbare Elemente** auswählen, um den Veröffentlichungsvorgang auszuführen.
- Klicken Sie auf der Registerkarte **Ermittlungauf Zugehörige Informationen anzeigen**, um alle zugehörigen Daten für die Bedrohungssuche, die Sichtungssuche und die Ergänzungsdaten für das ausgewählte erkennbare Element anzuzeigen. Weitere Informationen finden Sie unter Untersuchungs-Canvas erkunden.

2. Auswahlvorgang **Bedrohungsinformationen** > **Bedrohungssuche – Ergebnisse** um den Veröffentlichungsvorgang auszuführen und die Daten manuell in TISC zu übertragen.
3. Wählen Sie mindestens einen Datensatz mit Ergebnissen der Bedrohungssuche aus.
4. Klicken Sie auf **Ergebnisse an TISC senden**.



Hinweis:

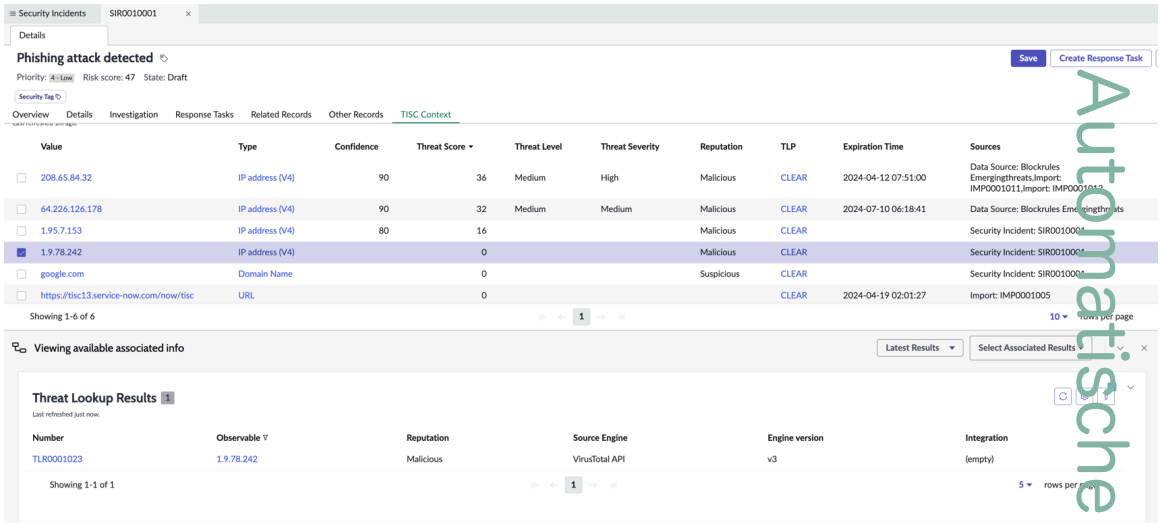
- Wenn das ausgewählte erkennbare Element der Bedrohungssuche in TISC nicht vorhanden ist, wird es im manuellen Modus zuerst als erkennbare Quelle erstellt. Sobald das erkennbare Quellelement einen TISC-Datensatz für ein erkennbares Element erstellt, wird der erkennbare Datensatz automatisch dem neu erstellten erkennbaren Element zugeordnet. Außerdem wird die ausgewählte Bedrohungssuche an das neu erstellte erkennbare Element für die Bedrohungssuche im manuellen Modus übertragen.
- In einem automatischen Modus werden die erkennbaren Elemente nicht übertragen, wenn das erkennbare Element vorhanden ist. Dann werden die Bedrohungssuchen automatisch übertragen. Wenn die erkennbaren Elemente nicht vorhanden sind, werden die Bedrohungssuchen nicht gepusht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Es wird eine Bestätigungsmeldung angezeigt, dass das erkennbare Element (1.9.78.242) für den ausgewählten Bedrohungssuchdatensatz in TISC nicht vorhanden ist. Es dauert einige Zeit, um ein erkennbares Element zu erstellen und den Bedrohungssuchdatensatz des erkennbaren Elements in TISC automatisch zuzuordnen.
   Sobald verarbeitet und übertragen wurde, können Sie die Ergebnisse sehen.
6. Wählen Sie **TISC-Kontext**aus.

Hinweis:
:

- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.



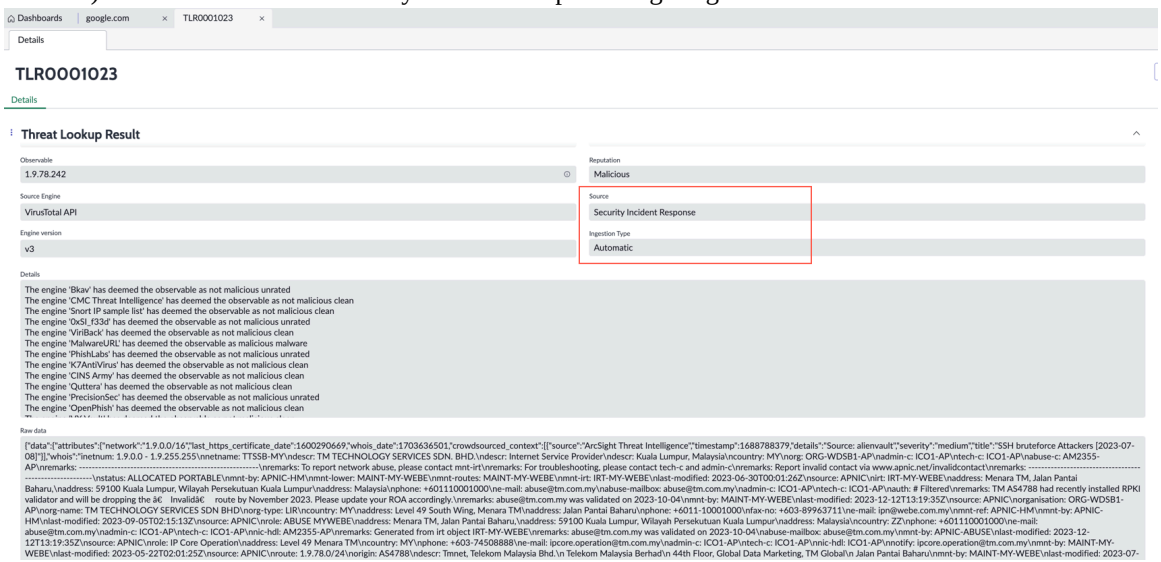
- **Bei einem manuellen Veröffentlichungsvorgang**: Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element aus SIR übertragen wurde, können diese Daten mithilfe von Quellen identifiziert werden, die einen Verweis auf den mit dem erkennbaren Element verknüpften Security Incident enthalten.
- **Bei einem automatischen Veröffentlichungsvorgang**: Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.
- **TISC-Kontext** zeigt alle dem SIR zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Über den TISC-Kontext können SIR-Analysten alle TISC-Ergänzungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuchen und Daten der Ergänzung erkennbarer Elemente.
- **„Zugeordnete Informationen anzeigen“** zeigt alle zugeordneten Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

7. In der Listenansicht werden alle Ergebnisse der Bedrohungssuche angezeigt. Wählen Sie jedoch einen beliebigen Datensatz aus, und klicken Sie auf die Schaltfläche **„Zugeordnete Informationen anzeigen“**.
8. Zeigen Sie die Ergebnisse der Bedrohungssuche an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie auf einen beliebigen Datensatz mit den Ergebnissen der Bedrohungssuche, um den Datensatz in der Formularansicht anzuzeigen. Dort werden auch der Push- oder **Erfassungstyp** (automatisch oder manuell) und **die Quelle** als Security Incident Response angezeigt.



Sichtungssuche an TISC senden

Mit dieser Funktion kann der Sicherheitsanalyst die Sichtungssuchdaten von SIR an TISC übertragen. Mithilfe des TISC-Kontexts kann der Analyst überprüfen, ob die Sichtungssuchdaten in TISC vorhanden sind. Wenn nicht, kann der Sicherheitsanalyst die Daten bei Bedarf veröffentlichen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

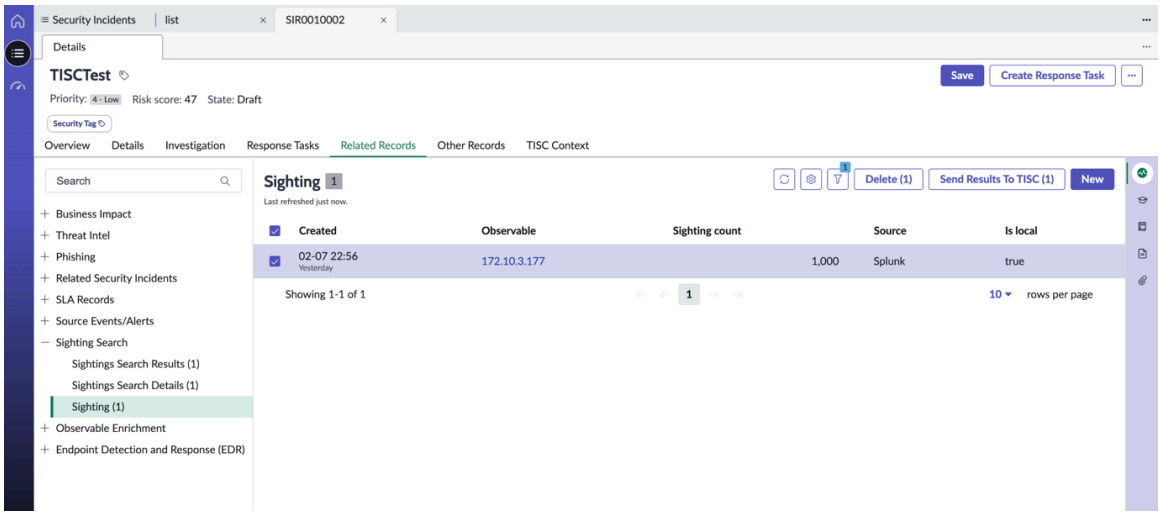
1. Navigieren Sie im SIR-Arbeitsbereich zur Registerkarte **Zugehörige Datensätze,** um die Aktion für die TISC-Integrationsfunktion auszuführen.

   Hinweis:

   - Sie können auch zur Registerkarte **Ermittlung** und dann zum Abschnitt **Einstiegspunktlisten** navigieren, der auf der linken Seite angezeigt wird, und **Zugehörige erkennbare Elemente** auswählen, um den Veröffentlichungsvorgang auszuführen.
   - Klicken Sie auf der Registerkarte **Ermittlungauf Zugehörige Informationen anzeigen**, um alle zugehörigen Daten für die Bedrohungssuche, die Sichtungssuche und die Ergänzungsdaten für das ausgewählte erkennbare Element anzuzeigen. Weitere Informationen finden Sie unter Untersuchungs-Canvas erkunden.

2. Auswahlvorgang **Sichtungssuche** > **Sichtungssuchergebnisse** um den Veröffentlichungsvorgang auszuführen und die Daten manuell in TISC zu übertragen.
3. Wählen Sie einen oder mehrere Datensätze mit Sichtungssuchergebnissen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

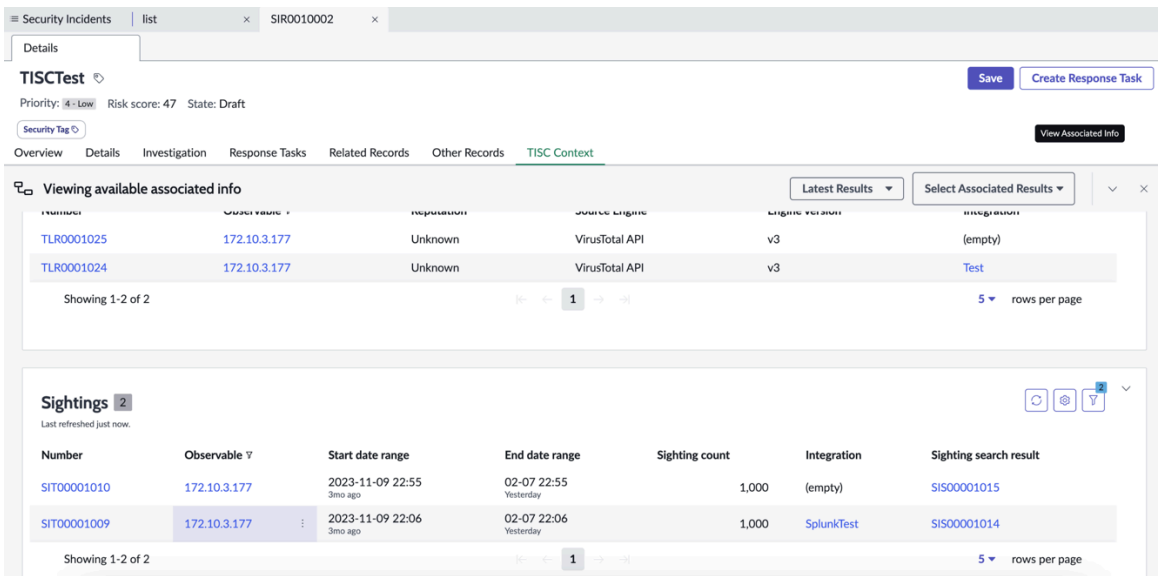


4. Klicken Sie auf **Ergebnisse an TISC senden**.

Hinweis:

- Wenn das ausgewählte erkennbare Element der Sichtungssuche in TISC nicht vorhanden ist, wird es im manuellen Modus zuerst als erkennbare Quelle erstellt. Sobald das erkennbare Quellelement einen TISC-Datensatz für ein erkennbares Element erstellt, wird der erkennbare Datensatz automatisch dem neu erstellten erkennbaren Element zugeordnet. Außerdem wird die ausgewählte Sichtungssuche an das neu erstellte erkennbare Element der Bedrohungssuche im manuellen Modus übertragen.
- In einem automatischen Modus werden die erkennbaren Elemente nicht übertragen, wenn das erkennbare Element vorhanden ist. Dann werden die Bedrohungssuchen automatisch übertragen. Wenn die erkennbaren Elemente nicht vorhanden sind, werden die Bedrohungssuchen nicht gepusht.

5. Wählen Sie **TISC-Kontext**aus.



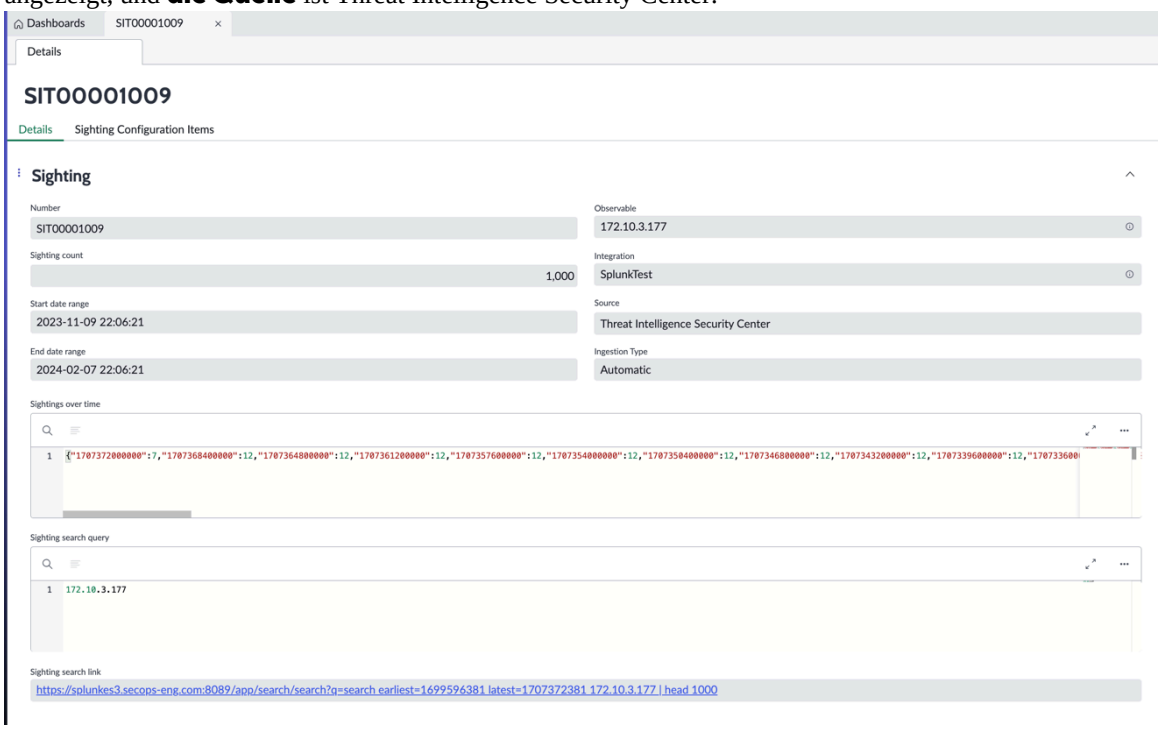
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

:

- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.
- **Bei einem manuellen Veröffentlichungsvorgang**: Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element aus SIR übertragen wurde, können diese Daten mithilfe von Quellen identifiziert werden, die einen Verweis auf den mit dem erkennbaren Element verknüpften Security Incident enthalten.
- **Bei einem automatischen Push-Vorgang**: Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.
- **TISC-Kontext** zeigt alle dem SIR zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Über den TISC-Kontext können SIR-Analysten alle TISC-Ergänzungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuchen und Daten der Ergänzung erkennbarer Elemente.
- **„Zugeordnete Informationen anzeigen"** zeigt alle zugeordneten Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

6. Sobald der Datensatz verarbeitet wurde, wählen Sie ihn aus, und klicken Sie auf **Zugehörige Informationen anzeigen**.
7. Zeigen Sie die Ergebnisse an.
8. Klicken Sie auf einen beliebigen Datensatz mit Sichtungssuchergebnissen, um den Datensatz in der Formularansicht anzuzeigen. Dort wird auch der Push- oder **Erfassungstyp** (automatisch oder manuell) angezeigt, und **die Quelle** ist Threat Intelligence Security Center.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergänzung erkennbarer Elemente an TISC senden

Mit dieser Funktion kann der Sicherheitsanalyst die Sichtungssuchdaten von SIR an TISC übertragen. Mithilfe des TISC-Kontexts kann der Analyst überprüfen, ob die Sichtungssuchdaten in TISC vorhanden sind. Wenn nicht, kann der Sicherheitsanalyst die Daten bei Bedarf veröffentlichen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

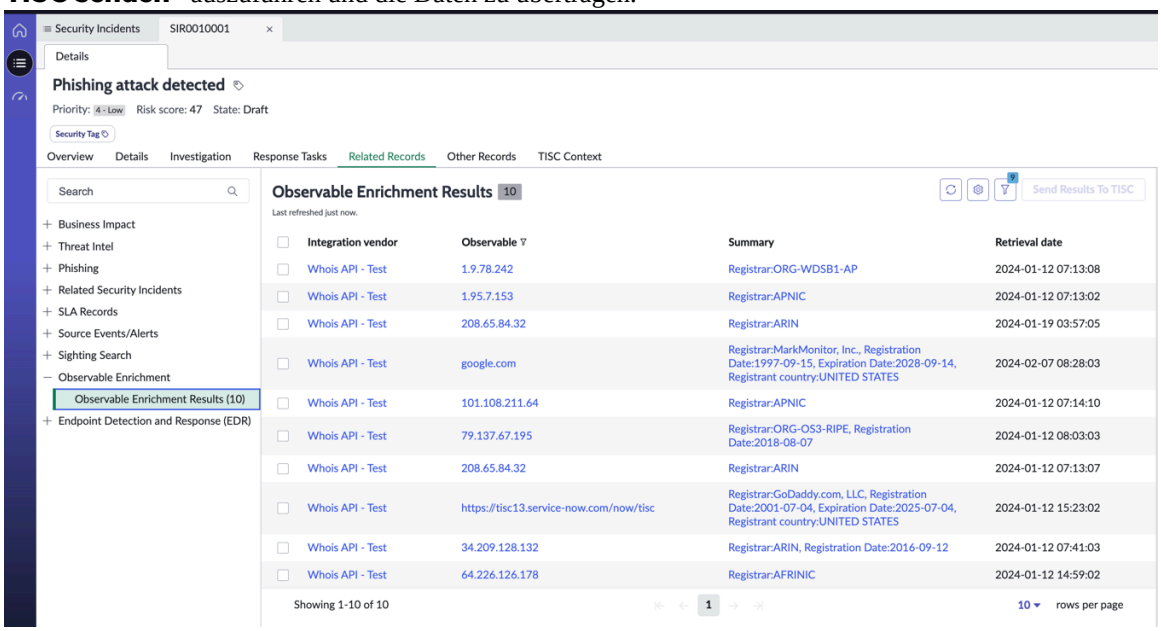
1. Navigieren Sie im SIR-Arbeitsbereich zur Registerkarte **Zugehörige Datensätze,** um die Aktion für die TISC-Integrationsfunktion auszuführen.

   Hinweis:

   - Sie können auch zur Registerkarte **Ermittlung** und dann zum Abschnitt **Einstiegspunktlisten** navigieren, der auf der linken Seite angezeigt wird, und **Zugehörige erkennbare Elemente** auswählen, um den Veröffentlichungsvorgang auszuführen.
   - Klicken Sie auf der Registerkarte **Ermittlungauf Zugehörige Informationen anzeigen**, um alle zugehörigen Daten für die Bedrohungssuche, die Sichtungssuche und die Ergänzungsdaten für das ausgewählte erkennbare Element anzuzeigen. Weitere Informationen finden Sie unter Untersuchungs-Canvas erkunden.

2. Auswahlvorgang **Ergänzung erkennbarer Elemente** > **Erkennbare Elemente – Datenanreicherungs-Ergebnisse** um den Veröffentlichungsvorgang auszuführen und die Daten manuell in TISC zu übertragen.

3. Wählen Sie einen oder mehrere Datensätze erkennbarer Elemente aus, um den Vorgang **„Ergebnisse an TISC senden“** auszuführen und die Daten zu übertragen.



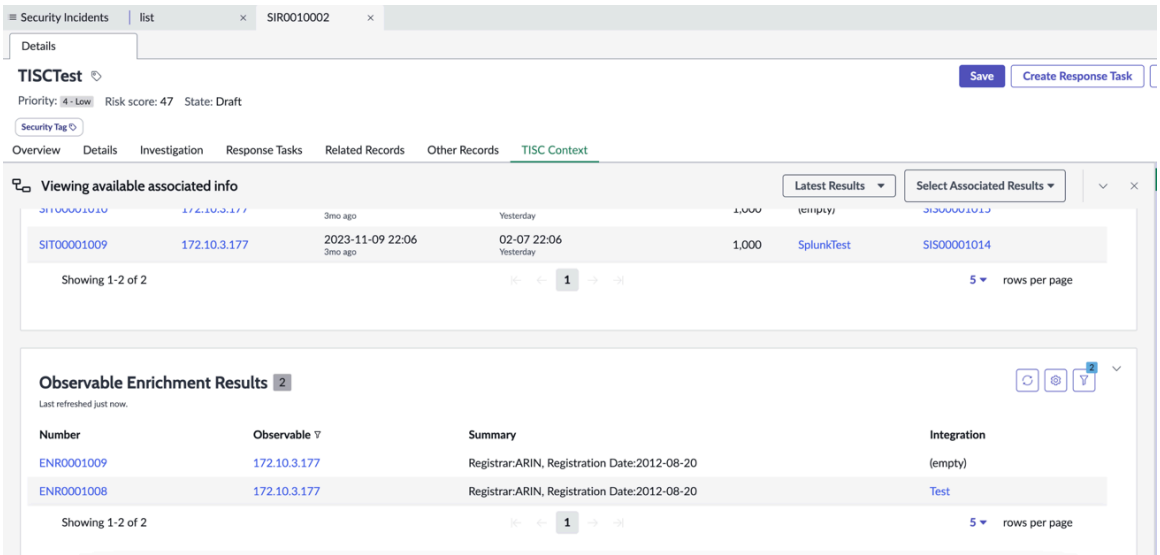
4. Klicken Sie auf **Ergebnisse an TISC senden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn das ausgewählte erkennbare Element nicht in TISC vorhanden ist, wird es zuerst als erkennbare Quelle erstellt. Sobald das erkennbare Quellelement einen TISC-Datensatz für erkennbare Elemente erstellt, wird der erkennbare Datensatz automatisch dem neu erstellten erkennbaren Element zugeordnet.
- Sobald der Push-Vorgang für erkennbare Elemente ausgeführt wurde, wird eine Informationsmeldung angezeigt, dass Observable 0.0.0.0 erfolgreich an TISC übertragen wurde. Es kann einige Zeit dauern, bis die Konvertierung in der TISC-Kontextregisterkarteenthalten ist.

5. Wählen Sie **TISC-Kontext**aus.



Hinweis:

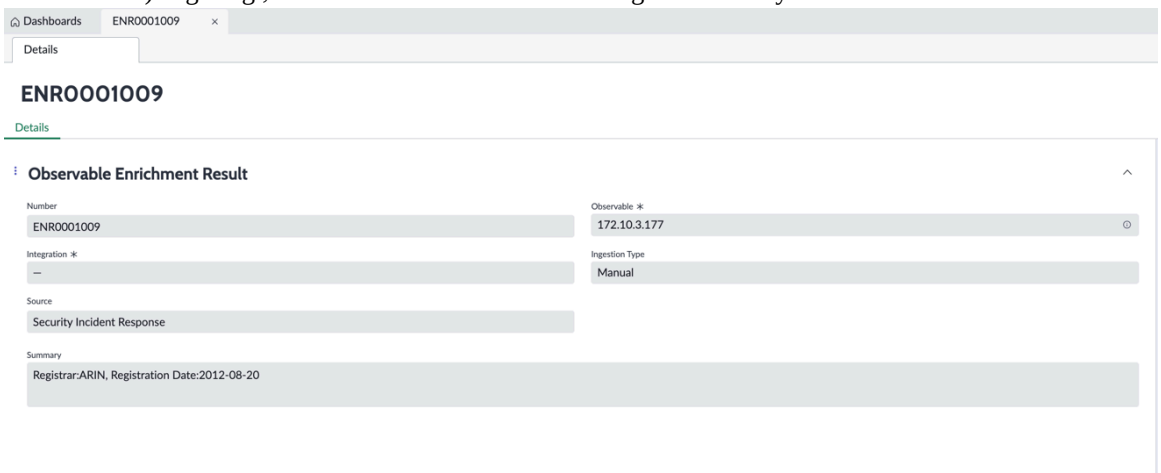
:

- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.
- **Bei einem manuellen Veröffentlichungsvorgang**: Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element aus SIR übertragen wurde, können diese Daten mithilfe von Quellen identifiziert werden, die einen Verweis auf den mit dem erkennbaren Element verknüpften Security Incident enthalten.
- **Bei einem automatischen Push-Vorgang**: Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.
- **TISC-Kontext** zeigt alle dem SIR zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Über den TISC-Kontext können SIR-Analysten alle TISC-Ergänzungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuchen und Daten der Ergänzung erkennbarer Elemente.
- **„Zugeordnete Informationen anzeigen"** zeigt alle zugeordneten Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

6. Zeigen Sie die Ergebnisse an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf einen beliebigen Datenanreicherungs-Ergebnisdatensatz für erkennbare Elemente, um den Datensatz in der Formularansicht anzuzeigen. Dort wird auch der Push- oder **Erfassungstyp** (automatisch oder manuell) angezeigt, und **die Quelle** ist Threat Intelligence Security Center.



Arbeiten mit dem TISC-Kontext

Der TISC-Kontext erleichtert das Anzeigen von Threat Intelligence-Daten wie erkennbaren Elementen im Arbeitsbereich für Security Incident Response.

Dies hilft Sicherheitsanalysten, Security Incidents effektiver zu erkennen, zu untersuchen und darauf zu reagieren.

Der TISC-Kontext im Arbeitsbereich für Security Incident Response ermöglicht es Sicherheitsanalysten, Security Incidents oder erkennbare Elemente zu TISC-Fällen direkt aus dem Arbeitsbereich hinzuzufügen sowie die Ergänzungsergebnisse und Informationen zu erkennbaren Elementen anzuzeigen, bei denen es sich um zugehörige Bedrohungsakteure, Angriffsmuster, Kampagnen usw.

Mit diesem Abschnitt können Sie:

1. Ordnen Sie einem TISC-Fall erkennbare Elemente zu.
2. Zeigen Sie Informationen zu zugehörigen erkennbaren Elementen an.
3. Zeigen Sie die Ergebnisse der Ergänzung erkennbarer Elemente an.

Ausführlichere Informationen und Vorgehensweisen finden Sie in den folgenden Abschnitten. Weitere Informationen zur Funktionsweise der Integration zwischen TISC- und SIR-Arbeitsbereichen finden Sie unter TISC-Integration mit SIR Workspace in Threat Intelligence-Sicherheitszentrum.

Fügen Sie dem TISC-Fall erkennbare Elemente hinzu

Verwenden Sie diesen Abschnitt, um einem TISC-Fall Security Incidents oder erkennbare Elemente hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

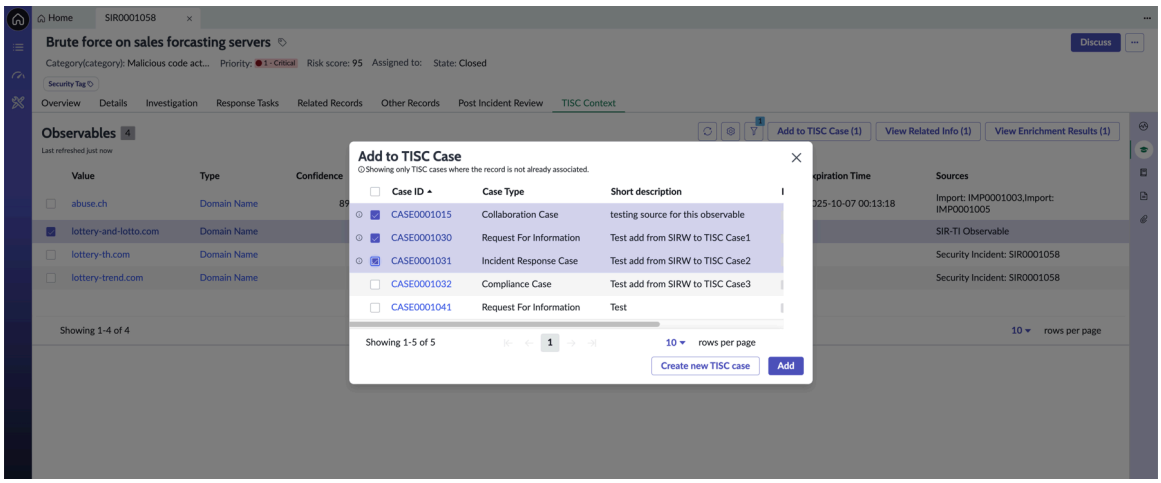
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**.
2. Suchen und öffnen Sie einen bestimmten Security Incident, den Sie untersuchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können dazu auch nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ filtern oder einen Incident-Status durchsuchen.

3. Wählen Sie die Registerkarte **TISC-Kontext**.
4. Klicken Sie auf die Schaltfläche **Zu TISC-Fall hinzufügen**.
   Das Dialogfeld „Zu TISC-Fall hinzufügen“ wird angezeigt, das nur die TISC-Fälle zeigt, bei denen der Datensatz noch nicht zugeordnet ist.
5. Wählen Sie die erkennbaren Elemente aus.
6. Wählen Sie einen oder mehrere Fälle aus, und klicken Sie auf **Hinzufügen**, um die Fälle den erkennbaren Elementen hinzuzufügen und sie dem Security Incident zuzuordnen.



Hinweis:
Sie können auch einen neuen Fall erstellen, indem Sie auf **Neuen TISC-Fall erstellen**klicken, wenn Sie noch keine Fälle haben.

Die folgenden Bestätigungsmeldungen werden angezeigt:

- Die folgenden erkennbaren Elemente wurden erfolgreich als Artefakte hinzugefügt.
- Die folgenden erkennbaren Elemente werden an TISC gesendet und anschließend den ausgewählten TISC-Falldatensätzen hinzugefügt.

Hinweis:
Die Verarbeitung und Zuordnung der Aktivitäten erkennbarer Elemente werden im Aktivitätenstrom veröffentlicht, sobald die Zuordnung abgeschlossen ist.

7. Zeigen Sie die zugehörigen Falldatensätze an, indem Sie sich für weitere Schritte beim Arbeitsbereich für Threat Intelligence-Sicherheitszentrum anmelden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter TISC-Integration mit SIR Workspace.

Hinweis:

Im Arbeitsbereich für Security Incident Response können Sie auch erkennbare Elemente mit Falldatensätzen über die Registerkarten **Untersuchung** und **Zugehörige Datensätze** verknüpfen.

Hinweis:

Um erkennbare Elemente aus **der Untersuchung**zuzuordnen, führen Sie die folgenden Schritte aus. Um die Zuordnung aus **zugehörigen Datensätzen** zuzuordnen, gehen Sie wie folgt vor Fügen Sie dem TISC-Fall erkennbare Elemente hinzu.Sie können auch zur Registerkarte **Ermittlung** navigieren und zum Abschnitt **Einstiegspunktlisten** navigieren, der links auf der Seite angezeigt wird, und **Zugeordnete erkennbare Elemente** auswählen um dem TISC-Fall erkennbare Elemente hinzuzufügen.

Zeigen Sie zugehörige Informationen aus TISC an

Verwenden Sie diesen Abschnitt, um die zugehörigen Informationen anzuzeigen, z. B. zugehörige Bedrohungsakteure, Angriffsmuster, Kampagnen und Fälle aus dem TISC-Arbeitsbereich in SIR.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**.
2. Suchen und öffnen Sie einen bestimmten Security Incident, den Sie untersuchen.
   Sie können dazu auch nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder nach dem Incident-Status filtern.
3. Navigieren Sie, sobald der Incident geöffnet ist, zur Registerkarte **TISC-Kontext**.
   Zugehörige Informationen anzeigen:

   In den Incident-Details können Sie zugehörige Informationen in mehreren Abschnitten anzeigen.

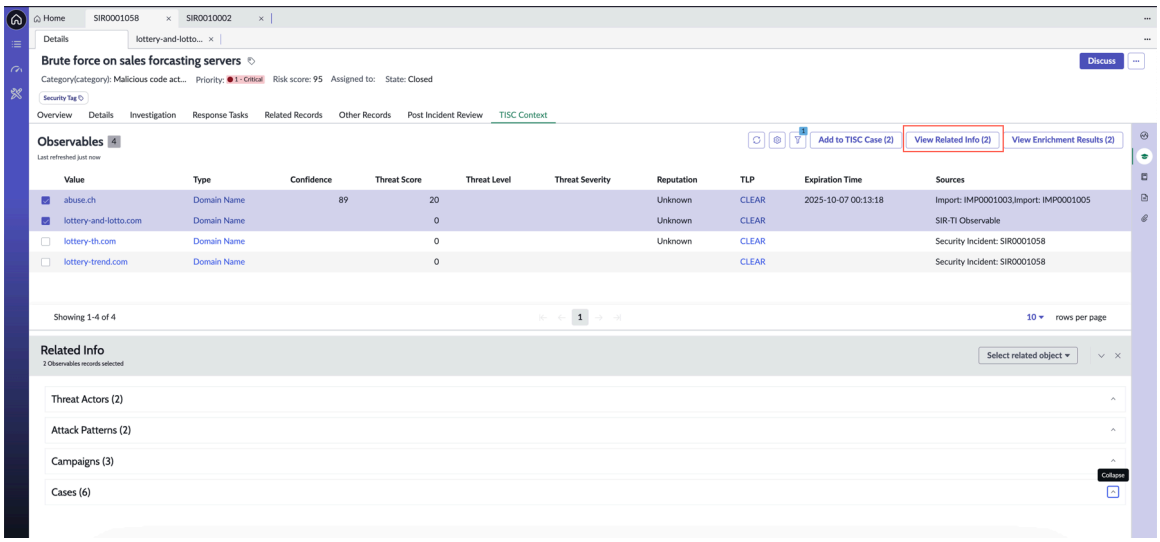
   a. Wählen Sie mindestens ein erkennbares Element aus.

   b. Klicken Sie auf die Schaltfläche **Zugehörige Informationen anzeigen**.
   In diesem Abschnitt werden die zugehörigen Informationen angezeigt, die sich auf die ausgewählten erkennbaren Elemente beziehen.

Name	Beschreibung
Bedrohungsakteure	Zeigt Informationen aus TISC für Bedrohungsakteure im Zusammenhang mit den ausgewählten erkennbaren Elementen an.
Angriffsmuster	Zeigt Informationen aus TISC für Angriffsmuster im Zusammenhang mit den ausgewählten erkennbaren Elementen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Kampagnen	Zeigt Informationen aus TISC für Kampagnen im Zusammenhang mit den ausgewählten erkennbaren Elementen an.
Fälle	Zeigt Informationen aus TISC für TISC-Fälle an, die sich auf die ausgewählten erkennbaren Elemente beziehen.



Datenanreicherungs-Ergebnisse anzeigen

Verwenden Sie diesen Abschnitt, um die Ergebnisse der Ergänzung erkennbarer Elemente anzuzeigen, z. B. Ergebnisse der Bedrohungssuche, Sichtungen und Ergänzungsergebnisse erkennbarer Elemente von TISC im SIR-Arbeitsbereich.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**.
2. Suchen und öffnen Sie einen bestimmten Security Incident, den Sie untersuchen.
   Sie können dazu auch nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder nach dem Incident-Status filtern.
3. Navigieren Sie, sobald der Incident geöffnet ist, zur Registerkarte **TISC-Kontext**.
   Datenanreicherungs-Ergebnisse werden angezeigt:

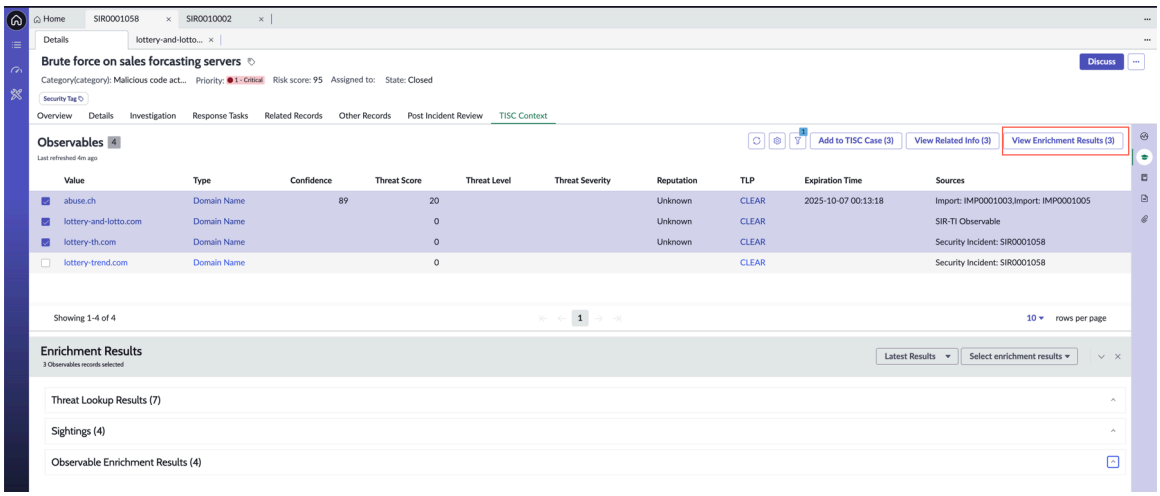
   In den Incident-Details können Sie zugehörige Informationen in mehreren Abschnitten anzeigen.

   a. Wählen Sie mindestens ein erkennbares Element aus.

   b. Klicken Sie auf die Schaltfläche **Datenanreicherungs-Ergebnisse anzeigen**.
   In diesem Abschnitt werden die Details angezeigt, die sich auf die ausgewählten erkennbaren Elemente beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Bedrohungssuche – Ergebnisse	Listet alle zugehörigen Ergebnisse der Bedrohungssuche für ausgewählte erkennbare TISC-Elemente auf.
Sichtungen	Listet alle zugehörigen Sichtungen für ausgewählte erkennbare TISC-Elemente auf.
Erkennbare Elemente – Datenanreicherungs-Ergebnisse	Listet alle zugehörigen Datenanreicherungs-Ergebnisse für erkennbare Elemente für ausgewählte erkennbare TISC-Elemente auf.



Berichte in Security Incident Response

Alle einem -Security Incident zugeordneten Berichte können im Abschnitt „Berichte“ analysiert und geteilt werden.

Der Analyst kann:

- Bericht erstellen
- Bearbeiten Sie einen Bericht
- Berichte löschen

Bericht erstellen

Analysten können in Security Incident Response einen Bericht erstellen, um den Status eines incident aufzunehmen, und ihn per E-Mail freigeben.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie **Reports** (Berichte) aus.

   Auf der Seite **„Bericht“** wird eine Liste aller Berichte angezeigt, die für den ausgewählten Incident erstellt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Neu**.
   Die Seite **„Vorlage auswählen“** wird mit einer Liste aller veröffentlichten Vorlagen angezeigt. Die Liste der Vorlagen ist nur verfügbar, wenn der Administrator Berichtsvorlagen veröffentlicht hat. Weitere Informationen finden Sie unter Erstellen Sie eine Berichtsvorlage in Security Incident Response.
5. Wählen Sie eine Berichtsvorlage aus.
   Der Bericht wird im Bearbeitungsmodus mit den in der Vorlage konfigurierten Incident-Daten geöffnet.
6. Wählen Sie **Erweitern** und fügen Sie die gewünschten Felder ein/entfernen Sie sie.
   - **Allgemeine SIR-Felder**: Liste der am häufigsten verwendeten Felder für einen Incident.
   - **Alle SIR-Felder**: Alle Felder im Zusammenhang mit einem Incident. Wenn Sie beispielsweise einen Incident-Bericht generieren und ein Feld mit der Bezeichnung Kurzbeschreibung hinzufügen möchten, können Sie dieses Feld unter **Alle SIR-Felder**auswählen. Wenn Sie ein Feld hinzufügen, wird die Kurzbeschreibung des incident im Bericht angezeigt.
   - **Zugehörige Datensätze**: Die zugehörigen Datensätze eines bestimmten Incidents. Wenn Sie dem Bericht beispielsweise zugeordnete erkennbare Elemente hinzufügen möchten, können Sie dies Ihrem Bericht hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt
   - **Skripts**: Um das Datum und die Uhrzeit des Berichts hinzuzufügen, können Sie Ihrem Bericht das Skript „Aktuelles Datum/Uhrzeit“ hinzufügen. Dadurch werden das Datum und die Uhrzeit der Berichterstellung im Bericht hinzugefügt.
7. Wählen Sie **Vorschau**, um eine Vorschau des Berichts anzuzeigen.
8. Wählen Sie **Inhalt speichern**, um die Änderungen zu speichern.
9. **Wahlweise:** Wählen Sie das Symbol „Berichtsdetails bearbeiten“, um den Namen und die Beschreibung des Berichts zu aktualisieren.
10. Wählen Sie **Veröffentlichen** aus, um den Bericht zu veröffentlichen.
11. Wählen Sie das Symbol Bericht in E-Mail freigeben aus.
    a. Geben Sie die E-Mail-Adressen des Empfängers in die Felder **An** und **Cc/Bcc** ein.
    b. Aktualisieren Sie den **Betreff und den E-Mail-Text der E-Mail**.
    c. Wählen Sie **Senden** aus, um den Bericht per E-Mail freizugeben.

Bearbeiten Sie einen Bericht

Analysten können einen nicht veröffentlichten Bericht in Security Incident Response ändern und per E-Mail freigeben.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie **Reports** (Berichte) aus.

   Auf der Seite **„Bericht“** wird eine Liste aller Berichte angezeigt, die für den ausgewählten Incident erstellt wurden.
4. Öffnen Sie den zu aktualisierenden Bericht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Bericht wird im Bearbeitungsmodus mit den in der Vorlage konfigurierten Incident-Daten geöffnet.

5. Bearbeiten Sie den Bericht nach Bedarf.
6. Wählen Sie **Vorschau**, um eine Vorschau des Berichts anzuzeigen.
7. Wählen Sie **Inhalt speichern**, um die Änderungen zu speichern.
8. **Wahlweise:** Wählen Sie das Symbol „Berichtsdetails bearbeiten“, um den Namen und die Beschreibung des Berichts zu aktualisieren.
9. Wählen Sie **Veröffentlichen** aus, um den Bericht zu veröffentlichen.
10. Wählen Sie das Symbol .
    a. Geben Sie die E-Mail-Adressen des Empfängers in die Felder **An** und **Cc/Bcc** ein.
    b. Aktualisieren Sie den **Betreff und den E-Mail-Text der E-Mail**.
    c. Wählen Sie **Senden** aus, um den Bericht per E-Mail freizugeben.

Berichte löschen

Sie können einen Bericht in Security Incident Response löschen, der sich im Status „Veröffentlicht“ oder „Entwurf“ befindet.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie **Reports** (Berichte) aus.

   Auf der Seite **„Bericht“** wird eine Liste aller Berichte angezeigt, die für den ausgewählten Incident erstellt wurden.
4. Öffnen Sie den zu löschenden Bericht.
5. Wählen Sie **Löschen**.
   Eine Bestätigungsmeldung wird angezeigt.
6. Wählen Sie **Löschen** aus, um den Bericht zu löschen.

Nutzen Sie eine Telefonkonferenz oder chatten Sie in zusammen Security Incident Response

Sie können mit -Analysten und betroffenen Benutzern zusammenarbeiten, um einen Incident in der Anwendung Security Incident Response zu lösen oder zu besprechen.

Zugehörige Informationen

Starten Sie eine Telefonkonferenz in Security Incident Response

Starten Sie einen Sidebar-Chat in Security Incident Response

Starten Sie eine Telefonkonferenz in Security Incident Response

Mithilfe einer Telefonkonferenz können Sicherheitsanalysten in Echtzeit mit anderen Analysten und betroffenen Benutzern zusammenarbeiten. Diese Anrufe erleichtern den Austausch von Informationen zur Lösung von Incidents.

Vorbereitungen

Stellen Sie sicher, dass Sie die folgenden Apps und Plugins installiert und aktiviert haben:

Automatische Übersetzung

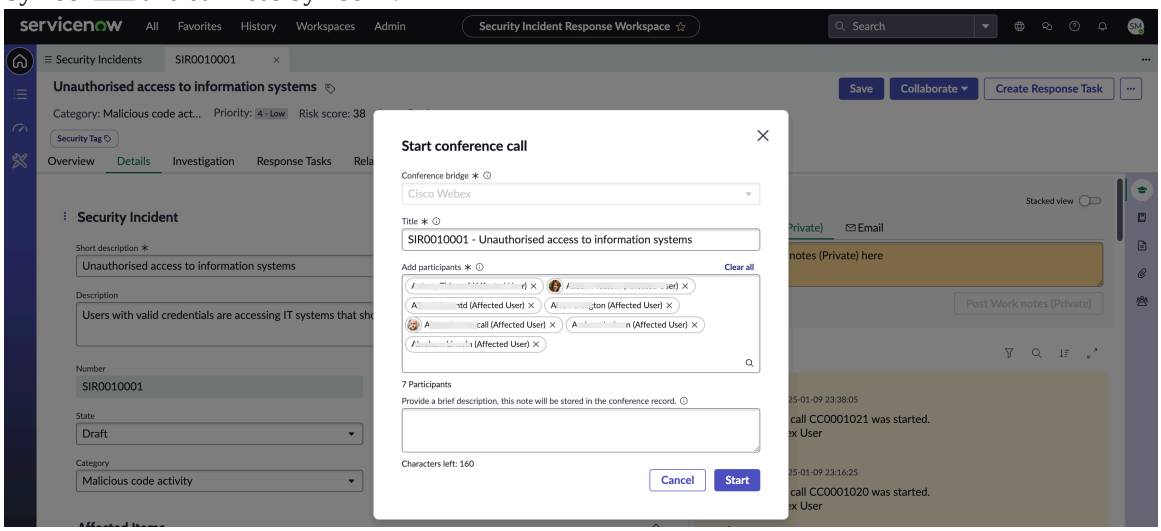
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Notify-Plugin (com.snc.notify).
- Notify-UI-Komponenten für die App „Konfigurierbare Arbeitsbereiche“.
- Visual Task Board (com.devsnc.snb_vtb)

Erforderliche Rolle: sn_si.analyst oder sn_si.manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen Security Incident, für den Sie eine Telefonkonferenz starten möchten.
3. Wählen Sie **Zusammenarbeit**und dann **Anruf beginnen aus**, oder wählen Sie das Telefonkonferenz-Symbol und dann das Symbol +.



Das Popup-Fenster Telefonkonferenz starten wird angezeigt.

4. Wählen Sie eine Konferenzbrücke im Feld **Konferenzbrücke** aus.
5. Geben Sie einen Titel für die Telefonkonferenz unter **Titel**an.

> **Hinweis:**
> Standardmäßig wird der Titel des incident als Titel des Anrufs ausgefüllt. Sie können den Standardtitel ändern.

6. Fügen Sie unter **Teilnehmer hinzufügen**Anrufteilnehmer hinzu, oder entfernen Sie sie.

> **Hinweis:**
> Je nach Konfiguration in den Telefonkonferenzeinstellungen wird eine vorab ausgefüllte Liste von Teilnehmern zu **Teilnehmer** hinzufügen hinzugefügt, oder eine **Empfehlungsliste** von Teilnehmern ist verfügbar. Weitere Informationen finden Sie unter Verwalten Sie Anwender und Gruppen für Telefonkonferenzen.

7. Geben Sie eine kurze Beschreibung für den Start der Telefonkonferenz an.
8. Wählen Sie **Start**.

Die Telefonkonferenz beginnt in der ausgewählten Konferenzbrücke. Alle Teilnehmer erhalten Benachrichtigungen per E-Mail und über die Konferenzbrücke. Die Teilnehmer können über den Link oder die Benachrichtigung an der Konferenz teilnehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Öffnen Sie den zugehörigen Incident in der Anwendung Security Incident Response, um die Details der Telefonkonferenz anzuzeigen.
10. **Wahlweise:** Wählen Sie **Einladung kopieren** aus, um Teilnehmer in einem aktiven Anruf hinzuzufügen.
11. Wählen Sie **Anruf beenden** aus.
    Wenn der letzte Teilnehmer die Telefonkonferenz verlässt, wird der Anruf beendet
12. **Wahlweise:** Um eine Telefonkonferenz neu zu starten, navigieren Sie zum Abschnitt **Abgeschlossen** und wählen Sie die Option **Erneut initiieren** für die gewünschte Telefonkonferenz aus.

Fügen Sie der aktiven Telefonkonferenz Teilnehmer hinzu

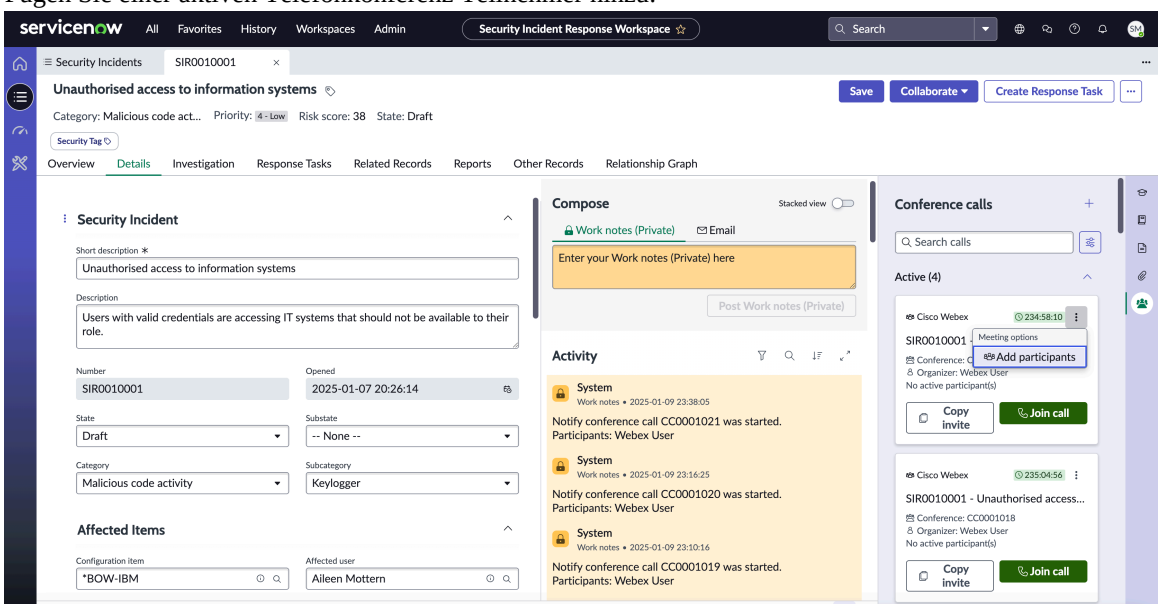
Sie können einer aktiven Telefonkonferenz Teilnehmer hinzufügen, wenn Sie sie vor dem Starten der Telefonkonferenz nicht hinzugefügt haben.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst, sn_si.manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie den Security Incident, für den Sie eine Telefonkonferenz starten möchten.
3. Wählen Sie das Telefonkonferenz-Symbol, um die Details der Telefonkonferenz anzuzeigen.
4. Fügen Sie einer aktiven Telefonkonferenz Teilnehmer hinzu:



   - Wählen Sie das Symbol für Besprechungsoptionen ⋮ für die aktive Telefonkonferenz, und wählen Sie **Teilnehmer hinzufügen**.
   - Wählen Sie im Abschnitt **Telefonkonferenzendie Option Einladung kopieren** aus, und geben Sie die Einladung für die gewünschten Teilnehmer frei.

Starten Sie einen Sidebar-Chat in Security Incident Response

Mithilfe von Sidebar können Sicherheitsanalysten basierend auf einem aufgabenbasierten oder interaktionsbasierten Datensatz des Arbeitsbereichs in Echtzeit mit anderen zusammenarbeiten. Diese Sidebar-Diskussionen erleichtern den Austausch von Informationen und Wissen, um Probleme schneller und mit besseren Ergebnissen zu lösen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.read

Vergewissern Sie sich, dass das Plugin „Omni-Experience – Standard-Funktionssatz“ aktiviert ist. Weitere Informationen finden Sie unter Installing Sidebar .

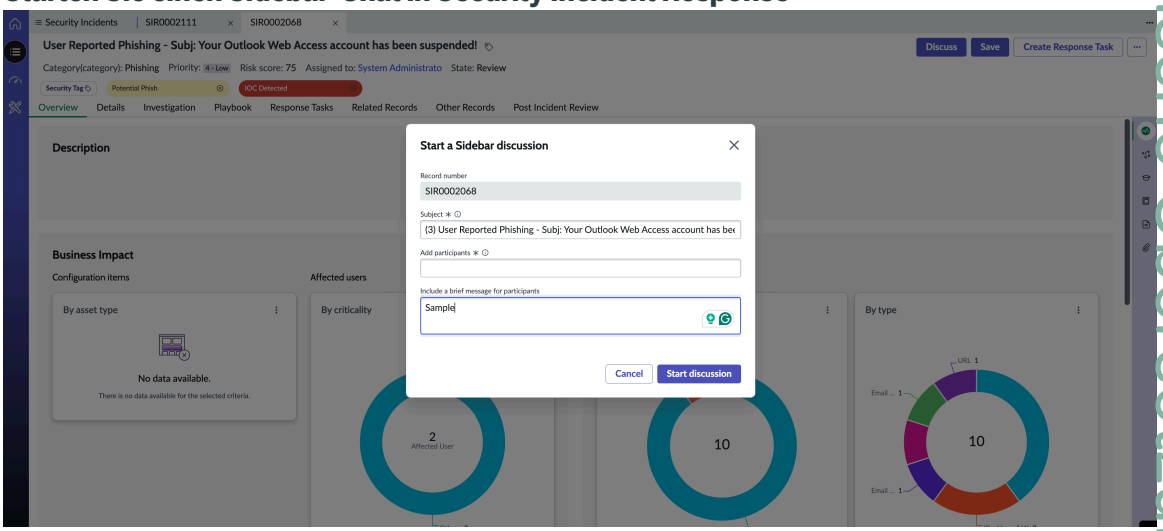
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen Sie das Symbol Listenansicht .
3. Öffnen Sie einen Security Incident, für den Sie eine Sidebar-Diskussion initiieren möchten.
4. Wählen Sie **Zusammenarbeit**und dann **Chat starten**aus.
   Das Dialogfeld Sidebar-Diskussion starten wird angezeigt.

Hinweis:
Durch die Integration von Sidebar in Microsoft Teams können Sidebar-Benutzer und Microsoft Teams-Benutzer über ihre jeweiligen Plattformen miteinander kommunizieren. Weitere Informationen finden Sie unter Sidebar and Microsoft Teams .

5. Füllen Sie im Dialogfeld Start a Sidebar (Sidebar-Diskussion starten) die Felder aus.

Starten Sie einen Sidebar-Chat in Security Incident Response



6. Wählen Sie **Start discussion (Diskussion starten)**.
7. Sie können zusätzliche Konfigurationen wie Schnellaktionen durchführen.
   Um die Verwendung von Aktionen einzuschränken, können Sie das Feld **Auf Gruppe anwenden** auf der Schnellaktionsseite verwenden. Weitere Informationen finden Sie unter Creating a quick action .

Zeigen Sie Incident-Details mit der Beziehung a rgraph an

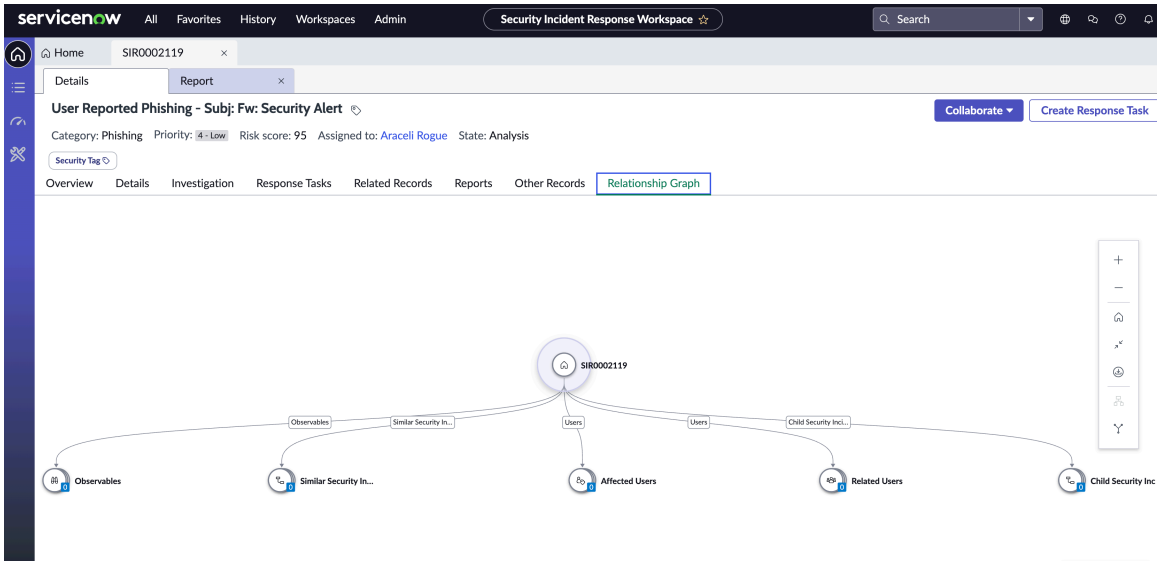
Das Beziehungsdiagramm bietet eine visuelle Darstellung der verbundenen Entitäten für Incidents, um die Analyse und das Verständnis von Security Incidents zu verbessern. Sie ermöglicht es Anwendern, einen vorhandenen Security Incident mit zugehörigen erkennbaren Elementen, Konfigurationselementen, ähnlichen offenen SIRs und anderen Entitäten zu verknüpfen.

Hinweis:
Diese Funktion ist nur im Arbeitsbereich Security Incident Response verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beziehungsdiagramm zeigt Details für einen Incident an.



Kategorieknoten für einen Incident

Sie können Ihrem Beziehungsdiagramm die folgenden Kategorieknoten hinzufügen:

Hinweis:
Das Beziehungsdiagramm ist zustandslos, und Sie können keine Aktualisierungen des Standarddiagramms speichern.

- Erkennbare Elemente
- Betroffene Anwender
- Ähnliche Security Incidents
- Untergeordnete Security Incidents
- Zugehörige Anwender
- Konfigurationselemente
- Zugehörige Configuration Items
- Antwortaufgaben
- Zugeordnete Phishing-E-Mails
- Zugehörige Phishing-Header
- Details der Sichtungssuche
- Bedrohungssuche – Ergebnis

Wenn Sie ein Beziehungsdiagramm für einen Incident öffnen, werden standardmäßig die folgenden Kategorieknoten hinzugefügt:

- Erkennbare Elemente
- Betroffene Anwender
- Ähnliche Security Incidents
- Untergeordnete Security Incidents
- Zugehörige Anwender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können dann wie folgt vorgehen:

- Vergrößern Sie ein beliebiges Objekt, passen Sie es an den Bildschirm an, und ziehen Sie die Knoten.
- Fügen Sie Unterknoten für jeden Knoten hinzu, falls verfügbar, und zeigen Sie Details des Unterknotens an.
- Blenden Sie einen beliebigen Knoten oder Unterknoten aus dem Diagramm aus.
- Zeigen Sie Details eines Unterknotens an.

Erstellen Sie ein Beziehungsdiagramm für den Incident

Sie können in Security Incident Response ein Knotenbeziehungsdiagramm erstellen, um einen vorhandenen Incident besser zu verstehen, indem Sie ihn mit schädlichen erkennbaren Elementen, zugehörigen Konfigurationselementen und anderen korrelieren.

Vorbereitungen

Hinweis:
Das Beziehungsdiagramm ist zustandslos, und Sie können keine Aktualisierungen des Standarddiagramms speichern.

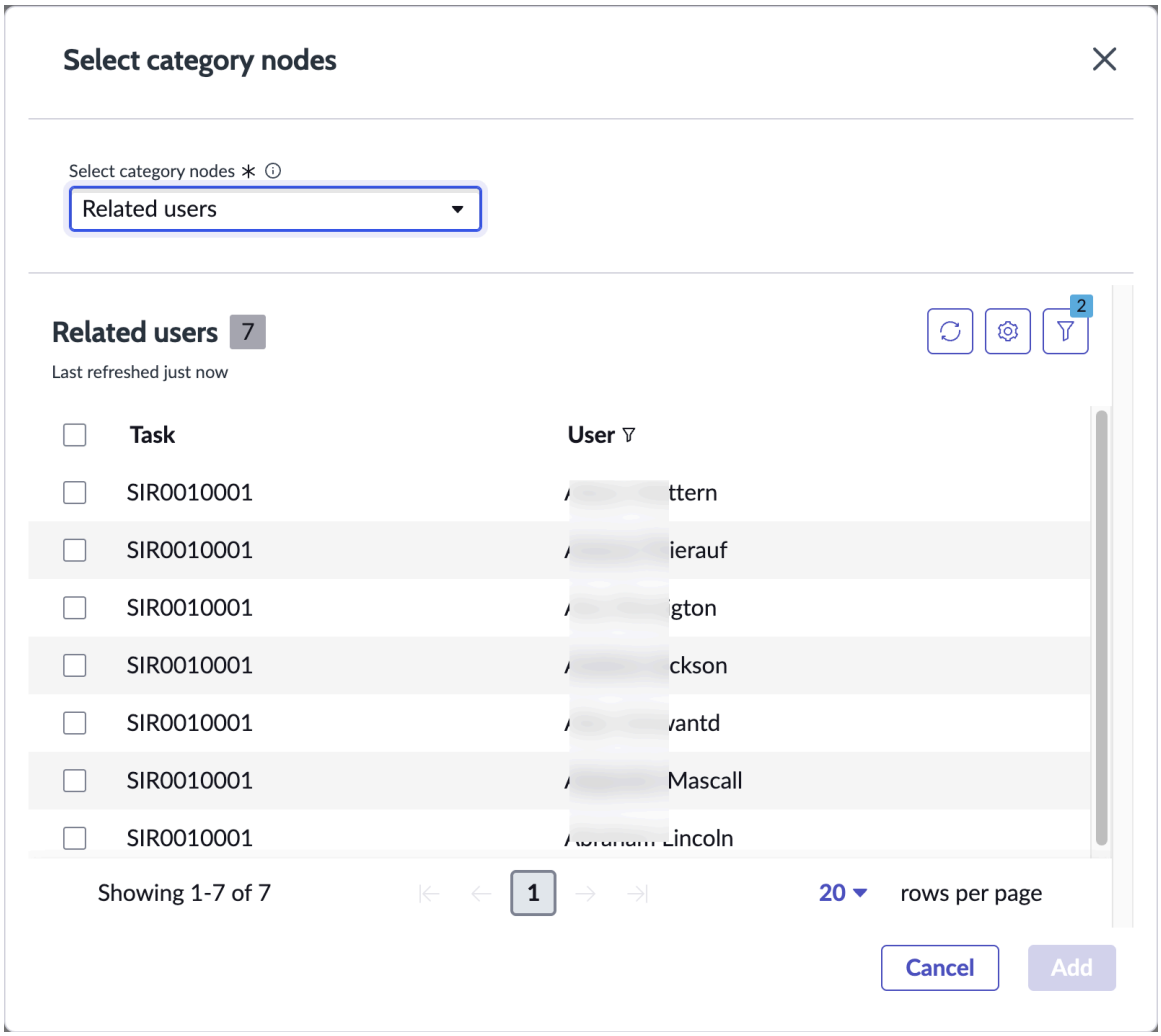
Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie **Beziehungsdiagramm**aus.

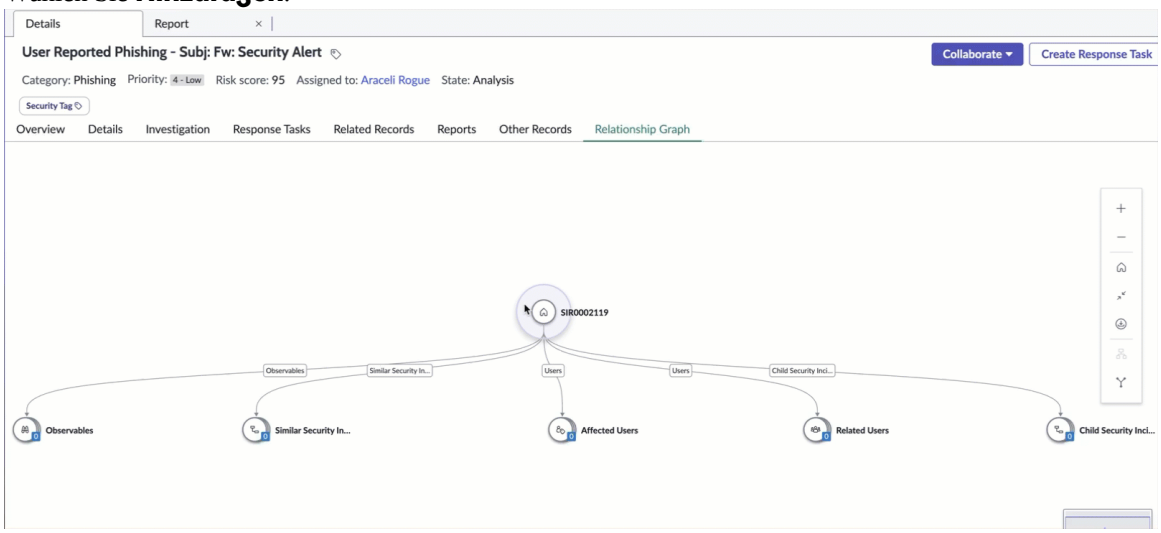
   Das Beziehungsdiagramm für den ausgewählten Incident wird mit dem übergeordneten Knoten und den Standardkategorieknoten geöffnet.
4. Wählen und halten Sie den übergeordneten Knoten (oder klicken Sie mit der rechten Maustaste darauf).
5. Wählen Sie **Linkknoten**aus.
   Die Seite **„Kategorieknoten auswählen“** wird angezeigt.
6. Wählen Sie einen Kategorieknoten aus der Liste **Kategorieknoten auswählen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Eine Liste aller zugehörigen Datensätze für die ausgewählte Kategorie wird angezeigt. Wenn Sie beispielsweise Betroffene Anwender in der Knotenkategorie auswählen, wird eine Liste aller von diesem Incident betroffenen Anwender angezeigt.

7. Wählen Sie die Datensätze aus der Liste aus.
8. Wählen Sie **Hinzufügen**.



Die Kategorie wird als Knoten hinzugefügt, und die zugehörigen Datensätze werden als Unterknoten in der Zuordnung hinzugefügt.

9. Wählen Sie das Export-Zuordnungssymbol um die Zuordnung auf Ihr System herunterzuladen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Der Teil der Zuordnung, der auf dem Bildschirm angezeigt wird, ist in der PDF-Datei verfügbar. Um die vollständige Zuordnung im PDF-Format zu erhalten, wählen Sie vor dem Exportieren der Zuordnung die Option An Bildschirm anpassen aus.

10. Wählen Sie einen Unterknoten und dann **Details anzeigen** aus, um die Details des Unterknotens anzuzeigen.

Security Incident Playbook

Sie können den Playbook-Flow für Security Incidents automatisch oder manuell aufrufen.

Ein Playbook ist nur sichtbar, wenn einem Security Incident mindestens ein Playbook zugeordnet ist. Die Playbook-Komponente funktioniert nur für die von Process Automation Designer (PAD) erstellten Prozesse und nicht für die vom Flow Designer erstellten Flows. Für die vorhandenen Flow Designer-fähigen Flows funktioniert es weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Es gibt zwei Möglichkeiten, das Playbook dem Security Incident zuzuordnen:

- Playbook automatisch aufrufen
- Playbook manuell hinzufügen

Playbook automatisch aufrufen

Damit ein Playbook automatisch aufgerufen wird, muss mit **dem Prozessautomatisierungs-Designer (PAD)**ein Prozess definiert werden. Wenn die Auslösebedingung erfüllt ist, wird automatisch die Playbook-Registerkarte gerendert und die Playbook-Aktivitäten werden angezeigt.

Playbook manuell hinzufügen

Um ein Playbook manuell aufzurufen, navigieren Sie zur Dropdown-Liste Formular-UI-Aktion, und wählen Sie **Playbook hinzufügen**aus. Weitere Informationen finden Sie unter Playbook hinzufügen

Hinweis:
Wenn bereits ein Playbook verfügbar ist, werden die neu hinzugefügten Playbooks parallel zu den vorhandenen Playbooks ausgeführt.

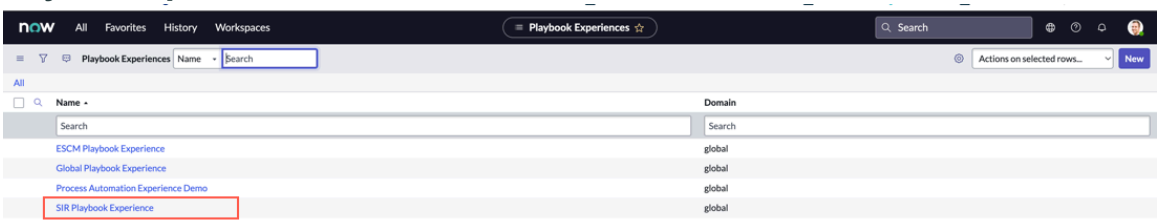
- Im Playbook können Analysten die Playbook-Karten nach Status filtern.
- Der Analyst kann ein Playbook abbrechen, indem er es über das Ellipse-Symbol auswählt.
- In jeder Aktivität kann der Analyst die in den Aktivitätskarten definierten Aktionen ausführen, z. B. Überspringen, „Als abgeschlossen markieren“, „Abbrechen“, oder Orchestration-Aktionen wie „An Sandbox senden“, „E-Mails durchsuchen“ usw.
- Jede dieser Aktionen ist in der Aktivitätsdefinition definiert, und die vollständige sichtbare Karte kann zum Zeitpunkt der Erstellung der Aktivitätsdefinition selbst angepasst werden.

Hinweis:
Alle zukünftigen Aktivitätsdefinitionen und die nächsten auszuführenden Schritte werden mit einem Schlosssymbol angezeigt und befinden sich für den Benutzer im schreibgeschützten Modus. Der Playbook-Anzeigemodus wird durch eine Konfiguration gesteuert, wie unten erläutert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

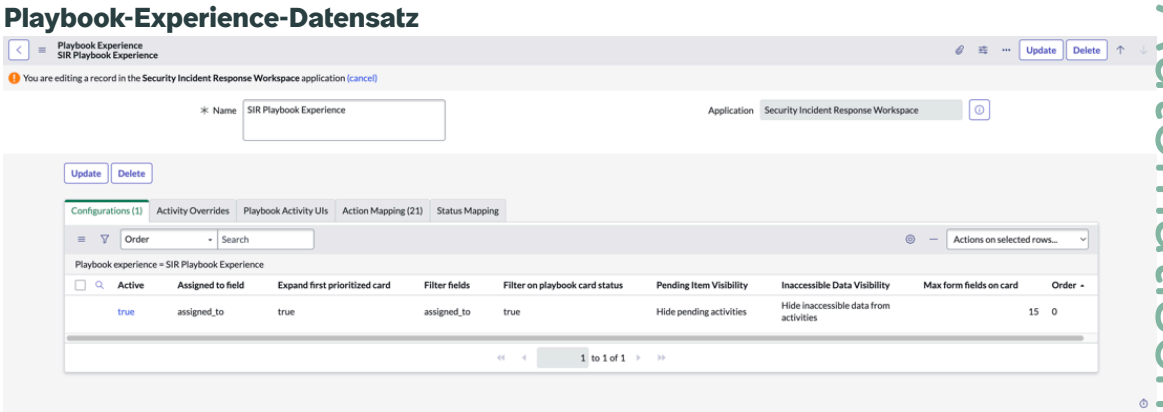
1. Navigieren zu **Alle** > **Playbook-Experiences**.
2. Wählen Sie auf der Seite „Playbook Experiences“ eine **SIR Playbook Experience**aus.

Playbook-Experience

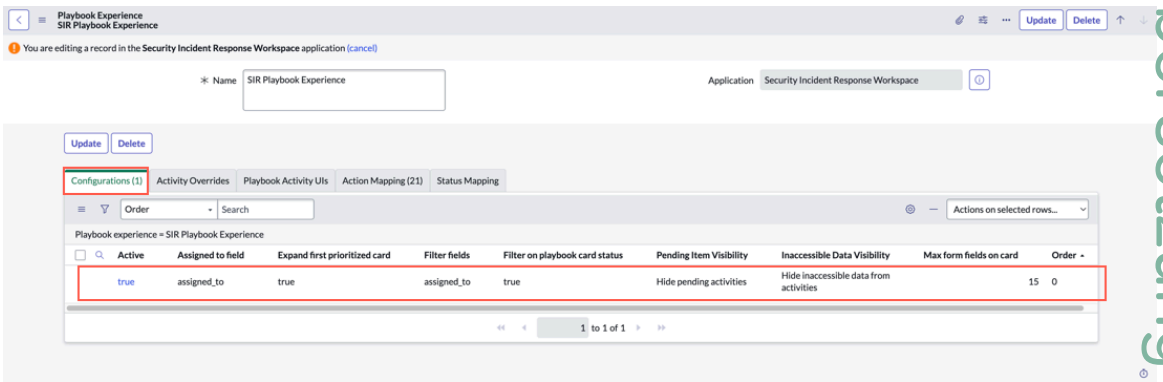


Die Seite **„Playbook Experience SIR Playbook Experience“** wird angezeigt.

Playbook-Experience-Datensatz



3. Klicken Sie auf den **Konfigurationsdatensatz**.

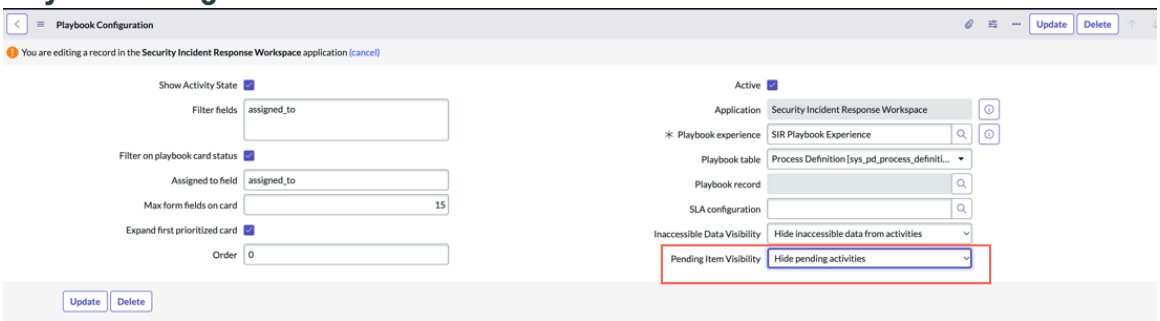


4. Klicken Sie auf der Registerkarte Konfiguration auf Konfiguration SIR Playbook-Experience.

Automatische Übersetzung

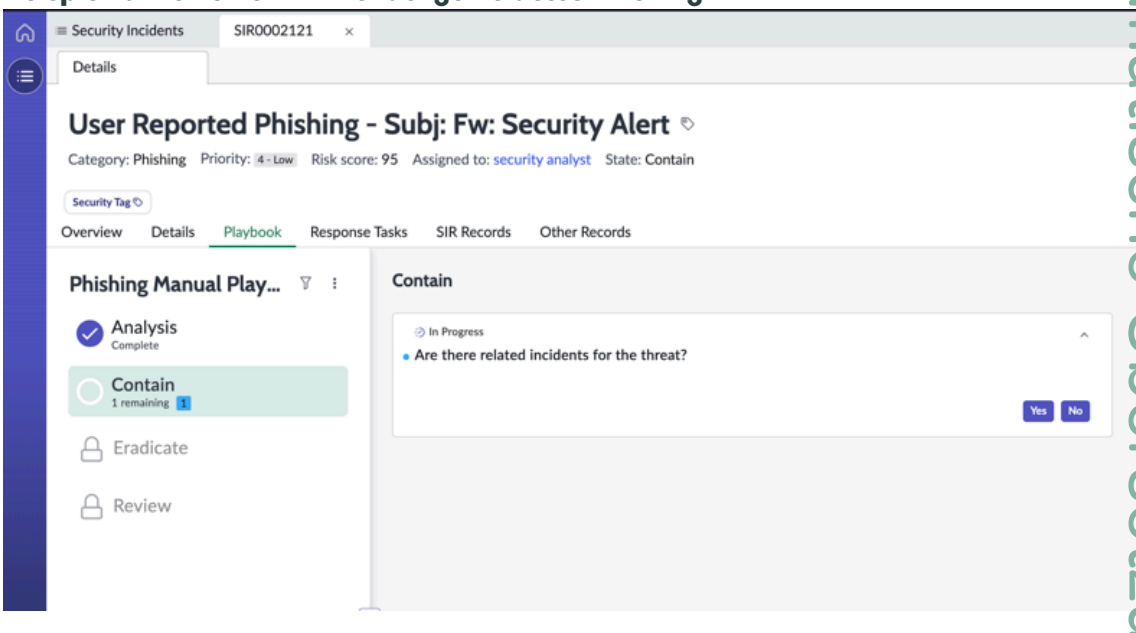
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook-Konfiguration



5. Navigieren Sie zur Dropdown-Liste des Felds **Sichtbarkeit ausstehender Elemente**, wählen Sie die gewünschte Option aus, und speichern Sie den Datensatz. Wählen Sie eine der folgenden Optionen aus:
   - **Ausstehende Aktivitäten ausblenden**: Wählen Sie diese Option aus, um die ausstehenden Aktivitäten auszublenden, die im Playbook-Abschnitt des Arbeitsbereichs angezeigt werden sollen.

Beispiel für von einem Anwender gemeldetes Phishing

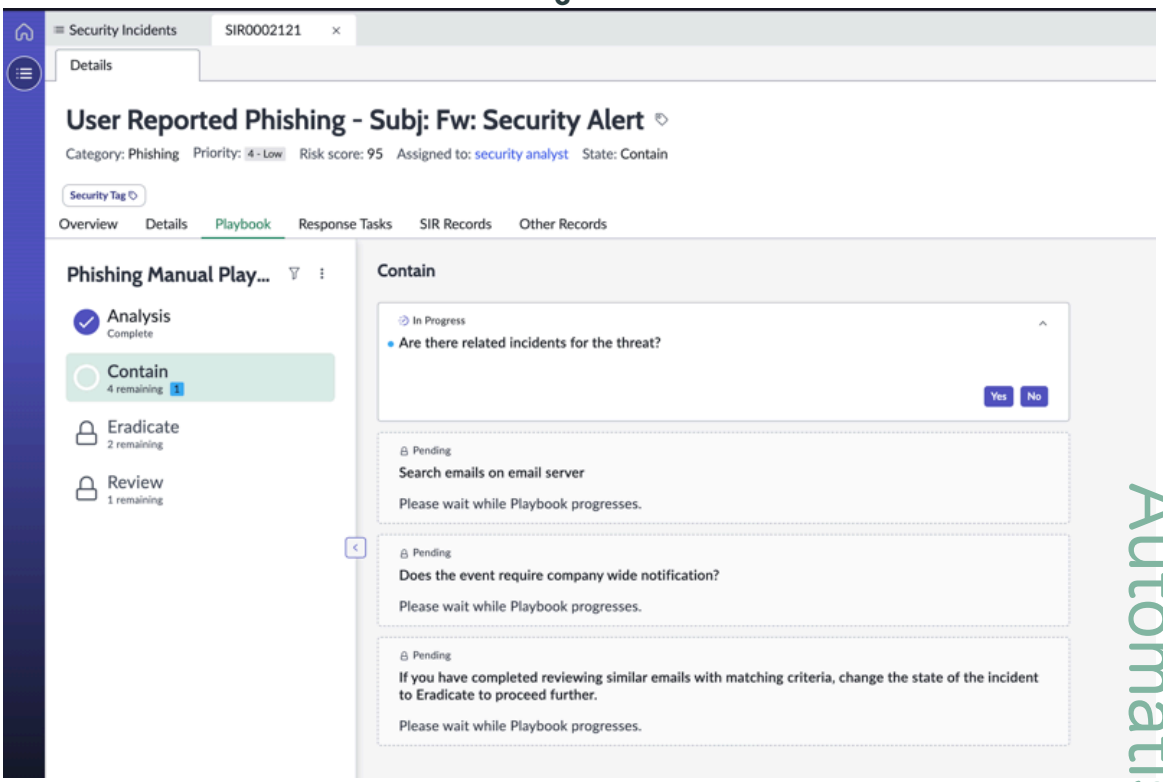


   - **Ausstehende Phasen und Aktivitäten anzeigen**: Wählen Sie diese Option aus, um ausstehende Phasen und Aktivitäten anzuzeigen, die im Playbook-Abschnitt des Arbeitsbereichs angezeigt werden sollen.

Automatische Übersetzung

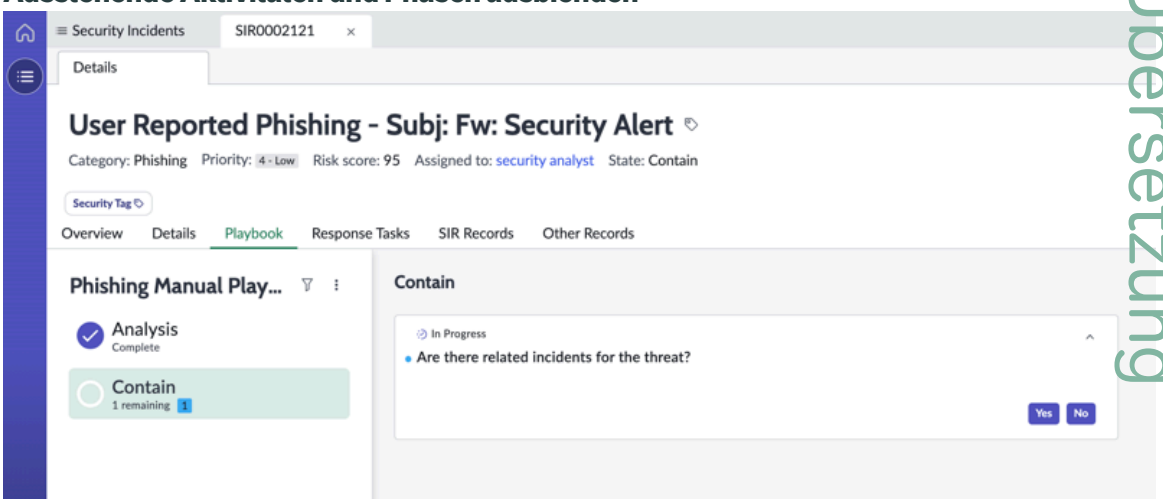
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausstehende Phasen und Aktivitäten anzeigen



- **Ausstehende Aktivitäten und Phasen ausblenden**: Wählen Sie diese Option aus, um ausstehende Aktivitäten und Phasen auszublenden, die im Playbook-Abschnitt des Arbeitsbereichs angezeigt werden sollen.

Ausstehende Aktivitäten und Phasen ausblenden

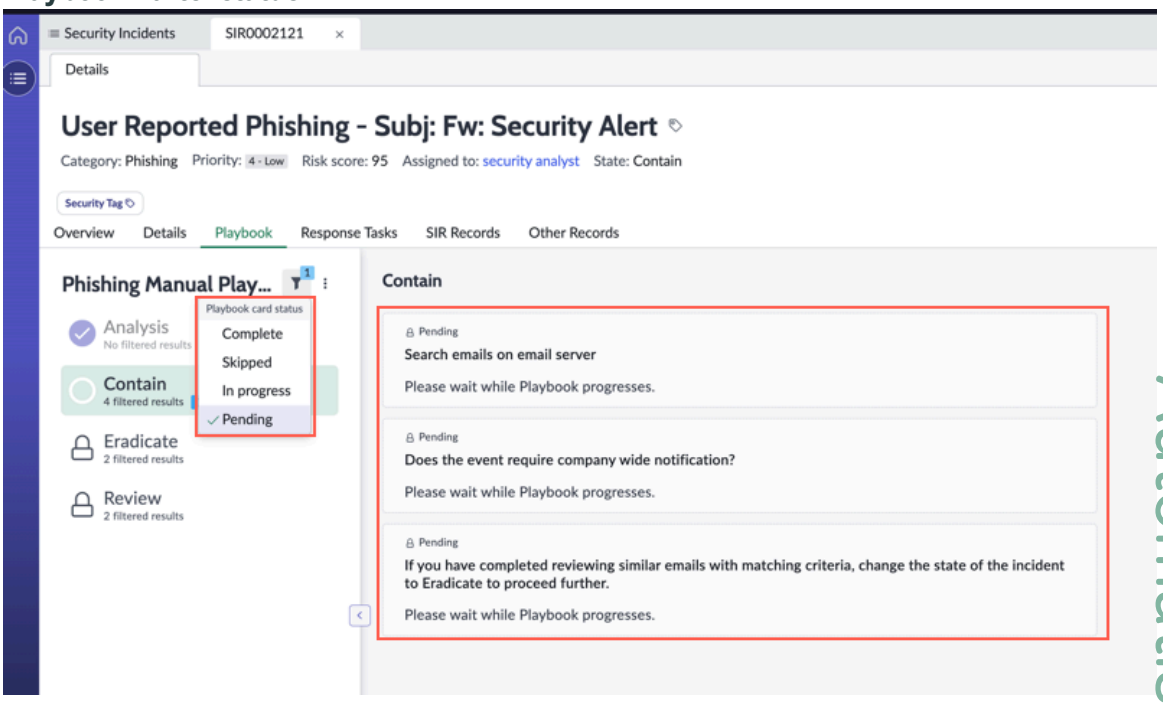


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verwenden Sie im Abschnitt „Playbook“ die Filteroption, um die Aktivitäten nach Playbook-Kartenstatus (Aktivitätsdefinition) zu filtern.

Playbook-Kartenstatus



Playbook hinzufügen

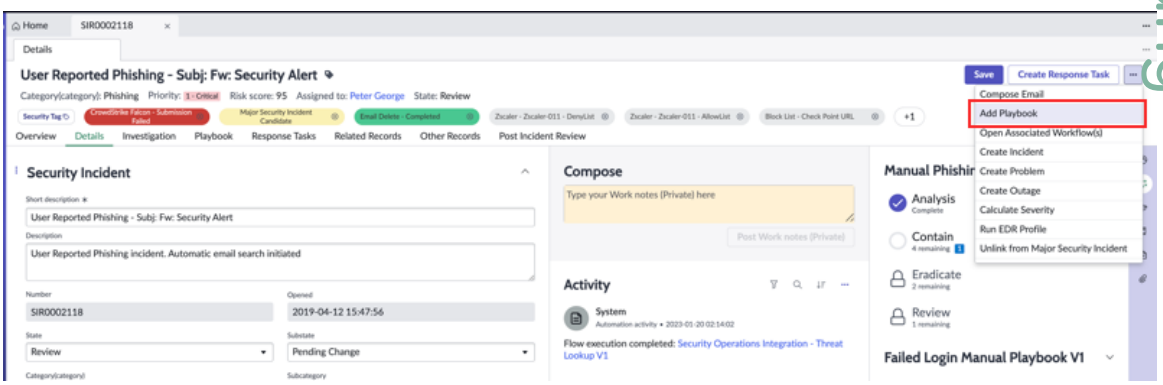
Verwenden Sie diesen Abschnitt, um Playbook manuell hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

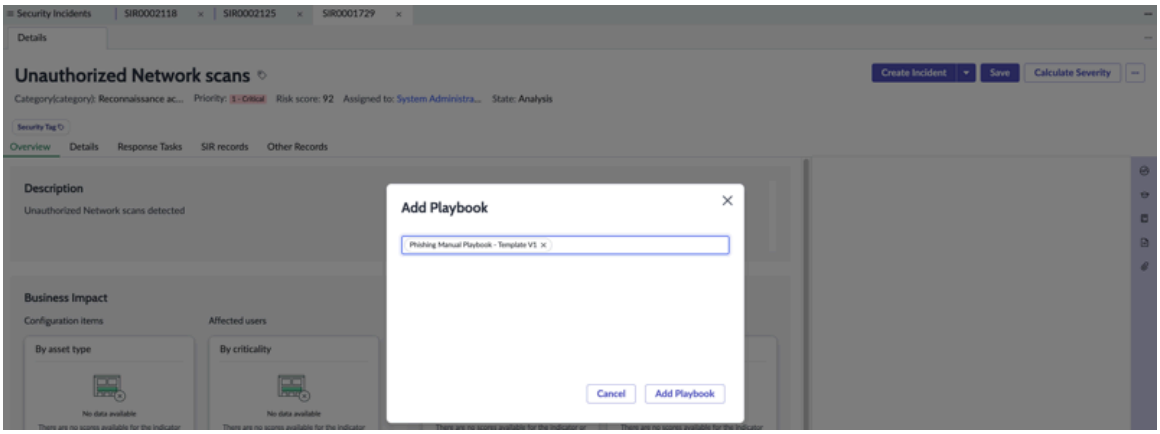
1. Navigieren zu **Alle** > **Security Incident** > **Security Analyst Workspace**.
2. Öffnen Sie einen Incident-Datensatz.
3. Klicken Sie auf **Playbook hinzufügen**.



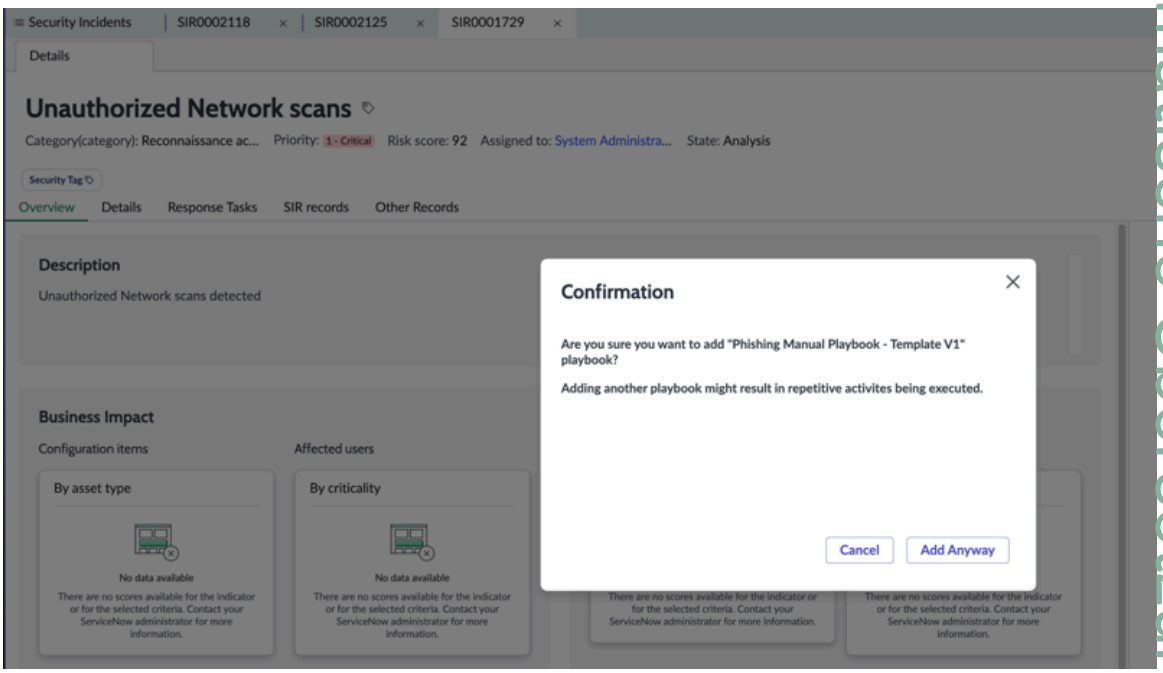
Das Dialogfeld **„Playbook hinzufügen“** wird angezeigt.

Automatische Übersetzung

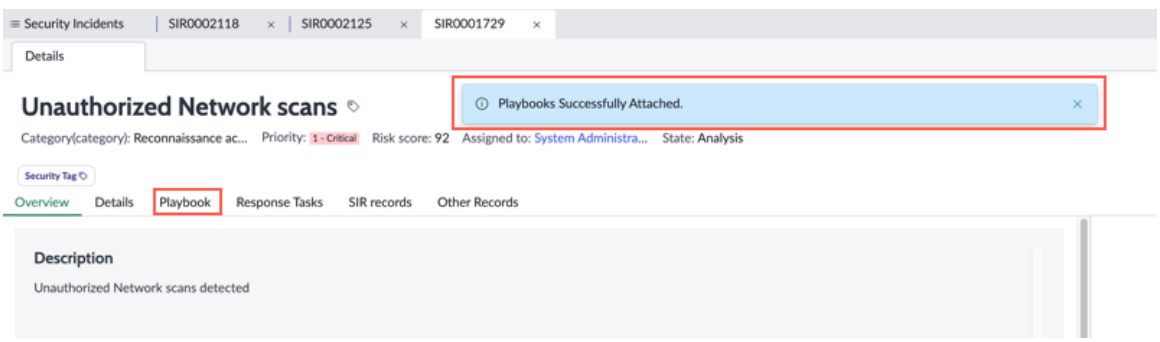
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Playbook-Vorlage aus.
5. Klicken Sie auf **Playbook hinzufügen**.
   Ein Dialogfeld mit einer Bestätigungsmeldung wird angezeigt, in dem Sie bestätigen müssen.
6. Klicken Sie auf **Trotzdem hinzufügen**.



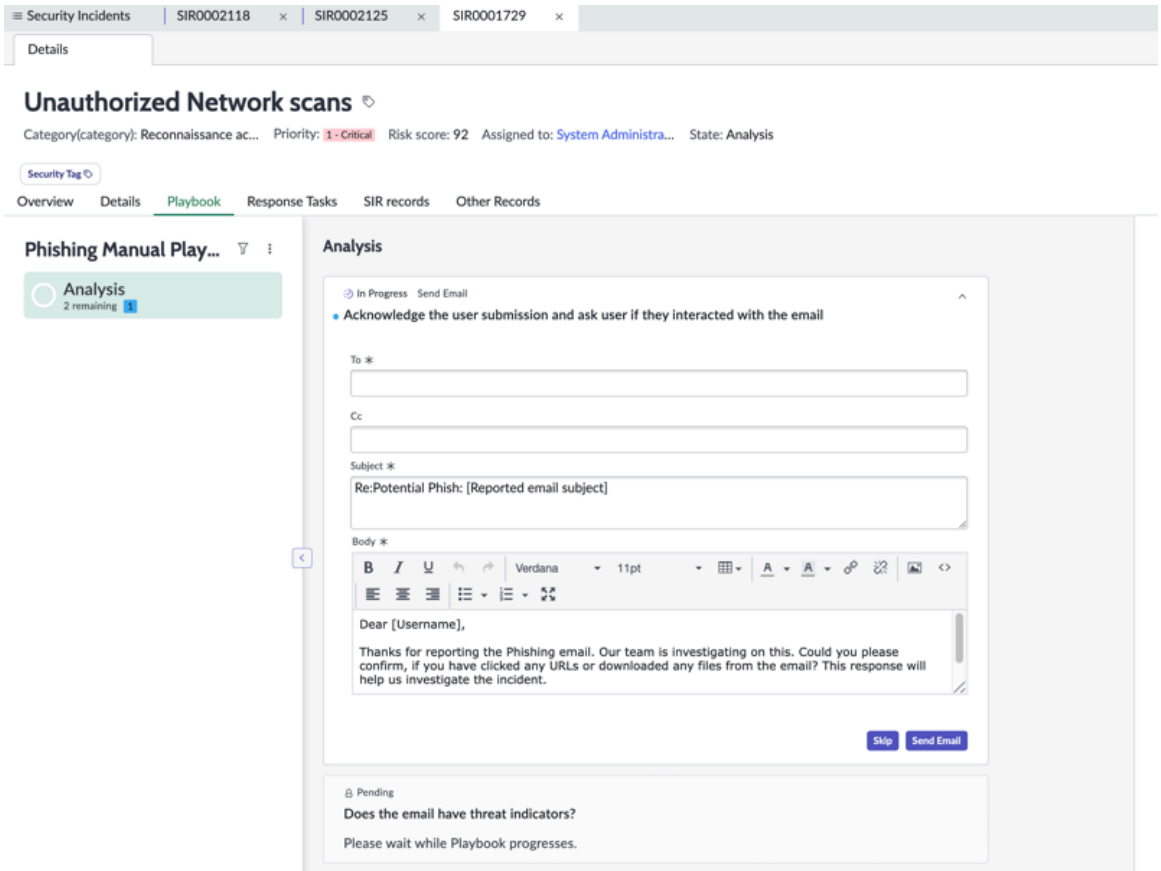
7. Das **Playbook** wird neben der Registerkarte **Details** hinzugefügt.



8. Klicken Sie auf die Registerkarte **Playbook**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Führen Sie die aufgeführten Aktivitäten aus, um zur nächsten Ebene zu wechseln.

Hinweis:
Wenn ein Security Incident einem Playbook zugeordnet ist, kann der Benutzer das Playbook bis zum Schließen oder Abbrechen des zugehörigen Playbooks nicht erneut mit demselben Security Incident verknüpfen.

Voraussetzungen für die Playbooks

Sie benötigen die folgenden Rollen und Plugins, um die Playbooks zu erstellen.

Erforderliche Rolle: admin.

- Aktivieren Sie das Plugin „Prozessautomatisierungs-Designer“ (PAD) [com.glide.pad.license].
- Aktivieren Sie die folgenden Plugins für eine Playbook-Experience:
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Aktivieren Sie die Security Operations-Spoke für den Zugriff auf Flows [com.snc.secops.spoke].
- Enterprise Security Case Management PAD Common.

Stellen Sie sicher, dass Sie die Plattformdokumentation zu Playbook-Experience und Process Automation Designer gelesen haben, bevor Sie mit diesem Leitfaden beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neuerstellung vorhandener Playbooks in Workflow-Studio

Sie können vorhandene Flows nicht direkt in Playbooks in Workflow-Studiokonvertieren. Jeder Flow Designer-Schritt, der eine Antwortaufgabe zur Anleitung des Analysten erstellt, muss in separate Aktionen oder Subflows unterteilt werden.

Sie dürfen vorhandene Flows nicht direkt in Playbooks in Workflow-Studiokonvertieren. Jeder Flow Designer-Schritt, der eine Antwortaufgabe zur Anleitung des Analysten erstellt, muss in separate Aktionen oder Subflows unterteilt werden. Durch die Verwendung dieser granularen Subflows oder Aktionen müssen Sie Aktivitätsdefinitionen erstellen. Nachdem Sie diese Aktivitätsdefinitionen erstellt haben, werden sie als Aktivitäten innerhalb der Phase in der Prozessdefinition hinzugefügt. Sie können Aktivitätsdefinitionen in mehreren Playbooks wiederverwenden.

Sie können jede Aktivität anpassen, um die darin erforderlichen Aktionen darzustellen und zu bestimmen, wie die Karte beim Erstellen der Aktivitätsdefinition aussehen soll. Die Aktivität kann E-Mail-Clients, Tabellen, Aktionen, KB-Artikel, URLs usw. anzeigen. Sie können definieren, wie die Aktivitätsdefinition und die zugrunde liegende Aktion oder die Subflows erstellt werden.

Weitere Informationen finden Sie in den folgenden Abschnitten.

- Aktivitätsdefinitionen
- Process Automation Designer

Aktivitätsdefinitionen

Now Platform stellt einige Aktivitätsdefinitionen innerhalb des Basissystems bereit. Darüber hinaus sind für die Playbooks, die das SIR Workspace-Basissystem verwenden, einige Aktivitätsdefinitionen im Basissystem unter der Anwendung „Enterprise Security Case Management PAD Common“ definiert.

Erforderliche Rolle: sn_si.admin.

Hier ist die Liste der Aktivitätsdefinitionen, die Teil des Basissystems sind:

Aktivitätsdefinition	Tabelle	Beschreibung	Anwendung
Warten-auf-Bedingung ohne Experience	Global [global]	Auf Bedingung warten ohne Experience	Enterprise Security Case Management PAD Common
An CSF X Sandbox übermitteln	Security Incident [sn_si_incident]	An die Sandbox übermitteln	Enterprise Security Case Management PAD Common
E-Mail senden	Security Incident [sn_si_incident]	Aktivität „E-Mail senden“ für SIR-Playbooks.	Enterprise Security Case Management PAD Common
E-Mail durchsuchen	Security Incident [sn_si_incident]	Durchsuchen Sie E-Mails auf dem E-Mail-Server	Enterprise Security Case Management PAD Common
Aufgabenstatus aktualisieren	Security Incident [sn_si_incident]	Aktualisiert den Aufgabenstatus	Enterprise Security Case Management PAD Common

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivitätsdefinition	Tabelle	Beschreibung	Anwendung
E-Mail löschen	Security Incident [sn_si_incident]	Löschen Sie E-Mails	Enterprise Security Case Management PAD Common
Ja/Nein-Ergebnis	Aufgabe [task]	Erwartetes Ergebnis	Enterprise Security Case Management PAD Common

Beispiel für eine Aktivitätsdefinition: E-Mail senden

Im Folgenden finden Sie ein Beispiel für die Definition der Aktivität „E-Mail senden“.

Standard

Die grundlegenden Details umfassen den Name (Bezeichnung), die Anwendung, die Beschreibung, die Tabelle und alle Anwendungen, von denen aus darauf zugegriffen werden kann.

Fügen Sie den Automatisierungsplan und die Aktivitäts-Experience hinzu, und übermitteln Sie sie. Bearbeiten Sie das Dokument nach dem Senden, um weitere Details für jede Registerkarte hinzuzufügen.

Automatisierungsplan

Der Automatisierungsplan ordnet die Back-End-Aktion oder die mit dem Flow Designer erstellten Subflows zu. In diesem Beispiel wird der Subflow **„E-Mail senden - ESCM-Aktivität“** verwendet.

Dieser Subflow ermöglicht das Senden einer E-Mail. Verfügt über die Kernlogik zum Senden einer E-Mail. Es sind alle Eingabe- und Ausgabefelder definiert.

Alle Eingabefelder werden im Abschnitt „Automatisierungsplan“ angezeigt. Jedes Eingabefeld kann so aktiviert werden, dass es nur für den Administrator im Standard-Modal, im Standard-Modal und im Konfigurationsbereich sichtbar ist:

- **Nur Administratorsichtbarkeit**: Wenn dies auf „Administrator“ festgelegt ist, kann nur der Administrator sie anzeigen.
- **In Standardmodell einbeziehen**: Wenn dies auf die Ansicht im Standardmodal festgelegt ist, wird es nur im Eigenschaftendialogfeld angezeigt.
- **In Standardmodell und Konfigurationsbereich einbeziehen**: Wenn dies auf die Ansicht im Standardmodal und im Konfigurationsbereich festgelegt ist, wird es im PAD-Konfigurationsbereich sowie im Eigenschaftendialogfeld angezeigt. Weitere Informationen finden Sie unter Aktivitätsdefinitionen

Sie können die Eingabefelder zum Zeitpunkt der Aktivitätsdefinition selbst definieren, sofern Sie diese Werte nicht zum Zeitpunkt der Konfiguration ändern müssen. Dies hilft dem Geschäftsprozessverantwortlichen, bei der Konfiguration einer Aktivität innerhalb eines Prozesses Zeit zu sparen.

Aktivitäts-Experience

Die Registerkarte „Aktivitäts-Experience“ definiert, wie die Aktivitätskarte zur Laufzeit gerendert wird. Das Basissystem bietet die folgenden Experience-Typen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Genehmigung
- Katalogelement
- Datensatz erstellen
- Instruktion
- Wissen
- Liste
- Benachrichtigung
- Datensatz

Basierend auf der Art der Experience, die Sie auswählen, werden die weiteren Felder ausgefüllt. Weitere Informationen finden Sie in der Now Platform-Dokumentation.

In diesem Beispiel ist **Datensatztyp** ausgewählt.

Hinweis:
Wenn Sie beispielsweise eine Tabelle rendern möchten, können Sie „Liste“ als Experience-Typ auswählen.

Zugeordneter Datensatz

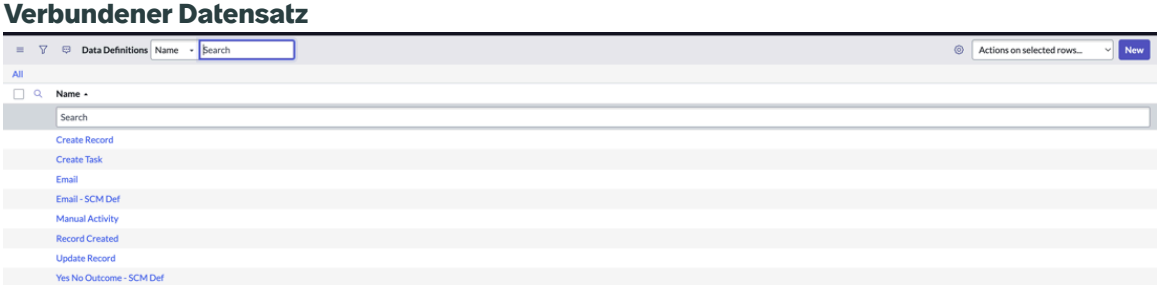
Verwenden Sie diesen Datensatz, um die zugehörigen Daten zur aktuellen Aktivität zu speichern. Dies würde die Laufzeitdaten sowie den Status der Experience erfassen.

- Zugeordnete Tabelle: Flow-Daten
- Zugeordneter Datensatz: VL
- Tabelle für den Experience-Status: Flow-Daten
- Experience-Statusdatensatz: VL

In diesem Beispiel wird die Flow-Datentabelle zum Erfassen der Laufzeitdaten verwendet. Die Laufzeitdaten können je nach Anwendungsfall variieren. In diesem Beispiel handelt es sich bei den Laufzeitdaten um Felder wie „An“, „CC“, „Betreff“ und „Text“. Für jeden Anwendungsfall muss eine Flowdatendefinition erstellt werden, um den Typ der Laufzeitdaten zu definieren.

1. Navigieren Sie zum linken Bereich, und geben Sie **sys_flow_data_definition.list**ein. Zeigt die Liste der Definitionen an, die für die Flow-Datentabelle erstellt wurden.

Verbundener Datensatz

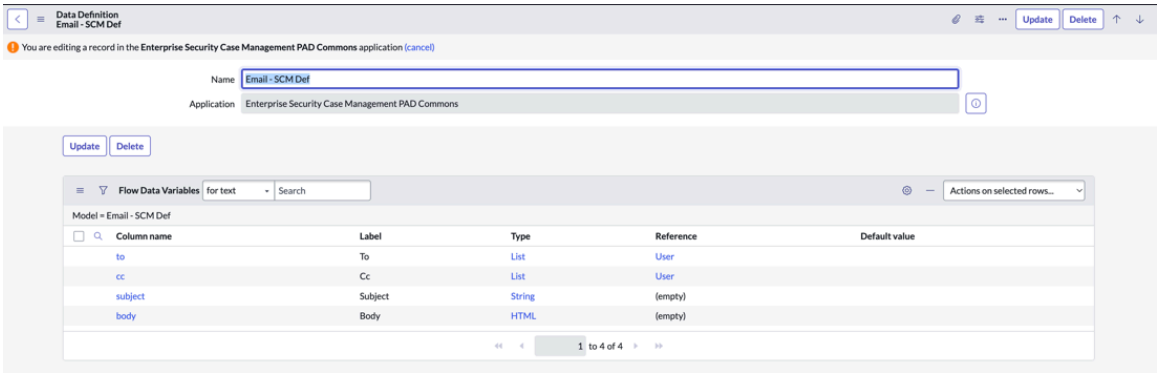


2. Öffnen Sie **E-Mail – SCM-Definition,** um die Definition im Zusammenhang mit diesem Beispiel anzuzeigen.

Automatische Übersetzung

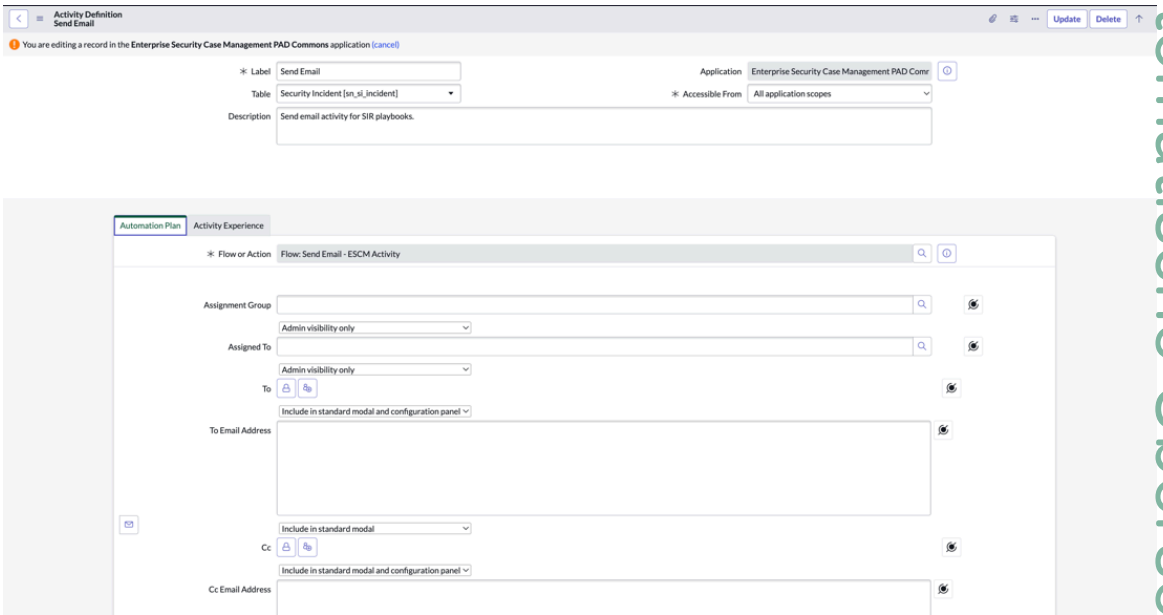
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail – SCM-Definition



Diese Flowdatendefinition muss vom Subflow oder der Aktion verwendet werden, die dieser Aktivitätsdefinition zugeordnet ist (Automatisierungsplan verweisen), um die Laufzeitdaten zu erfassen.

Aktivitätsdefinitionen

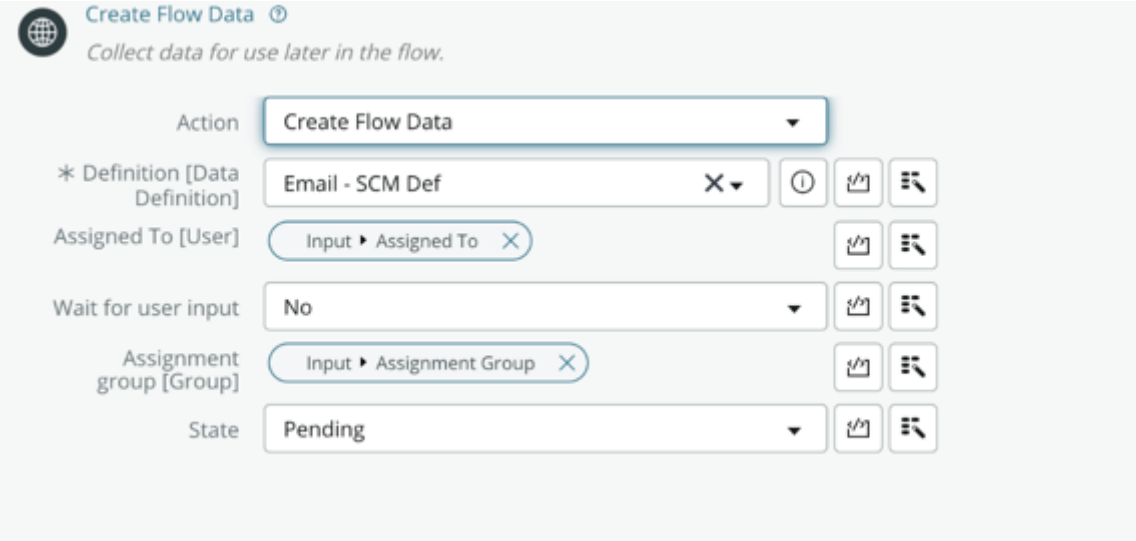


3. Öffnen Sie in diesem Beispiel den folgenden Subflow: **Send Email - ESCM Activity (E-Mail senden - ESCM-Aktivität)**. Unter dem Schritt **Flow-Daten erstellen** wird die von Ihnen erstellte Flow-Datendefinition dem Feld **Definition** zugeordnet. Dieser Flow-Datensatz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird im gesamten Subflow verwendet. In diesem Beispiel wird der Aktivitätskartenstatus (Experience-Status) in der Flow-Datentabelle erfasst.

E-Mail senden: ESCM-Aktivität



Hinweis:

Wenn Sie die Laufzeitdaten in einem anderen Tabellendatensatz als der Flow-Datentabelle erfassen möchten, z. B. in einer Antwortaufgabe. Sie können die zugeordnete Tabelle als Antwortaufgabentabelle auswählen. Der zugeordnete Datensatz sollte auf den vom Subflow erstellten Antwortaufgaben-Datensatz festgelegt werden.

In ähnlicher Weise erfasst die Experience-Statustabelle den Status der Aktivitätskarte. Im Basissystem wird das Statusfeld der Flow-Datentabelle dem Aktivitätskartenstatus zugeordnet. Wenn also die Flow-Datentabelle zum Erfassen des Experience-Status verwendet wird, wird der Status der Aktivitätskarte automatisch aktualisiert. Sie können auch eine andere Tabelle als die Flow-Datentabelle verwenden, um den Experience-Status zu erfassen.

Wenn Sie beispielsweise den Status der Antwortaufgabe dem Status der Aktivitätskarte zuordnen möchten, ist dies möglich. So gehen Sie vor:

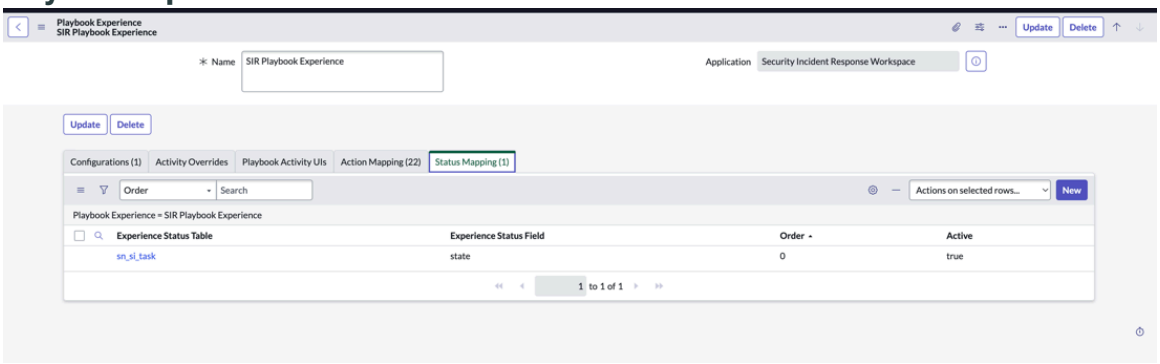
1. Navigieren zu **Alle** > **Playbook-Experiences**.

Playbook-Experiences

2. Öffnen Sie **die SIR Playbook-Experience**.
3. Zugehörige Liste **„Statuszuordnung** öffnen“.

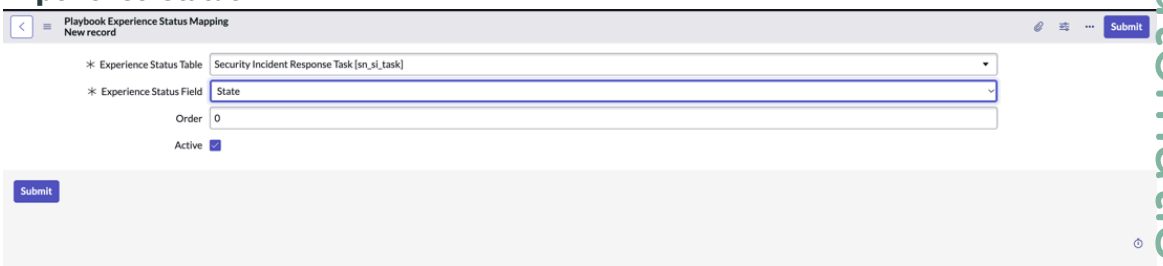
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook-Experience



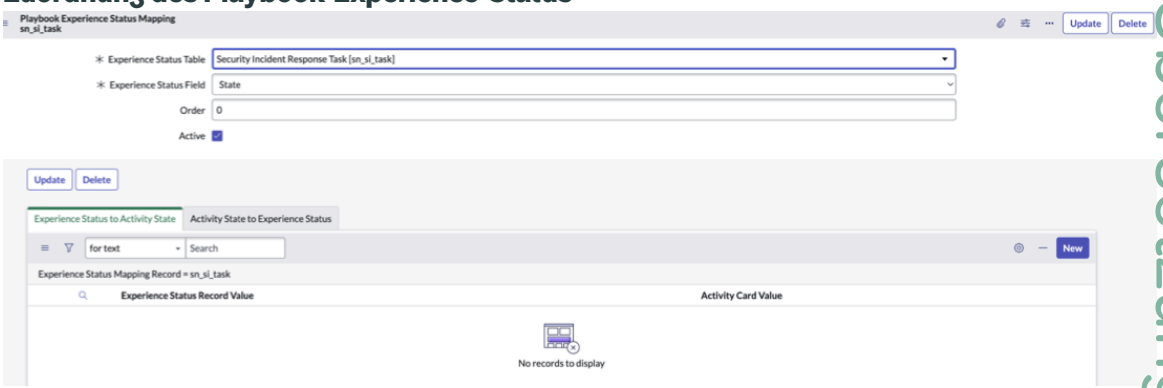
4. Geben Sie das Feld **Antwortaufgabe** für Experience-Statustabelle ein.
5. Geben Sie das Feld **Status** gegen Experience-Status ein.

Experience-Status



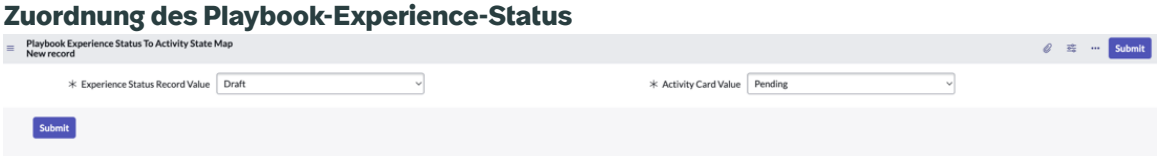
6. Klicken Sie auf **Absenden**. Der Datensatz wird erstellt.

Zuordnung des Playbook-Experience-Status



7. Ordnen Sie unter Experience-Status zu Aktivitätsstatus die Status der Antwortaufgabe dem Status der Aktivitätskarte zu.
8. Auf der linken Seite werden die Status der Antwortaufgabe angezeigt, auf der rechten Seite der Status der Aktivitätskarten.

Zuordnung des Playbook-Experience-Status

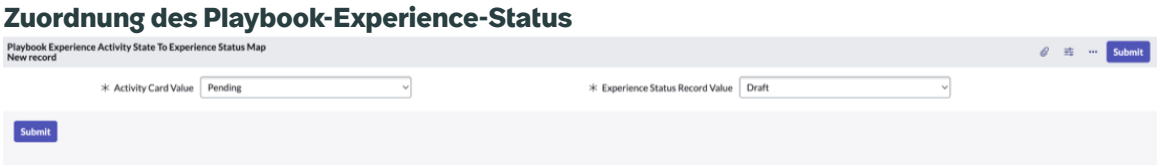


9. Die Zuordnung kann bidirektional sein. Ordnen Sie die Status auch unter „Aktivitätsstatus“ der zugehörigen Liste „Experience“ richtig zu. Dieser Schritt ist die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Umkehrung des vorherigen Schritts. In diesem Fall wird auf der linken Seite der Status der Aktivitätskarte und auf der rechten Seite der Status der Antwortaufgabe angezeigt.



Details

- Tag-Line: E-Mail senden
- Symbol: Umschlaggliederung (in der Anwenderoberfläche nicht angezeigt)
- Titel: **Aktivität** > **Aktivitätsinstanz** > **Bezeichnung**. Hier haben wir die Bezeichnung der Aktivitätsinstanz ausgewählt. Dieses Dot-Walking ersetzt den Bezeichnungswert als Titel dynamisch zur Laufzeit.
- Beschreibung: **Aktivität** > **Aktivitätsinstanz** > **Beschreibung**. Hier haben wir die Beschreibung der Aktivitätsinstanz ausgewählt. Dieses Dot-Walking ersetzt den Bezeichnungswert als Titel dynamisch zur Laufzeit.
- Titel des Status „Ausstehend“: Senden Sie eine E-Mail-Benachrichtigung. Dies ist der Titel, wenn sich die Aktivität im Status „Ausstehend“ befindet.
- Beschreibung des Status „Ausstehend“: Fordert die Bestätigung des E-Mail-Betreffs und des Textes vor dem Senden auf. Dies ist die Beschreibung der Aktivitätskarte, wenn der Status „Ausstehend“ lautet. Datensatzfelder: In diesem Beispiel sind Datensatzfelder ausgewählt.

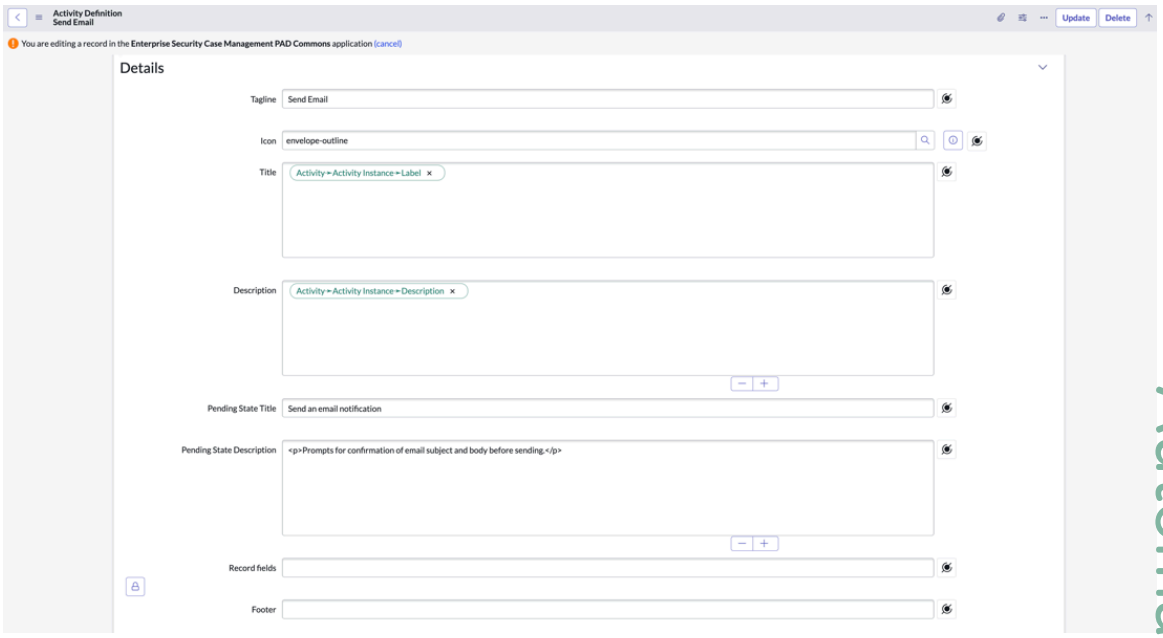
  Datensatzfelder sind eine durch Kommas getrennte Liste von Feldnamen, die für den zugeordneten Datensatz in einer Name-Wert-Paarliste angezeigt werden sollen. Daten werden auf dem Server vorab abgerufen, Dot-Walking wird unterstützt, und **canRead()**-Berechtigungen werden für jedes Feld ausgewertet.

- Fußzeile: Für dieses Beispiel ist keine Fußzeile definiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fußzeile ist ein Text in einem grauen Bereich der Kartenfußzeile. Sie können der Anzeige beliebige aussagekräftige Informationen hinzufügen.

Aktivitätsdefinition – E-Mail senden

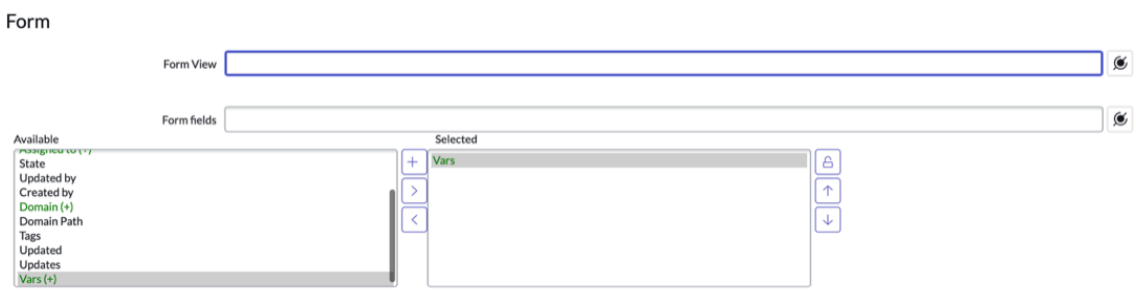


Formular

- Formularansicht: sammeln_Daten
- Formularfelder:

In diesem Beispiel wird die Ansicht „college_data“ verwendet, um die Felder anzuzeigen, die dem Anwender zum Eingeben von Eingaben angezeigt werden müssen. Die Ansicht „Collect_data“ ist eine von der Plattform bereitgestellte Ansicht, die der Flow-Datentabelle entspricht. Alternativ können Sie die Formularansicht leer lassen und Variablen aus der Liste der Werte auswählen, die für Formularfelder verfügbar sind. (Klicken Sie auf das Schlosssymbol, um die Liste der verfügbaren Werte zu öffnen).

Formularansicht



Anhänge

Beispiel:

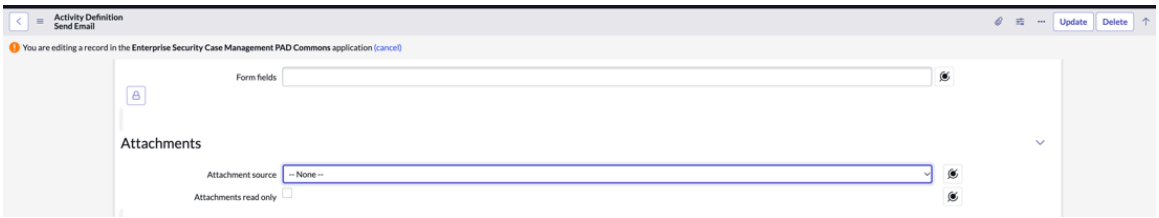
- Anhangsquelle ist leer.
- „Schreibgeschützter Anhang“ nicht ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Anhangquelle: Dropdownliste. Welche Anhänge auf der Karte angezeigt werden sollen: Anhänge, die an den übergeordneten Datensatz angehängt sind, an den zugeordneten Datensatz oder an keine.
2. Anhang schreibgeschützt: Wahr oder Falsch. Verhindern, dass der Anwender die vorhandenen Anhänge umbenennt oder löscht.

Aktivitätsdefinition – E-Mail senden



Funktionen

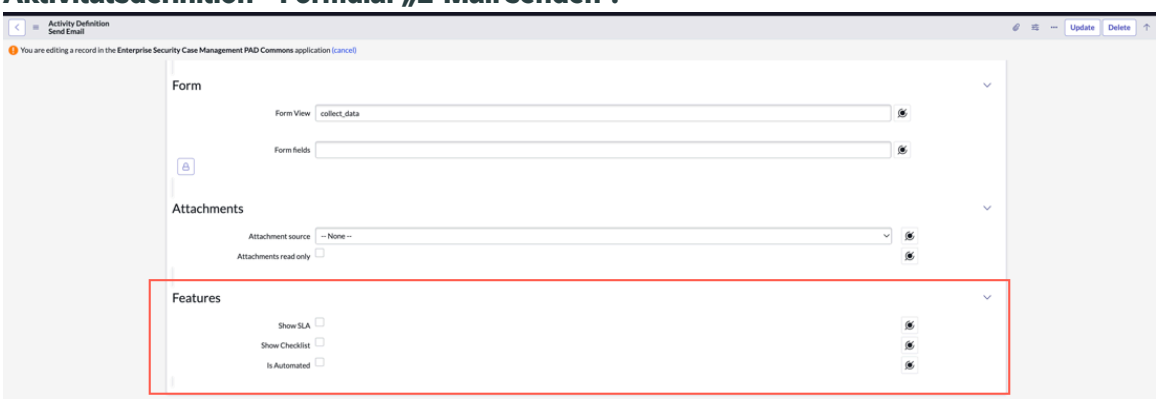
In diesem Beispiel

- SLA anzeigen – Gelöscht
- Prüfliste anzeigen – Gelöscht
- Ist automatisiert: Gelöscht

SLA anzeigen: Wahr/Falsch. Rendert einen SLA-Timer im Header der Karte für den zugeordneten Datensatz. Das SLA wird gemäß dem SLA-Konfigurationsdatensatz ausgewählt, der in der Playbook-Konfiguration angegeben ist.

1. Prüfliste anzeigen – Wahr oder Falsch. Rendert alle Prüflisten, die an den zugeordneten Datensatz angehängt sind. Die Prüfliste kann bearbeitet werden, und Änderungen werden gespeichert, ohne dass eine deklarative Aktion erforderlich ist.
2. Ist automatisiert – Wahr oder Falsch. Bei „wahr“ werden der **Tagline**und **das Symbol**mit dem Text **Automatisierte Aufgabe** und einem automatisierten Symbol überschrieben.

Aktivitätsdefinition – Formular „E-Mail senden“.



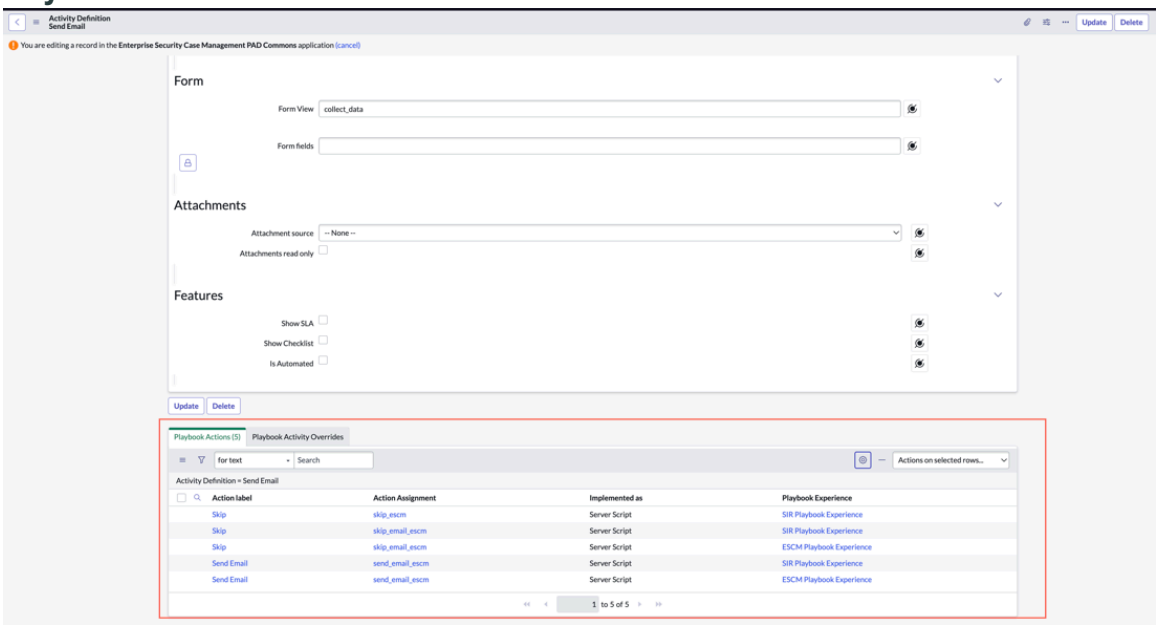
Playbook-Aktionen in der Aktivitätsdefinition

Dieser Abschnitt enthält die Aktionen, die auf der Aktivitätskarte gerendert werden. In diesem Beispiel sind die Aktionen **Überspringen**und **E-Mail senden**.

Um der Aktivitätskarte eine neue Aktion hinzuzufügen, müssen Sie in der zugehörigen Liste **„Playbook-Aktionen“** unten auf der Seite einen Datensatz erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook-Aktionen



1. Klicken Sie auf **Neu**.
2. Wählen Sie die vorhandene Aktivitätsaktion im Feld „Aktionszuweisung“ aus.
3. Wählen Sie **SIR Playbook-Experience** gegen das Feld Playbook-Experience aus.

Erstellt eine Aktivitätsaktion

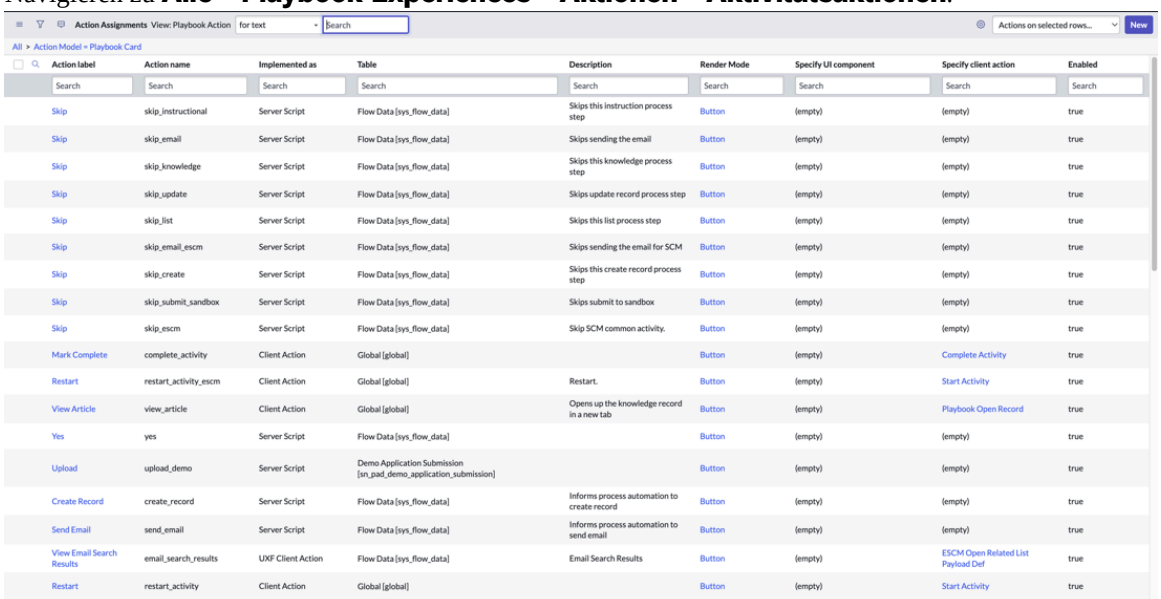
Im Folgenden finden Sie das Verfahren zum Erstellen einer Aktivitätsaktion.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Playbook-Experiences** > **Aktionen** > **Aktivitätsaktionen**.



2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Now Platform-Dokumentation erfahren Sie, wie Sie diese Aktionen erstellen. In diesem Beispiel wird Überspringen als Serverskript implementiert.

3. **Playbook-Überschreibung:**

   Wenn Sie den vorhandenen Aktivitäts-Experience-Typ überschreiben möchten, ist dies möglich. Weitere Informationen finden Sie in der Now Platform-Dokumentation. Keine Playbook-Überschreibungen für dieses Beispiel.

An CSF X Sandbox übermitteln

„An CSF X Sandbox übermitteln“ ist ein Beispiel für einen Aktivitätsdefinitionsprozess.

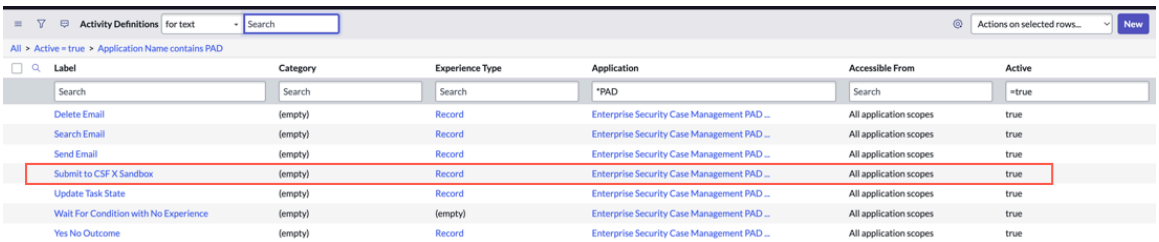
Standard

Die grundlegenden Details umfassen den Name (Bezeichnung), die Anwendung, die Beschreibung, die Tabelle und alle Anwendungen, von denen aus darauf zugegriffen werden kann.

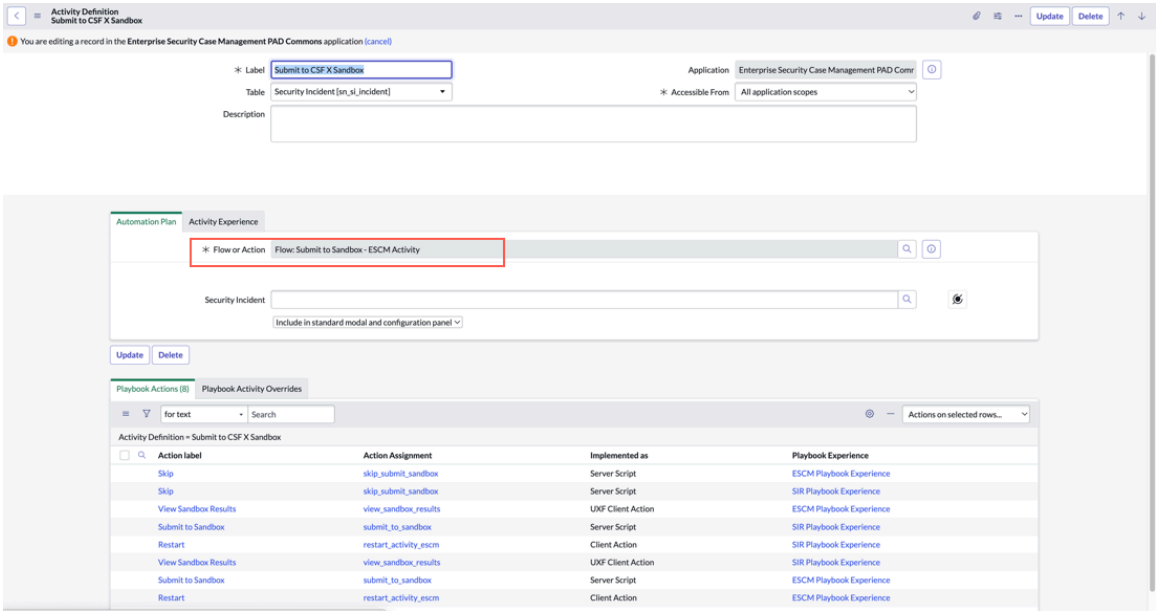
Fügen Sie den Automatisierungsplan und die Aktivitäts-Experience hinzu, und übermitteln Sie sie. Bearbeiten Sie das Dokument nach der Übermittlung, um weitere Details auf den einzelnen Registerkarten hinzuzufügen.

Automatisierungsplan

Der Automatisierungsplan ordnet die mit dem Flow Designer erstellte Back-End-Aktion/den Back-End-Subflow zu. In diesem Beispiel wird der Subflow „ **An die Sandbox übermitteln – ESCM-Aktivität“**verwendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieser Subflow ermöglicht das Senden der schädlichen erkennbaren Elemente an die Sandbox. Es sind alle Eingabe- und Ausgabefelder definiert.

„Security Incident“ ist das Eingabefeld.

Aktivitäts-Experience

In diesem Beispiel ist **Datensatztyp** ausgewählt.

Zugeordneter Datensatz

Der zugeordnete Datensatz speichert die zugeordneten Daten, die sich auf die aktuelle Aktivität beziehen. Dies würde die Laufzeitdaten sowie den Status der Experience erfassen.

- Zugeordnete Tabelle: Flow-Daten
- Zugeordneter Datensatz: VL
- Tabelle für den Experience-Status: Flow-Daten
- Experience-Statusdatensatz: VL

Details

- Tag-Line: E-Mail senden
- Symbol: Umschlaggliederung
- Titel: **Aktivität** > **Aktivitätsinstanz** > **Bezeichnung**. Hier haben wir die Bezeichnung der Aktivitätsinstanz ausgewählt. Dieses Dot-Walking ersetzt den Bezeichnungswert als Titel dynamisch zur Laufzeit.
- Beschreibung: VL (Subflow-Ausgabe wird zugeordnet)
- Titel für Status „Ausstehend“: leer
- Beschreibung des Status „Ausstehend“: leer
- Datensatz-Felder
- Footer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular

- Formularansicht: leer
- Formularfelder: leer

Anhänge

Beispiel:

- Anhangsquelle: Keine
- Anhang schreibgeschützt: Nicht aktiviert

1. Anhangsquelle: Dies ist ein Dropdown-Menü. Welche Anhänge auf der Karte angezeigt werden sollen: Anhänge, die an den übergeordneten Datensatz angehängt sind, an den zugeordneten Datensatz oder an keine.
2. Anhang schreibgeschützt: Dies ist ein Wahr/Falsch-Wert. Verhindern, dass der Anwender die vorhandenen Anhänge umbenennt oder löscht.

Funktionen

In diesem Beispiel

- SLA anzeigen – Deaktiviert
- Prüfliste anzeigen – Nicht aktiviert
- Ist automatisiert: Nicht aktiviert

Playbook-Aktionen in der Aktivitätsdefinition

Dieser Abschnitt enthält die Aktionen, die auf der Aktivitätskarte gerendert werden.

Dieses Beispiel enthält die Aktionen Überspringen, Sandbox-Ergebnisse anzeigen, An die Sandbox übermitteln und Neustart.

Um der Aktivitätskarte eine neue Aktion hinzuzufügen, müssen Sie in der zugehörigen Liste „Playbook-Aktionen“ unten auf der Seite einen neuen Datensatz erstellen.

Playbook-Überschreibung

Keine Playbook-Überschreibungen für dieses Beispiel.

Beispiel-Playbooks für SIR Workspace

Sie können Playbooks für SIR Workspace schnell und einfach erstellen oder konfigurieren, ohne komplizierten Code zu schreiben. Sie können diese Playbooks verwenden, um Sicherheitsbedrohungen schrittweise zu beheben. Sie können den Playbook-Flow für Security Incidents automatisch oder manuell aufrufen.

Security Incident Response stellt die folgenden Playbooks mit dem Basissystem bereit:

- Playbook für manuelles Phishing
- Playbook für automatisiertes Phishing
- Playbook für manuelle Malware

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Playbook für automatisierte Malware
- Playbook für das Handbuch für fehlgeschlagene Anmeldung

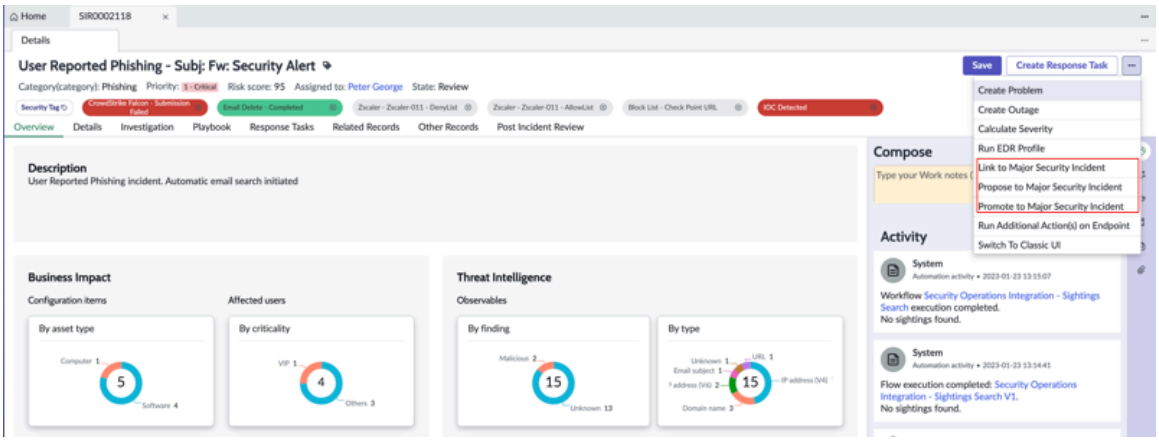
Arbeiten mit MSI-Datensätzen

Mit dem Arbeitsbereich für Security Incident Response können Sie Security Incidents als schwerwiegende Security Incidents vorschlagen, heraufstufen oder verknüpfen, wenn die Incidents als kritische Bedrohung für die Organisation identifiziert werden.

Nachdem Sie Management schwerwiegender Sicherheits-Incidents (MSIM) in Ihrer Instanz Now Platform installiert haben, können Sie den Übergang von Security Incidents zu schwerwiegenden Incidents handhaben.

Die UI-Aktionen Management schwerwiegender Sicherheits-Incidents (MSIM) werden rechts oben im Banner des Security Incident-Formulars im SIR-Arbeitsbereich angezeigt. Wählen Sie die zutreffende UI-Aktion aus.

Hinweis:
Einige Aktionen sind kontextbezogen. Beispielsweise ist die Aktion Verknüpfung aufheben nur verfügbar, wenn der Security Incident bereits vorgeschlagen oder heraufgestuft oder mit einem schwerwiegenden Security Incident verknüpft ist.



Als schwerwiegenden Security Incident vorschlagen

Einen Security Incident als schwerwiegenden Security Incident (Major Security Incident, MSI) vorschlagen.

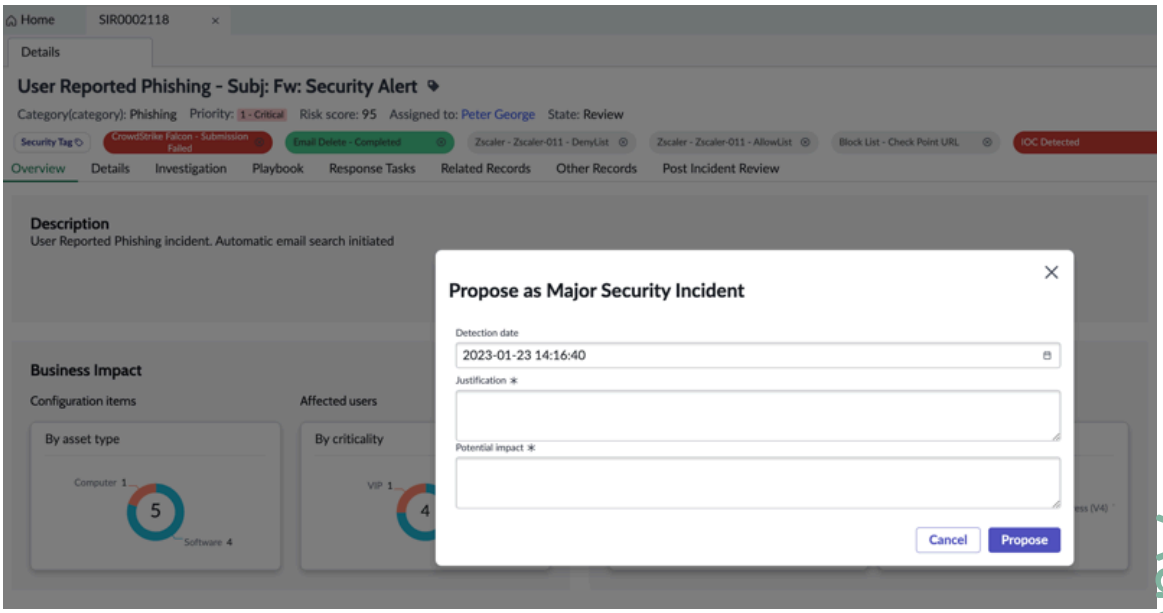
Vorbereitungen

Erforderliche Rolle: sn_si.analyst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Klicken Sie **auf Schwerwiegenden Security Incident vorschlagen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie im Formular Felder wie Erkennungsdatum, Begründung und Potenzielle Auswirkung aus.
5. Klicken Sie auf **Vorschlagen**.
   Der Incident-Datensatz wird als Kandidaten für einen schwerwiegenden Security Incident vorgeschlagen. Nachdem der Incident-Datensatz als Kandidaten für schwerwiegenden Security Incident vorgeschlagen wurde, wird das Tag **Kandidat für schwerwiegenden Security Incident** angewendet und im Banner des Formulars für Security Incidents angezeigt.

> **Hinweis:**
> Klicken Sie **auf Verknüpfung mit schwerwiegendem Security Incident aufheben aufheben**, um die Verknüpfung des incident aufzuheben, wenn Sie ihn nicht vorschlagen möchten oder wenn der Incident keine kritischen Auswirkungen hat. Der Incident wird nicht verknüpft und in der Listenansicht dem Sicherheitsanalysten zur Korrektur angezeigt.

Zu schwerwiegendem Security Incident heraufstufen

Stufen Sie einen Security Incident zu einem schwerwiegenden Security Incident herauf.

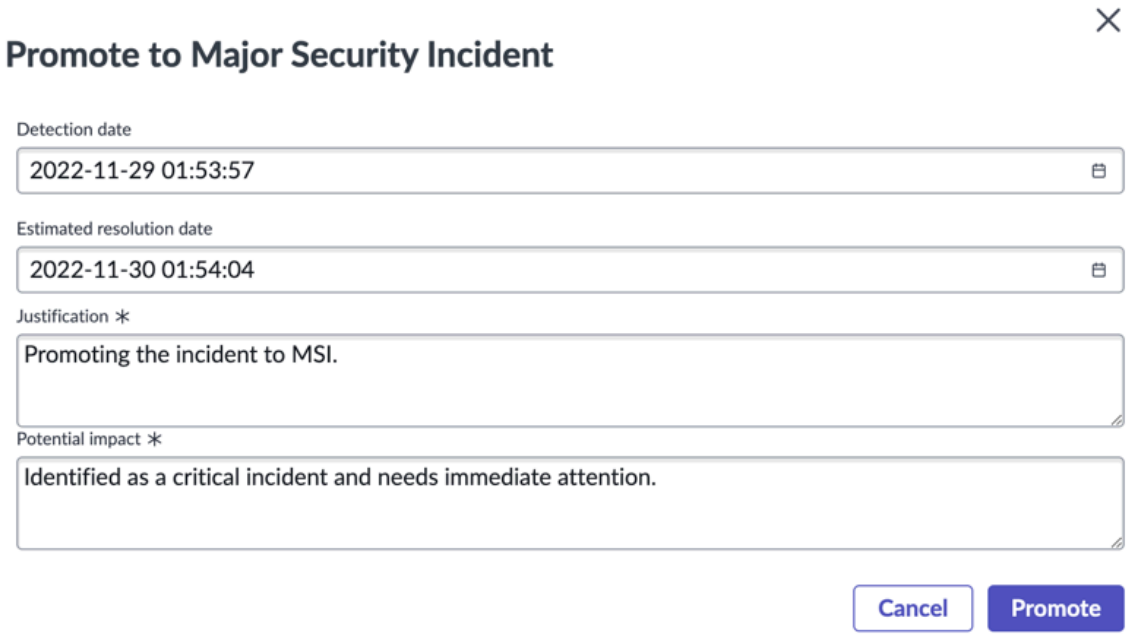
Vorbereitungen

Erforderliche Rolle: sn_si.analyst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Klicken Sie auf **Zu schwerwiegendem Security Incident heraufstufen**.
4. Füllen Sie im Formular Felder wie Erkennungsdatum, Geschätztes Lösungsdatum, Begründung und Potenzielle Auswirkung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Heraufstufen**.
   Der Incident-Datensatz wird als schwerwiegender Security Incident heraufgestuft.
   Nachdem der Incident-Datensatz als schwerwiegender Security Incident heraufgestuft wurde, wird das Tag **Schwerwiegender Security Incident** angewendet und im Formularbanner angezeigt.

> **Hinweis:**
> Sie können auch die Verknüpfung des schwerwiegenden Security Incident aufheben, wenn der Incident nicht kritisch ist. Der Incident wird dann aufgehoben und in der Listenansicht zur Korrektur durch den Sicherheitsanalysten aufgeführt.

Mit schwerwiegendem Security Incident verknüpfen

Verknüpfen Sie einen Security Incident mit einem schwerwiegenden Security Incident als untergeordneten Incident(s).

Vorbereitungen

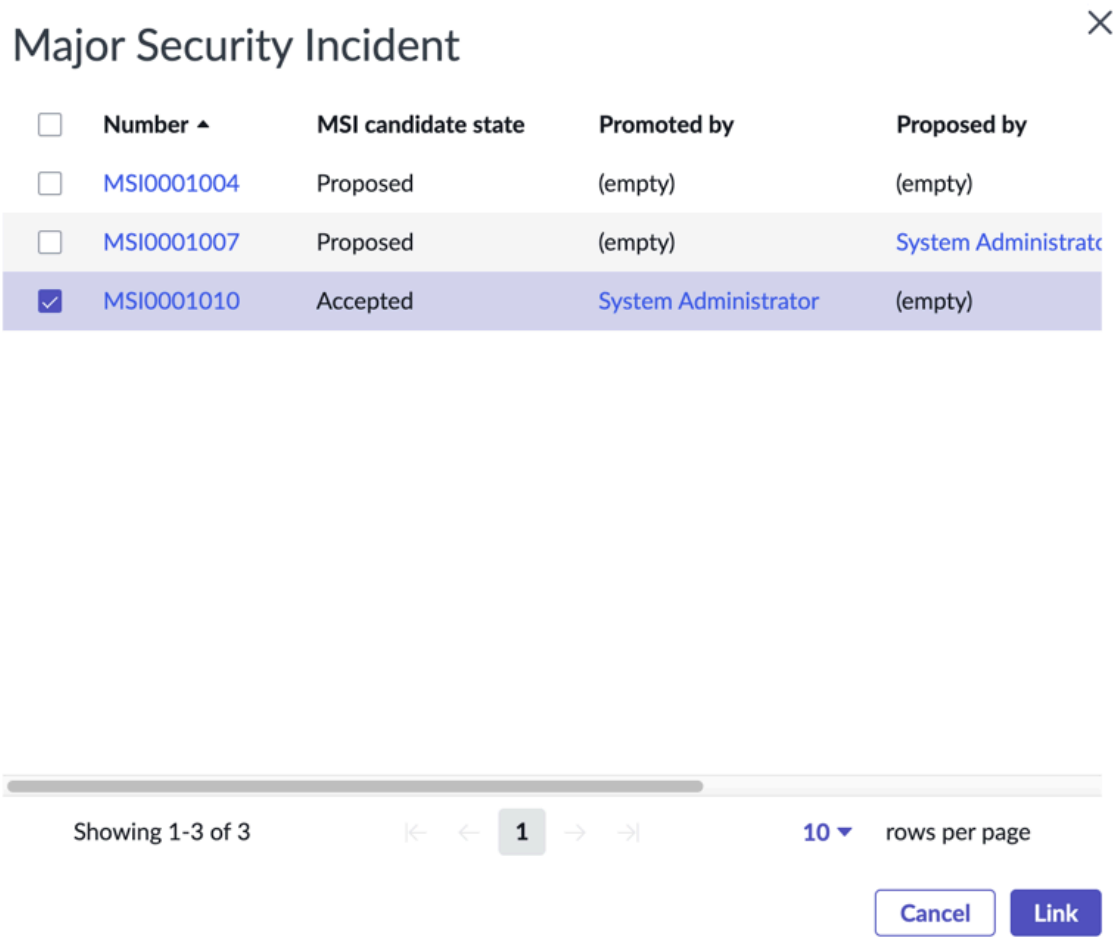
Erforderliche Rolle: sn_si.analyst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Klicken Sie **auf Mit schwerwiegendem Security Incident verknüpfen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Incidents aus, die mit einem schwerwiegenden Security Incident verknüpft werden sollen.
5. Klicken Sie auf **Link**.
6. Der Incident-Datensatz ist als untergeordneter Incident des schwerwiegenden Security Incident verknüpft. Nachdem der Incident als untergeordneter Incident mit einem schwerwiegenden Security Incident verknüpft wurde, wird das Tag **Schwerwiegender Security Incident** angewendet und im Formularbanner angezeigt.

Arbeiten mit Formular-UI-Aktionen

Im Folgenden finden Sie die UI-Aktionen, die im Formular „Security Incident“ angezeigt werden.

So navigieren Sie zu den UI-Aktionen des Formulars:

1. Gehe zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen Sie einen beliebigen Security Incident aus der Listenansicht aus.
3. Alle UI-Aktionen sind in der oberen rechten Ecke des Formulars „Security Incident“ zu finden.

UI-Aktionen für Arbeitsbereich-Formulare

Feldname	Beschreibung
Diskutieren	Erstellen oder starten Sie eine Sidebar-Diskussion für den Security Incident.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

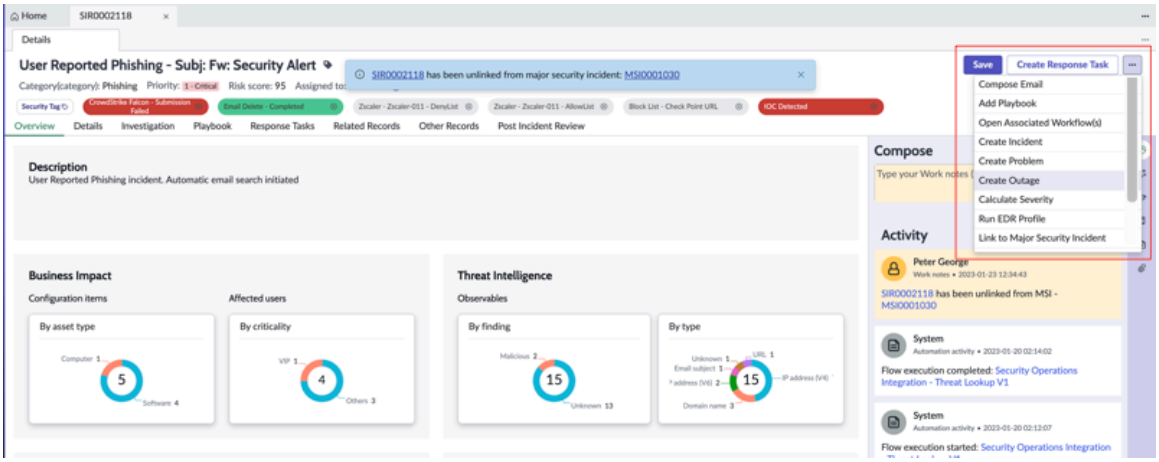
Feldname	Beschreibung
Speichern	Speichern oder aktualisieren Sie den Security Incident Response-Datensatz, nachdem Sie Änderungen vorgenommen haben.
Antwortaufgabe erstellen	Erstellen Sie eine Antwortaufgabe für den Security Incident.
E-Mails verfassen	Verfassen Sie E-Mails für den Security Incident.
Playbook hinzufügen	Fügen Sie das Playbook für den Security Incident manuell hinzu.
Incident erstellen	Erstellen Sie einen Incident innerhalb des Security Incident.
Kundenservicefall erstellen	Erstellen Sie einen Kundenservicefall für den Security Incident, der vom Team für Kundenservice-Management (CSM) nachverfolgt wird. **Hinweis:** Diese Option ist nur verfügbar, wenn Kundenservice-Management (CSM) installiert ist.
Verknüpfte(n) Workflow(s) öffnen	Öffnen Sie alle Workflow-Kontexte, die dem Security Incident zugeordnet sind. Diese Option ist nur sichtbar, wenn Workflows vorhanden sind.
Change Request erstellen	Erstellen Sie eine Change-Anforderung innerhalb des Security Incident.
Problem erstellen	Erstellen Sie ein Problem innerhalb des Security Incident.
Ausfall erstellen	Erstellen Sie einen Ausfall innerhalb des Security Incident.
Schweregrad berechnen	Berechnen Sie den Schweregrad eines Security Incident mit vordefinierten Rechnern. Der Schweregrad wird basierend auf den in den Rechnern vordefinierten Regeln berechnet. Der Schweregrad eines incident beruht auf der Risikopunktzahl, der Geschäftsauswirkung und der Priorität.
EDR-Profil ausführen	Wählen Sie das EDR-Profil für die gewünschte Integration aus, und führen Sie es aus. **Hinweis:** Diese Option ist nur verfügbar, wenn Integrationen installiert sind.
Mit schwerwiegendem Security Incident verknüpfen	Verknüpfen Sie einen Security Incident mit einem schwerwiegenden Security Incident.
Risikoereignis melden	Melden Sie diesen Security Incident als Risikoereignis an das Risikomanagement-Team. Das Risikomanagementteam analysiert das Ereignis und stellt sicher, dass solche Ereignisse und die zugehörigen Verluste nicht erneut auftreten. **Hinweis:** Diese Option ist nur verfügbar, wenn Risikomanagement installiert ist.
Verknüpfung mit schwerwiegendem Security Incident aufheben	Verknüpfung mit schwerwiegendem Security Incident aufheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
Als schwerwiegenden Security Incident vorschlagen	Schlagen Sie einen Security Incident als schwerwiegenden Security Incident vor.
Zu schwerwiegendem Security Incident heraufstufen	Heraufstufen eines Security Incident als schwerwiegenden Security Incident.
Zusätzliche Aktion(en) für Endpunkt ausführen	Führen Sie zusätzliche Aktionen für den Endpunkt aus. **Hinweis:** Diese Option ist nur verfügbar, wenn Endpunktintegrationen installiert sind. Beispiel: FireEye HX
Neues Ereignis in MISP erstellen	Sie können Ereignisse in MISP automatisch oder manuell erstellen und ändern. **Hinweis:** Diese Option ist nur verfügbar, wenn die MISP-Integration installiert ist.
Ordnen Sie die MITRE ATT&K-Technik zu	Ordnen Sie dem Security Incident MITRE ATT&K-Techniken zu. **Hinweis:** Diese Option ist verfügbar, wenn MITRE ATT&K installiert ist.
MITRE ATT&K-Info anzeigen	Zeigt die MITRE ATT&K-Informationen an, die dem Security Incident zugeordnet sind. **Hinweis:** Diese Option ist verfügbar, wenn MITRE ATT&K installiert ist.
Dem Sicherheitsfall hinzufügen	Fügen Sie den Security Incident einem vorhandenen oder neuen Security Incident hinzu. **Hinweis:** Diese Option ist verfügbar, wenn Threat Intel installiert ist.
Zu klassischer UI wechseln	Ermöglichen Sie dem Analysten, zwischen klassischer und neuer UI zu wechseln, damit er auch an den vorhandenen Funktionen arbeiten kann, die im neuen Arbeitsbereich noch nicht verfügbar sind.
Abbrechen	Brechen Sie einen Security Incident ab. Nachdem Sie „Alle zugehörigen Datensätze wie Antwortaufgaben **abbrechen** “ ausgewählt haben, werden auch die untergeordneten Security Incidents abgebrochen.
Löschen	Löschen Sie einen Security Incident-Datensatz.

4. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Sie können die UI-Aktionen oben auf der Seite sehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Workflow zum Schließen von Security Incidents

Schließen Sie den Security Incident, indem Sie den Incident-Status aktualisieren.

Vorbereitungen

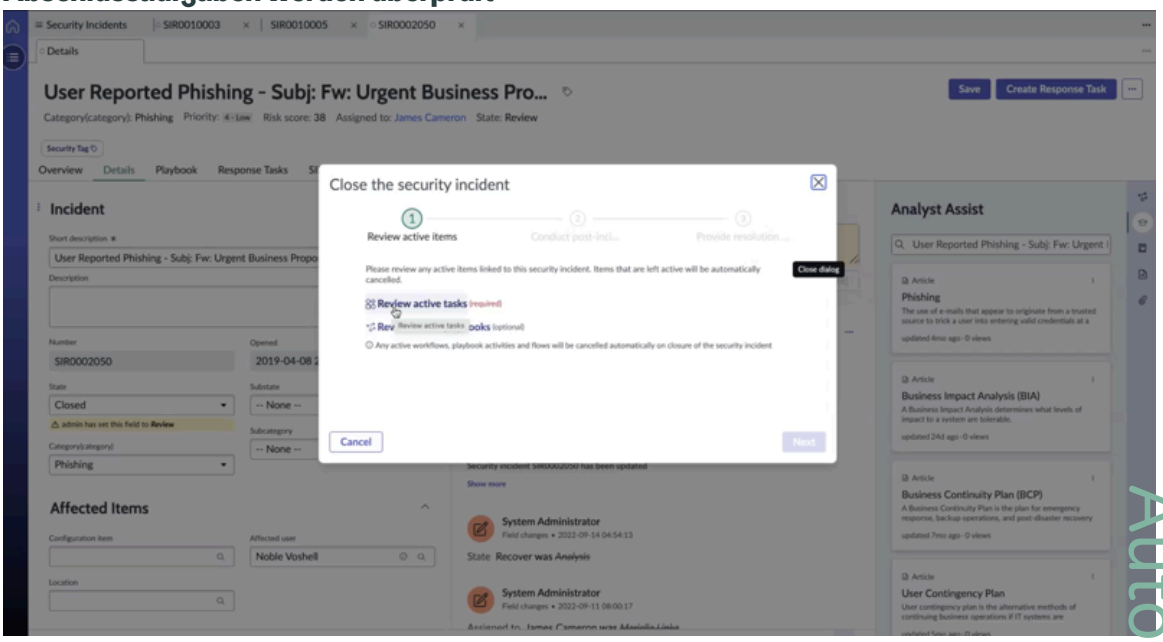
Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wechseln Sie beispielsweise zu **Listen** > **Security Incidents** > **Offene Incidents**.
3. Öffnen Sie einen Incident, den Sie schließen möchten.
4. Wechseln Sie zur Registerkarte **Details**.
5. Führen Sie einen Drilldown zum Incident-Status durch, und wählen Sie **Schließen**aus.
6. Führen Sie die Abschlussaktivitäten durch.
   - Dies ist ein obligatorischer Schritt zur Überprüfung einer Aufgabe, bevor ein Security Incident geschlossen wird. Alle Antwortaufgaben müssen vom Analysten überprüft und geschlossen oder abgebrochen werden, bevor sie als Security Incident geschlossen werden. Wenn der Analyst auf **„Aktive Aufgaben überprüfen“**klickt, wird der Benutzer zur Registerkarte **„Antwortaufgaben“** weitergeleitet. Es wird eine Sitzungsnachricht mit der Meldung angezeigt, dass Sie gerade einen Security Incident schließen. Klicken Sie auf **„Fortsetzen“**.
   - Klicken Sie auf **Fortsetzen**. Der erste Schritt: Überprüfen Sie, ob die aktiven Aufgaben beim Schließen des Security Incident abgeschlossen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

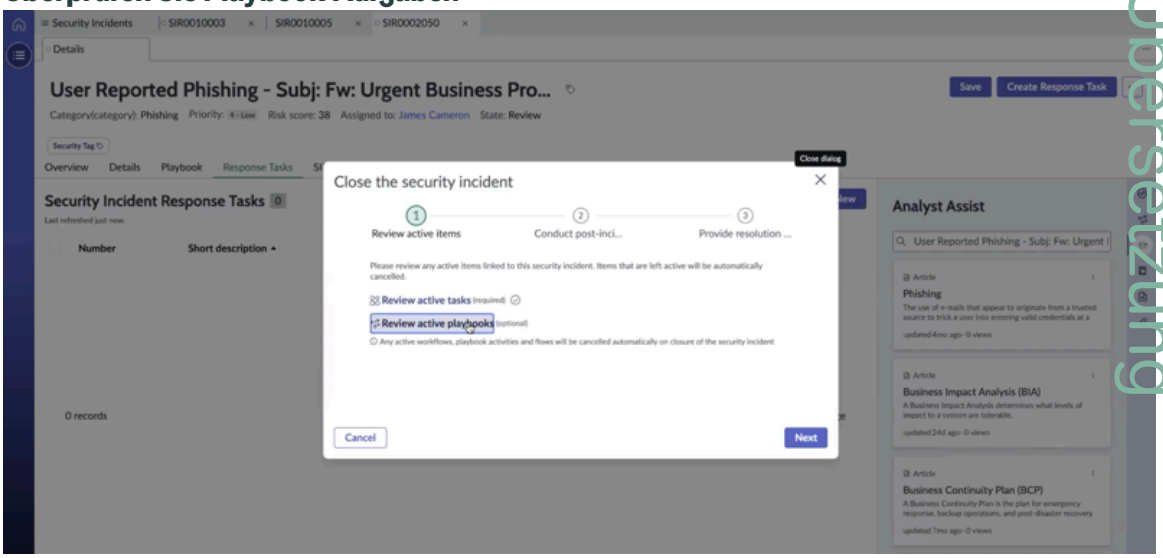
Abschlussaufgaben werden überprüft



- Fahren Sie mit dem nächsten Schritt fort, um die aktiven Playbooks für den Analysten zu überprüfen. Dies ist ein optionaler Schritt. Sie können auf den Link klicken, um die aktive Playbook-Aufgabe zu überprüfen und bei Bedarf zu schließen.

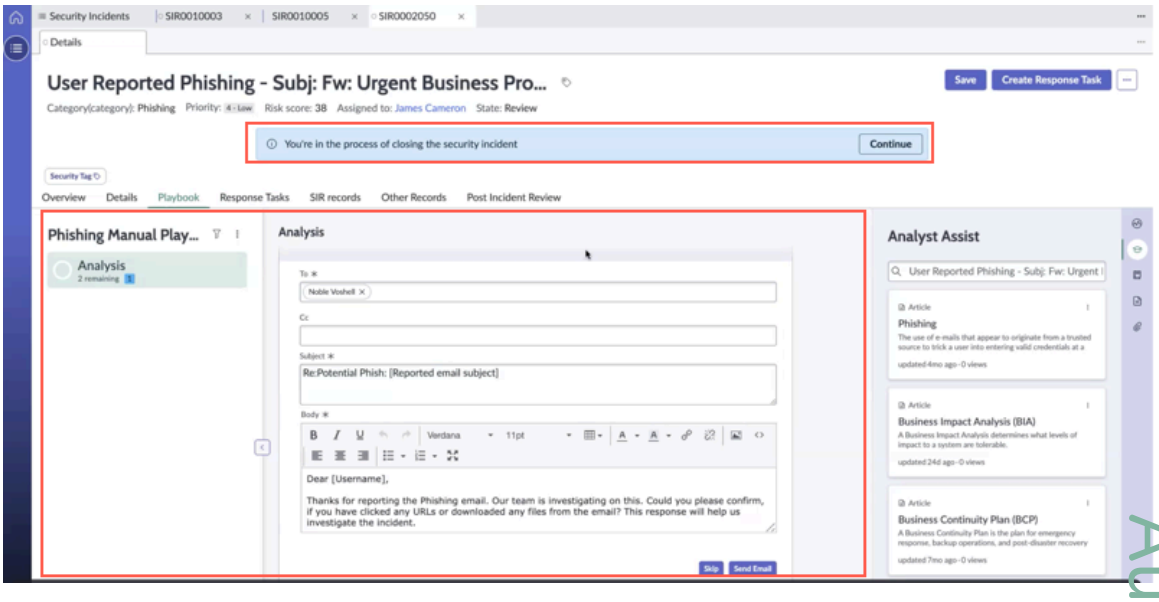
Hinweis:
Alle aktiven Workflows, Playbook-Aktivitäten und Flows werden beim Schließen des Security Incidents automatisch abgebrochen.

Überprüfen Sie Playbook-Aufgaben



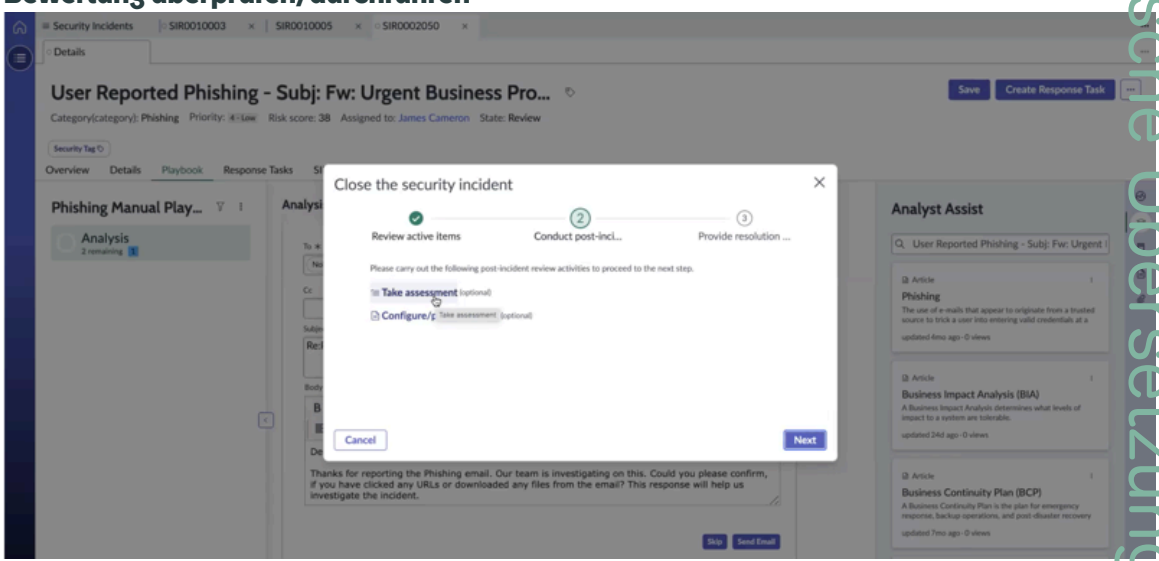
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



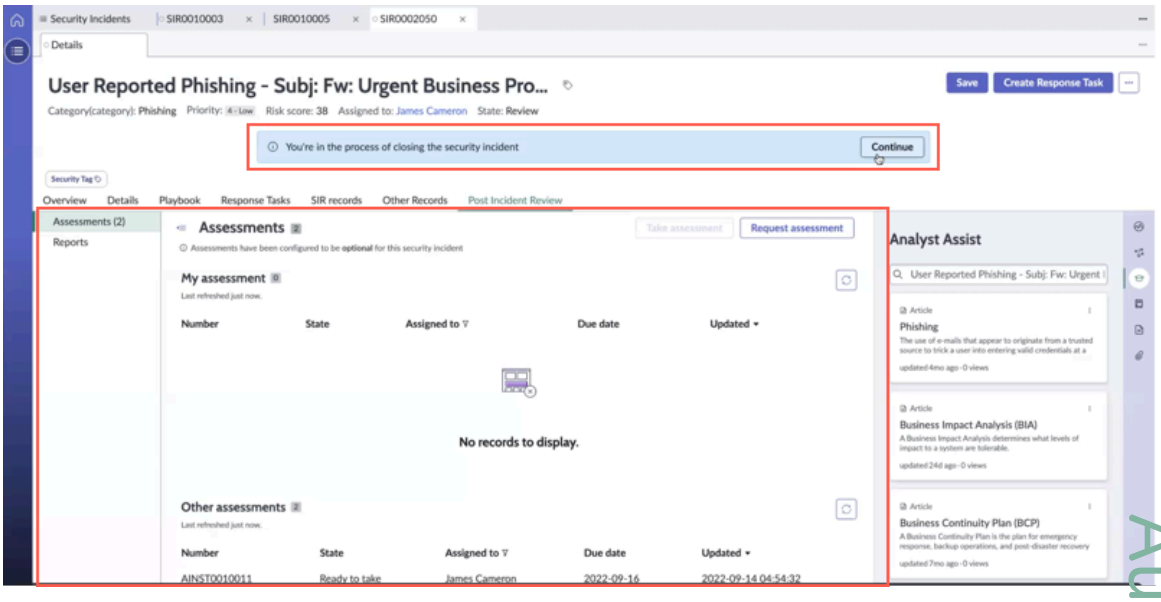
- Überprüfungsbericht nach Incident: Sie werden jetzt zur Überprüfung der Aktivitäten nach dem Incident verschoben, um mit dem Abschluss fortzufahren. Wenn die Bewertung optional ist, überspringen Sie den Schritt, oder wenn die Bewertung obligatorisch ist, nehmen Sie die Bewertung vor und schließen Sie sie ab.

Bewertung überprüfen/durchführen

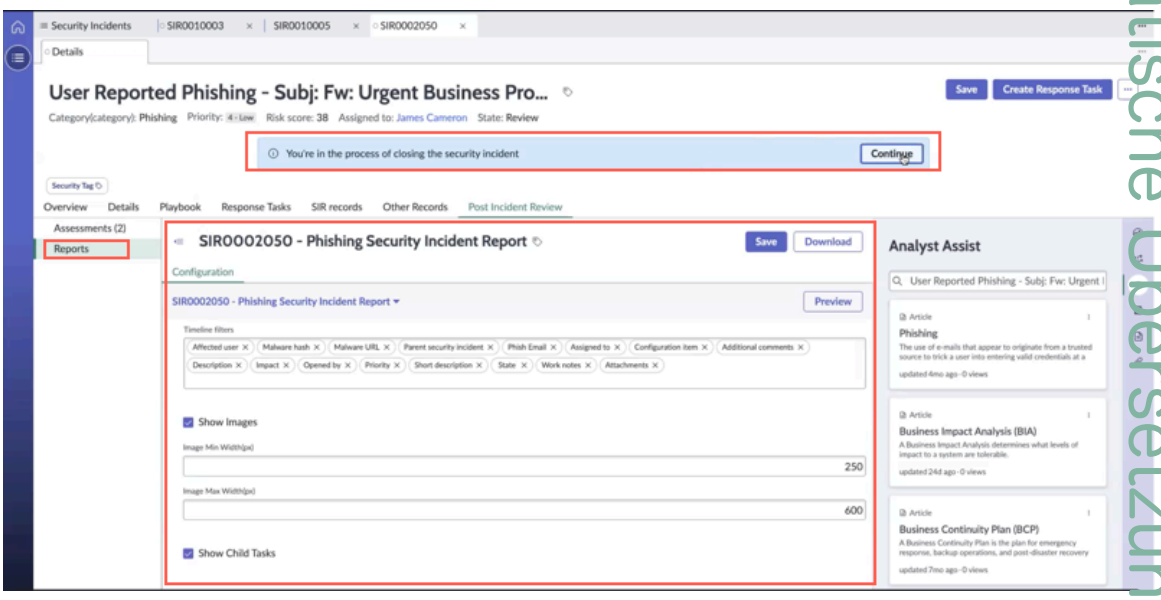


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Bericht konfigurieren/in Vorschau anzeigen: Dies ist wiederum ein optionaler Schritt. Klicken Sie auf den Link, um den Bericht zu überprüfen und mit **dem nächsten** Schritt fortzufahren.

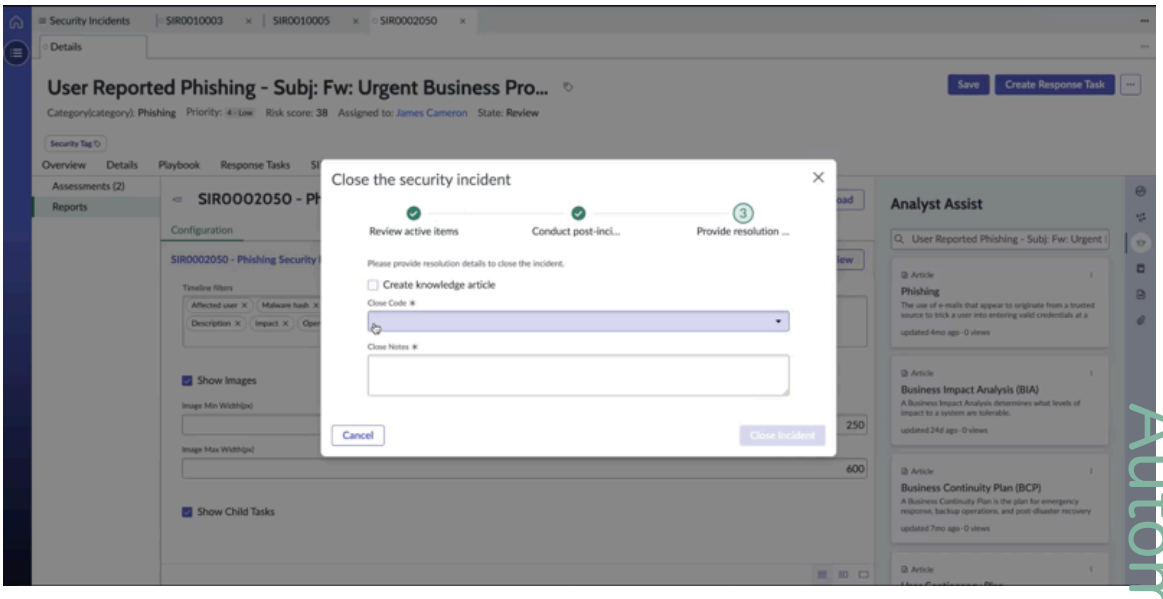


- Lösungsdetails bereitstellen: Der Analyst kann das Kontrollkästchen aktivieren, um Wissensartikel automatisch zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geben Sie den Abschlusscode und die Abschlussnotizen ein, und klicken Sie auf **Incident schließen**.



Hinweis:
Wenn der Analyst **das Dialogfeld „Security Incident schließen“** abbricht, kann er zufällig zur Registerkarte **Details** navigieren und den Incident-Status in „ **Schließen“** ändern, um mit dem Abschluss fortzufahren.

SIR-Arbeitsbereichs-Dashboards anzeigen

In diesem Abschnitt werden die wichtigen Metriken zur Analyse des Prozesses Security Incident Response beschrieben, z. B. neue Security Incidents oder das durchschnittliche Alter der offenen Security Incidents.

In der klassischen Anwenderoberfläche sind unter der Homepage und unter Performance Analytics -Dashboards einige Standard-Dashboards verfügbar, wenn das Plugin Performance Analytics für Security Incident Response installiert ist. All diese Optionen sind jetzt im neuen Arbeitsbereich im Abschnitt **„SIR-Dashboards“** verfügbar.

Standard-Dashboards unter Homepage:

- Security Incident Response – Übersicht
  - Übersicht über Analysten
  - Managerübersicht (in zukünftigen Versionen unterstützt)
  - CISO-Übersicht (unterstützt in zukünftigen Versionen)
- **Platform Analytics für** *`Security Incident Response`*
  - Security Incident-Explorer
  - CISO-Dashboard (zukünftiges Release)
  - Security Incident-Management
  - KPIs von Security Incident-Management Premium
  - Effizienz von Security Operations
  - Kontextsensible Analysen – SI-Dashboard

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für Security Incident Response-Dashboards wie das CISO-Dashboard kann es zu Wiederholungen von Dashboards in Standard- und Plattformanalysen kommen. Wenn das Plugin installiert ist, sind in diesen Dashboards zusätzliche Inhalte vorhanden, die nicht als Duplikat verfügbar sind.

Benutzer müssen das Plugin „“ installieren, damit die unter „Platform Analytics for Security Incident Response Dashboards“ aufgeführten Dashboards im -Arbeitsbereich angezeigt werden. Andernfalls sind nur die Standarddashboards verfügbar.

In der aktuellen Version von SIR Workspacesind im Abschnitt **„SIR-Dashboards“** die folgenden Dashboards verfügbar. Die anderen fehlenden Dashboards werden in späteren Releases verfügbar sein.

Security Incident Response-Dashboards

Dashboard	Beschreibung
Standard-Dashboard	
Sicherheitsanalyst – Übersicht	Mit diesem Dashboard können Sicherheitsanalysten eine Zusammenfassung der Security Incidents basierend auf den Arbeiten des Analysten mit kritischer Priorität, den Arbeiten mit hoher Priorität, den Security Incidents, die dem Analysten zugewiesen sind, den Aufgaben, die den Analysten zugewiesen sind, und der Incident-Anzahl anzeigen.
Performance Analytics (PA) für Security Incident Response-Dashboards	
Security Incident-Explorer	Mit diesem Dashboard können Sicherheitsmanager und Analysten Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkung gruppiert anzeigen. Mit diesen Ansichten können Manager und Analysten schnell Einblicke in die Häufigkeit von Angriffen und die betroffenen Business Services erhalten.
Security Incident-Management	Mit diesem Dashboard können Sicherheitsmanager auf einfache Weise das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung verfolgen.
CISO-Dashboard	Zur Unterstützung in einem zukünftigen Release vorgeschlagen.
Effizienz von Security Operations	Mit diesem Dashboard können Manager und Analysten allgemeine Effizienzmetriken anzeigen und die Leistung des SOC messen.
KPIs von Security Incident-Management Premium	Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/ Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung nachverfolgen und anzeigen.
Kontextbezogene Analytics – S	Mit diesem Dashboard können Manager und Analysten die offenen Security Incidents, das durchschnittliche Alter der offenen Security Incidents,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Dashboards (Fortsetzung)

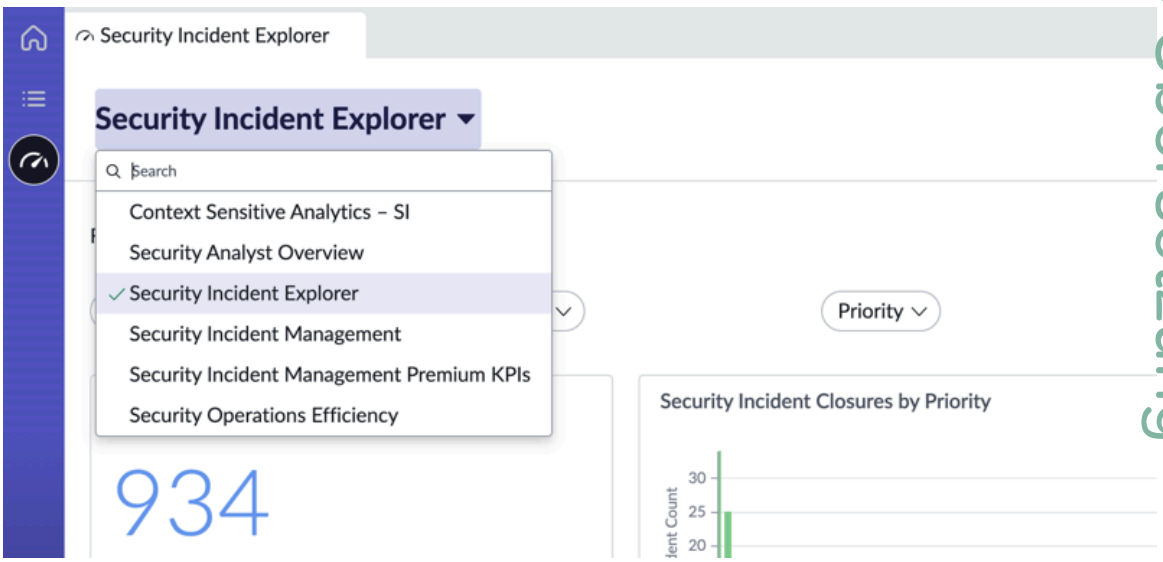
Dashboard	Beschreibung
	die durchschnittliche Abschlusszeit von Security Incidents, den Prozentsatz der Security Incidents, die am selben Tag geöffnet und geschlossen wurden, und den Prozentsatz der anzeigen Incidents, die in den letzten 5 Tagen und 30 Tagen nicht aktualisiert wurden.

Greifen Sie auf SIR- und PA-Dashboards zu

Über das Symbol **„SIR-Dashboards“,** das auf der linken Seite der Startseite des Arbeitsbereichs angezeigt wird.

Hinweis:
Benutzer mit den Zugriffsrechten sn_si.manager oder sn_si.admin können die Dashboards bearbeiten. Die Benutzer müssen sich im gleichen Bereich der Dashboards befinden, die der Benutzer bearbeiten möchte. Wenn beispielsweise das Übersichts-Dashboard für Sicherheitsanalysten im SIR-Arbeitsbereich verfügbar ist, muss sich der Benutzer auch im gleichen SIR-Arbeitsbereich befinden, um Änderungen am Dashboard vorzunehmen.

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident-Management**.
2. Klicken Sie auf das Symbol **SIR-Dashboard** .
3. Wählen Sie das gewünschte Dashboard aus der Dropdown-Liste aus.



Sie können die Dashboards bearbeiten, neue Elemente zu den Dashboards hinzufügen und eigene Dashboards erstellen. Weitere Informationen zur Verwendung von Dashboards finden Sie unter Mit reaktionsfähigen Dashboards arbeiten

Zeigen Sie das Dashboard mit der Übersicht über Sicherheitsanalysten an

Mit diesem Dashboard können Sicherheitsanalysten eine Zusammenfassung der Security Incidents basierend auf den Arbeiten der Analysten mit kritischer Priorität, den Arbeiten mit hoher Priorität, den Security Incidents, die dem Analysten zugewiesen sind, den Aufgaben, die den Analysten zugewiesen sind, und der Incident-Anzahl anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

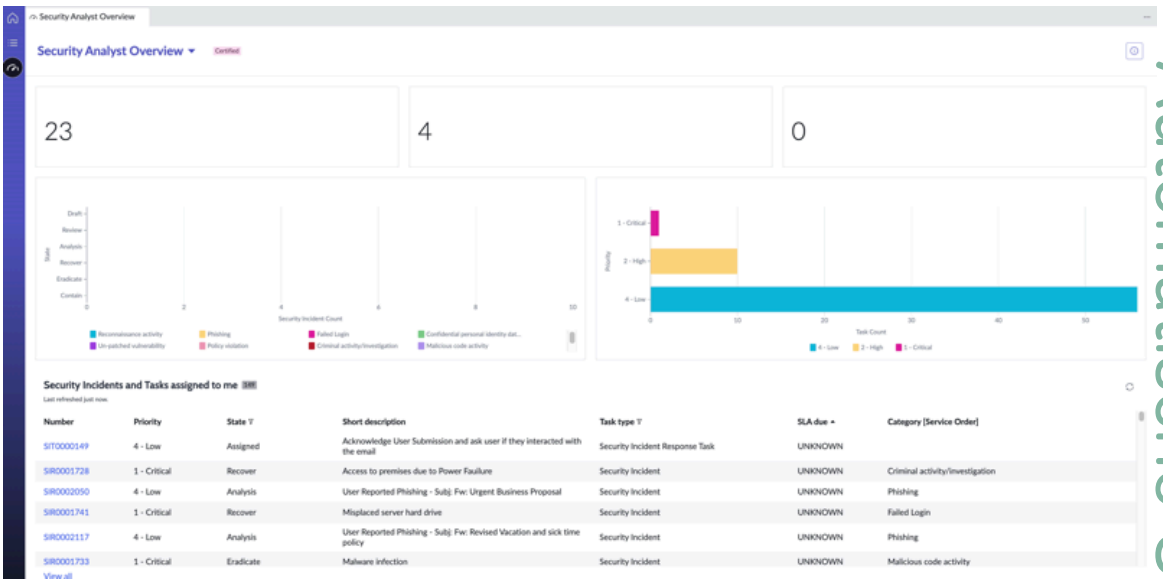
Vorbereitungen

Standardmäßig wird das Dashboard „Sicherheitsanalyst – Übersicht“ für Benutzer mit sn_si.analyst-Zugriff angezeigt.

Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (Schreiben)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“**, das auf der linken Seite der Startseite des Arbeitsbereichs angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Sicherheitsanalystenübersicht** aus.



Zeigen Sie das Dashboard „Sicherheitsanalystenübersicht“ für weitere Aktionen an. Ausführliche Informationen zum Dashboard mit der Übersicht über Sicherheitsanalysten finden Sie unter Security Incident Response Platform Analytics-Lösungen.

Zeigen Sie das Dashboard „Security Incident Explorer“ an

Mit diesem Dashboard können Sicherheitsmanager Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkung gruppiert anzeigen.

Vorbereitungen

Standardmäßig wird das Security Incident Explorer-Dashboard für Benutzer mit sn_si.manager-Zugriff angezeigt.

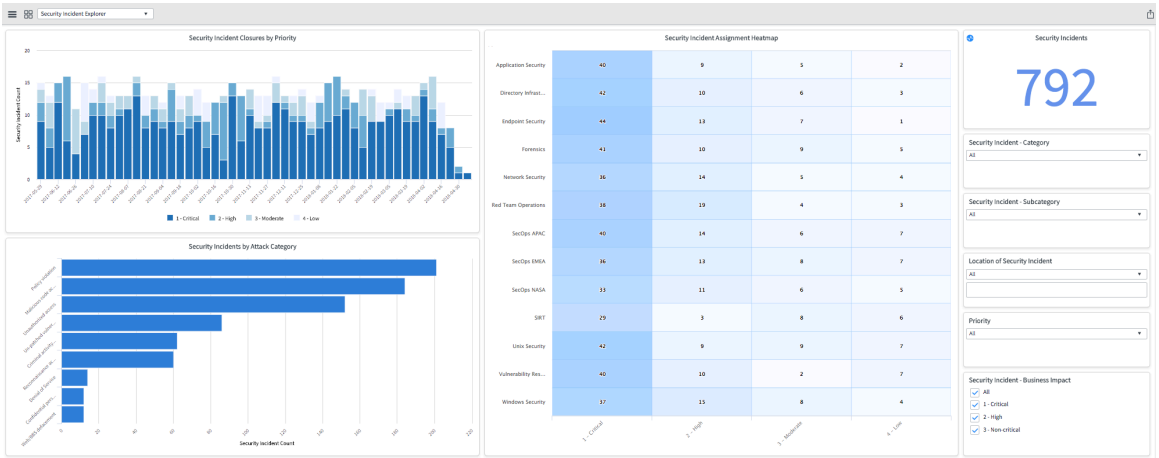
Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (Schreiben)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“**, das auf der linken Seite der Startseite des Arbeitsbereichs angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Security Incident Explorer** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie das Security Incident Explorer-Dashboard für weitere Aktionen an. Ausführliche Informationen zum Security Incident Explorer-Dashboard finden Sie unter Security Incident Explorer-Dashboard

Im aktuellen Release wird die folgende Liste von Berichten im Dashboard des Security Incident Explorers nicht unterstützt:

- Heatmap für Security Incident-Zuweisung: Heatmap-Visualisierung ist nicht verfügbar.
- Security Incident-Zuordnung – Zuordnungsvisualisierung ist nicht verfügbar.

Zeigen Sie das Dashboard Security Incident-Management an

Mit diesem Dashboard können Sicherheitsmanager auf einfache Weise das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung verfolgen.

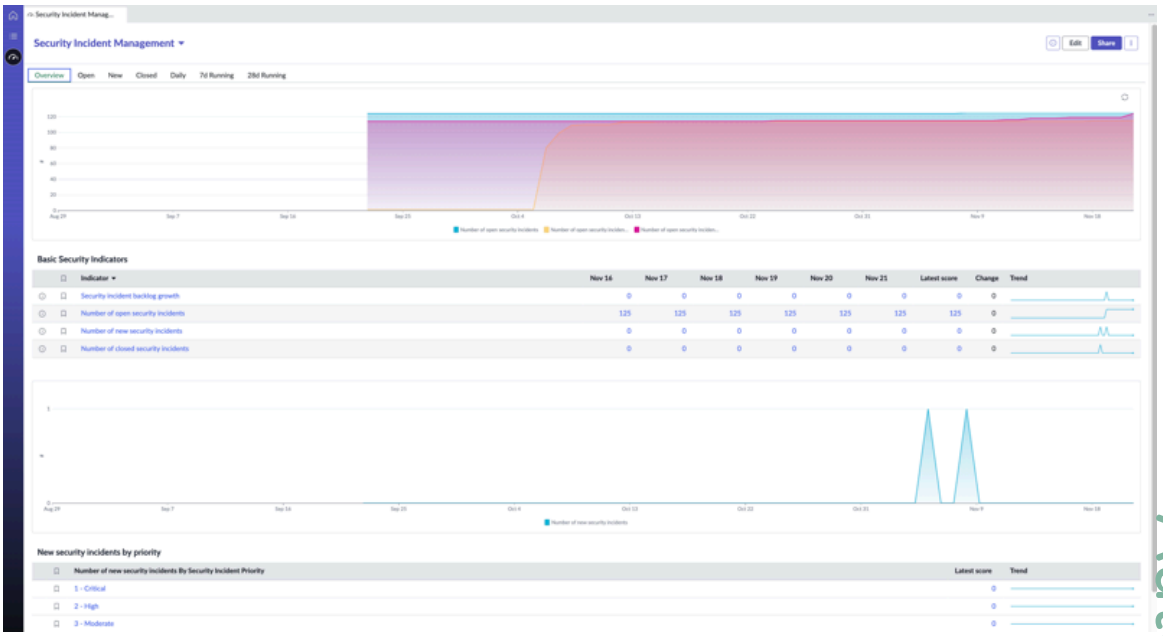
Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“**, das auf der linken Seite der Startseite des Arbeitsbereichs angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Security Incident Management** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie das Dashboard Security Incident Management für weitere Aktionen an. Ausführliche Informationen zum Dashboard für Security Incident-Management finden Sie unter Dashboard für Security Incident-Management

Zeigen Sie das Effizienz-Dashboard von Security Operations an

SOC-Manager (Security Operations Center) können allgemeine Effizienzmetriken anzeigen und die individuelle Leistung der SOC-Teammitglieder in der Organisation messen.

Vorbereitungen

In der aktuellen Version wird der folgende Bericht im Dashboard für die Effizienz von Security Operations nicht unterstützt:

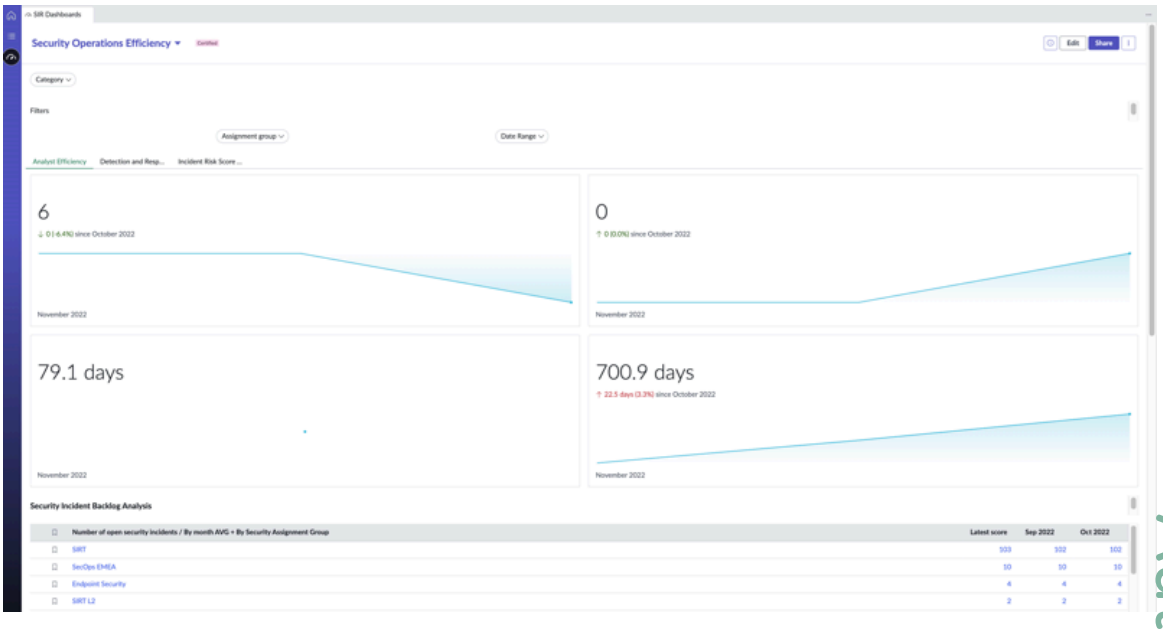
- „Analyse der Security Incident-Phase – Workbench“ ist nicht verfügbar

Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (schreiben)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“**, das auf der linken Seite der Startseite des Arbeitsbereichs angezeigt wird.
3. Wählen Sie **Effizienz von Security Operations** in der Dropdown-Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie das Effizienz-Dashboard von Security Operations an, um weitere Aktionen anzuzeigen. Ausführliche Informationen zum Dashboard für die Effizienz von Security Operations finden Sie unter Dashboard für die Effizienz von Security Operations

Zeigen Sie das KPI-Dashboard „Security Incident Response Premium“ an

Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung nachverfolgen und anzeigen.

Vorbereitungen

Im aktuellen Release wird die folgende Liste von Berichten im Dashboard „Security Incident Response Premium KPIs“ nicht unterstützt:

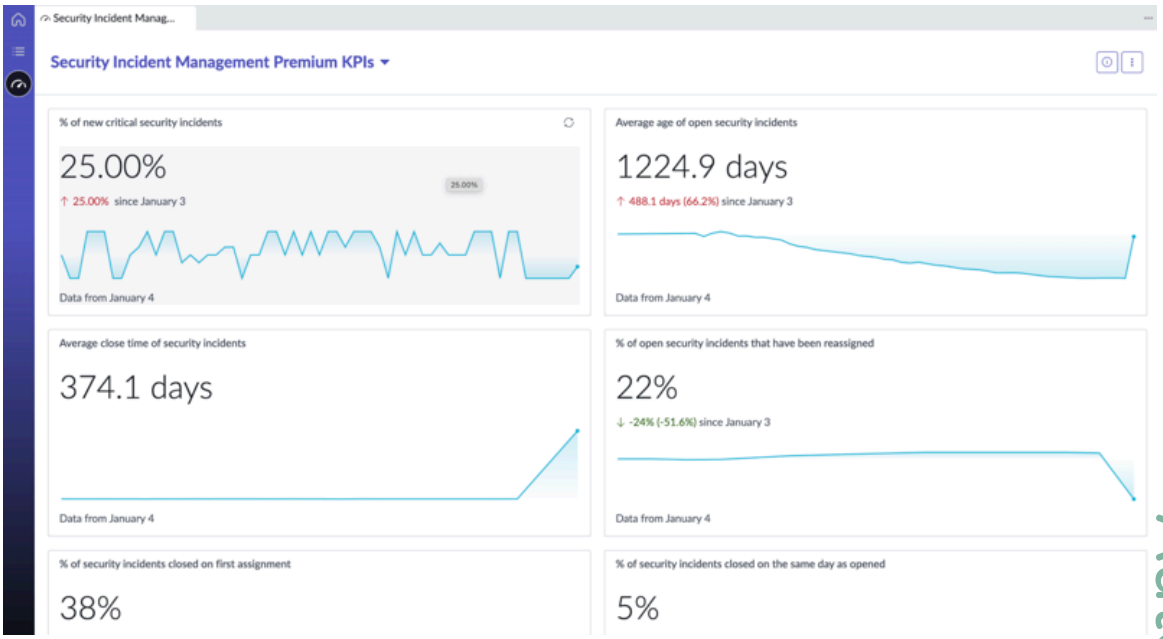
- Nach Status verarbeiten – Workbench ist nicht verfügbar
- Nach Alter verarbeiten – Workbench ist nicht verfügbar
- Security Incidents, die mehr als 30 Tage offen sind, nach Zuweisungsgruppe und Status – Heatmap-Visualisierung ist nicht verfügbar.
- Security Incidents, die nach Zuweisungsgruppe und Status nicht mehr als 30 Tage aktualisiert wurden – Heatmap-Visualisierung ist nicht verfügbar.
- Security Incidents mit Beauftragtem, der nicht aktiv ist: Heatmap-Visualisierung ist nicht verfügbar.

Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (schreiben)

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“**, das auf der linken Seite der Startseite des Arbeitsbereichs angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Security Incident Response Premium-KPIs** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie das KPI-Dashboard von Security Incident Response Premium an, um weitere Aktionen anzuzeigen.
   Ausführliche Informationen zum KPI-Dashboard „Security Incident Response Premium“ finden Sie unter Security Incident Management Premium-Dashboard

Zeigen Sie das Dashboard für kontextbezogene Analysen - SI an

Mit diesem Dashboard können Manager und Analysten die offenen Security Incidents, das durchschnittliche Alter der offenen Security Incidents, die durchschnittliche Abschlusszeit von Security Incidents, den Prozentsatz der Security Incidents, die am selben Tag geöffnet und geschlossen wurden, und den Prozentsatz der anzeigen Incidents, die in den letzten 5 Tagen und 30 Tagen nicht aktualisiert wurden.

Vorbereitungen

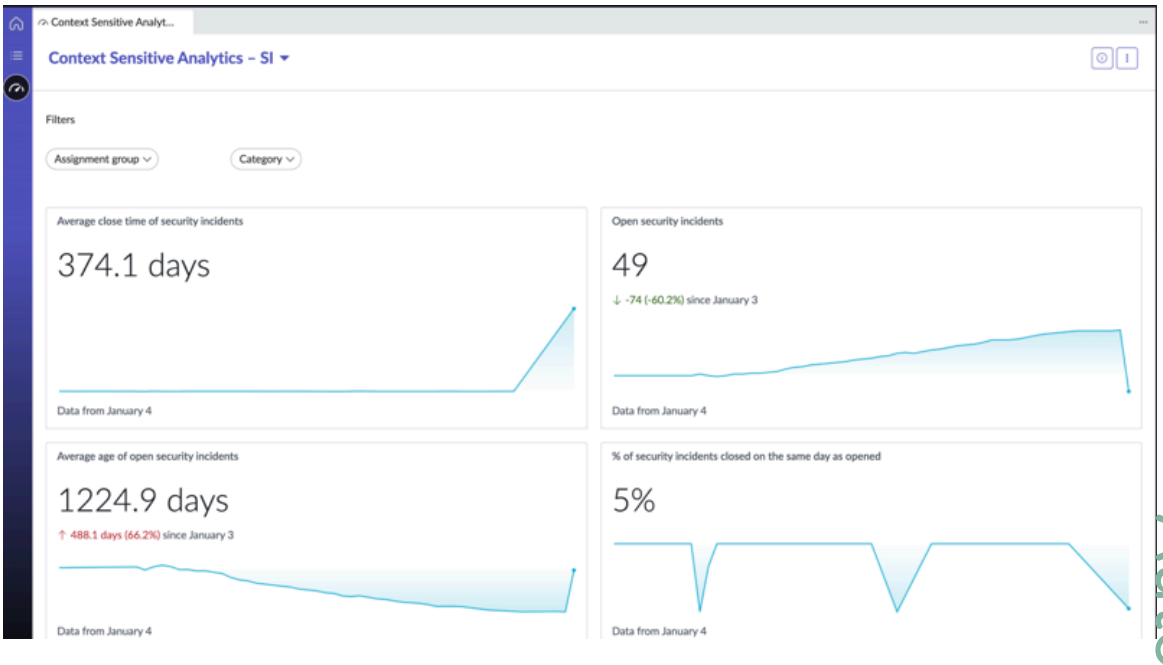
Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (schreiben)

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“**, das auf der linken Seite der Startseite des Arbeitsbereichs angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Kontextsensible Analysen – SI** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie das Dashboard „Kontextbezogene Analysen – SI“ für weitere Aktionen an.

CISO-Dashboard anzeigen

Dieses Dashboard bietet den Chief Information Security Officers (CISOs) einen allgemeinen Überblick über Security Incidents und wöchentliche Incident-Trends in der Instanz in Form von grafischen Diagrammen. Mit diesen Diagrammen können Sie die Leistung des Security Operations Center (SOC) effektiv anzeigen und analysieren.

Vorbereitungen

- Erforderliche Rolle: sn_si.admin und sn_si.cso: Incidents bearbeiten und anzeigen.
- Stellen Sie sicher, dass die App Performance Analytics for Security Incident Response installiert ist.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Das CISO-Dashboard und das CISO-Übersichts-Dashboard waren in der klassischen Anwenderoberfläche zwei verschiedene. Jetzt wurden die Funktionen der beiden Dashboards jedoch unter dem CISO-Dashboard zusammengeführt.

Das CISO-Dashboard bietet wöchentlich wichtige Einblicke zu Ihren Security Incidents. Sie können Indikatoren einrichten und Daten-Snapshots der Incidents sammeln, die den Bedingungen in den Indikatoreigenschaften entsprechen. Die gesammelten Daten werden dann mithilfe von Widgets im Dashboard visualisiert.

Sie können die wöchentlichen Trends mithilfe der Widgets im CISO-Dashboard visualisieren. Die Daten oder Statistiken für die Trends Ihrer Security Incidents werden aus den Eigenschaften des wöchentlichen Incident-Indikators gesammelt, die von der Organisation definiert werden. Mit den folgenden Diagrammen können Sie wichtige Einblicke gewinnen:

Automatische Übersetzung

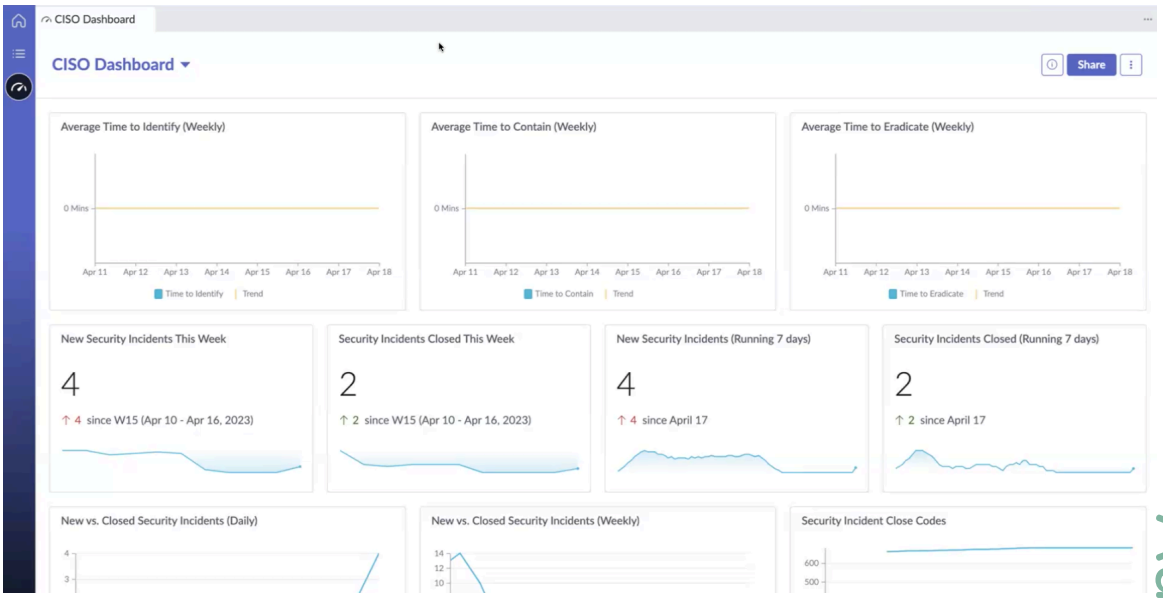
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Durchschnittliche Zeit für Identifizierung (wöchentlich)**: Dieses Diagramm veranschaulicht die durchschnittliche wöchentliche Zeit, die für die Identifizierung eines Security Incident benötigt wird.
- **Durchschnittliche Zeit bis zur Eindämmung (wöchentlich)**: Dieses Diagramm veranschaulicht die durchschnittliche wöchentliche Zeit, die für die Eindämmung eines Security Incident benötigt wird.
- **Durchschnittliche Zeit bis Beseitigung (wöchentlich)**: Dieses Diagramm veranschaulicht die durchschnittliche wöchentliche Zeit, die für die Beseitigung eines Security Incident benötigt wird.
- **Neue Security Incidents diese Woche**: Dieses Diagramm zeigt die Anzahl der neuen Security Incidents in dieser Woche.
- **Diese Woche geschlossene Security Incidents**: Dieses Diagramm zeigt die Anzahl der in dieser Woche geschlossenen Security Incidents.
- **Neue Security Incidents (Ausführung 7 Tage)**: Dieses Diagramm veranschaulicht die Anzahl der neuen Security Incidents, die für eine Woche ausgeführt werden.
- **Geschlossene Security Incidents (Ausführung 7 Tage)**: Dieses Diagramm veranschaulicht die Anzahl der neuen Security Incidents, die geschlossen sind, aber für eine Woche ausgeführt werden.
- **Neue vs. geschlossene Incidents (täglich)**: Dieses Diagramm veranschaulicht den Vergleich zwischen den täglichen neuen Security Incidents und den täglichen geschlossenen Security Incidents.
- **Neue vs. geschlossene Incidents (wöchentlich)**: Dieses Diagramm veranschaulicht den Vergleich zwischen den wöchentlichen neuen Security Incidents und den wöchentlich geschlossenen Security Incidents.
- **Geschlossen-Codes für Security Incident**: Dieses Diagramm veranschaulicht die Geschlossen-Codes der Security Incidents.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“** auf der linken Seite der Startseite des -Arbeitsbereichs.
3. Wählen Sie in der Dropdown-Liste **CISO-Dashboard** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie das CISO-Dashboard für weitere Aktionen an.

Zeigen Sie das Dashboard mit der Übersicht über das CISO-Reporting an

Dieses Dashboard bietet den Chief Information Security Officers (CISOs) eine allgemeine Berichtsübersicht über die Security Incidents und wöchentlichen Incident-Trends in der Instanz in Form von grafischen Diagrammen. Mit diesen Diagrammen können Sie die Leistung des Security Operations Center (SOC) effektiv anzeigen und analysieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin und sn_si.cso: Incidents bearbeiten und anzeigen.

Warum und wann dieser Vorgang ausgeführt wird
Das Dashboard „CISO Reporting Übersicht“ bietet wöchentlich wichtige Einblicke zu Security Incidents, und Sie können die wöchentlichen Trends mithilfe von Widgets visualisieren. Mit den folgenden Diagrammen können Sie wichtige Einblicke in die CISO-Berichterstellung gewinnen:

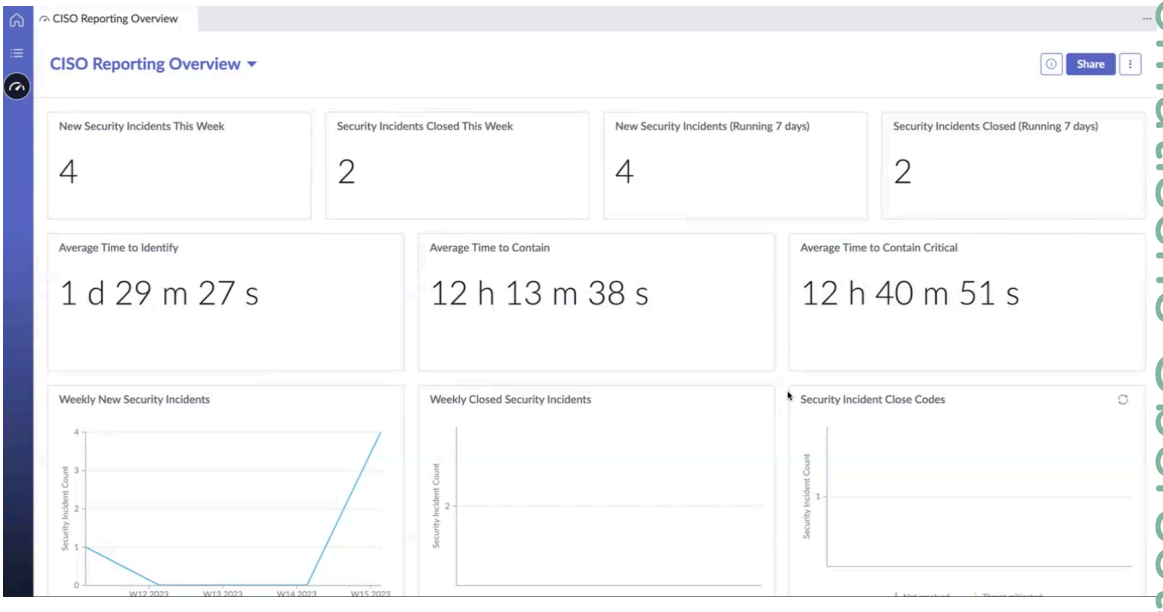
- **Neue Security Incidents diese Woche**: Auf dieser Kachel wird der Bericht zur Anzahl der neuen Security Incidents in dieser Woche angezeigt.
- **Diese Woche geschlossene Security Incidents**: Auf dieser Kachel wird der Bericht zur Anzahl der in dieser Woche geschlossenen Security Incidents angezeigt.
- **Neue Security Incidents (Ausführung 7 Tage)**: Auf dieser Kachel wird der Bericht zur Anzahl der neuen Security Incidents angezeigt, die für eine Woche ausgeführt werden.
- **Geschlossene Security Incidents (Ausführung 7 Tage)**: Auf dieser Kachel wird der Bericht zur Anzahl der neuen geschlossenen Security Incidents angezeigt, die für eine Woche ausgeführt werden.
- **Durchschnittliche Zeit bis Identifizierung**: Auf dieser Kachel wird der Bericht zur durchschnittlichen wöchentlichen Zeit angezeigt, die für die Identifizierung von Security Incidents benötigt wird.
- **Durchschnittliche Zeit bis zur Eindämmung**: Auf dieser Kachel wird der Bericht über die durchschnittliche wöchentliche Zeit angezeigt, die für die Eindämmung von Security Incidents benötigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Durchschnittliche Zeit bis zur Eindämmung kritischer Incidents**: Auf dieser Kachel wird der Bericht zur durchschnittlichen wöchentlichen Zeit angezeigt, die für die Eindämmung kritischer Security Incidents benötigt wird.
- **Wöchentliche neue Security Incidents**: Dieses Diagramm veranschaulicht den Bericht der wöchentlichen neuen Security Incidents.
- **Wöchentliche geschlossene Security Incidents**: Dieses Diagramm veranschaulicht den Bericht der wöchentlich geschlossenen Security Incidents.
- **Lösungscodes für Security Incident**: Dieses Diagramm veranschaulicht den Bericht mit den Lösungscodes der Security Incidents.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“** auf der linken Seite der Homepage des -Arbeitsbereichs.
3. Wählen Sie in der Dropdown-Liste **CISO Reporting Übersicht** aus.



4. Zeigen Sie das CISO Reporting-Dashboard für weitere Aktionen an.

Automatische Übersetzung

Zeigen Sie das Security Incident Manager-Übersichts-Dashboard an

Dieses Dashboard bietet Managern einen allgemeinen Überblick über die Security Incidents mit kritischer Priorität oder hoher Priorität auf Teamebene, SLAs, die in 24 Stunden ablaufen, und wöchentliche Incident-Trends in der Instanz in Form von Berichten und grafischen Diagrammen.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin: Dashboard zum Bearbeiten und Anzeigen.
- sn_si.manager: Dashboard anzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Security Incidents mit kritischer oder hoher Priorität oder SLAs, die sofortige Aufmerksamkeit erfordern, analysieren. Sie können die wöchentlichen Trends auch mithilfe der Widgets im Dashboard „Übersicht über Security Incident Manager“ visualisieren.

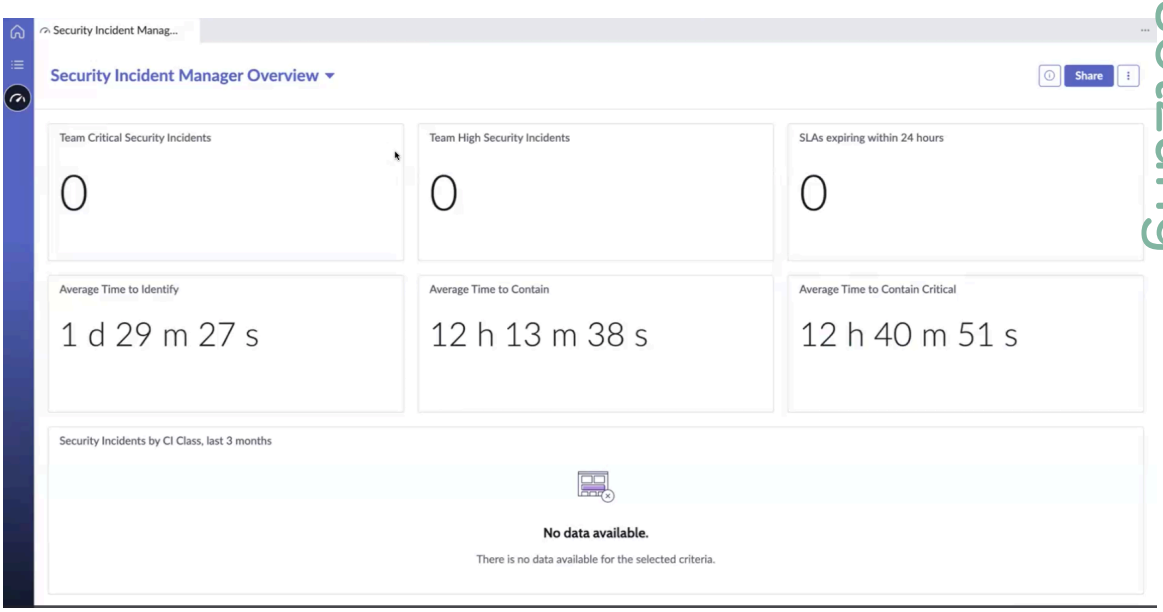
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Daten oder Statistiken für die wöchentlichen oder monatlichen Trends Ihrer Security Incidents werden aus den von der Organisation definierten Incident-Tabellen gesammelt. Mit den folgenden Diagrammen können Sie wichtige Einblicke gewinnen:

- **Kritische Security Incidents im Team**: Diese Kachel zeigt die Anzahl der kritischen Security Incidents für das Team in dieser Woche an.
- **Team Incidents mit hoher Sicherheit**: Diese Kachel zeigt die Anzahl der Incidents mit hoher Sicherheit für das Team in dieser Woche an.
- **SLAs, die in 24 Stunden ablaufen**: Diese Kachel zeigt die Anzahl der SLAs an, die innerhalb von 24 Stunden ablaufen.
- **Durchschnittliche Zeit bis Identifizierung**: Diese Kachel zeigt die durchschnittliche wöchentliche Zeit bis zur Identifizierung von Security Incidents an.
- **Durchschnittliche Zeit bis zur Eindämmung**: Diese Kachel zeigt die durchschnittliche wöchentliche Zeit bis zur Eindämmung von Security Incidents an.
- **Durchschnittliche Zeit bis zur Eindämmung kritischer Incidents**: Auf dieser Kachel wird die durchschnittliche wöchentliche Zeit angezeigt, die für die Eindämmung kritischer Security Incidents benötigt wird.
- **Security Incident nach CI-Klasse, letzte 3 Monate**: Dieses Diagramm veranschaulicht die Trends aller Security Incidents basierend auf der CI-Klasse für die letzten drei Monate.
- **Trend aller Security Incidents nach Kategorie**: Dieses Diagramm veranschaulicht die Trends aller Security Incidents basierend auf der Kategorie.
- **Trend aller Security Incidents nach Priorität**: Dieses Diagramm veranschaulicht die Trends aller Security Incidents basierend auf der Priorität.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **„SIR-Dashboards“** auf der linken Seite der Homepage des -Arbeitsbereichs.
3. Wählen Sie in der Dropdown-Liste **Security Incident Manager Übersicht** aus.



4. Zeigen Sie die Security Incident Manager-Übersicht an, um weitere Aktionen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie das Dashboard Security Incident Response Health an

Die Dashboard-Funktion Security Incident Response Health bietet eine zentralisierte Ansicht kritischer Aspekte im Zusammenhang mit der Implementierung des Prozesses zur Reaktion auf Incidents, aufgetretenen Problemen/Fehlern und Leistungsmetriken. Es dient als wichtiges Tool zur Überwachung und Optimierung der Effektivität der Fähigkeiten einer Organisation zur Reaktion auf Security Incidents.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst oder sn_si.analytics_read – Dashboard anzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Integrität der Security Incidents mithilfe der Widgets und Trenddiagramme für die einzelnen Anwendungen überwachen. Diese Statistiken stellen eine umfassende Integritätspunktzahl dar, die den Konfigurationsstatus und die Effektivität der Remediation in SIR-Anwendungen beschreibt. Das Security Incident Response Health-Dashboard unterstützt die folgenden vier Registerkarten:

- **Prozess**: Die Registerkarte zeigt eine Zusammenfassung aller Incidents aus verschiedenen Warnungssensoren, die wöchentlich gruppiert sind.
- **Implementierung**: Auf dieser Registerkarte werden die Anpassungen angezeigt, die Kunden in ihren Instanzen vornehmen, einschließlich Skripteinbindungen, Geschäftsregeln, Flows und Upgrades.
- **Probleme/Fehler**: Auf der Registerkarte werden Widgets angezeigt, die Fehler in Integrationsprozessen, Diskrepanzen bei der Erfassung von Rohdaten zu Incidents, ausgehende HTTP-Fehler in SIR-Anwendungen und Probleme bei der Ausführung von Playbooks hervorheben.
- **Leistung**: Auf dieser Registerkarte werden die Leistungsprobleme in den SIR-Anwendungen angezeigt, einschließlich Verlangsamungen bei Leistungsabfragen, Business-Regeln und Skripts.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen Sie auf der Homepage des SIR-Arbeitsbereichs das Symbol **SIR-Dashboards**.
3. Wählen Sie in der Dropdown-Liste **Security Incident Response-Integritäts-Dashboard** aus.
4. Wählen Sie die Registerkarte **Prozess** aus, um die Anzahl der Security Incidents anzuzeigen, die wöchentlich für jeden Warnungssensor im Diagramm ausgelöst wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Prozess“.

Sie können die folgenden Aufgaben ausführen:

a. Wählen Sie einen Warnungssensor im Diagramm aus, um die KPI-Details der Anzahl der Security Incidents anzuzeigen, die in einer Woche durch Warnungssensoren ausgelöst wurden.

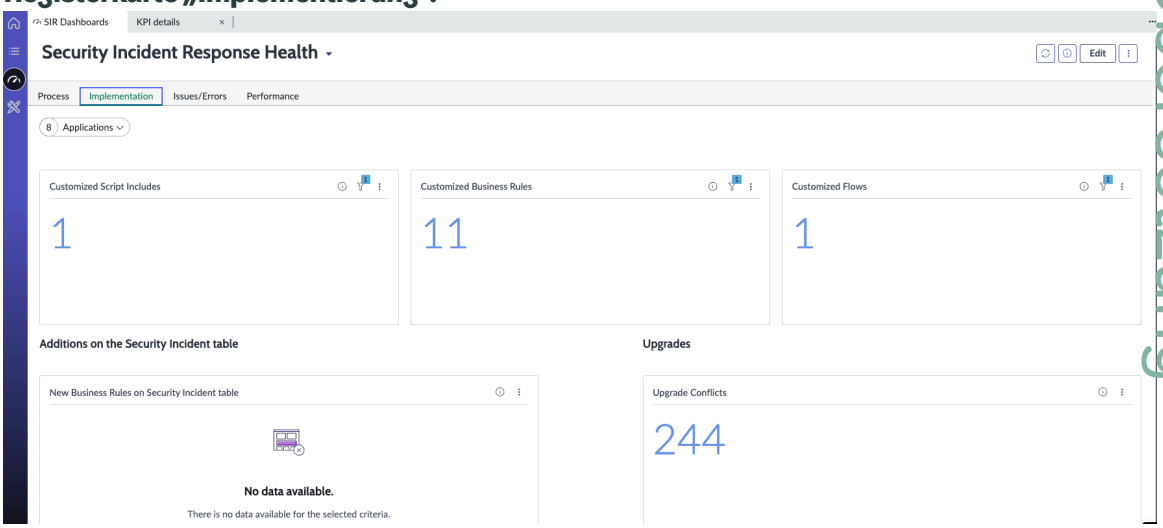
b. Um die KPI-Details für eine bestimmte Woche abzurufen, verwenden Sie die Option **Kalender**.

c. Um die vom Warnungssensor ausgelösten Security Incidents zu vergleichen, wählen Sie die Option **Datensätze vergleichen**.

d. Um den Diagrammtyp, Zeitreihen oder Analysen zu verwenden, wählen Sie die **Diagrammoptionen**aus.

5. Wählen Sie die Registerkarte **Implementierung** aus, um die Anzahl der Anpassungen anzuzeigen, die für die Security Incidents in Security Incident Response-Anwendungen erstellt wurden.

Registerkarte „Implementierung“.



Registerkarte**„Implementierung** “:

Sie können das zusammengefasste Dashboard für die Anzahl der Anpassungen anzeigen, die für jede Anwendung von Incident Response erstellt wurden.

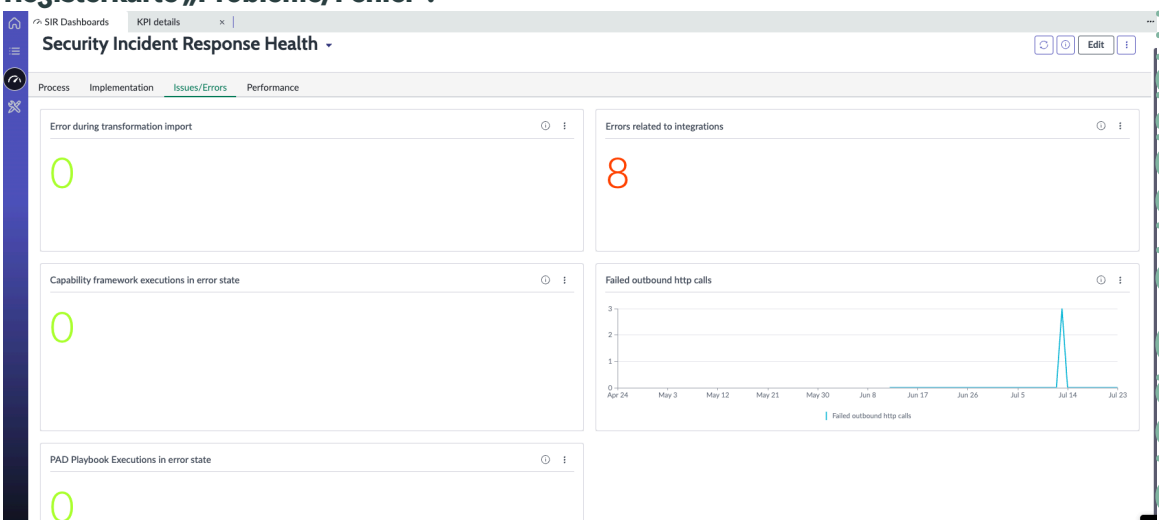
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Anwenderdefinierte Skripteinbindungen**: Dieses Widget zeigt die Anzahl der anwenderdefinierten Skripts an, die basierend auf Ihren Anforderungen in den SIR-Anwendungen hinzugefügt wurden.
- **Anwenderdefinierte Business-Regeln**: Dieses Widget zeigt die Anzahl der anwenderdefinierten Business-Regeln an, die basierend auf Ihren Anforderungen in den SIR-Anwendungen hinzugefügt wurden.
- **Anwenderdefinierte Flows**: Dieses Widget zeigt die Anzahl der anwenderdefinierten Flows an, die basierend auf Ihren Anforderungen in den SIR-Anwendungen hinzugefügt wurden.
- **Neue Business-Regel in Tabelle „Security Incident“**: Dieses Widget zeigt die Anzahl der Business-Regeln an, die in der Tabelle „Security Incident“ erstellt wurden.
- **Upgrade-Konflikte**: Dieses Widget zeigt die Anzahl der Konflikte an, die während Upgrades in den SIR-Anwendungen ausgelöst wurden.

6. Wählen Sie die Registerkarte **Probleme/Fehler,** um die Anzahl der Probleme oder Fehler anzuzeigen, die in Security Incident Response-Anwendungen ausgelöst wurden.

Registerkarte „Probleme/Fehler“.



Registerkarte**„Probleme/Fehler“** :

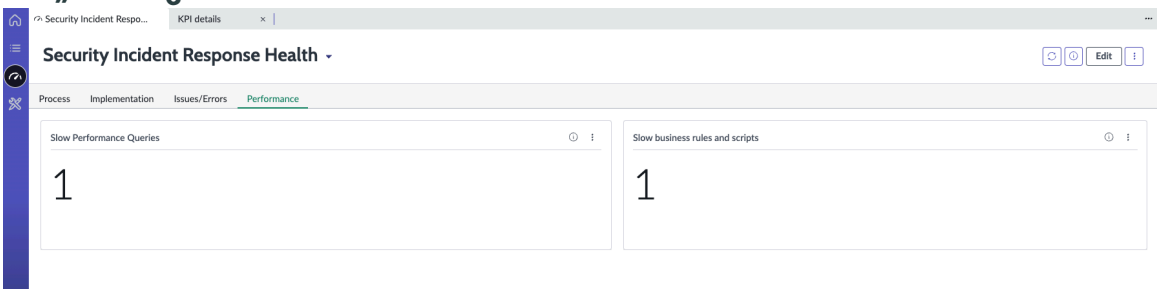
Sie können das aggregierte Dashboard für Probleme oder Fehler in Security Incident Response-Anwendungen anzeigen.

- **Fehler beim Transformationsimport**: Dieses Widget zeigt die Anzahl der Fehler an, die während des Transformationsimports in SIR-Anwendungen ausgelöst wurden.
- **Fehler im Zusammenhang mit Integrationen**: Dieses Widget zeigt die Anzahl der Fehler an, die während der SIR-Integrationen ausgelöst wurden.
- **Fähigkeits-Framework-Ausführungen im Fehlerstatus**: Dieses Widget zeigt die Anzahl der Fehler an, die während der Ausführungen des Fähigkeits-Frameworks in SIR-Anwendungen ausgelöst wurden.
- **Fehlgeschlagene ausgehende HTTP-Aufrufe**: Dieses Widget zeigt die Anzahl der fehlgeschlagenen ausgehenden HTTP-Aufrufe an, die in den SIR-Anwendungen ausgelöst wurden.
- **PAD Playbook-Ausführungen im Fehlerstatus**: Dieses Widget zeigt die Anzahl der PAD Playbook-Ausführungsfehler an, die in den SIR-Anwendungen ausgelöst wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie die Registerkarte **Performance**, um die Anzahl der Leistungsprobleme anzuzeigen, die in Security Incident Response-Anwendungen ausgelöst wurden.

Tab „Leistung“



Registerkarte „**Leistung“** :

Sie können das aggregierte Dashboard für Leistungsprobleme in Security Incident Response-Anwendungen anzeigen.

- **Langsame Leistungsabfragen**: Dieses Widget zeigt die Anzahl der Leistungsabfragen in den SIR-Anwendungen an, deren durchschnittliche Ausführungszeit mehr als 10 ms beträgt und bei mindestens 1000 Ausführungen gemittelt wird.
- **Langsame Business-Regeln und Skripts**: Dieses Widget zeigt die Anzahl der Business-Regeln und Skripts in den SIR-Anwendungen an, deren durchschnittliche Ausführungszeit mehr als 10 ms beträgt und deren Durchschnitt bei 1000 oder mehr Ausführungen liegt.

8. Sie können das Symbol **Aktualisieren** verwenden, um die Daten im Dashboard Security Incident Response Health zu aktualisieren.
9. Über das Symbol **Dashboard-Details anzeigen** können Sie die Details des Dashboards Security Incident Response Health anzeigen.
10. Mit der Option **Bearbeiten** können Sie die Details des Dashboards Security Incident Response Health ändern.
11. Über die Option **Mehr** können Sie im Dashboard Security Incident Response Health zusätzliche Aktionen ausführen.

Erstellung von Security Incidents

Security Incidents können manuell über das -Formular oder automatisch über Sicherheitsereignisse erstellt werden, die von integrierten Warnungsüberwachungstools von Drittanbietern wie Splunk empfangen werden.

Wichtig:
Die neuesten Funktionen in Security Incident Response sind ausschließlich in Arbeitsbereich für Security Incident Responseverfügbar. Installieren oder aktualisieren Sie auf die neueste Version Security Incident Response oder Arbeitsbereich für Security Incident Response, um auf Funktionen wie Schichtübergabe, Risikobewertungsrechner usw. zuzugreifen und sie zu nutzen.

Wenn Sie über eine Sicherheitsrolle verfügen, können Sie eine der folgenden Methoden verwenden, um Security Incidents manuell zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methoden zum manuellen Erstellen von Security Incidents

Methode	Beschreibung
Manuell aus der Security Incident-Liste erstellt	Klicken Sie in der Liste „Security Incident“ auf **Neu**, um einen neuen Security Incident zu erstellen.
Manuell aus dem Security Incident-Katalog erstellt	Sie können Security Incidents erstellen, indem Sie aus Kategorien von Sicherheitsbedrohungen auswählen, die im Security Incident-Katalog definiert sind.
Incident-Management	Klicken Sie im Formular „Incident“ in Incident Management **auf Sicherheits-Incident erstellen**, um einen neuen Security Incident zu erstellen.
Manuell konvertiert aus einer Sicherheitsanforderung	Klicken Sie im Formular „Sicherheitsanforderung **“ auf In Security Incident konvertieren**, um einen neuen Security Incident zu erstellen.
Manuell aus einer Ereignismanagement-Warnung erstellt	Klicken Sie im Formular „Ereignismanagement-Warnungen **“ auf Security Incident erstellen**, um einen neuen Security Incident aus einer Warnung zu erstellen.
Manuell aus einer Warnung erstellt	Klicken Sie im Formular „Ereignismanagement-Warnung“ **auf Sicherheits-Incident erstellen**, um einen neuen Security Incident zu erstellen.
Manuell aus einem Schwachstellen-Datensatz konvertiert (wenn das Plugin „Vulnerability Response“ aktiviert ist)	Klicken Sie im Formular „Angreifbare Elemente“ **auf Security Incident erstellen**, um einen neuen Security Incident zu erstellen.

Automatisierte Erstellung von Security Incidents

Im Allgemeinen sind Sicherheitsadministratoren für die Einrichtung von Warnungsregeln verantwortlich, die zur automatischen Generierung von Security Incidents verwendet werden.

Sicherheitsadministratormethode zum Erstellen von Security Incidents

Methode	Beschreibung
Automatisch anhand von Warnungsregeln erstellt	Security Incidents können basierend auf Warnungsregeln erstellt werden, die in der Anwendung Ereignismanagement in Ihrem Rechenzentrum definiert sind.

Manuelle Erstellung von Security Incidents

Security Incidents können Sie über das Formular „Security Incident“ sowie über mehrere andere Formulare erstellen.

Sie können Security Incidents basierend auf einem vorhandenen Datensatz in den folgenden Formularen erstellen:

- Über eine beliebige Liste mit Security Incidents
- Incident-Formular
- Ereignismanagement Warnungsformular
- Formular „Angreifbare Elemente“.
- Sicherheitsanforderungsformular

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Security Incident aus der Liste Security Incident

Zusätzlich zu den automatischen Methoden zur Erstellung von Security Incidents können Sie sie bei Bedarf auch manuell erstellen.

Dieses Video zeigt eine visuelle Übersicht darüber, wie Sie einen Security Incident aus der Security Incident-Liste erstellen können.

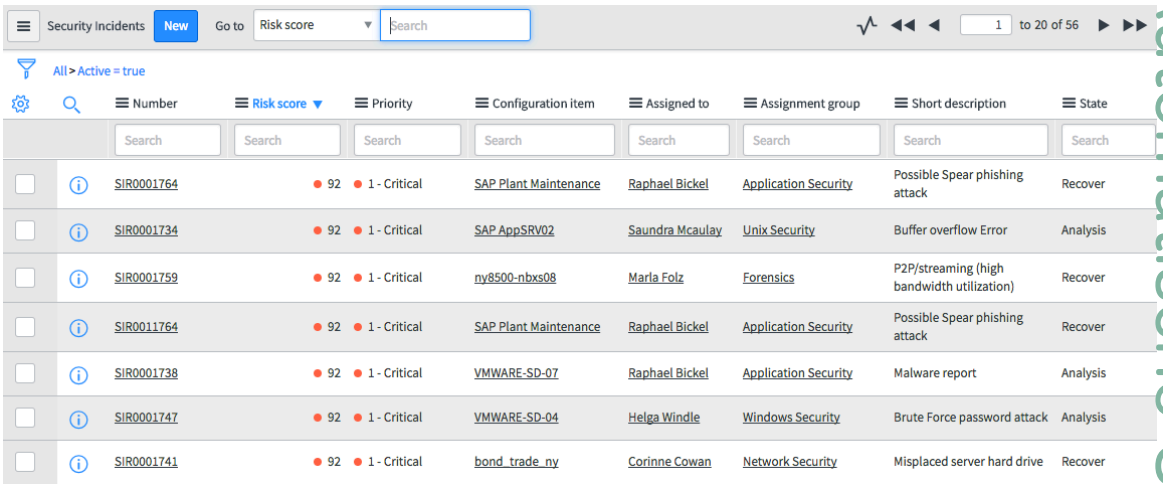
Erstellen Sie einen Security Incident aus der Liste Security Incident

Vorbereitungen

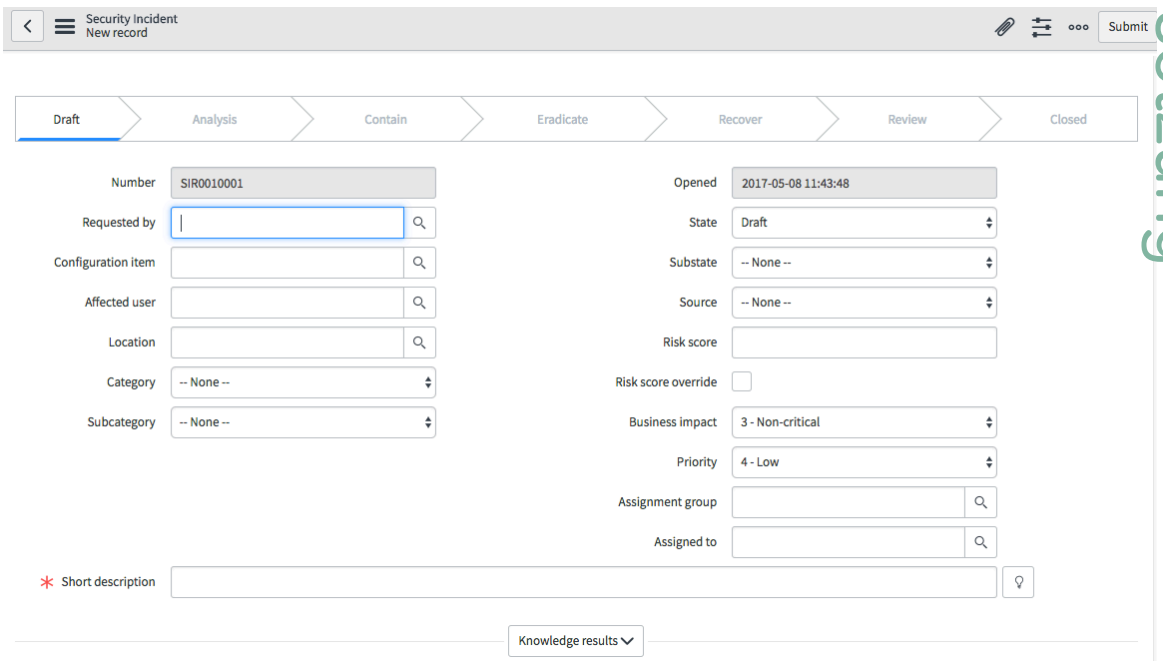
Erforderliche Rolle: sn_si.basic

Prozedur

1. Navigieren Sie zu einer beliebigen Liste der Security Incidents (z. B. **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**) an.



2. Klicken Sie auf **Neu**.



3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sicherheits-Tag auswählen	Wählen Sie bei Bedarf ein Sicherheits-Tag aus, um dem Datensatz Metadaten hinzuzufügen oder anzugeben, wer Zugriff auf diesen Security Incident-Datensatz haben soll. Dieses Feld wird nur angezeigt, nachdem der Security Incident gespeichert wurde.
Nummer	[Schreibgeschützt] Die Nummer des Security Incidents.
Angefordert von	Die Person, die die auszuführende Arbeit anfordert.
Konfigurationselement	Der Server, Computer, Router oder ein anderes Configuration Item, das bzw. der von dem Sicherheitsproblem betroffen ist.
Betroffener Anwender	Die von dem Sicherheitsproblem betroffene Person.
Standort	Standort der anfordernden Person oder Ressource. Wenn kein **Configuration Item** ausgewählt ist, wird dieses Feld mit dem Standort der anfordernden Person vorab ausgefüllt.
Kategorie	Die Kategorie, die den Typ des Sicherheitsproblems identifiziert Wenn eine Kategorie ausgewählt ist, wird ein Workflow zur Analyse dieses Problems ausgeführt, wenn der Datensatz gespeichert wird. Wenn Sie beispielsweise **Denial of Service**auswählen, wird der Workflow Security Incident – Denial of Service – Vorlage ausgeführt. Weitere Informationen finden Sie unter Workflow-Vorlagen für Security Incident Response.
Unterkategorie	Die Unterkategorie, die das Problem weiter definiert.
Geöffnet	[Schreibgeschützt] Zeigt das Datum und die Uhrzeit an, zu der der Incident geöffnet wurde.
Status	Aktueller Status des Security Incidents. Bei Erstellung eines Security Incident wird dieses Feld standardmäßig auf **Entwurf**gesetzt.
Substatus	Gibt an, ob der Security Incident ein ausstehendes Problem oder einen Change enthält.
Quelle	Identifiziert die Quelle des Security Incidents, z. B. E-Mail, Telefonanruf oder Netzwerküberwachung.
Warnungssensor	Sicherheitsintegration, über die Sie Warnungs- oder Ereignisdaten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen.
Warnungsregel	Die Regel im Sicherheitsprodukt, die die Erstellung dieses Security Incidents ausgelöst hat.
Risikopunktzahl	Zeigt die für diesen Security Incident berechnete Risikopunktzahl an. Der Wert basiert auf der Priorität des Security Incidents, der Art des Security Incidents (Denial of Service, Spear-Phishing oder böswillige Code-Aktivität) und der Anzahl der Quellen, die für einen Indikator eine fehlgeschlagene Reputationspunktzahl ausgelöst haben. Die Risikopunktzahl hilft Analysten bei der Priorisierung der Arbeit mit Security Incidents. Drei Eigenschaften von Security Incidents ermöglichen es Ihnen, einen farbcodierten Punkt zu bestimmen, der neben

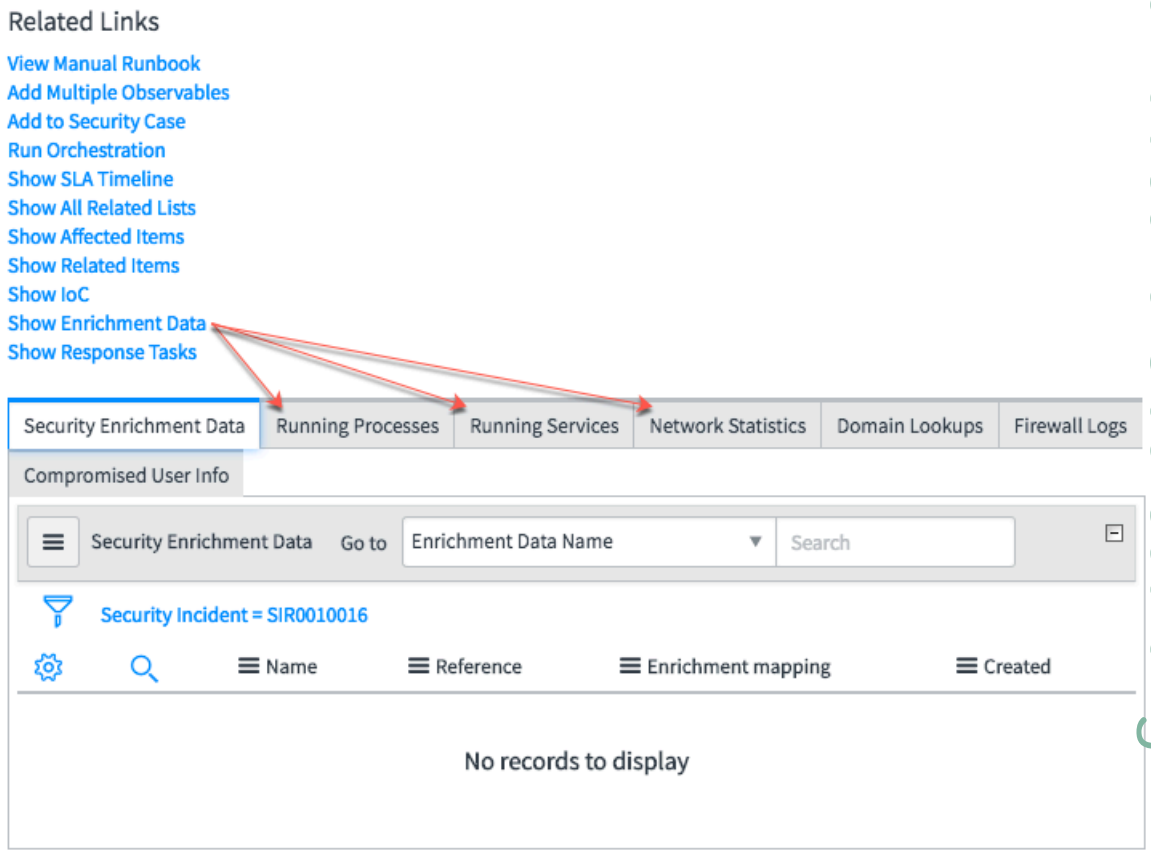
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	der Risikopunktzahl in der Listenansicht angezeigt wird, um sie leichter erkennbar zu machen. Wenn Sie Änderungen an bestimmten Feldern im Security Incident vornehmen, z. B. **Geschäftsauswirkung** oder **Priorität**, und den Datensatz speichern, wird die **Risikopunktzahl** automatisch neu berechnet und angezeigt. Der Change spiegelt sich auch in den Arbeitsnotizen und in der zugehörigen Liste „Risikopunktzahl-Audits“ wider. **Hinweis:** Die Risikopunktzahl wird auch neu berechnet, wenn betroffene Benutzer einem Security Incident, betroffenen Services oder angreifbaren Elementen zugeordnet werden. Sie können auch manuell eine neue **Risikopunktzahl**eingeben. Dies kann nützlich sein, wenn Sie möchten, dass ein bestimmter Security Incident in der Liste der zu analysierenden Security Incidents ganz oben bleibt. Wenn Sie eine neue **Risikopunktzahl**eingeben, wird das Kontrollkästchen **Risikopunktzahl überschreiben** automatisch aktiviert. Unabhängig von den im Security Incident vorgenommenen Änderungen wird eine manuell eingegebene Risikopunktzahl nicht automatisch neu berechnet. **Hinweis:** Wenn Sie Ihre Instanz von einem früheren Release aktualisiert haben, wurden die Risikopunktzahlen für alle Ihre offenen Security Incidents berechnet. Weitere Informationen finden Sie unter Informationen zu Security Incident-Rechnern.
Risikopunktzahlüberschreibung	Aktivieren Sie dieses Kontrollkästchen, um die automatische Aktualisierung der Risikopunktzahl zu überschreiben. Die Überschreibung wird in den Arbeitsnotizen berücksichtigt.
Geschäftsauswirkung	Wählen Sie die Bedeutung dieses Security Incidents für Ihr Unternehmen aus. Der Standardwert ist „Nicht kritisch“. Wenn Sie, nachdem der Security Incident-Datensatz gespeichert wurde, den Wert in den Feldern **Priorität** /oder **Risiko** ändern, wird die **Geschäftsauswirkung** neu berechnet.
Priorität	Wählen Sie die Reihenfolge aus, in der dieser Security Incident behandelt werden soll, basierend auf der Dringlichkeit. Wenn dieser Wert geändert wird, nachdem der Datensatz gespeichert wurde, kann sich dies auf die Berechnung **der Geschäftsauswirkung** auswirken.
Zuweisungsgruppe	Die Gruppe, der dieser Security Incident zugewiesen ist.
Zugewiesen an	Die Person, der die Analyse dieses Security Incident zugewiesen ist. Zuweisungen können manuell oder automatisch durchgeführt werden. Weitere Informationen finden Sie unter Sicherheitsanalysten werden zugewiesen.
Kurzbeschreibung	Kurze Beschreibung des Security Incident.
Wissensergebnisse	Während Sie die Kurzbeschreibung eingeben, werden Links zu zugehörigen Artikeln aus der Knowledge Base angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Das Scannen der Informationen könnte Ihr Problem lösen.

4. Klicken Sie mit der rechten Maustaste auf den Datensatz-Header, und wählen Sie **Speichern**aus.
   Wenn Sie dem Security Incident ein neues CI hinzugefügt haben, werden die folgenden Integrations-Workflows automatisch ausgeführt:
   - Security Operations – Flow für laufende Prozesse abrufen. Dieser Workflow ruft eine Liste der laufenden Prozesse für ein Configuration Item (CI) von einem Host oder Endpunkt ab.
   - Workflow „Security Incident Response - Get Laufende Services“.. Dieser Workflow ruft eine Liste der laufenden Services von Windows-basierten CIs ab.
   - Flow für Security Operations-Integrationen – Netzwerkstatistiken abrufen. Dieser Workflow ruft eine Liste aktiver Netzwerkverbindungen von einem Host oder Endpunkt ab.
5. Um die von diesen Workflows abgerufenen Informationen anzuzeigen, klicken Sie auf den zugehörigen Link **Ergänzungsdaten anzeigen**, und klicken Sie dann auf eine der angegebenen Registerkarten.



Hinweis:
Zusätzliche Workflows werden basierend auf den von Ihnen aktivierten Drittparteiintegrationen wie folgt ausgeführt Security Operations Carbon Black-Integration – Flow zum Abrufen laufender Prozesse

Zugehörige Informationen

Setup von Security Incident Response

Erstellen Sie einen Security Incident aus dem Security Incident-Katalog

Benutzer in Ihrem Unternehmen können den Security Incident-Katalog verwenden, um verschiedene Arten von sicherheitsbezogenen Analysen anzufordern.

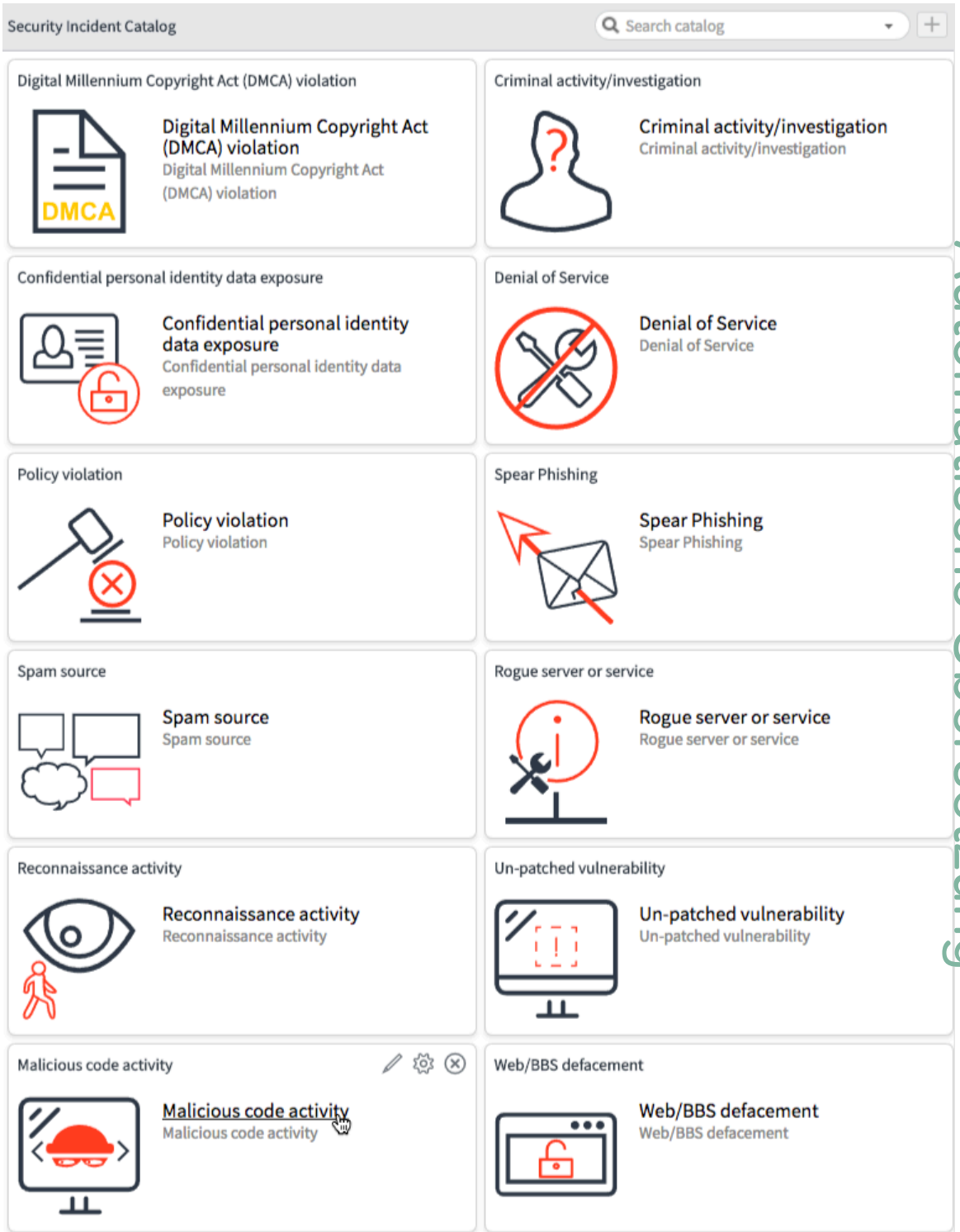
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

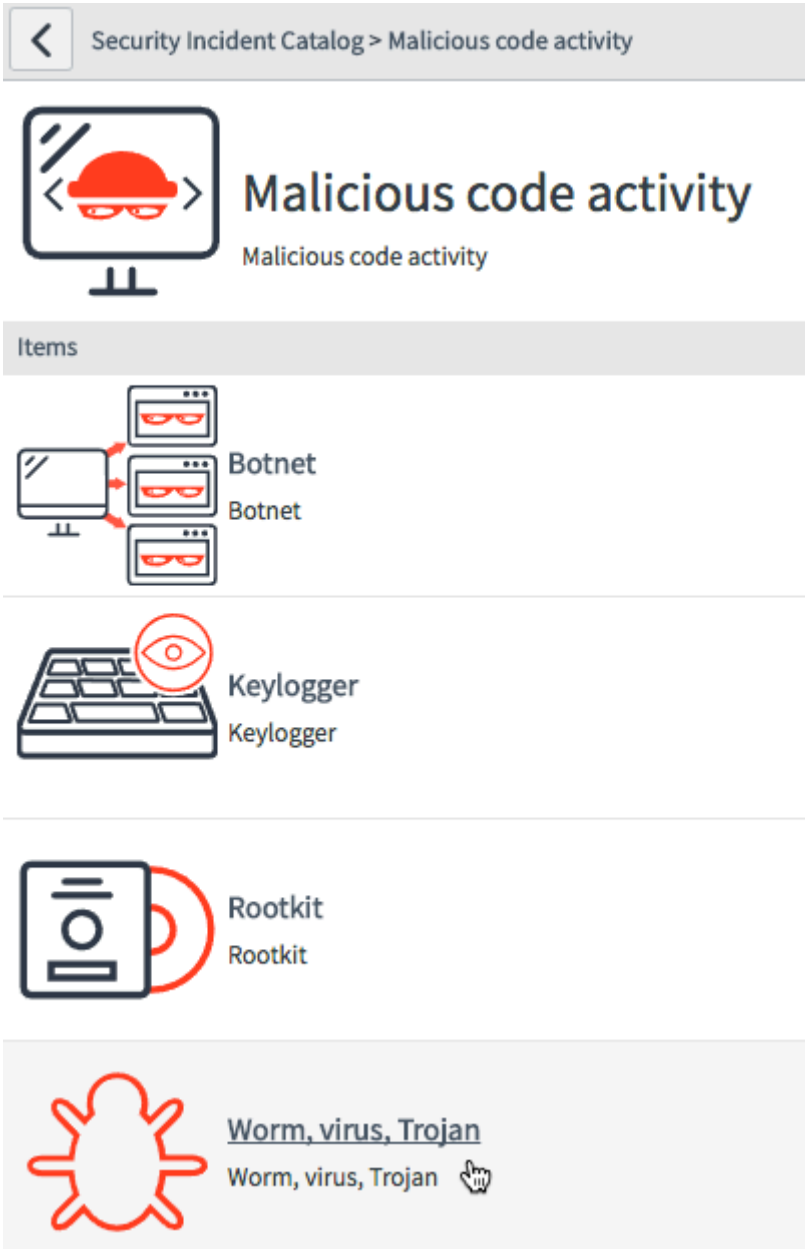
1. Navigieren zu **Alle** > **Selfservice** > **Security Incident-Katalog**.



2. Klicken Sie auf das Katalogelement, für das Sie eine Anforderung stellen möchten.
Wenn das Element, das Sie aus dem Hauptkatalog ausgewählt haben, Unterkategorien enthält, wird die Liste angezeigt. Im folgenden Beispiel wurde **Aktivität „Böswilliger Code“** ausgewählt.

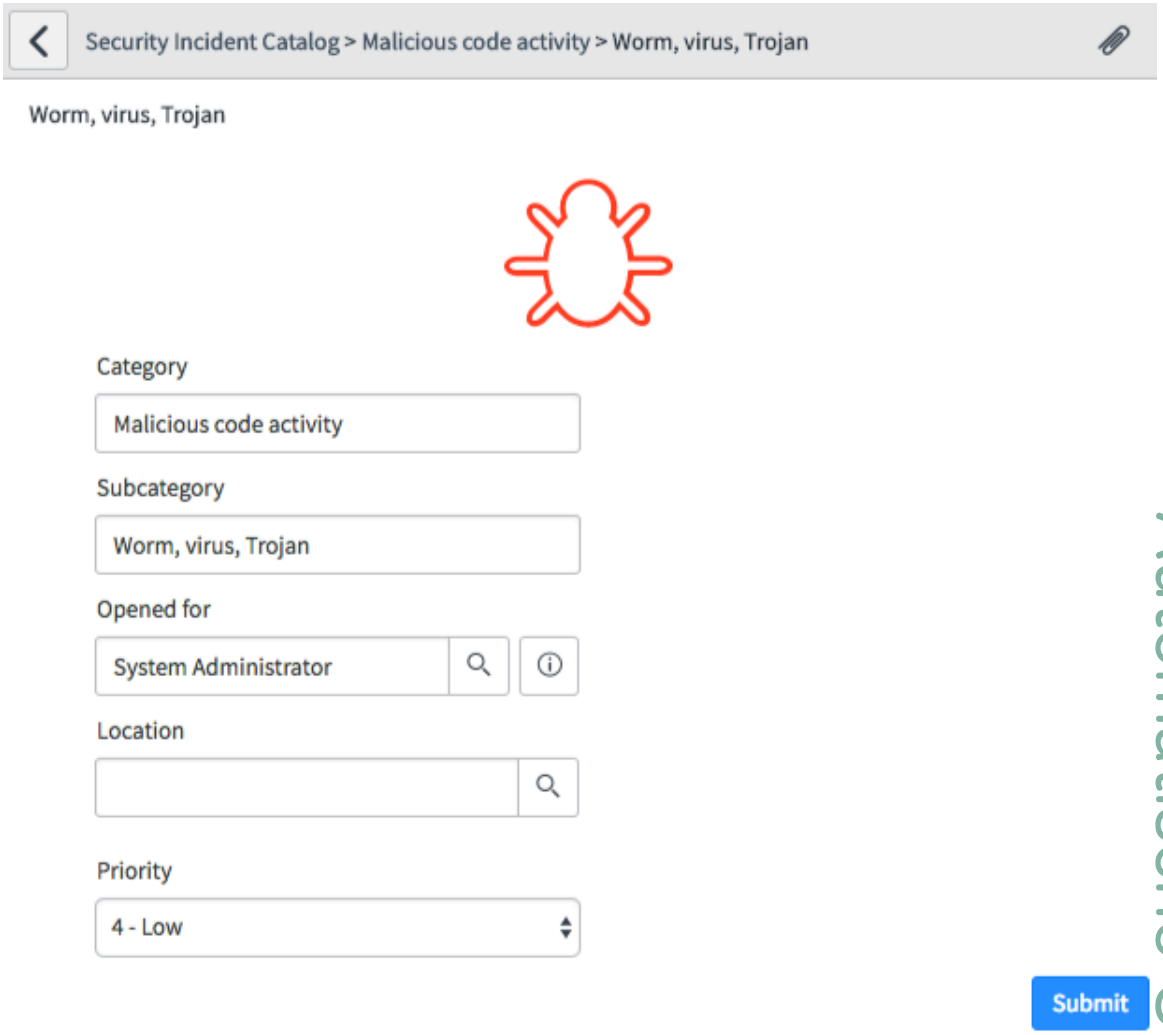
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf die Unterkategorie, die dem Typ der Anforderung, die Sie stellen möchten, am besten entspricht.
In diesem Beispiel wurde die Unterkategorie **Worm, Virus, Trojan (Wurm, Virus, Trojaner)** ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie die Informationen für die Anforderung ein, und klicken Sie auf **Absenden**.
   Die Anforderung wird an die Abteilung für Security Incidents gesendet.
5. Nachdem Sie die Anforderung übermittelt haben, können Sie ihren Fortschritt nachverfolgen, indem Sie zu navigieren **Selfservice** > **Meine Anforderungen**, und geben Sie die Anforderungsnummer ein.

Erstellt einen Security Incident aus einer Ereignismanagement-Warnung

Wenn Ereignismanagement aktiviert ist, können Sie Security Incidents manuell über das Warnungsformular erstellen.

Vorbereitungen

Das Event Management-Plugin erfordert ein separates Abonnement und muss von ServiceNow-Mitarbeitern aktiviert werden. Dieses Plugin enthält Demodaten und aktiviert zugehörige Plugins, wenn sie nicht bereits aktiv sind. Service Analytics wird automatisch aktiviert, wenn Ereignismanagement aktiviert wird.
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie auf die **Nummer** der Warnung.
3. Klicken Sie auf **Security Incident erstellen**.
4. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Erstellung von Security Incidents

Überwachungstools von Drittanbietern wie Splunk können in Security Incident Response integriert werden, sodass aus diesen Tools importierte Sicherheitsereignisse automatisch Security Incidents generieren. Sie können auch Daten aus Drittanbieter-Tools in Sicherheitswarnungen importieren.

Zur Integration von Warnungsüberwachungstools in Security Incident Responsemüssen Sie mit der REST API in die Importtabelle für Security Incidents [sn_si_incident_import] schreiben. Anschließend wird die Importsatz-Quelltabelle mithilfe der **Security Incident Transform-**Transformationszuordnungen Feldern in der Zieltabelle „Security Incident“ [sn_si.incident] zugeordnet.

Wenn Sie versuchen, CI-Datensätze zu importieren, die von der Transformationszuordnung nicht erkannt werden, prüft das Skript der Transformationszuordnung den Datensatz auf Folgendes (in dieser Reihenfolge), um eine Übereinstimmung zu finden:

- sys_id
- CI-Name
- Vollqualifizierter Domänenname
- IP-Adresse

Hinweis:
Wenn Sie feststellen, dass die Transformationszuordnung **für Security Incident-Transformationen** für das von Ihnen verwendete Tool zur Überwachung von Drittanbieterwarnungen nicht ausreicht, duplizieren Sie die Transformationszuordnung, erstellen Sie eine neue, und bearbeiten Sie die Felder nach Bedarf.

Aus Events und Warnungen erstellte Security Incidents

Wenn Ereignisse aus Warnungsüberwachungstools importiert werden, werden sie zuerst von Ereignismanagement verarbeitet und in Warnungen gruppiert. Diese Warnungen können verwendet werden, um Security Incidents basierend auf anpassbaren Warnungsregeln zu erstellen, oder manuell überprüft werden, um diese Warnungen auszuwählen, die als Security Incident untersucht werden sollen.

Eine Beispielwarnungsregel mit der Bezeichnung **Sicherheits-Incidents aus kritischen Warnungen erstellen** finden Sie im Modul Warnungsregeln der Anwendung Ereignismanagement. Diese Warnungsregel erstellt automatisch Security Incidents, wenn kritische sicherheitsbezogene Ereignisse von innerhalb von ServiceNow oder von Überwachungsanwendungen von Drittanbietern empfangen werden. Nachdem der Security Incident erstellt wurde, wird er aktualisiert, wenn neue Ereignisse empfangen werden. Sie können die Aufgabenvorlage in der Warnungsregel ändern, um die Anfangswerte für den von dieser Warnungsregel erstellten Security Incident zu ändern. Um jede Art von Security Incident zu behandeln, die Sie erstellen möchten, können Sie andere Warnungsregeln mit unterschiedlichen Bedingungen definieren.

Alternativ können Sie als Benutzer mit der Rolle „Sicherheitsadministrator“ einen Security Incident manuell erstellen, indem Sie in einer verdächtigen Warnung auf die Schaltfläche **Security Incident erstellen** klicken.

Es ist wichtig, dass die von externen Tools empfangenen Ereignisse die folgenden Informationen enthalten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Knoten, der auf den Namen, die IP-Adresse oder die sys_id des CI festgelegt ist, das zur betroffenen Ressource wird.
- Die Ereignisklassifizierung wird auf „Sicherheit“ festgelegt, um sie von anderen IT-Ereignissen zu unterscheiden.
- Die Ereignisbeschreibung, mit der die Beschreibung des Security Incident gefüllt wird.
- Die zusätzlichen Informationen können zusätzliche Informationen enthalten, die nicht in die zuvor aufgeführten Felder oder andere Ereignisfelder passen, z. B. Kategorie, Angriffsvektoren, Rückgabe-URL oder Korrelations-ID. Das Format ist eine Zeichenfolge, die Feldnamen zusammen mit ihren Werten auflistet. Verwendet wird das folgende JSON-Format:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Hinweis:
Wenn für jedes Feld-Wert-Paar das Feld im Security Incident, in dem der Spaltenname mit dem Wert „fieldName“ übereinstimmt, leer ist, wird es auf den Wert „fieldValue“ festgelegt. Wenn das Feld im Security Incident nicht leer ist, wird es nicht geändert. In beiden Fällen werden das Ereignis und alle in den zusätzlichen Informationen codierten Felder und Werte in einem Arbeitsnotizeintrag aufgezeichnet, der das Ereignis beschreibt. Wenn sich im Security Incident nichts ändert, wird kein Arbeitsnotizeintrag erstellt. Alle Felder in einem Security Incident, einschließlich anwenderdefinierter Felder, die Sie der Tabelle hinzufügen, können festgelegt werden.

In Sicherheitswarnungen importierte Daten

Wenn ein Ereignis mit weiteren JSON-codierten Daten erstellt wird, werden diese Daten in ein beliebiges Feld mit einem Namen importiert, der dem FeldName dieses Werts in den JSON-Daten entspricht.

Wenn Sie in Ihrer Drittanbieter-Überwachungssoftware (z. B. Splunk) Daten haben, die dem Basissystem nicht gemeinsam sind, können Sie der Warnungstabelle neue Felder hinzufügen, um den Datenimport zu ermöglichen. Das JSON-Format zum Importieren von Daten in Warnungen ist das gleiche Format, das zum Erstellen von Security Incidents aus Ereignissen und Warnungen verwendet wird:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Der einzige Unterschied besteht darin, dass die Daten im Feld immer mit fieldValue überschrieben werden.

Beim Importieren der Sicherheitsereignisdaten werden die Felder in der Warnungstabelle mit entsprechenden Feldnamen gefüllt. Wenn die Warnung später in einen Security Incident umgewandelt wird, füllen dieselben zusätzlichen Informationsdaten übereinstimmende Felder im Security Incident aus.

Erstellen Sie Security Incidents aus vom Anwender gemeldeten Phishing-E-Mails

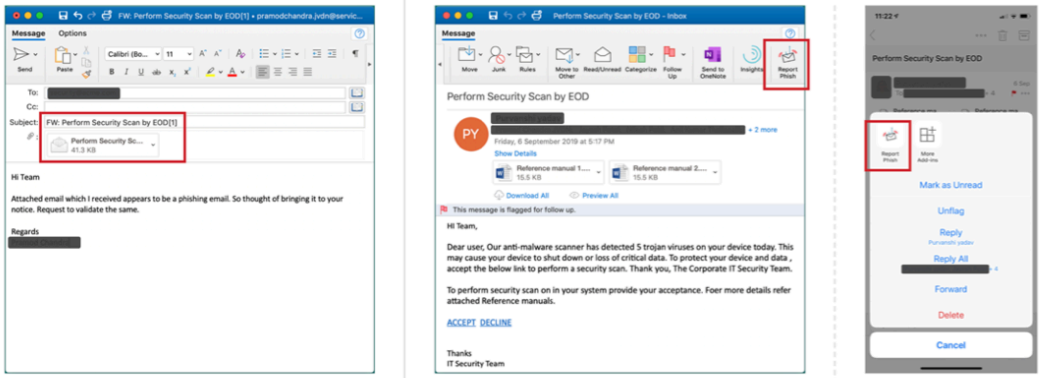
Verwenden Sie diese Funktion, um Security Incidents aus von Anwendern gemeldeten Phishing-E-Mails zu erstellen.

Die erweiterte Funktionalität für vom Benutzer gemeldetes Phishing umfasst Zusammenfassungsfunktionen, E-Mail-Headerextraktion und Konfiguration.

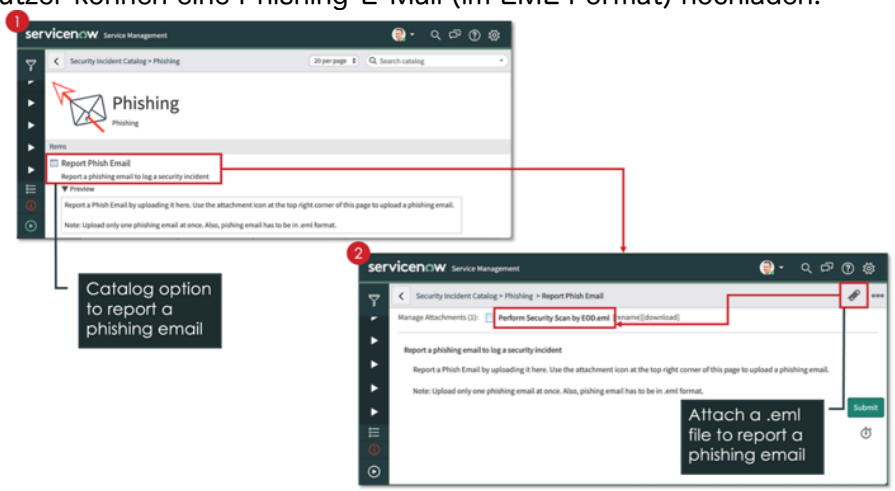
- Benutzer können Phishing-E-Mails auf verschiedene Arten melden:
  - E-Mails können als Anhänge weitergeleitet werden.
  - Wenn das Plugin **PhishAlarm** (früher bekannt als Wombat) mit dem Microsoft Outlook-Client konfiguriert wurde, können Benutzer:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf die Schaltfläche **Phishing melden**.
- Phishing-E-Mails von einem Mobilgerät mit der Option **Phishing** melden weiterleiten.



- Benutzer können eine Phishing-E-Mail (im EML-Format) hochladen.



- Von Benutzern gemeldetes Phishing enthält **eine Geschäftslogik für die Zusammenfassung**, die doppelte Phishing-E-Mails identifiziert, die von Benutzern in einer Organisation gemeldet wurden. Benutzer können diese Funktion für Folgendes verwenden:
  - Aggregieren Sie doppelte oder ähnliche von Anwendern gemeldete Phishing-Incidents (vom Unternehmen initiierte Phishing-Kampagnen).
  - Vermeiden Sie die Selektierung von doppelten, von Anwendern gemeldeten Phishing-Incidents, und reduzieren Sie den manuellen Aufwand für die Konsolidierung von Incidents.
  - Ermöglichen Sie Sicherheitsanalysten, an einem einzelnen, von einem Benutzer gemeldeten Phishing-Incident zu arbeiten.
- Stellt Phishing-E-Mail-Header innerhalb des vom Anwender gemeldeten Phishing-Incidents bereit.
  - Sicherheitsanalysten können nach wichtigen E-Mail-Headerinformationen im Incident suchen.
  - Der manuelle Aufwand zum Sammeln von Headerinformationen aus anderen Quellen ist nicht mehr erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die ursprünglich übermittelte Phishing-E-Mail wird als **Phishing-E-Mail-Datensatz** in einer neuen Tabelle gespeichert.
- Sicherheitsanalysten können Details der ursprünglichen Phishing-E-Mail anzeigen, z. B. Phishing-E-Mail-Inhalt, Header, Herkunft.
- Sicherheitsadministratoren können bestimmte Erweiterungen konfigurieren und vornehmen, unter anderem:
  - Konfigurationen zum Extrahieren von E-Mail-Headern aus dem E-Mail-Text (**Phishing-Übermittlungen von Meldungen melden**).
  - Filter zum Erfassen ausgewählter Header.
  - Konfigurationen für die Verarbeitung der Zuordnung von über- und untergeordneten Incidents, wenn doppelte Phishing-E-Mail-Datensätze identifiziert werden.
  - Flow Designer-Konfigurationen zum Ändern der Geschäftslogik der Zusammenfassung basierend auf den Anforderungen.

Richten Sie Erfassungsregeln für von Anwendern gemeldetes Phishing ein

Als Benutzer mit der Rolle `sn_si.admin` können Sie E-Mail-Abgleichregeln definieren, um von Benutzern gemeldete Phishing-E-Mails basierend auf bestimmten Kriterien zu filtern. Sie können beispielsweise eine Regel definieren, nach der alle E-Mails, die entweder direkt oder über die Schaltfläche Phishing melden an *`security@acme.com`* gesendet werden, als vom Anwender gemeldete Phishing-E-Mails kategorisiert werden. Weitere Informationen finden Sie unter Richten Sie Erfassungsregeln für von Anwendern gemeldetes Phishing ein.

Definieren Sie Eigenschaften für vom Benutzer gemeldetes Phishing

Definieren Sie die Headerinformationen, die aus vom Anwender gemeldeten Phishing-E-Mails erfasst werden müssen. Weitere Informationen finden Sie unter Definieren Sie Eigenschaften für vom Anwender gemeldetes Phishing

Phishing-E-Mail-Datensätze, die aus vom Anwender gemeldeten Phishing-E-Mails erstellt wurden

Von Benutzern gemeldete Phishing-E-Mails werden basierend auf den definierten E-Mail-Übereinstimmungsregeln in Security Incidents konvertiert. Weitere Informationen finden Sie unter Phishing-E-Mail-Datensätze, die aus vom Anwender gemeldeten Phishing-E-Mails erstellt wurden.

Transformieren Sie eine Phishing-E-Mail in einen Security Incident

Der Flow Phishing-E-Mail in Security Incident umwandeln konvertiert Phishing-E-Mail-Datensätze in Security Incidents. Weitere Informationen finden Sie unter Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um.

Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

Zeigen Sie die Details des Security Incident-Datensatzes an, einschließlich zugehöriger Listen, Arbeitsnotizen und anderer wichtiger Informationen. Weitere Informationen finden Sie unter Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden.

Erforderliche Komponenten und Plugins

Die Funktion „Von Anwendern gemeldetes Phishing“ in diesem Release ist eine erweiterte Version der bestehenden Funktionalität von „Von Anwendern gemeldetes Phishing“, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

im London-Release verfügbar war. Weitere Informationen finden Sie im Thema **Regeln zur Validierung von von Anwendern gemeldeten Phishing-Angriffen erstellen** in der London-Dokumentation.

Wichtige Installationsanweisungen

Diese Erweiterung ersetzt das vorhandene Design „Von Anwender gemeldetes Phishing“. Das neue Design enthält die folgenden Updates:

- Die vorhandenen eingehenden Aktionen für eingehende **Phishing-E-Mails, die von Anwendern gemeldet wurden** („Typ“ = „Weiterleiten“ und „Typ“ = „Neu“) wurden deaktiviert.
- Eine neue Aktion für eingehende **Phishing-E-Mail erstellen** ist jetzt verfügbar.
- Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um ist ein neuer Flow, der die Geschäftslogik für die Erstellung und Zusammenfassung von Security Incidents für das neue Design enthält. Sie müssen diesen Flow aktivieren, damit das neue Design wirksam wird.
- Die vorhandenen Regeln für von Benutzern gemeldetes Phishing wurden während des Upgrades beibehalten.

Hinweis:
Wenn Sie anwenderdefinierte Aktionen für eingehende E-Mails und anwenderdefinierte Workflows für von Anwendern gemeldete Phishing-Übermittlungen verwenden, müssen Sie sowohl das alte als auch das neue Design auf widersprüchliche oder überlappende Funktionen überprüfen.

Erweiterungsdetails für vom Anwender gemeldetes Phishing: Im Folgenden finden Sie die Details der Erweiterung:

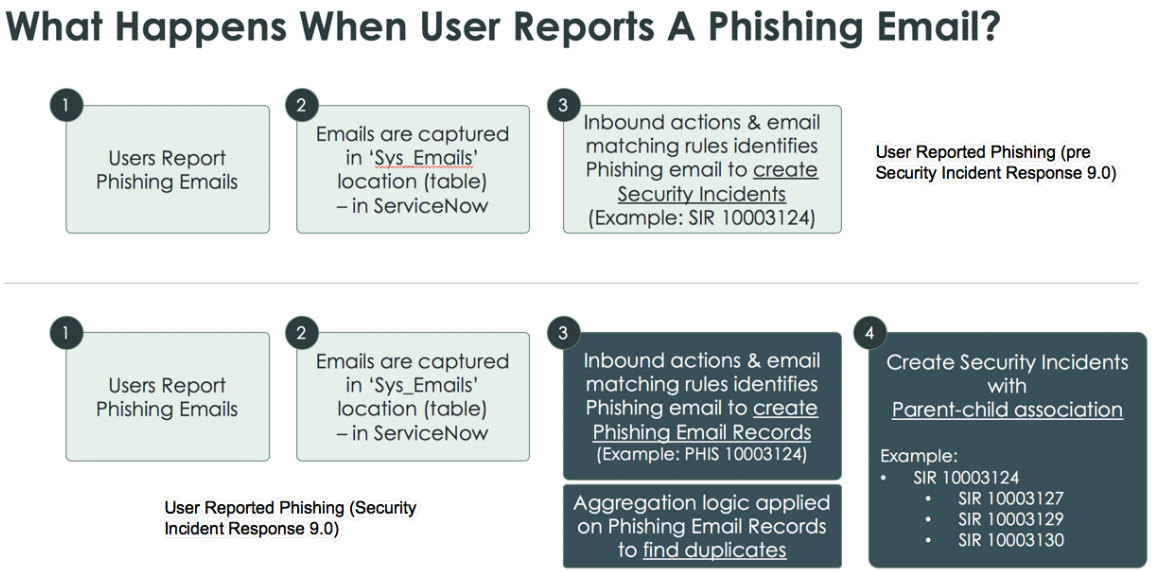
- Phishing-E-Mail auf mehrere Arten melden: Weitere Informationen finden Sie unter Erstellen Sie Security Incidents aus vom Anwender gemeldeten Phishing-E-Mails. Die Phishing-E-Mail wird dann in die Tabelle `sn_si_phishing_email` verschoben.
- Phishing-E-Mail-Datensätze werden erstellt: Wenn die E-Mail-Abgleichsregeln erfüllt sind (siehe Richten Sie Erfassungsregeln für von Anwendern gemeldetes Phishing ein), **erstellt die eingehende Aktion Phishing-E-Mail** erstellen einen Phishing-E-Mail-Datensatz. Die analysierten E-Mail-Header werden in der cm-Tabelle`sn_si_phishing_email_header` gespeichert und der Phishing-E-Mail als zugehörige Liste zugeordnet.
- Ähnliche Phishing-Datensätze in einem einzigen Security Incident zusammenfassen: Der Flow Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um erstellt Security Incidents aus den Phishing-E-Mail-Datensätzen und fasst ähnliche Datensätze in einem einzigen Incident zusammen. Die Zusammenfassungsbedingungen können in diesem Flow nach Bedarf geändert werden.

Hinweis:

- Die vor Release Security Incident Response 9.0 verfügbaren Aktionen für eingehende **Phishing-Meldungen, die von Anwendern gemeldet wurden,** sind jetzt deaktiviert. Security Incidents werden nicht mehr über die deaktivierten eingehenden Aktionen erstellt.
- Die Security Operations-Spoke-Anwendung muss installiert sein, damit das neue Design wirksam wird. Dies schließt den Flow Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um ein, der standardmäßig in einem inaktiven Status verfügbar ist. Aktivieren Sie diesen Flow, um Security Incidents aus den Phishing-E-Mail-Datensätzen zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt die Unterschiede zwischen dem alten und dem neuen Design:



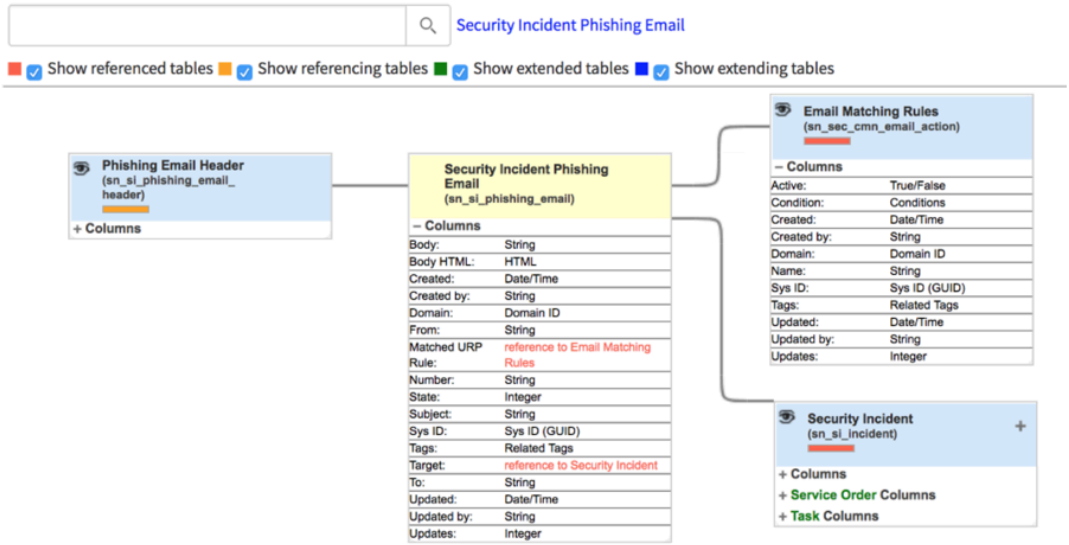
Zur Verwendung der erweiterten Funktion für von Benutzern gemeldetes Phishing sind die folgenden Plugins und Komponenten erforderlich:

- Security Support Common (*sn_sec_cmn*): Beinhaltet:
  - Eingehende Aktion
  - Neues Skript vom Typ „EmailUserReportedPhishing“.
  - Tabelle „Erfassungsregeln“.
- Security Incident Response (sn_si): Umfasst:
  - Tabelle „Security Incident“ (sn_si_incident)
  - Tabelle „Sicherheits-Phishing-E-Mails“ (sn_si_phishing_email)
  - Tabelle mit Sicherheits-Phishing-E-Mail-Headern (sn_si_phishing_email_header)
  - Datensatzersteller des EML-Uploads
- Security Operations-Spoke

  Flows und Subflows zum Aggregieren von E-Mails und zum Transformieren von Phishing-E-Mails in Security Incidents.

Die folgende Abbildung zeigt die neue Phishing-E-Mail-Tabelle mit Verweisen auf die übereinstimmende URP-Regel und den Zieldatensatz für Security Incidents (sn_si_incident).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Richten Sie Erfassungsregeln für von Anwendern gemeldetes Phishing ein

Als Benutzer mit der Rolle `sn_si.admin` können Sie E-Mail-Abgleichregeln definieren, um von Benutzern gemeldete Phishing-E-Mails basierend auf bestimmten Kriterien zu filtern. Sie können beispielsweise eine Regel definieren, nach der alle E-Mails, die entweder direkt oder über die Schaltfläche Phishing melden an *`security@acme.com`* gesendet werden, als vom Anwender gemeldete Phishing-E-Mails kategorisiert werden.

Vorbereitungen

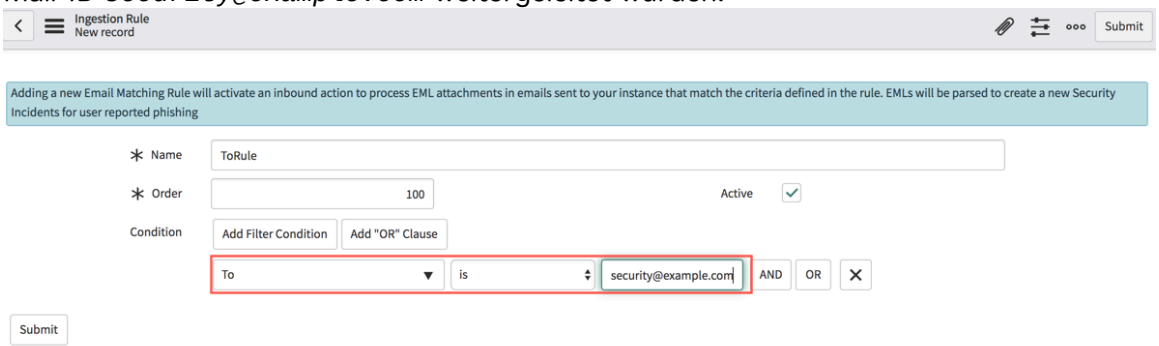
Erforderliche Rolle: sn_si.admin

Prozedur

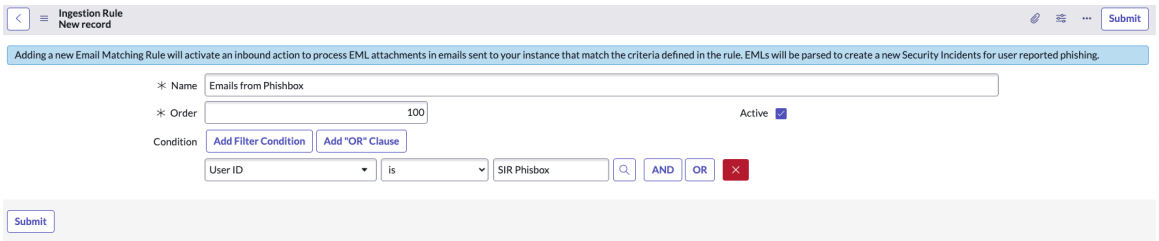
1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Erfassungsregeln – von Anwender gemeldetes Phishing**.
2. Klicken Sie auf **Neu**, um eine neue E-Mail-Abgleichregel zu erstellen.
3. Geben Sie einen Namen ein, und definieren Sie eine oder mehrere Bedingungen für die Regel.
4. Klicken Sie auf **Absenden**, um die Regel zu speichern.
   Im Folgenden finden Sie einige Beispiele für Regeln:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **ToRule**: Filtert E-Mails, die direkt gesendet oder an die E-Mail-ID *security@example.com* weitergeleitet wurden.



- **Anwender-ID-Regel**: Filtert E-Mails, die von einer bestimmten E-Mail-ID gesendet wurden.



Definieren Sie Eigenschaften für vom Anwender gemeldetes Phishing

Definieren Sie die Headerinformationen, die aus vom Anwender gemeldeten Phishing-E-Mails erfasst werden müssen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

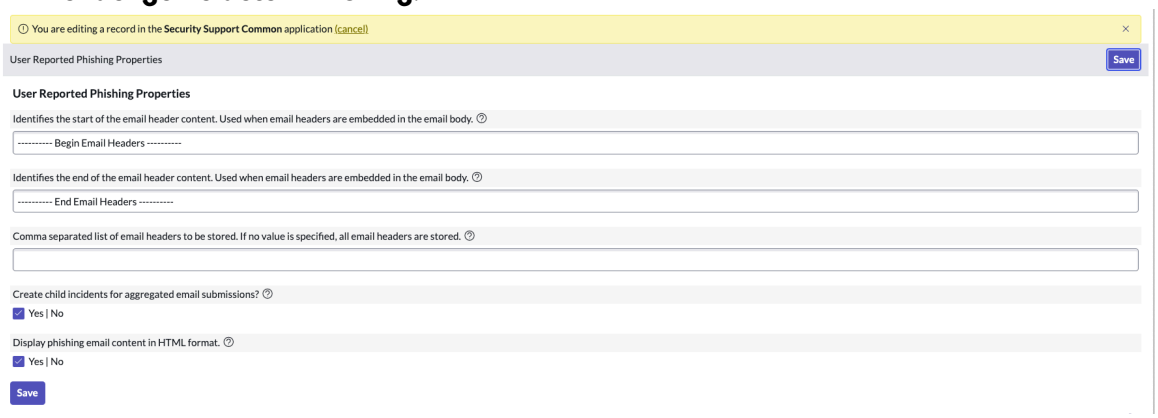
Verwenden Sie diese Optionen, um die folgenden Einstellungen für von Benutzern gemeldetes Phishing zu konfigurieren.

- Konfiguration zum Extrahieren von E-Mail-Headern aus dem E-Mail-Text. (**Phishing-Übermittlungen melden**.)
- Filtern Sie, um Header auszuwählen.
- Aktivieren oder deaktivieren Sie die Zuordnung zwischen über- und untergeordneten Elementen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Eigenschaften des vom Anwender gemeldeten Phishing**.



2. Geben Sie die Konfiguration zum Extrahieren von E-Mail-Headern aus dem E-Mail-Text an:
   - Geben Sie eine Zeichenfolge ein, die den Anfang des E-Mail-Headers identifiziert.
   - Geben Sie eine Zeichenfolge ein, die das Ende des E-Mail-Headers identifiziert.

   Hinweis:
   Wenden Sie diese Einstellungen nur auf Header an, die als Teil des E-Mail-Textes der Phishing-E-Mail erfasst wurden. Wenn beispielsweise das Plugin **„PhishAlarm“** (früher als Wombat bezeichnet) mit dem Microsoft Outlook-Client konfiguriert wurde und der Benutzer auf die Schaltfläche **„Phishing melden“** klickt, werden die E-Mail-Header gemäß der hier definierten Konfiguration erfasst. Die Headerinformationen werden nicht erfasst, wenn die Phishing-E-Mail als Anhang weitergeleitet wird.

3. Geben Sie Filter an, um Header zu entfernen, die für die Untersuchung des Security Incident nicht erforderlich sind.

   Geben Sie eine durch Kommas getrennte Liste von E-Mail-Headern ein, die aus der vom Anwender gemeldeten Phishing-E-Mail erfasst werden müssen. Wenn Sie hier keinen Wert angeben, werden alle Headerinformationen erfasst.

4. Aktivieren oder deaktivieren Sie die Zuordnung zwischen über- und untergeordneten Elementen. Standardmäßig ist die Option **Ja** aktiviert. Wählen Sie **„Ja“** aus, um anzugeben, dass untergeordnete Security Incidents erstellt werden müssen, wenn von Anwendern gemeldete Phishing-E-Mails zusammengefasst werden. Wenn Sie **Nein**auswählen, werden keine untergeordneten Security Incidents erstellt, aber die vom Anwender gemeldeten Phishing-E-Mails werden dem Security Incident zugeordnet, und der Security Incident-Datensatz wird aktualisiert. Weitere Informationen zur Erstellung von untergeordneten Security Incidents finden Sie unter Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um.

5. Aktivieren oder deaktivieren Sie die Option zum Anzeigen des Phishing-E-Mail-Inhalts im HTML-Format. Standardmäßig ist die Option **Ja** aktiviert. Wählen Sie **„Ja“**, um den Phishing-E-Mail-Inhalt im HTML-Format anzuzeigen. Wenn Sie **Nein**auswählen, ist der E-Mail-Inhalt im HTML-Format in einem Phishing-Datensatz nicht sichtbar.

Phishing-E-Mail-Datensätze, die aus vom Anwender gemeldeten Phishing-E-Mails erstellt wurden

Von Benutzern gemeldete Phishing-E-Mails werden basierend auf den definierten E-Mail-Übereinstimmungsregeln in Security Incidents umgewandelt.

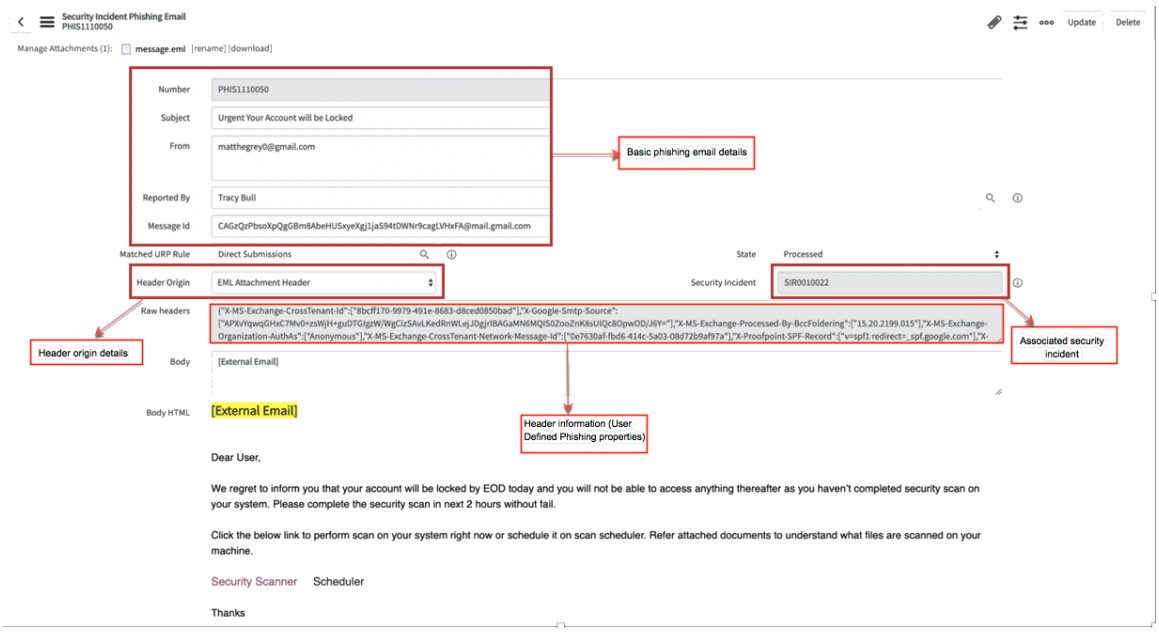
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine neue Phishing-E-Mail gemeldet wird, werden die folgenden Aktionen ausgeführt:

- Ein E-Mail-Datensatz wird in der Tabelle *„sys_email“* erstellt.
- Die Aktion **Phishing-E-Mail erstellen** wird für den E-Mail-Datensatz ausgeführt und verwendet die E-Mail-Übereinstimmungsregeln (siehe Richten Sie Erfassungsregeln für von Anwendern gemeldetes Phishing ein), um zu bestimmen, ob es sich um eine Phishing-E-Mail handelt.
- Wenn sie als Phishing-E-Mail identifiziert wurde, wird in der Tabelle „sn_si_phishing_email“ ein Phishing-E-Mail-Datensatz erstellt.
- Abschließend wird der Flow Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um angewendet, um den Phishing-E-Mail-Datensatz in einen Security Incident zu konvertieren.

Um die E-Mail-Details anzuzeigen, navigieren Sie zu **Security Incident** > **Alle Phishing-E-Mails anzeigen**. Eine Liste der Phishing-E-Mail-Datensätze wird angezeigt. Klicken Sie auf den Datumslink in der Spalte Erstellt, um den E-Mail-Datensatz anzuzeigen.

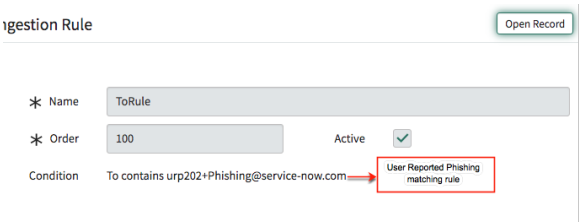


Security Incident – Details zu Phishing-E-Mail

Feldname	Beschreibung
Nummer	Die Nummer, die der vom Anwender gemeldeten Phishing-E-Mail zugewiesen ist.
Betreff	Betreff der E-Mail Die Betreffregel ist in simulierten Phishing-Kampagnen oder -Tests nützlich. In diesem Fall senden Organisationen betrügerische E-Mails an ihre eigenen Mitarbeiter, um ihre Reaktion auf Phishing und ähnliche E-Mail-Angriffe zu testen. Wenn bei simulierten Phishing-E-Mail-Tests der Microsoft Outlook-E-Mail-Client mit dem **PhishAlarm** -Plugin (früher als Wombat bezeichnet) verwendet wird, kann der Benutzer auf die Schaltfläche **Phishing melden** klicken, um die Phishing-E-Mail zu melden. Die E-Mail wird an das Security Operations-Team gesendet, wobei **Simuliertes Phishing** an den Betreff der E-Mail

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

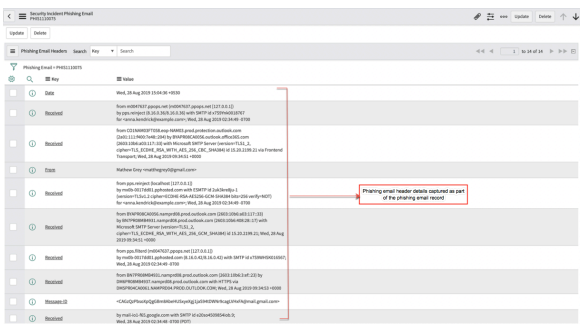
Security Incident – Details zu Phishing-E-Mail (Fortsetzung)

Feldname	Beschreibung
	angehängt wird. Dies wird verwendet, um die E-Mail als simulierte Phishing-E-Mail zu identifizieren.
Von	Die E-Mail-Adresse, von der diese Phishing-E-Mail stammt. Diese Informationen sind verfügbar, wenn die Phishing-E-Mail als EML-Dateianhang weitergeleitet wird oder wenn die ursprünglichen Header in die E-Mail eingebettet sind. Wenn der Benutzer die Phishing-E-Mail direkt weitergeleitet hat, ist die Absenderadresse möglicherweise nicht verfügbar.
Gemeldet von	Die E-Mail-ID des Anwenders, der diese Phishing-E-Mail gemeldet hat. Klicken Sie auf das **Informationssymbol**, um zusätzliche Details anzuzeigen.
Nachrichten-ID	Die der Nachricht zugewiesene ID.
Übereinstimmende URP-Regel	Die Regel für vom Anwender gemeldetes Phishing, die auf diese E-Mail angewendet werden soll. Klicken Sie auf das Informationssymbol, um zusätzliche Details anzuzeigen.
 Wie Sie in diesem Beispiel sehen können, zeigt das Feld **Bedingung** an, dass die ToRule auf diese E-Mail angewendet und ein Security Incident erstellt wird. Weitere Informationen zum Definieren von E-Mail-Übereinstimmungsregeln finden Sie unter Richten Sie Erfassungsregeln für von Anwendern gemeldetes Phishing ein.	
Status	Wenn in der Tabelle sn_si_phishing_email ein neuer Phishing-E-Mail-Datensatz erstellt wird, wird das Feld Status auf **Neu**festgelegt. Wenn dieser E-Mail-Datensatz in einen Security Incident konvertiert wird (siehe Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um), wird das Feld „Status“ auf **„Verarbeitet“**aktualisiert.

Headerursprung	Dieses Feld gibt an, wie die E-Mail-Header stammen oder wie der Anwender die Phishing-E-Mail gemeldet hat:
	• **E-Mail-Header**: Der Anwender hat die Phishing-E-Mail an das Security Operations-Team weitergeleitet.
	• **E-Mail-Text:**
	  ○ Der Anwender hat auf die Option **„Phishing melden“** geklickt (wenn das **PhishAlarm-** Plugin (früher als Wombat bezeichnet) mit dem E-Mail-Client konfiguriert wurde).
	  ○ Basierend auf der definierten Regel für vom Anwender gemeldetes Phishing wird die Phishing-E-Mail an das Security Operations-Team weitergeleitet.
	• **EML-Anlagen-Header**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident – Details zu Phishing-E-Mail (Fortsetzung)

Feldname	Beschreibung
	○ Anhang: Der Anwender hat die E-Mail als Anhang (EML-Datei) weitergeleitet. ○ Servicekatalog-Übermittlung: Der Benutzer hat die E-Mail als EML-Datei auf den Desktop heruntergeladen und dann an einem angegebenen Speicherort hochgeladen. Aus der E-Mail wird dann der Security Incident erstellt. • **EML-Anlagentext**: ○ Der Anwender hat auf die Option **„Phishing melden"** geklickt (wenn das **PhishAlarm-** Plugin (früher als Wombat bezeichnet) mit dem E-Mail-Client konfiguriert wurde). ○ Basierend auf der definierten Regel für vom Anwender gemeldetes Phishing wird die Phishing-E-Mail als Anhang an das Security Operations-Team weitergeleitet.
Security Incident	Dieses Feld ist leer, wenn die vom Anwender gemeldete Phishing-E-Mail zum ersten Mal gemeldet wird. Wenn der Flow Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um ausgeführt wurde, wird diese E-Mail in einen Security Incident-Datensatz konvertiert, und die Nummer dieses Datensatzes wird hier angezeigt.
Roh-Header	Dieses Feld zeigt die vollständigen Headerinformationen, die aus der E-Mail extrahiert wurden, wie auf der Seite Definieren Sie Eigenschaften für vom Anwender gemeldetes Phishing definiert. Die Header werden in Schlüssel-Wert-Paare analysiert und in der Liste Phishing-E-Mail-Header angezeigt.
	
Textkörper	Dies ist der Textkörper der vom Anwender gemeldeten Phishing-E-Mail.

Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um

Der Flow **Phishing-E-Mail in Security Incident umwandeln** ist ein neuer Flow, der Phishing-E-Mail-Datensätze in Security Incidents konvertiert oder transformiert.

Vorbereitungen

Hinweis:

Um die Funktion „Vom Benutzer gemeldetes Phishing" zu aktivieren, müssen Sie eine Kopie des Flows erstellen und ihn aktivieren. Wenn Sie anwenderdefinierte eingehende Aktionen und anwenderdefinierte Flows erstellt haben, um von Anwendern gemeldete Phishing-Übermittlungen zu verarbeiten, sind die hier vorgeschlagenen Flow-Änderungen nicht erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erforderliche Rolle: sn_si.admin
- Flow Designer-Spoke muss installiert sein.

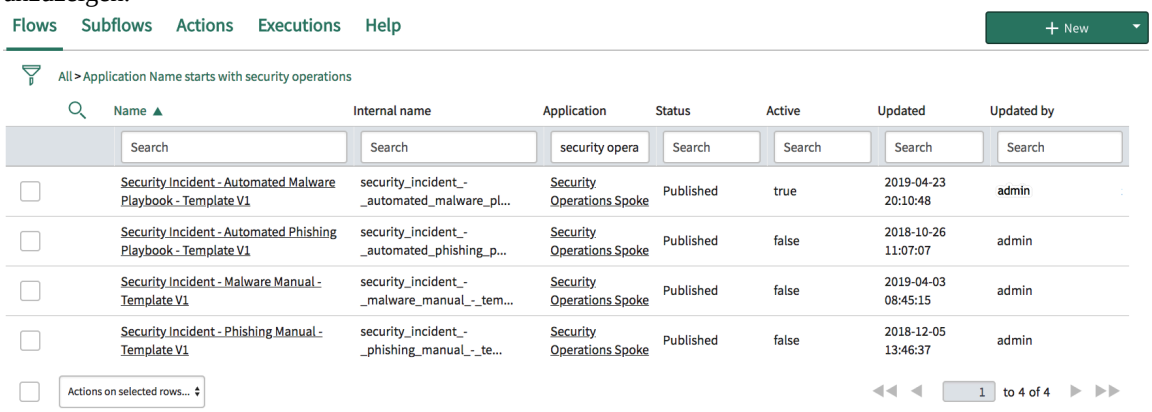
Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird automatisch gestartet, wenn ein Datensatz einer von einem Anwender gemeldeten Phishing-E-Mail erstellt wird, dessen Status auf **Neu** festgelegt ist. Dieser Flow enthält die Logik zum:

- Security Incidents aggregieren.
- Aktualisieren Sie Security Incidents mit relevanten Hinweisen.
- Fügen Sie Headerdaten hinzu.
- Erstellen Sie nach Bedarf untergeordnete Incidents.

Prozedur

- Navigieren zu **Flow Designer** > **Designer** um die mit der Security Operations-Spoke verfügbaren Flows anzuzeigen.

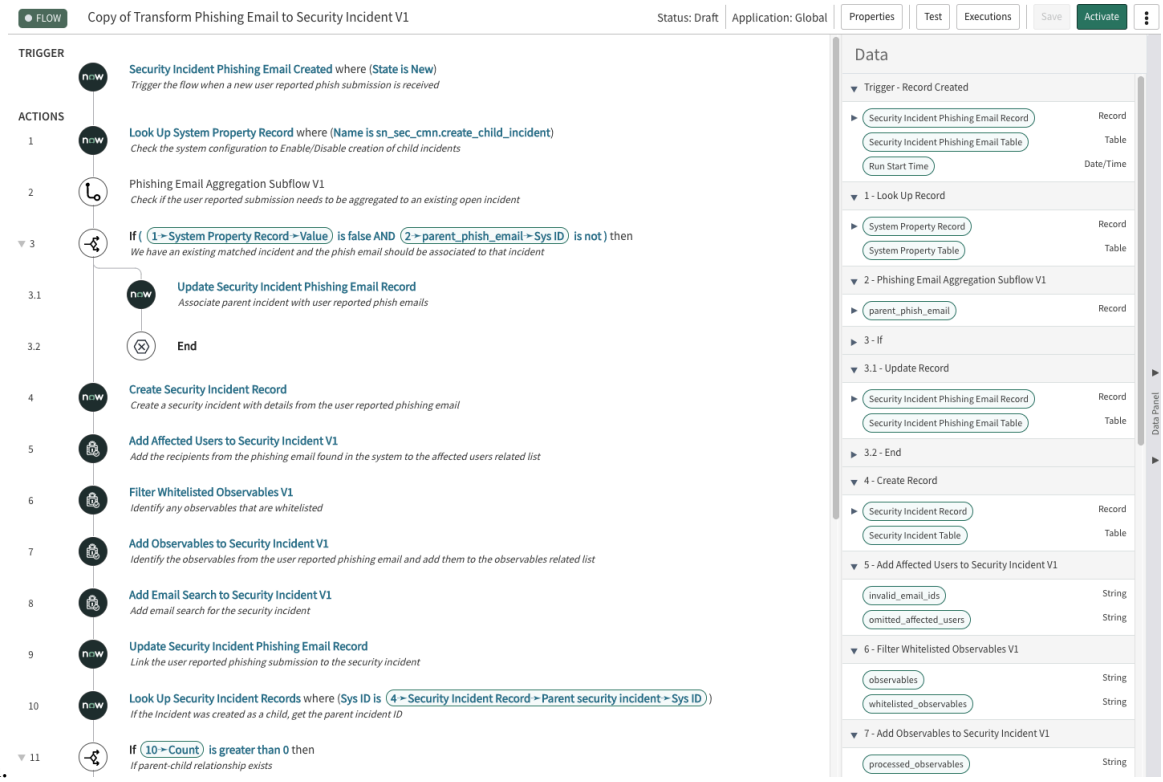


- Klicken Sie auf den Link **Phishing-E-Mail in Security Incidents umwandeln,** um den Flow anzuzeigen.
- Dieser Flow wird mit dem Basissystem bereitgestellt, befindet sich im **schreibgeschützten** Modus und kann nicht verwendet werden.

  Klicken Sie auf das Mehr-Symbol , erstellen Sie eine Kopie des Flows, und öffnen Sie ihn zur Verwendung. Sie können jetzt Änderungen an Ihrem Flow vornehmen, z. B. Auslöserbedingungen oder Aktionen ändern oder Aktionen hinzufügen und entfernen. Nachdem Sie die erforderlichen Änderungen vorgenommen haben, müssen Sie den Flow aktivieren

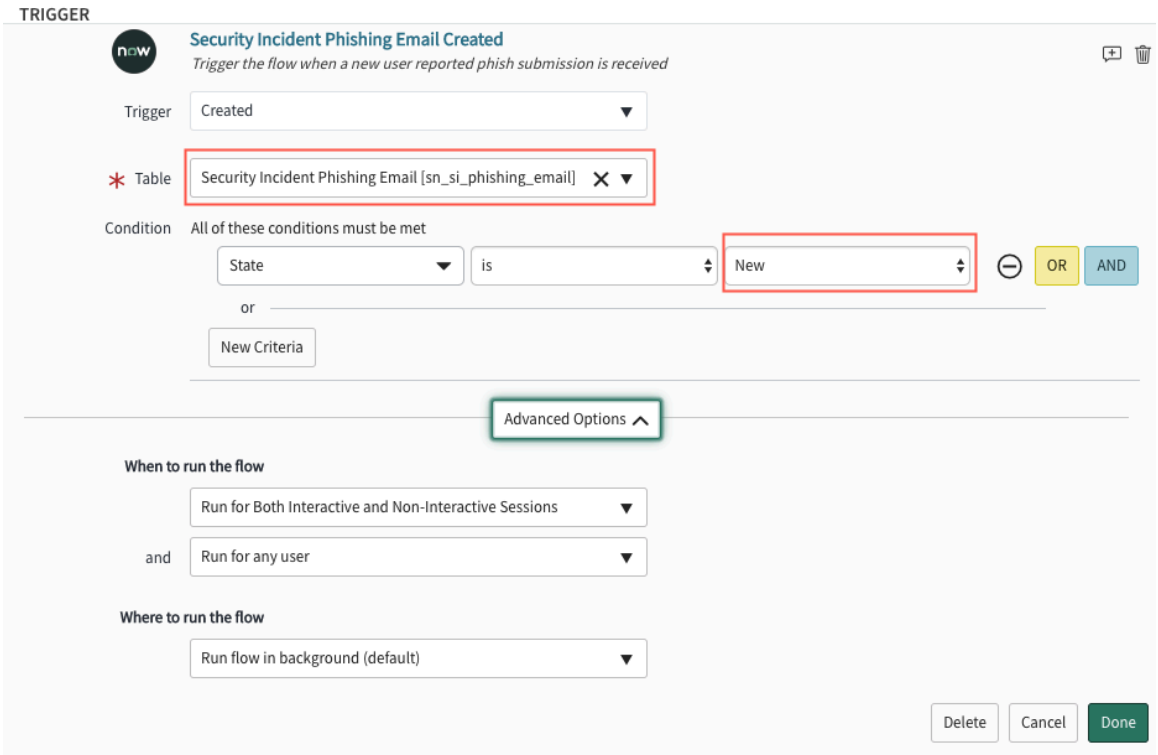
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Siehe Aktivieren Sie einen Security Incident Response -Flow), damit er ausgeführt werden kann.



Diese Abbildung zeigt den Auslöser und die mit dem Flow ausgeführten Schritte. Der rechte Bereich zeigt den Datenfluss. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

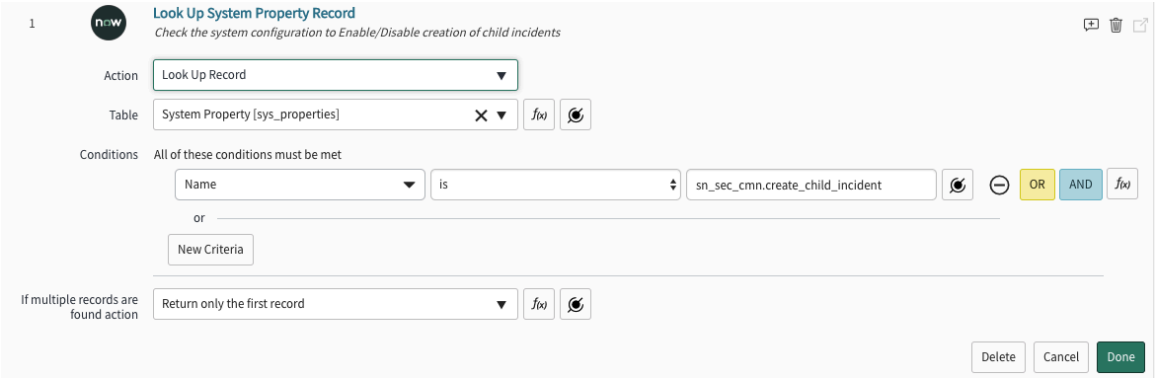
- Klicken Sie auf das Symbol **Auslöser**.
  Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser und die Aufgabe an, die ausgeführt werden sollen, wenn die Bedingungen erfüllt sind.
  Dieser Flow wird initiiert, wenn ein **neuer** Datensatz in die Tabelle „sn_si_phishing_email“ hochgeladen wird.



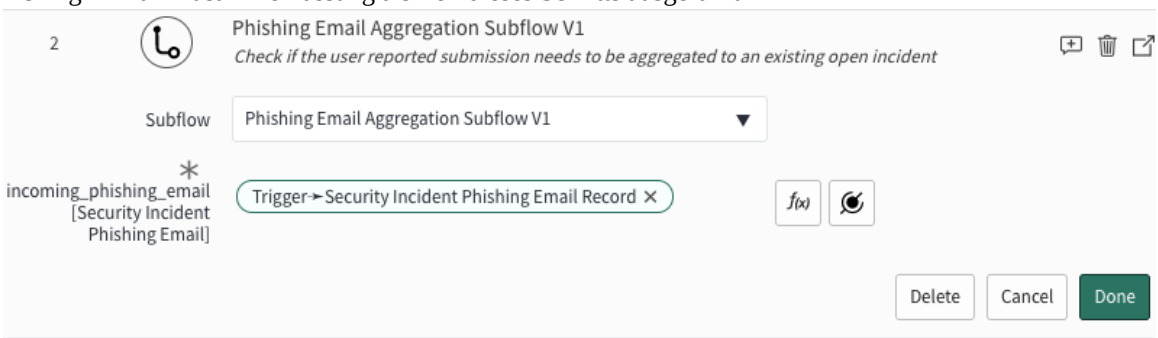
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

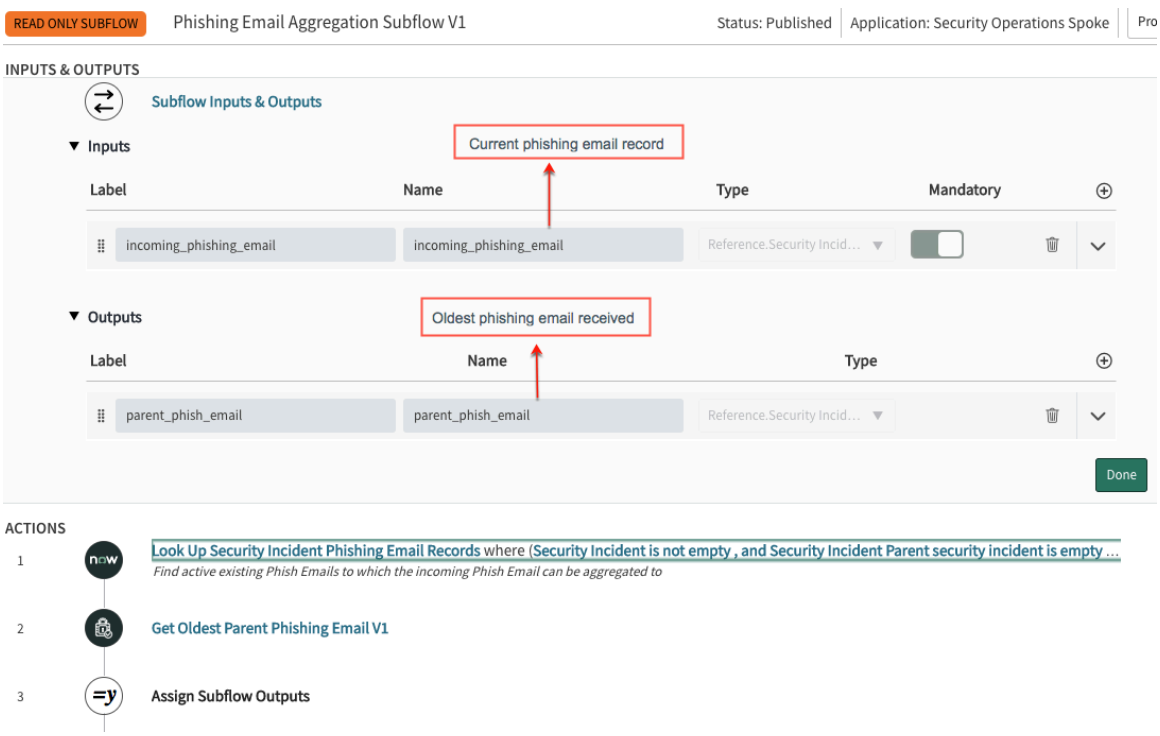
- In Schritt 1 überprüft der Flow, ob die **Option Untergeordnete Incidents für zusammengefasste E-Mail-Übermittlungen erstellen?** Die Kennzeichnung „“ wird auf der Seite Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um aktiviert oder deaktiviert.



- In Schritt 2 wird der älteste übergeordnete Security Incident identifiziert. Beachten Sie das Symbol in Schritt 2. Dies weist darauf hin, dass der Subflow der Phishing-E-Mail-Zusammenfassung als Teil dieses Schritts ausgeführt wird.

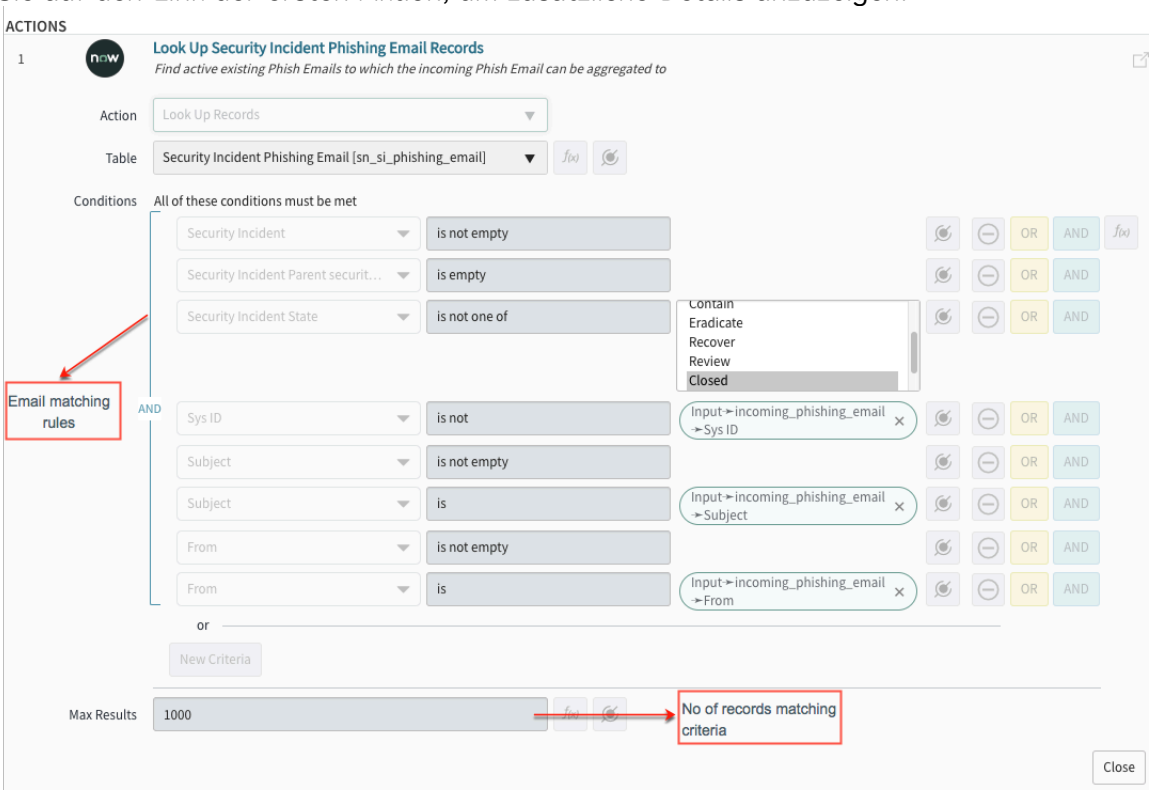


Klicken Sie auf das Aktionsdesigner-Symbol, um eine detaillierte Ansicht der Aktion anzuzeigen. Dieser Subflow prüft die Phishing-E-Mail und ordnet sie basierend auf den angegebenen Kriterien einem vorhandenen Security Incident zu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese beiden Aktionen werden ausgeführt, wenn dieser Subflow ausgeführt wird. Klicken Sie auf den Link der ersten Aktion, um zusätzliche Details anzuzeigen.



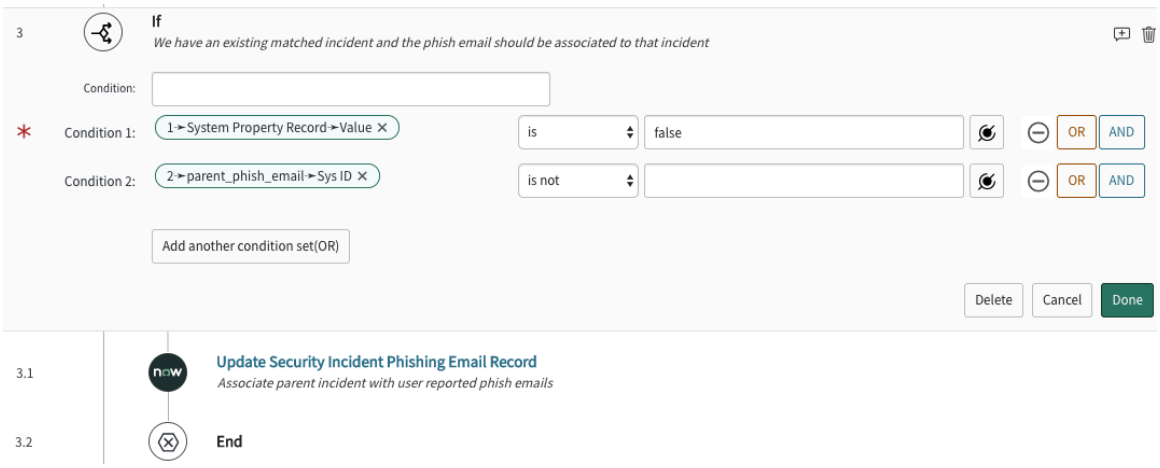
Diese Aktion überprüft die E-Mails, die den Kriterien für die neue eingehende E-Mail entsprechen, basierend auf Bedingungen wie:

- Der Status des Security Incidents lautet nicht **„Geschlossen“**.
- Der Betreff- oder Von-Wert stimmt mit den definierten E-Mail-Übereinstimmungsregelbedingungen überein (siehe Richten Sie Erfassungsregeln für von Anwendern gemeldetes Phishing ein).

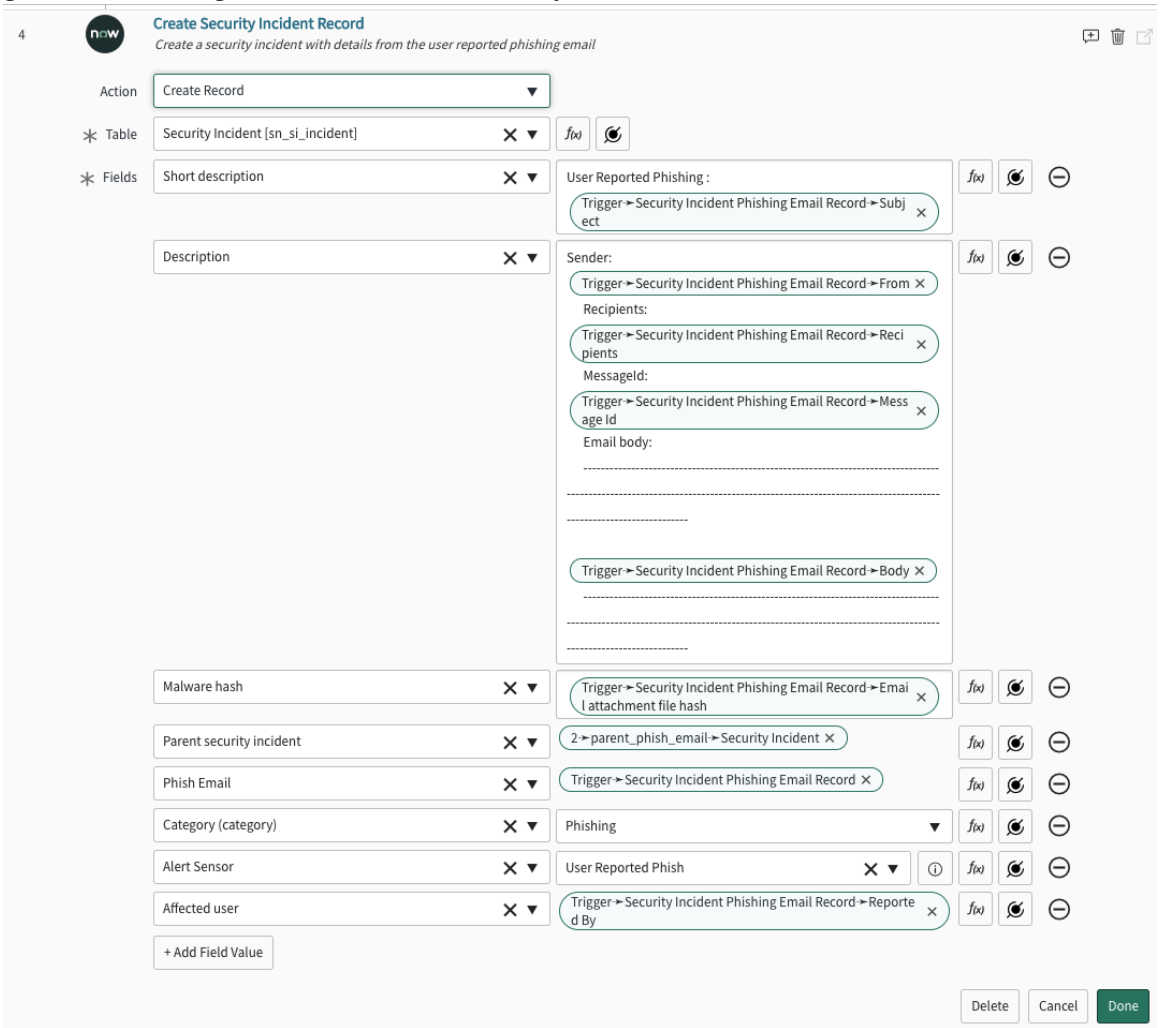
Wenn diese Bedingungen erfüllt sind, wird im Feld Max. Ergebnisse die Anzahl der Datensätze angezeigt, die den Kriterien entsprechen. Der älteste oder der erste Datensatz in der Liste wird als übergeordneter Datensatz festgelegt, für den die Security Incidents zusammengefasst werden.

- Schritt 3 ist nur anwendbar, wenn die **Option Untergeordnete Incidents für zusammengefasste E-Mail-Übermittlungen erstellen?** Kennzeichnung wurde auf der Seite Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um auf **Nein** festgelegt.
  In diesem Fall wird die Phishing-E-Mail dem Security Incident-Datensatz zugeordnet, und der Flow wird beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

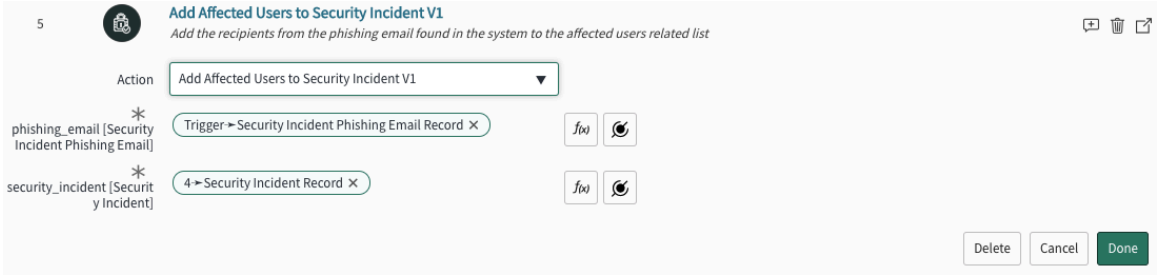


- Wenn die **Option Untergeordnete Incidents für zusammengefasste E-Mail-Übermittlungen erstellen?** auf **Ja**festgelegt wurde, wird der Flow weiter ausgeführt, und basierend auf der vom Anwender gemeldeten Phishing-E-Mail wird ein neuer Security Incident erstellt.

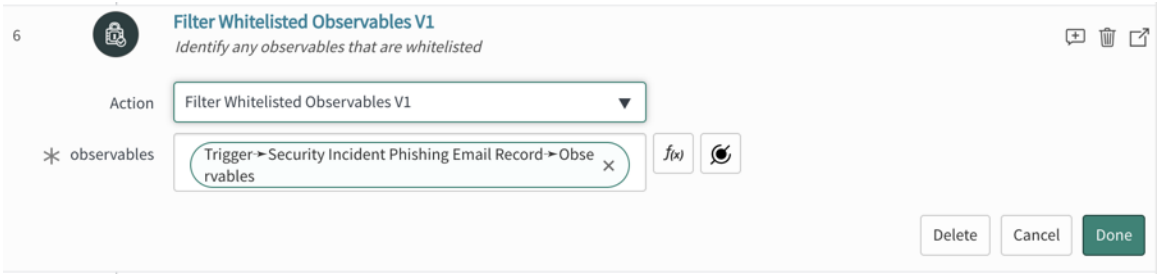


- In Schritt 5 werden die Benutzer, die die Phishing-E-Mail erhalten haben (Mitarbeiter in der Liste „An“ und „CC“ der Phishing-E-Mail), der zugehörigen Liste „Betroffene Benutzer“ im Datensatz „Security Incident“ hinzugefügt.

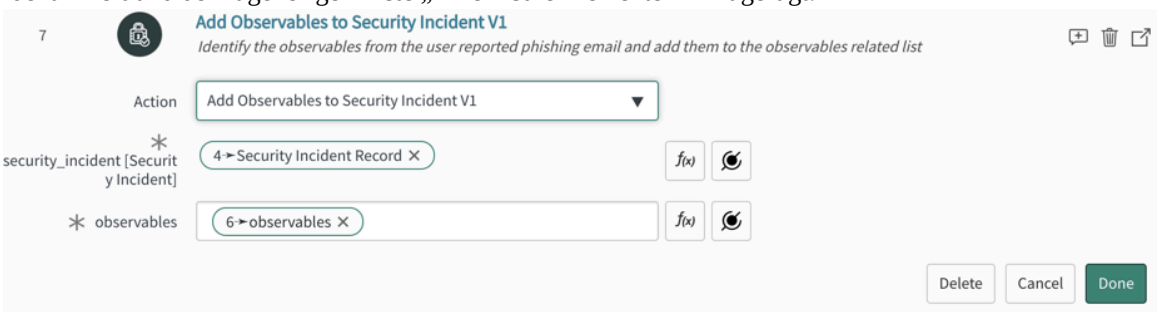
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



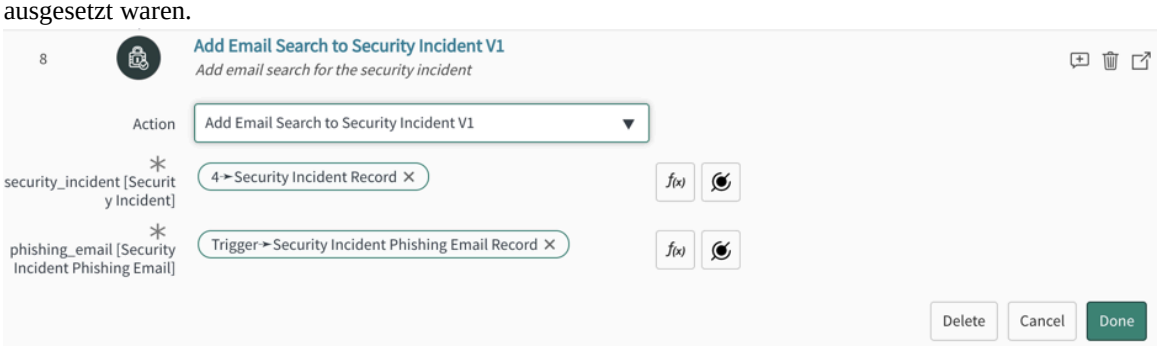
- In Schritt 6 werden erkennbare Elemente auf der Zulassungsliste aus der Liste der erkennbaren Elemente im Security Incident gefiltert.
  Diese erlauben, dass aufgelistete erkennbare Elemente dem Security Incident nicht hinzugefügt werden.



- In Schritt 7 werden unbekannte erkennbare Elemente aus der vom Anwender gemeldeten Phishing-E-Mail identifiziert und der zugehörigen Liste „Erkennbare Elemente“ hinzugefügt.

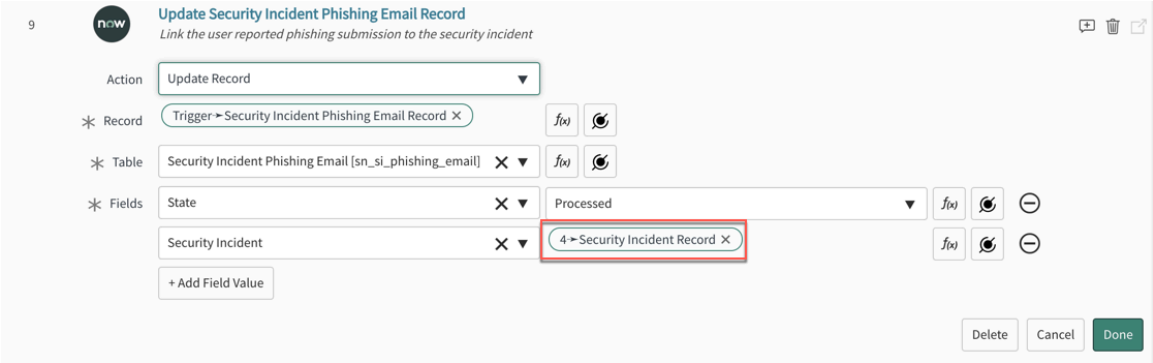


- In Schritt 8 wird eine E-Mail-Suchabfrage generiert, die eine Kombination aus dem Betreff und der Absenderadresse der E-Mail ist.
  Diese Informationen sind nützlich, um die Mitarbeiter in der Organisation zu identifizieren, die dem Phishing ausgesetzt waren.

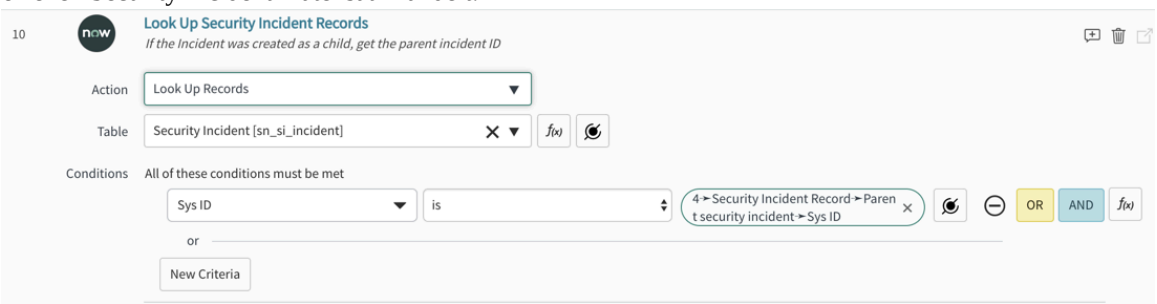


- In Schritt 9 wird die vom Anwender gemeldete Phishing-E-Mail mit dem Security Incident verknüpft und der Security Incident-Datensatz (in Schritt 4 erstellt) aktualisiert.

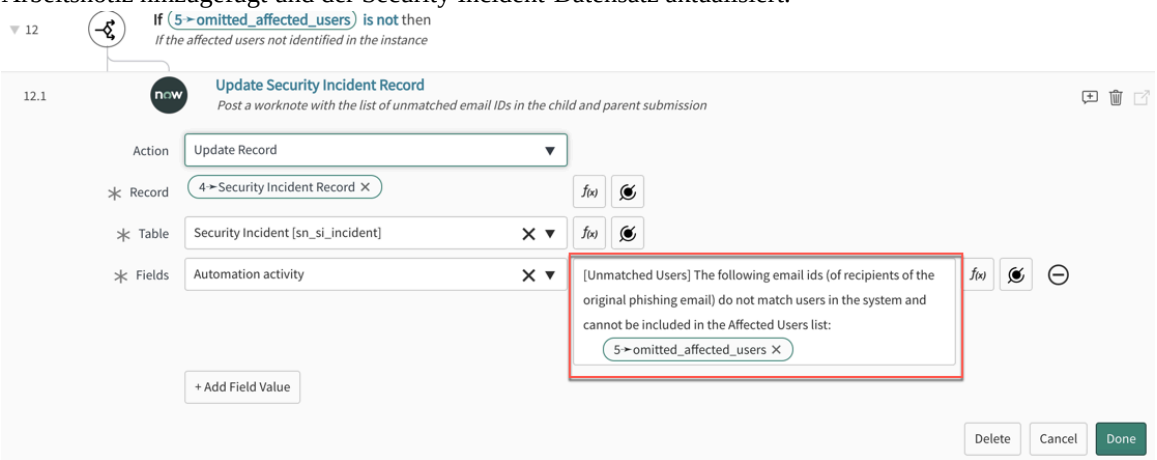
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- In Schritt 10 wird der übergeordnete Security Incident identifiziert, und es wird geprüft, ob es sich um einen offenen Security Incident-Datensatz handelt.

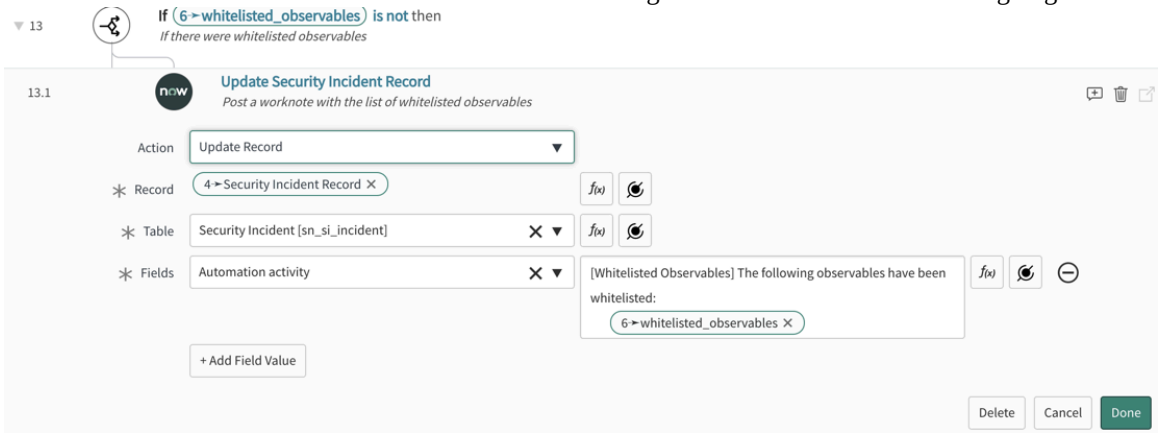


- Wenn die übergeordnete Sicherheit aktiv ist, werden den untergeordneten und den übergeordneten Security Incident-Datensätzen Notizen hinzugefügt, die angeben, wie sie einander zugeordnet sind.
- Wenn in Schritt 12 keine betroffenen Anwender gefunden wurden (in Schritt 5 des Flow), wird eine Arbeitsnotiz hinzugefügt und der Security Incident-Datensatz aktualisiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

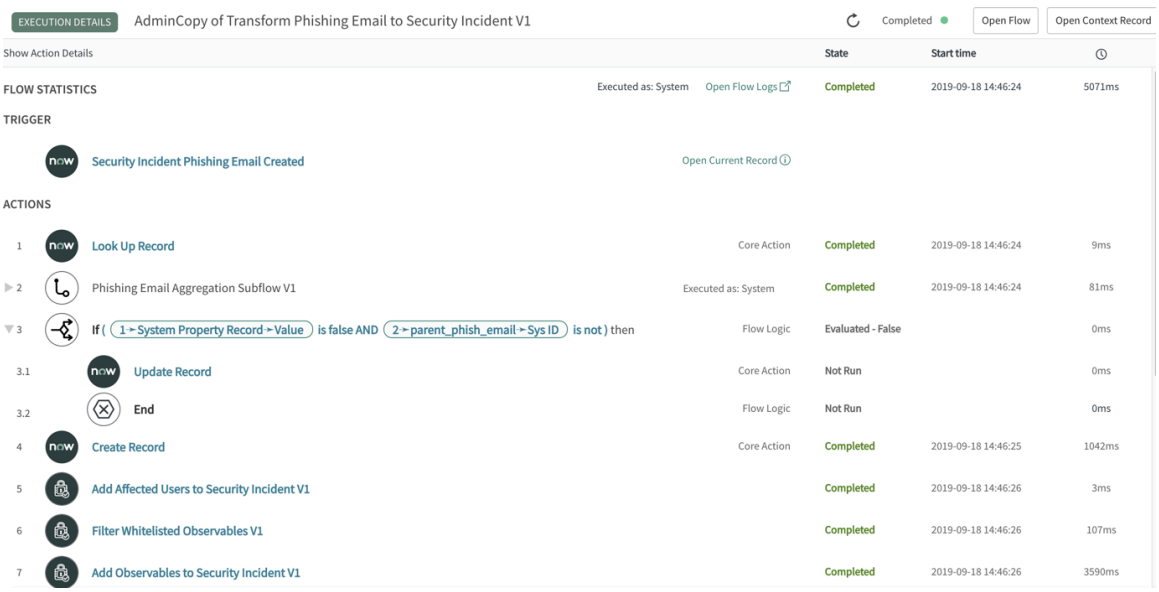
- In Schritt 13 wird eine Arbeitsnotiz mit der Liste der zulässigen erkennbaren Elemente hinzugefügt.



Nächste Maßnahme

Sie können auf **Test** klicken, um die Aktionen im Flow zu simulieren, bevor er veröffentlicht wird. Klicken Sie nach dem Testen des Flows auf **Aktivieren**, um den Flow zu aktivieren, damit er ausgeführt werden kann.

Klicken Sie auf **Ausführungen**, um die Ausführungsdetails des Flow anzuzeigen.



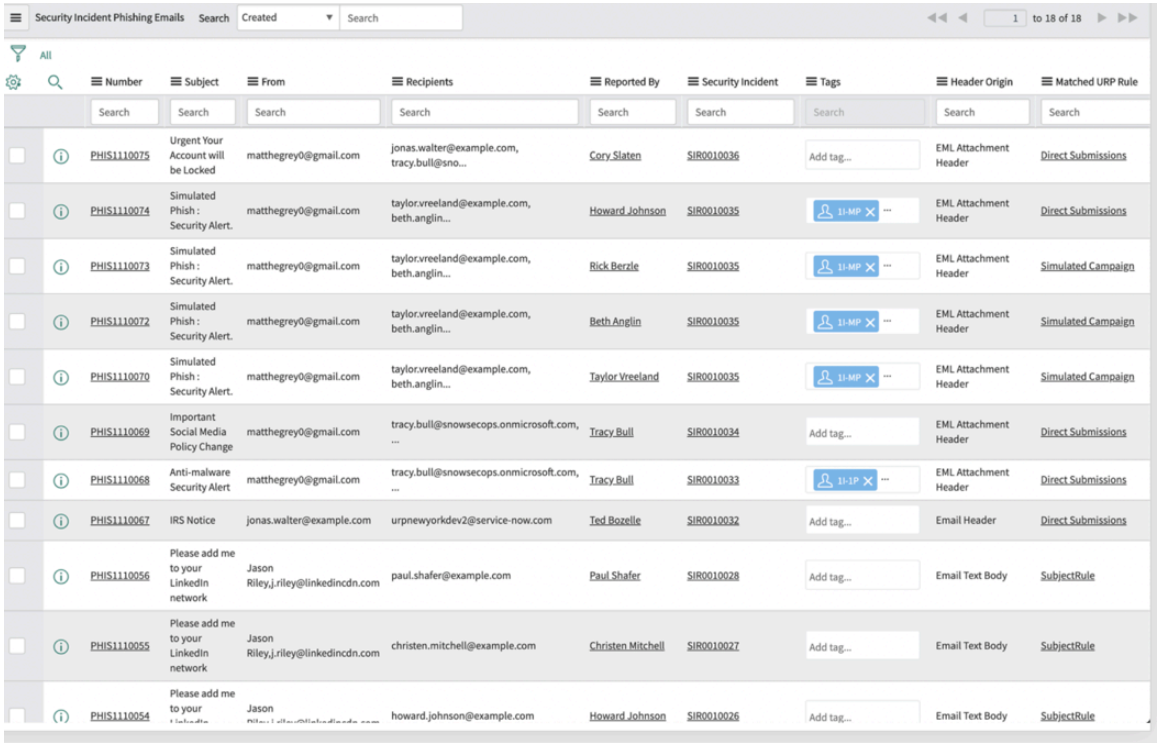
Wenn der Flow ausgeführt wurde, wird der Phishing-E-Mail-Datensatz in einen Security Incident konvertiert. Siehe Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

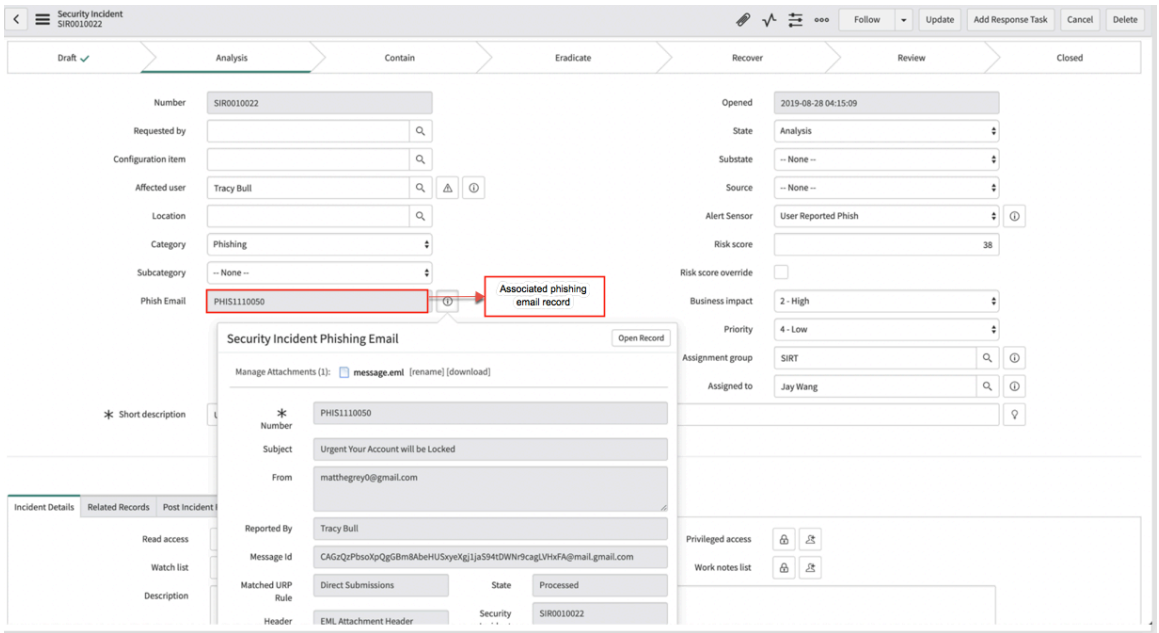
Phishing-E-Mail-Datensätze, die in der Tabelle *„sn_si_phishing_email“* gespeichert sind, werden in Datensätze zu Security Incidents konvertiert.

Klicken Sie auf, um den Security Incident anzuzeigen, der dem Phishing-E-Mail-Datensatz zugeordnet ist **Security Incident** > **Phishing-E-Mail** > **Alle Phishing-E-Mails anzeigen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie auf den Link in der Spalte „Security Incident“, die dem Phishing-E-Mail-Datensatz zugeordnet ist. Die Details des Security Incidents werden angezeigt.



Zugehörige Listen

Scrollen Sie nach unten zum Abschnitt „Zugehörige Links“ des Security Incidents, und klicken Sie **auf die zugehörige Liste Alle anzeigen**. Zeigen Sie Details wie untergeordnete Security Incidents, betroffene Anwender und zugehörige Phishing-E-Mails an.

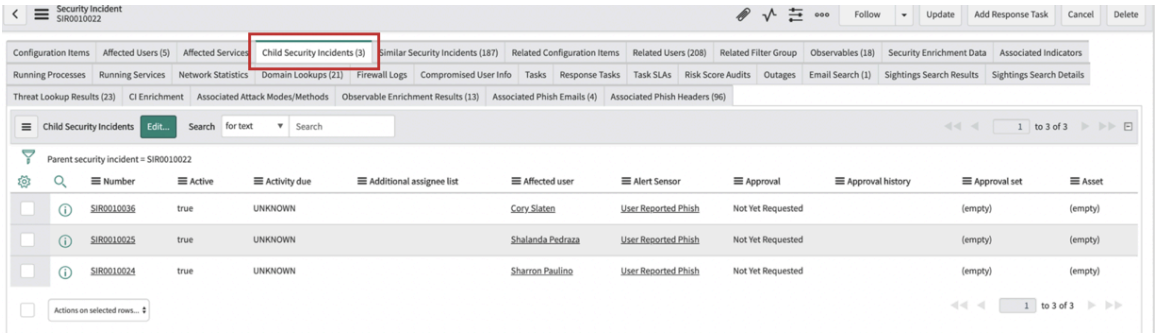
Untergeordnete Security Incidents

Klicken Sie auf die Registerkarte **Untergeordnete Security Incidents**. Sie können eine Liste der untergeordneten Security Incidents anzeigen, die dem übergeordneten Security Incident zugeordnet sind, basierend auf der angewendeten Zusammenfassungslogik. Für jeden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

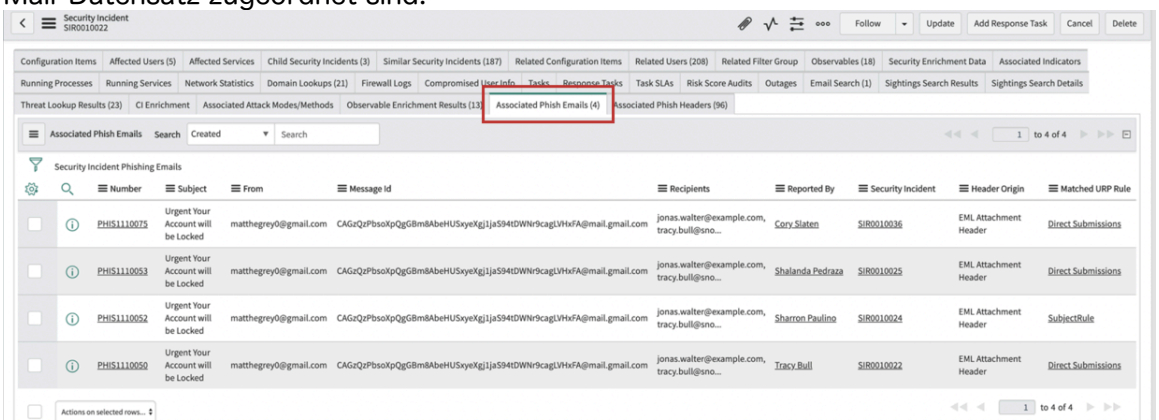
hinzugefügten untergeordneten Datensatz wird dem übergeordneten Datensatz eine automatisierte Systemaktivität hinzugefügt (im Abschnitt „Arbeitsnotiz“). Dadurch wird der Sicherheitsanalyst über den aggregierten untergeordneten Datensatz benachrichtigt.

Hinweis:
Sie können die untergeordneten Security Incidents hier nur anzeigen, wenn die Kennzeichnung **Untergeordnete Incidents für zusammengefasste E-Mail-Übermittlungen erstellen** auf der Seite „Eigenschaften von vom Anwender gemeldetem Phishing“ auf **Ja** gesetzt ist. Details siehe Definieren Sie Eigenschaften für vom Anwender gemeldetes Phishing.



Zugehörige Phishing-E-Mails

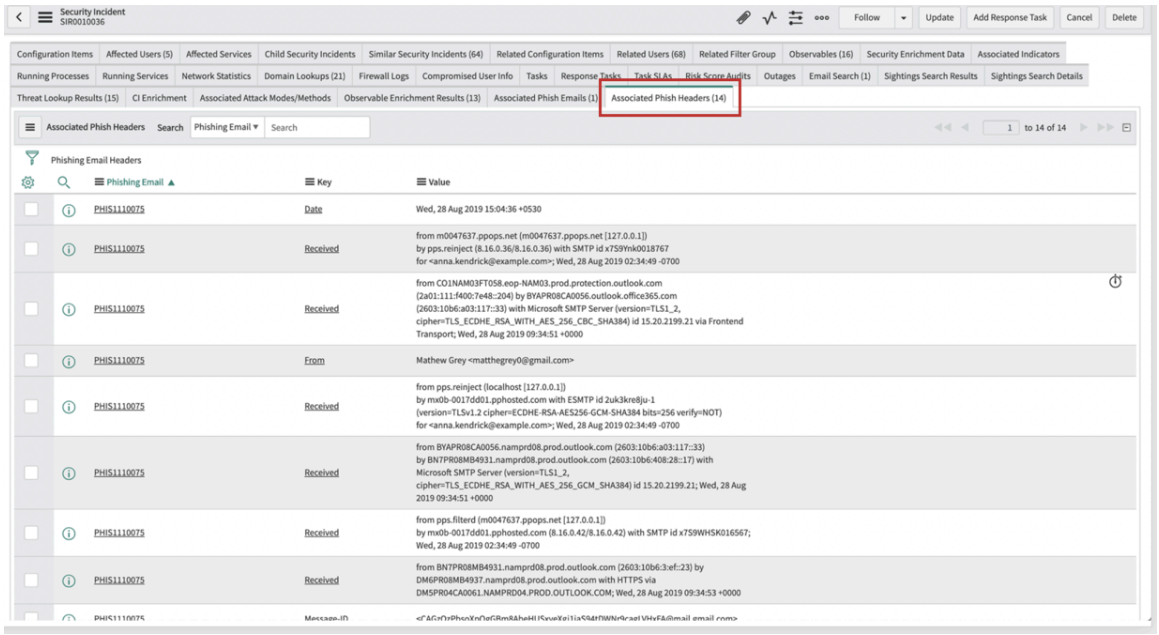
Klicken Sie auf die Registerkarte **Zugehörige Phishing-E-Mails**. Sie sehen eine Liste der Phishing-E-Mail-Datensätze (doppelte Datensätze), die dem übergeordneten Phishing-E-Mail-Datensatz zugeordnet sind.



Zugehörige Phishing-E-Mail-Header

Klicken Sie auf die Registerkarte **Zugehörige Phishing-E-Mails**. Sie sehen die Headerdetails der Phishing-E-Mail, die als Teil des Security Incident erfasst wurden. Sie können die Rollup-Header aller untergeordneten Datensätze und Phishing-E-Mail-Datensätze anzeigen, die im übergeordneten Security Incident zusammengefasst sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

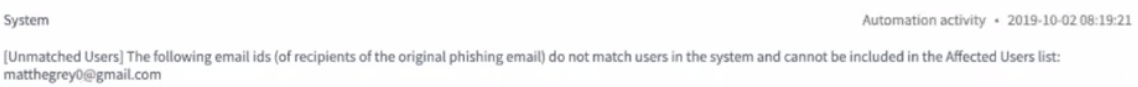


Erkennbare Elemente der zulässigen Liste

Während der -Flow Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um ausgeführt wird, können Sie den Status des Security Incidents überwachen. Wenn bestimmte erkennbare Elemente als erkennbare Elemente der zulässigen Liste markiert sind, werden sie nicht der zugehörigen Liste „Erkennbare Elemente“ hinzugefügt. Indem Sie die erkennbaren Elemente für die Zulassungsliste markieren, können Sie sicherstellen, dass nur die wichtigen Details angezeigt werden. Wenn beispielsweise www.google.com eine der URLs ist, die als zulässige Liste markiert wurden, wird die folgende Systemnachricht angezeigt. Die zulässigen erkennbaren Elemente der Liste stellen sicher, dass nur die wichtigen erkennbaren Elemente überwacht werden.

Nicht abgeglichene Anwender werden erfasst

Einige E-Mail-IDs in der Liste „An“ und „CC“ der Phishing-E-Mail gehören möglicherweise nicht zu Anwendern in der Organisation. Diese E-Mail-IDs werden als nicht übereinstimmende Anwender kategorisiert und sind nicht in der zugehörigen Liste „Betroffene Anwender“ enthalten. Es wird eine Arbeitsnotiz angezeigt, die angibt, dass dies Benutzer ohne Übereinstimmung sind.

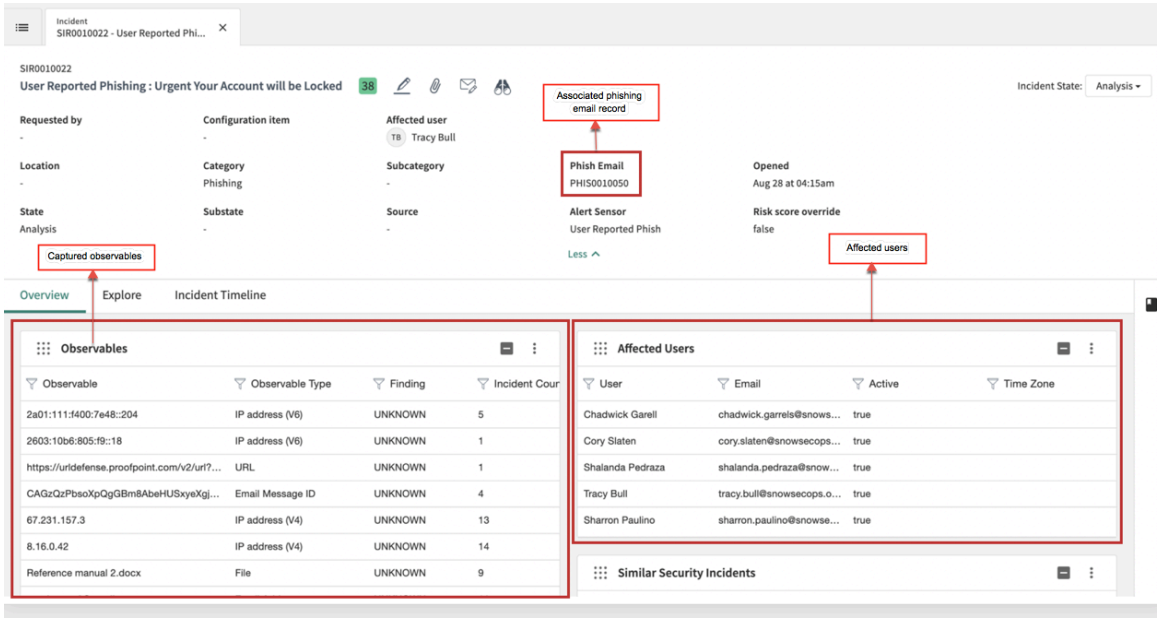


Von Benutzer gemeldetes Phishing im Arbeitsbereich für Sicherheitsanalysten

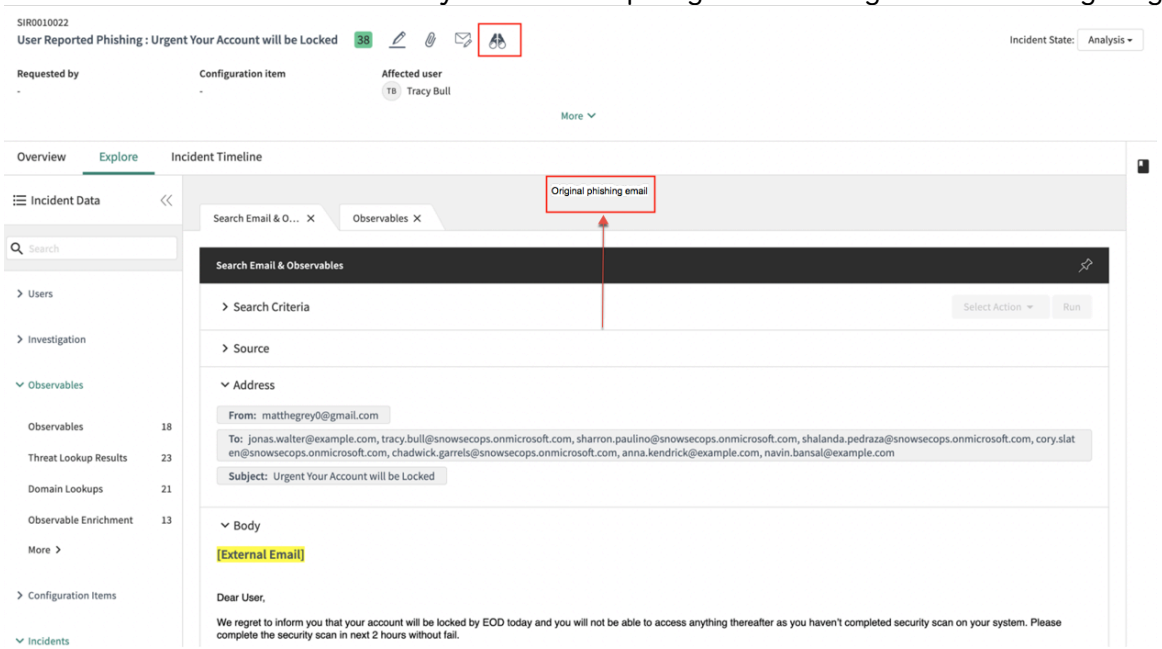
Sie können Security Incidents, die den Phishing-E-Mail-Datensätzen zugeordnet sind, im Arbeitsbereich für Sicherheitsanalysten anzeigen.

Navigieren zu **Security Incident** > **Neue UI**. Der -Arbeitsbereich wird in einer separaten Browser-Registerkarte geöffnet. Klicken Sie auf den Security Incident, der dem Phishing-E-Mail-Datensatz zugeordnet ist, um den Security Incident anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

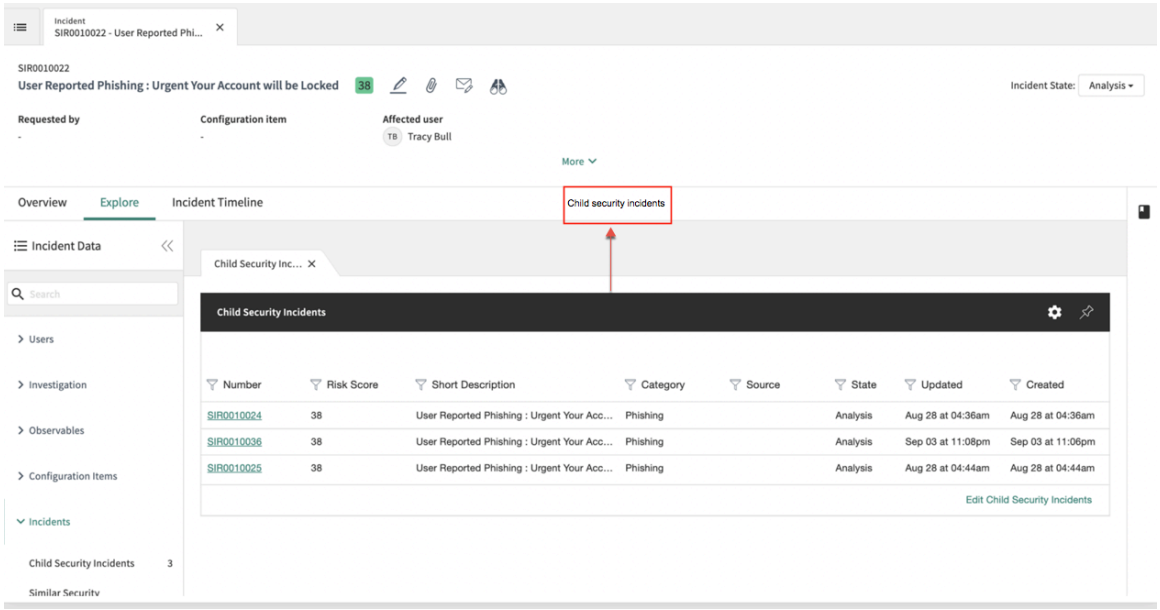


Klicken Sie auf das Feldstecher-Symbol. Die ursprüngliche Phishing-E-Mail wird angezeigt.

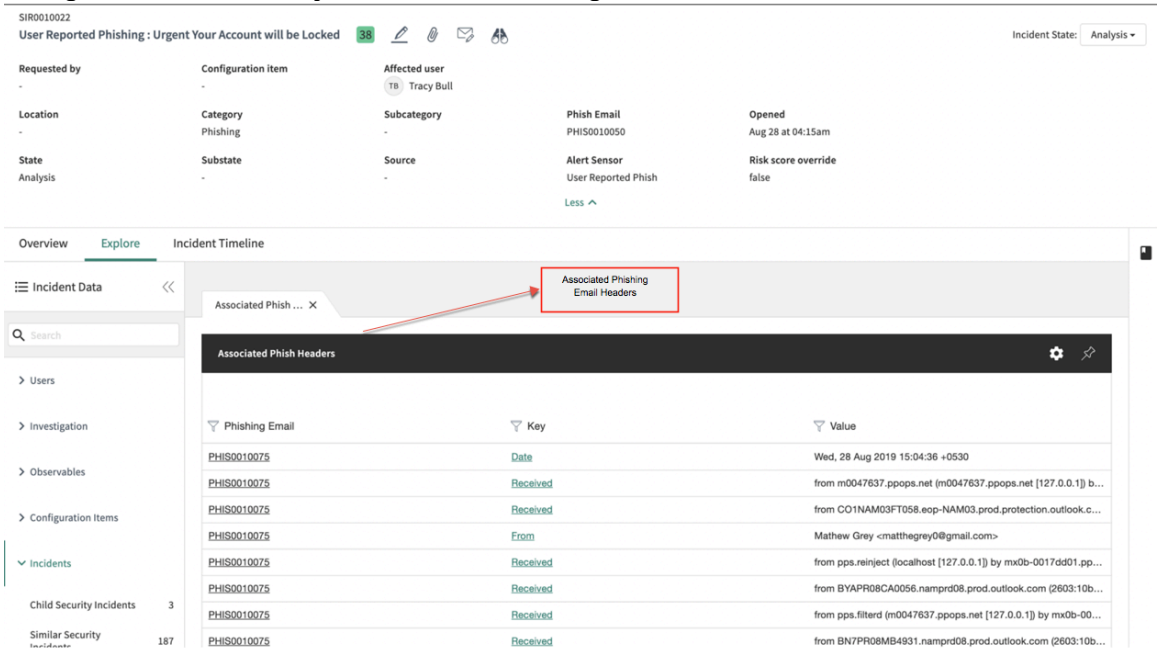


Klicken Sie auf der Registerkarte **Erkunden** auf **Incidents** > **Untergeordnete Security Incidents**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

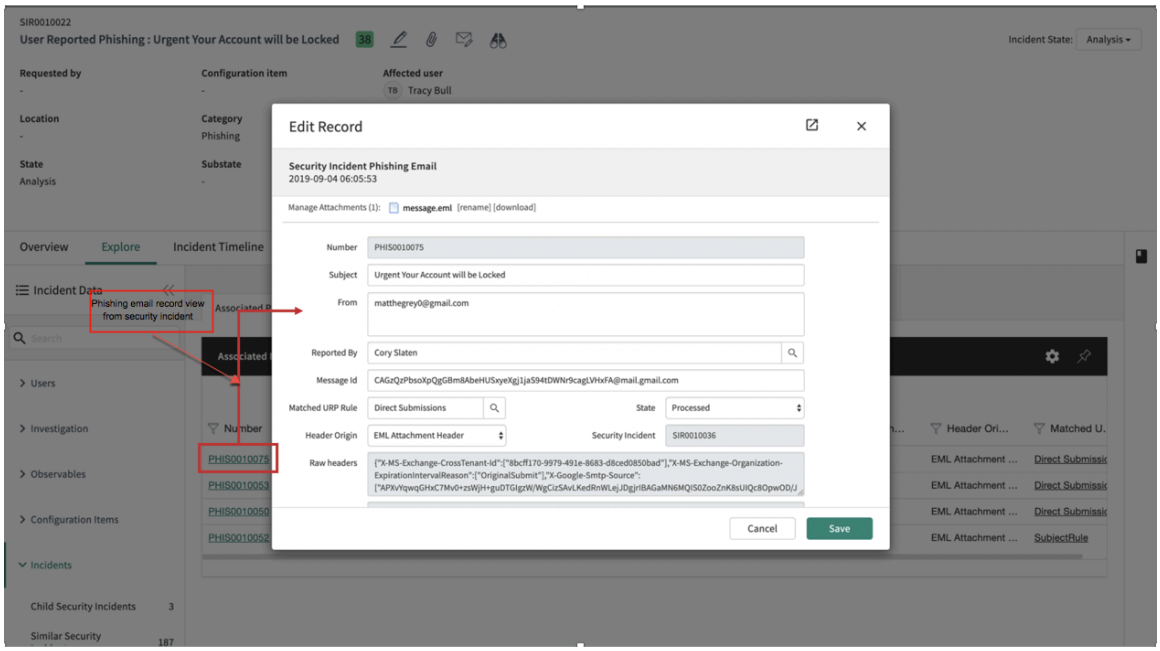


Klicken **Incidents** > **Zugehörige Phishing-Header** > . Sie können die aufgerollten Header aller untergeordneten Datensätze und Phishing-E-Mail-Datensätze anzeigen, die im übergeordneten Security Incident zusammengefasst sind.

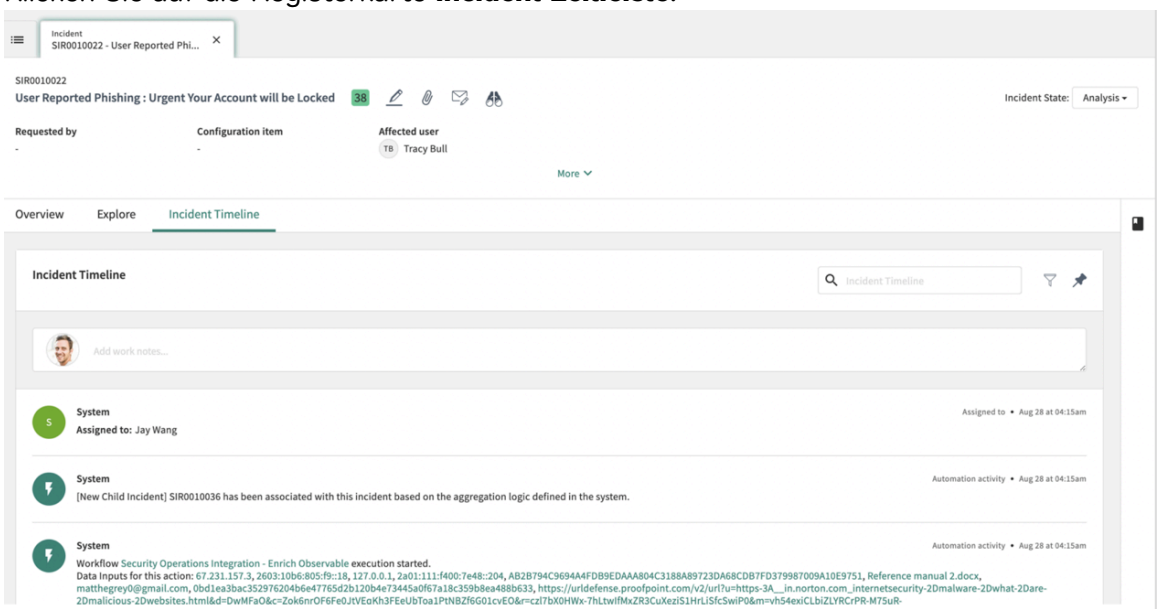


Klicken Sie auf den Phishing-E-Mail-Link, um den Phishing-E-Mail-Datensatz anzuzeigen, der dem Security Incident zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie auf die Registerkarte **Incident-Zeitleiste**.



Sie können die Systemupdates anzeigen, die Folgendes hervorheben:

- Es wurden doppelte untergeordnete Datensätze identifiziert.
- Erkennbare Elemente der zulässigen Liste.
- Anwender ohne Übereinstimmung, die die Phishing-E-Mail erhalten haben, aber nicht zur Liste der betroffenen Anwender gehören.

Häufige Fragen

Dieser Abschnitt behandelt einige der häufig gestellten Fragen zur erweiterten Funktion „Von Benutzern gemeldetes Phishing“.

1. Ich habe die neue Security Incident Response-Spoke installiert, kann jedoch keine von Anwendern gemeldeten Phishing-Incidents anzeigen.

   Standardmäßig wurde die Funktion „Vom Anwender gemeldetes Phishing“ deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese Funktion zu aktivieren, müssen Sie eine Kopie des schreibgeschützten Wandeln Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents um -Flows erstellen und ihn vor der Verwendung aktivieren.

2. Welche Vorsichtsmaßnahmen werden bei der Erfassung von Phishing-E-Mails und deren Umwandlung in Security Incidents im Umgang mit schädlichen Links und Anhängen in Phishing-E-Mails verwendet?

   Der Antivirenscanner ServiceNow scannt diese schädlichen Anhänge und Links. Um jedoch sicherzustellen, dass Sicherheitsanalysten die Incidents genau untersuchen können, erfasst die Anwendung Security Incident Response alle Artefakte, die Teil einer Phishing-E-Mail sind. Die Funktion „Vom Anwender gemeldetes Phishing“ deaktiviert jedoch die schädlichen Links in Phishing-E-Mails, damit Sicherheitsanalysten nicht versehentlich auf diese Links klicken. Sicherheitsanalysten müssen beim Herunterladen schädlicher Anhänge vorsichtig sein.

3. Erfassen wir alle schädlichen Dateien, die Teil der Phishing-E-Mails sind, um die Ergänzung zu Security Incidents zu ermöglichen?

   Ja, wir erfassen alle Dateien aus den Phishing-E-Mails. Sie können diese Details als Teil von erkennbaren Elementen für Security Incidents in Form eines Datei-Hashs anzeigen.

4. Senden wir schädliche Dateien und Links aus Phishing-E-Mails zur Untersuchung an eine Sandbox-Instanz?

   Derzeit unterstützen wir keine sofort einsatzbereiten Sandbox-Integrationen für die Untersuchung schädlicher Dateien und Links.

5. Gibt es ein Zeitfenster oder einen Auslöser, das die Dauer definiert, in der eingehende doppelte Phishing-E-Mail-Datensätze einem übergeordneten Security Incident zugeordnet werden?

   Doppelte Phishing-E-Mail-Datensätze werden nur für einen aktiven übergeordneten Security Incident zusammengefasst. Wenn der übergeordnete Incident geschlossen oder abgebrochen wird, wird die eingehende neue doppelte Phishing-E-Mail als neuer Security Incident erstellt. In diesem Szenario können Sie jedoch innerhalb des neuen Security Incident den geschlossenen oder abgebrochenen übergeordneten Security Incident in der zugehörigen Liste **„Ähnliche Security Incidents“** anzeigen.

   Hinweis:
   Dieses Verhalten kann mit dem Flow Designer konfiguriert werden.

6. Unterstützt die Funktion „Phishing-Bericht für Anwenderberichte“ nur die Verwendung des Microsoft Outlook **PhishAlarm-** Plugins (früher bekannt als Wombat) zum Erfassen von E-Mail-Headerdetails?

   Die Funktion „Vom Anwender gemeldet“ wurde zum Analysieren von E-Mail-Headern entwickelt und entspricht den RFC822-Standards. Ähnlich wie das **PhishAlarm** -Plugin (früher als Wombat bezeichnet) werden alle anderen Microsoft Outlook-Plugins unterstützt, die E-Mail-Header basierend auf den RFC822-Standards erfassen.

Datensatzerstellung aus Security Incidents

Nachdem Sie einen Security Incident erstellt und gespeichert haben, können Sie daraus einen Change Request (CHG)-, Incident- (INC) oder Problem-Datensatz (PRB) erstellen. Sie können auch einen Kundenservicefall aus jedem Security Incident erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Change, einen Incident oder ein Problem aus einem Security Incident

Nachdem Sie einen Security Incident erstellt und gespeichert haben, können Sie daraus einen Change Request (CHG)-, Incident- (INC) oder Problem-Datensatz (PRB) erstellen.

Vorbereitungen

Erforderliche Rolle: sn.si_basic oder höher

Prozedur

1. Öffnen Sie einen Security Incident mit einer dieser Methoden.
   - Öffnen Sie einen vorhandenen Security Incident, indem Sie zu navigieren **Security Incident** > **Nicht zugewiesen** > **Incidents**, und klicken Sie auf einen Security Incident.
   - Erstellen Sie einen Security Incident, indem Sie zu navigieren **Security Incident** > **Nicht zugewiesen** > **Incidents**, klicken Sie auf **Neu**, füllen Sie das Formular aus, und speichern Sie den Datensatz.
2. Klicken Sie mit der rechten Maustaste auf den Header des Security Incidents, und klicken Sie auf eine der folgenden Optionen:
   - **Change erstellen**
   - **Incident erstellen**
   - **Problem erstellen**

   Hinweis:
   Diese Auswahl gilt nur, wenn die Popup-Eigenschaft (sn_vul.popup) aktiviert ist. Wenn Sie auf eine dieser Schaltflächen klicken, wird ein Vorschaufenster geöffnet, in dem die Informationen aus dem Security Incident angezeigt werden, die zum Erstellen des Change, Incident oder Problem verwendet wurden. Das heißt das Konfigurationselement, sein Standort, seine Priorität sowie die Kurz- und Langbeschreibungen. Wenn Sie eine Change-Anforderung erstellen, können Sie die Felder **Priorität**, **Kurzbeschreibung**und **Beschreibung** bearbeiten. Wenn Sie einen Incident erstellen, können Sie die Felder **Auswirkung**, **Dringlichkeit**, **Kurzbeschreibung** und **Beschreibung** bearbeiten. Die Felder im zugehörigen Bildschirm „Security Incident“ sind nicht betroffen.
3. Klicken Sie auf **Absenden**, um den Change, den Incident oder das Problem zu erstellen.

Erstellt einen Kundenservicefall aus einem Security Incident

Security Incident Response wird mit einer Standardfeldzuordnung geliefert, die einen Security Incident einem Kundenservice (CS)-Fall zuordnet. Sie können einen CS-Fall aus einem beliebigen Security Incident erstellen, die **Priorität**bearbeiten und **optionale Notizen**hinzufügen.

Vorbereitungen

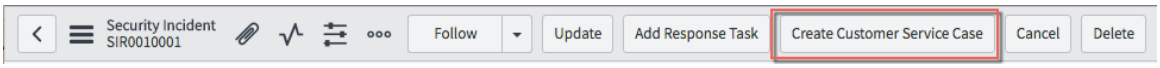
Erforderliche Rolle: sn_si.basic und sn_customerservice_agent

Hinweis:
Zum Ausführen dieser Aufgabe muss das Plugin Kundenservice aktiviert sein.

Prozedur

1. Navigieren Sie zu **Security Incident**.
2. Öffnen Sie den Security Incident, dem Sie einen CS-Fall hinzufügen möchten.
3. Klicken Sie im oberen Header **auf Kundenservicefall erstellen**.

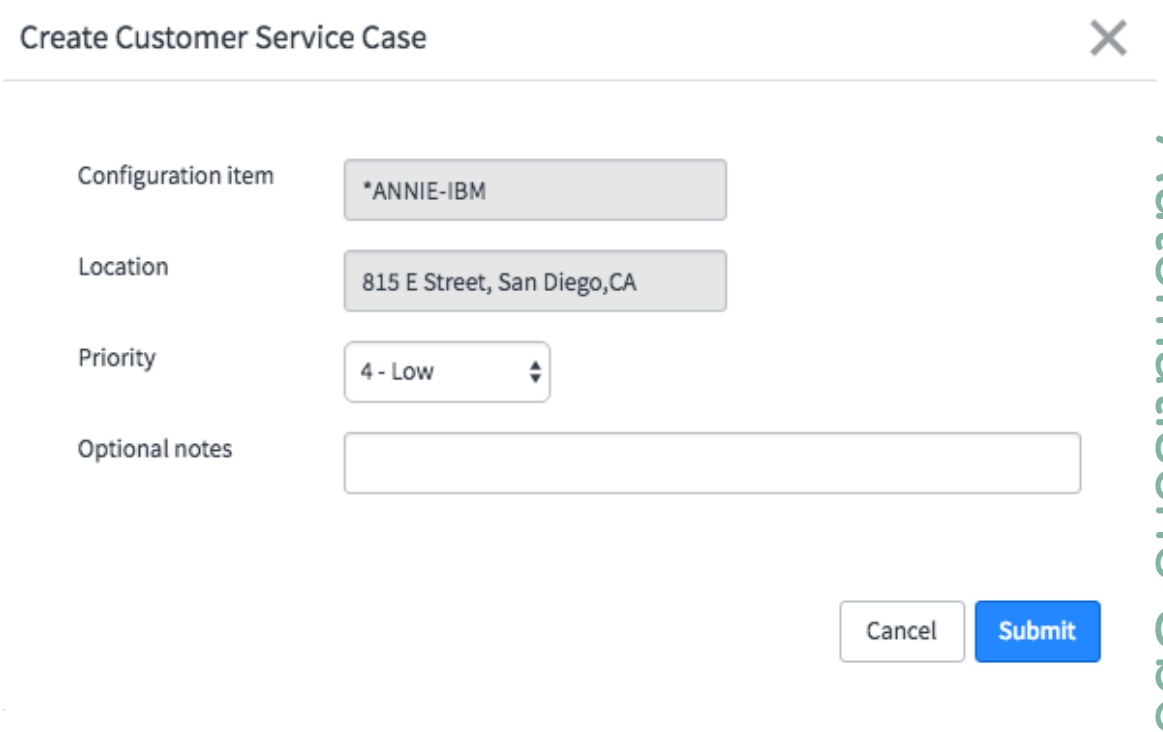
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Popup-Fenster ist basierend auf Ihrer Feldzuordnung bereits mit Informationen aus dem Security Incident gefüllt.

4. Sie können eine neue **Priorität** auswählen und **optionale Notizen**hinzufügen.

Hinweis:
Das Feld **Priorität** überschreibt die Standardeinstellung. Die **optionalen Hinweise** werden an den Incident angehängt.



5. Klicken Sie auf **Absenden**.
Ein CS-Fall wird erstellt und in der zugehörigen Liste „Customer Service Cases“ (Kundenservicefälle) im Security Incident angezeigt.
6. Sie können auf den CS-Falllink klicken, um den Fall nachzuverfolgen.

Zugehörige Informationen

Fallmanagement für den Kundenservice

Fügen Sie einem Sicherheitsfall einen Security Incident hinzu

Wenn Sie feststellen, dass ein Security Incident eine höhere Analyseebene erfordert, fügen Sie ihn einem neuen oder vorhandenen Fall hinzu.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

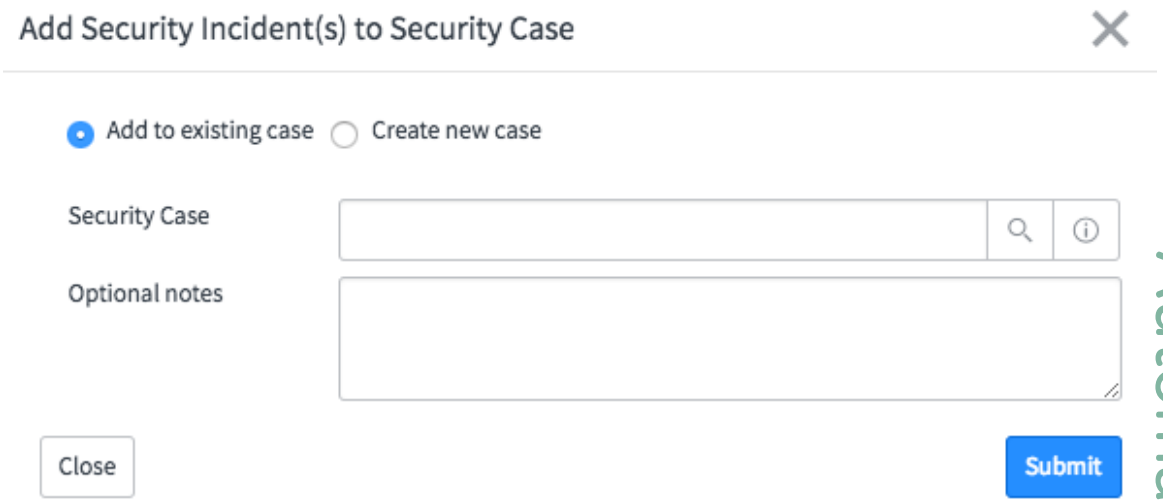
Erforderliche Rolle: sn_si.admin, sn_ti.case_user_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu dem Security Incident, der eine Eskalation erfordert, indem Sie auf klicken **Security Incident** > **Incidents** > **Mir zugewiesen**, und öffnen Sie den Security Incident.
2. Klicken Sie auf den zugehörigen Link **Zu Sicherheitsfall hinzufügen**.
   Das Dialogfeld **„Security Incident(s) zum Sicherheitsfall hinzufügen“** wird geöffnet.



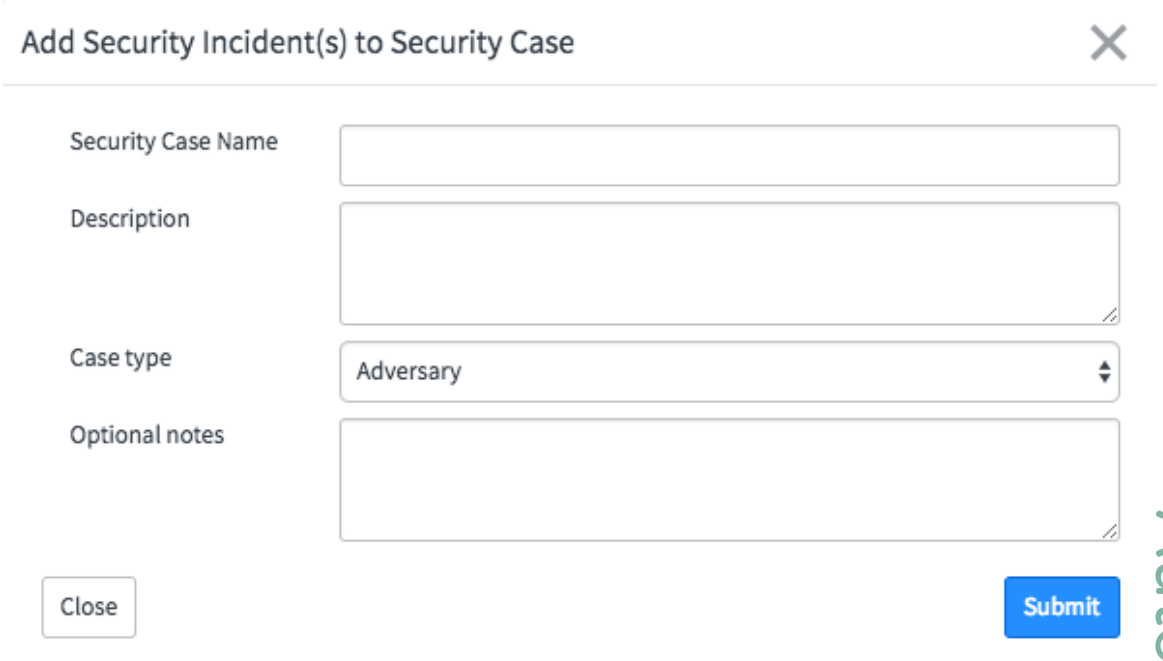
3. Wenn Ihnen ein Fall zugewiesen ist, dem Sie diesen Security Incident hinzufügen möchten, füllen Sie die Felder entsprechend aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
Sicherheitsfall	Wählen Sie den Sicherheitsfall aus.
Optionale Notizen	Geben Sie bei Bedarf zusätzliche Notizen ein, die für den Fallanalysten von Wert sein könnten.

4. Wenn Ihnen ein oder mehrere Fälle zugewiesen sind, Sie jedoch einen neuen Fall erstellen und ihm den Security Incident zuweisen möchten, klicken Sie auf **Neuen Fall erstellen,** um zusätzliche Felder anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wenn Ihnen keine Fälle zugewiesen sind, wird zuerst der obige Bildschirm geöffnet.

5. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Name des Sicherheitsfalls	Geben Sie den Namen des neuen Sicherheitsfalls ein.
Beschreibung	Geben Sie eine Beschreibung für den Fall ein.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus.
Optionale Notizen	Geben Sie bei Bedarf zusätzliche Notizen ein, die für den Fallanalysten von Wert sein könnten.

6. Klicken Sie auf **Absenden**.
Im oberen Bereich des Security Incident wird eine Nachricht zusammen mit einem Link zum neuen Fall angezeigt.

Zugehörige Informationen

Security Case Management

Erstellen Sie Antwortaufgaben

Nachdem ein Security Incident erstellt wurde, können Sie Antwortaufgaben erstellen, um einzelne Aktionen nachzuverfolgen, die als Reaktion auf das Sicherheitsproblem auszuführen sind.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zum entsprechenden Speicherort, um den Security Incident zu öffnen, für den Sie Aufgaben erstellen möchten.
   Zum Beispiel:
   - Um eine Antwortaufgabe basierend auf einem Ihnen zugewiesenen Security Incident zu erstellen, wählen Sie **Security Incident** > **Incidents** > **Mir zugewiesen**.
   - Um eine Antwortaufgabe basierend auf einem Ihrem Team zugewiesenen Security Incident zu erstellen, wählen Sie **Security Incident** > **Incidents** > **Dem Team zugewiesen** > **Incidents**.
   - Um eine Antwortaufgabe basierend auf einem nicht zugewiesenen Security Incident zu erstellen, wählen Sie **Security Incident** > **Incidents** > **Nicht zugewiesene Incidents**.
2. Öffnen Sie den Security Incident, für den Sie Antwortaufgaben hinzufügen möchten.
3. Klicken Sie im Header des Formulars auf die Schaltfläche **Antwortaufgabe hinzufügen**.

   Hinweis:
   Um eine andere Aufgabe zu erstellen, klicken Sie in der zugehörigen Liste des incident auf die Registerkarte **Aufgaben**.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Security Incident

Feld	Beschreibung
Sicherheits-Tag auswählen	Wenn Sie Sicherheits-Tagseinrichten und aktivieren, können Sie ein oder mehrere Tags auswählen, um dem Datensatz Metadaten hinzuzufügen, oder den Grad der Vertraulichkeit der Antwortaufgabe angeben. Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Nummer	[Schreibgeschützt] Die automatisch generierte Zahl Security Incident Response.
Übergeordnet	[Schreibgeschützt] Die Nummer des zugehörigen Security Incidents.
Konfigurationselement	Das von dem Sicherheitsproblem betroffene Konfigurationselement (Ressource).
Betroffener Anwender	Die von dem Sicherheitsproblem betroffene Person.
Priorität	Die Priorität, mit der bestimmt wird, wann diese Aufgabe ausgeführt wird.
Status	Der aktuelle Status der Sicherheitsantwortaufgabe. Bei Erstellung der Aufgabe wird dieses Feld standardmäßig auf **Entwurf**gesetzt.
Kompetenzen	Die für die Ausführung dieser Aufgabe erforderliche Kompetenz. Klicken Sie auf das Schlosssymbol, und wählen Sie die gewünschte Kompetenz aus. Nachdem Sie Ihre Auswahl abgeschlossen haben, klicken Sie erneut auf das Sperrsymbol.
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Person, der die Ausführung der Aufgabe zugewiesen ist.
Kurzbeschreibung	Eine Beschreibung der Aufgabe Security Incident Response.
Beschreibung	Eine Beschreibung für die ausgewählte Aufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sichere Notizen	Arbeitsnotizen, die verschlüsselt und für den Kunden nicht sichtbar sind.
Arbeitsnotizen	Die Arbeitsnotizen, die für den Kunden nicht sichtbar sind.
Zusätzliche Anmerkungen	Kommentare, die für den Kunden sichtbar sein sollen.

5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Hinweis:
Nachdem Sie Security Incident Response -Aufgaben erstellt haben, können Sie sie mit einer der folgenden Anwendungen im Modul **„Antwortaufgaben“** anzeigen:

- **Mir zugewiesen**.
- **Dem Team zugewiesen**.
- **Offene Aufgaben anzeigen**
- **Alle Aufgaben anzeigen**
- **Nicht zugewiesene Aufgaben**.

Verwalten Sie Predictive Intelligence für von Anwendern gemeldete Phishing-Meldung

Die Funktion „Predictive Intelligence für von Anwendern gemeldetes Phishing“ bietet eine leistungsstarke Lösung für die Selektierung und Priorisierung von von Anwendern gemeldeten Phishing-E-Mails.

In diesem Abschnitt wird Folgendes beschrieben:

- Predictive Intelligence für Phishing-Meldungen von Anwendern
- Erforderliche Komponenten und Plugins
- Generierung des endgültigen Urteils für vom Anwender gemeldetes Phishing
- Fehlerbehebung bei Predictive Intelligence für von Anwendern gemeldetes Phishing

Predictive Intelligence für Phishing-Meldungen von Anwendern

Diese Funktion unterstützt Sicherheitsanalysten beim Selektieren und Priorisieren von von Anwendern gemeldeten Phishing-E-Mails.

Das Predictive Intelligence-Framework bietet Lösungen zum Trainieren des Systems für die Vorhersage, Empfehlung und Organisation von Datenergebnissen. Weitere Informationen zu Predictive Intelligence finden Sie unter Predictive Intelligence. Mit diesem Framework können Sie Modelle erstellen, um automatisch vorherzusagen, ob eine von einem Anwender gemeldete Phishing-E-Mail verdächtig oder legitim ist.

Mithilfe von Verlaufsdaten zu Security Incidents, die von Anwendern zu Phishing gemeldet wurden (E-Mail-Header, E-Mail-Text und Selektierungsergebnisse, die durch die Abschlusscodes für Security Incidents erfasst wurden) können Sicherheitsanalysten das System trainieren, um die eingehenden, von Anwendern gemeldeten Phishing-Übermittlungen als solche zu klassifizieren, die weiter selektiert werden müssen (wahrscheinlich). verdächtig) und solche, bei denen es sich um legitime Übermittlungen handelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch die automatische Selektierung eingehender E-Mails können Sicherheitsanalysten die Incident-Warteschlange einfach priorisieren und sich auf Incidents konzentrieren, die wahrscheinlich in erster Linie ein Risiko für das Unternehmen darstellen, und weniger Aufwand für E-Mails aufwenden, bei denen die Wahrscheinlichkeit hoch ist, dass sie falsch positiv sind. Das Vorhersageergebnis liefert auch eine Vertrauensbewertung für die Klassifizierung, um eine granulare Priorisierung zu ermöglichen.

Erforderliche Komponenten und Plugins

Um Predictive Intelligence für von Anwendern gemeldetes Phishing zu verwenden, müssen Sie die folgenden Anwendungen installieren

Plugin-Name	Mindestversion
Security Incident Response	9.0.1 oder 10.0.2
Predictive Intelligence	Orlando-Version
Predictive Intelligence für Phishing-Meldungen von Anwendern	10.0.2

Hinweis:
Die folgenden neuen Verbesserungen sind mit Security Incident Response 10.4 verfügbar:

- Die Möglichkeit, Abschlusscodes aus anwenderdefinierten Feldern für das Modelltraining auszuwählen.
- Die Möglichkeit, Vorhersagen nach der Modellerstellung explizit zu aktivieren.
- Die Möglichkeit, mithilfe einer Entscheidungstabelle ein endgültiges Urteil über die Übermittlung von vom Anwender gemeldetem Phishing zu generieren. (erfordert Security Operations-Spoke 10.3.0)

Um die neuen Erweiterungen zu verwenden, müssen Sie die folgenden Anwendungen aktualisieren:

Plugin-Name	Führen Sie ein Upgrade auf durch
Security Incident Response	10.0.4
Predictive Intelligence für Phishing-Meldungen von Anwendern	10.3.1

Neue und aktualisierte Tabellen

- sn_sir_ml_urp_config (Neu): Enthält die Konfiguration für die URP-ML-Anwendung.
- sn_sir_ml_urp_feature (neu): Aus der E-Mail-Tabelle „sn_si_phishing“ extrahierte Datensätze.
- sn_sir_ml_urp_feature_import (Neu): Wird zum Hochladen historischer Phishing-E-Mail-Daten verwendet.
- sn_si_incident (aktualisiert): Die folgenden neuen Felder wurden hinzugefügt:
  - Vorhersage akzeptiert
  - Ergebnis der Vorhersage
  - Vertrauensbewertung
- **Skripteinbindungen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- URPMLUtil: Ruft die Konfiguration ab, führt den Vorhersageauftrag aus und verfolgt den Vorhersageprozess.
- URPMLProcessor: Extrahiert und verarbeitet Daten aus der Tabelle „sn_si_phishing_email“.
- URPMLAction: Führt einen Flow aus, um das Vorhersageergebnis zu akzeptieren.

Generierung des endgültigen Urteils für vom Anwender gemeldetes Phishing

Security Incident Response-Teams können jetzt das endgültige Urteil für einen von einem Benutzer gemeldeten Phishing-Datensatz basierend auf den Ergebnissen von Predictive Intelligence- und Bedrohungsanreicherungsintegrationen treffen.

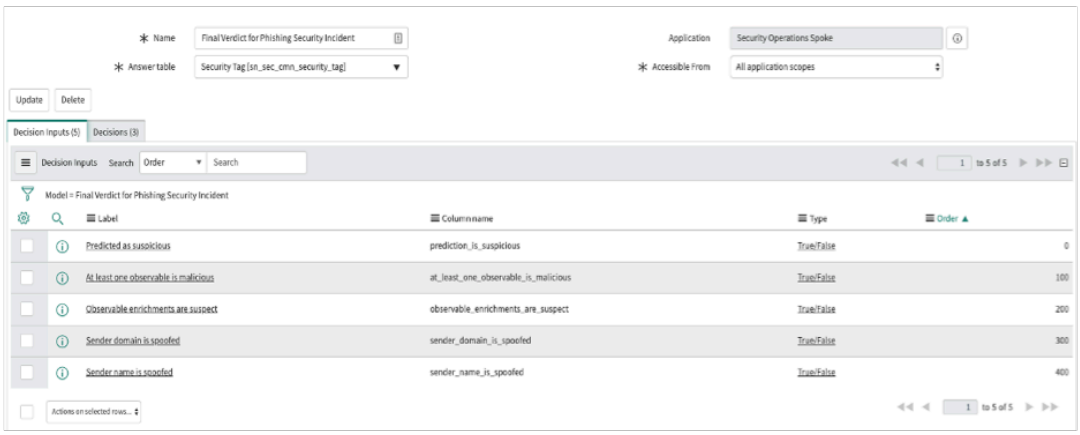
Diese Generierung des endgültigen Urteils wird durch ein Entscheidungstabellenkonstrukt aktiviert und in einem Flow genutzt.

Voraussetzungen

Stellen Sie sicher, dass alle in Erforderliche Komponenten und Plugins aufgeführten Plugins installiert wurden.

Navigieren zu **Predictive Intelligence für Phishing** > **Endgültiges Urteil** > **Endgültiges Urteil für Phishing-Security-Incident**.

Auf der Registerkarte **„Entscheidungseingaben“** werden die verschiedenen Bedingungen angezeigt, die ausgewertet wurden, um zum endgültigen Urteil zu gelangen.



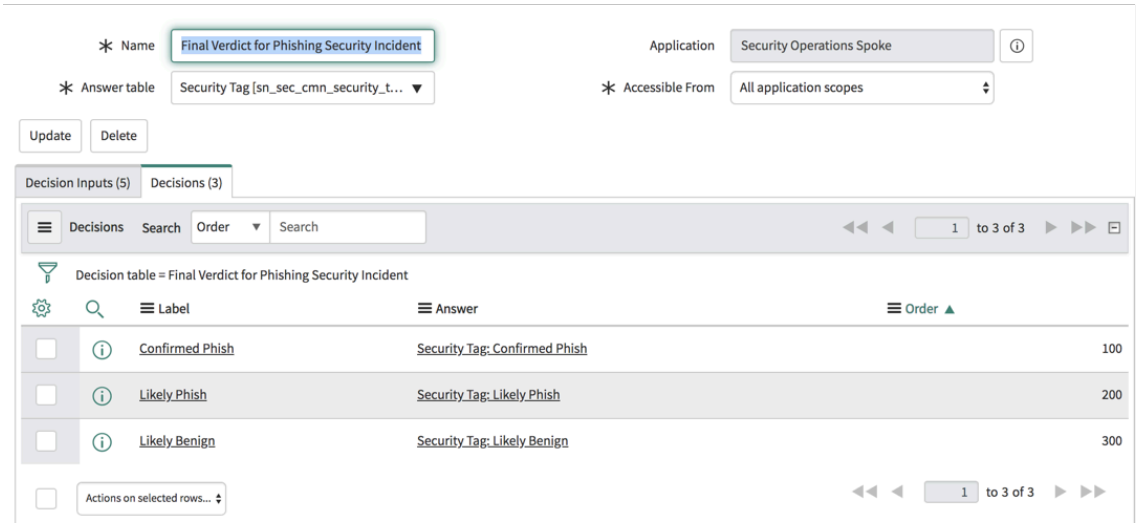
Die folgenden Bedingungen sind mit dem Basissystem verfügbar:

- Als verdächtig vorhergesagt: Wenn Predictive Intelligence die vom Benutzer gemeldete Phishing-E-Mail als **verdächtig**klassifiziert hat.
- Mindestens ein erkennbares Element ist schädlich: Wenn ein an dem Security Incident beteiligtes erkennbares Element (z. B. URL, Domäne, IP, Hash) von Threat Intelligence-Quellen als **schädlich** eingestuft wurde.
- Ergänzung erkennbarer Elemente ist verdächtig: Wenn die Ergänzung erkennbarer Elemente (z. B. Aktualität der Phishing-Domänenregistrierung, Land der Phishing-Domänenregistrierung) als verdächtig eingestuft wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Absenderdomäne ist gefälscht: Wenn der Verdacht besteht, dass die E-Mail-Domäne des Phishing-Fälschers eine vertrauenswürdige Domäne manipuliert.
- Absendername ist gefälscht: Wenn der Verdacht besteht, dass die E-Mail-Adresse des Phishing-Fälschers eines vertrauenswürdigen Mitarbeiters einer Organisation gefälscht wurde.

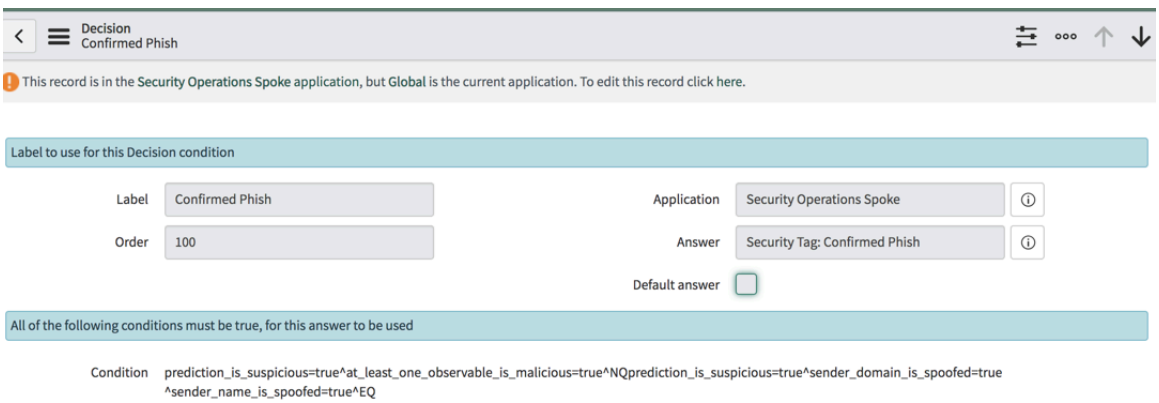
Die Registerkarte **„Entscheidungen“** zeigt die endgültigen Urteilsoptionen, die für einen bestimmten Security Incident getroffen werden können.



Die folgenden Entscheidungen sind mit dem Basissystem verfügbar:

- Bestätigtes Phishing: Wenn die Bedingungen dazu geführt haben, dass es sich bei dem endgültigen Urteil um eine bestätigte Phishing-E-Mail handelt.
- Wahrscheinlicher Phishing: Wenn die Bedingungen zu dem endgültigen Urteil als potenzieller Phishing-Versuch geführt haben.
- Wahrscheinlich gutartig: Wenn die Bedingungen zu dem endgültigen Urteil als gutartige Übermittlung geführt haben.

Sie können die Bedingungen sehen, die für jede der endgültigen Urteilsoptionen ausgewertet wurden. Klicken Sie auf den Link Bezeichnung, um die Bedingungen anzuzeigen.



Sie können die mit dem Basissystem bereitgestellte Entscheidungstabelle anpassen oder eine eigene Entscheidungstabelle erstellen. Diese Entscheidungstabelle kann in Playbooks

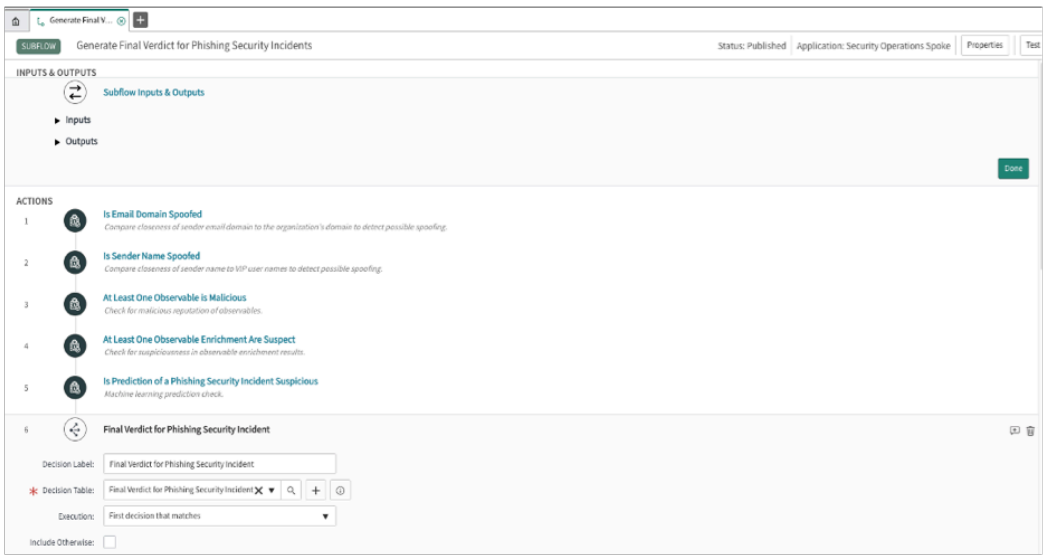
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für Security Incident Response genutzt werden. Der Subflow **„Endgültiges Urteil für Phishing-Security-Incidents generieren“** ist mit dem Basissystem verfügbar. Dieser Subflow generiert automatisch das endgültige Urteil für einen Phishing-Security Incident und wendet basierend auf dieser Entscheidung ein Sicherheits-Tag an. Sie können diesen Subflow als Teil des Playbooks **für automatisiertes Phishing** aufnehmen.

Die Eingaben für diesen Subflow sind:

- incident_id: Die Sys-ID des Phishing-Security Incidents.
- c_level_names: Kommagetrennte Liste von Namen (z. B. Namen von Führungskräften in der Organisation), die bei dem Phishing-Angriff wahrscheinlich gefälscht wurden.
- Trusted_domains: Kommagetrennte Liste der vertrauenswürdigen E-Mail-Domänen.
- richment_keywords: Kommagetrennte Liste von Stichwörtern, die die Bösartigkeit des erkennbaren Elements aus den Ergänzungsergebnissen angeben.
- sender_email (optional): Die E-Mail-Adresse des Absenders der Phishing-E-Mail.

Die Ausgabe dieses Flows kann **„Bestätigte Phishing“**, **„Wahrscheinliche Phishing“**oder **„Wahrscheinlich gutartig“**sein.



Fehlerbehebung bei Predictive Intelligence für von Anwendern gemeldetes Phishing

In diesem Abschnitt werden einige häufige Problemszenarien behandelt.

- Problem: Ich kann die Konfiguration von Predictive Intelligence nicht ändern.

  Lösung: Überprüfen Sie, ob Sie berechtigt sind. Sie müssen sich als Benutzer mit der Rolle ml_admin anmelden, um Schwellenwerte zu ändern. Einige Szenarien erfordern möglicherweise noch höhere Berechtigungen, wenn Sie beispielsweise das Trainingsdatenlimit ändern müssen. In solchen Szenarien müssen Sie sich an den Kundensupport wenden, um Unterstützung zu erhalten.

- Problem: Das Training des Modells ist fehlgeschlagen.

  Lösung: Überprüfen Sie, ob die URLs des ML-Planers eingerichtet wurden. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** und überprüfen Sie, ob die Eigenschaft *„glide.shared_service_scheduler.url“* konfiguriert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Problem: Vorhersageergebnisse sind für einen Security Incident nicht verfügbar.

  Lösung:

  - Überprüfen Sie, ob die Vorhersage-URL in der Systemeigenschaft *„glide.prediction_service.url“* eingerichtet wurde, und stellen Sie sicher, dass das Rechenzentrum mit der URL übereinstimmt.
  - Überprüfen Sie, ob die geplante Aufgabe „Von Anwender gemeldete Phishing-E-Mail vorhersagen“ aktiv ist.

Konfigurieren Sie Predictive Intelligence für von Anwendern gemeldete Phishing-Meldung

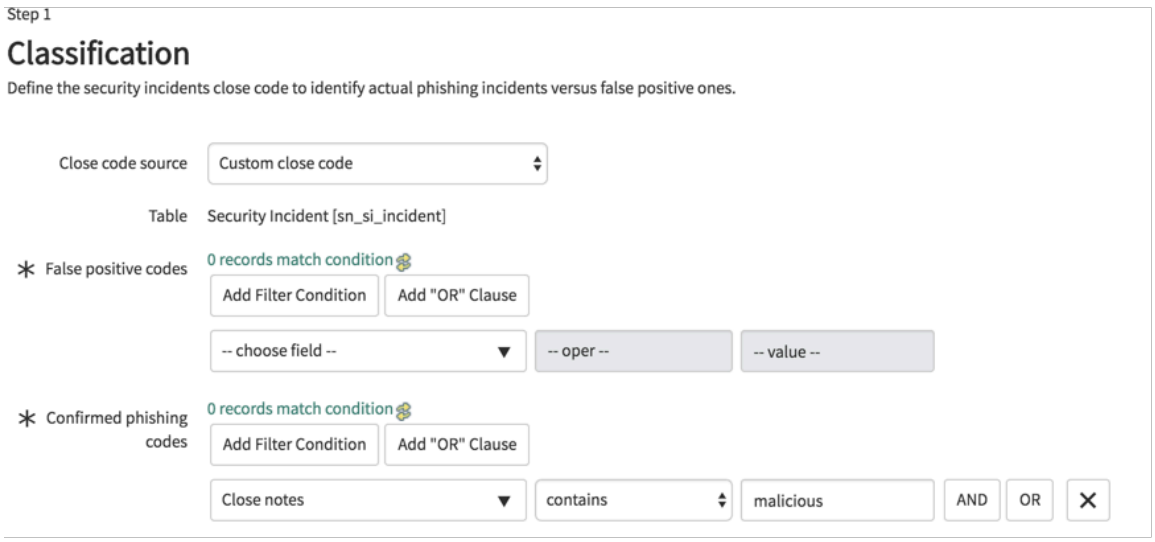
Konfigurieren Sie das Modell, und bereiten Sie es vor, um von Anwendern gemeldete Phishing-E-Mails zu identifizieren.

Vorbereitungen

Erforderliche Rolle: ml_admin

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence für Phishing** > **Konfiguration**.
2. Wählen Sie in Schritt 1 der Konfiguration eine der folgenden Optionen aus der Liste Lösungscodequelle aus:
   - Standard-Abschlusscode: Wählen Sie diese Option aus, um die standardmäßigen Abschlusscodes für Security Incidents anzugeben, die vom Trainingsmodell verwendet werden müssen, um schädliche und legitime E-Mails zu identifizieren. Klicken Sie auf das Sperrsymbol, und wählen Sie mindestens einen Falsch positive Codes oder Bestätigte Phishing-Codes aus.
   - Benutzerdefinierter Abschlusscode: Wählen Sie die Option Benutzerdefinierter Abschlusscode aus, wenn Sie Abschlusscodes aus anwenderdefinierten Feldern definieren möchten, die als Teil Ihrer vorhandenen Verfahren zur Reaktion auf Incidents verwendet werden können. Um einen Abschlusscode zu definieren, wählen Sie ein Feld aus der Tabelle „Security Incident“ aus, und geben Sie eine oder mehrere Filterbedingungen an.



3. Importieren Sie in Schritt 2 Verlaufsdaten, die zum Trainieren des Modells verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie die Datenquelle für den Import der Verlaufsdaten aus. Kann sein:

- Tabelle „Von Anwender gemeldete Phishing-E-Mail“: Sie können die Anzahl der Datensätze anzeigen, die als Verlaufsdaten importiert werden können. Wählen Sie diese Option aus, und klicken Sie auf **Importieren**.
- Anwenderdefinierte Datenquelle: Sie können eine einzelne formatierte CSV-Datei anhängen, die historische Datensätze enthält. Wählen Sie die Datei aus, und klicken Sie auf **Importieren**.

Hinweis:
Die CSV-Datei, die Sie importieren, muss die folgenden Header enthalten:

- Bezeichnung
- Header
- Haupttext

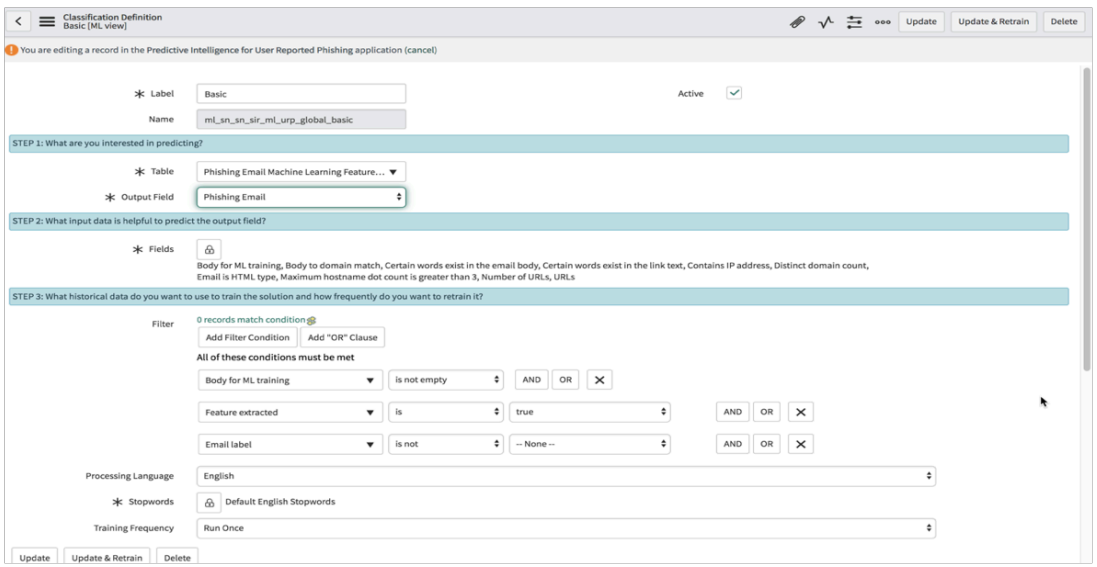
Jeder Datensatz muss in der Spalte „Bezeichnung“ in der CSV-Datei ein Tag für „Böswillig“ oder „Legitim“ enthalten.

Klicken Sie auf **Import abbrechen,** um den Import der Daten zu beenden. Der Importvorgang wird abgebrochen, und alle bisher importierten Datensätze werden gelöscht.

4. Nachdem Sie die Verlaufsdaten importiert haben, klicken Sie auf den Link, um die Seite zu aktualisieren. Sie können dann entweder weitere Trainingsdaten importieren oder mit dem nächsten Schritt fortfahren.
5. Überprüfen Sie in Schritt 3, ob die Anzahl der für das Training verfügbaren Datensätze die Mindestanforderungen erfüllt.

Hinweis:
Die Standardwerte für die maximale und minimale Anzahl von Trainingsdatensätzen werden angezeigt. Diese Schwellenwerte können auf der Seite mit den Eigenschaften von Platform Machine Learning geändert werden. Wenden Sie sich an den Kundensupport, um Unterstützung zu erhalten.

6. Wenn die Trainingsdaten ausreichend sind, klicken Sie auf **Modell trainieren**.
Sie können die Eingaben für das Training im Bildschirm unten aktualisieren.



7. Folgende Vorhersageeingaben können Sie ändern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Was möchten Sie vorhersagen?
- Welche Eingabedaten sind hilfreich, um das Ausgabefeld vorherzusagen?
- Welche Verlaufsdaten möchten Sie zum Trainieren der Lösung verwenden und wie häufig möchten Sie sie erneut trainieren?

Die Standardwerte für diese Eingaben werden angezeigt. Sie können sie ändern und auf eine der folgenden Optionen klicken:

- **Aktualisieren**: Aktualisiert die Definition des Trainingsmodells.
- **Aktualisieren und erneut trainieren**: Aktualisiert die Trainingsmodelldefinition und trainiert das Modell neu (löst die Funktion **„Modell trainieren“** aus).

8. Wenn Sie das Training des Modells abgeschlossen haben, aktivieren Sie abschließend das Kontrollkästchen **Vorhersage aktivieren**.
   Vorhersagen werden jetzt für jeden von einem Benutzer gemeldeten Phishing-Datensatz bereitgestellt, der dieses Modell verwendet. Wenn Sie keine Vorhersagen mehr für die vom Benutzer gemeldeten Phishing-Datensätze mehr abgeben möchten, deaktivieren Sie das Kontrollkästchen **Vorhersage aktivieren**, und klicken Sie auf **Deaktivieren**.

Sicherheitsanalysten werden zugewiesen

Abhängig von Ihren Einstellungen im Bildschirm SIR Administrationskonfiguration können Sie Sicherheitsanalysten manuell zu Security Incidents zuweisen. automatisch mithilfe eines Workflows; oder automatisch durch Verwendung der automatischen Zuweisung.

Manuelle Zuweisung von Analysten

Sie können den Bildschirm Security Incident Response Administrationskonfiguration so konfigurieren, dass Sicherheitsanalysten manuell zugewiesen werden, wenn jemand oder die Anwendung SIR einen Security Incident erstellt oder eine Sicherheitsantwortaufgabe generiert.

Wenn ein Security Incident oder eine Antwortaufgabe nicht automatisch zugewiesen werden kann, können Sie im Bildschirm SIR Administrationskonfiguration so festlegen, dass die manuelle Zuweisung von Sicherheitsanalysten erforderlich ist. Dies ist eine gute Option, wenn Sie eine begrenzte Anzahl von Sicherheitsanalysten für die Durchführung von Anforderungen haben oder wenn Sie diese einfach nicht automatisch zuweisen möchten.

Workflowbasierte Zuweisung von Sicherheitsanalysten

Sie können den Bildschirm Security Incident Response Administrationskonfiguration so konfigurieren, dass ein ausgewählter Workflow zur Zuweisung des Sicherheitsanalysten verwendet wird, wenn jemand oder die SIR-Anwendung einen Security Incident oder eine Sicherheitsantwortaufgabe erstellt.

Im Konfigurationsbildschirm für die Administration von Security Incidents können Sie einen Workflow verwenden, um jedem Security Incident oder jeder Security Response-Aufgabe einen Analysten zuzuweisen. Diese Option ist eine gute Wahl für Organisationen, die einen anwenderdefinierten Prozess zur Lösung von Sicherheitsproblemen verwenden oder einen automatisierten Prozess haben.

Automatische Zuweisung von Sicherheitsanalysten

Sie können den Bildschirm Security Incident Response Administrationskonfiguration so konfigurieren, dass der Sicherheitsanalyst automatisch zugewiesen wird, wenn jemand oder die Anwendung SIR einen Security Incident oder eine Sicherheitsantwortaufgabe erstellt. Die automatische Zuweisung ermöglicht es Ihnen, basierend auf den Anforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihrer Organisation die Kriterien zu definieren, nach denen Analysten automatisch Security Incidents zugewiesen werden.

Automatische Zuweisung von Service Desk-Mitarbeitern auf Grundlage von Mitarbeiterbewertungen

Wenn die automatische Zuweisung aktiviert ist und ein Security Incident oder eine Antwortaufgabe erstellt wird, werden die folgenden Aktionen ausgeführt:

- Die verfügbaren Sicherheitsanalysten werden basierend auf den in der Konfiguration definierten Kriterien bewertet.
- Der Aufgabe wird automatisch ein geeigneter Sicherheitsanalyst zugewiesen.
- Die Aufgabe wird in den Status **Zugewiesen** versetzt.

Wenn die Konfiguration so eingerichtet ist, dass mehr als ein Satz von Bedingungen berücksichtigt wird, z. B. Kompetenzen, Standort, Zeitzone oder Gruppenabdeckungsbereich, werden die Sicherheitsanalysten basierend auf den Einstellungen für die Gewichtungseigenschaft und anderen Kriterien bewertet. Diese Konfigurationseinstellungen helfen Ihnen bei der automatischen Zuweisung von Service Desk-Mitarbeitern basierend auf optionalen Eigenschaften. Die berechneten Bewertungen werden verwendet, um den besten Service Desk-Mitarbeiter für den Security Incident oder die Antwortaufgabe zu bestimmen. Im Konfigurationsbildschirm der Anwendung kann eine beliebige Kombination von bewertungsbasierten Methoden aktiviert werden.

Beim Erstellen einer Aufgabe wird eine Bewertung für jeden Typ der aktivierten Auswahlkriterien für alle verfügbaren Außendienstmitarbeiter berechnet. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die automatische Zuweisung berücksichtigt.

Die Einstellungen für die Gewichtungseigenschaften für automatische Zuweisungen finden Sie unter **Security Incident** > **Administration** > **Eigenschaften**, sind in den Bewertungsberechnungen enthalten.

Mit diesen Werten können Sie Prioritäten für die Auswahlkriterien für die automatische Zuweisung festlegen, die für Ihre Organisation wichtiger sind. Legen Sie die Prioritätswerte zwischen 1 (weniger wichtig) und 10 (wichtig) fest.

Ein Beispiel dafür, wie sich die Gewichtungseigenschaften auf die Bewertungen der Außendienstmitarbeiter auswirken, finden Sie unter Automatische Zuweisung von Service Desk-Mitarbeitern anhand mehrerer Auswahlkriterien.

Bereitschaftsplanung

Die Anwendung Bereitschaftsplanung hilft Ihnen, dafür zu sorgen, dass Mitglieder des dedizierten Support-Teams bereit stehen, um Probleme schon bei der Entstehung zu beheben. Sie können Rufbereitschaftszeitpläne, Dienstplanrotationen und Eskalationsrichtlinien einrichten, Benachrichtigungen für eine Gruppe eskalieren und den aktuellen Kontakt für eine Eskalation bestimmen. Die Anwendung identifiziert das zugewiesene und verfügbare Mitglied einer Supportgruppe, z. B. beim Zuweisen eines incident. Weitere Informationen finden Sie unter On-Call Scheduling . Die Bereitschaftsplanung für Security Incident Response funktioniert genauso.

Automatische Zuweisung von Außendienstmitarbeitern mithilfe des Standorts

Service Desk-Mitarbeiter können basierend auf dem Startstandort in ihrem Benutzerdatensatz und dem Standort der Aufgaben automatisch zugewiesen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die automatische Zuweisung nach Standort wird durchgeführt, wenn die Konfigurationsoption **Automatische Auswahl von Service Desk-Mitarbeitern berücksichtigt Standort von Service Desk-Mitarbeitern** aktiviert ist.

Wenn eine Aufgabe (Security Incident oder Reaktionsaufgabe) erstellt wird, wird für die Aufgabe der Service Desk-Mitarbeiter berücksichtigt, der dem Aufgabenstandort am nächsten ist. Wenn die Anwendung so konfiguriert ist, dass nur der Standort berücksichtigt wird, wird die Aufgabe automatisch dem nächstgelegenen Service Desk-Mitarbeiter zugewiesen.

Wenn eine Aufgabe erstellt wird, werden die Standorte von Service Desk-Mitarbeitern mit den folgenden Bereichen verglichen, um die Standortbewertung für jeden Service Desk-Mitarbeiter zu bestimmen.

Berechnung der Standortberechnung

Entfernung (km) vom Außendienstmitarbeiter zur Aufgabe	Bewertung
0 bis 0,1	1
0,11 bis 0,5	0.9
0,51 bis 5	0,7
5.1 bis 10	0,5
10,1 bis 20	0,4
20,1 bis 30	0,3
30,1 bis 40	0,2
40,1 bis 100	0.1
>100	0

Wenn die Anwendung für die Verwendung anderer Auswahlkriterien wie Kompetenzen, Zeitzone oder Zeitplan konfiguriert ist, werden die Bewertungen aller Auswahlkriterien gewichtet und summiert. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die Aufgabe automatisch zugewiesen. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern anhand mehrerer Auswahlkriterien.

Automatische Zuweisung von Kompetenzen an Service Desk-Mitarbeiter

Service Desk-Mitarbeiter können basierend auf ihren Kompetenzen und den für die Ausführung der Aufgabe erforderlichen Kompetenzen automatisch zugewiesen werden. ihren Benutzerdatensätzen mit Kompetenzen zuweisen **Kompetenzen** > **Anwender**.

Die automatische Zuweisung nach Kompetenzen kann durchgeführt werden, wenn die **automatische Auswahl von Service Desk-Mitarbeitern für Aufgaben erfordert, dass die Kompetenzkonfigurationsoption** auf **alle** oder **einige**festgelegt ist.

Wenn eine Aufgabe, die Kompetenzen enthält, automatisch zugewiesen wird, werden die Kompetenzen eines Service Desk-Mitarbeiters mit den für die Ausführung der Aufgabe erforderlichen Kompetenzen verglichen. Eine Bewertung wird basierend auf der Konfigurationsoption für Kompetenzen berechnet. Wenn die Option auf **einige** festgelegt ist, wird der Außendienstmitarbeiter mit der besten Übereinstimmung der Fähigkeiten der Aufgabe automatisch zugewiesen. Wenn die Option auf **alle** festgelegt ist, werden nur Außendienstmitarbeiter berücksichtigt, die alle erforderlichen Fähigkeiten besitzen. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

kein Service Desk-Mitarbeiter alle Kompetenzen besitzt, die zum Ausführen der Aufgabe erforderlich sind, wird niemand automatisch zugewiesen.

Eine Kompetenzbewertung wird wie folgt berechnet:

Skills_agent/Skills_task

Wobei:

- Skills_agent die Anzahl der Fähigkeiten des Außendienstmitarbeiters ist, die den für die Aufgabe erforderlichen Fähigkeiten entsprechen.
- Skills_task die Gesamtanzahl der für die Aufgabe erforderlichen Fähigkeiten ist.

Wenn eine Aufgabe beispielsweise vier Fähigkeiten erfordert und Außendienstmitarbeiter A drei davon und Außendienstmitarbeiter B zwei davon besitzt, dann ist die:

- A-Kompetenzbewertung des Service Desk-Mitarbeiters = 3/4 oder 0,75
- Kompetenzbewertung von Service Desk-Mitarbeiter B = 2/4 oder 0,5

Wenn die Anwendung für die Verwendung anderer Auswahlkriterien wie Standort oder Zeitzone konfiguriert ist, werden die Bewertungen aller Auswahlkriterien gewichtet und summiert. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die Aufgabe ausgewählt. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern anhand mehrerer Auswahlkriterien.

Automatische Zuweisung von Service Desk-Mitarbeitern anhand von Zeitzonen

Service Desk-Mitarbeiter können basierend auf der in ihren Benutzerdatensätzen definierten Zeitzone und der Zeitzone der Aufgaben automatisch zugewiesen werden.

Wenn die Option **Automatische Auswahl von Mitarbeitern, die Zeitzone für Aufgabenkonfiguration berücksichtigen** aktiviert ist, kann eine automatische Zuweisung nach Zeitzone durchgeführt werden.

Wenn eine Aufgabe erstellt wird, werden für die Aufgabe Mitarbeiter in der Zeitzone berücksichtigt, die der Zeitzone der Aufgabe am nächsten liegt. Wenn die Anwendung so konfiguriert ist, dass nur die Zeitzone berücksichtigt wird, kann die Aufgabe nur einem Service Desk-Mitarbeiter in derselben Zeitzone automatisch zugewiesen werden.

Hinweis:
Es ist wichtig, dass die Zeitzonen für den Mitarbeiter und die Aufgabe richtig eingestellt sind.

Wenn eine Aufgabe erstellt wird, werden Service Desk-Mitarbeiter anhand der Zeitzone der Aufgabe und der Zeitzone des Mitarbeiters mit der folgenden Formel bewertet:

1 - [abs(Task_tz – Agent_tz) ÷ 12]

wobei:

- abs die mathematische Funktion ist, um den absoluten Wert zu berechnen.
- Task_tz der Versatz zwischen der Zeitzone der Aufgabe und GMT ist.
- Agent_tz der Versatz zwischen der Zeitzone des Außendienstmitarbeiters und GMT ist.

Beispielsweise wird eine Aufgabe in New York City (GMT-4) erstellt, und zwei Außendienstmitarbeiter stehen zur Verfügung, um die Aufgabe auszuführen, einer in Los Angeles (GMT-7) und einer in Paris, Frankreich (GMT + 1).

Die Bewertung des Außendienstmitarbeiters in Los Angeles wird wie folgt berechnet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1 - abs((-4) - (-7)) ÷ 12 oder 0,75

Die Bewertung des Außendienstmitarbeiters in Paris wird wie folgt berechnet:

1 - abs((-4) - (+1)) ÷ 12 oder 0,58

Wenn die automatische Zuweisung einer Aufgabe nur auf der Zeitzone beruht, wird sie dem Service Desk-Mitarbeiter von Los Angeles aus zugewiesen.

Wenn die Anwendung für die Verwendung anderer Auswahlkriterien wie Kompetenzen oder Standort konfiguriert ist, werden die Bewertungen aller Auswahlkriterien gewichtet und summiert. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die Aufgabe ausgewählt. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern anhand mehrerer Auswahlkriterien.

Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Gruppenabdeckungsgebieten

Service Desk-Mitarbeiter können basierend auf dem Gruppenabdeckungsbereich, der in ihren Benutzerdatensätzen definiert ist, automatisch zugewiesen werden.

Automatische Zuweisung von Service Desk-Mitarbeitern anhand mehrerer Auswahlkriterien

Wenn eine Aufgabe erstellt wird, werden die Bewertungen der Service Desk-Mitarbeiter berechnet. Weitere Informationen finden Sie unter:

- Automatische Zuweisung von Außendienstmitarbeitern mithilfe des Standorts
- Automatische Zuweisung von Kompetenzen an Service Desk-Mitarbeiter
- Automatische Zuweisung von Service Desk-Mitarbeitern anhand von Zeitzonen

Die automatische Zuweisung basiert auf der folgenden Berechnung:

(Bewertungskriterium_1 x Gewichtung Kriterium_1) + (Bewertungskriterium_2 x Gewichtung Kriterium_2) + (Bewertungskriterium_3 x Gewichtung Kriterium_3)/Anzahl der verwendeten Kriterientypen:

Anzahl der verwendeten Kriteriumtypen = 1, 2 oder 3, abhängig von den verwendeten Einstellungen für Standort, Fähigkeiten und Zeitzone.

In diesem Beispiel wird die automatische Zuweisung von Außendienstmitarbeitern basierend auf Standort und Fähigkeiten berechnet. Das Beispiel basiert auf folgenden Annahmen.

- Die Konfigurationsoption **Bei der automatischen Auswahl von Agenten wird deren Standort berücksichtigt** ist für die Anwendung aktiviert.
- Die Konfigurationsoption **Für die automatische Auswahl von Agenten für Aufgaben müssen Fähigkeiten von Agenten vorhanden sein** ist für die Anwendung aktiviert.
- Die Eigenschaft **Gewichtung der Fertigkeit** ist für die Anwendung auf 10 festgelegt.
- Die Eigenschaft **Standortgewichtung** ist für die Anwendung auf 5 festgelegt.
- Außendienstmitarbeiter A und B stehen zur Verfügung, um eine Aufgabe auszuführen, und die Aufgabe erfordert vier spezifische Fähigkeiten.
- Service Desk-Mitarbeiter A Standort ist 8 Meilen vom Ort der Aufgabe entfernt und verfügt über drei der vier erforderlichen Kompetenzen.
- Der Standort von Service Desk-Mitarbeiter B ist eine Viertelmeile vom Standort entfernt und verfügt über zwei der erforderlichen Kompetenzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei der automatischen Zuweisung von Service Desk-Mitarbeitern wird folgende Berechnung verwendet: [(Standortbewertung x Standortgewichtung) + (Kompetenzbewertung x Kompetenzgewichtung)]/2

- Die Berechnung der automatischen Zuweisung für Service Desk-Mitarbeiter A lautet wie folgt: [(0,7 x 0,5) + (0,75 x 1)]/2 = 0,55
- Die Berechnung der automatischen Zuweisung für Agent B lautet: [(0,9 x 0,5) + (0,5 x 1)]/2 = 0,475

In diesem Beispiel wurde die Aufgabe automatisch Service Desk-Mitarbeiter A zugewiesen.

Verwaltung von Security Incidents und eingehenden Anforderungen

Nachdem ein Security Incident erstellt wurde, können zahlreiche Arten von Informationen hinzugefügt und angezeigt werden, während Ihre Analyse des Problems sich der Lösung nähert.

Wichtig:
Die neuesten Funktionen in Security Incident Response sind ausschließlich in Arbeitsbereich für Security Incident Responseverfügbar. Installieren oder aktualisieren Sie auf die neueste Version Security Incident Response oder Arbeitsbereich für Security Incident Response, um auf Funktionen wie Schichtübergabe, Risikobewertungsrechner usw. zuzugreifen und sie zu nutzen.

In diesem Abschnitt wird Folgendes beschrieben:

- Erstellen Sie eine eingehende Anforderung
- Verwalten Sie erkennbare Elemente
- Verwalten Sie Suchen und Scans
- on-demand orchestrationverwalten
- Berechnen Sie den Schweregrad eines Security Incident
- Verwalten Sie Aktivitäten nach Incidents
- Schließen Sie Security Incidents

Erstellen Sie eine eingehende Anforderung

Im Gegensatz zu Security Incidents haben eingehende Anforderungen im Allgemeinen eine niedrigere Priorität. Anforderungen für eine Suche, einen Scan oder ein neues Abzeichen sind Beispiele für eingehende Anforderungen.

Vorbereitungen
Erforderliche Rolle: Rolle sn_si.basic oder höher

Prozedur

1. Navigieren Sie zu einem der Anforderungsformulare.
   Beispiel: **Alle** > **Security Incident** > **Eingehende Anfragen** > **Mir zugewiesen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsanforderung

Feld	Beschreibung
Nummer	[Schreibgeschützt] Die automatisch generierte Nummer der Sicherheitsanforderung.
Unternehmen	Das anfordernde Unternehmen.
Standort	Der CI-Standort, falls zutreffend. Dieses Feld wird bereits gefüllt, wenn das CI ausgewählt wird.
Konfigurationselement	Das Configuration Item, das von der Anforderung betroffen ist.
Priorität	Die Priorität der Anforderung.
Geöffnet	[Schreibgeschützt] Datum und Uhrzeit, zu der die Anforderung geöffnet wurde.
Status	Der aktuelle Status der Sicherheitsanforderung. Bei Erstellung der Sicherheitsanforderung wird dieses Feld standardmäßig auf **Entwurf**gesetzt.
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Person, der die Ausführung der Arbeit zugewiesen ist.
Kurzbeschreibung	Kurze Beschreibung der Sicherheitsanforderung, die für die anfordernde Person sichtbar ist.
Beschreibung	Die vollständige Beschreibung der Anforderung, die für die anfordernde Person sichtbar ist.
Arbeitsnotizen	Arbeitsnotizen, die für die anfordernde Person sichtbar sind.

4. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.
5. Wenn Sie die Anforderung zu einem Security Incident eskalieren müssen, klicken Sie auf **In Security Incident konvertieren**.

Verwalten Sie erkennbare Elemente

Erkennbare Elemente sind Artefakte, die in einem Netzwerk oder Betriebssystem gefunden werden und wahrscheinlich auf einen Angriff hindeuten. Typische erkennbare Elemente sind IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen. Threat Intelligence Daten der Tabelle erkennbarer Elemente sind innerhalb eines Security Incident verfügbar.

Die Informationen zu erkennbaren Elementen umfassen Wert, Typ, Kontext und Zeitstempel.

Sie können erkennbare Elemente manuell oder automatisch über Suchanforderungen erstellen oder löschen.

Der Registerkarte **mit den Ergebnissen der Bedrohungssuche** wurde eine neue Spalte **„Ergebnis“** hinzugefügt. Mögliche Werte: „Böswillig“ und „Unbekannt“.

Wenn eine IoC-Suchanforderung kein erkennbares Element für einen Security Incident findet, wird sie als Unbekannt gekennzeichnet.

Wenn eine IoC-Suchanforderung ein erkennbares Element für einen Security Incident findet, wird sie als Böswillig gekennzeichnet.

Während eines Upgrades wird für vorhandene Elemente die **Spalte** „Ergebnis“ auf „Böswillig“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Daten der Tabelle Threat Intelligence erkennbarer Elemente sind zwar Teil eines Security Incidents, es ist jedoch keine andere Interaktion mit dem Modul Threat Intelligence enthalten. Für vollständige Bedrohungsfunktionen ist das Plugin Threat Intelligence im -Abonnement verfügbar.

Zugehörige Informationen

Erstellt ein erkennbares Element für einen Security Incident

Zeigen Sie IoC-Informationen für einen Security Incident an

Sie können IoC-Informationen anzeigen, z. B. erkennbare Elemente und Sichtungssuchergebnisse, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie IoC-bezogene Informationen anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Tab-Taste	Beschreibung
Erkennbare Elemente	Zeigen Sie erkennbare Elemente an, die dem Security Incident zugeordnet sind, oder fügen Sie sie manuell hinzu. Weitere Informationen finden Sie unter Verwalten Sie erkennbare Elemente.
Zugehörige Indikatoren	Wenn Threat Intelligence aktiviert ist, können Sie alle anderen Indikatoren anzeigen, die denselben Bedrohungsdatensätzen zugeordnet sind.
Ergebnisse der Sichtungssuche	Enthält Ergebnisse der Sichtungssuche.
Details einer Sichtungssuche	Enthält Details des Datensatzes „Sichtungssuche“.
Bedrohungssuchen	Speichert Ergänzungsdaten aus Malware-Erkennungssystemen. Diese Registerkarte wird nur angezeigt, wenn das Plugin Threat Intelligence installiert ist.
Zugehörige Angriffsmodi/-methoden	Wenn Threat Intelligence aktiviert ist, können Sie alle anderen Angriffstypen anzeigen, die denselben Bedrohungsdatensätzen zugeordnet sind.
Anforderungen für Sicherheitsprüfung	Wenn Threat Intelligence aktiviert ist, können Sie Scan- und Suchanforderungen anzeigen, die an den Security Incident angehängt sind.
Ressourcen mit ähnlichem IoC	Wenn Threat Intelligence aktiviert ist, können Sie alle anderen Ressourcen mit ähnlichen Indikatoren anzeigen.
Anwender mit ähnlichem IoC	Wenn Threat Intelligence aktiviert ist, können Sie alle anderen Benutzer mit ähnlichen Indikatoren anzeigen.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Betroffene Elemente anzeigen
- Zugehörige Elemente anzeigen
- Ergänzungsdaten anzeigen
- Antwortaufgaben anzeigen

5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Erstellt ein erkennbares Element für einen Security Incident

Sie können ein erkennbares Element in einem Security Incident erstellen, anzeigen und entsprechende Maßnahmen ergreifen. Die Verfügbarkeit von erkennbaren Elementen im Security Incident ist skalierbar und verkürzt die Antwortzeit.

Vorbereitungen

Erforderliche Rolle:

- sn_ti_observable.write (schreiben)
- sn_ti_observable.read (lesen)
- sn_ti_observable.admin (löschen)

Prozedur

1. Navigieren Sie zu **Security Incident**.
2. Wählen Sie einen Incident aus.
3. Klicken Sie auf die Registerkarte der zugehörigen Liste **erkennbare Elemente des Security Incidents**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie Sicherheits-Tags zum Hinzufügen von Metadaten zum Datensatz eingerichtet und aktiviert haben, können Sie ein oder mehrere Tags auswählen, um den Grad der Vertraulichkeit des erkennbaren Elements anzugeben. Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Wert	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist. **Hinweis:** Wenn eine Bedrohungsprüfung eine IP-Adresse oder einen Hash durchführt, Malware zurückgegeben oder ein anderer Fehler auftritt, werden die IP-Adresse oder der Hash-Wert automatisch der Tabelle „Erkennbares Element“ [sn_ti_observable] hinzugefügt. Daher kann im Formular „Erkennbare Elemente“ gesucht werden.
Erkennbarer Typ	Wählen Sie die Klassifizierung des erkennbaren Elements aus, z. B. eine IP-Adresse oder einen Datei-Hash. Diese erkennbaren Typen sind im Modul **„Erkennbare Typen“** definiert.
Incident-Anzahl	Die Häufigkeit, mit der der Wert des erkennbaren Elements gefunden wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ist Zusammensetzung	Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn der **Typ des erkennbaren Elements** auf etwas anderes als **Zusammensetzung des erkennbaren Elements**festgelegt ist und dieses neue erkennbare Element eine Zusammensetzung ist, aktivieren Sie dieses Kontrollkästchen. Wenn der **Typ des erkennbaren Elements** bereits auf **Zusammensetzung des erkennbaren Elements**festgelegt ist, ist das Kontrollkästchen aktiviert und schreibgeschützt. Eine erkennbare Elementzusammensetzung ist ein erkennbares Element, das untergeordnete erkennbare Elemente enthält.
Ergebnis	Wählen Sie eine der folgenden Optionen aus: ○ **Böswillig**: Gibt an, dass das erkennbare Element für die Organisation schädlich ist. ○ **Verdächtig**: Gibt an, dass das erkennbare Element für die Organisation schädlich sein könnte. ○ **Clean**: Gibt an, dass das erkennbare Element für die Organisation nicht schädlich ist. ○ **Unbekannt**: Gibt an, dass der Fund des erkennbaren Elements noch bestimmt werden muss. ○ Standardwert: Unbekannt. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche. **Hinweis:** Nach einem Upgrade werden vorhandene erkennbare Elemente als schädlich markiert.
Betreiber	Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Ist Zusammensetzung** aktiviert ist. Abhängig von Ihrer Einstellung in diesem Feld werden die erkennbaren Elemente und ihre untergeordneten Elemente bei der Entscheidung, ob ein zugehöriger Indikator vorhanden ist, berücksichtigt. Legen Sie dieses Feld auf **UND** fest, wenn alle untergeordneten erkennbaren Elemente vorhanden sein müssen, damit ein zugeordneter Indikator als vorhanden betrachtet wird. Legen Sie diese Option auf **ODER** fest, wenn eines der untergeordneten erkennbaren Elemente vorhanden ist, damit ein zugeordneter Indikator als vorhanden betrachtet wird.
Darf nicht vorhanden sein	Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn diese Option ausgewählt ist, gibt dieses Feld an, dass das potenzielle Problem in der Abwesenheit des erkennbaren Elements liegt (z. B. in einem fehlenden Registrierungsschlüssel).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

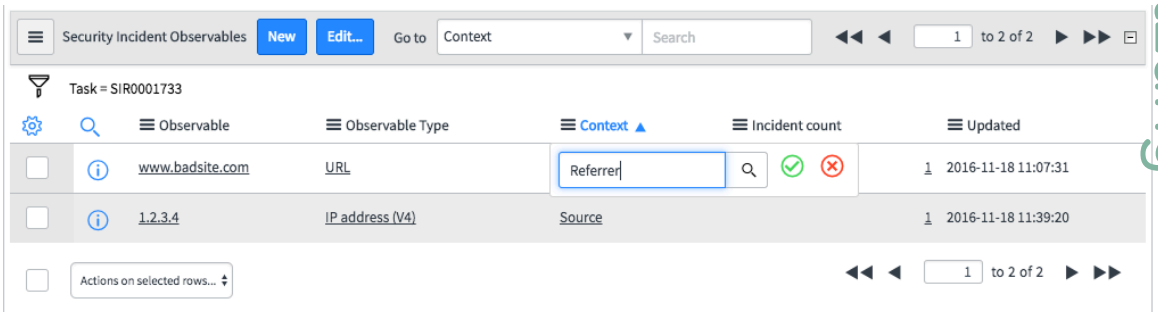
Feld	Beschreibung
Standort	Mit den Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie Laden Sie weitere IoC-Daten in dieses Feld laden.
Notizen	Geben Sie zusätzliche Notizen zum erkennbaren Element ein.

6. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

Zugehörige Liste	Beschreibung
Zugehörige Indikatoren	Listet Indikatoren auf, die von der Bedrohungsquelle identifiziert wurden.
Zugehörige Aufgaben	Listet Changes auf, die dem erkennbaren Element zugeordnet sind.
Untergeordnete erkennbare Elemente	Listet zugehörige erkennbare Elemente auf, die von der Bedrohungsquelle identifiziert wurden.
Übereinstimmende Ressourcen für IP	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die über eine übereinstimmende IP-Adresse verfügen.
Quelle erkennbare Elemente	Listet die Quellen dieses erkennbaren Elements zusammen mit dem Konfidenzniveau der Quelle auf.
Sicherheitsanmerkungen	Listet Sicherheitsanmerkungen auf, die diesem erkennbaren Element hinzugefügt wurden.

7. Zurück zum Security Incident: Folgende Informationen sind verfügbar.

Hinweis:
Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Konfigurationselementen oder Benutzern, die ihm zugeordnet sind. Die **zugehörigen Listenregisterkarten Zugehörige Konfigurationselemente** und **Zugehörige Benutzer** werden entsprechend aktualisiert.



Spalte	Definition
Erkennbares Element	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.
Erkennbarer Typ	Der spezifische Typ des erkennbaren Elements.
Kontext	Vom Anwender ausgewählt. Die Auswahlmöglichkeiten lauten wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Definition
	○ IP: Quelle oder Ziel **Hinweis:** Wenn Threat Intelligence und Palo Alto Networks – Firewall aktiviert sind, führt das Ändern oder Hinzufügen eines Werts zu diesem Feld die Ausführung des Workflows „ Protokolldaten-Flow abrufen Security Operations Palo Alto Networks – Protokolldaten abrufen“ aus. Der Workflow ruft angereicherte Bedrohungsprotokolldaten von der Firewall ab und hängt sie an den Security Incident an. Die Informationen werden auch analysiert und im Abschnitt „Firewall-Protokolle“ auf der Registerkarte **Ergänzungsdaten** angezeigt. ○ URL: Referrer **Hinweis:** Wenn der Benutzer auf einen Link in einer Phishing-E-Mail klickt, ist ein Referrer die URL des letzten Jumps, bevor auf die Malware-URL zugegriffen wird.
Incident-Anzahl	Anzahl der Incidents, in denen dieses erkennbare Element angezeigt wird. Dieser Wert wird automatisch aktualisiert, wenn das erkennbare Element manuell oder über einen Workflow zu einem anderen Incident hinzugefügt wird.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Liste.

Hinweis:
Wenn das Plugin Threat Intelligence „ installiert ist, können Sie das erkennbare Element auch in der Liste „ **Erkennbare Elemente“** im **IoC-Repository**anzeigen.

Zugehörige Informationen

Bearbeiten Sie eine Liste erkennbarer Elemente für Security Incidents

Fügen Sie mehrere erkennbare Elemente für Security Incidentshinzu

Verwalten Sie erkennbare Dateielemente

„Erkennbare Dateielemente verwalten“ bietet strenge Sicherheitsmaßnahmen zum Speichern verdächtiger Dateien und aktiviert den Dateityp „Erkennbare Elemente“ für die Sandbox-Integration.

Vorbereitungen

Erforderliche Rolle: sn_ti_malicius_attachment_access (hochladen)

Erkennbare Elemente des Dateityps hochladen:

- Automatisch: Wenn die Security Incidents für die Phishing-E-Mails erstellt werden, werden die Anhänge in der Phishing-E-Mail als erkennbare Elemente des Dateityps erstellt.
- Manuell: Ein Sicherheitsanalyst kann die verdächtigen Dateien auch hochladen, um erkennbare Elemente vom Typ Dateityp zu erstellen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können erkennbare Elemente vom Typ Dateityp für einen Security Incident erstellen und anzeigen. Die verdächtigen Dateien, die Teil der erkennbaren Elemente sind, werden an einem bestimmten Ort gespeichert, auf den der Sicherheitsanalyst zugreifen kann, um die Datei nur mit einer bestimmten Rolle herunterzuladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

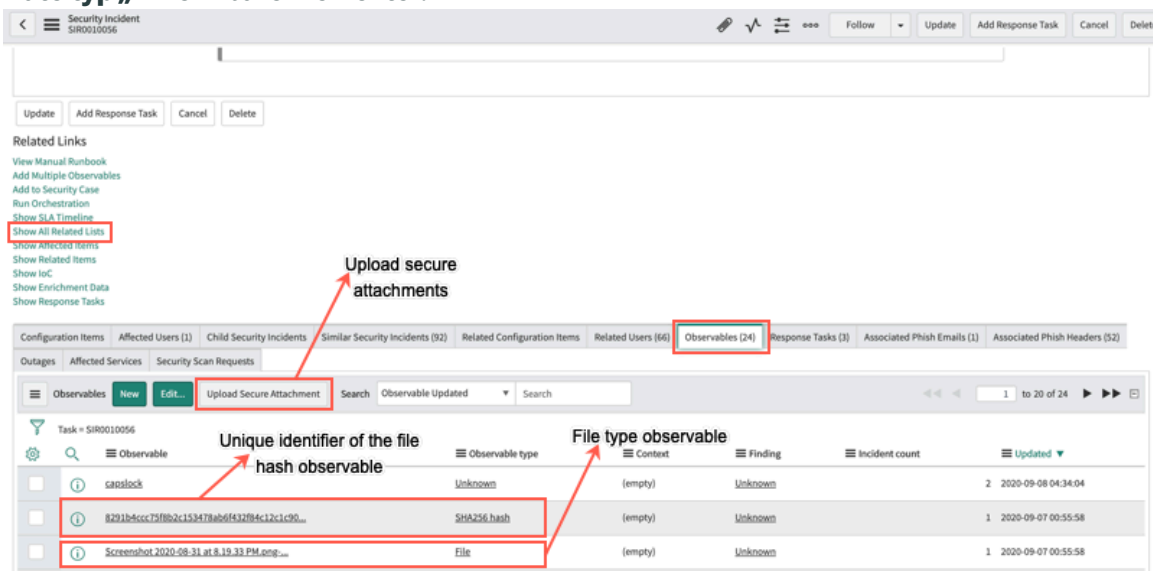
Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie auf der Registerkarte **Alle zugehörigen Listen anzeigendie Option Erkennbare Elemente aus**.

   Wenn die Phishing-E-Mail Anhänge enthält, werden diese Anhänge standardmäßig als erkennbare Elemente des Dateityps im entsprechenden Security Incident erstellt. Jeder Anhang wird als zwei erkennbare Elemente erstellt, z. B. Dateityp und erkennbares Datei-Hash-Element.

3. So laden Sie die sicheren Anhänge manuell hoch:
   - Klicken Sie auf **Sicheren Anhang hochladen**.
   - Klicken Sie unter „Sichere Anhänge hochladen“ **auf Datei auswählen**, um eine oder mehrere Dateien hochzuladen. Jede Datei wird als ein einzelner erkennbarer Datensatz betrachtet.
   - Klicken Sie auf **„Erkennbare Dateielemente erstellen“**, um die erkennbaren Dateitypen zu erstellen, z. B. eines ist der Dateityp und das andere ist der Datei-Hash, der ein eindeutiger Bezeichner ist.

Dateityp „Erkennbare Elemente“.



Wählen Sie den Dateityp des erkennbaren Elements aus, das für weitere Integrationen wie Sandbox, Bedrohungssuche verarbeitet werden soll. Darüber hinaus können Sie die Anhänge auch aus dem Dateityp Observable herunterladen.

Hinweis:

Die Bedrohungssuche (VirusTotal) ruft die Datei aus den gesicherten Anhängen für die erkennbaren Elemente des neuen Dateityps ab, und die folgenden Systemeigenschaften gelten nicht für die erkennbaren Elemente des neuen Dateityps.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zur Schnellreferenz: Der erkennbare Dateityp wird dem erkennbaren Hash-Element als untergeordnetes Element zugeordnet, und das erkennbare Hash-Element wird als untergeordnetes Element dem erkennbaren Dateielement zugeordnet.

Wenn die Phishing-E-Mail-Anhänge die definierte Größe überschreiten, werden die erkennbaren Elemente nicht erstellt. Sie müssen die Systemeigenschaften ändern, um die größeren Dateien zu unterstützen.

Systemeigenschaften für die Dateigröße

Systemeigenschaft	Beschreibung
glide.email.inbound.max_total_attachment_size_bytes	Wenn Sie die Phishing-E-Mail direkt weiterleiten, verwenden Sie diesen Systemeigenschaftenwert, um die Dateigröße von 18 MB auf die gewünschte Dateigröße zu erhöhen.
com.glide.attachment.max_get_size	Wenn Sie die Phishing-E-Mail als Anhang weiterleiten, verwenden Sie diesen Systemeigenschaftswert, um die folgenden Systemeigenschaften im globalen Bereich zu erstellen und die Dateigröße von 5 MB auf die gewünschte Größe zu erhöhen.

Sie können auch wie folgt einen neuen erkennbaren Dateityp erstellen:

a. Klicken Sie auf **Neu**.

b. Wählen Sie den **erkennbaren Elementtyp Kategorie: Datei**aus

c. Klicken Sie auf **Hochladen**, um eine Datei anzuhängen.

Bearbeiten Sie eine Liste erkennbarer Elemente für Security Incidents

Sie können bearbeiten, welche erkennbaren Elemente in der Liste einem Security Incident zugeordnet sind.

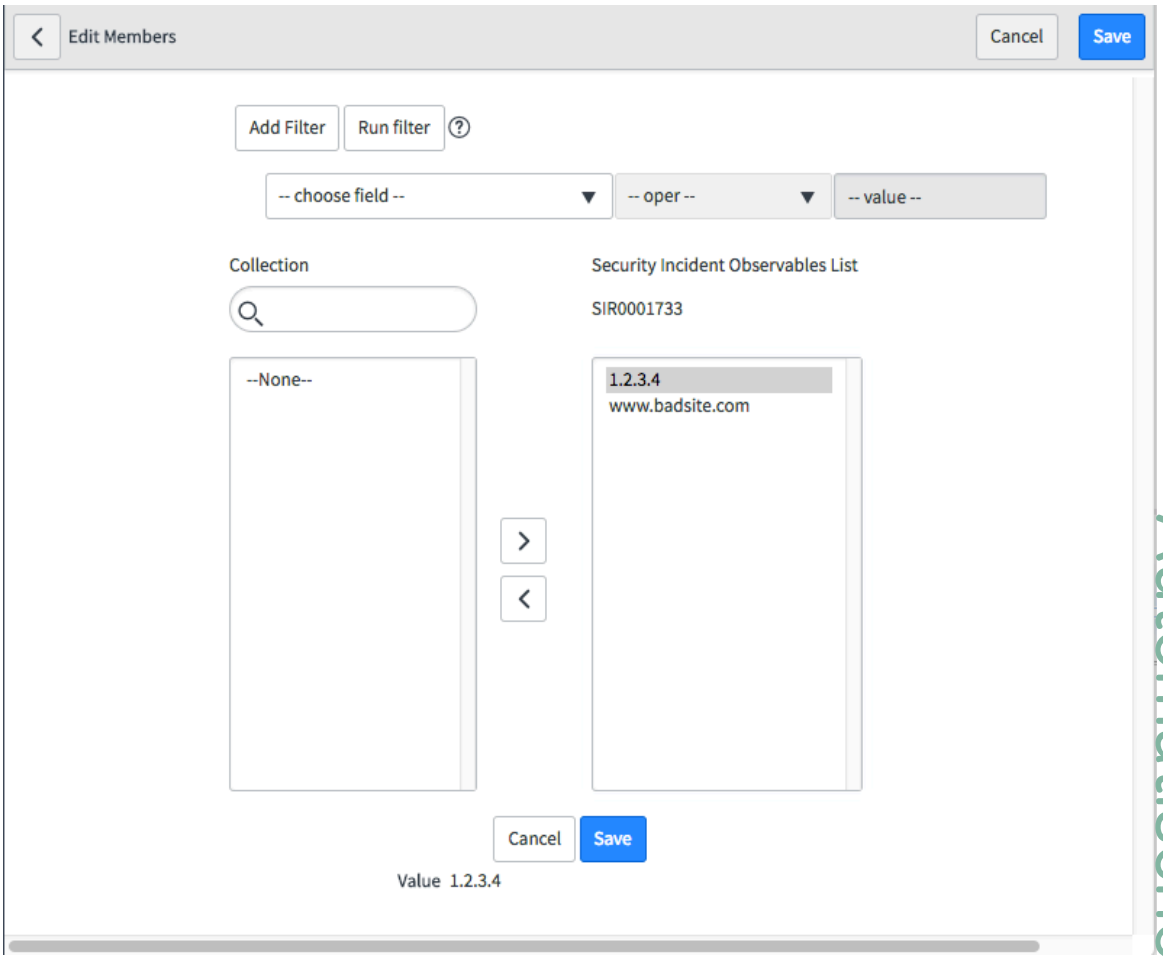
Vorbereitungen

Erforderliche Rolle: sn_si.basic

Prozedur

1. Navigieren Sie zu **Security Incident**.
2. Wählen Sie einen Incident aus.
3. Klicken Sie auf die Registerkarte der zugehörigen Liste **erkennbare Elemente des Security Incidents**.
4. Klicken Sie auf **Bearbeiten**.
5. Fügen Sie der Liste erkennbare Elemente hinzu, oder entfernen Sie sie.
   Erstellen Sie einen Filter für lange Listen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie auf **Speichern**.

> **Hinweis:**
> Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Konfigurationselementen oder Benutzern, die ihm zugeordnet sind. Die **zugehörigen Listenregisterkarten Zugehörige Konfigurationselemente** und **Zugehörige Benutzer** werden entsprechend aktualisiert. Wenn das Plugin Threat Intelligence aktiviert ist und Sie mindestens eineSecurity Incident Response-Integrationen -Integrationsimplementierung aktiviert haben, führt das Plugin Security Operations-Integration – Funktionalität zur Bedrohungssuche einen oder mehrere Workflows aus, und für die von Ihnen hinzugefügten erkennbaren Elemente werden Bedrohungssicherheitssuchen durchgeführt. Die Ergebnisse werden auf der Registerkarte **Ergebnisse der Bedrohungssuche** angezeigt.

Zugehörige Informationen

Fügen Sie mehrere erkennbare Elemente für Security Incidentshinzu

Erstellt ein erkennbares Element für einen Security Incident

Fügen Sie mehrere erkennbare Elemente für Security Incidentshinzu

Um Zeit zu sparen, können Sie der Liste erkennbarer Elemente des Security Incident mehrere erkennbare Elemente hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti_write

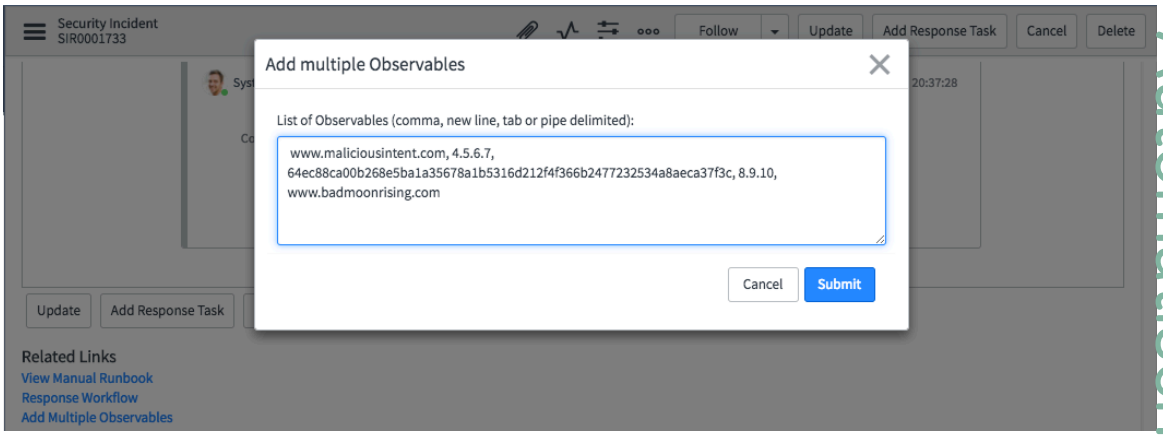
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn mehrere erkennbare Elemente für Security Incidents hinzugefügt werden, werden Duplikate während der Verarbeitung ignoriert.

Prozedur

1. Navigieren Sie zu **Security Incident**.
2. Wählen Sie einen Incident aus.
3. Klicken Sie auf den zugehörigen Link **Mehrere erkennbare Elemente hinzufügen**.
4. Geben Sie mehrere erkennbare Elemente ein, oder fügen Sie sie ein.
   Einträge können einen beliebigen erkennbaren Elementtyp aufweisen. Akzeptierte Formate: Komma, neue Zeile, Registerkarte oder Pipe-Trennzeichen.



Hinweis:
Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Konfigurationselementen oder Benutzern, die ihm zugeordnet sind. Die **zugehörigen Listenregisterkarten Zugehörige Konfigurationselemente** und **Zugehörige Benutzer** werden entsprechend aktualisiert.

Hinweis: Nicht automatisch erkannte erkennbare Werte werden dem Typ „Unbekannt“ zugewiesen.

5. Klicken Sie auf **Absenden**.

Automatische Protokolldatenanreicherung erkennbarer Elemente für Security Incidents

Wenn bestimmte Anwendungen und Integrationen eingerichtet sind, einschließlich Threat Intelligence und der Palo Alto Networks – Firewall -Integration, können Informationen erkennbarer Elemente in einem Security Incident automatisch mit Bedrohungsprotokolldaten angereichert werden, wenn die Quell-IP für die zugehörigen erkennbaren Elemente geändert wird.

Wenn eine Änderung auftritt, initiiert eine Geschäftsregel einen Workflow, der Daten aus Bedrohungsprotokollen in Ihrer Firewall abruft und die Informationen der erkennbaren Elemente im Security Incident anreichert.

Bevor erkennbare Elemente angereichert werden können, müssen die folgenden Schritte ausgeführt werden.

- Threat Intelligence muss aktiviert sein.
- Die Palo Alto Networks-Firewall- Integration muss aktiviert und konfiguriert sein. Dies kann auch Richten Sie SSH-Anmeldeinformationen für den MID-Server einenthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem dieses Setup abgeschlossen wurde, bewirkt die Änderung der Quell-IP von erkennbaren Elementen, die einem Security Incident zugeordnet sind, dass eine Geschäftsregel den Workflow **„Security Operations Palo Alto Networks – Protokolldaten abrufen“** ausführt. Workflow-Aktivitäten stellen eine Suchabfrage an der Firewall in die Warteschlange und geben eine Auftrags-ID zurück, die verwendet wird, um Bedrohungsprotokolldaten von der Firewall abzurufen und sie als XML-Datei an den Security Incident anzuhängen.

Zugehörige Informationen

Ruft den Flow zur Ergänzung der AutoFocus-Sitzungsinformationen ab

Workflow für das Firewall-Startprogramm für Security Operations-Integration Palo Alto Networks .

Security Operations Palo Alto Networks: Wert-Workflow zum Überprüfen und Blockieren

Protokolldaten-Flow abrufen

Rufen Sie den WildFire-Datenanreicherungs-Flow ab

Veröffentlichen Sie erkennbare Elemente in einer Drittanbieter-Beobachtungsliste

Sie können ein oder mehrere erkennbare Elemente oder zugehörige Indikatoren in einer Drittpartei-Beobachtungsliste veröffentlichen. Derzeit unterstützt diese Funktionalität nur die Implementierung CrowdStrike Falcon Host.

Vorbereitungen

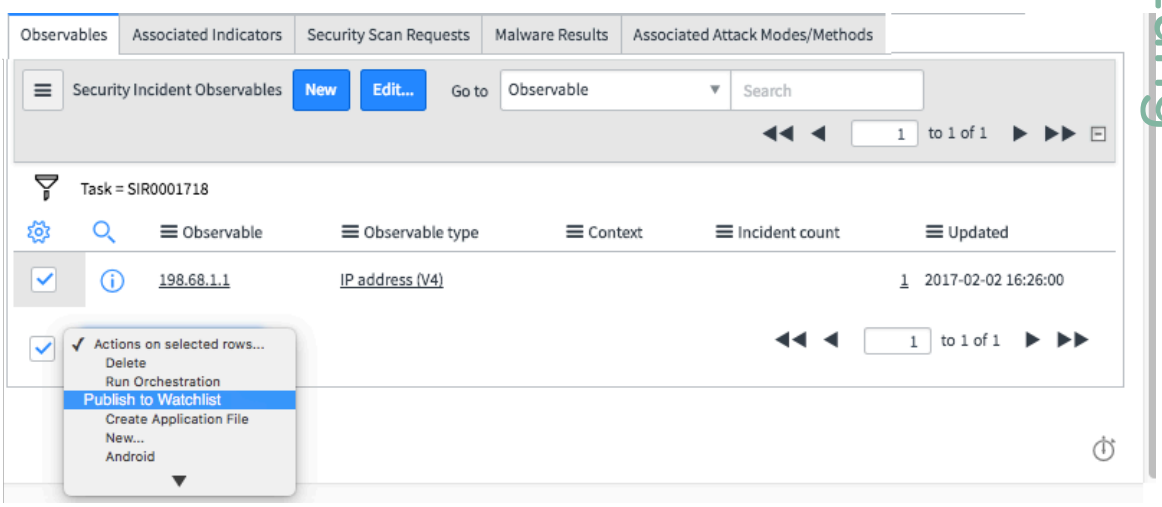
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Prozedur

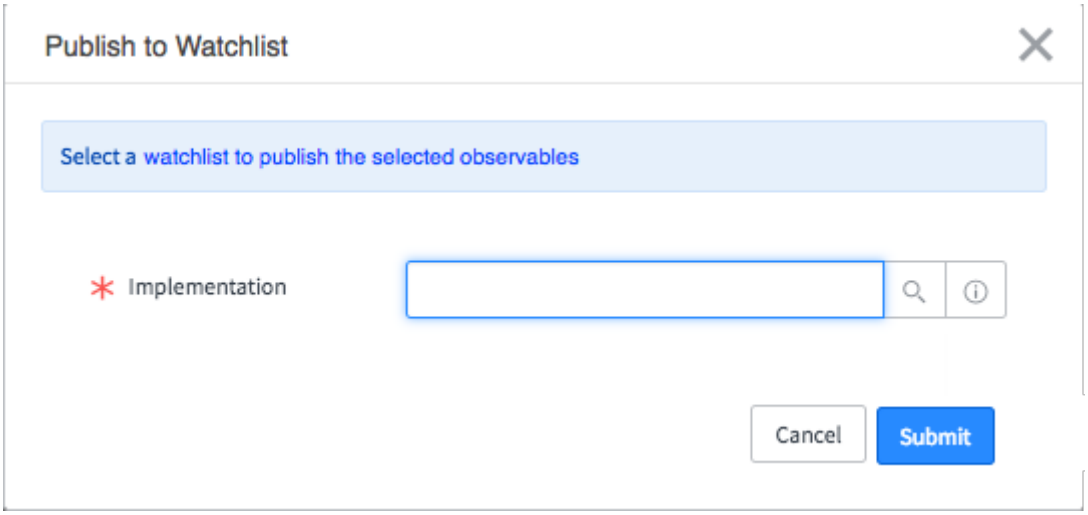
1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie auf der Registerkarte **Zugehörige Listedie Option Erkennbare Elemente** aus.
3. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen...** auf **In Beobachtungsliste veröffentlichen**.



Das Dialogfeld wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie die Implementierung ein, oder wählen Sie sie aus.

> **Hinweis:**
> Ein Workflow wird von Security Operations-Integration: Fähigkeit „In Beobachtungsliste veröffentlichen“. ausgelöst, wenn Sie die Implementierung des CrowdStrike Falcon Host auswählen.

5. Klicken Sie auf **Absenden**.

Verwalten Sie Suchen und Scans

Sie können Suchvorgänge und Schwachstellen-Scans in Security Incidents und im Security Incident-Katalog durchführen, um potenzielle Bedrohungen und Schwachstellen zu identifizieren.

Senden Sie eine IoC-Suchanforderung aus einem Security Incident

Eine IoC-Suche wird automatisch ausgeführt, wenn erkennbare Elemente zu einem Security Incident hinzugefügt werden. Wenn Ihr Security Incident Anhänge enthält, können Sie diese auch einfach mit einem Klick auf eine Schaltfläche finden.

Vorbereitungen

Für automatische IoC-Suchen muss das Plugin Threat Intelligence aktiviert sein.

Erforderliche Rolle: sn_si.basic

> **Hinweis:**
> Standardmäßig ist der **Suchtyp** für **Datei** inaktiv.

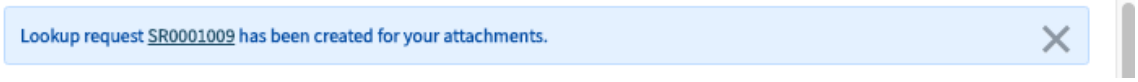
Prozedur

1. Erstellen Sie einen neuen Security Incident, oder öffnen Sie einen vorhandenen, wenn Sie neue Dateien anhängen möchten.
2. Klicken Sie auf das Büroklammer-Symbol im Formularheader, und hängen Sie eine oder mehrere Dateien an.
3. Wenn Sie Ihre Eingaben im Formular abgeschlossen haben, klicken Sie mit der rechten Maustaste auf den Formular-Header, und wählen Sie **Speichern**aus.
   Nachdem der Datensatz gespeichert wurde, wird die Schaltfläche **Anhänge suchen** angezeigt.
4. Klicken Sie auf **Anhänge suchen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Arbeitsnotizen unter **„Incident-Details“** enthalten Informationen zum Fortschritt des Suchprozesses.

5. Sie können auf die Suchnummer am Ende der Nachricht klicken, um den Suchdatensatz anzuzeigen. Sie können auf den Referenzlink „Suche“ klicken, um detaillierte Ergebnisse anzuzeigen.



Senden Sie eine IoC-Suchanforderung aus dem Security Incident Catalog

Wenn das Plugin Security Incident Response aktiviert ist, können Sie Bedrohungssuchen für Dateien, Hash-Werte, URLs und IP-Adressen aus dem Security Incident-Katalog übermitteln. Die Anforderungen werden übermittelt, und Sie können die Ergebnisse im Modul **Meine Anforderungen** anzeigen.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Suchen werden automatisch für den Standardsuchtyp für jede im Suchdatensatz aufgeführte Suchquelle ausgeführt. Die Ergebnisse der Suchanforderung sind im Modul **„My Requests“ (Meine Anforderungen)** verfügbar.

Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Security Incident-Katalog**.
2. Klicken Sie auf **IoC-Suche**.
3. Klicken Sie auf **Dateien, Hash-Werte, URLs oder IP-Adressen suchen**.
4. Geben Sie einen oder mehrere der folgenden Werte ein:

IoC-Suchanforderung

Zu suchendes Element	Beschreibung
Dateien	Klicken Sie auf das Büroklammer-Symbol, suchen Sie die zu suchenden Dateien, und hängen Sie sie an. **Hinweis:** Standardmäßig ist der **Suchtyp** für **Datei**inaktiv. Dateien werden konvertiert und als Hash-Wert übermittelt.
URLs	Geben Sie im Feld **URLs** die zu suchenden URLs ein, getrennt durch Kommas. Beispiel: www.abc.com,www.xyz.net.
IP-Adressen	Geben Sie im Feld **IP-Adressen** die IP-Adressen ein, nach denen Sie suchen möchten, getrennt durch Kommas.
Hash-Werte	Geben Sie im Feld **Hash-Werte** die zu suchenden Hash-Werte ein, getrennt durch Kommas.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zu suchendes Element	Beschreibung
	Hinweis: Wenn der **Suchtyp** für **Datei** inaktiv ist, ist dieser Wert die Standardaktion für **Datei-** und **Hash-Werte**.

5. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Absenden**.
6. Um den Status und/oder die Ergebnisse der Suchen anzuzeigen, navigieren Sie zu **Selfservice** > **Meine Anforderungen**.
7. Klicken Sie auf die SR-Nummer für die Anforderung.
   In den Arbeitsnotizen unter **„Aktivität“** werden die während der Suche ausgeführten Aufgaben aufgelistet, einschließlich der Erstellung einzelner Suchen für jede Datei, jedes Hash-Werts, jeder URL oder IP-Adresse und der Suchergebnisse.

Senden Sie eine Schwachstellen-Scan-Anforderung aus einem Security Incident

Wenn Ihr Security Incident ein oder mehrere Konfigurationselemente aufweist (Server, Computer usw.), können diese im Formular Security Incident Response auf Schwachstellen gescannt werden.

Vorbereitungen

Das Vulnerability Response-Plugin muss aktiviert sein.

Erforderliche Rolle: sn_si.write

Prozedur

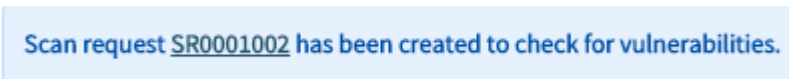
1. Erstellen Sie einen Security Incident, und beziehen Sie mindestens eine Ressource ein.
   Sie können auch einen vorhandenen Incident öffnen, der Konfigurationselemente enthält.
2. Wenn Sie Ihre Eingaben im Formular abgeschlossen haben, klicken Sie mit der rechten Maustaste auf den Formular-Header, und wählen Sie **Speichern**aus.
   Nachdem der Datensatz gespeichert wurde, wird der zugehörige Link **Auf Schwachstellen scannen** angezeigt.

   Hinweis:
   Wenn die zugehörige Liste **Auf Schwachstellen scannen** nicht angezeigt wird, müssen Sie zu navigieren **Schwachstelle** > **Scanner**, richten Sie mindestens einen Scanner ein, und legen Sie den Standardwert auf **true**fest.

3. Klicken Sie **auf Auf Schwachstellen prüfen**.

   Hinweis:

   Oben im Formular „Security Incident“ wird eine Nachricht zusammen mit einem Link zum Scan-Datensatz angezeigt.

4. Sie können auf die Nummer der Scan-Anforderung klicken, um den Scan-Datensatz anzuzeigen.
   Die Incident-Details zeigen die Ergebnisse der Prüfung im Datensatz Sicherheitsscananforderung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Senden Sie eine Schwachstellen-Scan-Anforderung aus dem Security Incident Response-Katalog

Sie können Schwachstellen-Scans für CIs und IP-Adressen aus dem -Katalog Security Incident Response übermitteln. Die Anforderungen werden übermittelt, und Sie können die Ergebnisse im Modul **Meine Anforderungen** anzeigen.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Security Incident-Katalog**.
2. Klicken Sie auf **Schwachstellen-Scan**.
3. Klicken Sie auf **Konfigurationselement und IP-Adressen scannen**.
4. Geben Sie einen oder mehrere der folgenden Werte ein, die gescannt werden sollen.

Schwachstellenscanner

Zu scannendes Element	Beschreibung
Konfigurationselement	Wählen Sie im Feld **Zu scannendes Konfigurationselement** das zu scannende CI aus.
IP-Adressen	Geben Sie im Feld **Zu scannende IP-Adressen** die IP-Adressen ein, getrennt durch Kommas.

5. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Absenden**.
   Wenn ein erkennbares Element gefunden wird, wird ein Indikator gemäß STIXX-Standards erstellt.
6. Um den Status und/oder die Ergebnisse der Prüfungen anzuzeigen, navigieren Sie zu **Selfservice** > **Meine Anforderungen**.
7. Klicken Sie auf die SR-Nummer für die Anforderung.
   In den Arbeitsnotizen unter **„Aktivitäten“** werden die während der Prüfung ausgeführten Aufgaben aufgelistet, einschließlich der Erstellung einzelner Prüfungen für jedes CI oder jede IP-Adresse, sowie der Ergebnisse der Prüfungen.

on-demand orchestrationverwalten

Während der Analyse Security Incident Response von möchte ein Sicherheitsanalyst möglicherweise eine Aufgabe ausführen, die von einem Security Incident-Workflow gesteuert wird. Führen Sie beispielsweise eine Prozesssicherung für ein bestimmtes CI aus. Dies kann mit bedarfsgesteuerter Orchestrierung erreicht werden.

Jede registrierte Anwendung von Security Operations enthält mehrere bedarfsgesteuerte Orchestrierungen im Basissystem. Sie können nach Bedarf anwenderdefinierte bedarfsgesteuerte Orchestrationendefinieren.

Die bedarfsgesteuerte Orchestrierung kann über eine Auswahlliste am Ende der folgenden Listen und Formulare in Security Incident Responseaufgerufen werden:

- Formular „Security Incident“.
- Security Incident-Liste

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zugehörige Liste erkennbarer Elemente des Security Incidents
- Zugehörige Liste „Konfigurationselemente“.

Hinweis:

- Eine Eigenschaft in Security Support Common mit der Bezeichnung **sn_sec_cmn.use_on_demand_tbl_as_allowed** definiert, welche Workflows für die Ausführung bei Bedarf verfügbar sind.
- Wenn die Eigenschaft auf **true**festgelegt ist, sind nur Workflows verfügbar, die in der Tabelle „Orchestration bei Bedarf“ [sn_sec_cmn_on_demand_orchestration] angegeben sind.
- Wenn die Eigenschaft auf **„false“** (Standard) festgelegt ist, sind alle Workflows für in der SecOps-Anwendungsregistrierung konfigurierte Anwendungen verfügbar.
- Je nach Einstellung der Eigenschaft wird die Liste der verfügbaren Workflows auf die Art der zu analysierenden Informationen zugeschnitten.

Führen Sie eine bedarfsgesteuerte Orchestrierung über das Formular „Security Incident“ durch

Die bedarfsgesteuerte Orchestrierung kann über eine Auswahlliste unten im Formular „Security Incident“ aufgerufen werden.

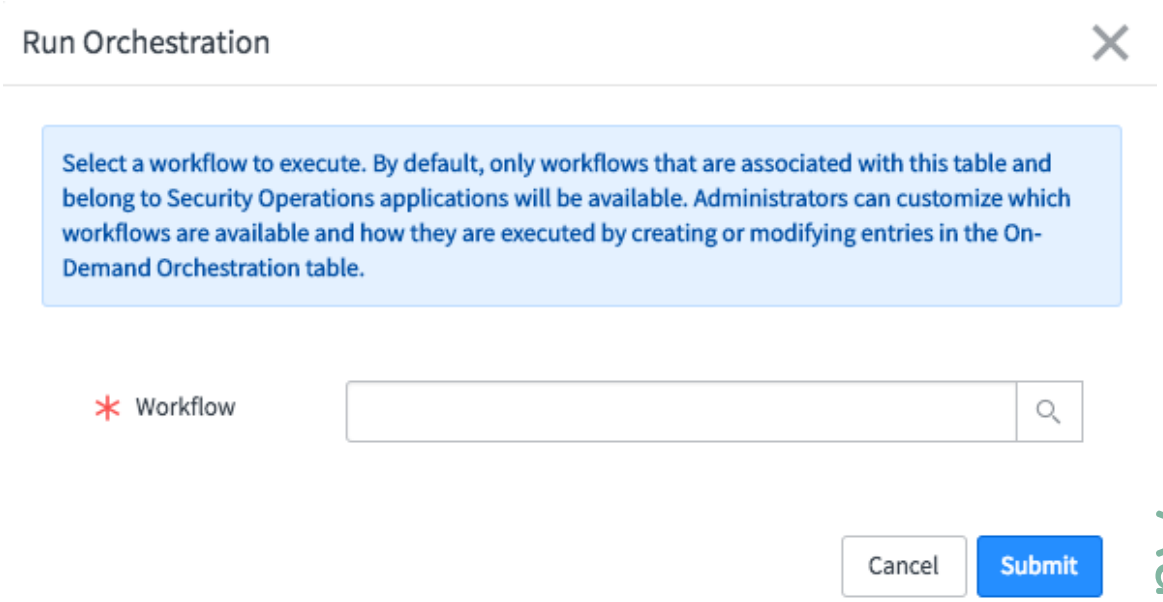
Vorbereitungen

Erforderliche Rolle: sn_si.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
2. Wählen Sie den Datensatz (Security Incident, erkennbares Element oder CI), für den Sie einen Workflow ausführen möchten.
3. Klicken Sie auf den zugehörigen Link **Orchestration ausführen**.
   Das Dialogfeld **„Orchestrierung ausführen“** wird geöffnet. Die Darstellung des Dialogfelds hängt von der Einstellung der Eigenschaft sn_sec_cmn.use_on_demand_tbl_as_whitelist in Security Support Common ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf das Suchsymbol, und wählen Sie den Workflow aus, den Sie ausführen möchten.
   Der ausgewählte Workflow wird ausgeführt. Details finden Sie unter Security Incident Response Orchestration Workflows und Aktivitäten.

Führen Sie eine bedarfsgesteuerte Orchestrierung aus der Liste „Security Incident“ durch

Die bedarfsgesteuerte Orchestrierung kann über die Liste „Security Incident“ sowie über zugehörige Listen in Security Incident Responseaufgerufen werden.

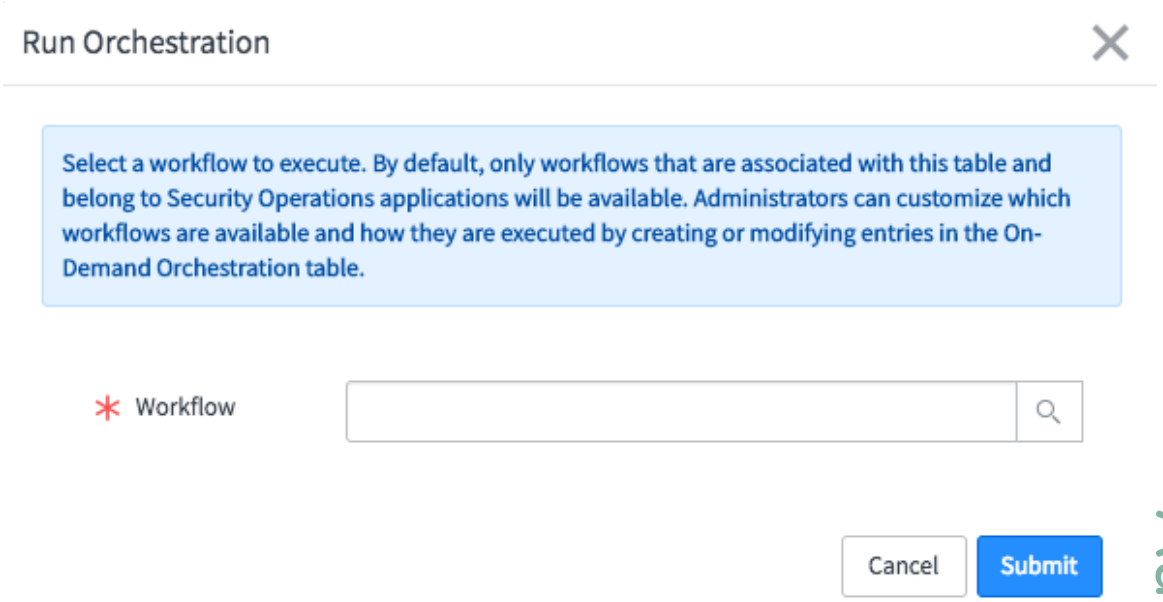
Vorbereitungen

Erforderliche Rolle: sn_si.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
2. Aktivieren Sie das Kontrollkästchen neben dem Security Incident, für den Sie einen Workflow ausführen möchten.
3. Klicken Sie unten auf dem Bildschirm auf die Auswahlliste **Aktionen für ausgewählte Zeilen**, und klicken Sie auf **Orchestration ausführen**.
   Das Dialogfeld **„Orchestrierung ausführen“** wird geöffnet. Die Darstellung des Dialogfelds hängt von der Einstellung der Eigenschaft sn_sec_cmn.use_on_demand_tbl_as_whitelist in Security Support Common ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf das Suchsymbol, und wählen Sie den Workflow aus, den Sie ausführen möchten. Der ausgewählte Workflow wird ausgeführt. Details finden Sie unter Security Incident Response Orchestration Workflows und Aktivitäten.

Definieren Sie neue bedarfsgesteuerte Orchestrationen

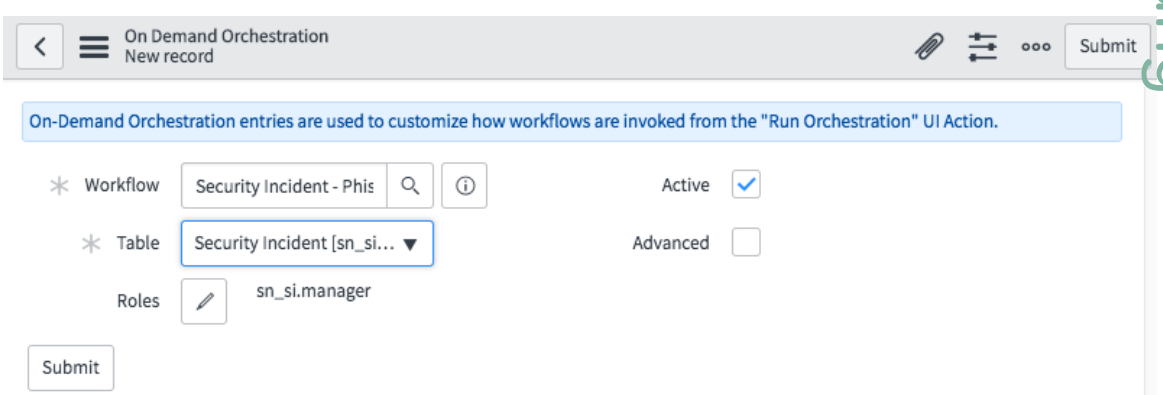
Im Basissystem können Sie bei Bedarf Orchestrationen auswählen, die vordefinierte Workflows ausführen. Sie können neue bedarfsgesteuerte Orchestrationen definieren, um anzupassen, wie Workflows über die Auswahllisten **Orchestration ausführen** aufgerufen werden.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Orchestration bei Bedarf**
2. Klicken Sie auf **Neu**.



3. Füllen Sie die Felder entsprechend aus.

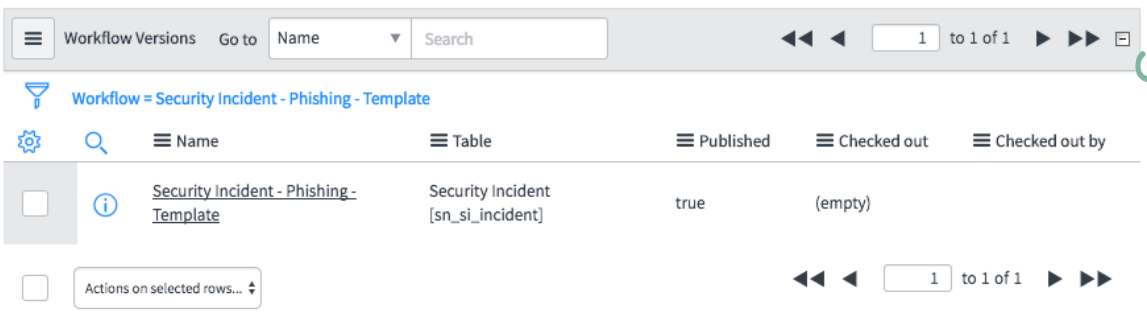
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Orchestration bei Bedarf

Feld	Beschreibung
Workflow	Wählen Sie den Workflow aus, der in die Auswahlliste **Orchestration ausführen** aufgenommen werden soll.
Tabelle	Wählen Sie die Tabelle aus, für die der ausgewählte Workflow ausgeführt wird. Wenn die Tabelle nicht mit der für den ausgewählten Workflow konfigurierten Tabelle übereinstimmt, müssen Sie das Kontrollkästchen **Erweitert** aktivieren und das **Ausführungsskript** so ändern, dass der richtige Datensatz bei der Ausführung an den Workflow übergeben wird.
Rollen	Wählen Sie nach Bedarf zusätzliche Rollen aus, um einzuschränken, wer diesen Workflow in der Auswahlliste **„Orchestration ausführen"** sehen kann.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diesen Datensatz für die bedarfsgesteuerte Orchestrierung zu aktivieren.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um das Ausführungsskript so zu ändern, dass der richtige Datensatz an die ausgewählte Tabelle für diesen Workflow übergeben wird.
Ausführungsskript	Ändern Sie das Ausführungsskript so, dass der richtige Datensatz für diesen Workflow an die ausgewählte Tabelle übergeben wird. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Erweitert** aktiviert ist.

4. Klicken Sie mit der rechten Maustaste auf den Datensatz-Header, und wählen Sie **Speichern**aus.
   Die zugehörige Liste **Workflow-Versionen** wird angezeigt.



5. Wenn Sie weitere Änderungen am Workflow vornehmen müssen, müssen Sie ihn auschecken.

Zugehörige Informationen

Arbeiten Sie mit Workflow-Versionen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie neue Security Operations-Anwendungen für die Orchestrierung bei Bedarf

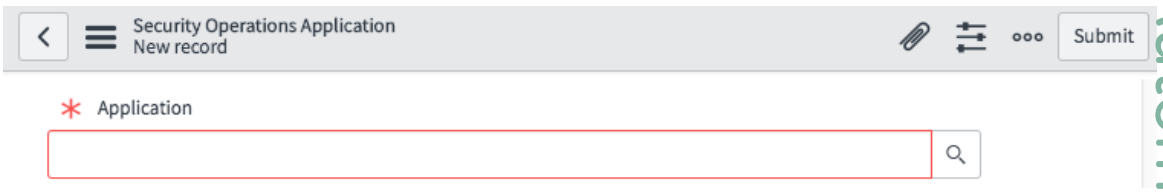
Im Basissystem werden Security Operations-Anwendungen automatisch registriert, wenn sie aktiviert werden. Durch die Registrierung können die Workflows, die den -Anwendungen zugeordnet sind, für Orchestration-Anforderungen bei Bedarf verfügbar sein. Bei Bedarf können Sie neue Anwendungen definieren und ihnen Workflows für die Orchestrierung bei Bedarf zuordnen.

Vorbereitungen

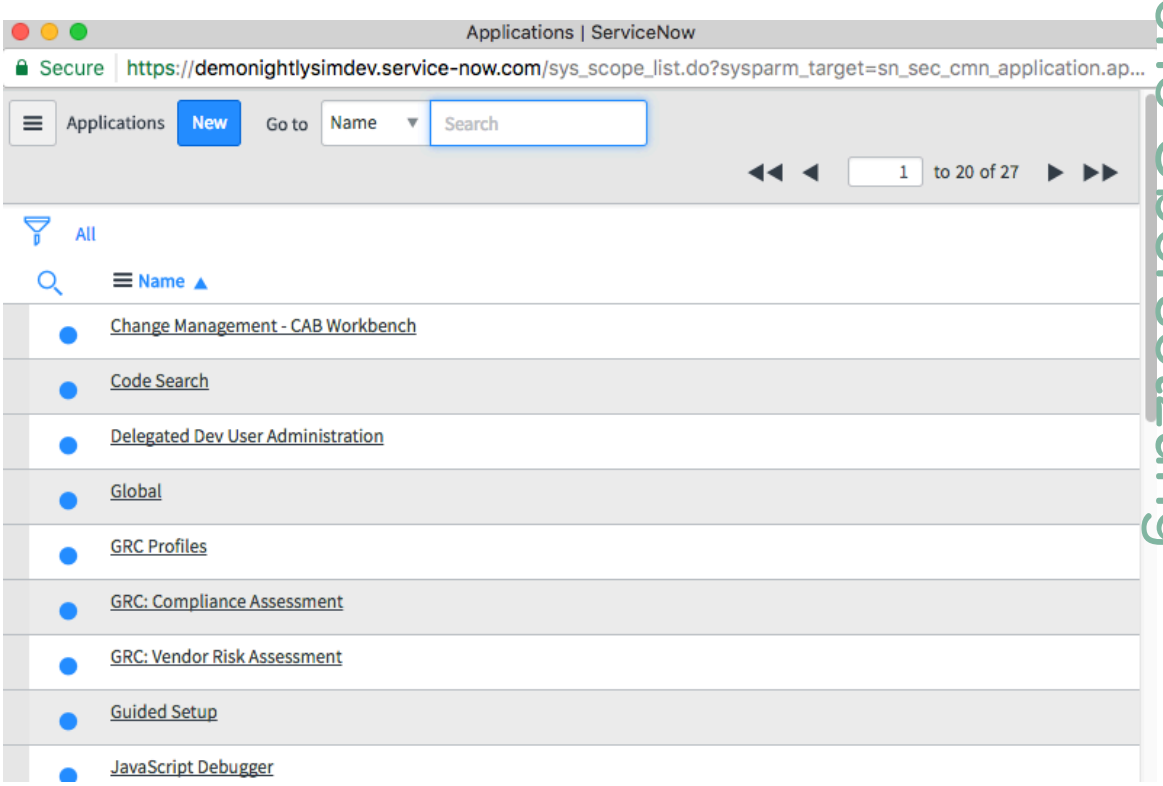
Erforderliche Rolle: sn_si.write

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **SecOps-Applikationsregistrierung**und klicken Sie auf **Anwendung registrieren**.
   Der Bildschirm der Anwendung „Security Operations“ wird angezeigt.



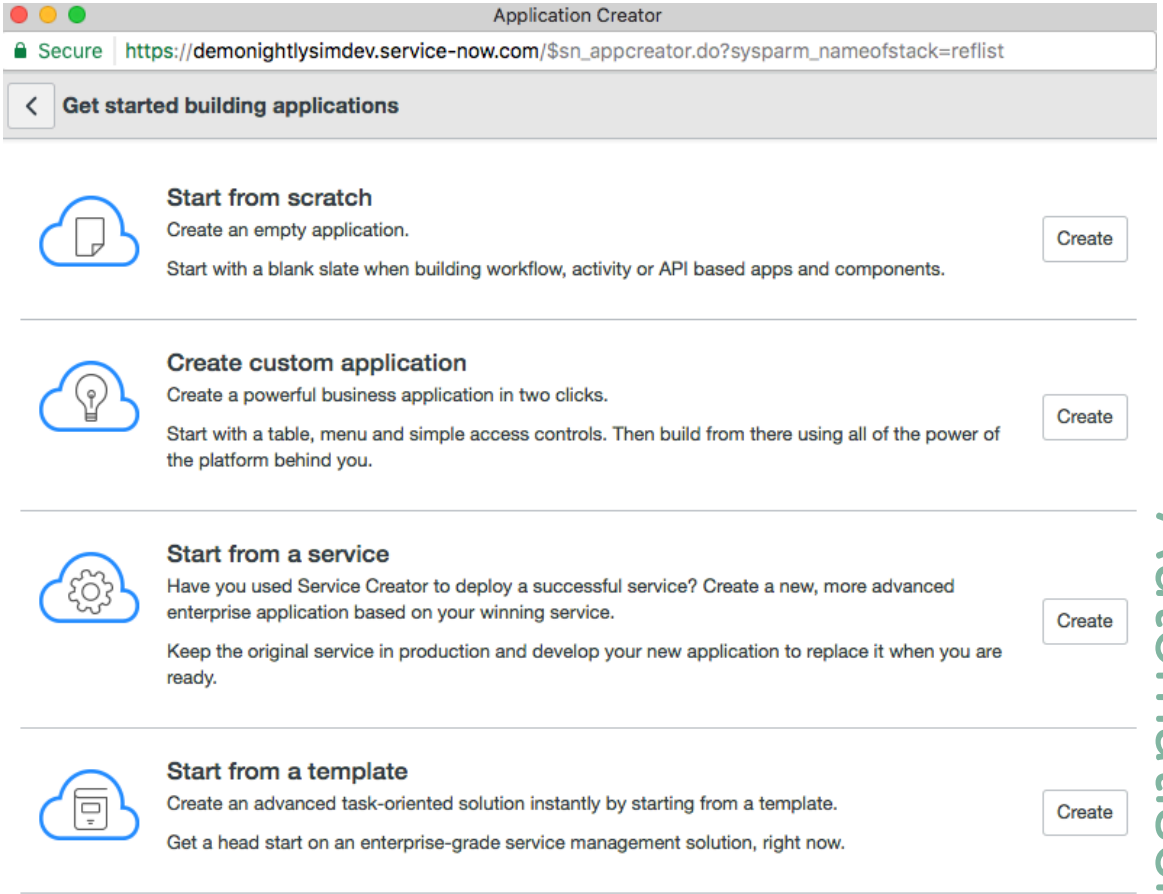
2. Klicken Sie im Feld **Anwendung** auf das Suchsymbol (Lupe).
   Der Bildschirm „Anwendungen“ wird angezeigt.



3. Klicken Sie auf **Neu**.
   Der Bildschirm „Applikationsersteller“ wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die angezeigten Optionen hängen von den Anwendungen ab, die Sie aktiviert haben. Ausführliche Informationen zum Erstellen neuer Anwendungen finden Sie unter Building applications .

4. Nachdem die Anwendung generiert wurde, können Sie Skripts zum Einrichten der bedarfsgesteuerten Orchestrierung erstellen.

Hinweis:
Das Einrichten einer bedarfsgesteuerten Orchestrierung für neue Anwendungen erfordert fortgeschrittene technische Kenntnisse über die Skripterstellung und das Erstellen von Auslösern für die Skripts (Business-Regeln, UI-Aktionen, Workflows usw.). Weitere Informationen erhalten Sie von ServiceNow Professional Services.

Automatische Übersetzung

Fügen Sie einem Security Incident Informationen hinzu

Nachdem ein Security Incident erstellt wurde, können Sie weitere Details hinzufügen, um die Analyse zu unterstützen, z. B. Zugriffsrollen und verschiedene Arten von Notizen.

Vorbereitungen
Erforderliche Rolle: sn_si.basic

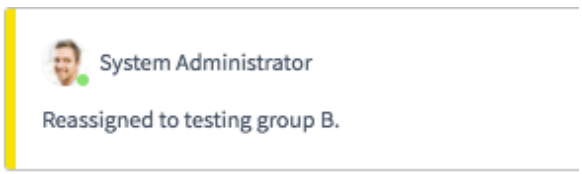
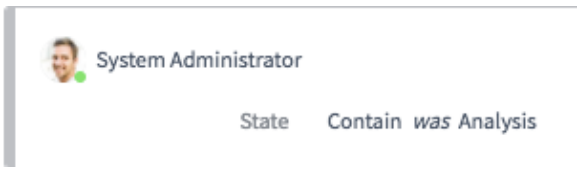
Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf die Registerkarte **Incident-Details**.
3. Füllen Sie die Felder nach Bedarf aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

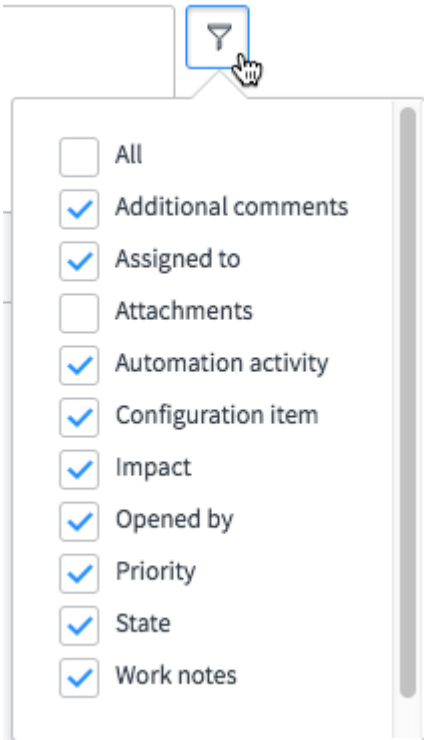
Feld	Beschreibung
Lesezugriff	Gewährt einem Benutzer mit der **speziellen Zugriffsrolle** Lesezugriff auf den Security Incident. Der Benutzer kann Arbeitsnotizen lesen und schreiben. **Hinweis:** ○ Wenn ein Benutzer sowohl den Listen **„Lesezugriff“** als auch **„Privilegierter Zugriff“** hinzugefügt wird, bleiben nur die Berechtigungen **für den privilegierten Zugriff** erhalten. ○ Anwender mit der Rolle „sn_si.admin“ können sowohl Lesezugriff als auch privilegierten Zugriff ändern.
Beobachtungsliste	Klicken Sie auf das Schlosssymbol, um Benutzer hinzuzufügen, die benachrichtigt werden, wenn Änderungen am Security Incident auftreten. Nachdem das Feld entsperrt wurde, stehen Optionen zum Hinzufügen oder Entfernen mehrerer Benutzer oder zum Eingeben von Benutzer-E-Mail-Adressen zur Verfügung. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf das Schlosssymbol, um das Feld zu sperren.
Privilegierter Zugriff	Erteilt einem Benutzer mit der **speziellen Zugriffsrolle** Lese- und Schreibzugriff auf alle Felder des Security Incidents außer **Zugewiesen an**. Benutzer mit speziellen Zugriffsrollen haben ein eigenes Modul, das alle ihnen zugewiesenen Security Incidents enthält. Es stehen ihm keine anderen Module zur Verfügung. Das Modul „ **Für mich sichtbar** “ kann niemand sonst sehen. **Hinweis:** Nur ein zugewiesener Benutzer oder jemand mit einer Sicherheitsrolle (z. B. sn_si_analyst oder sn_si.admin) kann das Feld **Zugewiesen an** ändern. Wenn ein Benutzer sowohl den Listen **„Lesezugriff“** als auch **„Privilegierter Zugriff“** hinzugefügt wird, bleiben nur die Berechtigungen **für den privilegierten Zugriff** erhalten.
Arbeitsnotizenliste	Klicken Sie auf das Sperrsymbol ( ), um Benutzer hinzuzufügen, die benachrichtigt werden, wenn neue Arbeitsnotizen hinzugefügt werden. Nachdem das Feld entsperrt wurde, stehen Optionen zum Hinzufügen oder Entfernen mehrerer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Benutzer oder zum Eingeben von Benutzer-E-Mail-Adressen zur Verfügung. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf das Schlosssymbol, um das Feld zu sperren.
Beschreibung	Geben Sie eine vollständige Beschreibung des Security Incidents ein, zusammen mit allen Informationen, die helfen, die Ursache zu finden oder das Problem zu beheben.
Sichere Notizen	Nur Anwenderrollen mit sn_si.admin und sn_si.analyst können die sicheren Notizen anzeigen oder bearbeiten.
Arbeitsnotizen	Geben Sie Arbeitsnotizen ein, die für den Kunden nicht sichtbar sind. Arbeitsnotizen werden im **Aktivitätsbereich** angezeigt.
Aktivität	Zeigt manuell in Arbeitsnotizen eingegebene Informationen und alle dynamisch aktualisierten Aufgabenaktivitäten (Aktionen, Kommentare, Arbeitsnotizen usw.) in zugehörigen Datensätzen für diesen Security Incident an. Arbeitsnotizen werden mit einem gelben Farbband angezeigt.  Automatisch generierte Notizen werden mit einem grauen Farbband angezeigt. 

4. Sie können die Arten der im Feld **Aktivität** angezeigten Informationen einschränken, indem Sie auf das Filtersymbol ( ) klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Mit dem Kontrollkästchen **Automatisierungsaktivität** können Sie alle durch diesen Security Incident durchgeführten Ergänzungen einbeziehen, einschließlich Workflow-Aktivitäten, Aktualisierungen der Risikopunktzahl usw.

5. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:
   - Zugehörige Datensätze
   - Überprüfung nach Incident
   - Abschlussinformationen
6. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Fügen Sie einem Security Incident zugehörige Probleme, Changes und Incidents hinzu

Sie können zugehörige Datensätze, z. B. Probleme, Changes und Incidents, zu vorhandenen Security Incidents hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf die Registerkarte **Zugehörige Datensätze**.
3. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Problem	Wählen Sie einen Problem-Datensatz (PRB) aus, der das zugrunde liegende Problem löst, das die Erstellung dieses Security Incident verursacht hat. Die PRBs für diesen Incident

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden normalerweise erstellt, indem Sie mit der rechten Maustaste auf den Header des Formulars „Security Incident“ klicken und **Problem erstellen**auswählen.
Übergeordnet	Wählen Sie einen Aufgabendatensatz aus, der sich auf das zugrunde liegende Problem bezieht, das die Erstellung dieses Security Incidents verursacht hat.
Übergeordneter Security Incident	Wählen Sie einen Security Incident-Datensatz aus, der sich auf das zugrunde liegende Problem bezieht, das die Erstellung dieses Security Incidents verursacht hat. Weitere Informationen finden Sie unter Übergeordnete und untergeordnete Security Incident-Beziehungen.
Incident	Wählen Sie einen Incident-Datensatz (INC) aus, der das zugrunde liegende Problem behebt, das zur Erstellung dieses Security Incidents geführt hat. Der Incident wird normalerweise erstellt, indem Sie mit der rechten Maustaste auf den Header des Formulars „Security Incident“ klicken und **Incident erstellen**auswählen.
Change-Anforderung	Wählen Sie einen Change Request (CHG)-Datensatz aus, der das zugrunde liegende Problem behebt, das zur Erstellung dieses Security Incidents geführt hat. Die Change-Anforderung wird normalerweise erstellt, indem Sie mit der rechten Maustaste auf den Header des Security Incident-Formulars klicken und **Change erstellen**auswählen.

4. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:
   - Incident-Details
   - Überprüfung nach Incident
   - Abschlussinformationen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Ruft eine Prozess-Sicherung für einen angereicherten Prozess in Windows auf

Ein Sicherheitsanalyst kann eine Prozesssicherung für einen bestimmten Prozess ausführen, sie in einer Datei speichern und sie an eine freigegebene Site in einem internen Netzwerk senden. Ein Analyst kann dann einen Prozess auf der Deny-Liste anzeigen, der in einem Security Incident rot hervorgehoben ist, und zusätzliche Analysen durchführen.

Vorbereitungen

Die folgenden Elemente sind erforderlich:

- Ein Client mit Windows Vista oder höher oder ein Server mit Windows Server 2008 oder höher.
- Das installierte Befehlszeilendienstprogramm ProcDump mit einer Systemumgebungsvariablen, die auf den Pfad der ausführbaren procdump-Datei verweist. Der Name der Variable muss PROCDUMP lauten. Dieser Name wird in einem PowerShell-Skript verwendet.

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren Sie zu dem Security Incident mit dem angereicherten Prozess, für den Sie einen Procdump aufrufen möchten, indem Sie auf klicken **Alle** > **Security Incident** > **Offene Incidents anzeigen**, und öffnen Sie einen Security Incident.
2. Klicken Sie auf die Registerkarte **Ergänzungsdaten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf den Ergänzungsdatensatz **„Laufende Prozesse abrufen“**.
4. Aktivieren Sie die Kontrollkästchen für die laufenden Prozesse, für die Sie einen Procdump ausführen möchten, klicken Sie auf die Dropdown-Liste Aktionen für ausgewählte Zeilen unten in der Liste, und klicken Sie auf **Procdump ausführen**.
   Die **Meldung Prodump-Workflow für ausgewählten Prozess initiiert** wird oben in der Liste angezeigt, und der **Workflow Security Incident Response – Procdump-Workflow ausführen** wird ausgeführt.

Zeigen Sie Informationen in einem Security Incident an

Über die zugehörigen Links können Sie mehrere andere Aktionen für einen vorhandenen Security Incident ausführen.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. In **„Zugehörige Links**“ können Sie die folgenden Aufgaben ausführen:

Option	Bezeichnung
Manuelles Runbook anzeigen	Zeigen Sie eine Liste der für diesen Security Incident verfügbaren Runbooks an.
Antwort-Workflow	Zeigen Sie alle Workflows an, die diesem Incident zugeordnet sind.
Mehrere erkennbare Elemente hinzufügen	Fügt eine Liste von erkennbaren Elementen in durch Kommas, neuen Zeilen, Registerkarten oder Pipes getrennten Formaten hinzu.
Dem Sicherheitsfall hinzufügen	Fügt den Security Incident einem oder mehreren Sicherheitsfällen hinzu. Sie können auch einen neuen Security Case erstellen und diesen Security Incident hinzufügen.
QRadar-IP-Zusammenfassungen abrufen	Wenn eine QRadar-Integration verfügbar ist und gültige CIs, Quell- und Ziel-IP-Adressen enthält, löst sie die QRadar-Workflows aus und zeigt die Ergebnisse in Arbeitsnotizen an.
Orchestration ausführen	Wählen Sie einen Security Operations-Workflow aus, und führen Sie ihn aus.
View SLA timeline	Sie können eine SLA-Zeitleiste aus einem Aufgaben-SLA-Datensatz oder aus einer SLA-Definition anzeigen.
Alle zugehörigen Listen anzeigen	Zeigt alle standardmäßigen zugehörigen Listen und alle manuell hinzugefügten Listen an. **Hinweis:** Manuell hinzugefügte Elemente sind nur in dieser Ansicht verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Betroffene Elemente anzeigen	Zeigt die Listen der CIs, Benutzer und Services an, die direkt von diesem Incident betroffen sind
Zugehörige Elemente anzeigen	Zeigt die Listen der zugehörigen Incidents, CIs, Benutzer und Gruppen an, die von diesem Incident betroffen sind.
IoC anzeigen	Zeigt die Listen der erkennbaren Elemente, Indikatoren, Malware, Modi und Methoden sowie Sicherheitsscan-Anforderungen an, die diesem Incident zugeordnet sind.
Ergänzungsdaten anzeigen	Zeigt die Listen der Ergänzungsdaten, Prozesse, Services, Statistiken, Suchen, Firewall-Protokolle und gefährdeten Anwenderinformationen an, die diesem Incident zugeordnet sind.
Antwortaufgaben anzeigen	Zeigt die Listen der Aufgaben, SLAs, Risikopunktzahl-Audits, Ausfälle und Exchange-Suchen an, die diesem Incident zugeordnet sind.
Details im externen System anzeigen	Wenn dieser Security Incident aus einer externen Anwendung, direkt oder durch Ereignisse, generiert wurde und ein Link zu den Ursprungsdaten bereitgestellt wurde, wird die URL durch die Aktion **Details in externem System** anzeigen geöffnet. Sie können die Protokolle anzeigen und durchsuchen, von denen dieser Incident generiert wurde.
Auf Schwachstellen scannen	Wenn Vulnerability Response aktiviert ist und Sie mindestens ein betroffenes CI für den Security Incident ausgewählt haben, können Sie eine Scan-Anforderung senden, um zu bestimmen, welche Schwachstellen im CI vorhanden sind.

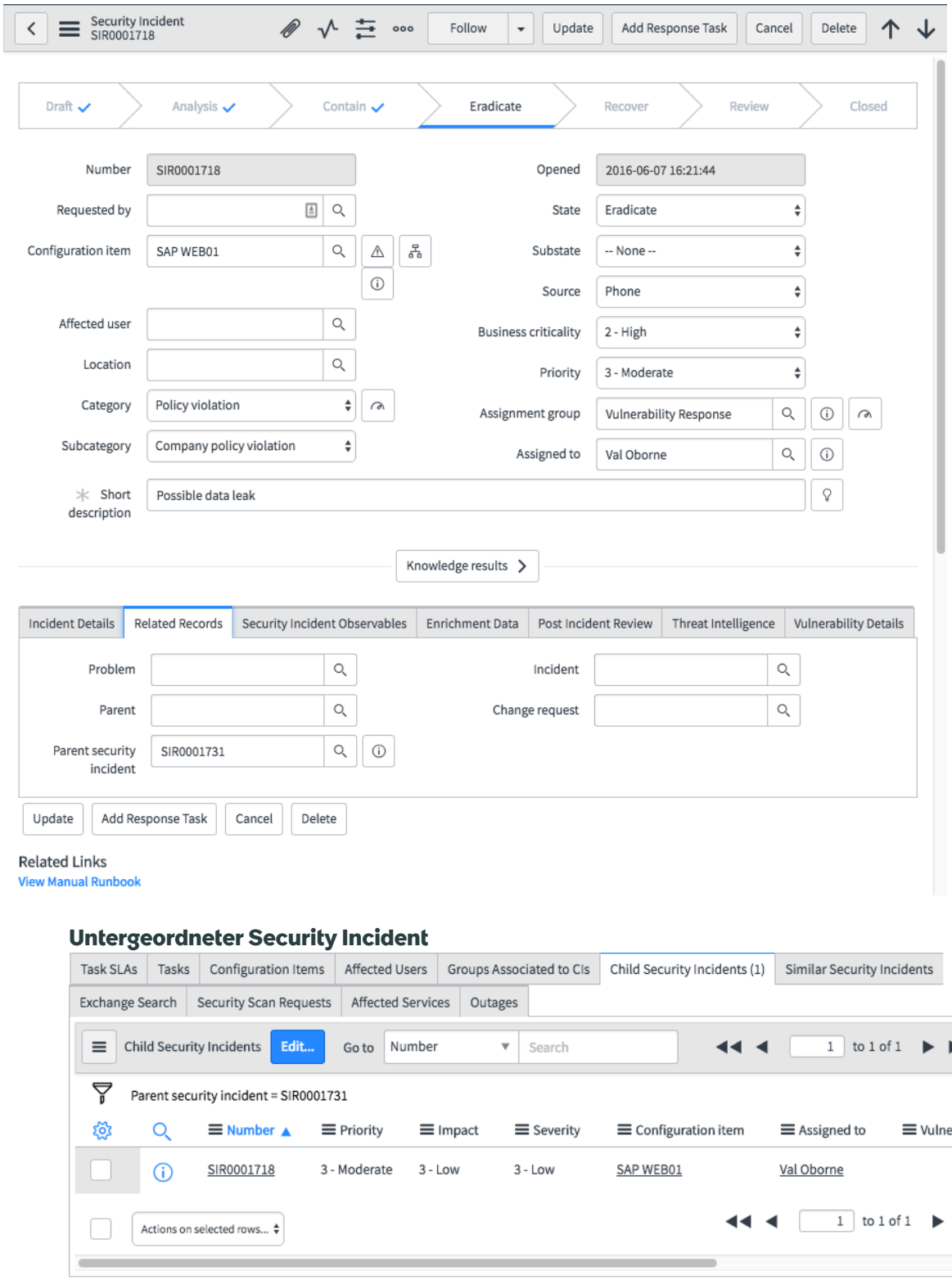
Übergeordnete und untergeordnete Security Incident-Beziehungen

Sie können die Auswirkungen eines bestimmten Problems mithilfe von über- und untergeordneten Security Incident-Beziehungen in Security Incident Responsezuordnen und nachverfolgen.

Auf der Registerkarte **Zugehörige Datensätze** können Sie jedem Formular Security Incident Response ein **übergeordnetes Security Incident-** Problem hinzufügen. Diese Funktion macht den Incident automatisch zu einem untergeordneten Element, das auf der Registerkarte **Zugehörige Listen – Untergeordnete Security Incidents** des übergeordneten Problems angezeigt wird.

Hinweis:
Sie können einen vorhandenen übergeordneten Security Incident nicht zu einem untergeordneten Incident machen, indem Sie für beide Incidents dieselbe Nummer verwenden.

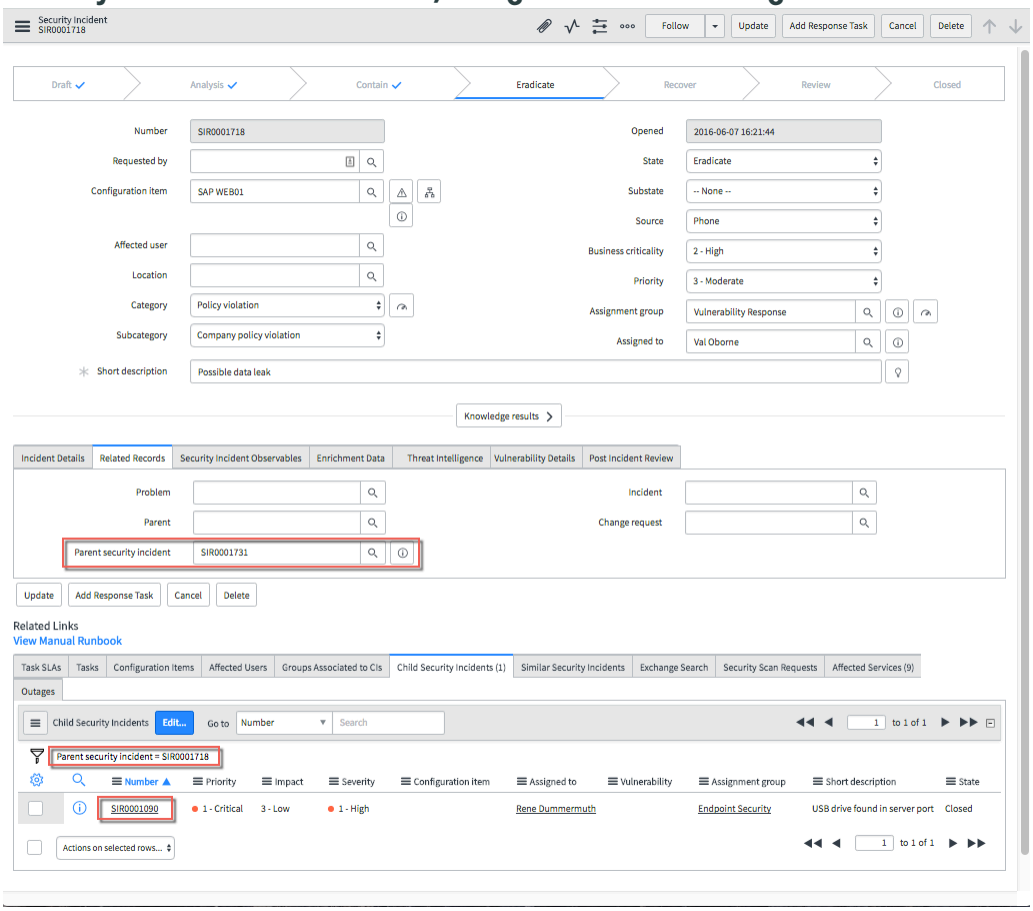
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können jedem **Security Incident-Datensatz auch einen oder mehrere untergeordnete Security Incidents** hinzufügen, indem Sie auf die Schaltfläche **Bearbeiten** auf der Registerkarte **Untergeordnete Security Incidents** klicken. Im folgenden Beispiel sind alle drei Datensätze verbunden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incidents für Großeltern-, übergeordnete und untergeordnete Elemente

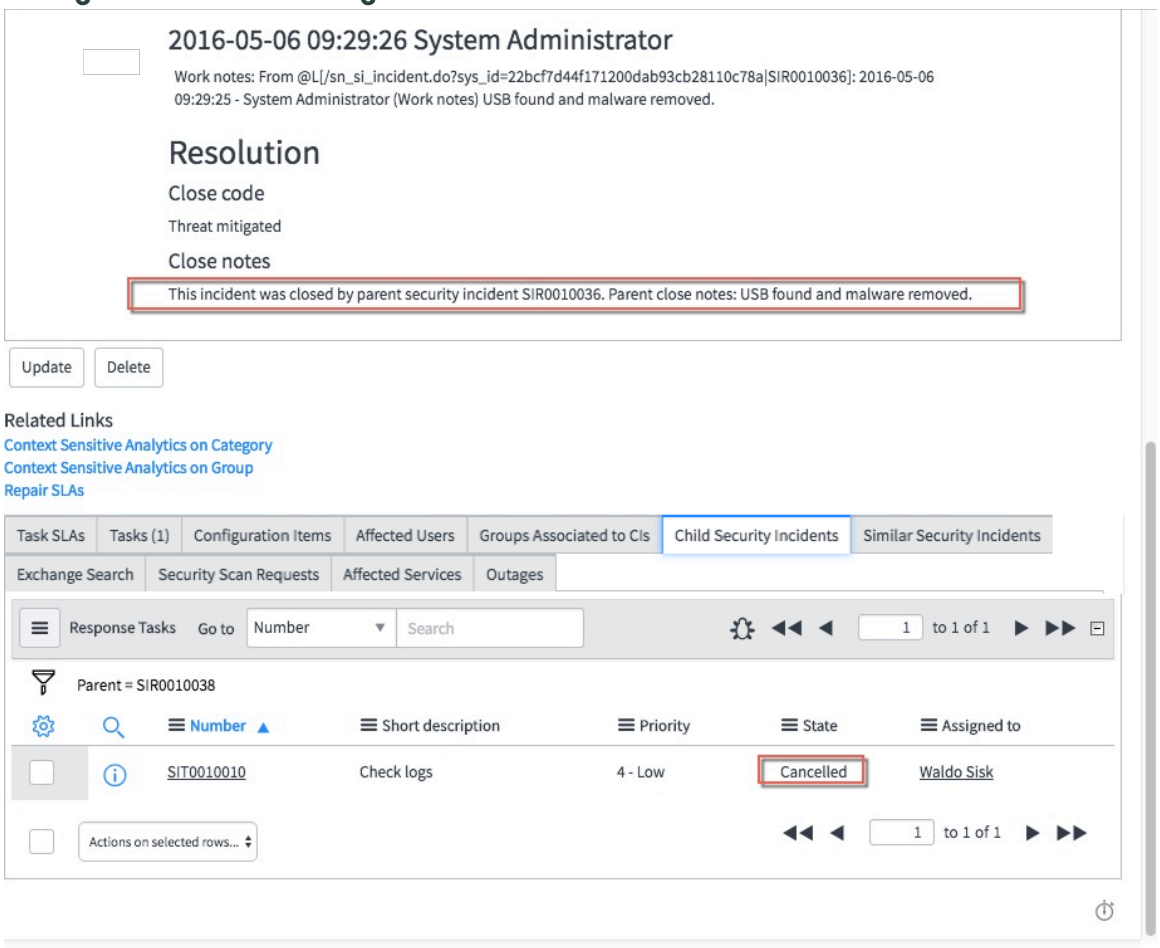


Hinweis: Alle im übergeordneten Element aufgezeichneten Arbeitsnotizen werden an alle aktiven untergeordneten Elemente in **Aktivitäten** unter der Registerkarte **Incident-Details** weitergegeben.

Wenn ein übergeordnetes Element geschlossen oder abgebrochen wird, werden auch alle aktiven untergeordneten Elemente geschlossen oder abgebrochen. Alle aktiven **Antwortaufgaben** für die untergeordneten Incidents werden abgebrochen. Wenn keine weiteren offenen **Aufgaben**vorhanden sind, wird der untergeordnete Incident geschlossen. Beim Schließen zeichnet das **Interview nach dem Incident** den Abschluss auf, und die auf der Registerkarte **Abschlussinformationen** gefundenen Informationen werden vom übergeordneten Element an die untergeordneten Elemente weitergegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untergeordnete Antwortaufgabe schließen



Zeigen Sie betroffene Elemente für einen Security Incident an

Sie können betroffene Elemente anzeigen, z. B. CIs, betroffene Benutzer und betroffene Services, die einem Security Incident zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie betroffene Elemente anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **Betroffene Elemente anzeigen**.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Tab-Taste	Beschreibung
Konfigurationselemente	Betroffene Configuration Items (CI). Nachdem die betroffenen CIs identifiziert wurden, können Sie die betroffenen Ressourcen manuell aus dieser zugehörigen Liste hinzufügen.
Betroffene Anwender	Nachdem die betroffenen Anwender identifiziert wurden, können Sie sie manuell aus dieser zugehörigen Liste hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tab-Taste	Beschreibung
Betroffene Services	Zeigen Sie Business-Services an, die dem Security Incident zugeordnet sind, oder fügen Sie sie hinzu. **Hinweis:** Wenn ein betroffenes CI hinzugefügt wird, nachdem der Security Incident geöffnet wurde, empfiehlt es sich, mit der rechten Maustaste in den Formular-Header zu klicken und **Betroffene Services neu laden**auszuwählen.

Hinweis:
Wenn die Integrationsfunktion „Security Operations Integration – Laufende Prozesse abrufen“ aktiv ist und Sie einem Security Incident ein CI hinzufügen, wird der Workflow „Laufende Prozesse abrufen“ ausgeführt und ruft eine Liste der laufenden Prozesse für das CI ab.

Wenn die Integrationsfunktion „Security Operations Integration – Host isolieren“ aktiv ist, können Sie ein oder mehrere CIs auswählen und ihre Systemverbindungen mit anderen Geräten einschränken. Aktivieren Sie dazu die Kontrollkästchen für die CIs, und klicken Sie in der Auswahlliste **Aktionen für ausgewählte Zeilen aufHost isolieren**.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Zeigen Sie zugehörige Elemente für einen Security Incident an

Sie können zugehörige Elemente anzeigen, z. B. ähnliche und untergeordnete Security Incidents, zugehörige Benutzer, Schwachstellen-Gruppen und angreifbare Elemente, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie zugehörige Elemente anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **Verwandte Elemente anzeigen**.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Tab-Taste	Beschreibung
Untergeordnete Security Incidents	Wählen Sie einen Aufgabendatensatz aus, der sich auf das Problem bezieht, das die Erstellung dieses Security Incidents verursacht hat.
Ähnliche Security Incidents	Zeigen Sie alle anderen Security Incidents an, die einem der gleichen erkennbaren Elemente zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tab-Taste	Beschreibung
Zugehörige Configuration Items	Zeigt eine Liste von Security Incidents an, die Konfigurationselemente mit demselben erkennbaren Element wie dieser Security Incident enthalten. Diese Liste kann mit der Filtergruppe **„CI-Ausschlüsse“** gefiltert werden. Wenn einem Security Incident ein erkennbares Element hinzugefügt wird, wird diese Liste automatisch aktualisiert. Standardmäßig werden erkennbare Elemente mit dem Kontexttyp „Ziel“ ausgeschlossen.
Zugehörige Anwender	Zeigt eine Liste von Security Incidents an, die Anwender mit denselben erkennbaren Elementen wie dieser Security Incident enthalten. Diese Liste kann mit der Filtergruppe **„Benutzerausschluss“** gefiltert werden. Wenn einem Security Incident ein erkennbares Element hinzugefügt wird, wird diese Liste automatisch aktualisiert. Standardmäßig werden erkennbare Elemente mit dem Kontexttyp „Ziel“ ausgeschlossen.
Zugehörige Filtergruppe	Nachdem die Konfigurationselemente identifiziert wurden, werden automatisch übereinstimmende CIs oder Filtergruppen hinzugefügt.
Schwachstellengruppen	Wenn Vulnerability Response aktiviert ist, können Sie Schwachstellen-Gruppen anzeigen, die diesem Security Incident zugeordnet sind.
Angreifbare Elemente	Wenn Vulnerability Response aktiviert ist, können Sie angreifbare Elemente anzeigen, die diesem Security Incident zugeordnet sind.
Risiken	Wenn eines der Core-Plugins für Risikomanagement (Policy and Compliance Management, Audit, Management oder Risk Management) aktiviert ist, können Sie die mit dem Security Incident verbundenen Risiken anzeigen oder hinzufügen. Sie können diese zugehörige Liste über das Kontextmenü des Formular-Headers unter hinzufügen **Konfigurieren** > **Zugehörige Listen**.
Konfigurationselement-Ereignisse	Wenn Ereignismanagement aktiviert ist, können Sie Ereignisse anzeigen.
Warnmeldungen zu Konfigurationselement	Wenn Ereignismanagement aktiviert ist, können Sie Warnungen anzeigen.
Kundenservicefälle	Wenn Kundenservice aktiviert ist, können Sie Informationen zum Fall Kundenservice anzeigen.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Zeigen Sie Ergänzungsdaten für einen Security Incident an

Sie können Ergänzungsdaten anzeigen, z. B. laufende Prozesse, laufende Services und Netzwerkstatistiken, die einem Security Incident zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie Ergänzungsdaten anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **Ergänzungsdaten anzeigen**.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Hinweis:
Rohdatendetails werden in einem Anhang zum Ergänzungsdatensatz gespeichert. Wenn sie die Feldgrenze überschreiten, werden die angezeigten Details abgeschnitten.

Tab-Taste	Beschreibung
Laufende Prozesse	Speichert die vom Workflow Security Incident Response **„Laufende Prozesse abrufen“** erstellten Datensätze.
Laufende Services	Speichert die vom Workflow Security Incident Response **„Laufende Services abrufen“** erstellten Datensätze.
Netzwerkstatistiken	Speichert die vom Workflow Security Incident Response **„Netzwerkstatistiken abrufen“** erstellten Datensätze.
Domänensuchen	Wenn das Plugin WhoisXML-API-Integration aktiviert ist, speichert die Datensätze, die durch eine Whois-Suche erstellt wurden.
Firewall-Protokolle	Speichert Ergänzungsdaten aus Firewall-Protokollen, z. B. die Palo Alto Network-Firewall-Protokolle.
Info zu gefährdetem Anwender	Speichert Accounts, bei denen identifiziert wurde, dass sie durch ein „Have I Been Pwned?“ gefährdet sind. Suche

Hinweis: Die Registerkarte **„Sicherheitsergänzungsdaten“** zeigt Roh-Ergänzungsdaten aus Security Incident Response -Workflows, z. B. Abrufen von Netzwerkstatistiken oder aus laufenden Prozessen. Diese Registerkarte kann angezeigt werden, indem Sie auf den zugehörigen Link **Alle zugehörigen Listen anzeigen** klicken.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Zeigen Sie Informationen zu Antwortaufgaben für einen Security Incident an

Sie können Informationen zu Antwortaufgaben anzeigen, z. B. Aufgaben-SLAs, Risikopunktzahl-Audits und Ausfälle, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie Antwortaufgaben anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **Antwortaufgaben anzeigen**.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Tab-Taste	Beschreibung
Aufgaben	Zeigt Aufgaben an, die bereits für den Security Incident definiert sind. Sie können manuell eine Antwortaufgabe erstellen.
Antwortaufgaben	Zeigt Aktionen an, die als Reaktion auf den Security Incident ausgeführt werden sollen.
Aufgaben-SLAs	Zeigen Sie aktive Aufgaben-SLAs an, die für den Security Incident definiert wurden, oder fügen Sie sie hinzu.
Risikopunktzahl-Audits	Ein Audit-Datensatz für jede Instanz einer Risikopunktzahl, die geändert wird.
Ausfälle	Zeigen Sie neue Ausfalldatensätze an, die dem Security Incident zugeordnet sind, oder fügen Sie sie manuell hinzu.
E-Mail-Suche	Eine Liste von Datensätzen, die Suchkriterien zum Ausführen von Abfragen auf einem E-Mail-Server enthält, z. B. einem Microsoft Exchange Server® (basierend auf der installierten Implementierung), und die erhaltenen Ergebnisse speichert. **Hinweis:** Wenn Security Operations-Integration – Funktion zum Suchen und Löschen von E-Mails nicht aktiv ist, wird der zugehörige Link **„E-Mail-Suche“** nicht angezeigt.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Zeigen Sie zugehörige Ereignisse und Warnungen in Security Incidents an

Während ein Security Incident bearbeitet wird, können Sie die Details der Ereignisse anzeigen. Bei Warnungen können Sie diese Warnungen anzeigen und bestätigen und daraus bei Bedarf Incidents oder Security Incidents erstellen.

Vorbereitungen

Dazu muss das Support-Plugin „Security Incident Response Ereignismanagement“ aktiviert sein.

Erforderliche Rolle: si.sn_agent

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu einer beliebigen Liste der Security Incidents (z. B. **Alle** > **Security Incident** > **Incidents** > **Nicht zugewiesene Incidents**) an.
2. Wenn die Ressourcen, die von dem von Ihnen angezeigten Security Incident betroffen sind, innerhalb der letzten 24 Stunden Warnungen oder Ereignisse erhalten haben, werden eine oder beide der folgenden zugehörigen Listen angezeigt.
   - CI-Warnungen für Security Incidents
   - Security Incident CI-Ereignisse
3. Klicken Sie auf die zugehörige Liste, die Sie anzeigen möchten.

Zugehörige Liste	Beschreibung
CI-Warnungen für Security Incidents	Sie können Details für Warnungen anzeigen, die innerhalb der letzten 24 Stunden eingegangen sind. Sie können auf **Bestätigen** klicken, um anzugeben, dass Sie die Warnung kennen und dass sie bearbeitet wird. Verwenden Sie **„Schließen“**, um anzugeben, dass die Warnung nicht wichtig ist.
Security Incident CI-Ereignisse	Sie können Details für Ereignisse anzeigen, die innerhalb der letzten 24 Stunden empfangen wurden.

Zeigen Sie die Zuordnung von Security Incidents zu Kundenservicefällen an

Security Incident Response wird mit einer Standardfeldzuordnung geliefert, die einen Security Incident einem Kundenservice -Fall zuordnet. Sie können die Standardzuordnung vom Security Incident zum CS-Fall anzeigen.

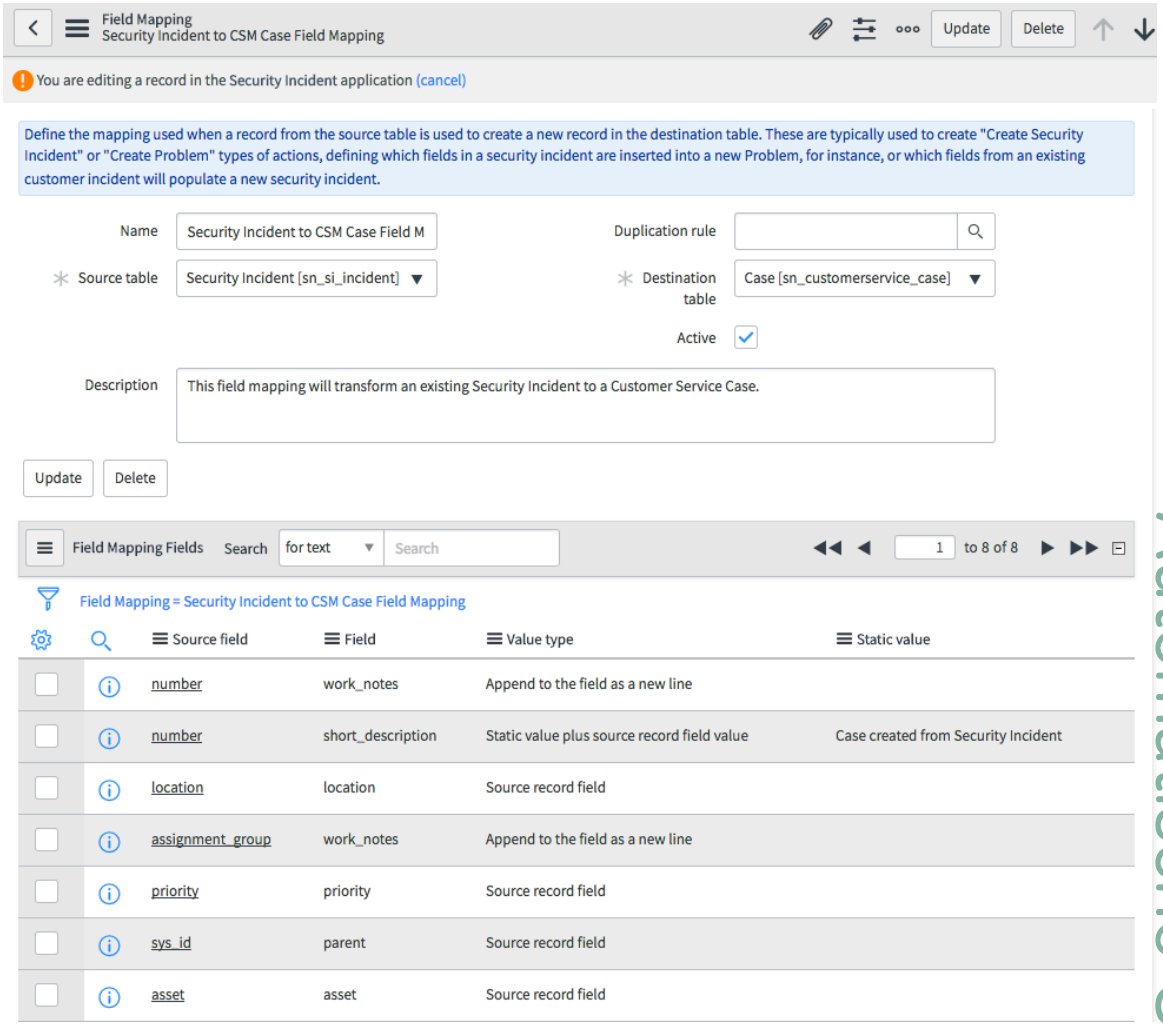
Vorbereitungen

Erforderliche Rolle:sec_cmn.read

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldzuordnung**.
2. Klicken Sie auf **Feldzuordnung von Security Incident zu CSM-Fall,** um die Standardzuordnung anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Sie können die Zuordnung nach Bedarf bearbeiten.

4. Wenn Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **Aktualisieren**.

Zeigen Sie ein Security Incident Response-Runbook an

Runbooks geben Ihnen Zugriff auf Verfahren im Zusammenhang mit den Aufgaben, an denen Sie arbeiten.

Vorbereitungen

Erforderliche Rolle: sn.si.knowledge_admin

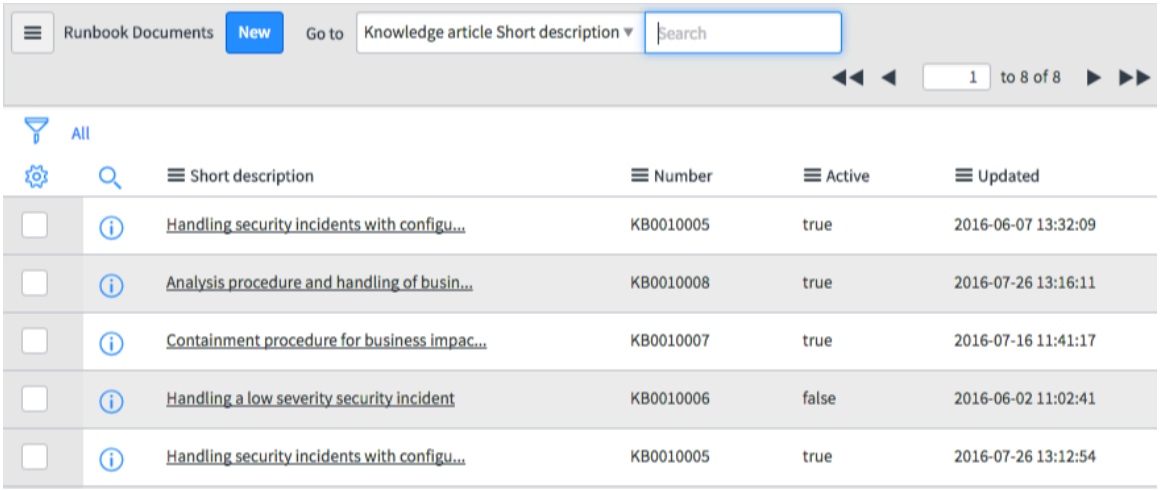
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Manuelles Runbook** > **Runbook-Dokumente anzeigen**.

2. Wählen Sie ein Runbook aus der Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie zum Erstellen eines Runbooks auf **Neu**.
   Weitere Informationen finden Sie unter Runbook erstellen.

Identifizieren Sie alle Configuration Items, die von einem Security Incident betroffen sind

Wenn Sie wissen, welche Ressource (Server, Desktop oder anderes Konfigurationselement) hinter einem Security Incident steckt, und zugehörige Ressourcen und Geschäftsservices identifizieren möchten, die betroffen sein können, können Sie die Zuordnung für Business Service Management (BSM) verwenden.

Vorbereitungen
Erforderliche Rolle: admin oder sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die BSM Map zeigt die vor- und nachgelagerten Abhängigkeiten für ein ausgewähltes Stamm-CI an.

Es gibt zwei Methoden, mit denen Sie die BSM Map für ein CI anzeigen können:

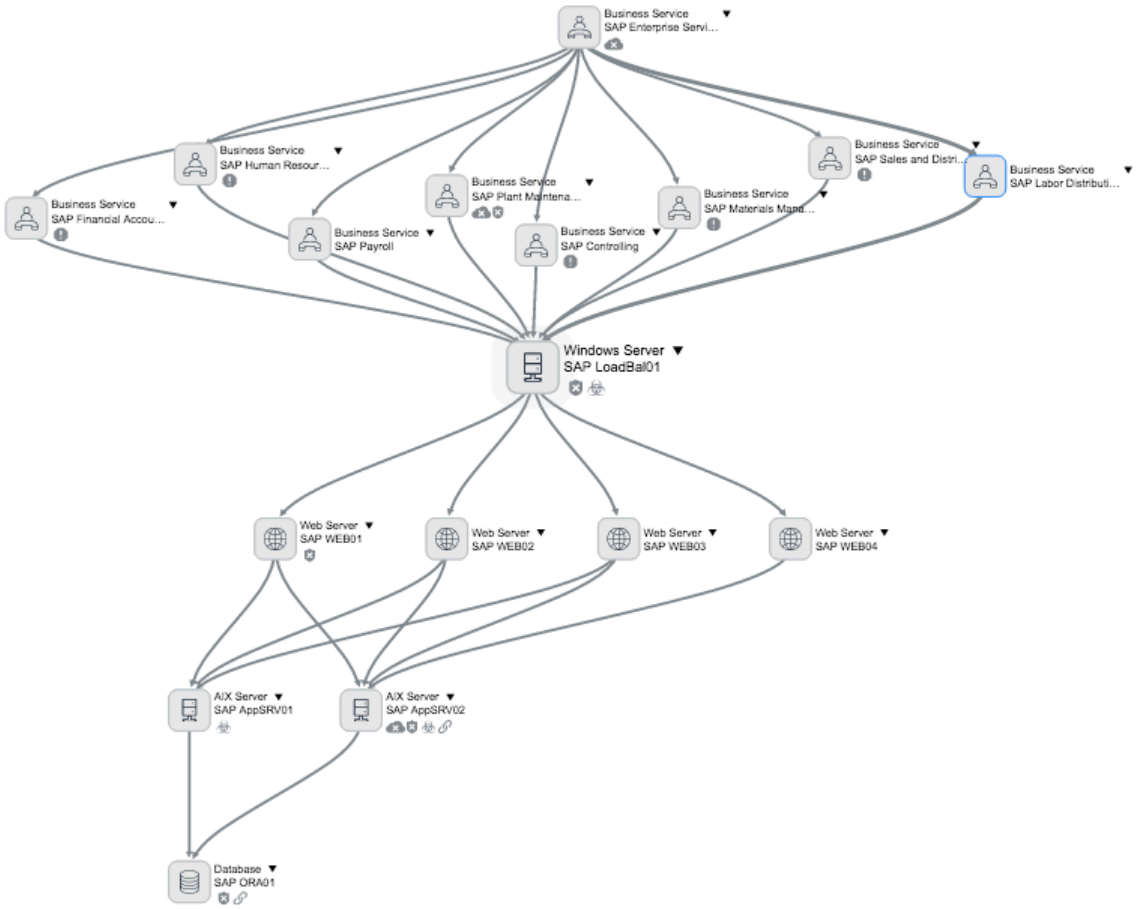
- Wenn Sie CIs aus dem Kontext einer Aufgabe anzeigen möchten, zeigen Sie sie im Formular „Security Incident“ an.
- Wenn Sie CIs nicht aus der Aufgabenansicht anzeigen möchten, zeigen Sie sie in der Navigationsleiste an.

Prozedur

1. Füllen Sie im Formular „Security Incident“ das Feld **Konfigurationselement** aus, und klicken Sie auf das BSM Map-Symbol ( ).
   Auf dem Bildschirm „BSM-Zuordnung“ wird die Zuordnung für den letzten Incident angezeigt, auf den Sie in Incident-Management zugegriffen haben, oder den letzten Security Incident, auf den Sie in Security Incident-Management zugegriffen haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf die Symbole neben einem Konfigurationselement, um verschiedene Arten von Details zur Ressource (Server, Desktop oder anderes CI) anzuzeigen.
   Klicken Sie beispielsweise auf (⚠), um die mit dem CI verknüpften Warnungen anzuzeigen.

   Hinweis:
   Um eine Liste aller verfügbaren Symbole anzuzeigen, klicken Sie über der BSM Map auf **Filter**, und erweitern Sie **Filteraufgabentypen**.

3. Um die Karte in verschiedenen Konfigurationen anzuordnen, wählen Sie eines der über der Karte aufgeführten Formate (**Vertikal**, **Horizontal**, **Radius**), oder klicken Sie auf **Filter**, um die Karte zur einfacheren Anzeige zu filtern.

4. Wenn Sie die BSM Map über das Formular „Security Incident“ geöffnet haben, können Sie dem Security Incident ein abhängiges CI hinzufügen, indem Sie mit der rechten Maustaste darauf klicken und **Betroffene CIs hinzufügen**auswählen.
   Sie können auch mehrere CIs gleichzeitig hinzufügen. Ziehen Sie ein Feld um die CIs, die Sie hinzufügen möchten, klicken Sie mit der rechten Maustaste auf das Feld, und wählen Sie **Betroffene CIs hinzufügen**aus.
   Die CIs werden der zugehörigen Liste Betroffene CIs des Security Incident hinzugefügt.

Berechnen Sie den Schweregrad eines Security Incident

Sie können den Schweregrad eines Security Incident mit vordefinierten Rechnern berechnen.

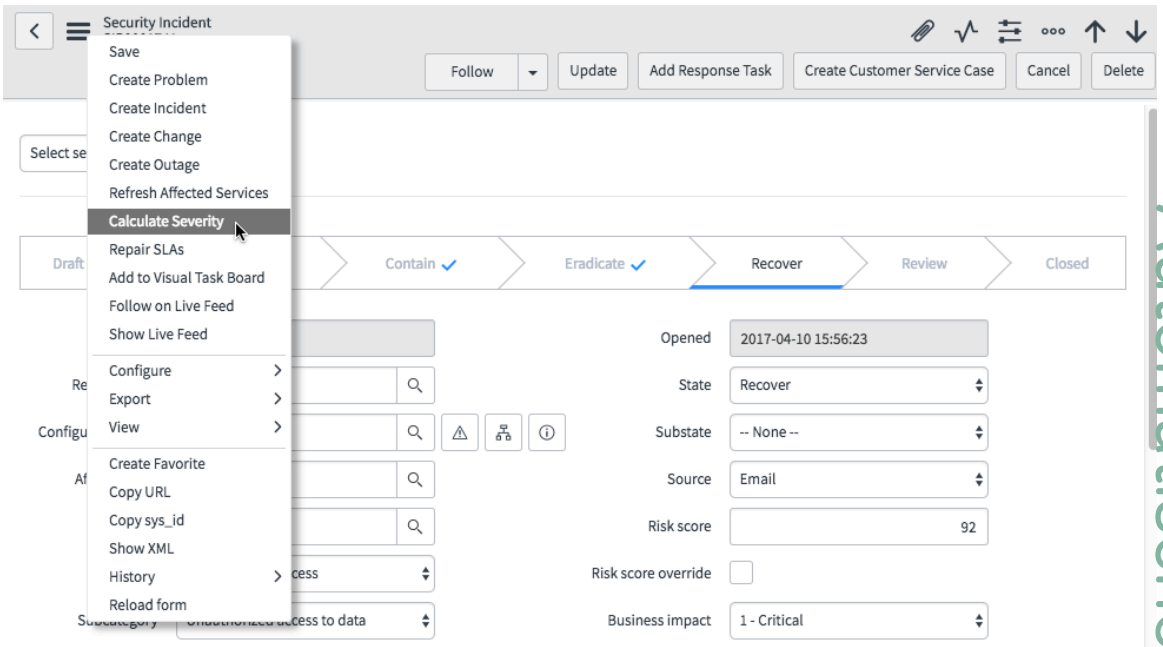
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, dessen Schweregrad Sie berechnen möchten.
2. Klicken Sie auf das Kontextmenü des Formular-Headers, und wählen Sie **Schweregrad berechnen**aus:



Der Schweregrad wird basierend auf den vordefinierten Regeln für Basis-Rechner berechnet. Weitere Informationen finden Sie unter Informationen zu Security Incident-Rechnern.

Suchen und löschen Sie Phishing-E-Mails

Das Löschen von Phishing-E-Mails kann dazu beitragen, das Risiko eines bestimmten Angriffs in einer Organisation zu reduzieren. Sie können Phishing-E-Mails auf Ihrem E-Mail-Server verwalten, indem Sie sie suchen, Genehmigungen erteilen und löschen.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.cap_email_read

Sie können bestimmen, wie viele Benutzer Ziel eines Phishing-Angriffs waren, indem Sie einen E-Mail-Datensatz abfragen, der einem Security Incident zugeordnet ist.

Unterstützte Software:

- Microsoft® Exchange Server 2010

Einschränkung: Wenn Sie den Textkörper von E-Mails durchsuchen, können Sie maximal 1.500 Postfächer durchsuchen.

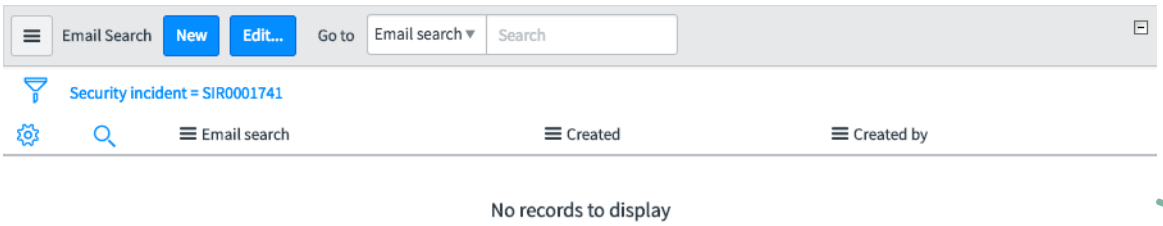
Warum und wann dieser Vorgang ausgeführt wird
Diese Funktion wird von Security Operations Integration - Flow zum Suchen und Löschen von E-Mails verwendet, um eine Abfrage für Ihren E-Mail-Server auszuführen. Abhängig von den von Ihnen ausgewählten Suchkriterien identifiziert die Suche alle E-Mails innerhalb eines Phishing-Angriffs und gibt die Gesamtzahl der betroffenen E-Mails oder Details aus den betroffenen E-Mails zurück.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

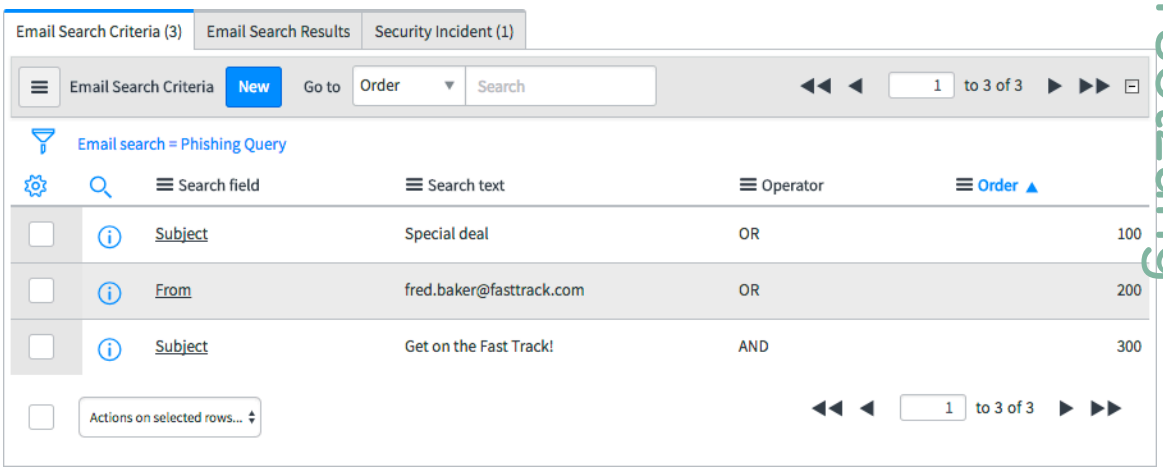
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Wählen Sie einen Security Incident aus.
3. Wenn die zugehörige Liste **E-Mail-Suche** nicht sichtbar ist, klicken Sie auf den zugehörigen Link **Alle zugehörigen Links anzeigen**.
4. Klicken Sie auf die zugehörige Liste **E-Mail-Suche**.



5. Klicken Sie auf **Neu**.
6. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Name	Name der Suchabfrage
Abfrage von Kriterium	Eine Vorschau der Abfrage, die auf dem E-Mail-Server ausgeführt wird. Wird aus allen zugeordneten aktiven Suchkriteriendatensätzen generiert.
Beschreibung	Beschreiben Sie, wonach die Suchabfrage sucht.

7. Klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und wählen Sie **Speichern** aus.



8. Klicken Sie auf die Registerkarte **E-Mail-Suchkriterien** und anschließend auf **Neu**.
9. Füllen Sie die Felder entsprechend aus, oder bearbeiten Sie sie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
E-Mail-Suche	Zeigt den Namen der E-Mail-Suche an. Sie können sie bei Bedarf ändern.
Suchfeld	Feld zum Suchen im E-Mail-Server. Das Suchfeld bietet folgende Auswahlmöglichkeiten: **Betreff** Mit diesem Kriterium wird nach E-Mails gesucht, die den im Feld **„Suchtext“** angegebenen Betreffzeilentext enthalten. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail, einschließlich Empfangsdatum der E-Mail, Lesestatus der E-Mail, Empfänger und Nachrichten-ID, zurückgegeben. **Von** Mit diesem Kriterium wird nach E-Mails gesucht, die die vollständige E-Mail-Adresse des Absenders enthalten (z. B. jane.doe@abc.com), die im Feld **Suchtext** angegeben ist. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail, einschließlich Empfangsdatum der E-Mail, Lesestatus der E-Mail, Empfänger und Nachrichten-ID, zurückgegeben. **Hinweis:** Sie können die Felder **Von** und **Empfänger** nicht in derselben Abfrage verwenden. **Empfänger** Mit diesem Kriterium wird nach E-Mails gesucht, die die vollständige E-Mail-Adresse des Empfängers enthalten (z. B. john.doe@abc.com), die im Feld **Suchtext** angegeben ist. Außerdem wird in den Feldern „An“, „Cc“ und „Bcc“ nach E-Mails gesucht. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail, einschließlich Empfangsdatum

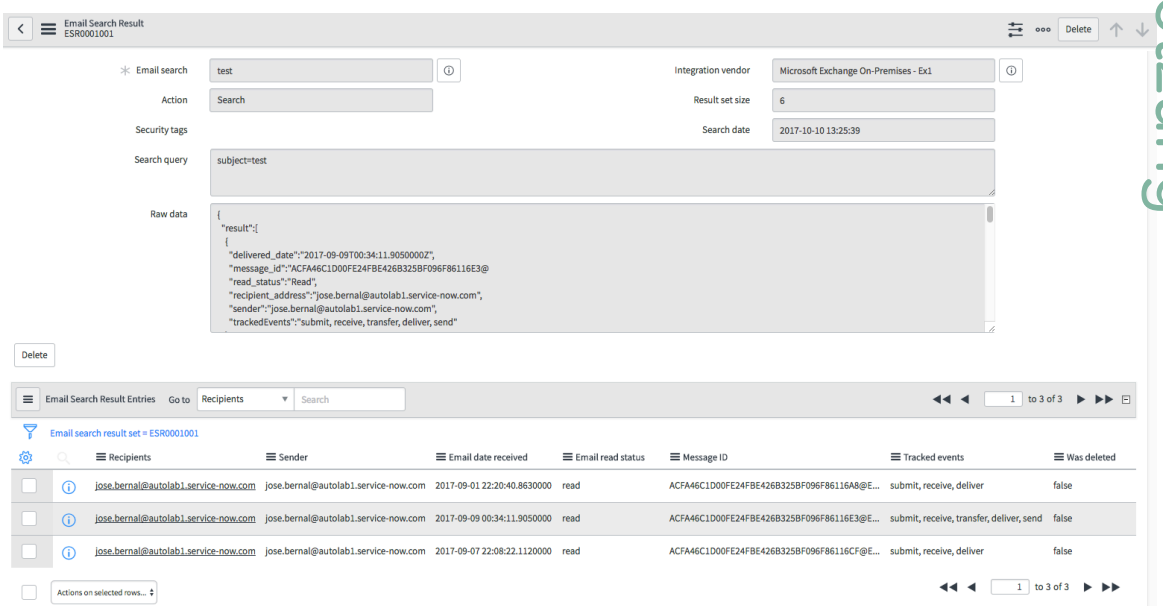
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	der E-Mail, Lesestatus der E-Mail, Empfänger und Nachrichten-ID, zurückgegeben. **Hinweis:** Sie können die Felder **Von** und **Empfänger** nicht in derselben Abfrage verwenden. **Textkörper** Mit diesem Kriterium wird nach E-Mails gesucht, die den im Feld **Suchtext** angegebenen Textkörper enthalten. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. **Hinweis:** Wenn Sie den Textkörper von E-Mails durchsuchen, können Sie maximal 1.500 Postfächer durchsuchen. **Cc:** Mit diesem Kriterium wird nach E-Mails gesucht, die die vollständige Cc-E-Mail-Adresse enthalten (z. B. jane.doe@abc.com), die im Feld **„Suchtext“** angegeben ist. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. **Bcc:** Mit diesem Kriterium wird nach E-Mails gesucht, die die vollständige Bcc-E-Mail-Adresse enthalten (z. B. jane.doe@abc.com), die im Textfeld **„Suchen“** angegeben ist. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. **Anhang** Mit diesem Kriterium wird nach E-Mails gesucht, die entweder den Namen der Anhangdatei oder Anhanginhalte enthalten, die im Feld **„Suchtext“** angegeben sind. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Für die Suche im Anhanginhalt werden nur Nur-Text-Anhänge unterstützt. **Aufbewahrungsrichtlinie** Mit diesem Kriterium wird nach E-Mails gesucht, die Aufbewahrungsrichtliniennummern enthalten, die im Textfeld **„Suchen“** angegeben sind. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese E-Mail-Suchabfrage zu aktivieren.
Betreiber	Mögliche Werte sind UND und ODER. Sie können definieren, wie Suchkriterien kombiniert werden, um auf dem E-Mail-Server ausgeführt zu werden.
Bestellung	Die Reihenfolge, in der die Suchabfrage aus den Suchkriterien erstellt wird.
Suchtext	Der zu suchende Text. Einfache Anführungszeichen, doppelte Anführungszeichen und Doppelpunkte werden nicht unterstützt.

10. Klicken Sie auf **Absenden**.
11. Wiederholen Sie diese Schritte nach Bedarf, um zusätzliche Suchkriterien zu definieren.
12. Sie können die Suchergebnisse anzeigen, indem Sie auf die Registerkarte **E-Mail-Suchergebnisse** klicken.

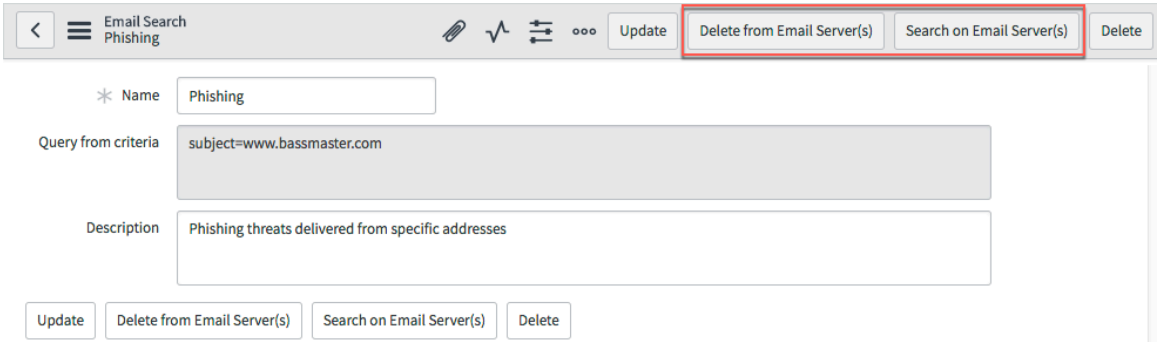


Jede Zeile des Formulars „E-Mail-Suchergebniseinträge“ steht für eine separate E-Mail.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Nachdem Sie einen Suchkriteriendatensatz erstellt haben, werden im Formular „E-Mail-Suche“ zwei Schaltflächen angezeigt: **„Aus E-Mail-Server(n) löschen“** und **„Auf E-Mail-Server(n) suchen“**.



14. Um auf dem ausgewählten Server nach E-Mails zu suchen, die den von Ihnen definierten Suchkriterien entsprechen, klicken Sie **auf Auf E-Mail-Server(n) suchen**.

Erstellen Sie einen Wissensartikel zu Security Incidents

Während Sie mit Security Incidents und Reaktionsaufgaben arbeiten, werden automatisch Wissensartikel angezeigt, die relevante Informationen zur Aufgabe liefern, die Sie gerade ausführen. Ihre Organisation kann Artikel in der Knowledge Base für Security Incidents erstellen und verwalten.

Vorbereitungen

Erforderliche Rolle: sn_si.knowledge_admin

Warum und wann dieser Vorgang ausgeführt wird

Wissensartikel teilen Sicherheitsinformationen, dokumentieren die Arten von Cyberbedrohungen, denen Ihr Unternehmen ausgesetzt ist, und geben Antworten und Antworten auf diese Bedrohungen.

Bei Bedarf können Sie Wissensartikel in Runbooks organisieren, die Zuordnungen zwischen den Artikeln und bestimmten Aufgaben erstellen. Beispielsweise können Sie ein Runbook mit Bedingungen konfigurieren, die die Anzeige eines Knowledge Base-Artikels über Phishing verursachen, wenn Sie einen Security Incident für einen Phishing-Angriff erstellen. Weitere Informationen finden Sie unter Erstellt ein Security Incident Response-Runbook.

Wissensartikel in Runbooks können auch bestimmten Aufgaben in einem Playbook zugeordnet werden. Weitere Informationen finden Sie unter Ordnen Sie einen Wissensartikel einer Playbook-Aufgabe zu.

Wissensartikel bieten unter anderem folgende Vorteile.

- Mitarbeiter haben eine Informationsquelle, die sich leicht durchsuchen lässt.
- Informationen können auf dem neuesten Stand gehalten werden, da Wissensartikel einem definierten Lebenszyklus unterliegen: Erstellung, Überprüfung und Aktualisierung, Veröffentlichung und Löschung.
- Wenn Sie eine Sicherheitsanforderung, einen Incident oder eine Antwortaufgabe manuell erstellen, wird während der Eingabe der Kurzbeschreibung eine Liste relevanter Artikel angezeigt.

Hinweis:
Es ist wichtig, jeder Knowledge Base für Security Incidents einen Knowledge Manager zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Katalog & Wissen** > **Wissen**.
2. Klicken Sie auf das Symbol Artikel erstellen ( ).
3. Füllen Sie die entsprechenden Felder im Formular aus.

Wissensformular

Feld	Beschreibung
Nummer	Die automatisch generierte KB-Nummer.
Knowledge Base	Die für diesen Artikel ausgewählte Knowledge Base.
Kategorie	Die Kategorie für diesen Artikel.
Veröffentlicht	Wann dieser Wissensartikel veröffentlicht wurde. Dieser Wert wird festgelegt, wenn der Artikel erstellt wird, und aktualisiert, wenn der Artikel veröffentlicht wird.
Gültig bis	Wann dieser Wissensartikel abläuft. Dieser Artikel wird nach diesem Datum oder wenn kein Datum ausgewählt ist, nicht in Suchergebnissen angezeigt.
Image	Ein Bild, das bei einer Suche im veralteten Wissensportal neben dem Artikel angezeigt wird.
Workflow	[Schreibgeschützt] Der Veröffentlichungsstatus des Artikels, z. B. Entwurf oder Veröffentlicht. Wann Durch Einfügen eines neuen Artikels aus einem vorhandenen Artikel wird der Status des neuen Artikels auf **Entwurf**zurückgesetzt.
Quelle	Die Aufgabe, für die dieser Knowledge Base-Artikel erstellt wurde, als Reaktion darauf, falls vorhanden. Dieses Feld wird automatisch festgelegt, wenn Sie den Knowledge Base-Artikel aus einem Aufgabendatensatz erstellen.
Link zu Anhang	Kontrollkästchen zum automatischen Herunterladen einer angehängten Datei, wenn ein Benutzer auf den Artikel zugreift, anstatt die Artikelansicht zu öffnen. Fügen Sie dem Artikel einen Anhang hinzu, um diese Option zu verwenden.
Anhänge anzeigen	Kontrollkästchen zum Anzeigen von Anlagen für Benutzer, die diesen Knowledge Base-Artikel anzeigen. Anhänge werden unter dem Artikeltext angezeigt. Fügen Sie dem Artikel einen oder mehrere Anhänge hinzu, um diese Option zu verwenden.
Kurzbeschreibung	Der Titel des Artikels. Dieser Titel erscheint beim Durchsuchen der Knowledge Base-Artikel oben im Artikel.
Text	Inhalt für den Artikel. Verwenden Sie den WYSIWYG-HTML-Editor zum Erstellen von Inhalten. Beim Durchsuchen von Knowledge Base-Artikeln wird eine Vorschau des Inhalts angezeigt.

Hinweis:
Wenn Sie einen Wissensartikel erstellen, der einer Playbook-Aufgabe zugeordnet werden soll, setzen Sie das Feld **Knowledge Base** auf **Security Incident Response-Runbook**.

4. Klicken **einreichen** um den Artikel zu erstellen.

Nächste Maßnahme

Alle zusätzlichen Schritte, die zum Veröffentlichen des Artikels erforderlich sind, wie z. B. Genehmigungen, hängen von ab Veröffentlichungs-Workflow für die Knowledge Base.

Zugehörige Informationen

Erstellt ein Security Incident Response-Runbook

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eskalieren Sie einen Security Incident

Wenn für einen Security Incident ein Eskalationspfad vorhanden ist, ist im Header des Security Incident die Schaltfläche Eskalieren verfügbar.

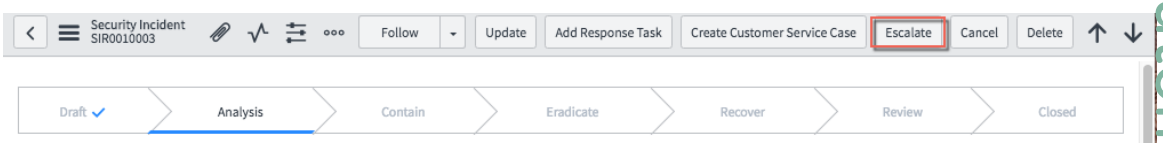
Vorbereitungen

Erforderliche Rolle: sn_si.admin

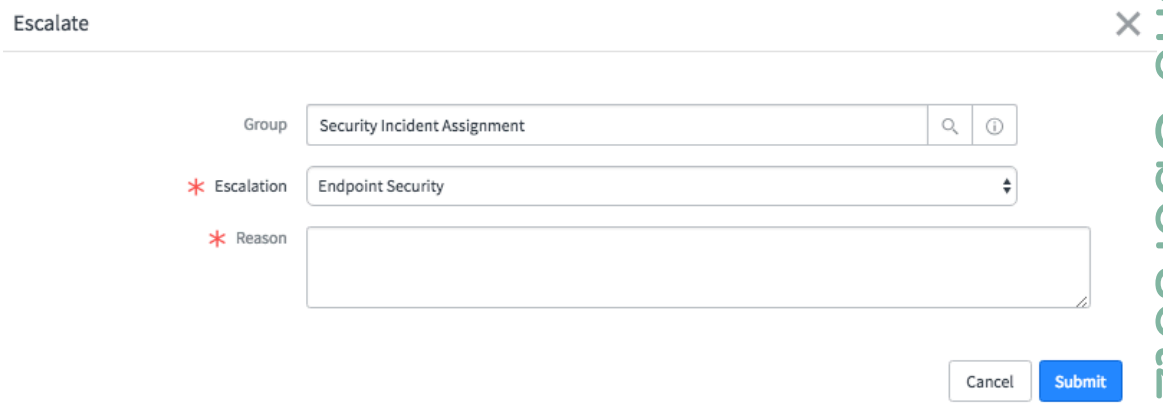
Sie müssen eine Eskalationsgruppe erstellt haben, um diese Schaltfläche anzuzeigen. Weitere Informationen finden Sie unter Erstellen Sie eine anwenderdefinierte Eskalationsgruppe Security Operations ..

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Öffnen Sie den Incident, den Sie eskalieren möchten.
3. Klicken Sie auf die Schaltfläche **Eskalieren**.



4. Wählen Sie eine Eskalationsgruppe aus.
5. Geben Sie einen Grund für die Eskalation ein.



6. Klicken Sie auf **Absenden**.
   Aktualisiert **die Zuweisungsgruppe** und **„Zugewiesen an“** für den Security Incident.

Verwalten Sie Aktivitäten nach Incidents

Basierend auf den Anforderungen Ihres Unternehmens ist häufig eine Überprüfung der Herkunft und Behandlung von Security Incidents erforderlich.

Die Überprüfung nach Incident -Funktion in ServiceNow bietet viele Tools für die Automatisierung, Überwachung und Vereinfachung dieses Prozesses.

In diesem Abschnitt wird Folgendes beschrieben:

- Weisen Sie Rollen für die Überprüfung nach Incident zu
- Konfigurieren Sie eine Auslösebedingung für Bewertungen
- Führen Sie eine fragebogenbasierte Überprüfung nach Incident durch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie PIR-Zuweisungsregeln
- Bericht zur Überprüfung nach Incident

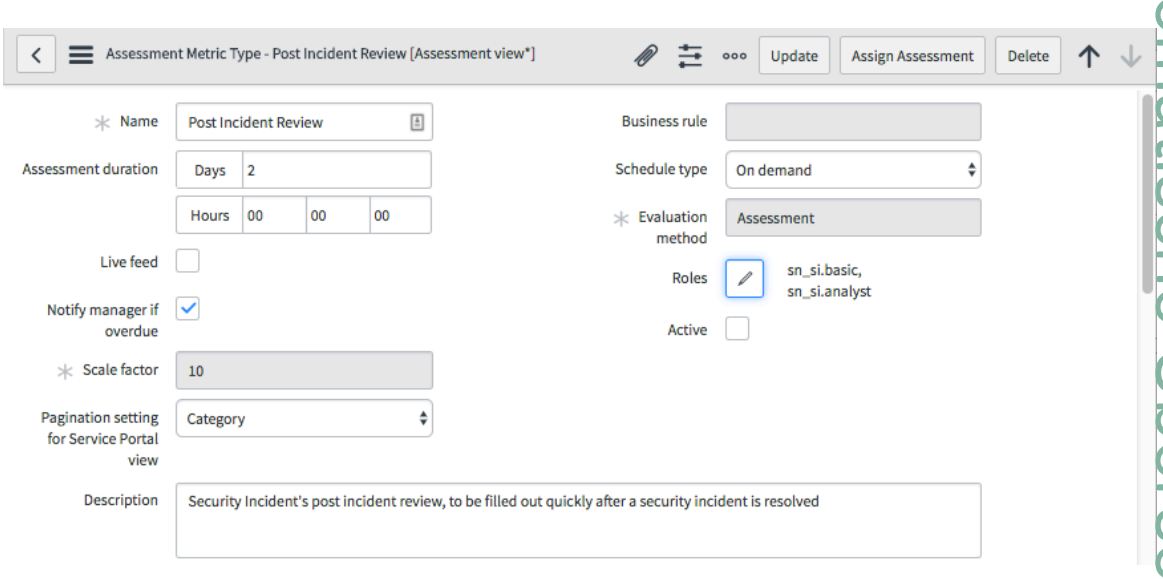
Weisen Sie Rollen für die Überprüfung nach Incident zu

Sie können Fragen an bestimmte vordefinierte Gruppen richten, indem Sie den Kategorien der Überprüfung nach Incidents (Post Incident Review, PIR) Rollen zuweisen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Bewertungen** > **Metrikdefinition** > **Typen**.
2. Suchen Sie in der Spalte **Typen** nach einem Datensatz **zur Überprüfung nach Incident**.
3. Öffnen Sie den Datensatz.
4. Weisen Sie eine oder mehrere Rollen für diese Fragenkategorie zu.



5. Klicken Sie auf **Aktualisieren**.
6. Navigieren zu **Anwenderadministration** > **Anwender**.
7. Wählen Sie einen Anwender aus
8. Fügen Sie dem Benutzerdatensatz eine oder mehrere Metriktyprollen hinzu.

> **Hinweis:**
> Die Rollen müssen den Rollen entsprechen, die in der Kategorie Überprüfung nach Incident zugewiesen sind.

Bericht zur Überprüfung nach Incident

Mit der Funktion zur Überprüfung nach Incidents (PIR) können Sie die Berichte zur Überprüfung nach Incidents über die Registerkarte Überprüfung nach Incidents einrichten und herunterladen.

Der Sicherheitsadministrator kann die Berichtsvorlagen erstellen und konfigurieren und diese Vorlagen mithilfe der Berichtskonfiguration dem Security Incident zuordnen. Ein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsanalyst kann den Bericht dann anzeigen oder herunterladen, nachdem der Security Incident gelöst und der Status in den Status Überprüfen geändert wurde.

Wenn der Incident nach erfolgreicher Konfiguration in den Status „Geschlossen“ versetzt wird, wird ein PDF-Bericht generiert und an den Security Incident angehängt.

Hinweis:
Die Berichtfunktion ist anwendbar und wird ab Orlando Patch9 unterstützt.

Um Ihre Berichte zur Überprüfung nach Incidents anzupassen, müssen Sie die folgende Konfiguration vornehmen.

1. **Berichtsvorlagen**: Sie können die folgenden Berichtsvorlagenfunktionen anpassen und konfigurieren, um dem Bericht zusätzliche Informationen hinzuzufügen:
   a. Zeitleiste
   b. Branding
   c. Vorlagenskripts
2. **Berichtkonfiguration**

In diesem Abschnitt wird das Konfigurationsverfahren beschrieben:

Berichtsvorlagen

Verwenden Sie den Abschnitt Berichtsvorlagen, um primäre und zusätzliche Berichtsvorlagen zu erstellen, die auf die Security Incidents angewendet werden, um den Bericht zur Überprüfung nach Incident zu generieren. Sie können den Bericht entsprechend Ihren Anforderungen formatieren und konfigurieren. Die Vorlagen helfen Ihnen auch, die Bewertungsdetails in die Vorlage aufzunehmen.

Im Folgenden finden Sie einige optionale Schritte, die beim Erstellen der Vorlage ausgeführt werden können:

1. Konfigurieren der Branding-Informationen.
2. Seitengröße und Seitenrand einrichten.
3. Hinzufügen von Feldern im Zusammenhang mit Security Incidents (sowohl anwenderdefiniert als auch standardmäßig).
4. Mit den folgenden vordefinierten anwenderdefinierten Token:
   a. `$sessionUser`: gibt den angemeldeten Anwendernamen zurück
   b. `$date`: gibt das aktuelle Datum zurück
   c. `$if_not_null_start#&#$if_not_null_end`Wenn diese Tags für Felder verwendet werden, werden die Tags nur angezeigt, wenn der Wert vorhanden ist. Beispiel:
      - `${if_not_null_start:problem}`
      - `Problem Category: ${problem.category}`
      - `${if_not_null_end:problem}`
5. Einschließen der zugehörigen Listendaten mithilfe der Vorlagenskripts. Weitere Informationen finden Sie im Abschnitt weiter unten unter **Vorlagenskripts**.
6. Einbeziehen der Zeitleisteninformationen mithilfe der Zeitleistenfilter. Weitere Informationen finden Sie im Abschnitt weiter unten unter **Zeitleiste**.
7. Vorlageninhalte wie Anhänge, Tabellen und Bilder verwalten und formatieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die erweiterten Funktionen der Symbolleiste für Berichtsvorlagen sind nur ab der Paris-Release-Version verfügbar.

Wichtige Punkte für Berichtsvorlagen:

1. Die an die Berichtsvorlage angehängten Bilder werden nur dann im Bericht zur Überprüfung nach Incident angezeigt, wenn sie in der Tabelle „sys_attachment“ enthalten sind.

   Hinweis:
   Bilder, die in der Tabelle „db_image“ ausgewählt wurden, werden nicht im Bericht zur Überprüfung nach Incident angezeigt.

2. Videos werden im Bericht zur Überprüfung nach Incident nicht unterstützt.
3. Die URLs in der PDF-Datei können nicht angeklickt werden. Um die nicht anklickbaren URLs zu aktivieren, wird (.) mit (Punkt) gekennzeichnet.
4. Der Bericht wird nicht generiert, wenn die Größe der Berichtsvorlage 50 MB überschreitet.
5. Die für den Inhalt der Berichtsvorlage ausgewählte Schriftartfamilie wird nicht auf die PDF-Datei angewendet, wenn sie vom PDF-Generator nicht unterstützt wird.

   Hinweis:
   Wenn die entsprechende Schriftart nicht vorhanden ist, identifiziert der PDF-Generator die alternative, am nächsten liegende Schriftart und generiert dann die PDF-Datei.

6. Wenn Sie höhere Seitenrandwerte angeben, schlägt das Generieren des Berichts zur Überprüfung nach Incident fehl. Beispiel: Oberer und unterer Rand > 450 und linker und rechter Rand > 450.
7. Wenn die Berichtsvorlage einen großen Text ohne Leerzeichen enthält, wird der Text möglicherweise gekürzt. Zeigen Sie eine Vorschau des Texts an, und ändern Sie ihn entsprechend.

Der -Sicherheitsadministrator kann den Bericht über die Schaltfläche **Vorschaubericht** anzeigen, die auf der Seite mit den Berichtsvorlagen verfügbar ist.

Hinweis:

Wählen Sie einen Security Incident aus, um eine Vorschau eines Berichts mit dieser Vorlagenoption anzuzeigen, und klicken Sie auf **Vorschaubericht**.

Branding

Sie können den Namen der Branding-Vorlage, das Kopf- und Fußzeilenbild sowie den Kopf- und Fußzeilentext hinzufügen, Seitenzahlen generieren und den Branding-Datensatz nach der Erstellung in die Berichtsvorlage aufnehmen.

Im Folgenden finden Sie ein Beispiel für ein Branding-Berichtsformat:

Kernpunkte des Brandings in Berichtsvorlagen:

1. Die maximal zulässige Größe für das Header- und Footerbild beträgt 5 MB. Wenn die Größe den angegebenen Grenzwert überschreitet, wird im Security Incident die Fehlermeldung „Bildformat kann nicht erkannt werden“ angezeigt.
2. Die Länge des Fußzeilentexts ist auf 100 Zeichen beschränkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

a. Wenn sich der Text des Fußzeilenbilds und der Berichtsinhalt während der Vorschau überschneiden, müssen Sie Änderungen am Branding-Datensatz vornehmen.

b. Wenn der Fußzeilentext einen URL-Link enthält, kann er sich mit dem Fußzeilenbild überlappen. Zeigen Sie eine Vorschau an, und korrigieren Sie sie nach Bedarf.

Zeitleiste

Die Konfiguration der Zeitleiste ermöglicht Ihnen das Erstellen und Ändern der Zeitleistenfilter nach Bedarf. Sie können die Aktivitätstypen filtern, die in den Bericht aufgenommen werden sollen, konfigurieren, ob die untergeordneten Aufgaben in den Bericht aufgenommen oder ausgeschlossen werden sollen, und konfigurieren, ob die Bilder in den Bericht aufgenommen oder ausgeschlossen werden sollen.

Wenn Sie eine Zeitleistenkonfiguration verwenden und ausfüllen möchten, müssen Sie das Tag wie unten erwähnt hinzufügen: `${timeline:timeline name}`. Im Setup werden zwei Beispiel-Zeitleistenkonfigurationen bereitgestellt, die in der Phishing-Berichtsvorlage und der Standardberichtsvorlage verwendet werden. Sie können die -Konfigurationen ändern und wiederverwenden.

Vorlagenskripts

Verwenden Sie die Vorlagenskripts, um die Daten der zugehörigen Listen, Datums- und Zeitstempel und andere Daten einzubeziehen, die nicht direkt Dot-Walk-fähig sind. Es folgt ein Beispiel:

Erstellen Sie ein Vorlagenskript zum Anzeigen der zugehörigen Liste in der Berichtsvorlage:

1. Um die Daten der zugehörigen Liste vorzubereiten, rufen Sie die Methode PostIncidentReportUtils.fetchRelatedListDataForReport auf.
2. Um die step1-Daten im Tabellenformat und -stil darzustellen, rufen Sie die ReportTemplateUtil.constructTablefunction-Methode auf.

Wenn Sie ein Vorlagenskript verwenden und ausfüllen möchten, müssen Sie das Tag-Vorlagenskript-Tag als `${template_script:script name}`hinzufügen.

Im Folgenden finden Sie einige Beispielvorlagenskripts zum Konfigurieren und Ändern Ihrer Nachfolgeberichte zu Incidents.

Skriptname	Beschreibung
format_current_date	Gibt das aktuelle lokale Datum und die aktuelle Uhrzeit im Format TTMMJJJJ 00.00 AM oder PM zurück. Beispiel: 21. Januar 2021 15:51 PST.
si_affected_users	Gibt die betroffenen Anwender aus der zugehörigen Liste in Tabellenform zurück.
si_assessments	Gibt die Ergebnisse der Bewertung nach Incident in Tabellenform zurück.
si_associated_phish_emails	Gibt die zugeordneten Phishing-E-Mails aus der zugehörigen Liste in Tabellenform zurück.
si_associated_phish_headers	Gibt die zugeordneten Phishing-Header aus der zugehörigen Liste in Tabellenform zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Skriptname	Beschreibung
si_business_criticality	Gibt einen farbcodierten Wert für die Geschäftskritikalität zurück.
si_malicius_observables	Gibt die schädlichen erkennbaren Elemente aus der zugehörigen Liste in Tabellenform zurück.
si_observables	Gibt die erkennbaren Elemente aus der zugehörigen Liste in Tabellenform zurück.
si_priority	Gibt einen farbcodierten Prioritätswert zurück.
si_response_tasks	Gibt die Antwortaufgaben aus der zugehörigen Liste in Tabellenform zurück.
si_time_to_identify	Gibt die Dauer zurück, die im Status Entwurf und Analyse verbracht wurde.
si_time_to_resolve	Gibt die Zeit bis zur Lösung des incident zurück.

Wichtige Punkte von Berichtsvorlagenskripts:

1. Wenn eine zugehörige Liste mit mehr als 5 Spalten hinzugefügt wird, werden die Tabellendaten während der PDF-Generierung gekürzt. Die Mindestbreite jeder Spalte ist auf 124 px festgelegt.
2. Wenn ein Vorlagenskript den Inhalt aufgrund technischer Probleme nicht in der Berichtsvorlage laden kann, wird im Bericht die Fehlermeldung „Fehler beim Auswerten des Vorlagenskripts“ angezeigt, und der Sicherheitsadministrator muss die Richtigkeit des Skripts bewerten, um das zu beheben Problem.
3. si_assessments: Standardmäßig werden alle Bewertungskategorien einem Bericht hinzugefügt. Der Sicherheitsadministrator kann die Daten filtern, indem er das Vorlagenskript nach Bedarf ändert. Fügen Sie den Parameter `categories: sys_id1, # sys_id2;` hinzu, um die Daten zu filtern.
4. Zeit für Lösung und Zeit für Identifizierung von Skripts: Verwenden Sie die Definitionsdatensätze, die Teil der zugehörigen Liste der Metriken sind. Wenn die Definitionsdatensätze für den Security Incident nicht verfügbar sind, erstellen oder fügen Sie sie hinzu, um die Werte für die beiden Felder auszufüllen.

Hinweis:

Standardmäßig hat der -Sicherheitsadministrator keinen Zugriff zum Anzeigen der Versionsdatensätze einer Tabelle. Sie müssen die Administratorrolle hinzufügen, um auf die Versionsdatensätze zuzugreifen und zur vorherigen Version zurückzukehren.

Berichtkonfiguration

Verwenden Sie den Abschnitt „Berichtskonfiguration“, um die Bedingungen einzurichten und die Berichtsvorlagen auf die Security Incidents anzuwenden. Sie können derselben Bedingung einen primären Bericht und mindestens eine zusätzliche Berichtsvorlage hinzufügen.

Im Folgenden finden Sie eine Beispielbedingung zum Anwenden der Phishing-Berichtsvorlage auf Incidents der Phishing-Kategorie und eine weitere Bedingung zum Anwenden der Standardberichtsvorlage auf alle Security Incidents. Die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardberichtsvorlage wird auf die Security Incidents angewendet, wenn die Bedingungen nicht erfüllt sind.

Verfahren zum Deaktivieren der neuen Implementierung

1. Deaktivieren Sie die folgenden Geschäftsregeln:
   a. PIR-PDF generieren
   b. Wissen über Abschluss neu erstellen
2. Aktivieren Sie die folgenden Geschäftsregeln:
   a. In „Überprüfen und schließen“ PIR generieren
   b. Wissen über Abschluss erstellen
   c. [PIR bei Abschluss/Abbrechen/Löschen erneut generieren]
3. Aktivieren Sie die UI-Regel *`Hide PIR field when empty`*.
4. Wechseln Sie zum Formularlayout im Formular „Security Incident“. Im Abschnitt **„Überprüfung nach Incident“** :
   a. Entfernen Sie die PIR-Berichtsauswahl aus dem PIR-Abschnitt
   b. Fügen Sie dem PIR-Abschnitt das Feld „Nachfolgebericht zum Incident“ hinzu

Konfigurieren Sie die Eigenschaften des PIR-Berichts (Post Incident Review) für untergeordnete Security Incidents

Sie können die folgenden beiden PIR-Berichtseigenschaften für untergeordnete Security Incidents konfigurieren:

- **sn_si.generate_vir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_vir**

Hinweis:
Benutzer mit der Rolle „Systemadministrator“ [admin] können die Eigenschaften von anzeigen. Benutzer mit der Rolle „Sicherheitsadministrator“ [sn_si.admin] können sie ändern.

Konfigurieren Sie PIR-Berichtseigenschaften für untergeordnete Security Incidents

Eigenschaft	Monatlich
sn_si.generate_vir_report_for_child_si	Mit dieser Option wird die Generierung von PIR-Berichten (Post Incident Review) für untergeordnete Security Incidents aktiviert. • **Typ**: true | false • **Standardwert**: false • **Speicherort**: Navigieren Sie zu Alle > Systemeigenschaften > Alle Eigenschaften.
sn_si.include_child_si_timeline_in_vir	Option, um die Zeitleiste der untergeordneten Security Incidents in den PIR-Bericht des übergeordneten Security Incident aufzunehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie PIR-Berichtseigenschaften für untergeordnete Security Incidents (Fortsetzung)

Eigenschaft	Monatlich
	• **Typ**: true | false • **Standardwert**: false • **Speicherort**: Navigieren Sie zu Alle > Systemeigenschaften > Alle Eigenschaften.

Verwalten Sie den Bericht zur Überprüfung nach Incident

Der Bericht zur Überprüfung nach Incidents verwaltet enthält die Informationen, die vom Sicherheitsadministrator konfiguriert und angewendet wurden. Sicherheitsanalysten können die Zeitleistenfilter zur Laufzeit ändern und herunterladen.

Vorbereitungen
Erforderliche Rolle: sn.si_analyst

Warum und wann dieser Vorgang ausgeführt wird
Der Sicherheitsanalyst kann eine der verfügbaren primären oder zusätzlichen Berichtsvorlagen auswählen, die Zeitleistenfilter konfigurieren, eine Vorschau des Berichts anzeigen und ihn herunterladen. Der Sicherheitsanalyst kann den Bericht auch direkt mit der zuletzt angewendeten Zeitleistenkonfiguration herunterladen.

Der Sicherheitsanalyst kann über die Registerkarte Überprüfung nach Incidents auf die Berichte zugreifen.

Prozedur

1. Navigieren Sie zu dem Security Incident im Überprüfungsstatus.
2. Klicken Sie auf die Registerkarte **Überprüfung nach Incident**.
3. Wenn sich der Security Incident im Status **Überprüfen** befindet:
   Berichtsvorlage:
   - Standardmäßig wird die primäre Berichtsvorlage, die auf der Setupseite konfiguriert wurde, auf den Security Incident angewendet und steht zum Herunterladen zur Verfügung.
   - Analysten können andere Berichte aus der Dropdown-Liste auswählen, um den Bericht zu konfigurieren und herunterzuladen.
4. **Konfigurieren/in Vorschau anzeigen:**

   Ein Sicherheitsanalyst kann eine Vorschau der Berichtsvorlagenkonfiguration anzeigen und diese ändern. In der aktuellen Konfiguration kann der Sicherheitsanalyst nur die Zeitleistenfilter ändern.

   Falls die Konfiguration für den primären Bericht geändert wird, bevor der Security Incident geschlossen wird, wird der Bericht zur Überprüfung nach Incident, der an den Security Incident angehängt ist, entsprechend den vom Sicherheitsanalysten vorgenommenen Änderungen aktualisiert. Nach dem Abschluss kann der Analyst die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration ändern und den Bericht unterwegs herunterladen. Der angehängte Bericht würde jedoch der letzten Konfiguration vor dem Abschluss folgen.

Um den Bericht zu konfigurieren/in Vorschau anzuzeigen, gehen Sie wie folgt vor:

a. Wählen Sie auf der **Registerkarte „Nachfolgeprüfung zum Incident“** in der Dropdown-Liste „Berichtsvorlage“ die gewünschte Berichtsvorlage aus.

b. Klicken Sie auf die Registerkarte **Konfigurieren/Vorschau**.

c. **Aktualisieren** oder konfigurieren Sie die Zeitleistenfilter nach Bedarf.

d. Verwenden Sie das Kontrollkästchen **Bilder anzeigen**, um die Bilder in die Zeitleiste aufzunehmen oder auszuschließen. Wenn diese Option deaktiviert ist, werden nur die Namen der Bilder in die Zeitleiste aufgenommen.

e. Verwenden Sie das Kontrollkästchen **Untergeordnete Aufgaben anzeigen,** um alle dem Security Incident zugeordneten untergeordneten Aufgaben aufzulisten.

5. **Speichern Sie** die Konfiguration, und klicken Sie auf die Registerkarte **Vorschau**, um eine Vorschau des Berichts anzuzeigen und ihn herunterzuladen.

6. Klicken Sie auf **Herunterladen**, um den Bericht direkt herunterzuladen.

Konfigurieren Sie eine Auslösebedingung für Bewertungen

Definieren Sie Regelbedingungen, und generieren Sie erforderliche und optionale Bewertungen für bestimmte Security Incidents.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Hinweis:

Um die Funktion „Auslöserbedingungen für die Überprüfung nach Incidents“ zu verwenden, müssen Sie ein Upgrade auf Security Incident Response 11.0 durchführen. Vor dem Upgrade müssen Sie alle Anpassungen rückgängig machen, die am Metriktyp der Überprüfung nach Incident und an den Auslöserbedingungen vorgenommen wurden. Darüber hinaus müssen Sie möglicherweise auch die Anpassungen rückgängig machen, die an den Business-Regeln vorgenommen wurden, die für die Überprüfung nach Incident spezifisch sind.

- Abgeschlossene Bewertungen anfordern
- Store-Beauftragter

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Überprüfung nach Incident – Bewertungen-Setup**.

2. Klicken Sie im Abschnitt **für Auslösebedingungen für Bewertungen Konfigurieren** auf **Konfigurieren**.

Hinweis:

Im Formular „Bewertungskonfigurationen“ und im Abschnitt „Bewertungskonfigurationen“ ist das Kontrollkästchen **Bewertungen generieren** standardmäßig aktiviert.

- Wenn Sie das Kontrollkästchen aktivieren, wird für jeden Security Incident eine optionale Bewertung erstellt.
- Wenn Sie das Kontrollkästchen deaktivieren, werden keine Bewertungen generiert. Die Bewertungsregeln werden nicht angezeigt, und Sie können keine Bedingungen für die Security Incidents konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie im Formular „Bewertungskonfigurationen“ im Abschnitt Bedingungen die erforderlichen Informationen an.

   a. Geben Sie im Feld **Name** den Namen der Regel an.

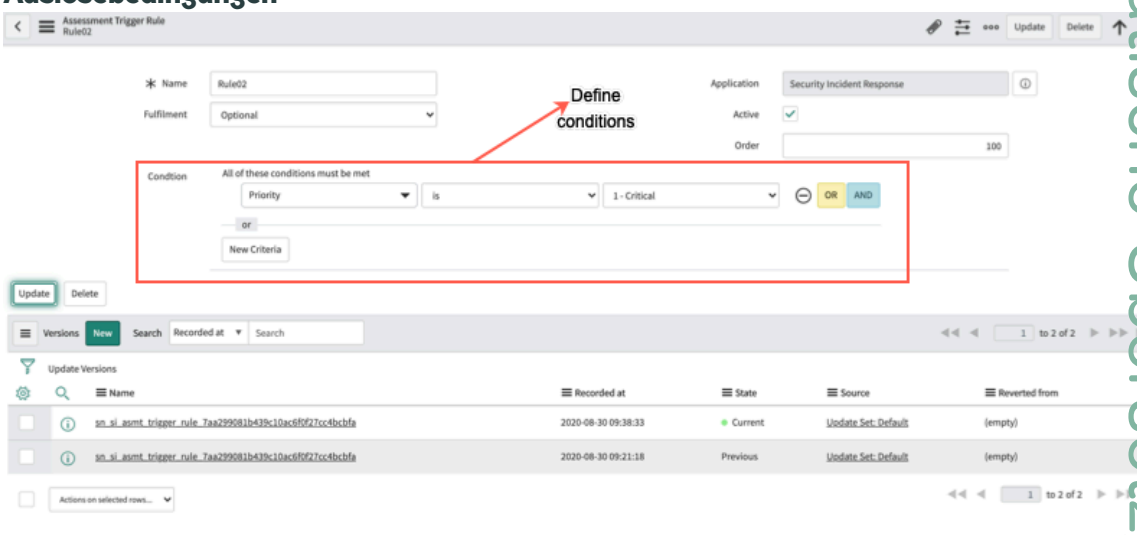
   b. Geben Sie im Feld **Erfüllung** den Erfüllungstyp an.

   c. Um eine Bedingung zu konfigurieren, klicken Sie auf den Regeldatensatz, und definieren Sie Bedingungen im Feld **Bedingung**.

   Hinweis:

   - Wenn Sie eine Regel erstellen, ohne im Feld **Bedingung** eine Bedingung zu definieren, wird die Bedingung als wahr ausgewertet, und die Regel gilt für alle Security Incidents.
   - Sie können eine bestimmte Regel definieren, um die Bewertungen entweder obligatorisch oder optional zu machen. Für die verbleibenden Security Incidents, die nicht den definierten Regeln entsprechen, werden keine Bewertungen generiert.

Auslösebedingungen



Beispiele für Auslösebedingungen für Bewertungen

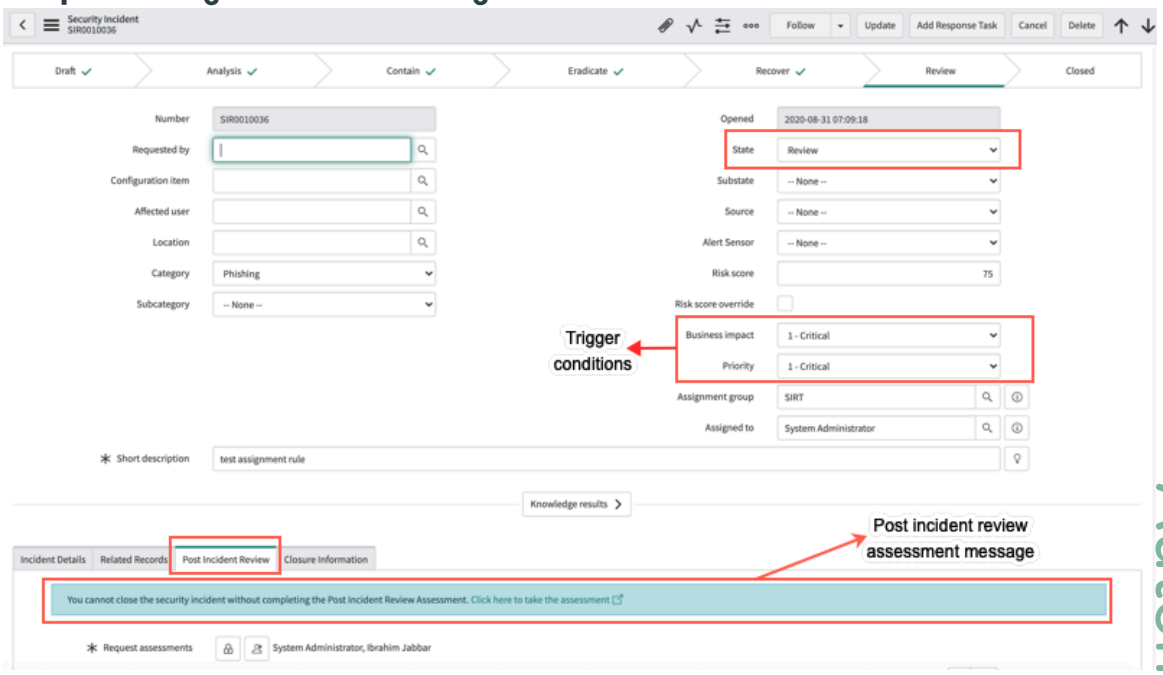
Die folgenden Beispiele zeigen verschiedene Szenarien, wie obligatorische und optionale Auslösebedingungen für Bewertungen generiert werden.

- Generieren Sie im Formular „Auslösebedingung für Bewertungen“ obligatorische Bewertungen, wenn die **Priorität** und **die Geschäftsauswirkung** für einen Security Incident auf der Seite **„Bewertungsauslöserregel“** auf **„Kritisch“** festgelegt sind. In einem solchen Szenario können die Sicherheitsanalysten den Incident erst schließen, wenn die obligatorischen Bewertungen abgeschlossen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für obligatorische Bewertung



- Wie Sie in diesem Beispiel sehen können, können Sicherheitsanalysten bei einem Security Incident mit dem Status **Überprüfen** den Security Incident nicht schließen, ohne die **Bewertung der Überprüfung nach Incident**abzuschließen. Es ist ein Bewertungslink verfügbar, um die Bewertung an die Sicherheitsanalysten zu übergeben, die dem Incident zugewiesen sind (oder die die Bewertung angefordert haben).
- Generieren Sie im Formular „Auslösebedingung für Bewertungen“ optionale Bewertungen, wenn die **Priorität** und **die Geschäftsauswirkung** für einen Security Incident auf **Hoch**festgelegt sind. Wenn in diesem Beispiel die Sicherheitsanalysten die Bewertungen nicht abschließen und den Security Incident nicht schließen, werden die Bewertungen automatisch abgebrochen.
- Falls die obligatorischen oder optionalen Bewertungen nicht mit dem Security Incident übereinstimmen, werden für diese Security Incidents keine Bewertungen generiert. Ein Sicherheitsanalyst kann den Security Incident schließen, ohne die Bewertung der Überprüfung nach Incident abzuschließen.

Führen Sie eine fragebogenbasierte Überprüfung nach Incident durch

Sie können entscheiden, dass eine Überprüfung des Security Incident nach dem Incident gerechtfertigt ist. Eine Überprüfung nach Incident beschreibt, was passiert ist, hilft bei der Bestimmung, warum der Incident aufgetreten ist, und identifiziert, wie er in Zukunft vermieden oder behandelt werden kann.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.manager, sn_si.analyst

Hinweis:

Jeder Benutzer kann unabhängig von seiner Rolle an einem Fragebogen zur Überprüfung nach Incident teilnehmen. Einer Überprüfung können Rollen zugewiesen werden.

Warum und wann dieser Vorgang ausgeführt wird

Die Anwendung ServiceNow Security Incident Response kann die Erfassung von Informationen zur Überprüfung nach Incident von allen Personen automatisieren, die an einem Security Incident beteiligt sind, indem Fragebogen verwendet werden. Wenn Sie sich für die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwendung eines Fragebogens als Teil einer Überprüfung nach Incident entscheiden, wird eine Liste mit Fragen, die für den Security Incident relevant sind, an die anwenderdefinierte Teilnehmerliste gesendet. Wenn ein Benutzer den Fragebogen ausfüllt, wird automatisch ein Nachfolgebericht zum Incident generiert. Der Bericht fasst alle Informationen im Zusammenhang mit dem Security Incident sowie alle Antworten zusammen, die bei der Überprüfung nach dem Incident enthalten sind.

Eine erste Liste von Fragen wird zwar mit dem Basissystem bereitgestellt, ist jedoch anpassbar. Sie können Kategorien erstellen und ihnen neue Fragen hinzufügen oder einzelne Fragen innerhalb vorhandener Kategorien ändern. Sie können Fragen basierend auf Rollen stellen. Sie können definieren, wann bestimmte Fragen gestellt werden. Es gibt Fragen, die Sie beispielsweise nur für Ihre UNIX-Server oder nur bei kriminellen Aktivitäten stellen. Sie können Fragen definieren, die abhängig von der Antwort auf eine andere Frage oder vom Wert in einem Feld im Formular gestellt werden. Es kann sogar Fragen geben, die vollständig durch Abfragen der Datenbank gefüllt werden.

Nachdem der Security Incident gelöst und in den Status **Überprüfen** versetzt wurde, werden Bewertungen für alle zugewiesenen Benutzer und Benutzer generiert, die direkt aus der Liste **Bewertungen anfordern** hinzugefügt wurden.

Der Fragebogen kann ein hilfreiches Tool sein, um Informationen über die Behandlung des Security Incident aus verschiedenen Quellen zu sammeln.

Während der Überprüfung können Sie der Liste weitere Anwender hinzufügen oder vorhandene Anwender aus der Liste entfernen, es sei denn, sie haben bereits mit dem Ausfüllen des Fragebogens begonnen. Wenn Sie der Liste neue Benutzer hinzufügen, erhalten sie die Fragen, wenn der Datensatz gespeichert wird. Der Security Incident kann erst geschlossen werden, wenn alle Fragebogen ausgefüllt wurden. Sobald Fragebögen von den einzelnen Benutzern ausgefüllt werden, wird der Nachfolgebericht zum Incident automatisch generiert (und erneut generiert) und auf der **Registerkarte Überprüfung nach Incident** angezeigt.

So starten Sie eine Überprüfung nach Incident:

Prozedur

1. Erstellen Sie einen Security Incident, oder öffnen Sie einen vorhandenen, indem Sie zu navigieren **Security Incident** > **Incidents** > **Mir zugewiesen (oder „An Team zugewiesen“ oder „Nicht zugewiesene Incidents“)**.
2. Klicken Sie auf die Registerkarte **Überprüfung nach Incident**.
3. Das Feld **Bewertungen anfordern** enthält standardmäßig die Person im Feld **Zugewiesen** an. Klicken Sie auf das Schlosssymbol, um weitere Anwender zur Überprüfungsliste hinzuzufügen. Nachdem das Feld entsperrt wurde, stehen Optionen zum Hinzufügen oder Entfernen mehrerer Benutzer und Rollen oder zum Eingeben von Benutzer-E-Mail-Adressen zur Verfügung.
4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf das Schlosssymbol, um das Feld zu sperren.

   Hinweis:
   Sie können auch Bedingungen definieren, die bei Erfüllung in einem Security Incident dazu führen können, dass bestimmte Benutzer automatisch dem Feld **Bewertungen anfordern** für diesen Security Incident hinzugefügt werden. Wenn beispielsweise die **Kategorie** eines Security Incidents in **Phishing**geändert wird, können bestimmte Personen, die über Erfahrung mit Phishing-Bedrohungen verfügen, der Liste der Überprüfungen nach Incidents hinzugefügt werden. Weitere Informationen finden Sie unter Erstellen Sie PIR-Zuweisungsregeln.

5. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Incident in den Status **Überprüfen** übergeht (oder sofort, wenn er sich bereits im Status **Überprüfen** befindet), erhält jeder Benutzer in der Überprüfungsliste eine erste E-Mail-Benachrichtigung . Wenn das Fälligkeitsdatum näher rückt, werden Erinnerungen gesendet. Wenn ein Benutzer über den E-Mail-Link oder über den Fragebogen zugreift **Überprüfung nach Incident** > **Meine ausstehenden Überprüfungen**, werden die angezeigten Fragen aus allen Kategorien ausgewählt, die auf diesen Security Incident passen. Wenn neue Benutzer vor dem Fälligkeitsdatum zur Überprüfungsliste hinzugefügt werden, erhalten sie Benachrichtigungen, wenn der Security Incident gespeichert wird.

Wenn Benutzer ihre Fragebögen ausfüllen, werden im Nachfolgebericht zum Incident die entsprechenden Daten zusammengestellt und auf der Registerkarte **„Nachfolgeprüfung zum Incident“** angezeigt. Die Fragebogendaten werden auf der Registerkarte **Ergebnisse** angezeigt.

Erstellen Sie Kategorien für Fragebogen zur Überprüfung nach Incidents

Sie können die im Basissystem enthaltenen Fragebogenkategorien verwenden oder eigene Kategorien erstellen.

Vorbereitungen
Erforderliche Rolle: sn.si_admin

Warum und wann dieser Vorgang ausgeführt wird
So erstellen Sie eine neue Kategorie von Fragen:

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Überprüfung nach Incident**.
2. Klicken Sie **auf Fragen überprüfen**.
   Eine Liste der Kategorien wird angezeigt, zusammen mit ihrer Reihenfolge und den Filtern, die definieren, unter welchen Bedingungen die Fragen gestellt werden (z. B. nur, wenn die Kategorie des Security Incidents `Kriminelle Aktivität`lautet). Jede Kategorie ist ein Abschnitt im Fragebogen zur Überprüfung nach Incident, und die Fragen in jeder Kategorie sind nur enthalten, wenn der Security Incident dem Bedingungsfilter entspricht. Beispielsweise würden Sie für eine Kategorie von Fragen, die nur Linux-Server betreffen, einen Filter einrichten, der Security Incidents auswählt, bei denen der betroffene Ressourcentyp Linux-Server ist. In dieser Kategorie würden Sie dann alle Fragen erstellen, die erforderlich sind, wenn sich ein Security Incident auf einem Linux-Server befindet. Sie verwenden eine der im Basissystem bereitgestellten Kategorien oder erstellen eine neue Kategorie. Dieses Verfahren geht davon aus, dass Sie eine neue Kategorie erstellen möchten, bevor Sie Fragen definieren.
3. Klicken Sie in der Liste der Kategorien **auf Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Security Incident

Feld	Beschreibung
Name	Name für die Kategorie, die im Fragebogen zum Security Incident angezeigt wird.
Typ	Überprüfung nach Incident ist der Standard.
Stakeholder erstellen	Nicht verwendet von Security Incident Response.
Tabelle	Dieses Feld wird automatisch zugewiesen, sobald das Formular übermittelt wird.
Filter	Geben Sie die Bedingung ein, die bestimmt, wann Fragen in dieser Kategorie verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn ein Security Incident-Datensatz diesem Filter entspricht, werden die Fragen in eine Überprüfung nach Incident für diesen Security Incident aufgenommen. Filter können alle Daten im Datensatz oder in anderen mit diesem Datensatz verknüpften Datensätzen verwenden. Zum Beispiel die Abteilung des Managers des anfordernden Benutzers.
Anwendung	Bereichsanwendung für den Incident.
Gewichtung	Numerischer Wert, der die Bedeutung dieser Metrik im Vergleich zu anderen Metriken in derselben Kategorie darstellt. Standardmäßig beträgt die Gewichtung 10.
Gesamtmetriken	Anzahl der von der Kategorie verwendeten Metriken.
Beschreibung	Beschreibung des Fragebogens.

5. Klicken Sie auf **Senden**, um die Kategorie zu speichern.

Verfassen Sie Fragen zur Überprüfung nach Incident

Sie können die im Basissystem enthaltenen Fragen verwenden oder eigene Fragen erstellen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die Methoden zum Sammeln von Informationen zur Überprüfung nach Incidents können in Form von Fragen oder in Form von Daten erfolgen, die automatisch mithilfe von Skripts erfasst werden.

Fragen können von den Antworten auf andere Fragen abhängen. Sie können beispielsweise fragen, ob alle erforderlichen Protokolle verfügbar waren. Wenn die Antwort „Nein“ lautet, stellen Sie eine Folgefrage, um sicherzustellen, welche der erforderlichen Protokolle nicht aktiviert wurden.

Bei der Skriptdatenerfassung, auch als Skriptmetriken bezeichnet, werden Daten im Zusammenhang mit dem Security Incident über von Ihnen geschriebene Skripts erfasst. Diese Aktion kann weit über die Daten im Security Incident-Datensatz selbst hinausgehen. Beispielsweise könnte eine Skriptmetrik die letzte Ausfallzeit für einen von diesem Security Incident betroffenen Server erfassen.

Schließlich können Sie die beiden Typen kombinieren. Fragen können Standardwerte enthalten, die aus einem Skript oder einfach aus einem Feld im Security Incident-Datensatz übernommen werden. Wenn Sie den Fragetyp Standardantwort von verwenden, können Sie auswählen, ob der Benutzer die Frage immer beantworten soll – wobei der Standardwert einen Anfangswert bereitstellt – oder ob dem Benutzer die Frage nur gestellt werden soll, wenn Skript oder Feld ist leer.

So erstellen Sie eine neue Frage:

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Überprüfung nach Incident**.
2. Klicken Sie auf die Kategorie, für die Sie eine neue Frage erstellen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die Registerkarte **Bewertungsmetriken**.
4. Klicken Sie auf **Neu**.
   Sie können auch auf eine vorhandene Frage klicken, um sie zu ändern.
5. Füllen Sie die entsprechenden Felder im Formular aus.

Metrikformular

Feld	Beschreibung
Name	Name der Metrik (Frage oder Skript) Handelt es sich bei der Metrik um eine geskriptete Datensammlung, wird dieser Name im Nachfolgebericht zum Incident angezeigt.
Kategorie	Die Kategorie, zu der die Metrik gehört. Das System füllt diese Kategorie automatisch auf, wenn Sie eine neue Metrik aus dem Formular „Metrikkategorie“ erstellen. **Hinweis:** Sie können die Kategorie nicht ändern, wenn das Feld **Abhängig von** gesetzt ist oder eine andere Metrik von dieser Metrik abhängt.
Methode	Gibt den Typ der Metrik wie folgt an: ○ *Assessment*: Eine Frage ohne Standardwert. Es gibt verschiedene Datentypen, die im Feld **„Datentyp“** auf der Registerkarte **„Feldtyp“** definiert werden können, z. B. Kontrollkästchen, Auswahllisten und Texteingaben. ○ *Script*: Geskriptete Metrik. Erhält Werte durch Schreiben eines benutzerdefinierten Skripts. Die Methode *Script* ist mit den Datentypen **Dauer**, **Anzahl**und **Prozentsatz** kompatibel. ○ *Default answer from field*: Eine Frage, bei der die Standardantwort aus einem ausgewählten Feld im Security Incident stammt. Wenn Sie diese Option auswählen, werden der Registerkarte **Allgemein** zwei Felder hinzugefügt: ▪ *Default answer*: Wählen Sie das Feld im Security Incident aus, das die Standardantwort für die Frage enthält. Für die Frage „Wer hat diesen Incident ursprünglich gemeldet?“ ist das Feld **Angefordert** von eine wahrscheinliche Auswahlmöglichkeit. ▪ *Ask question*: Gibt an, wann die Frage gestellt werden soll: immer oder nur, wenn das Feld **Standardantwort** leer ist. Im obigen Beispiel würde die Frage gestellt, wenn das Feld **Angefordert von** leer ist. ○ *Default answer from script*: Eine Frage, bei der die Standardantwort aus einem Skript stammt. Die Antwort kann eine Zahl, eine Zeichenfolge oder ein Prozentsatz sein. Auf der Registerkarte **Allgemein** wird ein Feld hinzugefügt: *Ask question*: als Gibt an, wann die Frage gestellt wird: immer oder nur, wenn das Skript keine Standardantwort bereitstellt. Das Skript wird in der Registerkarte **Feldtyp** definiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn Sie einen **Datentyp** auswählen, der mit der ausgewählten **Methode**nicht kompatibel ist, ändert das System die **Methode** automatisch in einen kompatiblen Wert.
Gewichtung	[Erforderlich] Numerischer Wert, der die Bedeutung dieser Metrik im Vergleich zu anderen Metriken in derselben Kategorie darstellt. Standardmäßig beträgt die Gewichtung 10. Dieses Feld ist sichtbar und erforderlich, es sein denn der **Datentyp** ist **Datum**, **Datum/Zeit** oder **Zeichenfolge**. Diese Datentypen werden nicht in die Ergebnisberechnungen einbezogen.
Bestellung	[Erforderlich] Numerischer Wert, der die Reihenfolge der Metrikfrage in Bewertungsfragebögen in Relation zu anderen Metrikfragen in derselben Kategorie bestimmt. Die Metrik mit dem kleinsten Wert für die Reihenfolge erscheint als erste Frage im Kategoriebereich. Standardmäßig ist die Reihenfolge 100. **Hinweis:** Es spielt keine Rolle, welchen Wert für die Reihenfolge Sie für Metriken mit der Skriptmethode verwenden, da sie nicht in Fragebögen angezeigt werden.
Aktiv	Checkbox, die bestimmt, ob diese Metrik verwendet wird. Wenn das Kontrollkästchen nicht aktiviert ist, ist der Metrikdatensatz nicht vorhanden.
Obligatorisch	Checkbox, die die Metrikfrage für Bewertungsfragebogen obligatorisch (ausgewählt) oder optional (deaktiviert) macht. Benutzer können Fragebögen erst einreichen, wenn sie gültige Antworten auf alle obligatorischen Fragen geben, die durch eine rote Feldstatusanzeige gekennzeichnet sind. Dieses Feld ist nur sichtbar, wenn das Feld **Abhängig** von leer ist und der Datentyp nicht **Kontrollkästchen**ist.

6. Klicken Sie auf die Registerkarte **Allgemein**, und füllen Sie die Felder entsprechend aus.

Registerkarte „Allgemein“

Feld	Beschreibung
Frage	Text, der als Frage in Fragebogen zur Überprüfung von Security Incidents verwendet werden soll. Geben Sie eine klare, einfache Frage ein, die leicht zu beantworten ist, z. B. **Wie haben wir den Incident eingedämmt?**
Beschreibung	Informationen zur Metrik und deren Auswertung. Wenn *Method***Bewertung**ist, fügen Sie Details hinzu, damit Benutzer verstehen, wie die Frage beantwortet wird. Dieser Text wird als Hinweis angezeigt, wenn ein Benutzer auf den Fragentext im Fragebogen verweist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Abhängig von und Angezeigt wenn	Wählen Sie im Feld **Abhängig von** eine Frage aus, von der die aktuelle Frage abhängt. Beispiel: Die Frage „Welche zusätzlichen Protokolle wurden benötigt?“ hängt von der Frage „Waren alle benötigten Protokolle verfügbar?“ ab. Verwenden Sie als Nächstes das Feld **Angezeigt wenn**, um anzugeben, wann die abhängige Frage in Fragebogen angezeigt werden soll. Beispiel: Wenn die abhängige Frage nur gestellt werden soll, wenn der Benutzer die Frage „Waren alle benötigten Protokolle verfügbar?“ mit „ **Nein** “ antwortet. Frage zu beantworten im Feld **Angezeigt wenn** die Option **Nein**. **Hinweis:** Das System verhindert die Erstellung rekursiver Abhängigkeiten zwischen Metriken. Wenn beispielsweise Metrik A von Metrik B abhängt, kann Metrik B nicht von Metrik A abhängen.

7. Klicken Sie auf die Registerkarte **Feldtyp**, und füllen Sie die Felder entsprechend aus.

Registerkarte „Feldtyp“.

Feld	Beschreibung
Datentyp	Der Datentyp der erwarteten Antwort, von dem die Liste der verfügbaren Typen für die ausgewählte Methode abhängt. Wenn die Methode **Bewertung** ist, bestimmt der Datentyp, wie Benutzer die entsprechende Frage in Fragebögen beantworten. Wenn die Methode **Skript** ist, bestimmt der Datentyp, wie das System die Bewertungsergebnisse berechnet. **Hinweis:** Wenn eine andere Metrik von dieser Metrik abhängt, kann der Datentyp nicht geändert werden.
Antworten zufällig	Checkbox, die bestimmt, ob die Antwortoptionen für diese Metrikfrage jedes Mal in zufälliger Reihenfolge angezeigt werden, wenn ein Anwender einen Bewertungsfragebogen öffnet, der die Frage enthält. Die Antworteinstellung kann durch die Reihenfolge beeinflusst werden, in der Antwortoptionen angezeigt werden. Dies kann zu verzerrten Ergebnissen führen. Durch Randomisieren von Antwortmöglichkeiten kann diese Verzerrung vermieden werden. Dieses Feld ist nur sichtbar, wenn Sie **Likert-Skala** oder **Auswahl** im Feld **Datentyp** auswählen.
Abhängiges Plugin	[Erforderlich, wenn *Method* **Skript** ist.] Plugin, das die im Skript abgefragten Tabellen enthält. Das System führt das Metrikskript nur dann aus, wenn das Plugin aktiv ist. Die standardmäßig verfügbaren Werte sind **Asset Management**, **CMDB**, **Kern**, **Cost Management**, **Procurement** und **Software Asset Management**. Dieses Feld ist nur sichtbar, wenn *Method* auf **Skript festgelegt** ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Wenn der Standardwert „Core“ verwendet wird, wird das Skript immer ausgeführt. ○ Wenn Sie Administrator sind, können Sie dem Feld weitere Plugins hinzufügen.
Skaladefinition	Eine Einstellung, die bestimmt, ob kleinere oder größere numerische Werte einer guten Bewertung bei den Bewertungsergebnisberechnungen entsprechen. Wählen Sie **Niedrig** aus, wenn niedrigere numerische Werte besser sind, z. B. für eine Metrik, die die Anzahl der Fehler für einen Lieferanten misst. Wählen Sie **Hoch**, wenn größere numerische Werte besser sind, z. B. für eine Metrik, die die Benutzerzufriedenheit auf einer Skala von eins bis fünf misst. Der Standardwert ist **Hoch**. Dieses Feld ist sichtbar und erforderlich, es sei denn, *Data type* ist **Datum**, **Datum/Uhrzeit**oder **Zeichenfolge**. Die Ergebnisse für diese Datentypen werden nicht in die Ergebnisberechnungen einbezogen.
Min.	Niedrigster numerischer Wert, der als Antwortoption bei Assessments oder als skalierter Wert in einer Skriptmetrik verwendet werden soll. Dieses Feld ist nur sichtbar und nur erforderlich, wenn bestimmte Datentypen ausgewählt sind. Wenn der Datentyp **Auswahl-** oder **Likert-Skala**ist, ist dieses Feld schreibgeschützt und wird automatisch basierend auf der kleinsten Metrikdefinition *Value*festgelegt.
Max.	Höchster numerischer Wert, der als Antwortoption oder skalierter Wert verwendet werden soll. Dieses Feld ist nur sichtbar und nur erforderlich, wenn bestimmte Datentypen ausgewählt sind. Wenn der Datentyp **Auswahl-** oder **Likert-Skala**ist, ist dieses Feld schreibgeschützt und wird automatisch basierend auf der größten Metrikdefinition *Value*festgelegt.
Skript	Skript, das die gewünschten Systeminformationen abruft. Das Skript hat eine Eingabevariable, die mit der ID des Security Incidents (primär) festgelegt wird, und drei mögliche Ausgabevariablen, die vom Skript festgelegt werden: „string_result“, „scaled_result“ und „actual_result“. Wenn der Datentyp Zeichenfolge ist, ist nur „string_result“ erforderlich. Dieses Feld ist sichtbar und erforderlich, wenn *Method* auf **Skript festgelegt**ist oder der Standardwert aus einem Skript stammt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vorlage	Ein vordefinierter Satz allgemeiner Antworten, die für die Frage verwendet werden sollen. Beispielsweise würde eine Häufigkeitsvorlage wahrscheinlich mit dem Wert „Nie“ beginnen und bis zum obersten Wert „Immer“ hochsteigen. Dieses Feld ist nur sichtbar und erforderlich, wenn *Data type* den **Wert Vorlage**hat. **Hinweis:** Wenn eine andere Metrik von dieser Metrik abhängt, kann die Vorlage nicht geändert werden.

8. **Wahlweise:** Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf **Aktualisieren**.

Erstellen Sie PIR-Zuweisungsregeln

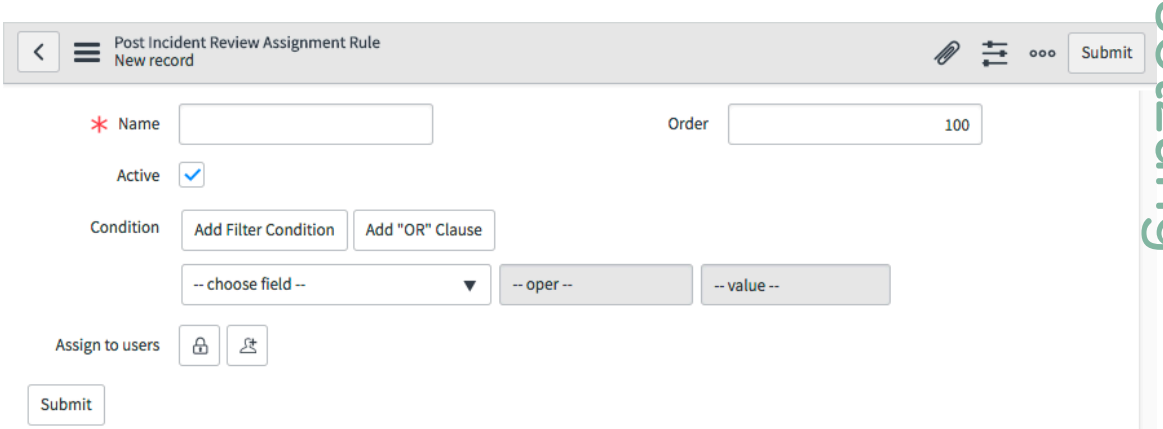
Zusätzlich zum manuellen Hinzufügen von Benutzern zur Bewertungsliste für die Überprüfung nach Incident für einen Security Incident können Sie Zuweisungsregeln für das automatische Hinzufügen von Benutzern zur Liste definieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.manager, sn_si.analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Überprüfung nach Incident – Bewertungen-Setup**.
2. Führen Sie einen Drilldown zum Abschnitt **„Benutzerzuweisungsregeln“** durch.
3. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie auf **Neu**.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Zuweisungsregel.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Regel zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

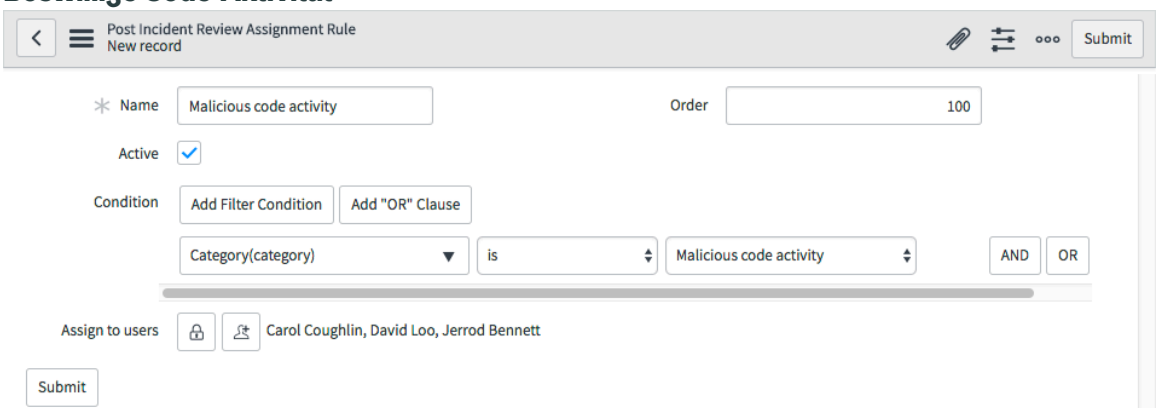
Feld	Beschreibung
Bestellung	Geben Sie einen numerischen Wert ein, um anzugeben, wo in der Liste der Zuweisungsregeln diese Regel angezeigt werden soll. Niedrigere Zahlen erscheinen oben in der Liste. **Hinweis:** Nur die erste übereinstimmende Zuweisungsregel wird ausgeführt, und nur die in dieser Regel definierten Benutzer werden der Bewertungsliste hinzugefügt.
Bedingung	Verwenden Sie den Bedingungsgenerator , um die Bedingungen zu definieren, die im Security Incident erfüllt sein müssen, damit diese Regel ausgeführt wird. Weitere Informationen finden Sie im folgenden Beispiel.
Zu Anwendern zuweisen	Klicken Sie auf das Schlosssymbol, um der Überprüfungsliste Anwender hinzuzufügen. Nachdem das Feld entsperrt wurde, stehen Optionen zum Hinzufügen oder Entfernen mehrerer Benutzer und Rollen oder zum Eingeben von Benutzer-E-Mail-Adressen zur Verfügung.

6. Klicken Sie auf **Absenden**.

Example: Böswillige Code-Aktivität

In der hier gezeigten Zuweisungsregel zur Überprüfung nach Incidents werden die drei identifizierten Benutzer (die zufällig Experten im Umgang mit Schadcodeaktivitäten sind) hinzugefügt, wenn ein Security Incident, bei dem das Feld **Kategorie** auf **Böswillige Code-Aktivität** festgelegt ist, in den Status „ **Überprüfen** “ übergeht Liste der Anwender, die den Fragebogen zur Überprüfung nach Incident für diesen Security Incident erhalten.

Böswillige Code-Aktivität



Schließen Sie Security Incidents

Wenn ein Security Incident in den Status Überprüfen übergegangen ist, können Sie ihn schließen und einen entsprechenden Abschlusscode eingeben. Abschlusscodes können später gesucht werden, um die Lokalisierung zu erleichtern.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:

In früheren Versionen von Security Incident Responsekonnten Benutzer Security Incidents oder Anforderungen als Spam schließen. Im Release Istanbul ist die Spam-Option nicht mehr verfügbar. Security Incidents oder Spam-Anforderungen können je nach Bedarf abgebrochen oder gelöscht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn der Security Incident, den Sie schließen möchten, noch nicht geöffnet ist, navigieren Sie zu **Security Incident** > **Incidents** > **Alle Incidents anzeigen**, und suchen Sie den Security Incident, den Sie schließen möchten.

   Hinweis:
   Wenn für diesen Security Incident Bewertungen der Überprüfung nach Incident vorhanden sind, die für diesen Security Incident noch nicht abgeschlossen wurden, kann der Security Incident nicht geschlossen werden. Zurück zu **Security Incident** > **Überprüfung nach Incident** > **Alle unvollständigen Überprüfungen**, suchen Sie die unvollständigen Überprüfungen, und bitten Sie die Überprüfer, ihre Überprüfungen abzuschließen oder die verbleibenden Bewertungen abzubrechen.

2. Klicken Sie auf die Registerkarte **Abschlussinformationen**, und füllen Sie die Felder entsprechend aus.

   Security Incident

Feld	Beschreibung
Wissensartikel erstellen	Wählen Sie dieses Feld aus, um automatisch einen Entwurf eines Knowledge Base-Artikels zu erstellen, der den Inhalt der Überprüfung nach Incident enthält.
Abschlusscode	Wählen Sie den Lösungscode aus, der den Grund für das Schließen dieses Security Incidents am besten beschreibt. ○ Untersuchung abgeschlossen ○ Bedrohung gemindert ○ Schwachstelle gepatcht ○ Ungültige Schwachstelle ○ Nicht behandelt ○ Falsch positiv
Geschlossen von	Zeigt den Benutzer an, der den Security Incident geschlossen hat, nachdem der Datensatz aktualisiert wurde.
Abgeschlossen	Zeigt Datum und Uhrzeit des Abschlusses an, nachdem der Datensatz aktualisiert wurde.
Abschlussnotizen	Geben Sie zusätzliche Notizen ein, die das Ergebnis des Schließens dieses Security Incidents beschreiben.

3. Klicken Sie auf **Aktualisieren**.

4. Der zugewiesene Benutzer kann den **Status** manuell in **Geschlossen**ändern.
   Wenn ein übergeordneter Incident geschlossen wird, werden alle Antwortaufgaben, die zu dem untergeordneten Incident gehören, abgebrochen. Wenn keine anderen Aufgabentypen vorhanden sind, wird der untergeordnete Incident ebenfalls geschlossen.

Fügen Sie einem Security Incident Abschlussinformationen hinzu

Wenn sich ein Security Incident im Status „Überprüfung“ oder „Geschlossen“ befindet, können Sie Abschlussinformationen eingeben.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf die Registerkarte **Zugehörige Datensätze**.
3. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Wissensartikel erstellen	Aktivieren Sie dieses Kontrollkästchen, um einen Wissensartikel mit dem Inhalt des Nachfolgeberichts zum Incident zu generieren.
Abschlusscode	Wählen Sie den Abschlusscode aus, der den Grund für das Schließen des Security Incidents am besten beschreibt.
Geschlossen von	[Schreibgeschützt] Zeigt den Benutzer an, der den Security Incident geschlossen hat.
Abgeschlossen	[Schreibgeschützt] Zeigt das Datum und die Uhrzeit des Schließens des Security Incidents an.
Abschlussnotizen	Wie der Security Incident geschlossen wurde, einschließlich gelernter Lektionen, Lösung usw.

4. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:
   - Incident-Details
   - Überprüfung nach Incident
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Beschränken Sie den Zugriff auf Security Incidents

Verwalten Sie den Zugriff auf Security Incidents, die vertrauliche Informationen enthalten. Sie können Einschränkungen für Security Incidents erzwingen, um zu bestimmen, wer auf einen bestimmten Incident zugreifen kann, und den Zugriff auf bestimmte Benutzer oder Gruppen zu beschränken.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Mit Einschränkungen für Security Incidents können Sie verhindern, dass andere Benutzer in einer bestimmten Organisation auf kritische Security Incidents zugreifen. Mit diesen Einschränkungen können Sie die Security Incidents, auf die ein Benutzer zugreifen kann, präziser steuern. Sie können eine Einschränkung für Security Incidents erzwingen, indem Sie das Kontrollkästchen **Einschränkung erzwingen** aktivieren und dann die Benutzer oder Gruppen auswählen, die auf den jeweiligen Security Incident zugreifen dürfen.

Nachdem Sie die Einschränkung für bestimmte Security Incidents erzwungen und den Zugriff auf bestimmte Anwender oder Gruppen beschränkt haben, können alle anderen verbleibenden Anwender in Ihrer Organisation nicht auf diese Security Incidents zugreifen, selbst wenn sie nach einem bestimmten eingeschränkten Security Incident suchen.

Prozedur

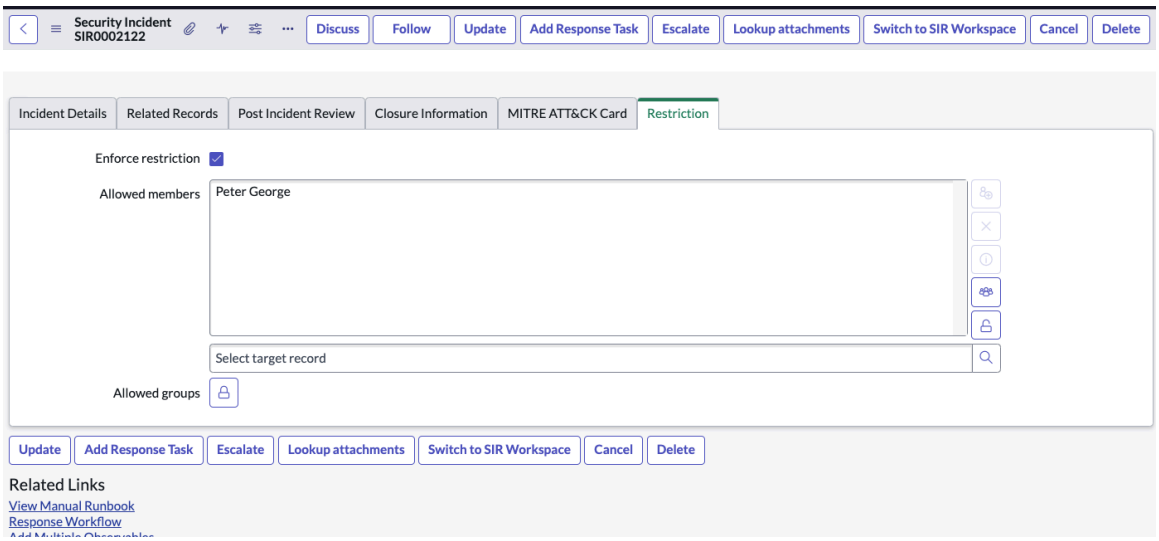
1. Öffnen Sie einen Security Incident, den Sie einschränken möchten.
2. Wenn Sie die klassische Anwenderoberfläche verwenden, gehen Sie wie folgt vor:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf die Registerkarte **Einschränkung**.

b. Aktivieren Sie das Kontrollkästchen **Einschränkung erzwingen**, um die Einschränkung des Security Incident zu aktivieren.



c. Klicken Sie im Feld Zulässige Mitglieder auf das , um die Benutzer auszuwählen, die auf den Security Incident zugreifen können.

d. Wählen Sie das Symbol , um sich selbst als zulässigen Benutzer hinzuzufügen.

e. Wählen Sie das Symbol um Anwender hinzuzufügen oder zu entfernen.

f. Klicken Sie im Feld Zulässige Gruppen auf das , um die Gruppen auszuwählen, die auf den Security Incident zugreifen können.

g. Wählen Sie das Symbol um Gruppen hinzuzufügen oder zu entfernen.

> **Hinweis:**
> Wenn das Kontrollkästchen **Einschränkung** erzwingen für den Security Incident aktiviert ist, haben nur sn_si.admin und die zulässigen Mitglieder oder Gruppen Zugriff auf den Security Incident.

h. Klicken Sie auf **Aktualisieren**.

3. Wenn Sie SIR Workspace verwenden, gehen Sie wie folgt vor:

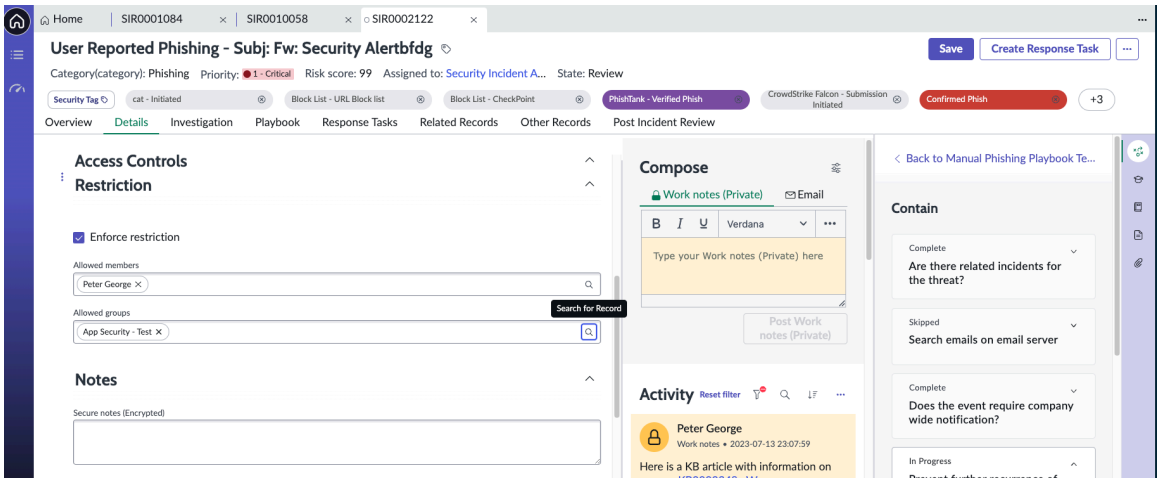
a. Klicken Sie im Security Incident auf die Registerkarte **Details**.

b. Scrollen Sie nach unten, und klicken Sie auf den Abschnitt **Einschränkung**.

c. Aktivieren Sie das Kontrollkästchen **Einschränkung erzwingen**, um die Einschränkung des Security Incident zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Wählen Sie im Feld Zulässige Mitglieder mithilfe der Suchoption die Benutzer aus, die auf den Security Incident zugreifen können.

e. Wählen Sie im Feld Zulässige Gruppen mithilfe der Suchoption die Gruppen aus, die auf den Security Incident zugreifen können.

> **Hinweis:**
> Wenn das Kontrollkästchen **Einschränkung** erzwingen für den Security Incident aktiviert ist, haben nur sn_si.admin und die zulässigen Mitglieder oder Gruppen Zugriff auf den Security Incident.

f. Klicken Sie auf **Speichern**.

Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace

Security Incident Response enthält eine neue Anwenderoberfläche namens Security Analyst Workspace, die leistungsstarke Tools zur Unterstützung bei der Analyse enthält, darunter das Playbook, eine Vorschauansicht und Registerkarten für die Bearbeitung mehrerer Security Incidents.

Die leistungsstarken Tools in Security Analyst Workspace wurden speziell für Sicherheitsanalysten entwickelt und ermöglichen es Ihnen, das ständig größer werdende Datenvolumen im Zusammenhang mit Security Incidents zu analysieren. Automatisierte Aktionen reduzieren die Zeit für die Untersuchung von Security Incidents erheblich, was den Unterschied zwischen dem Stoppen eines Angriffs und dem Auftreten eines Verstoßes ausmachen kann.

Vor der Verwendung von Security Analyst Workspace

Bevor Sie Security Analyst Workspaceverwenden können, müssen Sie sicherstellen, dass auf Ihrer Instanz mindestens London Patch 3 installiert ist und Sie die richtigen Rollen definiert haben hat die Anwendung Security Incident Response UI aus dem heruntergeladen ServiceNow Store.

> **Hinweis:**
> Wenn auf Ihrer Instanz eine Version vor London Patch 3 ausgeführt wird, müssen Sie das Plugin „Security Incident Response UI“ über den HI-Kundenservice anfordern.

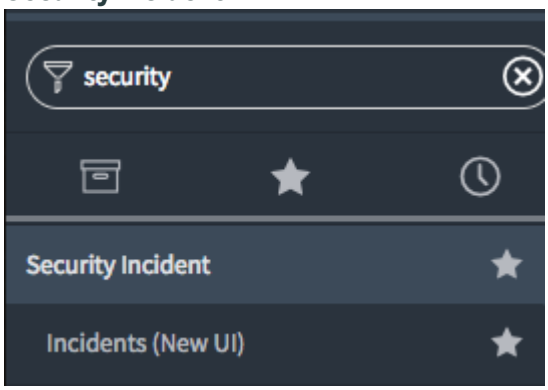
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf Security Analyst Workspace zugreifen

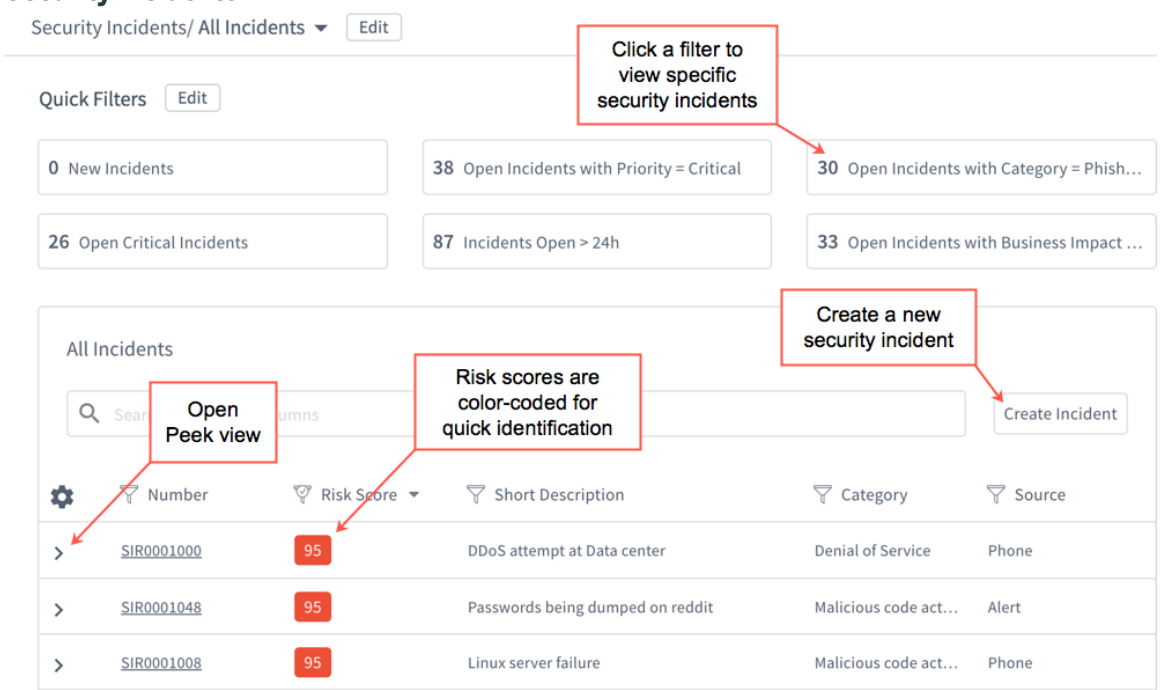
Um auf diesen neuen Arbeitsbereich zuzugreifen, navigieren Sie zu **Security Incident** > **Incidents (neue UI)**.

Security Incident



Der -Arbeitsbereich wird in einer separaten Browser-Registerkarte geöffnet.

Security Incidents

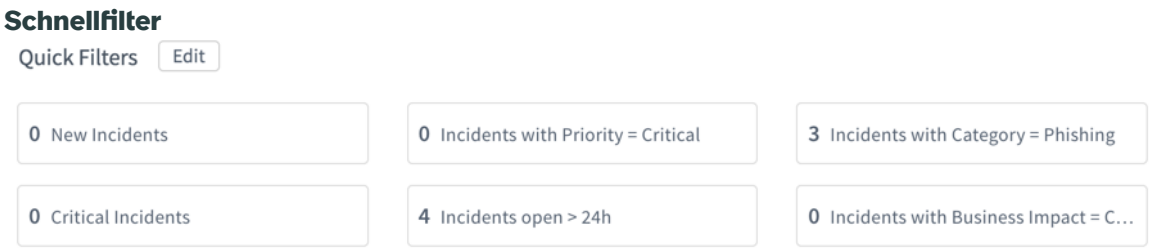


Suchen Sie die Security Incidents, die Sie mit Schnellfiltern analysieren möchten

Security Analyst Workspace bietet mehrere Tools zum Filtern der Liste der Security Incidents, sodass Sie die zu analysierenden Security Incidents schnell finden können. Mit den Schnellfiltern können Sie eine Teilmenge der Security Incidents basierend auf den Kriterien im Filter auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



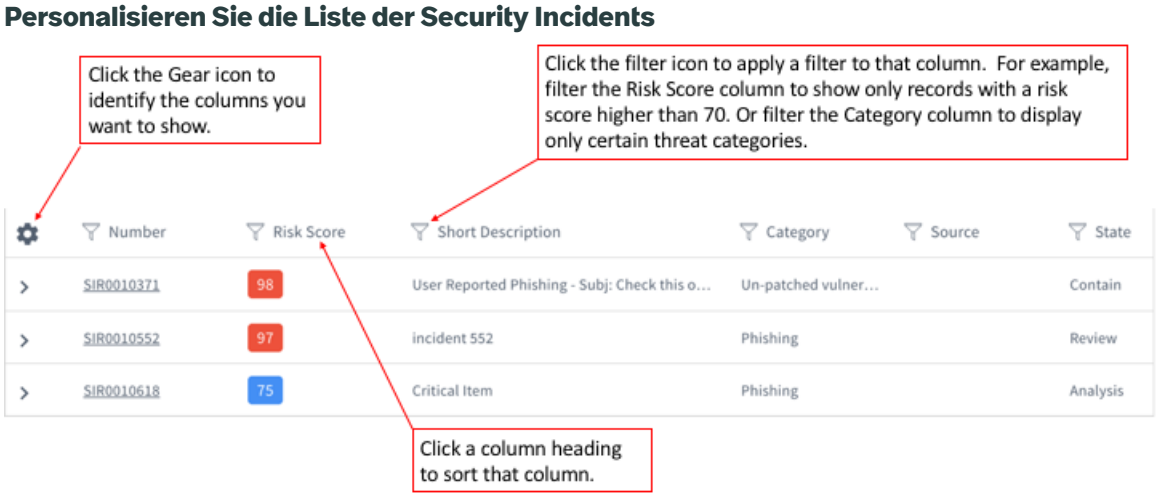
Klicken Sie einfach auf den Schnellfilter, den Sie verwenden möchten.

Hinweis:
Sie können auf eine **Bearbeiten-** Schaltfläche klicken, um anzugeben, welche Schnellfilter auf dem Listenbildschirm angezeigt werden sollen. Es muss mindestens ein Filter ausgewählt werden, maximal sechs.

In der klassischen Umgebung können Sie zusätzliche Schnellfilter sowie primäre Filter für Security Analyst Workspacedefinieren. Weitere Informationen finden Sie unter Richten Sie primäre und sekundäre Filter für ein Security Analyst Workspace.

Personalisieren Sie die Liste der Security Incidents

Wie bei allen Listen in Ihrer Instanz bietet Security Analyst Workspace Tools zum Personalisieren der Liste und zum Sortieren der angezeigten Informationen entsprechend Ihren Analyseanforderungen.

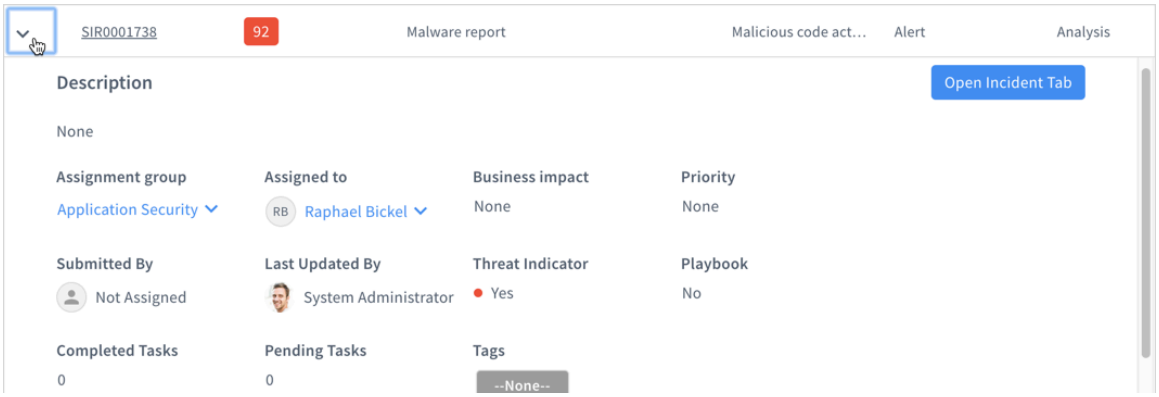


Sparen Sie Zeit mit der Vorschauansicht

Bevor Sie einen Security Incident-Datensatz öffnen, können Sie mithilfe der Vorschauansicht Zeit sparen. Mit dieser Funktion können Sie wichtige Sicherheitsartefakte schnell finden, ohne die gesamte Seite neu laden zu müssen. Klicken Sie einfach links neben der Nummer eines Security Incidents auf das Symbol **>**, um einen Blick darauf zu werfen.

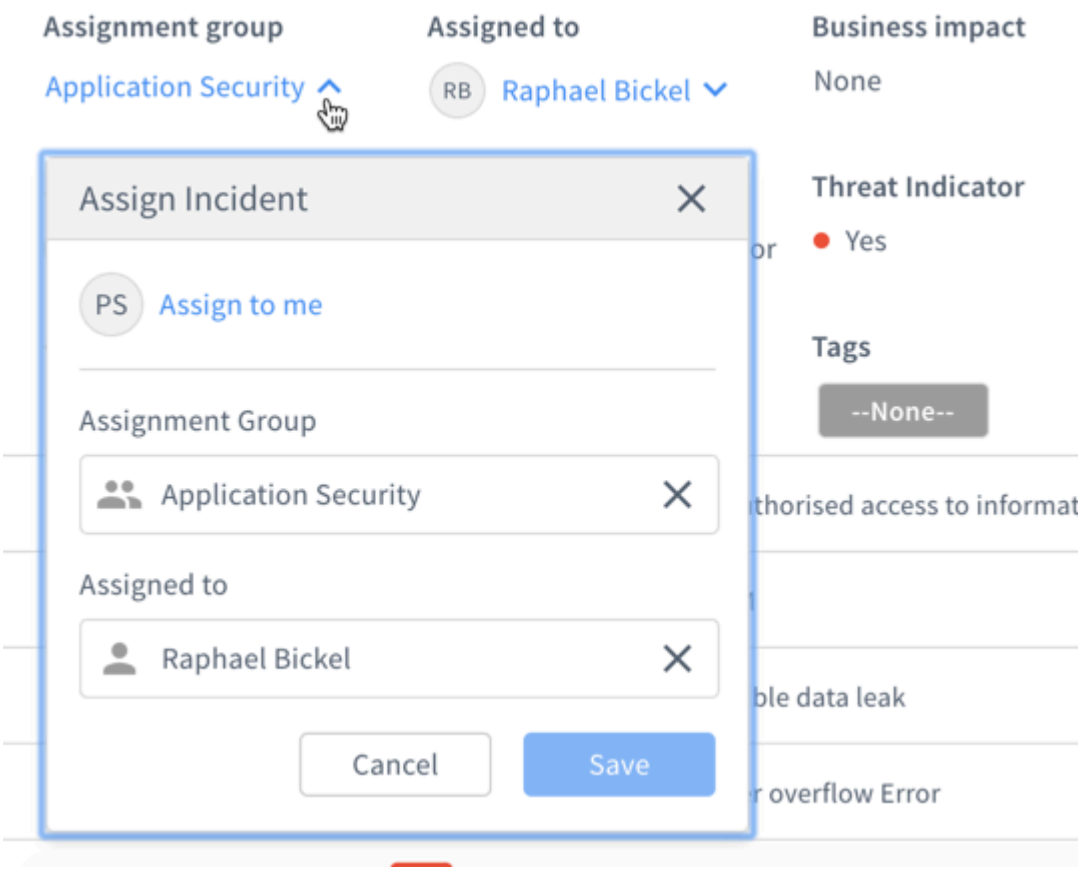
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorschauansicht



Die Vorschauansicht bietet einen Snapshot wichtiger Informationen in einer einzigen Ansicht. Diese Ansicht kann wertvolle Zeit sparen, wenn Sie mit mehreren Incidents arbeiten. Sie können auf die Abwärtspfeile bestimmter Felder klicken, um On-the-fly-Aktualisierungen vorzunehmen, z. B. die Zuweisung einer Zuweisungsgruppe oder eines bestimmten Analysten.

Details der Vorschauansicht



Führen Sie Schnellaktionen für einen Security Incident aus

Nachdem Sie einen bestimmten Security Incident ausgewählt und geöffnet haben, können Sie für den Datensatz zeitsparende Aktionen ausführen.

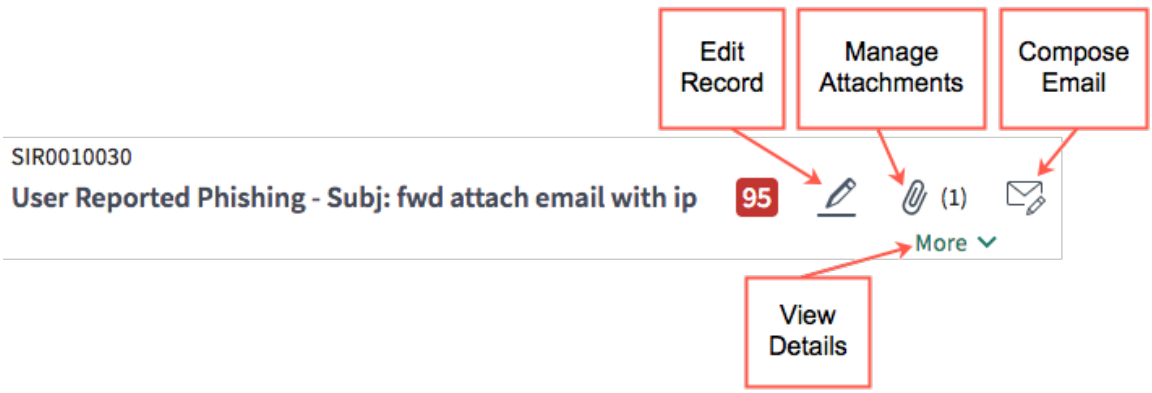
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Ihr Security Incident geöffnet ist, klicken Sie auf das Symbol **„Datensatz bearbeiten“,** um schnelle Änderungen an einem der zugehörigen Felder vorzunehmen. Wenn der Datensatz geschlossen ist, können Sie nur sein Tag ändern.
- Klicken Sie auf **Anhänge verwalten**, um Dateien an den Security Incident anzuhängen. Sie können auch angehängte Dateien herunterladen oder entfernen und die auf die Anhänge angewendete Verschlüsselung bearbeiten.
- Klicken Sie auf **E-Mail erstellen,** um eine schnelle E-Mail an einen Kollegen zu senden. E-Mails können Freiform-E-Mails sein, oder Sie können vordefinierte E-Mails senden, die aus einer Liste von Vorlagen ausgewählt wurden. Gesendete E-Mails und empfangene Antworten werden in der Incident-Zeitleiste erfasst.

Hinweis:
Sie können anwenderdefinierte Vorlagen erstellen, die wiederverwendbare Inhalte für E-Mails und E-Mail-Benachrichtigungen enthalten. Variablen können zum Einfügen spezifischer Informationen für einen Security Incident oder eine Warnung verwendet werden, z. B. Betreffzeile, Priorität oder Bedrohungskategorie. Verwenden Sie die Tabelle „Security Incident“ [sn_si_incident] für E-Mails und E-Mail-Benachrichtigungen im Zusammenhang mit Security Incident Response. Weitere Informationen finden Sie unter E-Mail-Vorlagen

- Klicken Sie auf **Mehr**, um einen schnellen Snapshot des Security Incident anzuzeigen, z. B. Beschreibung, Geschäftsauswirkung und Priorität. Sie können auch auf den Abwärtspfeil in den Feldern **Zuweisungsgruppe** und **Zugewiesen an** klicken, um in Echtzeit Änderungen an diesen Feldern vorzunehmen.

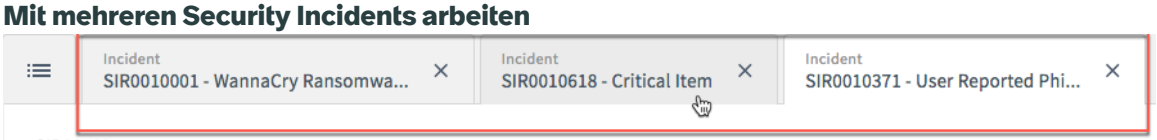
Zuweisungsgruppe



Mit mehreren Security Incidents arbeiten

Über die Registerkarten der Oberfläche können Sie mehrere Security Incidents gleichzeitig geöffnet lassen, sodass Sie mit einem einzigen Klick zwischen ihnen wechseln können. Dies kann Zeit sparen und ermöglicht es Ihnen, das Gesamtbild zu erkennen, wenn Bedrohungen aus mehreren Quellen erkannt werden.

Mit mehreren Security Incidents arbeiten



Zeigen Sie Analyseinformationen auf den Registerkarten für Security Incidents an

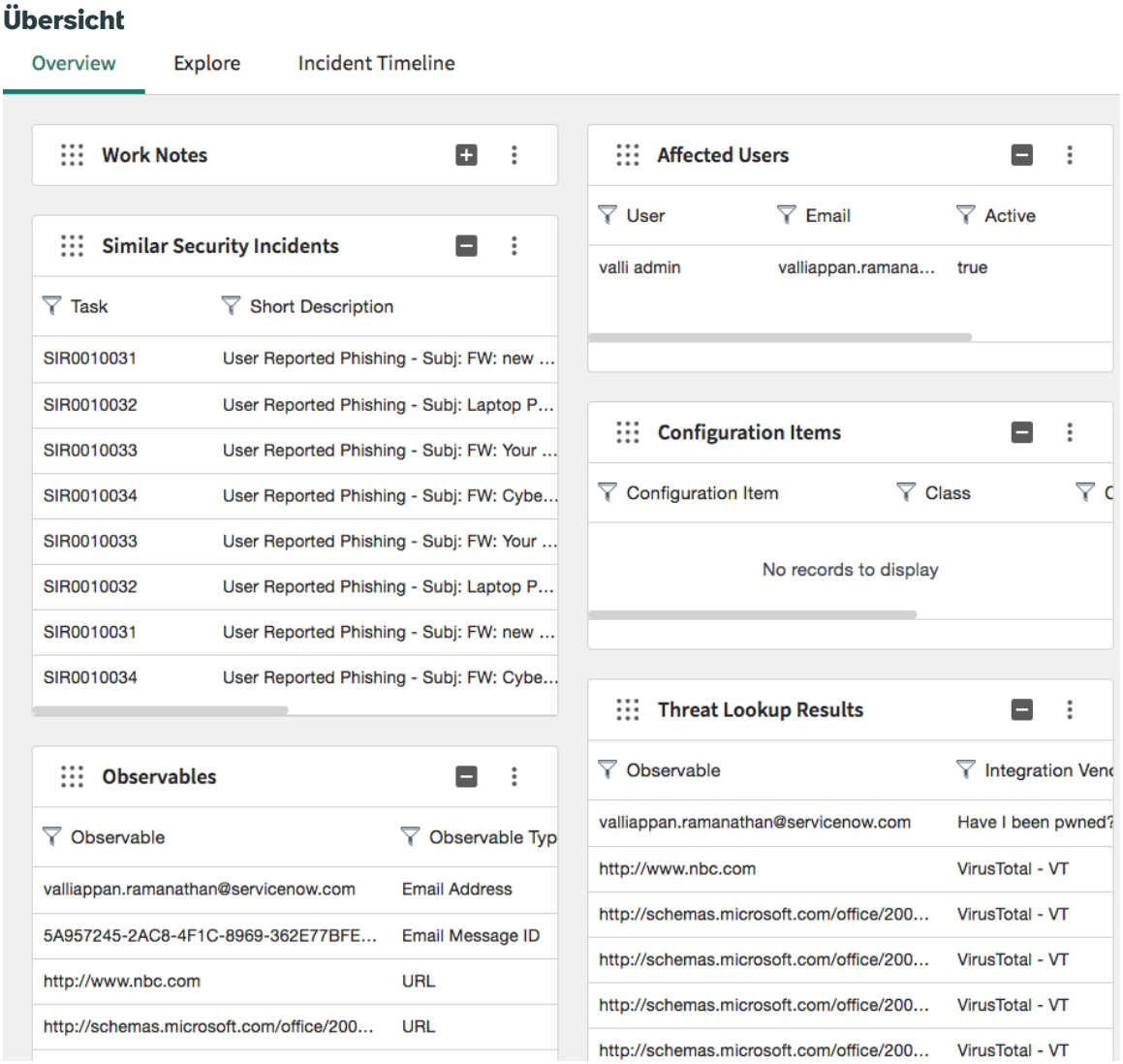
Wenn Sie einen Security Incident-Datensatz öffnen, werden drei Registerkarten angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Übersicht
- Untersuchen
- Incident-Zeitleiste

Registerkarte „Übersicht“

Verwenden Sie die Registerkarte **Übersicht**, um Informationen zu einem Security Incident an zentraler Stelle anzuzeigen. Sie müssen keine andere Anwendung oder Konsole öffnen.

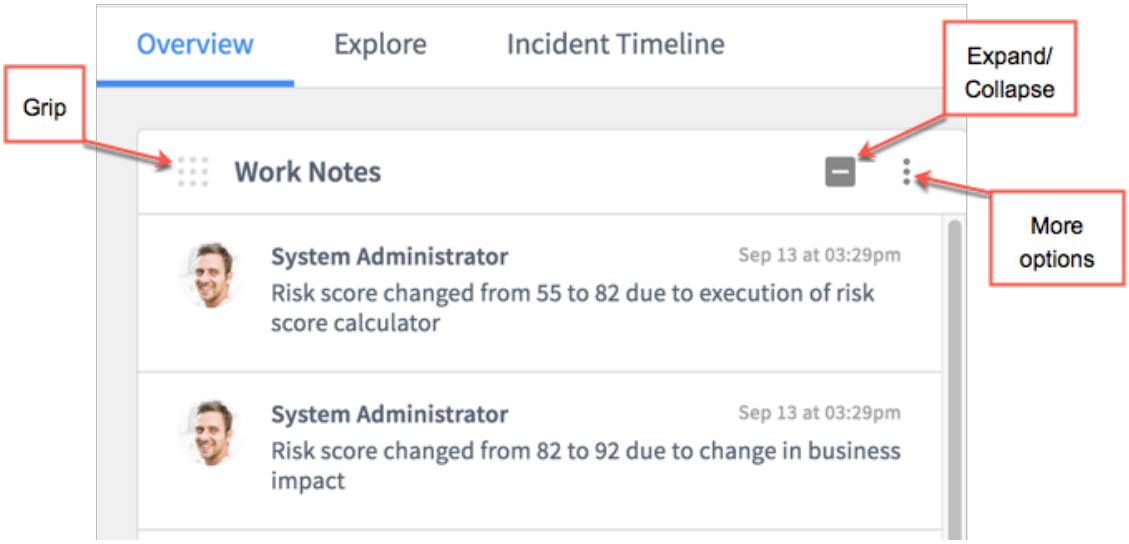


Die Kacheln, die auf der Registerkarte **Übersicht** angezeigt werden, können angepasst werden. Sie können sie nach Bedarf reduzieren und erweitern, und Sie können sie verschieben, indem Sie das **Greifsymbol** ziehen. Klicken Sie auf das Symbol **„Weitere Optionen“**, um eine Kachel zu löschen oder ihren Überschriftentext zu ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

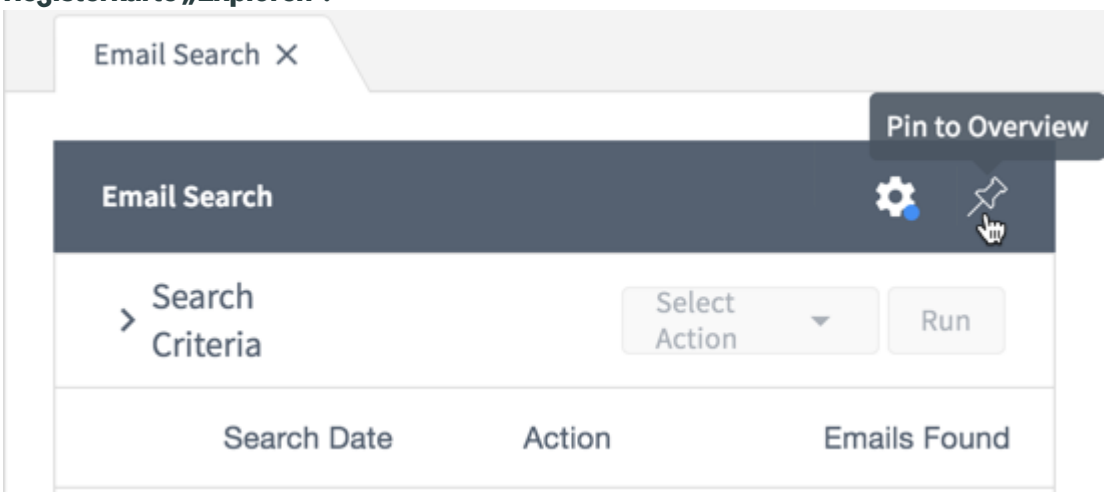
Registerkarte „Übersicht“



Registerkarte Erkunden

Konfigurieren Sie die auf der Registerkarte **Übersicht** angezeigten Kacheln auf der Registerkarte **Erkunden**. Wählen Sie einfach die Kacheln, die Sie anzeigen möchten, im linken Bereich aus, und klicken Sie auf das Symbol **„Anheften“**. Angeheftete Kacheln werden automatisch auf der Registerkarte **Übersicht** angezeigt.

Registerkarte „Exploren“.



Der linke Bereich der Registerkarte **„Erkunden** “ enthält eine Vielzahl von Informationen, die Sie auf der Registerkarte **„Übersicht“** anzeigen können. Erweitern Sie beispielsweise **Erkennbare Elemente**, um diese zugehörigen Listen anzuzeigen.

- Erkennbare Elemente
- Bedrohungssuche – Ergebnisse
- Ergebnisse des Sicherheitsscans
- Domänensuchen
- Ergänzung erkennbarer Elemente

Zusätzliche zugehörige Listen sind unter **Benutzer**, **Konfigurationselemente**und **Incidents**verfügbar.

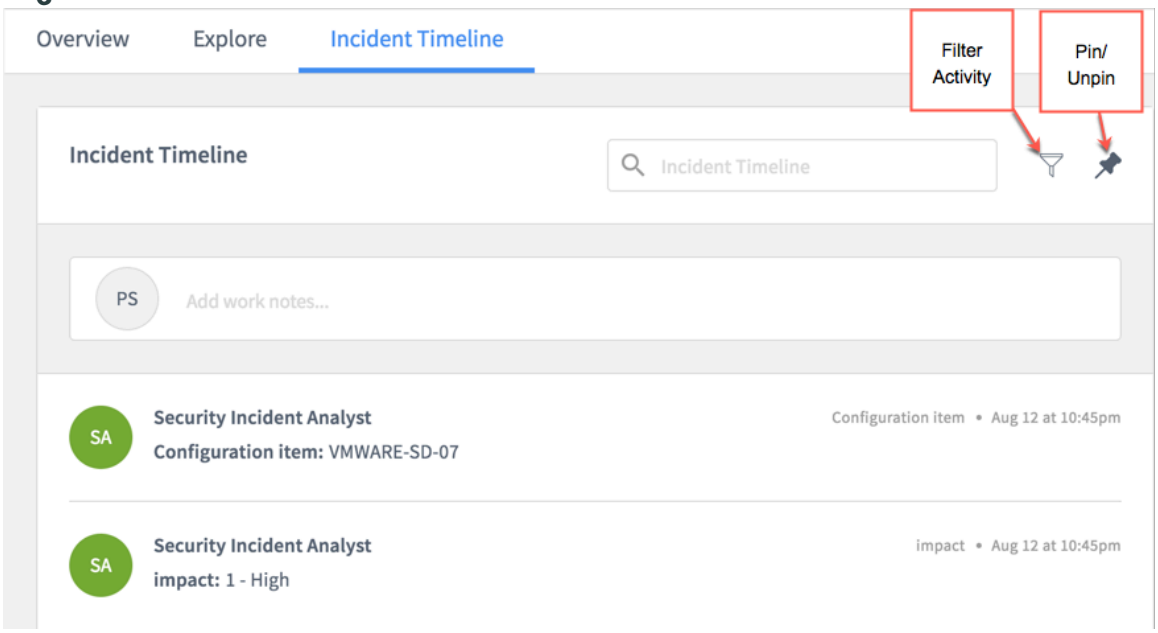
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte Incident-Zeitleiste

Verwenden Sie die Registerkarte **Incident-Zeitleiste** während Ihrer Untersuchung zu Nachverfolgungszwecken. Jedes Mal, wenn eine Aktion für einen Security Incident ausgeführt wird, zeichnet das System dies in der Incident-Zeitleiste auf.

- Sie können der Zeitleiste Arbeitsnotizen auch manuell hinzufügen, indem Sie sie in das Feld **Arbeitsnotizen hinzufügen** eingeben und auf **Veröffentlichen**klicken.
- Sie können mithilfe des Suchfelds auch nach einer bestimmten Zeitleistenaktivität suchen.
- Über das Symbol **„Aktivität filtern“** können Sie nur die Arten von Zeitleistenaktivitäten anzeigen, die Sie sehen möchten (z. B. nur Incidents, die von einem bestimmten Analysten erstellt wurden).
- Sie können die Incident-Zeitleiste zur Registerkarte **Übersicht** hinzufügen oder entfernen, indem Sie auf das Symbol **Anheften/Löschen** klicken.

Registerkarte Incident-Zeitleiste



Behandeln Sie Security Incidents mit dem Playbook

Beheben Sie bestimmte Arten von Sicherheitsbedrohungen schrittweise mit den integrierten Playbooks für Sicherheitsanalysten. Beispielsweise kann ein -Analyst das Playbook verwenden, um Phishing-Angriffe und Bedrohungen zu beheben, die durch Aktivitäten mit böswilligem Code verursacht werden. Weitere Informationen finden Sie unter Beheben Sie Sicherheitsbedrohungen mit dem Playbook.

Beheben Sie Sicherheitsbedrohungen mit dem Playbook

Verwenden Sie das Playbook, um bestimmte Arten von Sicherheitsbedrohungen schrittweise zu beheben. Beispielsweise können Sie mit Playbooks Phishing-Angriffe und Bedrohungen lösen, die durch schädliche Codeaktivitäten verursacht werden.

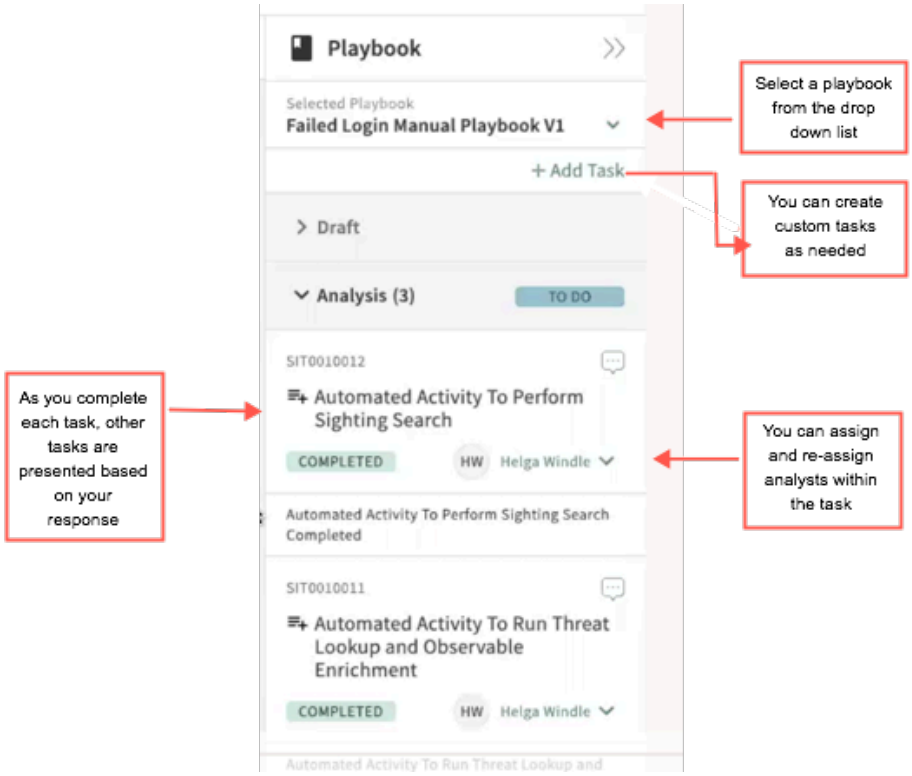
Vorbereitungen
Erforderliche Rolle: sn_si.admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Jede Gruppe von Aufgaben (Analyse, Eindämmung usw.) führt Sie durch eine Reihe von Fragen und anderen Aktivitäten zur Lösung der Bedrohung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

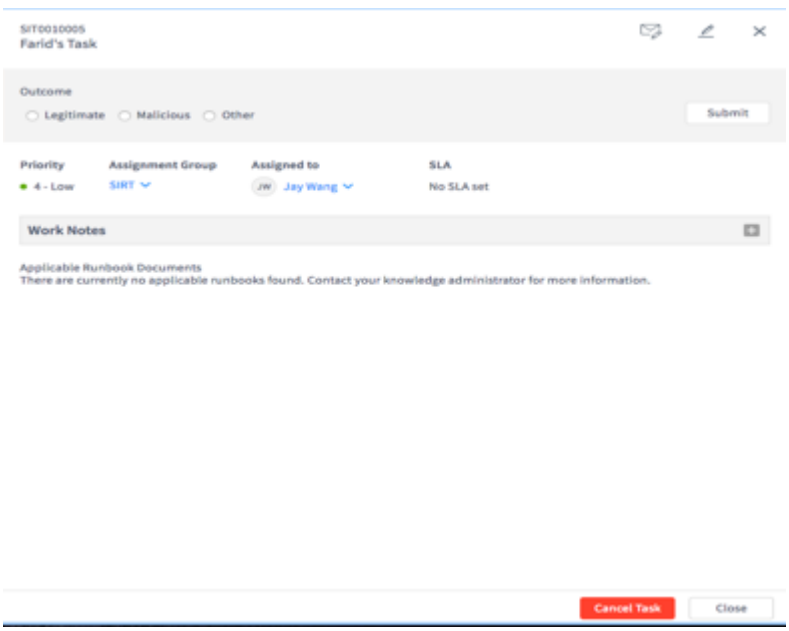
Playbook



Geben Sie bei der Bearbeitung der einzelnen Aufgaben Arbeitsnotizen ein, um ähnliche Angriffe in Zukunft analysieren zu können. Nachdem eine Bedrohung identifiziert wurde, können Sie die Informationen im Playbook auch verwenden, um sie unter Quarantäne zu stellen, ähnlich betroffene Assets zu isolieren und Malware zu entfernen.

Wissensartikel, die in jeder Aufgabe enthalten sind, enthalten Tipps und andere Informationen, um Sie bei der Ausführung der erforderlichen Schritte zu unterstützen.

Wissensartikel



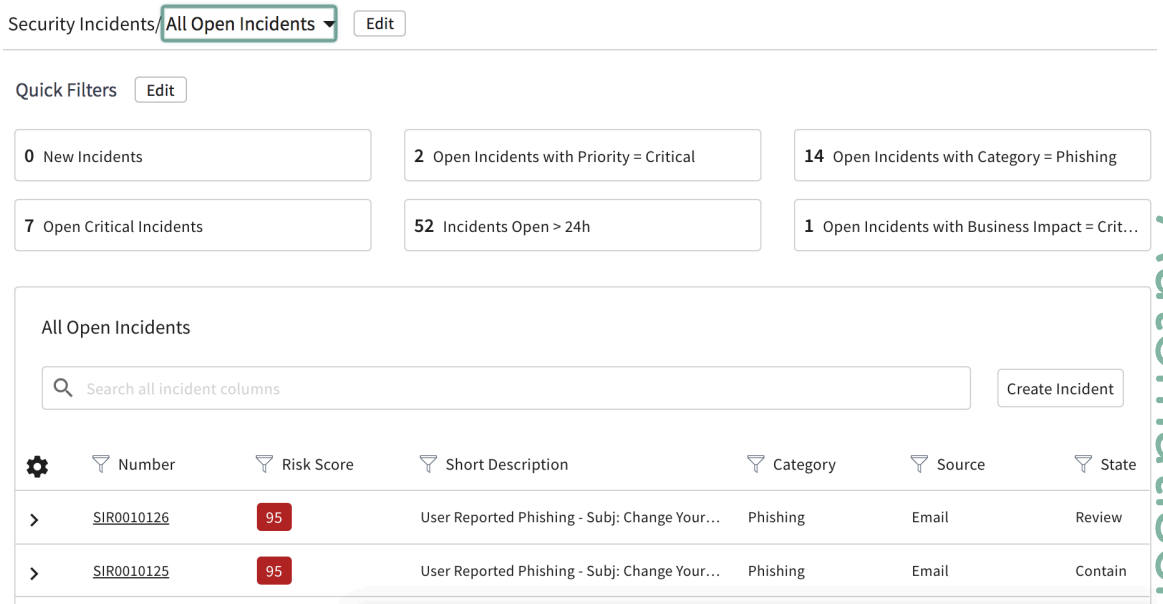
Das -Basissystem enthält Wissensartikel für jede der Playbook-Aufgaben. Sie können jedoch eigene Wissensartikel schreiben und sie Playbook-Aufgaben zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ein Beispiel für die Verwendung des Playbooks zum Analysieren und Beheben einer bestimmten Bedrohung finden Sie unter Von Benutzern gemeldete Phishing-Angriffe mit Playbook lösen.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents (neue UI)**.
   Der Bildschirm Security Incidents zeigt Security Incidents, die Ihnen zugewiesen wurden.



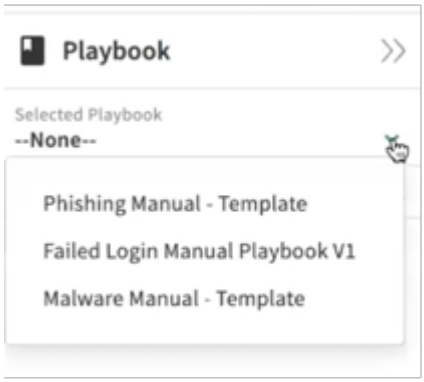
2. Sie können auf die Auswahlliste **Mir zugewiesen** klicken, um einen anderen Filter auszuwählen, z. B. „Alle offenen Incidents“ oder „Alle nicht zugewiesenen Incidents“.
   Alternativ können Sie auf einen der Schnellfilter klicken, um Security Incidents eines bestimmten Typs anzuzeigen, z. B. nur kritische Incidents.
3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

   Erwägen Sie die Priorisierung von Security Incidents mit hohen Risikopunktzahlen.

4. Wenn der Playbook-Bereich am rechten Bildschirmrand geschlossen ist, klicken Sie auf das Playbook-Symbol ( ), um ihn zu öffnen.
   Wenn dem Security Incident kein Playbook zugewiesen ist, können Sie wie unten gezeigt ein Playbook aus der Auswahlliste Ausgewähltes Playbook auswählen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können dem Security Incident auch ein anderes Playbook zuweisen. Um ein Playbook in die Auswahlliste Ausgewähltes Playbook aufzunehmen oder das Playbook für einen Security Incident zu ändern, finden Sie weitere Informationen unter Aktivieren Sie Playbooks für die Analystenauswahl.

Das für den Typ der Sicherheitsbedrohung spezifische Playbook wird geöffnet. Sie ist in Kategorien mit ähnlichen Aufgaben unterteilt. Beispielsweise verwenden Sie die Aufgaben in der **Analysegruppe**, um die Gültigkeit und den Umfang der Bedrohung zu bestimmen. Die Gruppe **„Eindämmen“** enthält Aufgaben zum Eingrenzen der Bedrohung für einen bestimmten Benutzer oder ein bestimmtes Asset. Die Aufgaben in der Gruppe **„Beseitigen“** führen Sie durch den Prozess des Entfernens der Malware oder des erneuten Abbildens des Hosts.

5. Klicken Sie auf die erste Gruppe (**Analyse**), und klicken Sie dann auf die erste Aufgabe im Playbook.
6. Folgen Sie den Anweisungen in der Aufgabe.
   - Bei einigen Aufgaben wird eine Frage gestellt, z. B. „Ist E-Mail Teil der Kampagne?“. Führen Sie die erforderliche Analyse durch, um die Frage zu beantworten, und wählen Sie **Ja** oder **Nein**aus.
   - Wenn Sie Wissensartikel definiert und mit Playbook-Aufgaben verknüpfthaben, werden die Artikel angezeigt, wenn Sie mit der Arbeit an einer Aufgabe beginnen.
   - Einige Aufgaben sind vorübergehend. Sie weisen Sie lediglich an, eine Aktion auszuführen, z. B. das Hinzufügen erkennbarer Elemente zu einem Security Incident. Nachdem Sie die Aktion abgeschlossen haben, klicken Sie auf **Als abgeschlossen markieren**.

   Wenn Sie Aufgaben abschließen, werden Ihnen basierend auf den von Ihnen getroffenen Entscheidungen nachfolgende Aufgaben vorgelegt. Ausgegraute Gruppen (z. B. **Wiederherstellen**, **Überprüfen**usw.) können durch Ihre Auswahl aktiviert werden.
7. Arbeiten Sie an jeder Aufgabe weiter, bis Sie alle Aufgaben abgeschlossen haben, um die Bedrohung zu beheben und den Security Incident zu schließen.

Zugehörige Informationen

Fügen Sie dem Playbook eine anwenderdefinierte Aufgabe hinzu

Von Benutzern gemeldete Phishing-Angriffe mit Playbook lösen

Das Phishing-Playbook führt Sie durch die Aufgaben, die zum Analysieren und Lösen eines Phishing-Angriffs erforderlich sind, der von einem Mitarbeiter Ihres Unternehmens gemeldet wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

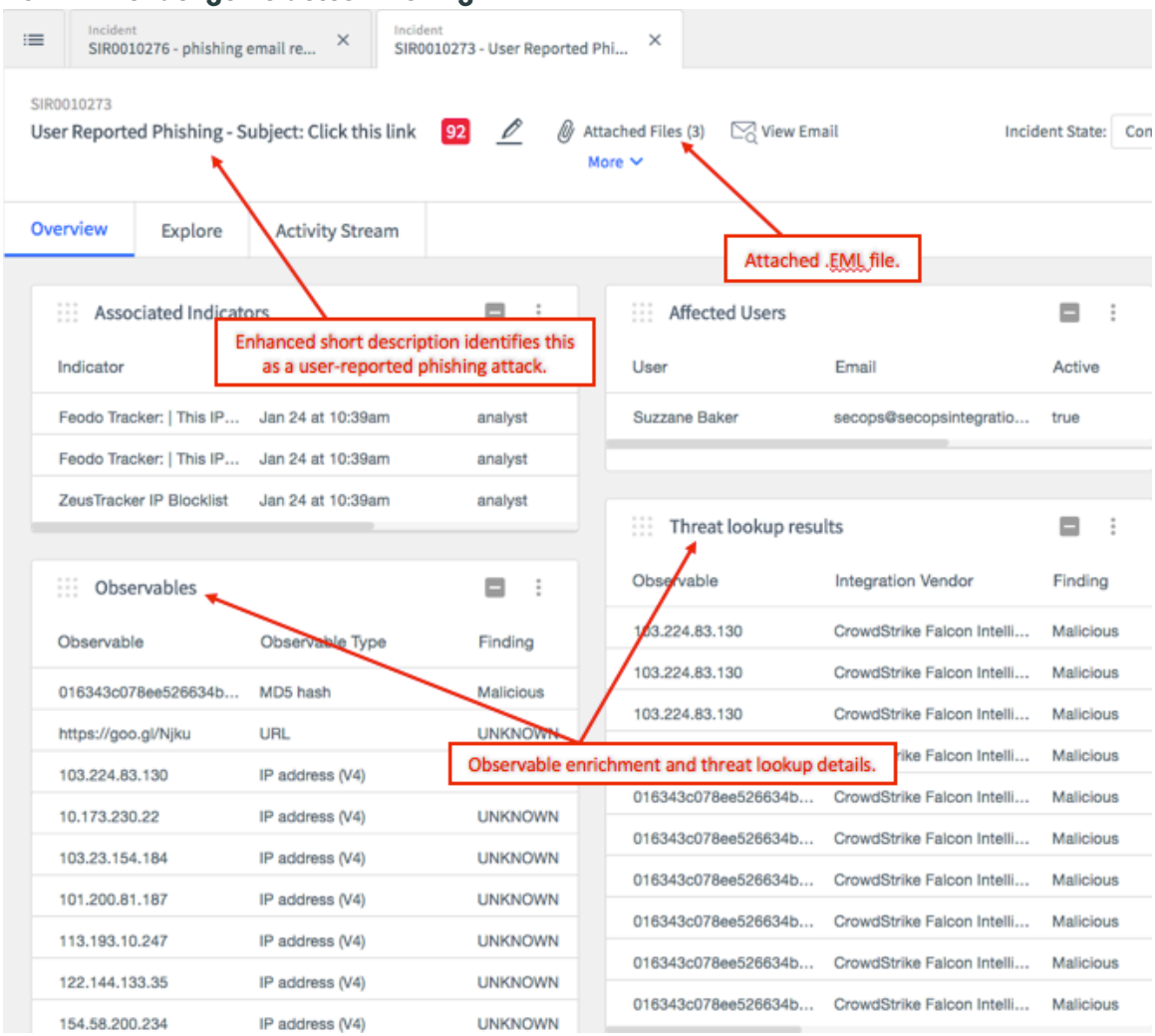
Wie Security Incidents aus von Benutzern gemeldeten Phishing-Angriffen erstellt werden

Während des Setups von Security Incident Response erstellt Ihr Systemadministrator eine Reihe von E-Mail-Übereinstimmungsregeln, mit denen E-Mails identifiziert werden können, die Anzeichen eines Phishing-Angriffs enthalten. Wenn Mitarbeiter eine verdächtige E-Mail erhalten, die die allgemeinen Anzeichen eines Phishing-Angriffs enthält (wie in Ihren Sicherheitsrichtlinien definiert), können sie diese als EML-Anhang an die von Ihrer Organisation festgelegte Phishing-E-Mail-Adresse senden.

Wenn die E-Mail an der Phishing-E-Mail-Adresse empfangen wird, wird der EML-Anhang analysiert und die darin enthaltenen Informationen mit den E-Mail-Übereinstimmungsregeln verglichen. Wenn eine Übereinstimmung gefunden wird, wird ein Security Incident erstellt, der die folgenden Informationen enthält:

- Die Kurzbeschreibung enthält Phishing vom Anwender gemeldet, gefolgt vom eigentlichen Betreff der ursprünglichen E-Mail.
- Die EML-Datei wird an den Security Incident angehängt.
- Wenn die EML erkennbare Elemente enthält, werden diese analysiert, und es werden automatisch Ergänzungs- und Bedrohungssuchen durchgeführt.

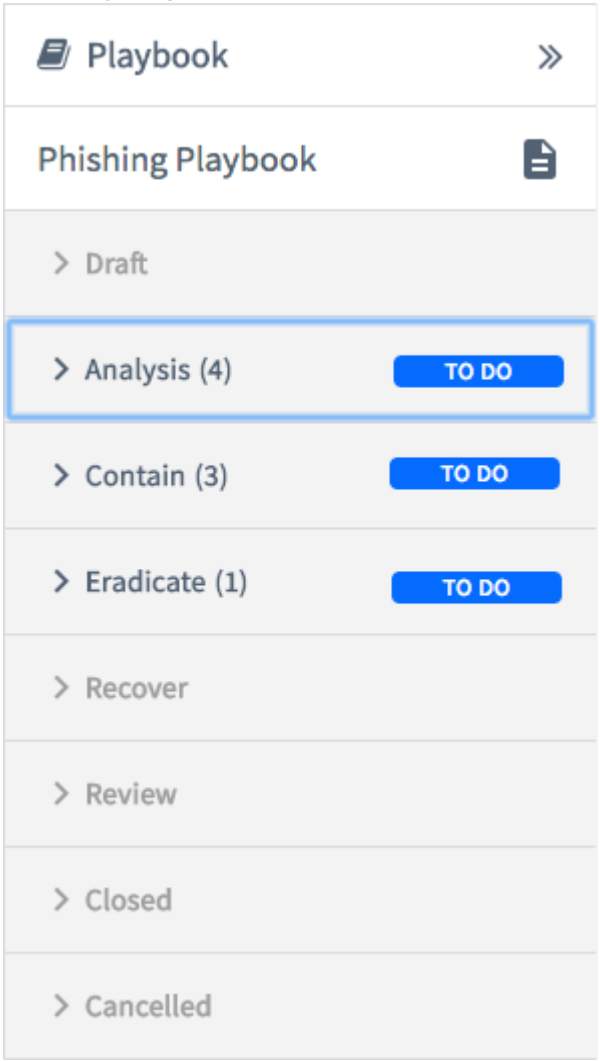
Vom Anwender gemeldetes Phishing



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Security Incident der Kategorie „Phishing“ geöffnet wird, ist das Phishing-Playbook automatisch verfügbar. Klicken Sie einfach auf das Playbook-Symbol ( ), um das Playbook zu öffnen.

Phishing-Playbook



Das Phishing-Playbook enthält Aufgaben, mit denen Sie eine Phishing-Bedingung analysieren, eindämmen und beseitigen können. Die Aufgaben sind in Status organisiert (z. B. **Analyse**, **Eindämmen**usw.). Wenn alle Aufgaben für einen Status abgeschlossen wurden, leitet Sie das Playbook zum nächsten Status.

Details von Security Incidents werden analysiert

Wenn sich der Security Incident im Status „Analyse“ befindet, erhalten Sie Aufgaben zur Durchführung einer grundlegenden Untersuchung des Incidents, einschließlich:

- Bestimmen der Gültigkeit des incident.
- Untersuchen der Auswirkungen der potenziellen Bedrohung.
- Koordinierung einer effektiven Reaktion auf den Incident

Während Sie die Aufgaben durcharbeiten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Machen Sie sich mit den Wissensartikeln vertraut.
- Öffnen Sie den E-Mail-Anhang, und untersuchen Sie ihn auf typische Phishing-Elemente.
- Überprüfen Sie die Ergebnisse der Bedrohungssuche.

Enthält den Security Incident

Wenn sich der Security Incident im Status **„Eindämmen“** befindet, erhalten Sie Aufgaben, um die Details der E-Mail zu überprüfen. Um sicherzustellen, dass keine Bedrohungen in Ihre Organisation gelangen können, aktualisieren Sie Ihre Netzwerkabwehrmaßnahmen in Form von Signaturen und Regeln für das Intrusive Defence System (IDS) und das Intrusive Prevention System (IPS).

Während Sie die Aufgaben durcharbeiten:

- Ergreifen Sie Maßnahmen, um die Auswirkungen von Bedrohungen zu begrenzen, z. B. die Isolierung der betroffenen Geräte.
- Untersuchen Sie die an die E-Mail angehängten erkennbaren Elemente.
- Ermitteln Sie, ob E-Mail-Inhalte einer bekannten Bedrohung zugeordnet sind, einschließlich:
  - URL
  - E-Mail-Absender
  - Phishing-URL
  - IP-Adresse des SMTP-Servers des Absenders

Die Malware wird gelöscht

Nachdem Sie aktualisierte Signaturen und Regeln für Ihre Antivirenlösung bereitgestellt haben, verwenden Sie die Aufgaben im Status „ **Beseitigen** “, um festzustellen, ob Malware vorhanden ist, und entsprechend zu behandeln.

Während Sie die Aufgaben durcharbeiten:

- Scannen Sie die Endpunkte betroffener Geräte auf Malware.
- Entfernen Sie alle gefundenen Malware.
- Als letzten Ausweg können Sie die Hostgeräte löschen und ein neues Image erstellen.

Überprüfung des Security Incidents

Wenn Sie bei der Ausführung der Analyseaufgaben festgestellt haben, dass ein Phishing-Angriff ein falscher Alarm war, wechselt der Security Incident in den Status **Überprüfen**, und Sie müssen Ihre Benutzer benachrichtigen, damit sie wissen, dass der E-Mail-Anhang sicher geöffnet werden kann.

Der Security Incident wird geschlossen

Wenn alle Aufgaben im Playbook abgeschlossen wurden, wird der Security Incident in den Status **Geschlossen** versetzt. Sie müssen Abschlusskommentare eingeben, bevor der Incident geschlossen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident wird abgebrochen

Wenn sich ein Security Incident im Status **Überprüfen** befindet und Sie Ihre Benutzer erfolgreich darüber informiert haben, dass die E-Mail keine Bedrohung darstellt, wird der Status **Abgebrochen** aktiviert, und Sie können den Security Incident abbrechen.

Hinweis:
Die Aufgabe „Wiederherstellen“ wird im Phishing-Playbook nicht verwendet.

Ordnen Sie einen Wissensartikel einer Playbook-Aufgabe zu

Während Sie Sicherheitsbedrohungen mit dem Playbook Security Incident Response analysieren, können Sie Wissensartikel für jede Aufgabe anzeigen, sofern von Ihrer Organisation definiert. Wenn keine Wissensartikel vorhanden sind, können Sie sie erstellen und Playbook-Aufgaben zuordnen.

Vorbereitungen

Beachten Sie bei der Verwendung des Playbooks in Security Incident Responseden Text, der jeder Aufgabe zugeordnet ist. Die erste Aufgabe in der Kategorie Phishing lautet beispielsweise **Wurde Warnung von Mitarbeiter übermittelt?** Dies ist die Kurzbeschreibung der Aufgabe, und Sie benötigen diesen Text (genau so, wie er im Playbook angezeigt wird), um der Aufgabe einen Wissensartikel zuzuordnen.

Erforderliche Rolle: sn_sir.knowledge_admin und entweder sn_si.admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Katalog & Wissen** > **Wissen**.
2. Erstellen und veröffentlichen Sie einen Wissensartikel für eine bestimmte Playbook-Aufgabe.
3. Navigieren zu **Security Incident** > **Manuelles Runbook** > **Neues Runbook erstellen**.
4. Erstellen Sie ein Runbook, indem Sie die folgenden Informationen ausfüllen:

Feld	Beschreibung
Wissensartikel	Wählen Sie den veröffentlichten Wissensartikel aus, den Sie der Playbook-Aufgabe zuordnen möchten.
Tabelle	Wählen Sie Security Incident Response Aufgabe [sn_si_task] aus.
Bedingung	Legen Sie den Bedingungsgenerator auf Folgendes fest: ○ **Option:** Wählen Sie **Kurzbeschreibung**aus. ○ **Operator:**Auswählen **ist**. ○ **Eingabewert:** Geben Sie die Kurzbeschreibung für die Aufgabe genau so ein, wie sie im Playbook angezeigt wird.

5. Klicken Sie auf **Absenden**.
   Wenn Sie das Playbook das nächste Mal ausführen und diese Aufgabe auswählen, wird der zugehörige Wissensartikel angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen Sie einen Wissensartikel zu Security Incidents

Erstellt ein Security Incident Response-Runbook

Fügen Sie dem Playbook eine anwenderdefinierte Aufgabe hinzu

Das -Basissystem Security Analyst Workspace enthält eine Reihe von Aufgaben für jede Bedrohungskategorie. Sie können anwenderdefinierte Aufgaben erstellen, die den spezifischen Anforderungen Ihres Systems oder Ihrer Kunden entsprechen.

Vorbereitungen

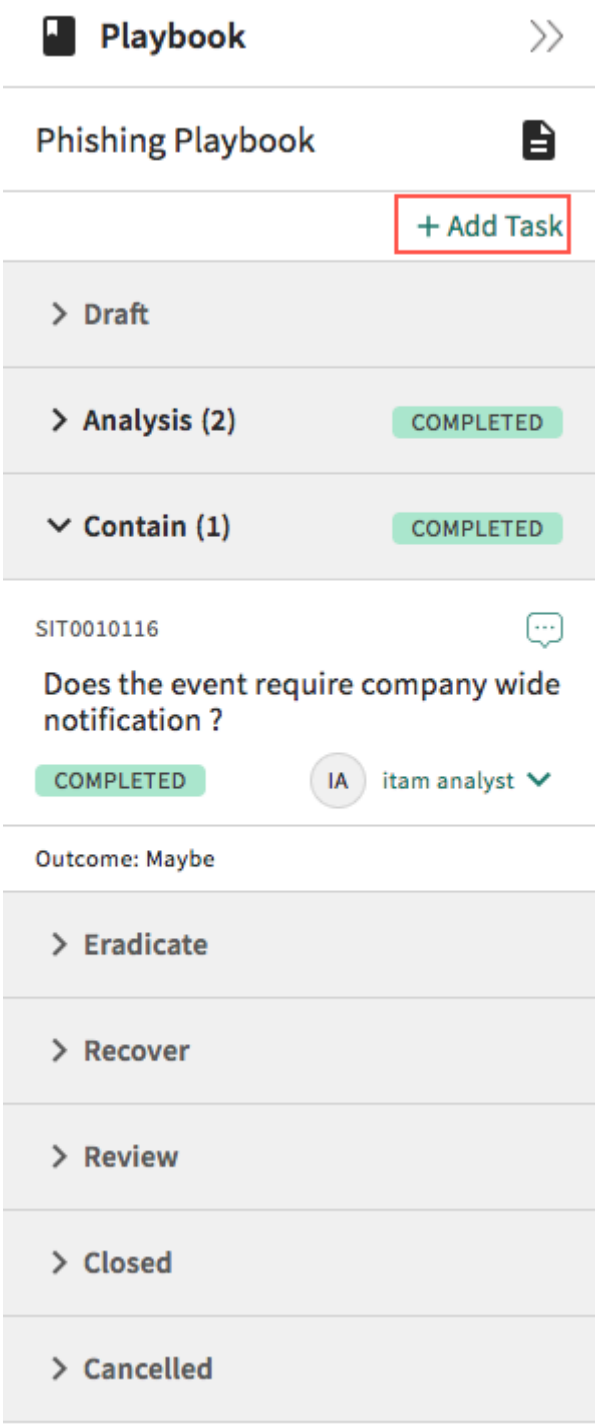
Erforderliche Rolle: sn_si.basic oder security_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

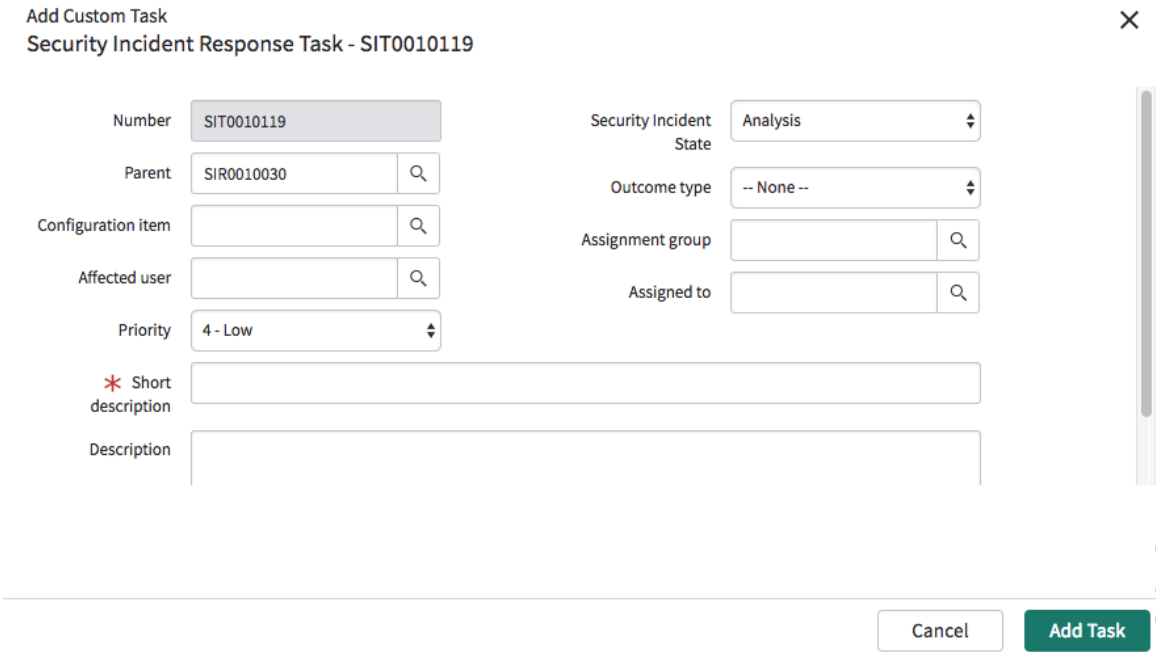
Prozedur

1. Klicken Sie bei geöffnetem Playbook **auf Aufgabe hinzufügen**.



Der Bildschirm „Anwenderdefinierte Aufgabe hinzufügen“ wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Nummer	[Schreibgeschützt] Die automatisch generierte Nummer der Security Incident-Aufgabe.
Übergeordnet	Die Nummer des zugehörigen Security Incidents.
Konfigurationselement	Das Configuration Item, das von dem Sicherheitsproblem betroffen ist, falls vorhanden.
Betroffener Anwender	Der Anwender, der von dem Sicherheitsproblem betroffen ist, falls vorhanden.
Priorität	Wählen Sie die Priorität aus, mit der bestimmt wird, wann diese Aufgabe ausgeführt werden soll.
Status des Security Incidents	Der aktuelle Status der Sicherheitsantwortaufgabe. Bei Bedarf können Sie einen zukünftigen Status auswählen.
Ergebnistyp	Wenn Sie über die Rolle sn_si.basic verfügen, wählen Sie **Ja/Nein** als Ergebnistyp aus. Mit der Rolle security_admin können Sie einen anwenderdefinierten Ergebnistyp mit mehreren anwenderdefinierten Ausgabewerten erstellen. Sie können beispielsweise eine Aufgabe mit abhängigen Werten basierend auf der Bedrohungskategorie definieren. Weitere Informationen finden Sie unter Auswahllisten
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Person, der die Ausführung der Aufgabe zugewiesen ist.
Kurzbeschreibung	Eine Beschreibung der Aufgabe „Playbook für Security Incidents“.
Beschreibung	Geben Sie eine Beschreibung für die ausgewählte Aufgabe ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf **Aufgabe hinzufügen**.
   Die Aufgabe wird nach der aktuellen Aufgabe in das Playbook eingefügt.

Sichtungssuchen nach von Anwendern gemeldeten Phishing- und Malware-Angriffen

Führen Sie Sichtungssuchen in E-Mails oder erkennbaren Elementen durch, um zu bestimmen, wie häufig bestimmte Arten von Angriffen, z. B. Phishing-Angriffe oder Kommunikation mit einer schädlichen IP-Adresse oder URL, in Ihrem Netzwerk auftreten. Jedes Auftreten gilt als Sichtung. Sichtungssuchen nach erkennbaren Elementen müssen für Ihre Protokollspeicher oder das SIEM (Security Information and Event Management, SIEM) konfiguriert werden.

Erfahren Sie, wie Sie die Sichtungssuchfunktion verwenden, um Phishing-Anwender zu finden und erkennbare Phishing- und Malware-Elemente im Protokollspeicher Ihres Netzwerks nachzuverfolgen.

Sehen Sie sich dieses dreiminütige Video an, um zu erfahren, wie Sie mit der Sichtungssuchfunktion Phishing-Anwender ausfindig machen und erkennbare Phishing- und Malware-Elemente im Protokollspeicher Ihres Netzwerks nachverfolgen können.

Die folgenden Begriffe werden verwendet, um von Benutzern gemeldete Phishing-Angriffe zu beschreiben:

- Phishing-Anwender: Ein Anwender, der eine Phishing-E-Mail erhalten hat.
- Betroffener Anwender: Ein Anwender, der mit der Phishing-URL interagiert hat, normalerweise durch Klicken auf einen Link in der Phishing-E-Mail. Durch diese Aktion werden dem Angreifer möglicherweise Anmeldeinformationen verfügbar gemacht.

Wenn Sie mit der Analyse eines Phishing-Incidents beginnen, können Sie eine E-Mail-Sichtungssuche oder eine Suche nach erkennbaren Elementen durchführen, um andere Anwender in Ihrer Organisation zu identifizieren, die von demselben Phishing-Angriff betroffen sind. Durchsuchen Sie Ihre Protokollspeicher, um Phishing-Angriffe und betroffene Anwender zu identifizieren. Nachdem Sie die Liste der betroffenen Benutzer identifiziert haben, erstellen Sie mit den in Security Incident Responseverfügbaren Tools untergeordnete Security Incidents, um umfassende Verfahren zur Reaktion auf Incidents durchzuführen.

Hinweis:
Sie können auch den folgenden Ansatz verwenden, um eine Sichtungssuche durchzuführen:

- Navigieren zu **Security Incidents** > **Alle Incidents anzeigen** und klicken Sie auf einen Security Incident.
- Klicken Sie auf **IoC anzeigen** unter Zugehörige Links. Eine Liste der erkennbaren Elemente wird angezeigt.
- Wählen Sie ein erkennbares Element aus der Liste aus, und wählen Sie in der Liste **Aktionen** eine der folgenden Optionen aus:
  - Sichtungssuche für Webdatenverkehr ausführen
  - Sichtungssuche für E-Mail-Datenverkehr ausführen
- Geben Sie den Zeitrahmen an, und klicken Sie auf **Suche**, um eine Sichtungssuche durchzuführen.

Sichtungssuchkonfigurationen gespeichert

Konfigurieren Sie Sichtungssuchen, und erstellen Sie gespeicherte Konfigurationen für SIEMs oder andere Protokollspeicher für Instanzen von erkennbaren Elementen, um das Vorhandensein schädlicher erkennbarer Elemente in Ihrer Umgebung festzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Gespeicherte Suchen und Inplace-Abfragen werden nur für die Splunk-Integration unterstützt.

Zugehörige Informationen

Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

Führen Sie eine E-Mail-Sichtungssuche nach von Anwendern gemeldeten Phishing-Angriffen durch

Suchen Sie nach Anwendern, die Phishing-E-Mails erhalten haben, basierend auf erkennbaren Elementen wie E-Mail-Betreff, Absendername oder Nachrichten-ID. Sie können diese Phishing-E-Mails dann eindämmen und in Ihrer Organisation entfernen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Durchsuchen Sie die Protokolle des Splunk-E-Mail-Verkehrs, um die Liste der Empfänger einer verdächtigen E-Mail zusammenzustellen. Die Suche kann anhand des E-Mail-Absenders, der E-Mail-Nachrichten-ID oder des E-Mail-Betreffs, der einem Security Incident zugeordnet ist, als Kriterium durchgeführt werden.

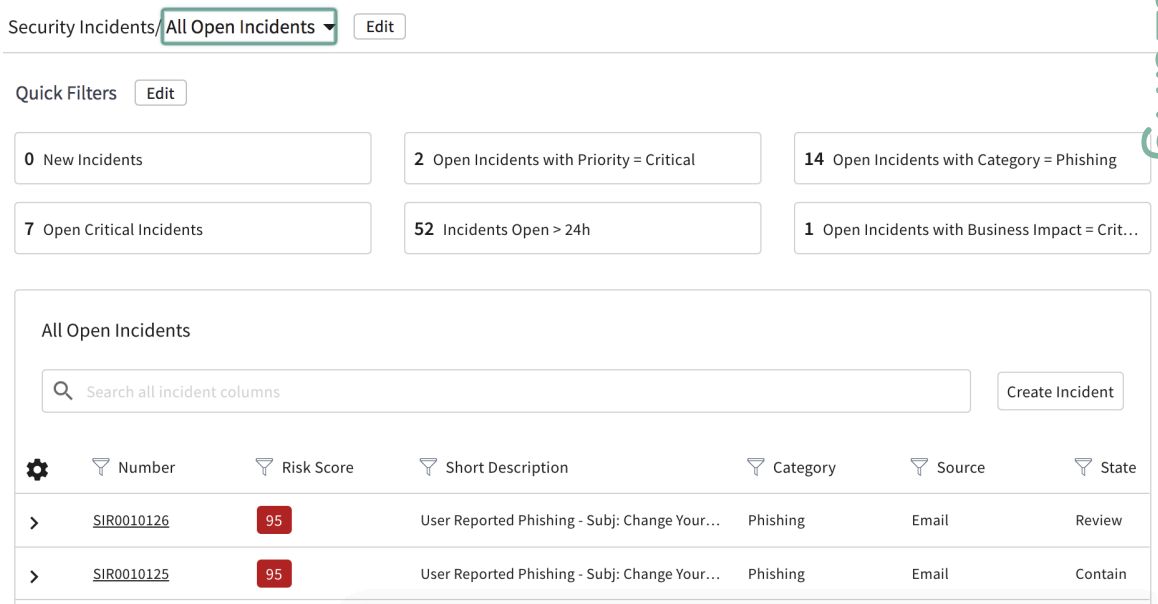
Hinweis:

- Diese Implementierung der Sichtungssuche für E-Mail-basierte erkennbare Elemente wurde nur mit dem Splunk Enterprise-Protokollspeicher getestet.
- Die Splunk-Protokollereignisse müssen Common Information Model (CIM) entsprechen, damit die Sichtungssuchabfrage genaue Ergebnisse zurückgibt.

Prozedur

1. Um die Ihrem Team zugewiesenen Security Incidents anzuzeigen, navigieren Sie zu **Security Incident** > **Incidents (neue UI)**.
2. Wählen Sie in der Liste **„Security Incidents“** einen der Filter aus, z. B. alle **offenen Incidents**, **alle Ihnen zugewiesenen Incidents**oder **alle Incidents**.

   Klicken Sie auf einen der **Schnellfilter**, um Security Incidents eines bestimmten Typs anzuzeigen, z. B. kritische Incidents oder Phishing-E-Mails.

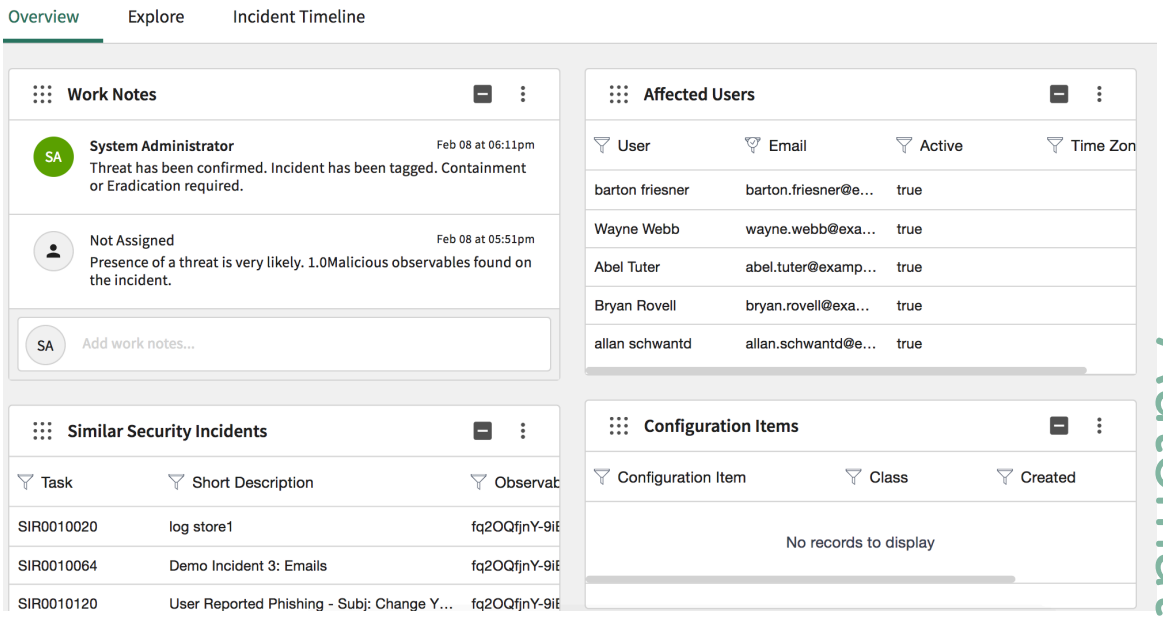


Automatische Übersetzung

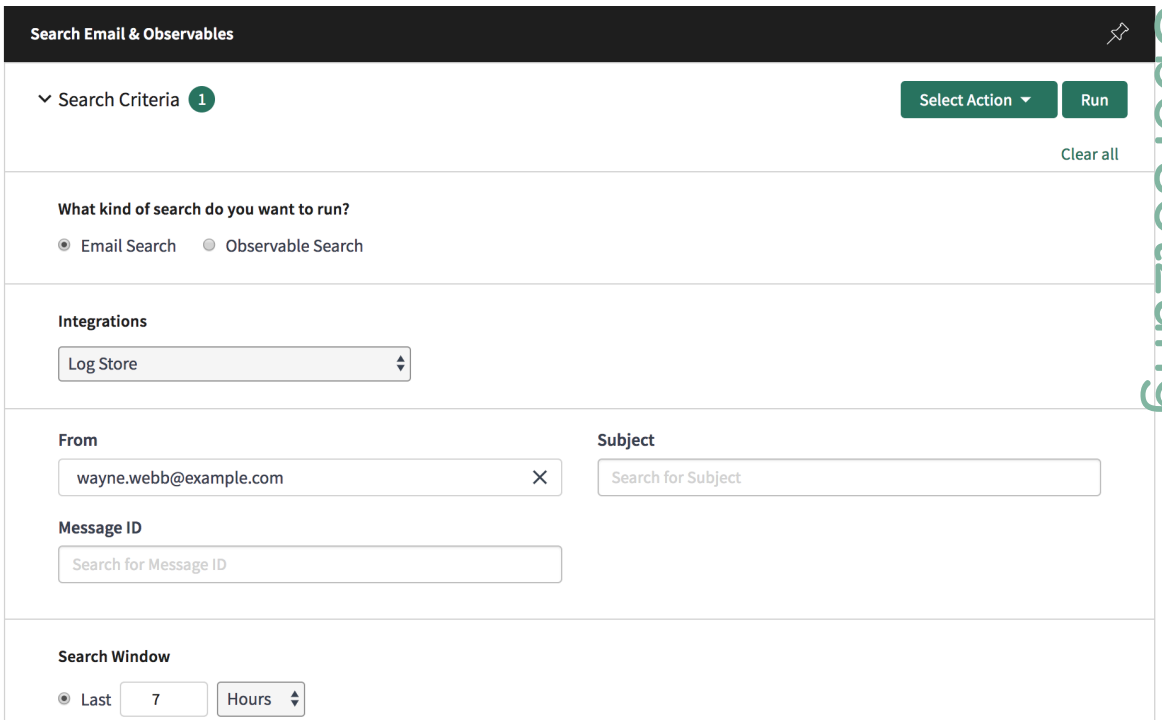
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

   Die Registerkarte „Übersicht“ bietet eine Übersicht über Security Incidents, einschließlich einer Liste erkennbarer Elemente, betroffener Benutzer und ähnlicher Security Incidents.



4. Klicken Sie auf die Registerkarte **Erkunden**.
5. Navigieren Sie unter **Incident-Daten**zu **Ermittlung** > **E-Mails und erkennbare Elemente durchsuchen**.



6. Erweitern Sie den Abschnitt Suchkriterien.
7. Wählen Sie **E-Mail-Suche** als den Suchtyp aus, den Sie ausführen möchten, und geben Sie die restlichen Suchkriterien an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Suchkriterien“.

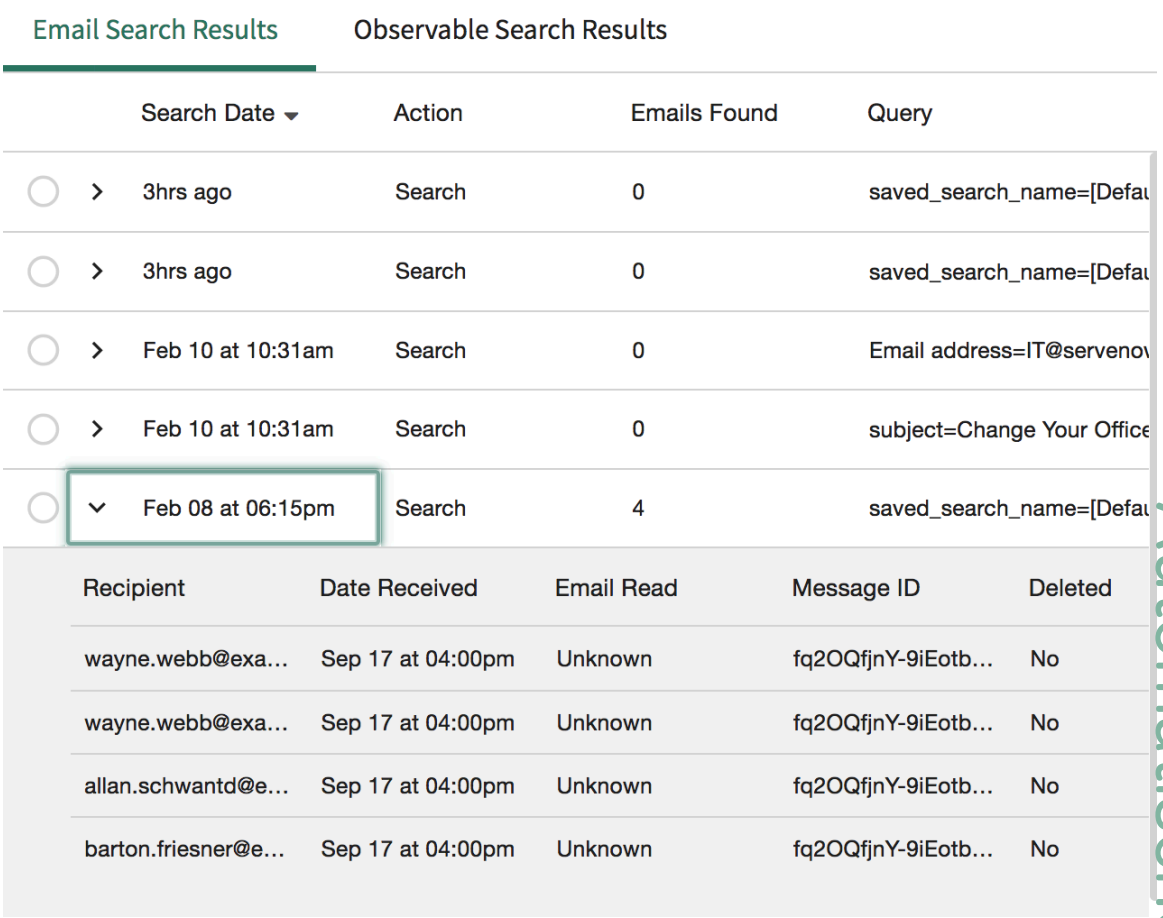
Feld	Beschreibung
Integrationen	Integrationstyp. Wählen Sie **Protokollspeicher** aus der Liste aus. **Hinweis:** Diese Funktion wird nur mit dem Splunk-Protokollspeicher unterstützt.
Von	Vollständige E-Mail-Adresse des Absenders (z. B. jane.doe@example.com).
Nachrichten-ID	E-Mail-Nachrichten-ID aus dem Protokollspeicher.
Betreff	Betreff der Phishing-E-Mail.
Suchfenster	Zeitfenster für die Suche (z. B. die letzten 24 Stunden).

8. Wählen Sie in der Liste **Aktion auswählendie Option Suchen** aus, und klicken Sie dann auf **Ausführen**.

   Der Splunk-Protokollspeicher wird anhand der von Ihnen eingegebenen Kriterien durchsucht, und die Benutzer, die Ziel des Phishing-Angriffs sind, werden auf der Registerkarte **E-Mail-Suchergebnisse** angezeigt. Die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail, einschließlich Empfangsdatum der E-Mail, Empfänger und Nachrichten-ID, werden angezeigt.

9. Um die Liste der Benutzer anzuzeigen, die die Phishing-E-Mail erhalten haben, klicken Sie auf das Symbol **>** in der Spalte Suchdatum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Um eine Liste der Benutzer anzuzeigen, die die E-Mail erhalten haben, navigieren Sie zu **Anwender** > **Betroffene Anwender**.

    Die Spalte Phishing-Anwender identifiziert die E-Mail-Empfänger.

    Hinweis:
    Auf der Seite „Betroffene Anwender“ werden nur die Anwenderdatensätze angezeigt, die in der ServiceNow-Instanz vorhanden sind.

11. Führen Sie die folgenden Schritte aus, um die Anwender, die Ziele des Phishing-Angriffs sind, weiter zu untersuchen:

    a. Aktivieren Sie die Kontrollkästchen neben den Anwendernamen.

    b. Wählen Sie in der Liste **Untergeordneten Security Incident erstellen aus**, und klicken Sie auf **Ausführen**.

    Es wird eine Meldung angezeigt, dass ein untergeordneter Security Incident erstellt wurde. Um die untergeordneten Security Incidents anzuzeigen, die einem übergeordneten Incident zugeordnet sind, klicken Sie auf die Registerkarte **Erkunden**, und navigieren Sie zu **Incidents** > **Untergeordnete Security Incidents**.

Ergebnisse

Die Liste der Benutzer mit Phishing-Assets wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie eine Sichtungssuche für erkennbare Elemente nach von Anwendern gemeldeten Phishing- und Malware-Angriffen durch

Führen Sie Sichtungssuchen für erkennbare Elemente durch, um herauszufinden, wie viele Anwender innerhalb eines bestimmten Zeitraums eine schädliche oder verdächtige Website besucht haben.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Suche im Netzwerkverkehr nach erkennbaren Elementen wie der URL, dem Zielhost oder der Ziel-IP-Adresse durchführen, die einem Security Incident zugeordnet sind.

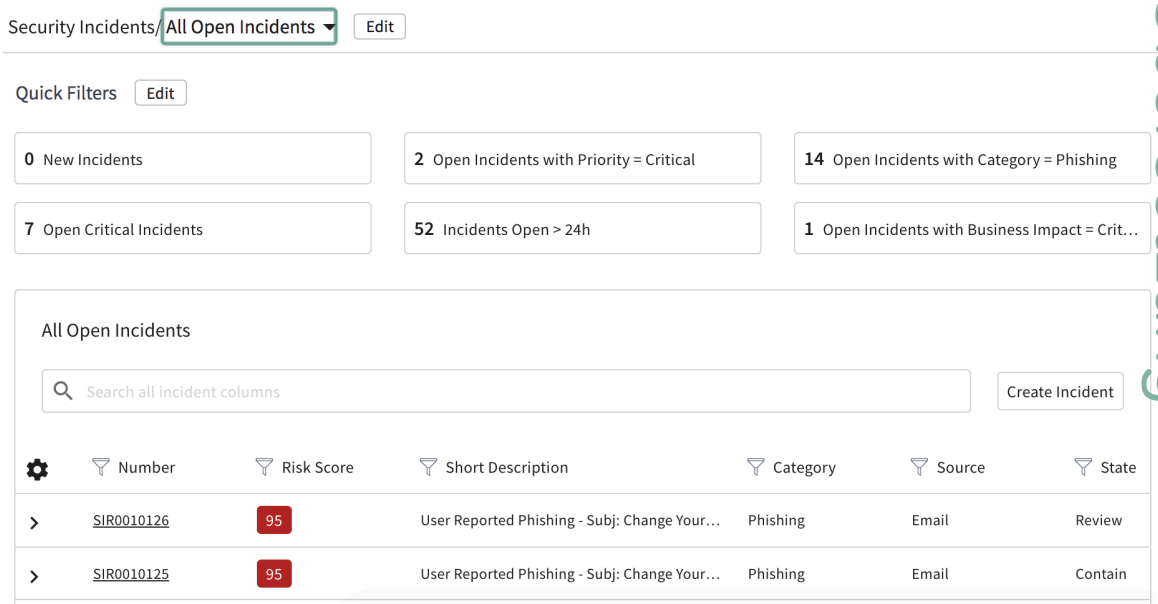
Hinweis:

- Diese Implementierung der Sichtungssuche nach erkennbaren Elementen wurde nur mit dem Splunk Enterprise-Protokollspeicher getestet.
- Die Splunk-Protokollereignisse müssen Common Information Model (CIM) entsprechen, damit die Sichtungssuchabfrage genaue Ergebnisse zurückgibt.

Prozedur

1. Um die Security Incidents anzuzeigen, die Ihrem Team zugewiesen sind, navigieren Sie zu **Security Incident** > **Incidents (neue UI)**.
2. Wählen Sie in der Liste **„Security Incidents“** einen anderen Filter aus, z. B. alle **mir zugewiesenen Incidents**, **alle offenen Incidents**oder **alle Incidents**.

   Klicken Sie auf einen der **Schnellfilter**, um Security Incidents eines bestimmten Typs anzuzeigen, z. B. kritische Incidents oder Phishing-E-Mails.

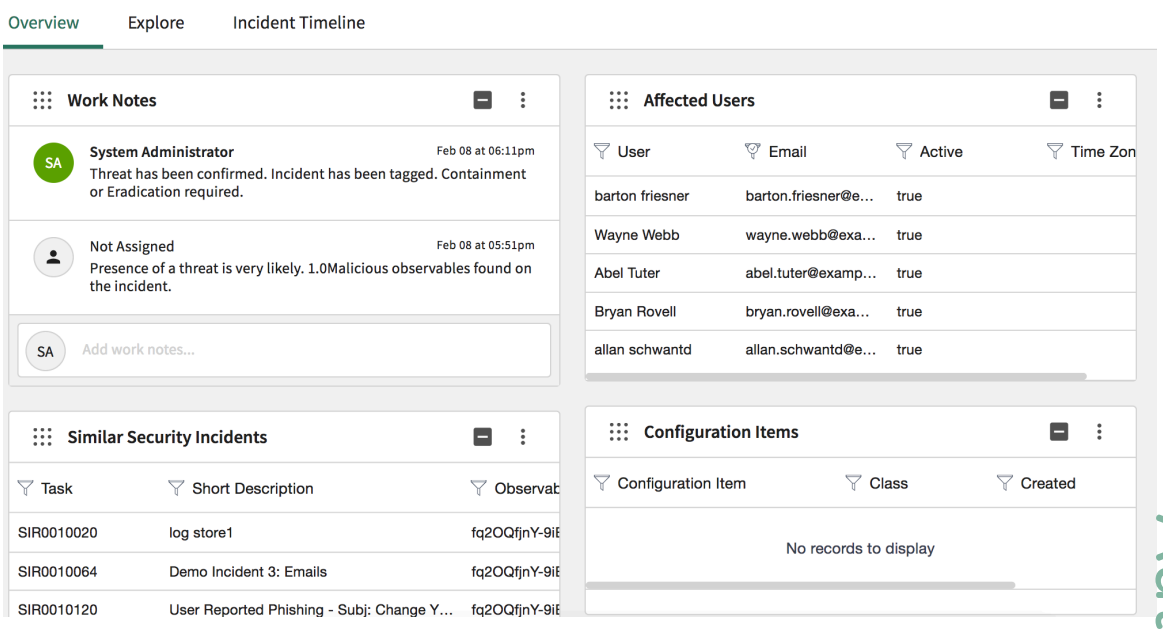


3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

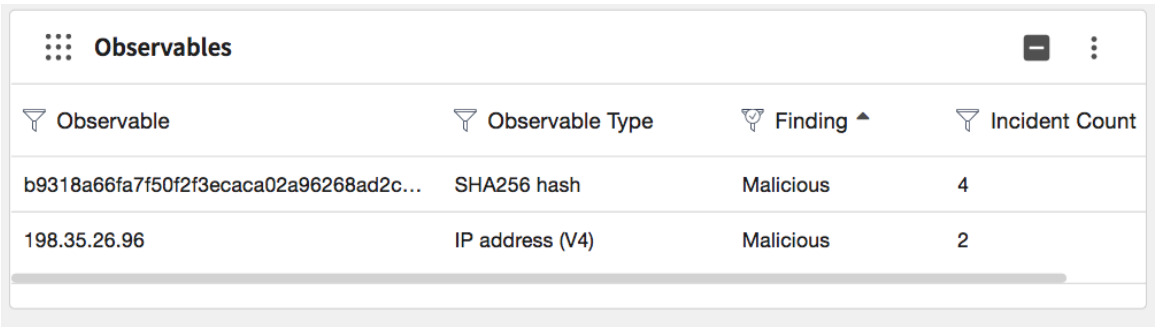
   Sie können eine Übersicht über den Security Incident anzeigen, einschließlich einer Liste erkennbarer Elemente, betroffener Benutzer und ähnlicher Security Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

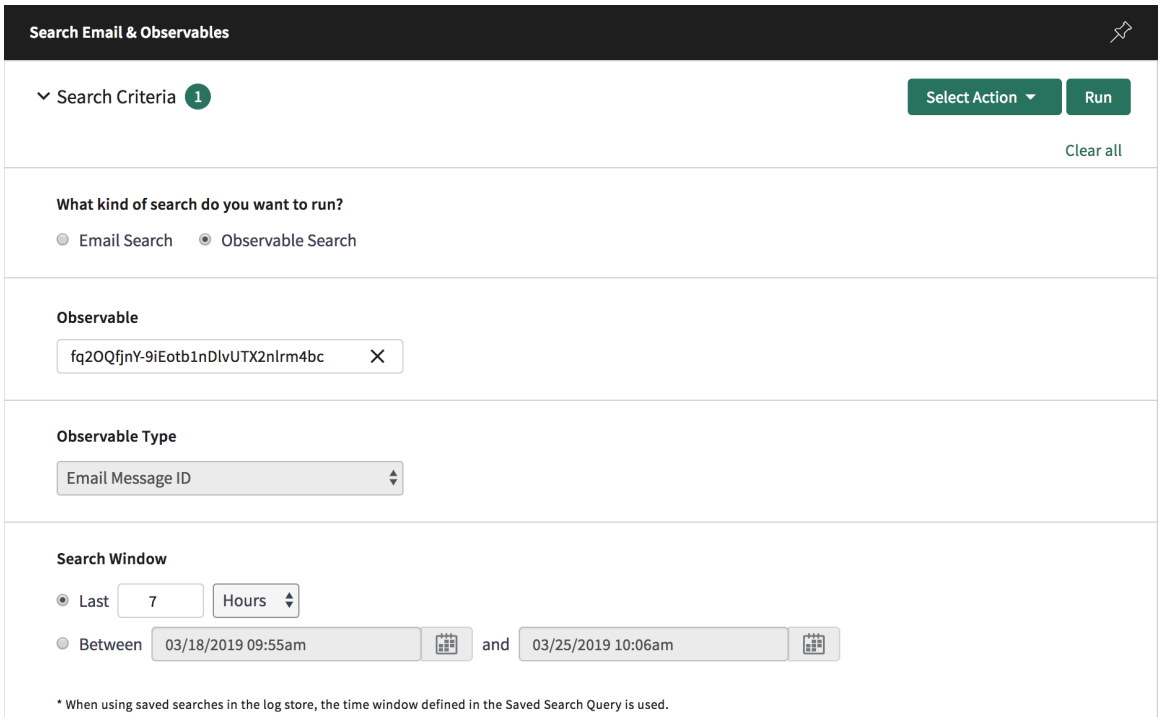


Beachten Sie, dass im Abschnitt „Erkennbare Elemente“ in der Spalte „Erkennbares Element“ die E-Mail-Adresse, der Betreff und die URL angezeigt werden. Beachten Sie auch, dass in der Spalte „Ergebnis“ zu sehen ist, dass die URL bei Übermittlung der Phishing-E-Mail automatisch gescannt und als bekannte schädliche URL eingestuft wurde. In der Spalte Incident-Anzahl werden die anderen Incidents angezeigt, die dasselbe erkennbare Element gemeinsam nutzen. Diese Artefakte zeigen an, dass Sie wahrscheinlich bereit sind, zu Eindämmungsverfahren für diesen Phishing-Angriff überzugehen, einschließlich der Bestimmung, wie viele Benutzer in der Organisation betroffen sind.

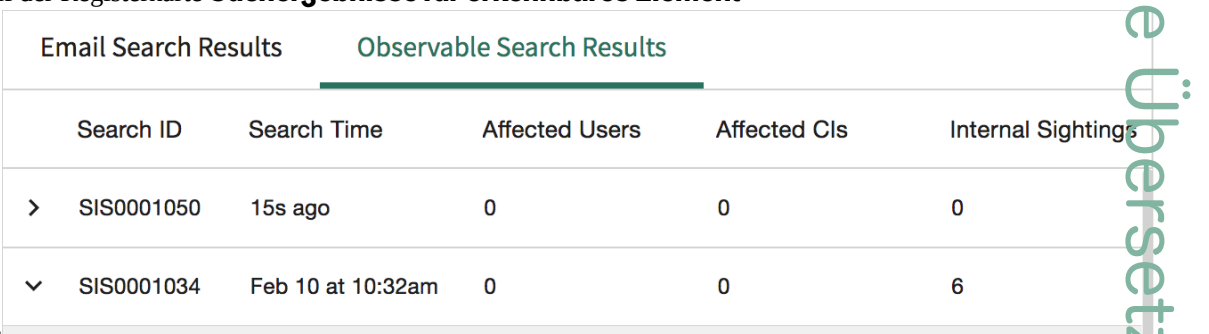


4. Navigieren zu **Untersuchen** > **Ermittlung** > **E-Mails und erkennbare Elemente durchsuchen**.
5. Erweitern Sie den Abschnitt Suchkriterien, und klicken Sie auf **Suche nach erkennbaren Elementen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Geben Sie das gesuchte erkennbare Element und ein Zeitfenster für die Suche ein (z. B. Letzte 24 Stunden).
7. Wählen Sie in der Liste **Aktion auswählen** die **Option Suchen**aus.
   Der Splunk-Protokollspeicher wird anhand der von Ihnen eingegebenen Kriterien durchsucht, und die wichtigsten Benutzer, die Ziel des böswilligen Angriffs sind, werden auf der Registerkarte **Suchergebnisse für erkennbares Element**



   angezeigt.
8. Um die Benutzer anzuzeigen, die die E-Mail erhalten haben, navigieren Sie zu **Anwender** > **Betroffene Anwender**.

   Die Spalte „Phishing-Benutzer“ identifiziert die Empfänger der Phishing-E-Mail, und die Spalte „Benutzerinteraktion“ identifiziert Benutzer, die auf eine Phishing-URL geklickt oder mit einer verdächtigen E-Mail-Adresse interagiert haben. Die Spalte „Anwenderinteraktion“ wird auf „true“ oder „false“ gesetzt, je nachdem, ob der Anwender auf den schädlichen Link oder die schädliche IP geklickt hat.

   Hinweis:
   Auf der Seite „Betroffene Anwender“ werden nur die Anwenderdatensätze angezeigt, die in der ServiceNow-Instanz vorhanden sind.

9. Um die Anwender, die auf die Phishing-E-Mail geklickt und möglicherweise ihre Anmeldeinformationen gefährdet haben, weiter zu untersuchen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Aktivieren Sie in den Spalten Phishing-Anwender und Anwenderinteraktion die Kontrollkästchen neben den Anwendernamen, die **true**anzeigen.

b. Klicken Sie auf **Untergeordneten Security Incident erstellen** und anschließend auf **Ausführen**. Es wird eine Meldung angezeigt, dass ein untergeordneter Security Incident erstellt wurde. Um die untergeordneten Security Incidents anzuzeigen, die einem übergeordneten Incident zugeordnet sind, klicken Sie auf die Registerkarte **Erkunden**, und navigieren Sie zu **Incidents** > **Untergeordnete Security Incidents**.

Ergebnisse
Die Liste der Benutzer mit Phishing-Assets wird angezeigt.

Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

Erstellen Sie mehrere Konfigurationsdatensätze für die Sichtungssuche, und verwenden Sie sie, wenn Sie mehrere Protokollspeicher abfragen oder die Suchparameter variieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

- Das CIM-Add-on muss auf der Splunk-Instanz installiert sein.
- Gespeicherte Suchen und Inplace-Abfragen werden nur für die Splunk-Integration unterstützt.

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch Konfigurationsdatensätze für Sichtungssuchen erstellen, um gespeicherte Suchen im Splunk-Enterprise-Protokollspeicher aufzurufen.

Hinweis:
Die Suchkonfigurationsabfragen beruhen darauf, dass Splunk-Protokolldaten konform mit dem Splunk Common Information Model (CIM) sind.

Mit gespeicherten Suchkonfigurationen können Sie:

- Erstellen Sie anwenderdefinierte Suchen, die mehrere Ereignisdatensätze kombinieren.
- Designeffiziente und effektive Suche.
- Verwenden Sie parametrisierte Eingaben in der gespeicherten Splunk-Suche.

Das -Basissystem enthält die in der folgenden Abbildung gezeigten Beispielkonfigurationen:

Gespeicherte Suchkonfigurationen

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

Die gespeicherte Suche und die Inplace-Konfigurationsabfragen sind Beispielabfragen und können durch entsprechende Parameter für Ihre Umgebung ersetzt werden. Erstellen Sie nach Bedarf zusätzliche gespeicherte Suchkonfigurationen. Wenn Sie eine gespeicherte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchkonfiguration definieren, müssen der Name und die Parameter in der Suchabfrage mit der in Ihrer Splunk-Instanz definierten gespeicherten Konfiguration übereinstimmen. Wenn der Name und die Parameter nicht identisch sind, werden bei einer Sichtungssuche möglicherweise keine genauen Ergebnisse angezeigt.

Hinweis:
Navigieren Sie in Ihrer Splunk-Instanz zur Seite Suchen, Berichte und Warnungen, und suchen Sie nach Ihrer gespeicherten Suchabfrage. Klicken Sie auf den Link **Berechtigungen**, um zur Seite „Berechtigungen“ zu navigieren. Wählen Sie das Optionsfeld **Alle Apps** aus, und aktivieren Sie die Option **Leseberechtigung** für **Jeder**. Dadurch wird der Spaltenwert „Freigabe“ für Ihre gespeicherte Suchabfrage von „Privat“ in „App“ geändert. Wenn dies nicht festgelegt ist, gibt die gespeicherte Suchabfrage möglicherweise keine Ergebnisse zurück.

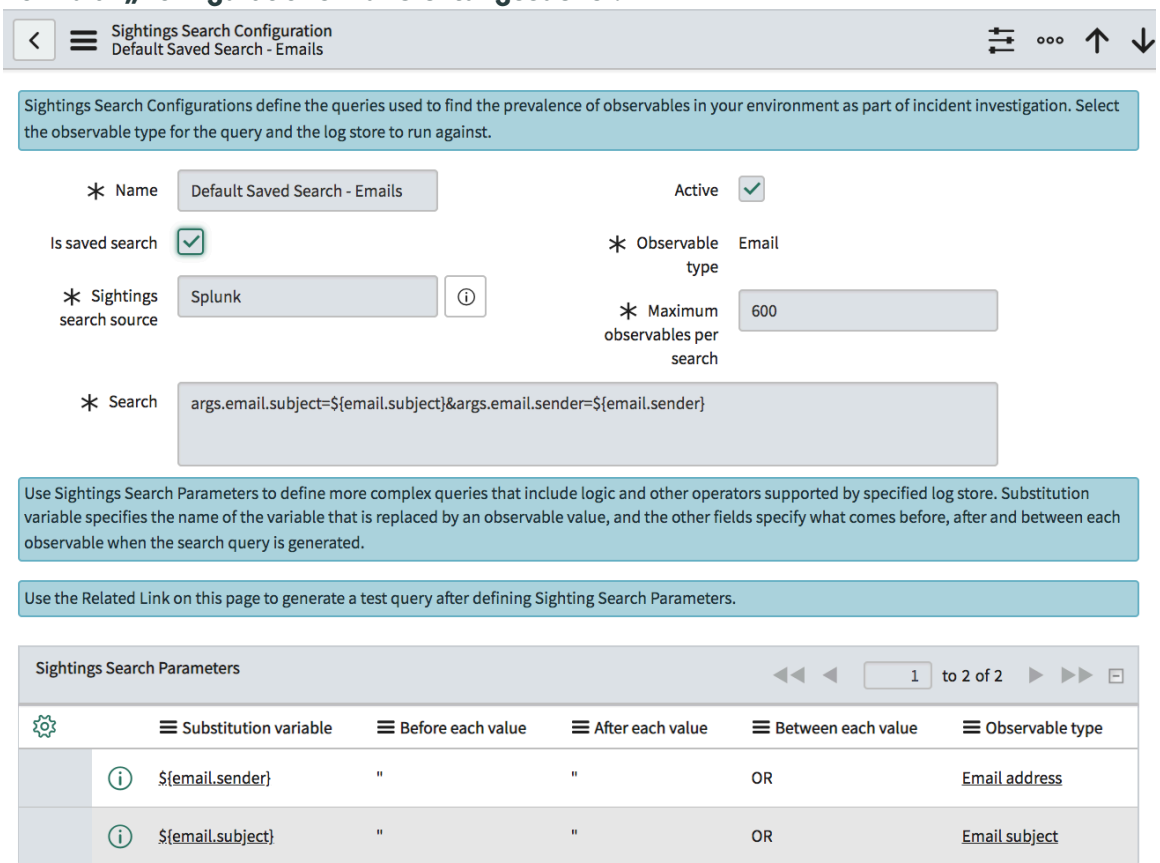
So überprüfen Sie, ob die gespeicherte Suchkonfiguration mit der in Ihrer Splunk-Instanz definierten Konfiguration übereinstimmt:

1. Navigieren zu **Einstellungen** > **Suchen, Berichte und Warnungen**.
2. Ändern Sie **den App-Kontext** in **Alle**.

   Eine Liste der Suchberichte wird angezeigt.
3. Bestätigen Sie, dass die gespeicherte Suchabfrage in der Liste vorhanden ist.

Das Formular „Konfigurationen für die Sichtungssuche“ enthält beispielsweise die E-Mail-Adresse und den E-Mail-Absender als Suchparameter:

Formular „Konfigurationen für Sichtungssuche“.



Definieren Sie in Ihrer Splunk-Instanz die gespeicherte Suche mit demselben Namen, Standardmäßige gespeicherte Suche – E-Mails, und denselben Suchparametern für die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Adresse und den E-Mail-Betreff. Wenn der Name und die Suchparameter nicht identisch sind, generiert die Sichtungssuche kein genaues Ergebnis.

Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfiguration** und erstellen Sie einen neuen Datensatz (Feldbeschreibungen finden Sie in der Tabelle).

Formular „Konfigurationen für Sichtungssuche“.

Feld	Beschreibung
Name	Name der Konfiguration
Ist gespeicherte Suche	Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt.
Sichtungssuchquelle	Die Quelle für die Sichtungssuche. Wählen Sie den Splunk-Protokollspeicher als Quelle aus.
Aktiv	Option für den gespeicherten Suchstatus. Nur aktive Suchkonfigurationen können verwendet werden, um eine Sichtungssuche durchzuführen.
Erkennbarer Typ	Der erkennbare Elementtyp kann ein beliebiger erkennbarer Elementtyp wie IP, Hash-Wert, URL, Domänenname usw. sein.
Maximale erkennbare Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die von der Suche zurückgegeben werden sollen.
Suchen	Die Standardsuchzeichenfolge ist `$(observable)`, Sie können jedoch Ihre eigene Suchabfrage definieren, indem Sie Parameter angeben, die vom Splunk-Protokollspeicher unterstützt werden.

2. Klicken Sie auf **Absenden**.

Ergebnisse
Sie haben einen Konfigurationsdatensatz für die Sichtungssuche erstellt.

Nächste Maßnahme
Nachdem Sie die Suchabfrage definiert haben, klicken Sie auf **Testabfrage für Sichtungssuche generieren**und geben eine Liste erkennbarer Elemente an, um eine Testabfrage basierend auf dieser gespeicherten Suchkonfiguration zu generieren.

Playbook-Ressourcen

Security Incident Response bietet eine Fülle von Playbook-Ressourcen, darunter eine umfangreiche Bibliothek mit Playbooks, Subflows und Aktionen. Sie können Playbooks schnell und einfach erstellen oder konfigurieren, ohne komplizierten Code zu schreiben. Sie können diese Playbooks verwenden, um Sicherheitsbedrohungen schrittweise zu beheben.

Playbook-Ressourcen umfassen Folgendes:

Security Incident Response Playbooks	Playbook-Aktionen für Security Incident Response
Die mit dem Basissystem bereitgestellten Playbooks sollen den Prozess der Untersuchung von Security Incidents	Komplexe Aktionen, die für die Erstellung von Playbooks von entscheidender Bedeutung sind, sind als **Aktionsbibliotheken**verfügbar. Mit diesen Aktionsbibliotheken können Sicherheitsadministratoren Playbooks erstellen,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response Playbooks	Playbook-Aktionen für Security Incident Response
durch die Automatisierung komplexer und alltäglicher Aufgaben beschleunigen. Playbooks sind hochgradig konfigurierbar und werden mit der Flow Designer-Technologie von ServiceNow erstellt. Kopieren Sie zum Konfigurieren das mit dem Basissystem bereitgestellte Playbook, und ändern Sie es mithilfe der einfachen grafischen Drag-and-Drop-Schnittstelle. Weitere Informationen finden Sie unter Security Incident Response Playbooks.	ohne komplizierten Code zu schreiben. Weitere Informationen finden Sie unter Playbook-Aktionen für Security Incident Response.

Aktivieren Sie einen Security Incident Response -Flow

Sicherheitsadministratoren und Flow-Designer können die -Flows Security Incident Response verwenden, um den Prozess der Lösung von Security Incidents in der Organisation zu automatisieren.

Vorbereitungen

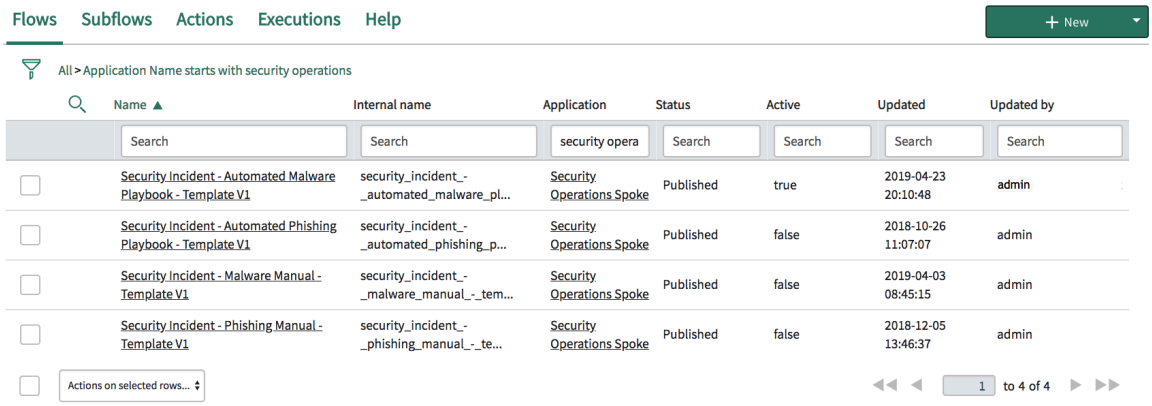
Erforderliche Rolle: sn_si.admin, action_designer und flow_designer

Warum und wann dieser Vorgang ausgeführt wird

Die mit dem Basissystem bereitgestellten Flows befinden sich in einem inaktiven Status. Aktivieren Sie diese Flows, bevor Sie sie verwenden.

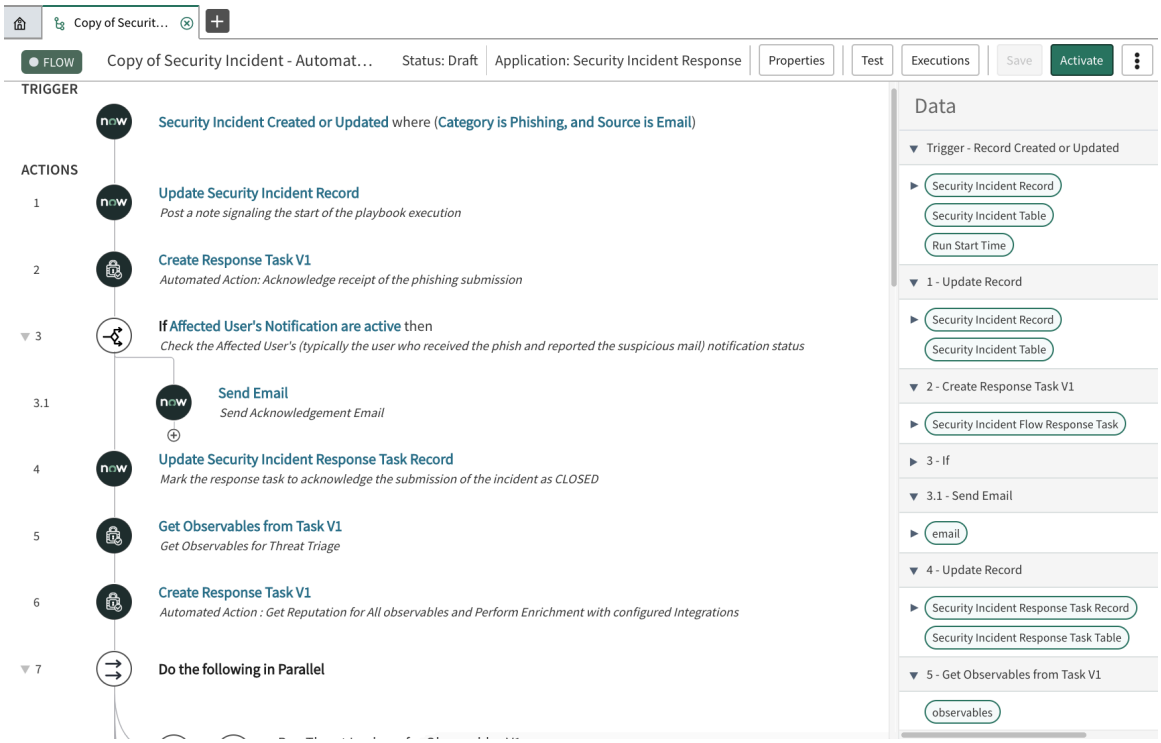
Prozedur

1. Laden Sie die Anwendung Security Operations Spokeherunter, und installieren Sie sie.
   Diese Spoke-Anwendung bietet Security Operations-Aktionen, die Sie beim Definieren Security Incident Response von -Flows verwenden können.
2. Navigieren zu **Flow Designer** > **Designer** und suchen Sie nach der Anwendung Security Operations Spoke, um die Flows im Zusammenhang mit Security Incidents anzuzeigen.
   Beachten Sie, dass



   den Status „Veröffentlicht“ aufweisen und inaktiv sind.
3. Wenn Sie beispielsweise den Flow „Automated Malware Playbook“ aktivieren möchten, klicken Sie auf den Link **Security Incident – Automated Phishing Playbook – Template V1 (Security Incident – Automated Phishing Playbook – Template V1),** um den Flow anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Sie können die mit dem Basissystem bereitgestellten Flows nicht bearbeiten, da es sich um schreibgeschützte Flows handelt. Sie können diese Flows unverändert verwenden oder eine Kopie erstellen und sie nach Bedarf ändern.

4. Klicken Sie auf **Aktivieren**, um den Flow zu aktivieren.

Ergebnisse
Der Playbook-Flow für automatisiertes Phishing ist aktiv und kann verwendet werden.

Security Incident Response Playbooks

Sie können den Playbook-Flow für Security Incidents automatisch oder manuell aufrufen.

Ein Playbook ist nur sichtbar, wenn einem Security Incident mindestens ein Playbook zugeordnet ist. Die Playbook-Komponente funktioniert nur für die von Process Automation Designer (PAD) erstellten Prozesse und nicht für die vom Flow Designer erstellten Flows. Für die vorhandenen Flow Designer-fähigen Flows funktioniert es weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Security Incident Response unterstützt zwei Arten von Playbooks:

- Prozessbasierte Playbooks
- Flow-basierte Playbooks

Zusätzlich zu den aufgeführten Playbooks gibt es in der Security Operations-Spoke auch Subflows, die über das Flows-Playbook aufgerufen werden können. Ransomware ist einer dieser Subflows.

Aktivieren Sie diese Flows, bevor Sie sie verwenden. Weitere Informationen hierzu finden Sie unter Flows für Security Incident Response aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozessbasierte Playbooks

Die Playbook-Komponente funktioniert nur für Playbooks, die in Workflow-Studio erstellt wurden, und nicht für Flows. Vorhandene Flow-basierte Playbooks funktionieren jedoch weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Security Incident Response stellt die folgenden Playbooks mit dem Basissystem bereit.

Playbook für manuelles Phishing

Das Playbook für manuelles Phishing bietet Ihren Analysten eine Schritt-für-Schritt-Anleitung, wie sie bestimmte Arten von Sicherheitsbedrohungen für Ihre Phishing-Aktivitäten manuell beheben können.

Übersicht

Die Vorlage „Manuelles Phishing-Playbook“ dient zum manuellen Ausführen der Phishing-Antwortaufgaben und enthält eine Folge von Aktionen einschließlich Auslöserbedingungen. Sie können die PAD-Vorlagen verwenden, um die Schritte im Playbook zur Reaktion auf Phishing auszuführen und diese Incidents effizient zu lösen.

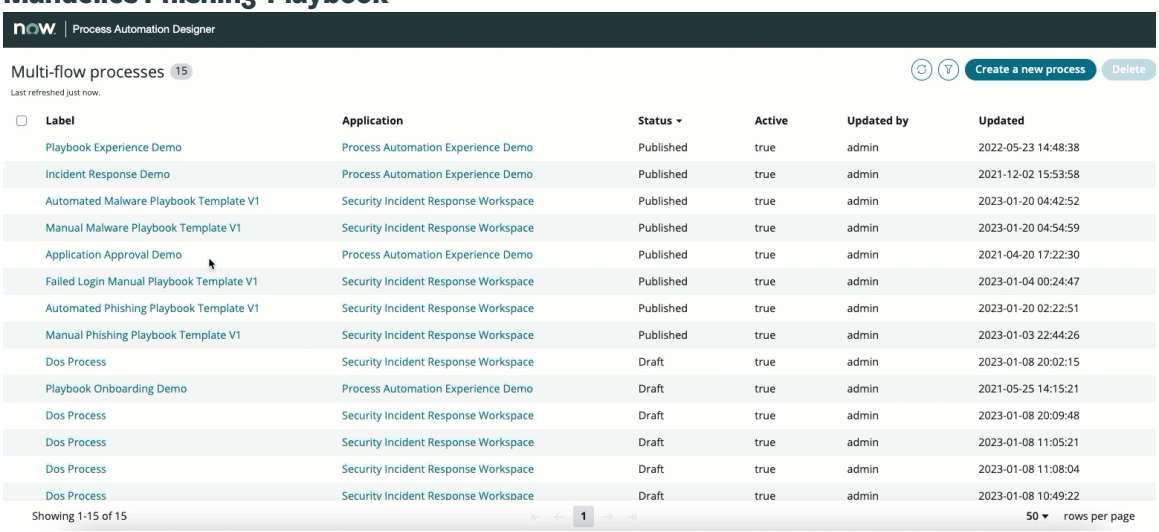
Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das Playbook für manuelles Phishing im Prozessautomatisierungs-Designer (PAD) aktivieren und dann alle Aufgaben ausführen, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incident:

- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Manuelles Phishing-Playbook



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt (Datum und Uhrzeit) zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für die jeweilige Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die in allen Phasen eingegebenen Details zu überprüfen. Sie können jedes Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Playbooks für manuelles Phishing in Workflow-Studio

Führen Sie diese Schritte aus, um Playbooks für manuelles Phishing in Workflow-Studiozu erstellen.

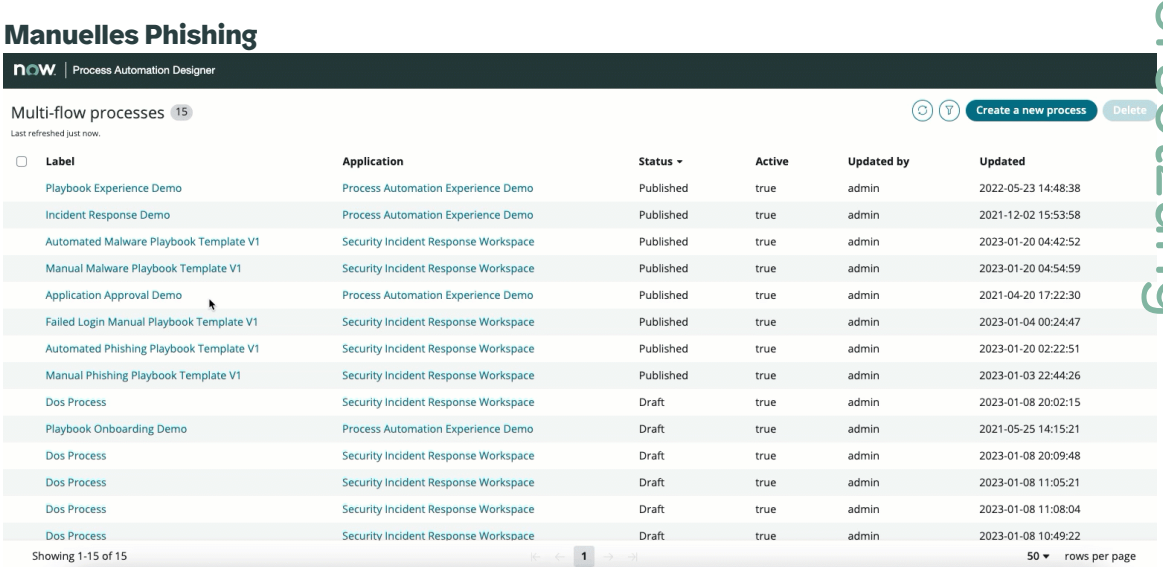
Vorbereitungen
Erforderliche Rolle: sn_si.admin oder sn_si.manager

Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Neu** und wählen Sie **Playbook**aus.

   Beispiel: Vorlage für manuelles Phishing-Playbook V1.

2. Geben Sie einen Namen für das Playbook, eine Beschreibung und die Anwendung ein, für die das Playbook erstellt wird.
3. Klicken Sie auf **Auslöser auswählen**.
4. Wählen Sie **Eigene Bedingungen für die Ausführung Ihres Prozesses definieren aus**, und wählen Sie die Auslöserbedingung für die Ausführung Ihres Playbooks aus.
5. Klicken Sie auf **Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Playbook ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslösebedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.



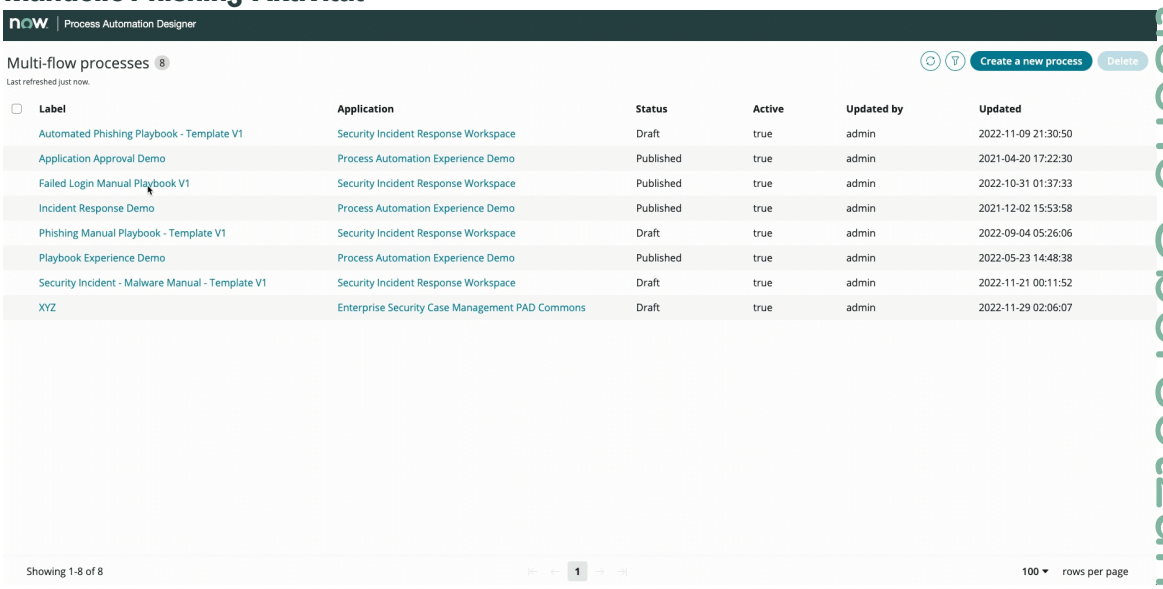
7. Klicken Sie auf **Zum Designer wechseln**.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie **auf Neue Phase hinzufügen**.
   Der Bereich mit den Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Geben Sie im Bereich mit den Stufeneigenschaften die folgenden Details ein: **Name**, **Beschreibung**, **Ausführungsbedingung**und **Startzeitpunkt angeben**.
   Die Felder **Bedingung für das Ausführen** und **Geben Sie an, wann gestartet werden** soll geben an, wann die Phase ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Weitere Phase hinzufügen**.
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie jeweils eine Phase für Analyse, Eindämmen, Beseitigen und Überprüfen erstellen. Im folgenden Beispiel startet die Phase **Analyse** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Phasenstart, nachdem die vorherige Phase abgeschlossen ist, und verfügt über eine Ausführungsbedingung, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nachdem Sie die Phasen hinzugefügt haben, müssen Sie für jede Phase Prozessaktivitäten hinzufügen.
12. Klicken Sie unter einer bestimmten Phase (z. B. Analysephase) **auf Weitere Aktivität hinzufügen**.
    Das Popup-Fenster „Aktivität hinzufügen“ wird geöffnet.
    a. Wählen Sie im Popup-Fenster „Aktivität hinzufügen“ die gewünschte Aktivitätsdefinition aus.
13. Klicken Sie auf **Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen konfiguriert werden. Auf ähnliche Weise können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

Manuelle Phishing-Aktivität



14. Fügen Sie im Bereich Aktivitätseigenschaften eine Ausführungsbedingung hinzu, und geben Sie an, wann die Aktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) wird angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie **auf Alle Eigenschaften anzeigen** und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Fügen Sie parallele Aktivitäten hinzu

Wenn das Feld **Startzeitpunkt** auf **Mit vorherigem**festgelegt ist, können parallele Aktivitäten initiiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Wechseln von einer Phase zur nächsten Phase

Wenn keine Ausführungsbedingung definiert ist, werden die Phasen und Aktivitäten nacheinander ausgeführt.

Mit der Ausführungsbedingung können Sie Aktivitäten oder Phasen überspringen. In diesem Beispiel **beginnt die Phase „Eindämmen", wenn das Ergebnis von „Hat die E-Mail Bedrohungsindikatoren?" angezeigt wird. ist Ja**.

Um von einer Phase zu einer anderen zu wechseln, können Sie die von der Plattform bereitgestellte **Aktivitätsdefinition „Update Record" (Datensatz aktualisieren)**verwenden. Dadurch wird das Statusfeld des Security Incidents aktualisiert und die Playbook-Ausführung wird mit der nächsten Phase fortgesetzt.

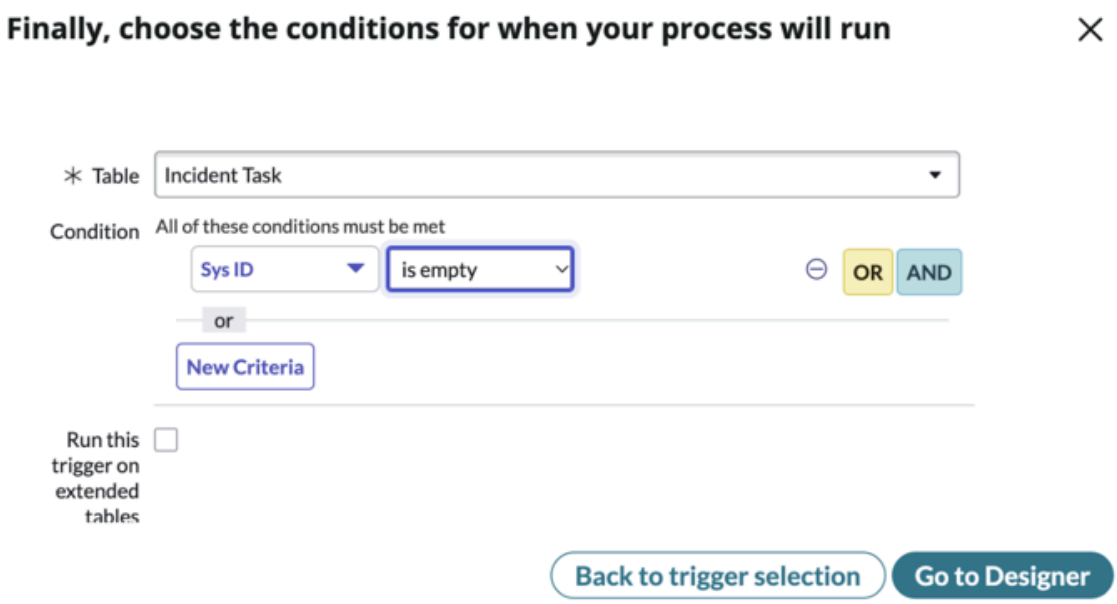
Die Herausforderung bei dieser Aktivitätsdefinition besteht jedoch darin, dass, wenn sich das Playbook in der Analysephase befindet und der Anwender den Status manuell auf „Überprüfung" aktualisiert hat, die Aktivität „Datensatz aktualisieren" den Status erneut in „Eindämmen" ändert, um das Playbook fortzusetzen Ausführung. Dadurch wird die vorgenommene manuelle Änderung überschrieben.

Um dies zu beheben, wird im Basissystem eine Aktivitätsdefinition namens **„Aufgabenstatus aktualisieren"** bereitgestellt. Diese Aktivität überschreibt den Status des Security Incidents nicht, wenn der aktuelle Sicherheitsstatus der Phase im Playbook vorausgeht.

Erstellen Sie eine Prozessdefinition mit einer Dummy-Auslöserbedingung

Eine Prozessdefinition erfordert immer eine Auslöserbedingung. Wenn Sie jedoch nicht sicher sind, wann der Prozess ausgelöst werden soll, können Sie trotzdem eine Prozessdefinition mit einer Dummy-Auslöserbedingung erstellen. Legen Sie die Auslöserbedingung fest, da **„sys_id" leer ist**. Diese Bedingung wird niemals erfüllt.

Prozessbedingungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mithilfe des Playbooks für manuelles Phishing

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook für manuelles Phishing im SIR-Analystenarbeitsbereich und seine Funktionen verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

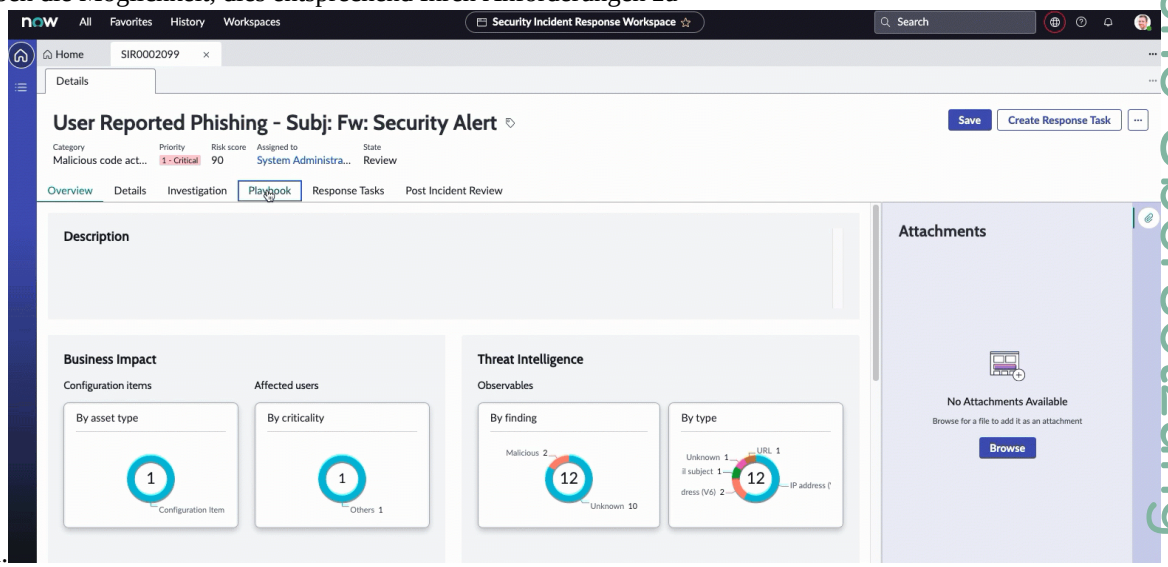
Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

   Hinweis:
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie auf der Registerkarte **„Playbook“** aktivieren, um sie anzuzeigen.

3. Klicken Sie auf das **Playbook für manuelles Phishing**.
4. Klicken Sie auf jede Phase, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen. Sie haben die Möglichkeit, dies entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase durchgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn Sie noch Aktivitäten oder Anwenderaktionen ausführen müssen, werden sie in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch Aktivitäten oder Anwenderaktionen erforderlich sind, klicken Sie auf die entsprechende Phase und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Playbook-Zusammenfassung für den Arbeitsbereich

Im Folgenden wird die Prozesszusammenfassung beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verstehen Sie das Flow-basierte Legacy-Playbook.
- Listen Sie mögliche Aktivitäten und Phasen nach der Analyse des Flows auf. Suchen Sie nach den Schritten, in denen eine echte Orchestrierung erstellt werden kann.
- Nehmen Sie jede Aktivität vor und überprüfen Sie, ob die vom Basissystem bereitgestellte Aktivitätsdefinition den Anwendungsfall erfüllen kann oder nicht.
- Listen Sie Aktivitätsanwendungsfälle auf, für die neue Aktivitätsdefinitionen implementiert werden müssen. Klassifizieren Sie sie: interaktiv, nicht interaktiv oder automatisiert. So erstellen Sie eine Aktivitätsdefinition:
  - Erstellen Sie einen Subflow oder eine Aktion für den Anwendungsfall.
  - Entscheiden Sie, ob die zugeordneten Daten in einer Flow-Datentabelle oder in einer anwenderdefinierten Tabelle erfasst werden müssen.
  - Wenn Sie eine Flow-Datentabelle verwenden, erstellen Sie eine Flow-Datendefinition in **sys_flow_data_definition**. Wählen Sie beim Erstellen eines Flow-Datensatzes im Subflow die erstellte Flow-Datendefinition aus.
  - Erstellen Sie eine **Aktivitätsdefinition**.
  - Ordnen Sie den Automatisierungsplan zu.
  - Füllen Sie die Eigenschaften **für die Aktivitäts-Experience** aus.
  - Erstellen Sie eine Aktion unter Playbook-Aktionen. Es muss eine Aktivitätsaktion vorhanden sein, um sie der Aktivitätsdefinition zuzuweisen.
  - Um die Standardkarten-Experience basierend auf dem ausgewählten Experience-Typ zu überschreiben, fügen Sie die Playbook-Überschreibung mithilfe des Aktivitäts-UI-Konzepts hinzu.
- Einige Aktivitäten können mit der Kennzeichnung „Auf Benutzereingabe warten“ im Subflow sowohl automatisch als auch interaktiv behandelt werden. Diese Eingabe kann während der Konfiguration der Aktivität in der Prozessdefinition übergeben werden.
- Nachdem Sie alle für Ihren Prozess erforderlichen Aktivitätsdefinitionen erstellt haben, beginnen Sie mit der Erstellung der Prozessdefinition mithilfe von Workflow-Studio.

Playbook für automatisiertes Phishing

Das Playbook für automatisiertes Phishing bietet Ihren Analysten eine Schritt-für-Schritt-Anleitung, wie sie bestimmte Arten von Sicherheitsbedrohungen in Ihren automatisierten Phishing-Aktivitäten beheben können.

Übersicht

Die Playbook-Vorlage für automatisiertes Phishing wurde zur Automatisierung der Phishing-Antwortaufgaben entwickelt und enthält eine Folge von Aktionen einschließlich Auslöserbedingungen. Sie können die Playbook-Vorlagen in Workflow-Studio verwenden, um die Schritte im Playbook zur Reaktion auf Phishing zu automatisieren und diese Incidents effizient zu lösen. Diese Playbook-Vorlage enthält eine Reihe von wiederverwendbaren Aktionen, mit denen Sie auf Phishing-Angriffe reagieren können. Jeder Flow hat einen Auslöser (Bedingung), eine Folge von Aktionen und Subflows, die Sie kommentieren können.

In diesem Playbook findet keine Benutzerinteraktion statt, wenn die Kategorie eines Security Incident auf Phishing festgelegt ist. Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das Playbook für automatisiertes Phishing in Workflow-Studioaktivieren. Dieses Playbook führt automatisch alle Aufgaben aus, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

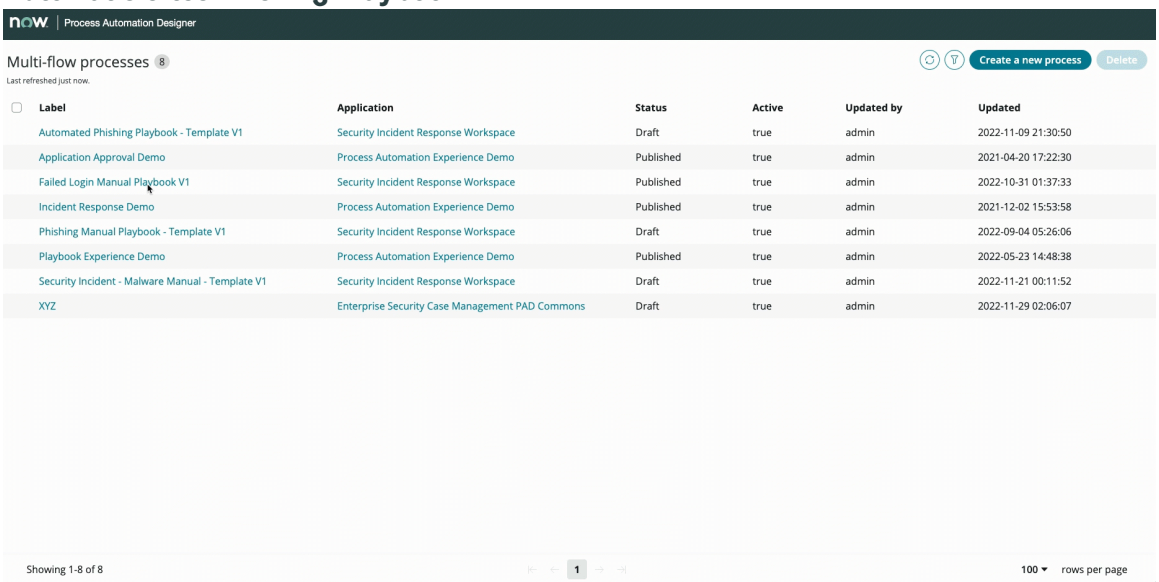
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incident:

- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatisiertes Phishing-Playbook



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt (Datum und Uhrzeit) zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für die jeweilige Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die in allen Phasen eingegebenen Details zu überprüfen. Sie können jedes Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für automatisiertes Phishing in PAD

Führen Sie diese Schritte aus, um Prozesse für automatisiertes Phishing im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

Prozedur

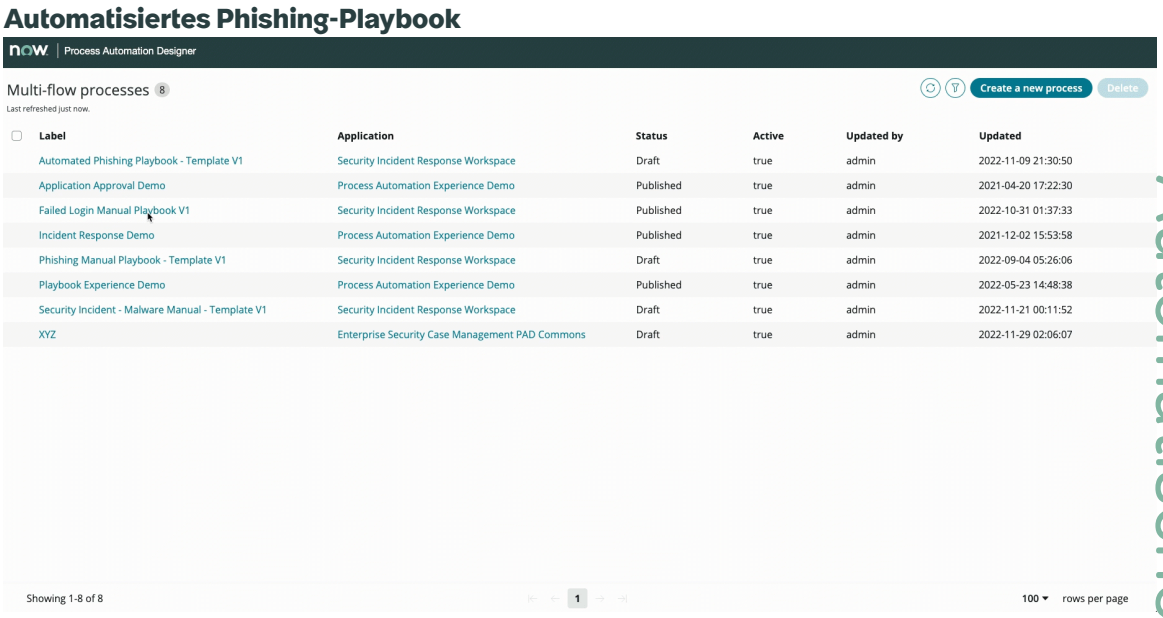
1. Klicken **ALLE** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**.

   Beispiel: Playbook-Vorlage für automatisiertes Phishing V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Auslöser auswählen**.
4. Wählen Sie **Eigene Bedingungen für die Ausführung Ihres Prozesses definieren aus**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken Sie auf **Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslösebedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.



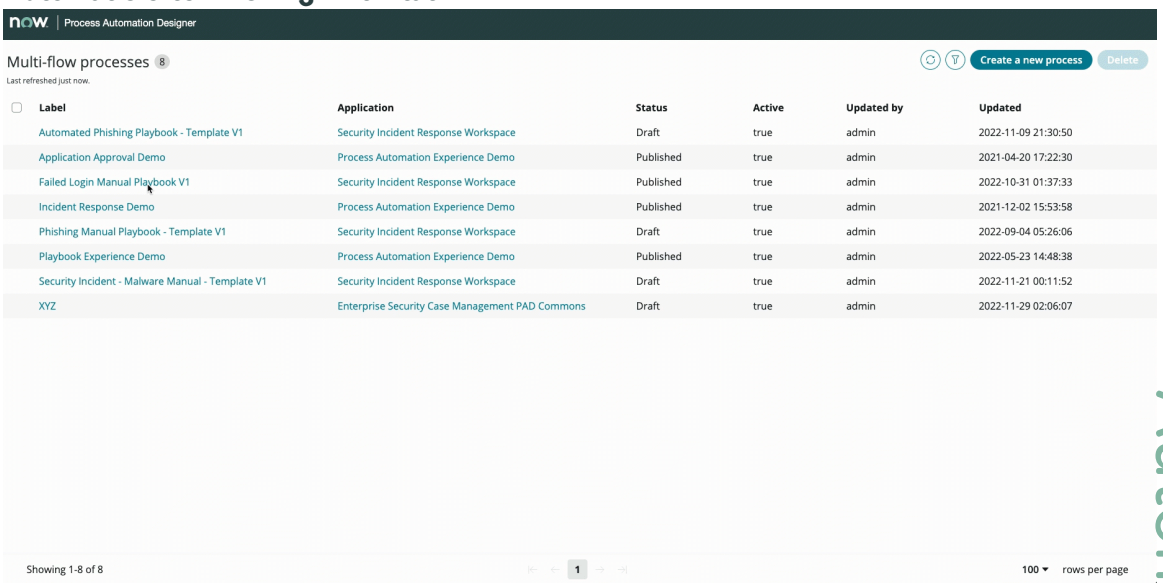
7. Klicken Sie auf **Zum Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie **auf Neue Phase hinzufügen**.
   Der Bereich mit den Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich mit den Stufeneigenschaften die folgenden Details ein: **Name**, **Beschreibung**, **Ausführungsbedingung**und **Startzeitpunkt angeben**.
   Die Felder **Bedingung für das Ausführen** und **Geben Sie an, wann gestartet werden** soll geben an, wann die Phase ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Weitere Phase hinzufügen**.
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie jeweils eine Phase für Analyse, Eindämmen, Beseitigen und Überprüfen erstellen. Im folgenden Beispiel startet die Phase **Analyse** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Phasenstart, nachdem die vorherige Phase abgeschlossen ist, und verfügt über eine Ausführungsbedingung, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nachdem Sie die Phasen hinzugefügt haben, müssen Sie für jede Phase Prozessaktivitäten hinzufügen.
12. Klicken Sie auf **Weitere Prozessaktivität hinzufügen** unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster „Aktivität hinzufügen“ wird geöffnet.
    a. Wählen Sie im Popup-Fenster „Aktivität hinzufügen“ die gewünschte Aktivitätsdefinition aus.
13. Klicken Sie auf **Neue Aktivität erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen konfiguriert werden. Auf ähnliche Weise können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

Automatisierte Phishing-Aktivität



14. Fügen Sie im Bereich Aktivitätseigenschaften eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) wird angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie **auf Alle Eigenschaften anzeigen** und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mithilfe des Playbooks für automatisiertes Phishing

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook für automatisiertes Phishing im SIR-Analystenarbeitsbereich und seine Funktionen verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

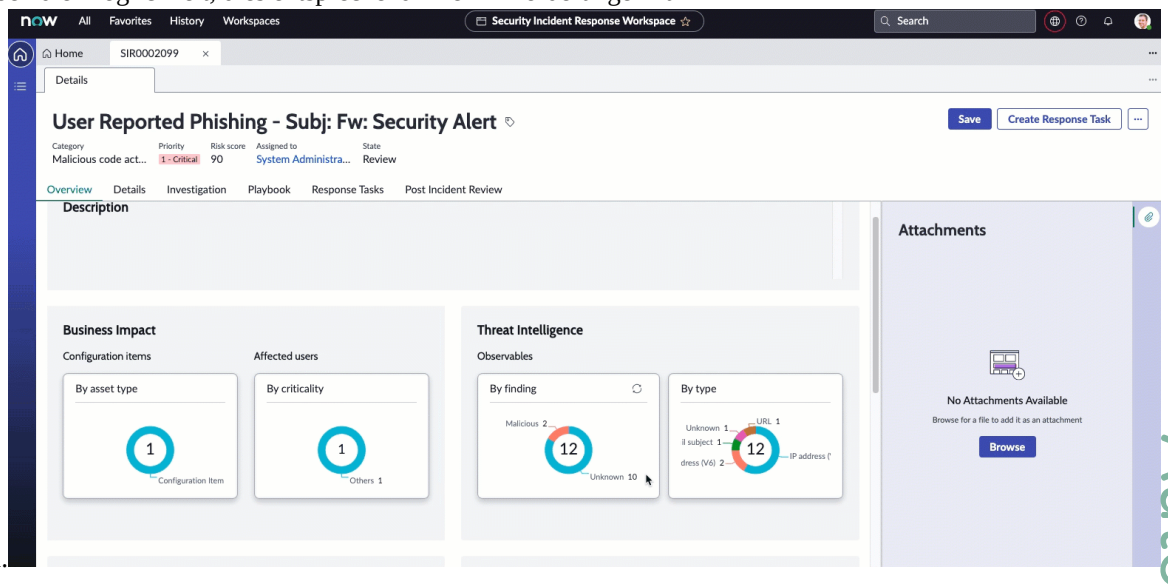
   Hinweis:
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie auf der Registerkarte **„Playbook“** aktivieren, um sie anzuzeigen.

3. Klicken Sie auf das **Playbook für automatisiertes Phishing**.
   Beim automatisierten Phishing werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Phase, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen. Sie haben die Möglichkeit, dies entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase durchgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn Sie noch Aktivitäten oder Anwenderaktionen ausführen müssen, werden sie in der entsprechenden Phase angezeigt.

7. Wenn in einer der Phasen noch Aktivitäten oder Anwenderaktionen erforderlich sind, klicken Sie auf die entsprechende Phase und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Playbook für manuelle Malware

Das Playbook zu manueller Malware bietet Schritt-für-Schritt-Anleitungen, wie Analysten manuelle Malware-Warnungen effizienter lösen können.

Mit der Playbook-Vorlage „Manuelle Malware“ können Sie die Schritte zur Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk manuell ausführen. Sie können die Playbook-Vorlagen in Workflow-Studio verwenden, um die Schritte im Playbook zu manueller Malware auszuführen und diese Warnungen effizient zu lösen. Dieses Playbook enthält Auslöserbedingungen, eine Folge von Aktionen und Subflows, die Sie kommentieren können. Dieses Playbook enthält eine Reihe von wiederverwendbaren Aktionen, mit denen Sie auf Malware-Angriffe reagieren können. Jeder Flow hat einen Auslöser (Bedingung), eine Folge von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn Malware erstellt oder aktualisiert wird. Sie müssen das Playbook für manuelle Malware in Workflow-Studio aktivieren und alle Aufgaben erstellen, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status der Malware-Warnung:

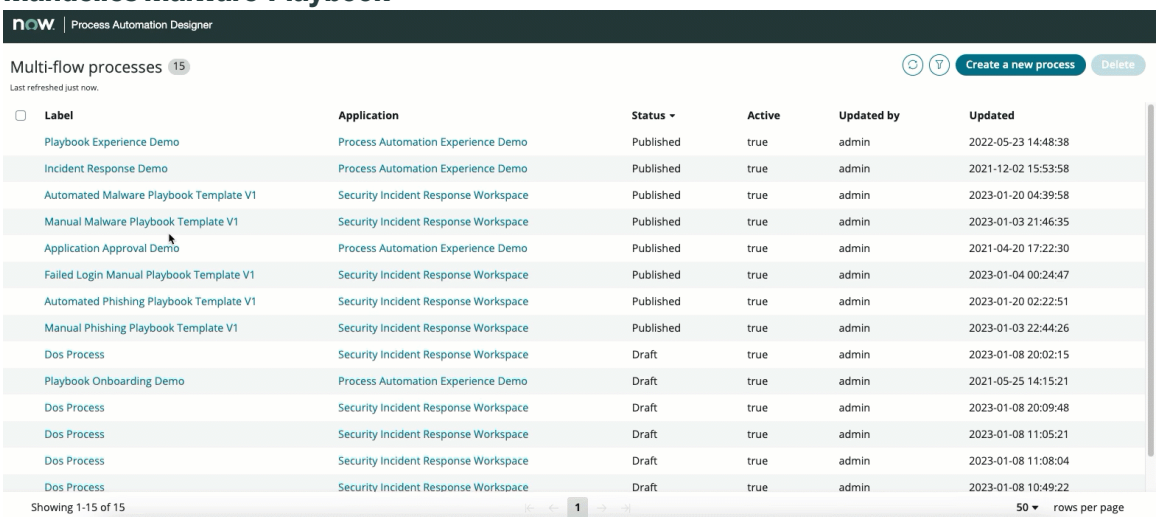
- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Manuelles Malware-Playbook



Nachdem Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt (Datum und Uhrzeit) zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für die jeweilige Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die in allen Phasen eingegebenen Details zu überprüfen. Sie können jedes Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für manuelle Malware in PAD

Führen Sie diese Schritte aus, um Prozesse für manuelle Malware im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

Prozedur

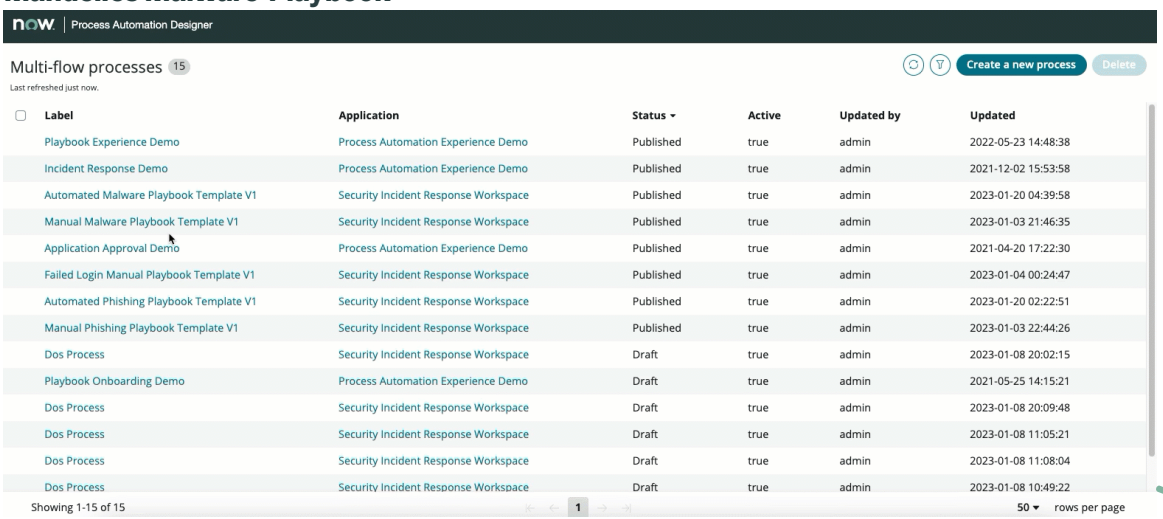
1. Klicken **ALLE** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**.

   Beispiel: Vorlage für manuelles Malware-Playbook V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie auf **Auslöser auswählen**.
4. Wählen Sie **Eigene Bedingungen für die Ausführung Ihres Prozesses definieren aus**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken Sie auf **Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslösebedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.

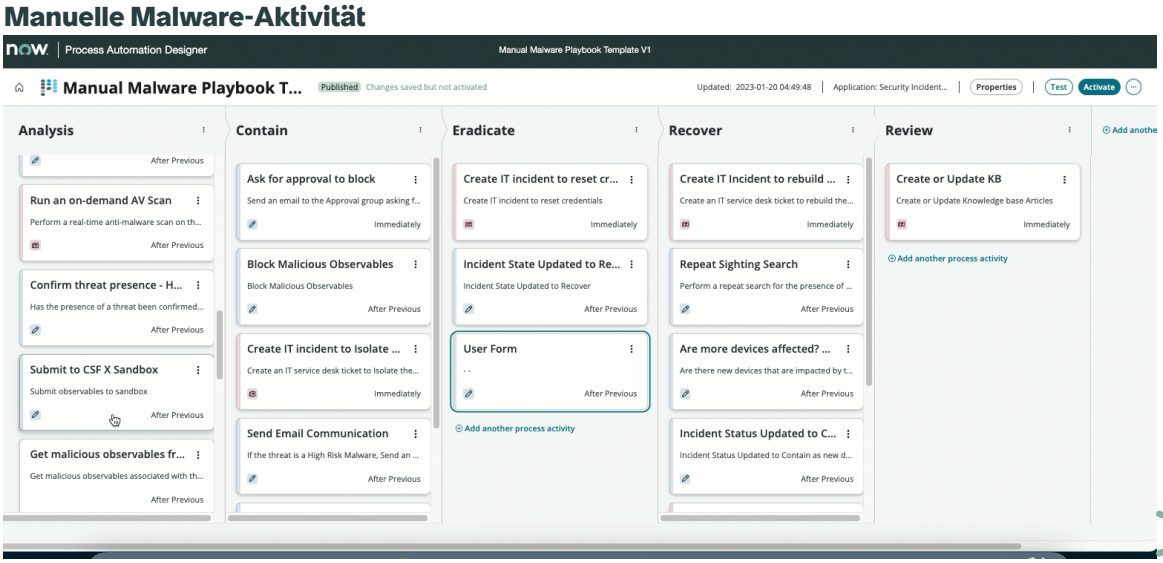
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Manuelles Malware-Playbook



7. Klicken Sie auf **Zum Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie **auf Neue Phase hinzufügen**.
   Der Bereich mit den Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich mit den Stufeneigenschaften die folgenden Details ein: **Name**, **Beschreibung**, **Ausführungsbedingung**und **Startzeitpunkt angeben**.
   Die Felder **Bedingung für das Ausführen** und **Geben Sie an, wann gestartet werden** soll geben an, wann die Phase ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Weitere Phase hinzufügen**.
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie jeweils eine Phase für Analyse, Eindämmen, Beseitigen und Überprüfen erstellen. Im folgenden Beispiel startet die Phase **Analyse** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Phasenstart, nachdem die vorherige Phase abgeschlossen ist, und verfügt über eine Ausführungsbedingung, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nachdem Sie die Phasen hinzugefügt haben, müssen Sie für jede Phase Prozessaktivitäten hinzufügen.
12. Klicken Sie auf **Weitere Prozessaktivität hinzufügen** unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster „Aktivität hinzufügen“ wird geöffnet.
    a. Wählen Sie im Popup-Fenster „Aktivität hinzufügen“ die gewünschte Aktivitätsdefinition aus.
13. Klicken Sie auf **Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen konfiguriert werden. Auf ähnliche Weise können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



14. Fügen Sie im Bereich Aktivitätseigenschaften eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) wird angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie **auf Alle Eigenschaften anzeigen** und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mithilfe des Playbooks für manuelle Malware

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook für manuelle Malware im SIR-Analystenarbeitsbereich und seine Funktionen verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

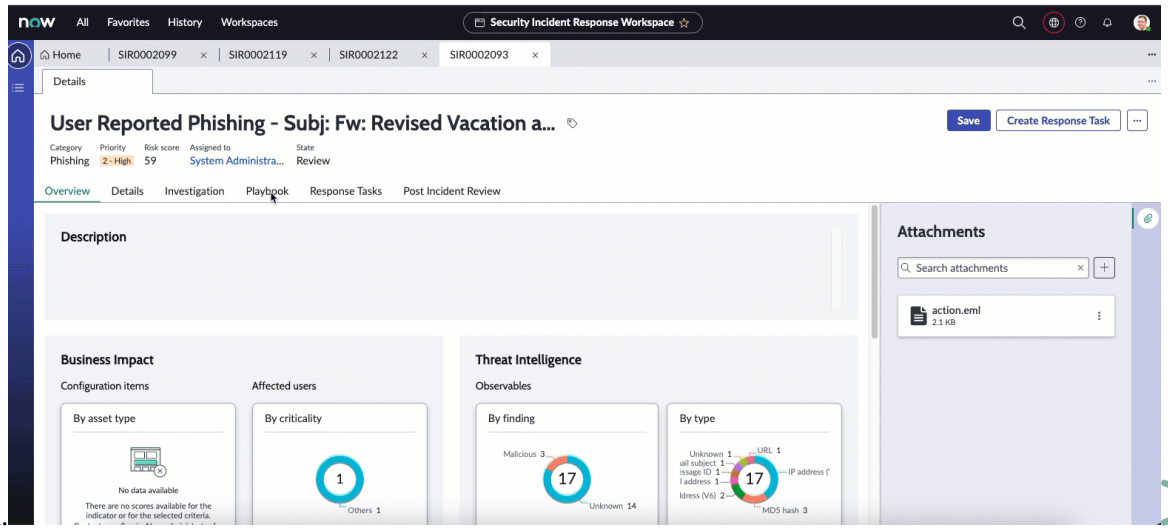
   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

   Hinweis:
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie auf der Registerkarte **„Playbook“** aktivieren, um sie anzuzeigen.

3. Klicken Sie auf das **Manuelles Malware-Playbook**.
   Bei manueller Malware werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Phase, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, dies entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase durchgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn Sie noch Aktivitäten oder Anwenderaktionen ausführen müssen, werden sie in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch Aktivitäten oder Anwenderaktionen erforderlich sind, klicken Sie auf die entsprechende Phase und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Playbook für automatisierte Malware

Das Automated Malware Playbook bietet eine Reihe von automatisierten Schritten, mit denen Analysten Malware-Warnungen effizienter lösen können.

Die Playbook-Vorlage für Automated Malware wurde entwickelt, um die Schritte zur Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk zu automatisieren. Sie können die Playbook-Vorlagen in Workflow-Studio verwenden, um die Schritte im Playbook für automatisierte Malware zu automatisieren und diese Warnungen effizient zu lösen. Dieses Playbook enthält Auslöserbedingungen, eine Folge von Aktionen und Subflows, die Sie kommentieren können. Dieses Playbook enthält eine Reihe von wiederverwendbaren Aktionen, mit denen Sie auf Malware-Angriffe reagieren können. Jeder Flow hat einen Auslöser (Bedingung), eine Folge von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das Playbook für automatisierte Malware in Workflow-Studioaktivieren. Dieses Playbook führt automatisch alle Aufgaben aus, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incident:

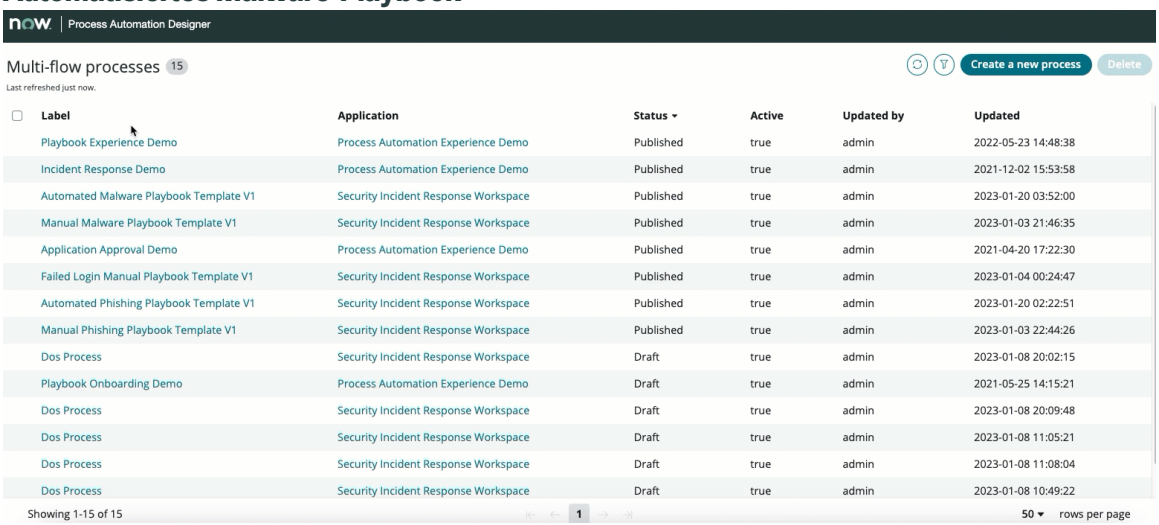
- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisiertes Malware-Playbook



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt (Datum und Uhrzeit) zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für die jeweilige Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die in allen Phasen eingegebenen Details zu überprüfen. Sie können jedes Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für automatisierte Malware in PAD

Führen Sie diese Schritte aus, um Prozesse für automatisierte Malware im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

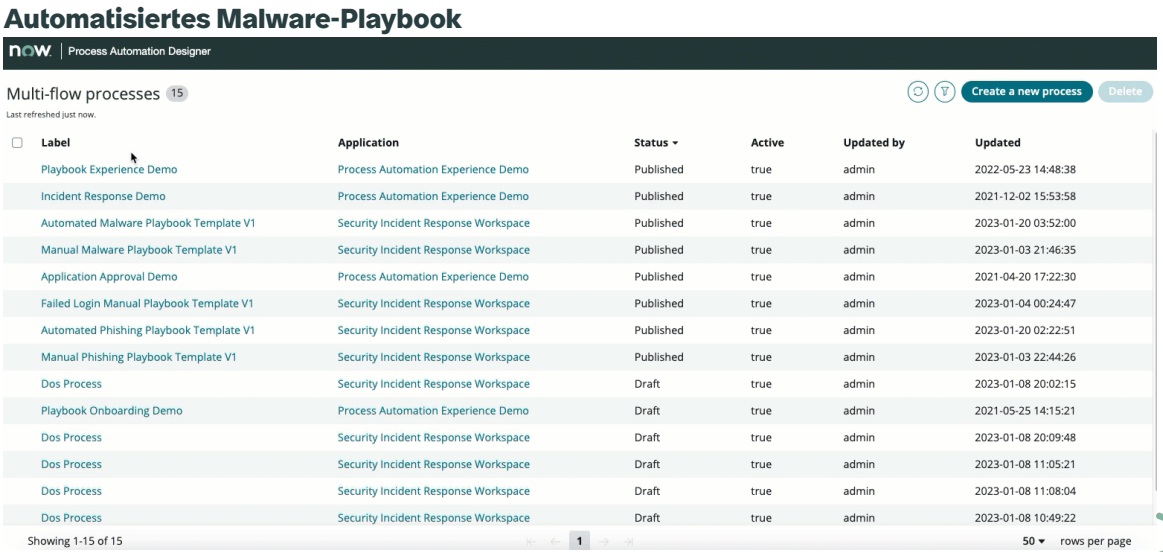
Prozedur

1. Klicken **ALLE** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**.

   Beispiel: Automated Malware Playbook Template V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie auf **Auslöser auswählen**.
4. Wählen Sie **Eigene Bedingungen für die Ausführung Ihres Prozesses definieren aus**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken Sie auf **Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslösebedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.

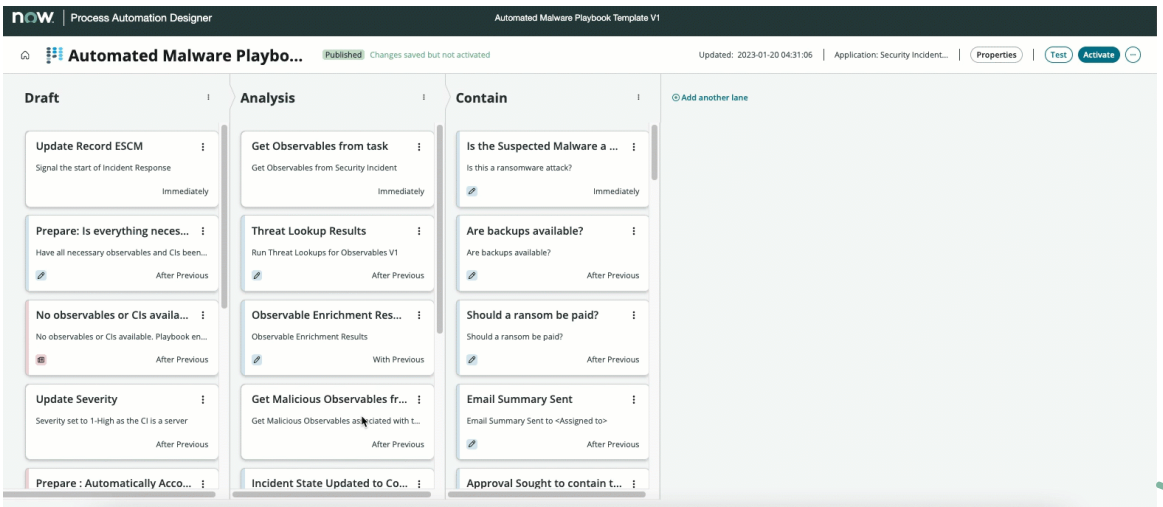
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Zum Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie **auf Neue Phase hinzufügen**.
   Der Bereich mit den Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich mit den Stufeneigenschaften die folgenden Details ein: **Name**, **Beschreibung**, **Ausführungsbedingung**und **Startzeitpunkt angeben**.
   Die Felder **Bedingung für das Ausführen** und **Geben Sie an, wann gestartet werden** soll geben an, wann die Phase ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Weitere Phase hinzufügen**.
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie jeweils eine Phase für Analyse, Eindämmen, Beseitigen und Überprüfen erstellen. Im folgenden Beispiel startet die Phase **Analyse** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Phasenstart, nachdem die vorherige Phase abgeschlossen ist, und verfügt über eine Ausführungsbedingung, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nachdem Sie die Phasen hinzugefügt haben, müssen Sie für jede Phase Prozessaktivitäten hinzufügen.
12. Klicken Sie auf **Weitere Prozessaktivität hinzufügen** unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster „Aktivität hinzufügen“ wird geöffnet.
    a. Wählen Sie im Popup-Fenster „Aktivität hinzufügen“ die gewünschte Aktivitätsdefinition aus.
13. Klicken Sie auf **Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen konfiguriert werden. Auf ähnliche Weise können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisierte Malware-Aktivität



14. Fügen Sie im Bereich Aktivitätseigenschaften eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) wird angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie **auf Alle Eigenschaften anzeigen** und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mithilfe des Playbooks für automatisierte Malware

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook für automatisierte Malware im SIR-Analystenarbeitsbereich und seine Funktionen verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

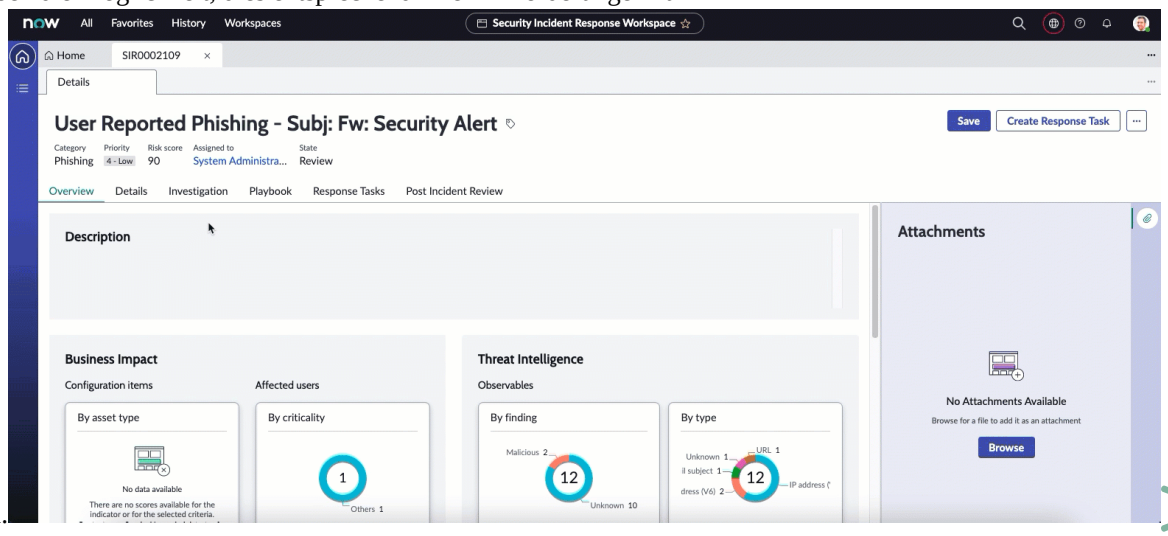
   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

   Hinweis:
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie auf der Registerkarte **„Playbook“** aktivieren, um sie anzuzeigen.

3. Klicken Sie auf das **Automated Malware Playbook**.
   Bei automatisierter Malware werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Phase, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, dies entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase durchgeführt wurden.
   Sie können sie an Ihre Anforderungen anpassen. Wenn Sie noch Aktivitäten oder Anwenderaktionen ausführen müssen, wird dies in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch Aktivitäten oder Anwenderaktionen erforderlich sind, klicken Sie auf die entsprechende Phase und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Playbook für das Handbuch für fehlgeschlagene Anmeldung

Das Playbook „Handbuch fehlgeschlagene Anmeldung“ bietet Anleitungen und hilft, die Untersuchung von Security Incidents mit fehlgeschlagener Anmeldung zu optimieren.

Wenn ein Benutzer bestimmte fehlgeschlagene Anmeldeversuche unternimmt (je nach SIM-Konfiguration), wird ein Security Incident erstellt. Diese fehlgeschlagenen Anmeldeversuche können entweder falsch positive Meldungen sein oder Versuche von Angreifern, sich Zugriff auf E-Mail-Accounts von Anwendern zu verschaffen.

Sie können die Playbook-Vorlagen in Workflow-Studio verwenden, um die Schritte im Playbook für fehlgeschlagene Anmeldungen auszuführen und Security Incidents für fehlgeschlagene Anmeldungen effizient zu beheben. Dieses Playbook enthält Auslöserbedingungen, eine Folge von Aktionen und Subflows, die Sie kommentieren können. Dieses Playbook enthält eine Reihe von wiederverwendbaren Aktionen, mit denen Sie auf Security Incidents mit fehlgeschlagener Anmeldung reagieren können. Jeder Flow hat einen Auslöser (Bedingung), eine Folge von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn ein Security Incident für eine fehlgeschlagene Anmeldung erstellt oder aktualisiert wird. Sie müssen das Playbook „Manuelles Anmeldeformular fehlgeschlagen“ in Workflow-Studio aktivieren und alle Aufgaben erstellen, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incident:

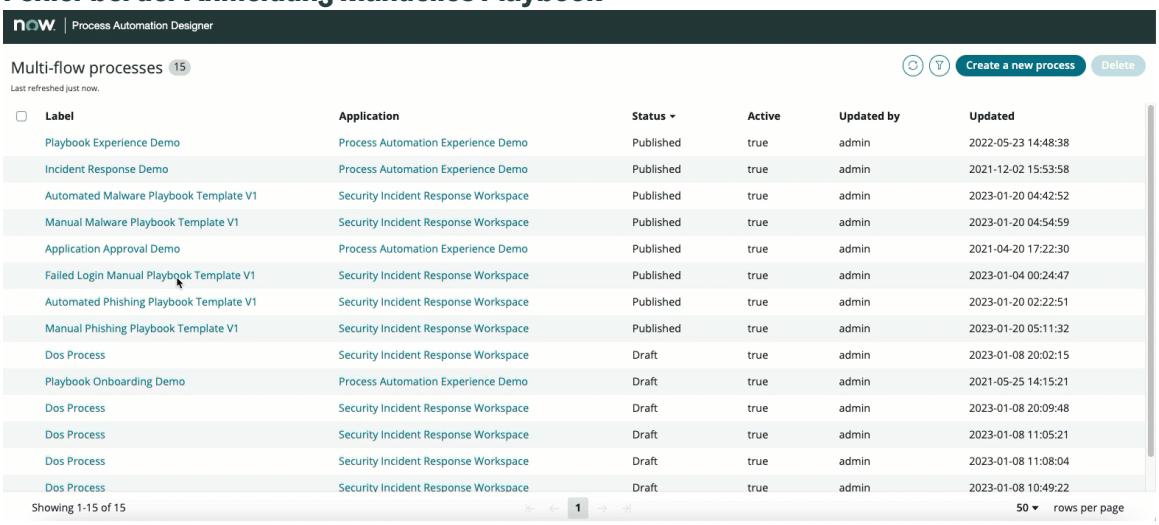
- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler bei der Anmeldung Manuelles Playbook



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt (Datum und Uhrzeit) zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für die jeweilige Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die in allen Phasen eingegebenen Details zu überprüfen. Sie können jedes Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für das Handbuch für fehlgeschlagene Anmeldung in PAD

Führen Sie diese Schritte aus, um Prozesse für das Handbuch für fehlgeschlagene Anmeldung im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

Prozedur

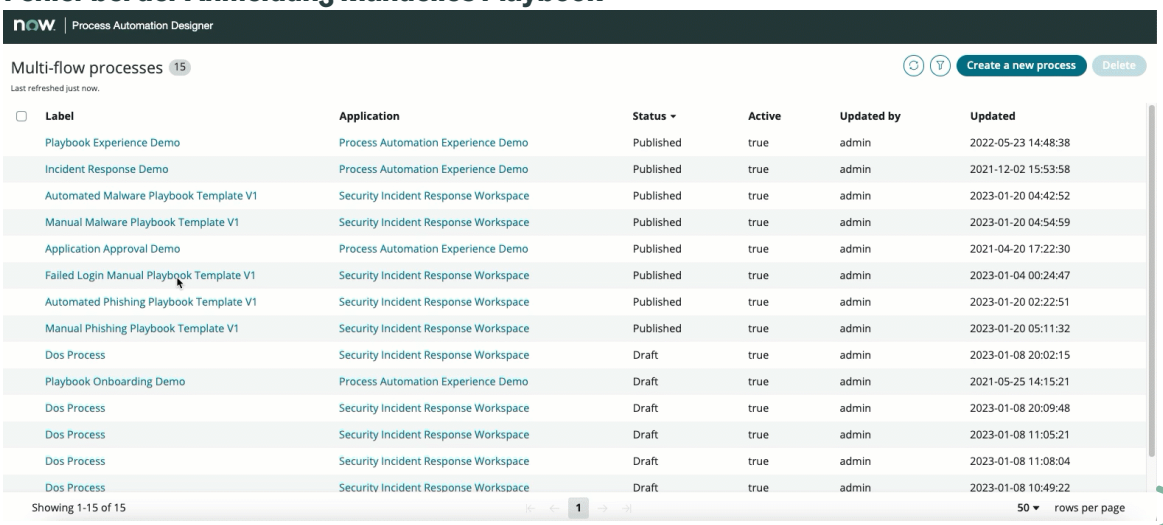
1. Klicken **ALLE** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**.

   Beispiel: Fehler bei der Anmeldung Manuelle Playbook-Vorlage V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie auf **Auslöser auswählen**.
4. Wählen Sie **Eigene Bedingungen für die Ausführung Ihres Prozesses definieren aus**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken Sie auf **Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslösebedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

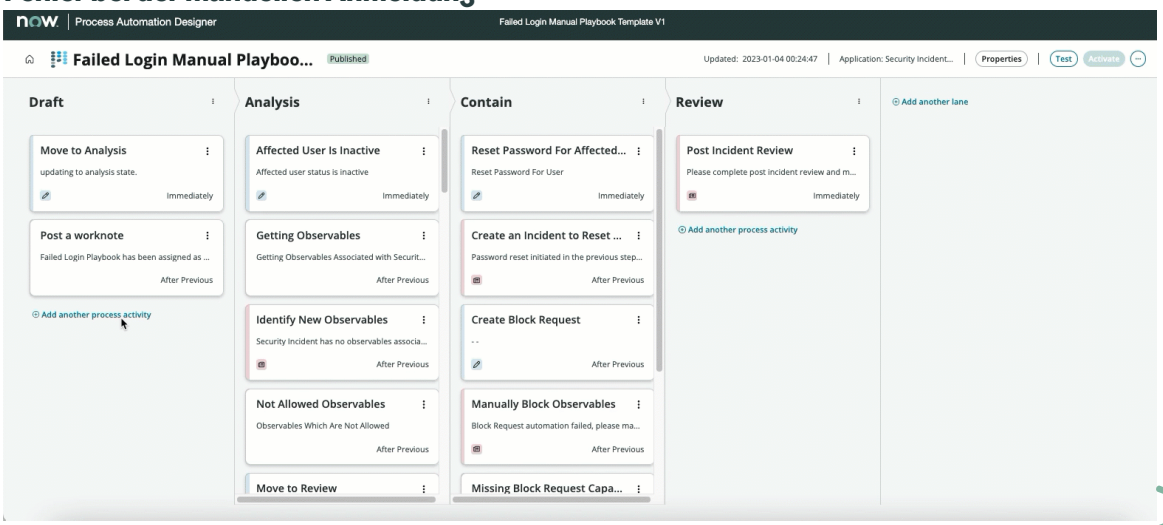
Fehler bei der Anmeldung Manuelles Playbook



7. Klicken Sie auf **Zum Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie **auf Neue Phase hinzufügen**.
   Der Bereich mit den Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich mit den Stufeneigenschaften die folgenden Details ein: **Name**, **Beschreibung**, **Ausführungsbedingung**und **Startzeitpunkt angeben**.
   Die Felder **Bedingung für das Ausführen** und **Geben Sie an, wann gestartet werden** soll geben an, wann die Phase ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Weitere Phase hinzufügen**.
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie jeweils eine Phase für Analyse, Eindämmen, Beseitigen und Überprüfen erstellen. Im folgenden Beispiel startet die Phase **Analyse** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Phasenstart, nachdem die vorherige Phase abgeschlossen ist, und verfügt über eine Ausführungsbedingung, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nachdem Sie die Phasen hinzugefügt haben, müssen Sie für jede Phase Prozessaktivitäten hinzufügen.
12. Klicken Sie auf **Weitere Prozessaktivität hinzufügen** unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster „Aktivität hinzufügen“ wird geöffnet.
    a. Wählen Sie im Popup-Fenster „Aktivität hinzufügen“ die gewünschte Aktivitätsdefinition aus.
13. Klicken Sie auf **Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen konfiguriert werden. Auf ähnliche Weise können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler bei der manuellen Anmeldung



14. Fügen Sie im Bereich Aktivitätseigenschaften eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) wird angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie **auf Alle Eigenschaften anzeigen** und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mithilfe des Playbooks „Manuelle Anmeldung fehlgeschlagen“.

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook „Manuelle Fehlgeschlagene Anmeldung“ im SIR-Analystenarbeitsbereich und seine Funktionen verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

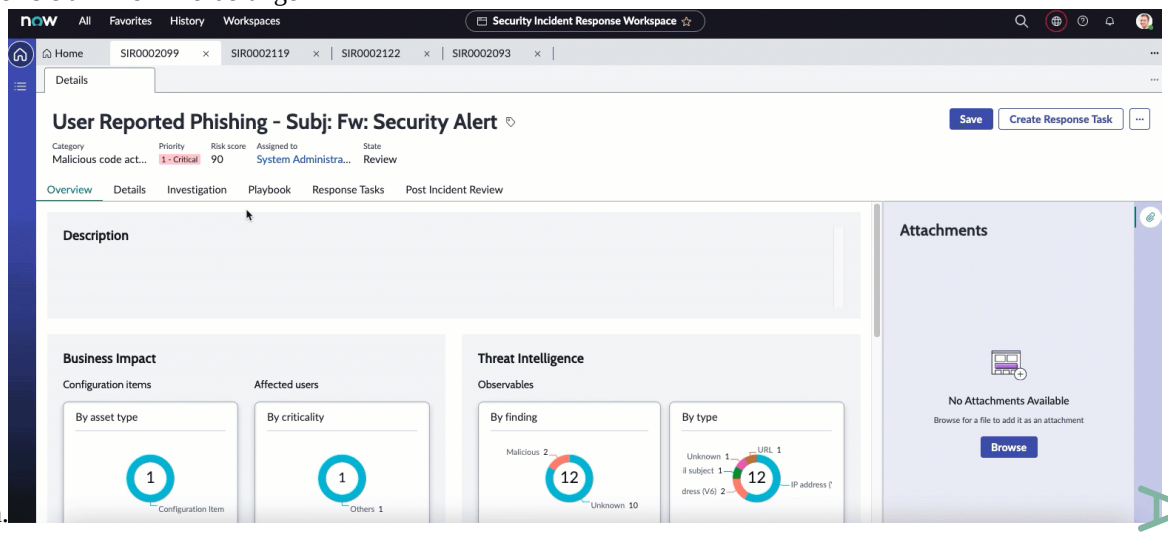
   Hinweis:
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie auf der Registerkarte **„Playbook“** aktivieren, um sie anzuzeigen.

3. Klicken Sie auf das **Playbook „Manuelle Anmeldung fehlgeschlagen“**.
   Für „Manuelle fehlgeschlagene Anmeldung“ werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Phase, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können sie an Ihre Anforderungen anpassen.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase durchgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn Sie noch Aktivitäten oder Anwenderaktionen ausführen müssen, wird dies in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch Aktivitäten oder Anwenderaktionen erforderlich sind, klicken Sie auf die entsprechende Phase und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Flow-basierte Playbooks

Mit Flow Designer können Sicherheitsadministratoren und Flow-Designautoren einfacher von manuellen oder undokumentierten Playbooks zu automatisierten und wiederholbaren Playbooks übergehen. Die Drag-and-Drop-Funktion bietet Flexibilität beim Verschieben von Objekten, Bedingungsprüfungen, parallelen Verzweigungen, Entscheidungstabellen und mehr.

Security Incident Response stellt die folgenden Playbooks mit dem Basissystem bereit.

Zusätzlich zu den aufgeführten Playbooks gibt es in der Security Operations-Spoke auch Subflows, die über das Flows-Playbook aufgerufen werden können. Ransomware ist einer dieser Subflows.

Aktivieren Sie diese Flows, bevor Sie sie verwenden. Weitere Informationen hierzu finden Sie unter Flows für Security Incident Response aktivieren.

Playbook für automatisiertes Phishing

Das Playbook für automatisiertes Phishing hilft Ihnen, bestimmte Arten von Sicherheitsbedrohungen schrittweise zu beheben. Mit den Flow Designer-Vorlagen können Sie die Schritte im Playbook zur Reaktion auf Phishing automatisieren und Incidents schnell und effizient lösen.

Sie können mit Flow Designer erstellte Vorlagen verwenden, um die Aufgaben im Playbook für die Phishing-Antwort zu automatisieren und Phishing-Angriffe in Ihrer Organisation zu analysieren und zu lösen.

Das Playbook zur Reaktion auf Phishing enthält die folgenden Flows und Subflows:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Incident – Automated Phishing Response Template: Diese Vorlage dient zur Automatisierung der Phishing-Antwortaufgaben und enthält eine Folge von Aktionen einschließlich eines Auslösers.
- Security Incident – Manuelle Phishing-Vorlage: Diese Vorlage ist der vorhandene manuelle Phishing-Antwort-Workflow. Legen Sie die Kategorie auf Phishing fest, um den Flow zu aktivieren.

Diese Vorlagen enthalten eine Reihe von wiederverwendbaren Aktionen, mit denen auf Phishing-Angriffe reagiert werden kann. Jeder Flow hat einen Auslöser (Bedingung), eine Folge von Aktionen und Subflows, die Sie zur besseren Lesbarkeit kommentieren können. Um auf diese Flows zuzugreifen, müssen Sie dieSecurity Operations-Spoke installieren.

Hinweis:
Aktivieren Sie diese Vorlagen, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter Flows für Security Incident Response aktivieren.

- Bedrohungssuchen für erkennbare Elemente ausführen: Führt Bedrohungssuchen für ausgewählte erkennbare Elemente durch.
- Erkennbare Elemente anreichern: Ermöglicht das Anreichern von erkennbaren Elementen mit zusätzlichen Informationen aus verschiedenen Quellen.
- Phishing-E-Mail-Auswirkung bewerten: Ermöglicht es Ihnen, die Auswirkungen der Phishing-E-Mail zu bewerten. Wenn Sie eine E-Mail an die Phishing-E-Mail-Adresse erhalten, analysiert dieser Subflow den EML-Anhang und vergleicht die Informationen mit den E-Mail-Übereinstimmungsregeln.
- Phishing-E-Mails beseitigen: Ermöglicht das Löschen oder Entfernen von Phishing-E-Mails, um das Risiko eines bestimmten Angriffs zu verringern.
- Sichtungssuche für erkennbare Elemente ausführen: Bestimmt die Verbreitung einer Bedrohung im Laufe der Zeit oder testet Korrektur- oder Beseitigungsmaßnahmen.
- Blockierungsanforderungen erstellen: Blockiert die Kommunikation mit erkennbaren Elementen, die dem Incident zugeordnet sind.

Diese Subflows stellen einen Satz wiederverwendbarer Vorgänge dar, die Sie in mehreren Playbooks verwenden können. Sie können diese Subflows verwenden, um anwenderdefinierte Vorlagen (Flows) gemäß Ihren Anforderungen zu definieren.

Um anwenderdefinierte Vorlagen (Flows) zu erstellen, befolgen Sie die Anweisungen unter Flows .

Führen Sie den Playbook-Flow zur automatisierten Reaktion auf Phishing aus

Mit dem Flow Designer können Sie Aufgaben im Playbook definieren und automatisieren, um Phishing-Angriffe auf Ihre Organisation zu analysieren und zu beheben.

Vorbereitungen

- Erforderliche Rolle: sn_si.admin, flow_designer und action_designer
- Installieren und konfigurieren Sie die folgenden Integrationen mit den richtigen Anmeldeinformationen:
  - Anforderung blockieren (Security Operations Palo Alto Networks NGFW Integration)
  - Ergänzung erkennbarer Elemente
  - Sichtungssuche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bedrohungssuche
- Microsoft Office Exchange

Warum und wann dieser Vorgang ausgeführt wird

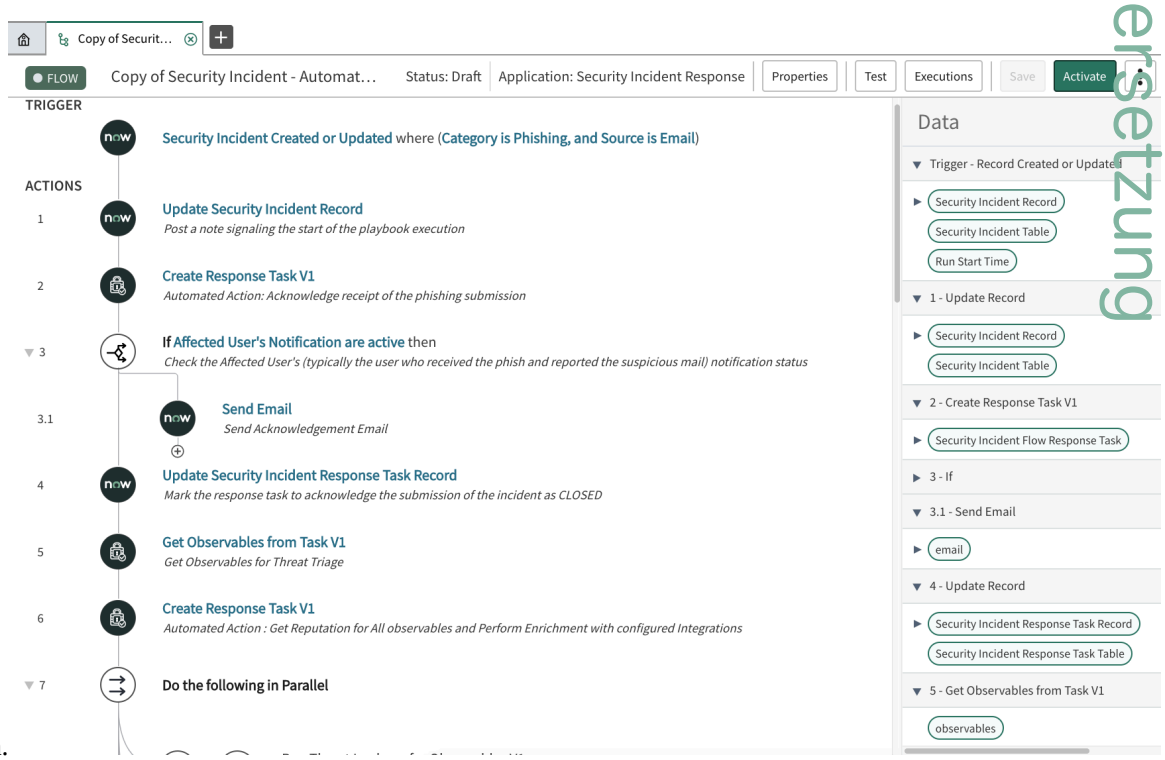
Wenn Mitarbeiter eine verdächtige E-Mail erhalten, die die allgemeinen Anzeichen eines Phishing-Angriffs enthält (wie in Ihren Sicherheitsrichtlinien definiert), können sie diese als EML-Anhang an die von Ihrer Organisation festgelegte Phishing-E-Mail-Adresse senden. Mit den im automatisierten Phishing-Playbook-Flow definierten Aufgaben können Sie eine Phishing-Bedingung selektieren, analysieren, eindämmen und beseitigen. Diese Aufgaben können als Teil verschiedener Incident-Status (z. B. Analyse, Eindämmen usw.) aufgerufen werden. Wenn ein Phishing-Security Incident erstellt wird, kann automatisch der automatisierte Phishing-Flow ausgelöst werden. Mit Flow Designer können Sie die Details der verschiedenen Aktionen zur Reaktion auf Incidents anzeigen, sobald sie aufgerufen werden.

Hinweis:
Der Playbook-Flow „Security Incident – Automated Phishing Response Template V1“ (Security Incident – Automated Phishing Response Template V1) ist schreibgeschützt. Sie können eine Kopie des Flows erstellen und nach Bedarf Änderungen vornehmen.

Die folgenden Schritte beschreiben, wie Sie eine Kopie der Phishing-Playbook-Vorlage erstellen und führen Sie durch einige der Aufgaben im Flow.

Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer** um die mit der Spoke Security Operations verfügbaren Flows anzuzeigen.
2. Klicken Sie auf den Link **Security Incident – Automated Phishing Response Template VI (Security Incident – Automated Phishing Response Template VI)**.
3. Klicken Sie auf der Seite „Flow“ auf das Mehr-Symbol , erstellen Sie eine Kopie des Flows, und öffnen Sie ihn zur Verwendung.
   Sie können die Auslöserbedingungen ändern, Aktionen hinzufügen oder entfernen und andere Änderungen am Flow



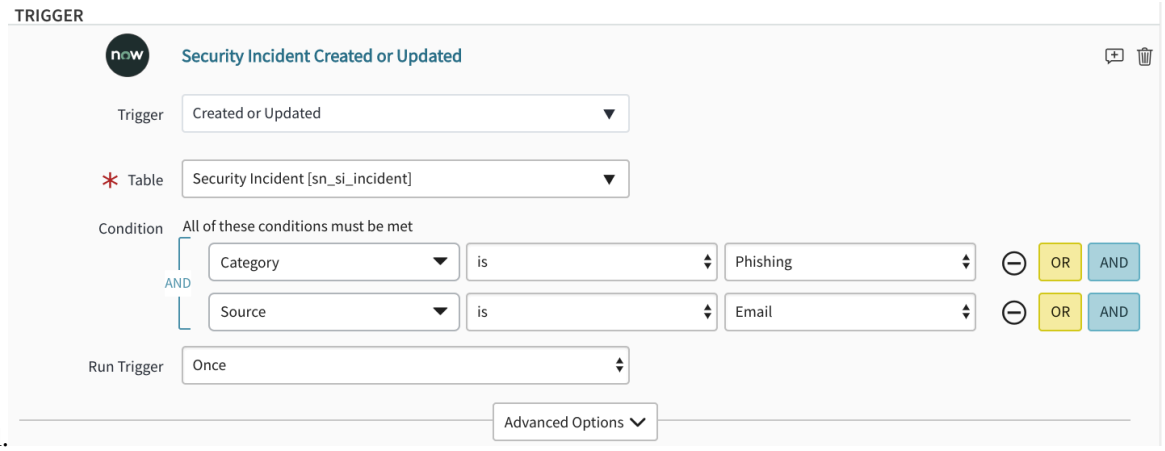
vornehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

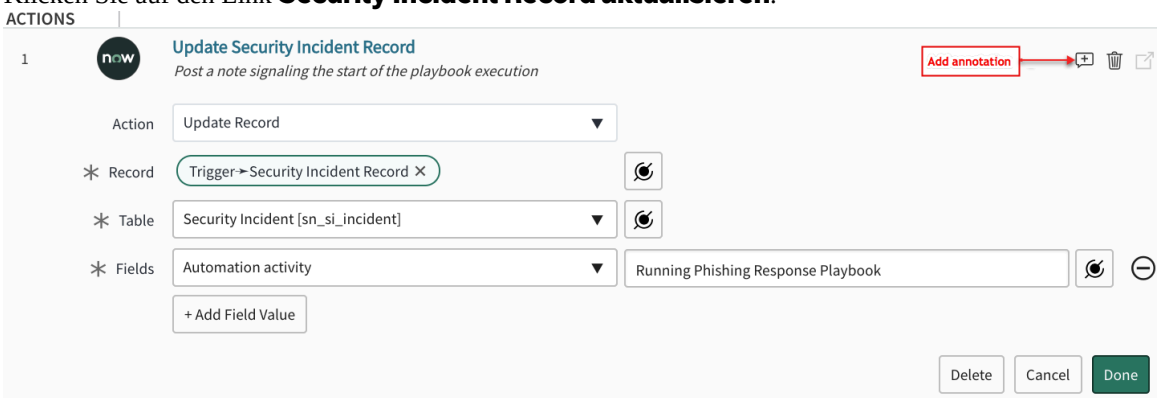
Diese Abbildung zeigt die Auslöserbedingungen und die Schritte, die der Flow ausführt. Der rechte Bereich zeigt den Datenfluss. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

4. Klicken Sie auf das Symbol **Auslöser**.
   Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser an und geben Sie an, wie oft der Flow den Auslöser ausführen soll.



   Wenn die im Flow definierten Bedingungen (Kategorie ist Phishing und Quelle ist E-Mail) im Incident-Datensatz erfüllt sind, werden die Aufgaben im automatisierten Phishing-Flow nacheinander ausgeführt. Sie können den Auslöser ändern, Anmerkungen hinzufügen, Bedingungen hinzufügen oder löschen usw.

5. Klicken Sie auf den Link **Security Incident Record aktualisieren**.

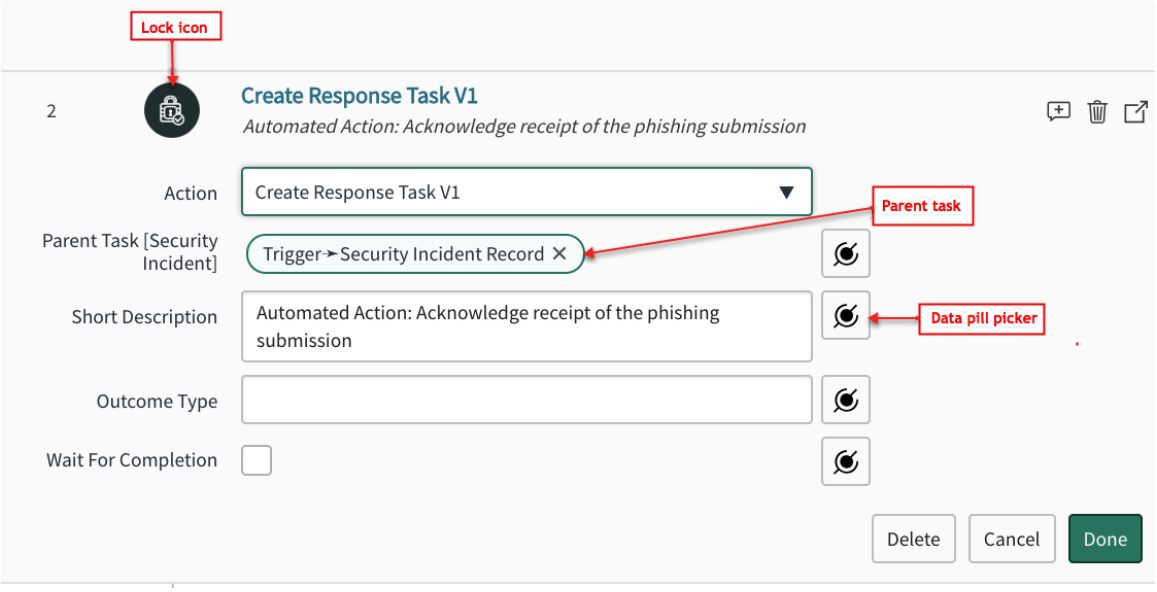


   „Security Incident Record aktualisieren“ ist der erste Schritt im Flow. Klicken Sie auf das Anmerkungssymbol , um dem Sicherheitsanalysten eine Notiz hinzuzufügen, dass ein Phishing-Incident aufgetreten ist und die Ausführung des automatisierten Phishing-Playbook-Flows begonnen hat.

6. Fahren Sie mit Schritt 2 im Flow fort, und klicken Sie auf den Link **Antwortaufgabe erstellen**.

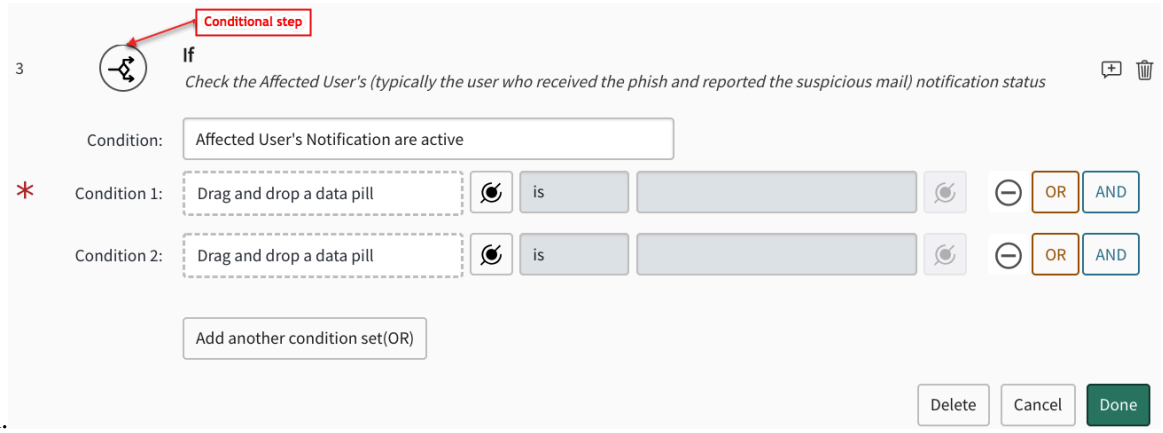
   In diesem Schritt erstellt der Flow eine automatisierte Antwortaufgabe, um dem Übermittler des Incidents oder dem betroffenen Anwender den Empfang zu bestätigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



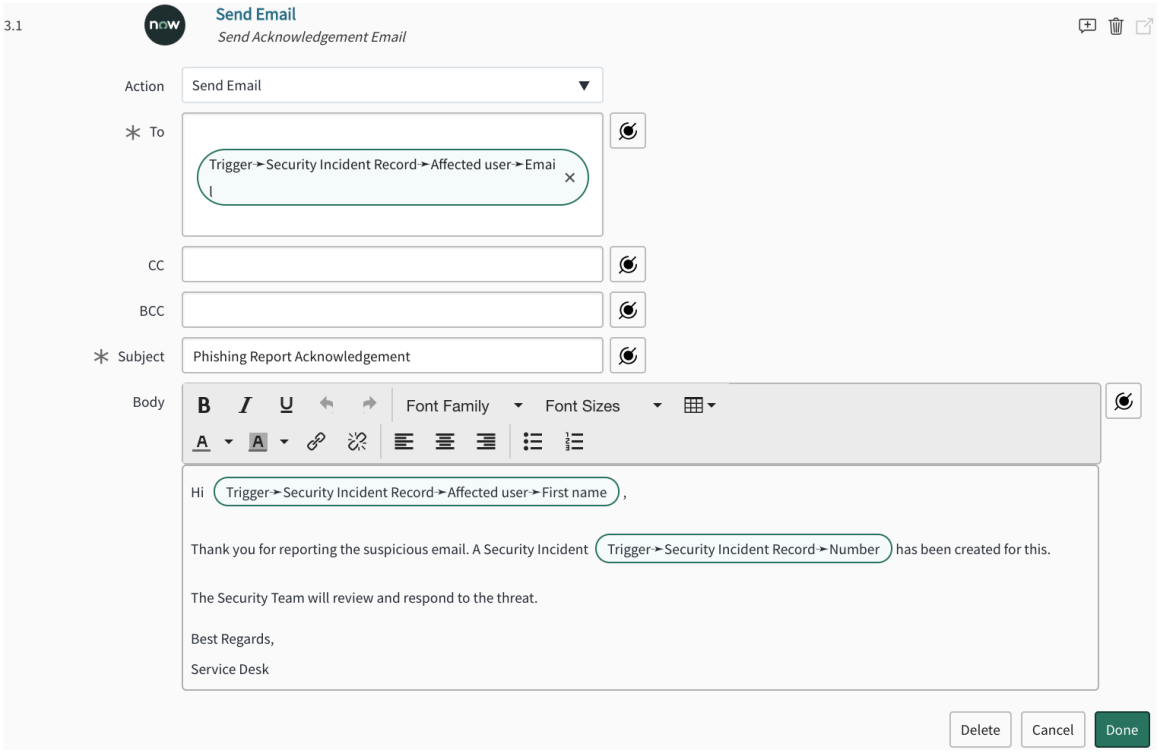
Beachten Sie, dass das Feld **Übergeordnete Aufgabe [Security Incident]**auf den übergeordneten Datensatz verweist, der diesem Schritt zugeordnet ist. Sie können jeden Referenzdatensatz auswählen, indem Sie das Datenpillen-Auswahlsymbol verwenden oder das entsprechende Referenzelement aus dem rechten Bereich ziehen. Beachten Sie das Sperrsymbol . Das Schlosssymbol zeigt an, dass für diesen Schritt kein Benutzereingriff erforderlich ist.

7. In Schritt 3 sammelt der Flow zusätzliche Details des betroffenen Benutzers (in der Regel der Benutzer, der den Incident übermittelt hat), um sicherzustellen, dass er erfolgreich eine Benachrichtigung senden kann. Sie können Bedingungen angeben, um zu überprüfen, ob der Status des betroffenen Anwenders „Aktiv“ ist und der Anwender Benachrichtigungen erhalten kann.



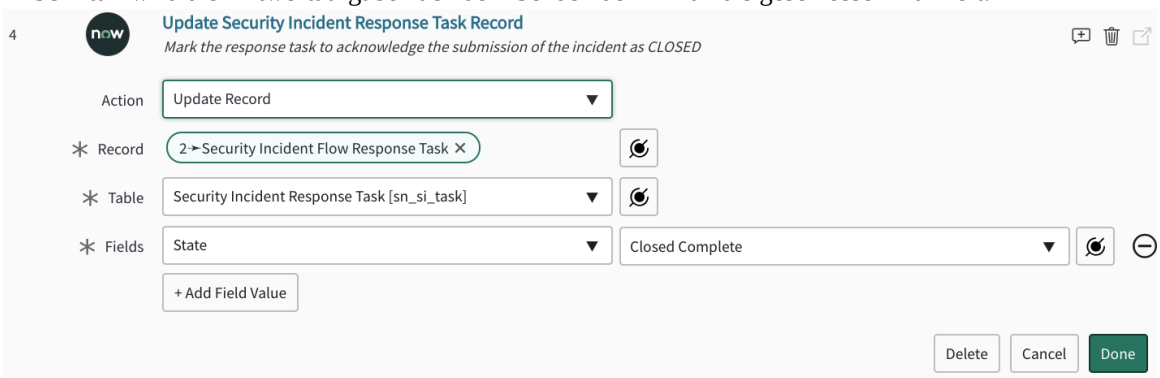
Beachten Sie das Symbol für den bedingten Schritt in Schritt 3. Der Flow führt den nächsten Schritt (3.1) nur aus, wenn die angegebenen Bedingungen erfüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

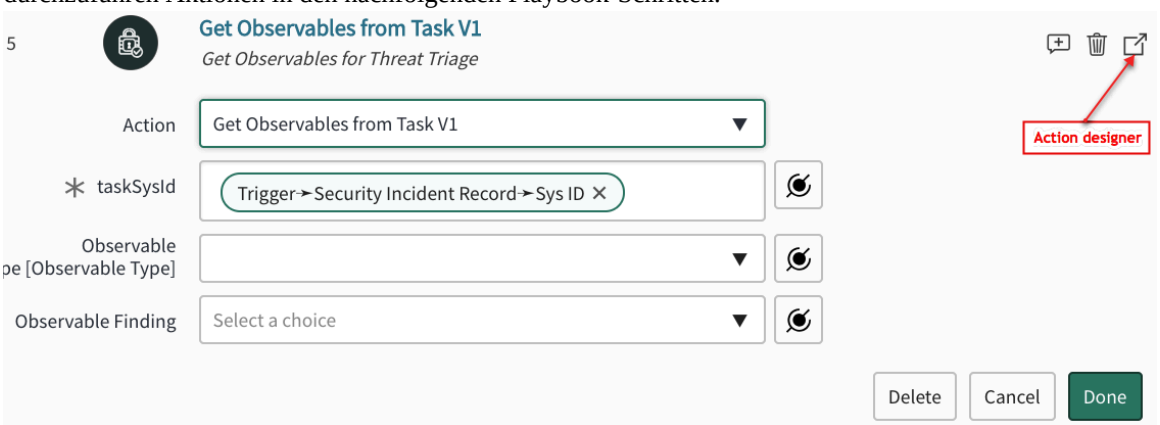


Wenn die in Schritt 3 definierten Bedingungen erfolgreich erfüllt wurden, wird die E-Mail gesendet.

8. In Schritt 4 wird die Antwortaufgabe nach dem Senden der E-Mail als geschlossen markiert.



9. In Schritt 5 werden alle am Incident beteiligten erkennbaren Elemente (z. B. E-Mail-Betreff, E-Mail-Adresse, von der die Phishing-E-Mail gesendet wurde, Phishing-URL) oder erkennbare Elemente, die einer ausgewählten Kategorie angehören (Hash, Datei oder Domäne), gesammelt, um zusätzliche Automatisierung durchzuführen Aktionen in den nachfolgenden Playbook-Schritten.

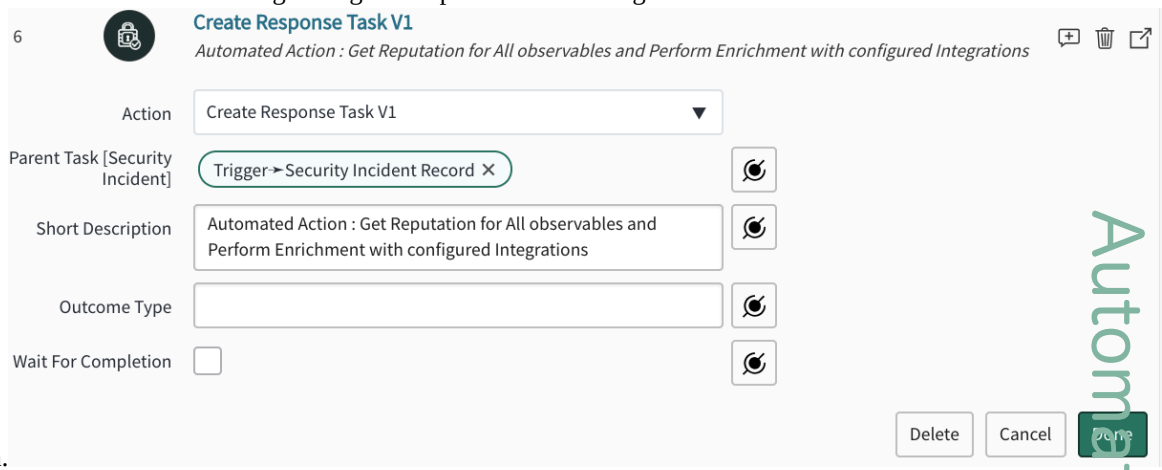


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

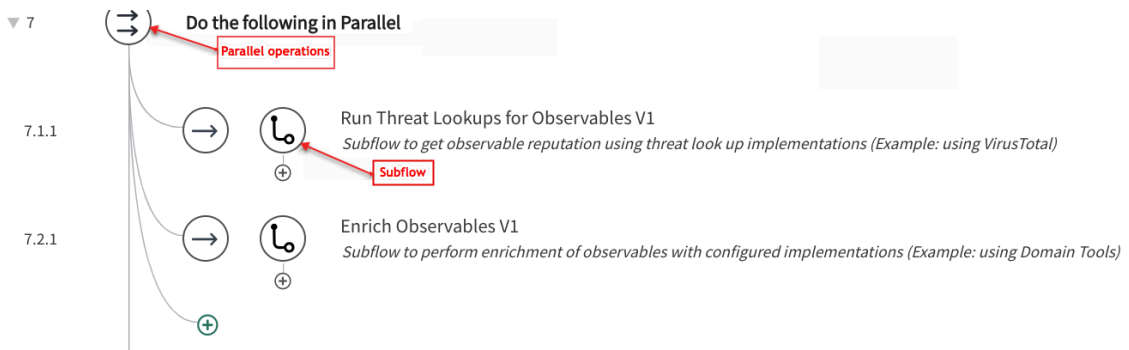
Klicken Sie auf das Aktionsdesigner-Symbol um eine detaillierte Ansicht der Aktion anzuzeigen.

Um die Seite „Aktionsdesigner“ anzuzeigen, erweitern Sie einen Schritt im Flow, und klicken Sie auf das Aktionsdesigner-Symbol.

10. In Schritt 6 wird eine automatisierte Antwortaufgabe erstellt.
Diese Aufgabe erfasst den Beginn des Prozesses zum Abrufen der Reputation aller erkennbaren Elemente und zur Ergänzung der Reputation mit konfigurierten Integrationen.



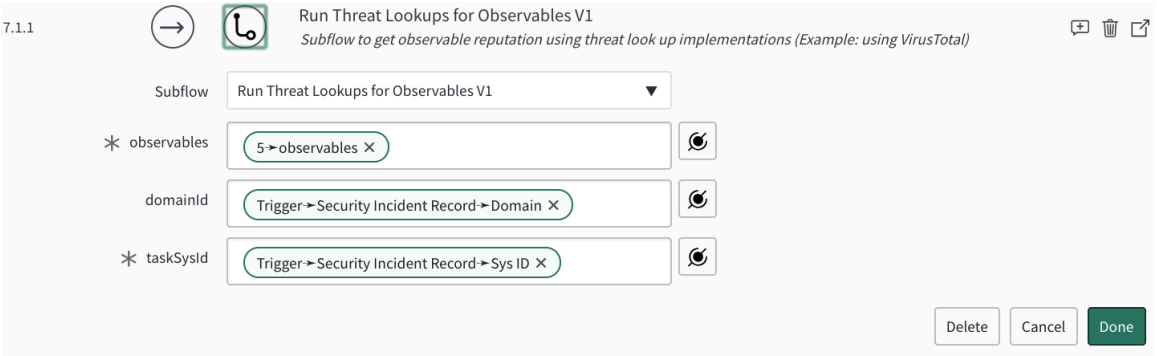
11. In Schritt 7 werden zwei Subflows aufgerufen:
    - Bedrohungssuchen für erkennbare Elemente ausführen: Dieser Subflow wird verwendet, um die Reputation aller erkennbaren Elemente mithilfe von Implementierungen der Bedrohungssuche abzurufen.
    - Erkennbare Elemente anreichern: Dieser Subflow wird verwendet, um die Anreicherung von erkennbaren Elementen mit konfigurierten Implementierungen durchzuführen.



Beachten Sie die Symbole für diese Aufgabe. Das Symbol für parallele Vorgänge gibt an, dass beide Aufgaben parallel ausgeführt werden, und das Subflow-Symbol gibt an, dass die ausgeführte Aufgabe ein Subflow ist (siehe unten):

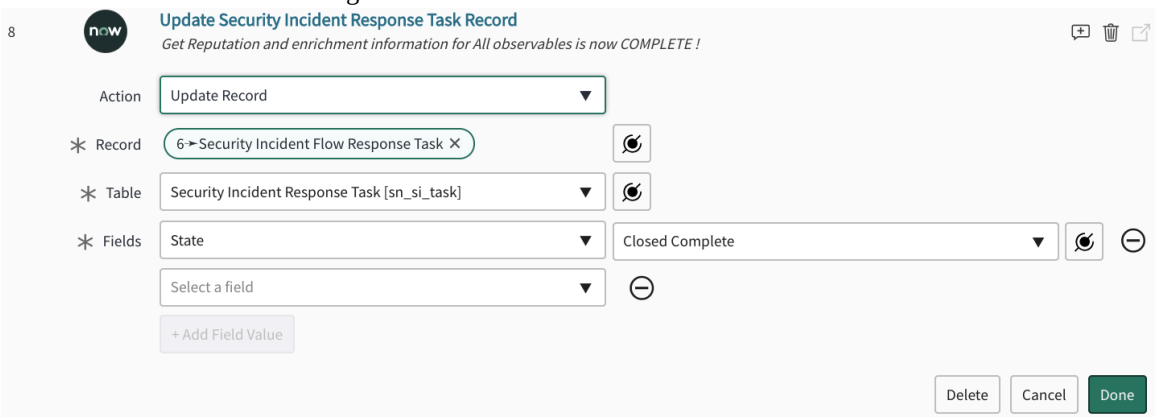
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

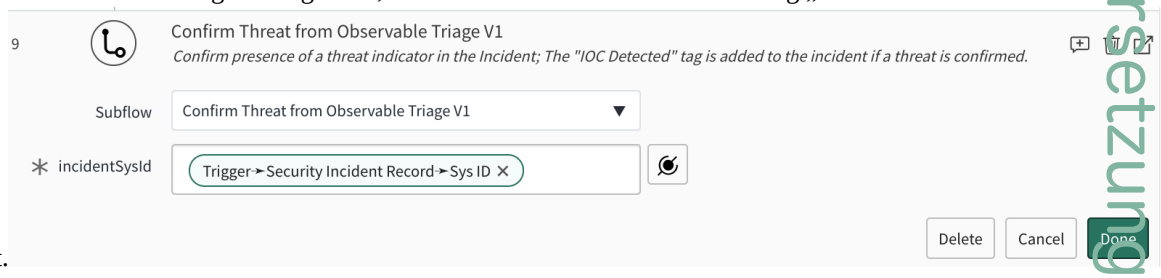


Beachten Sie die Zahl 5 im Feld „Erkennbare Elemente“. Dies zeigt an, dass die Bedrohungssuche für erkennbare Elemente ausgeführt wird, die in Schritt 5 abgerufen wurden. Dieser Subflow ruft wiederum vorhandene Workflows und Aktionen auf, wie im Subflow-Designergezeigt.

12. In Schritt 8 wird die Antwortaufgabe nach Abschluss der Subflows als Geschlossen markiert.

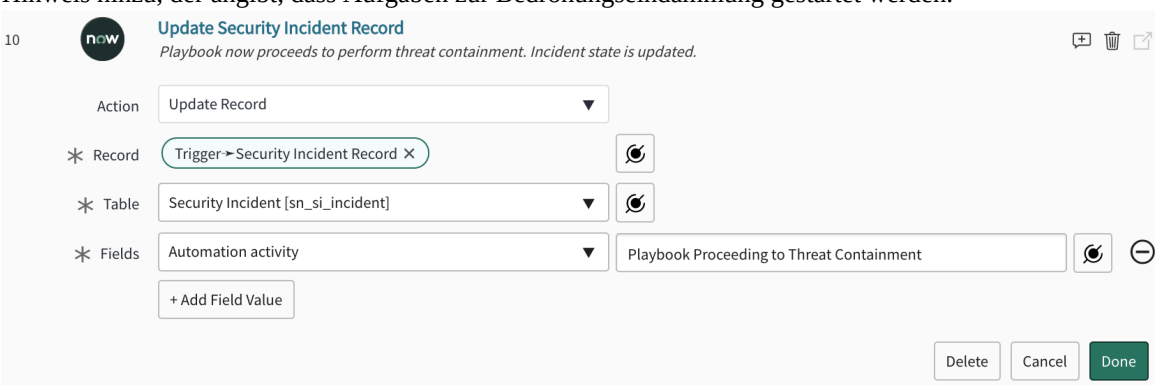


13. In Schritt 9 wird der Subflow „Bedrohung aus Selektierung erkennbarer Elemente bestätigen“ aufgerufen. Dieser Subflow wird verwendet, um das Vorhandensein eines Bedrohungsindikators im Incident zu bestätigen. Wenn die Bedrohung bestätigt wird, wird dem Incident die Kennzeichnung „IOC erkannt“



hinzugefügt.

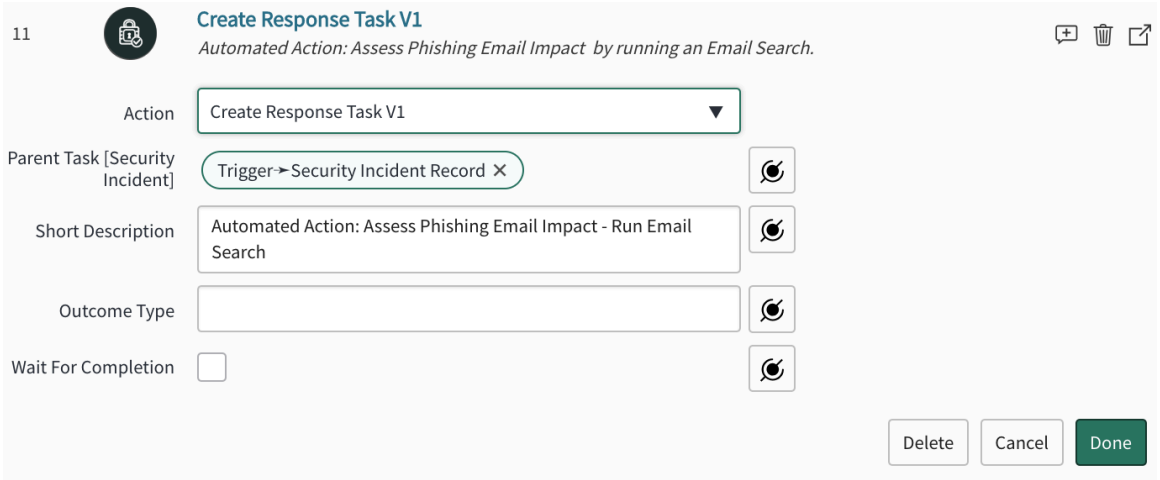
14. Wenn die Bedrohung bestätigt wird, aktualisieren Sie in Schritt 10 den Security Incident und fügen einen Hinweis hinzu, der angibt, dass Aufgaben zur Bedrohungseindämmung gestartet werden.



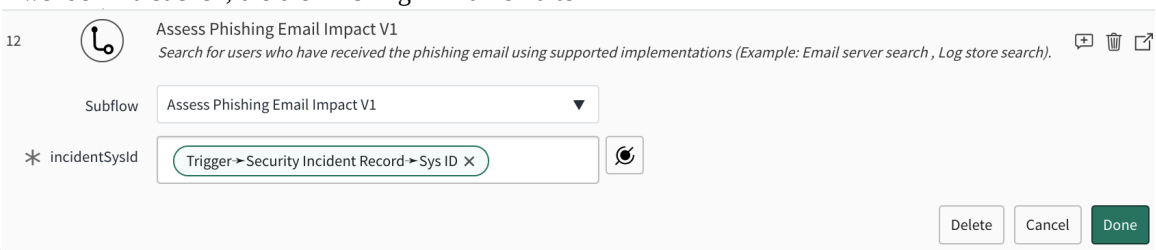
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

15. Schritt 11 ist eine automatisierte Antwortaufgabe, die den Start und den Abschluss der Aufgabe erfasst, anhand derer die Auswirkungen der Phishing-E-Mails bewertet werden.

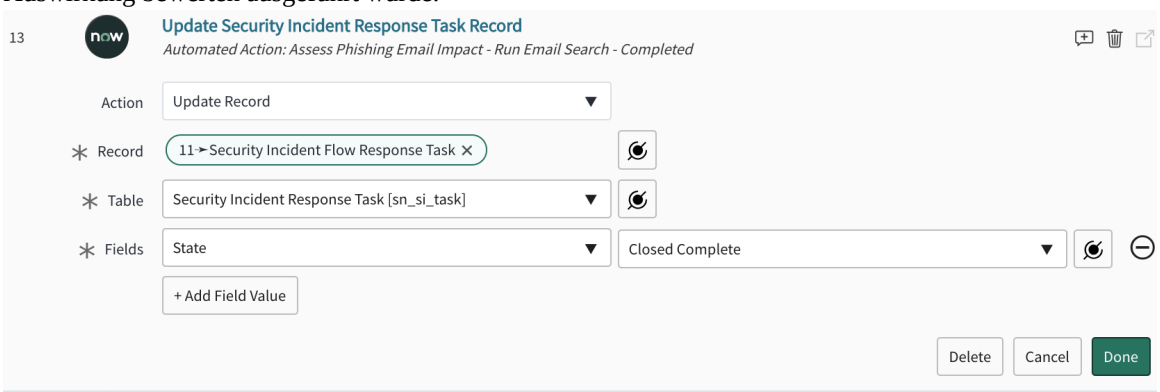


16. In Schritt 12 wird der Subflow Phishing-E-Mail-Auswirkung bewerten aufgerufen. Dieser Subflow wird verwendet, um mit unterstützten Implementierungen nach Anwendern zu suchen, die die Phishing-E-Mail erhalten

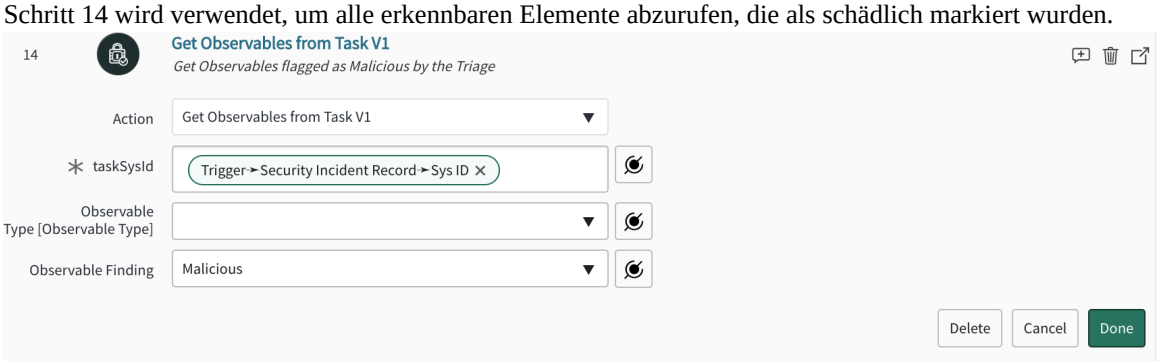


haben.

17. In Schritt 13 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow Phishing-E-Mail-Auswirkung bewerten ausgeführt wurde.

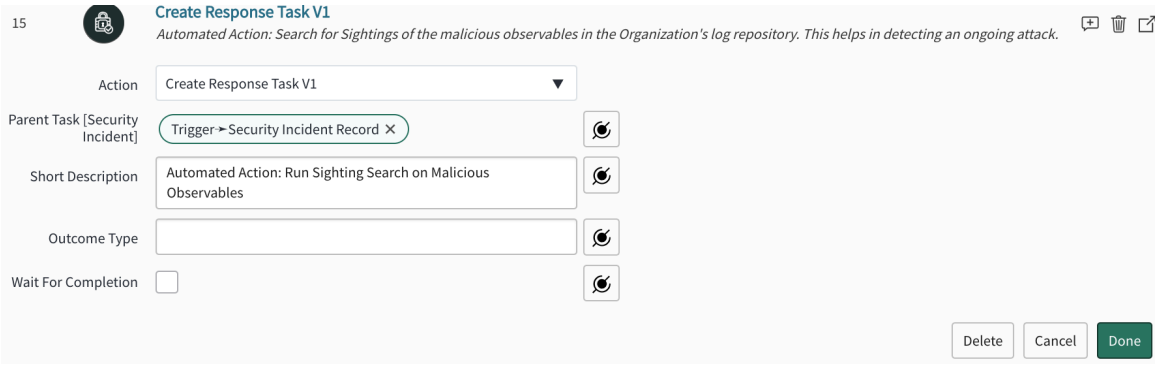


18. Schritt 14 wird verwendet, um alle erkennbaren Elemente abzurufen, die als schädlich markiert wurden.

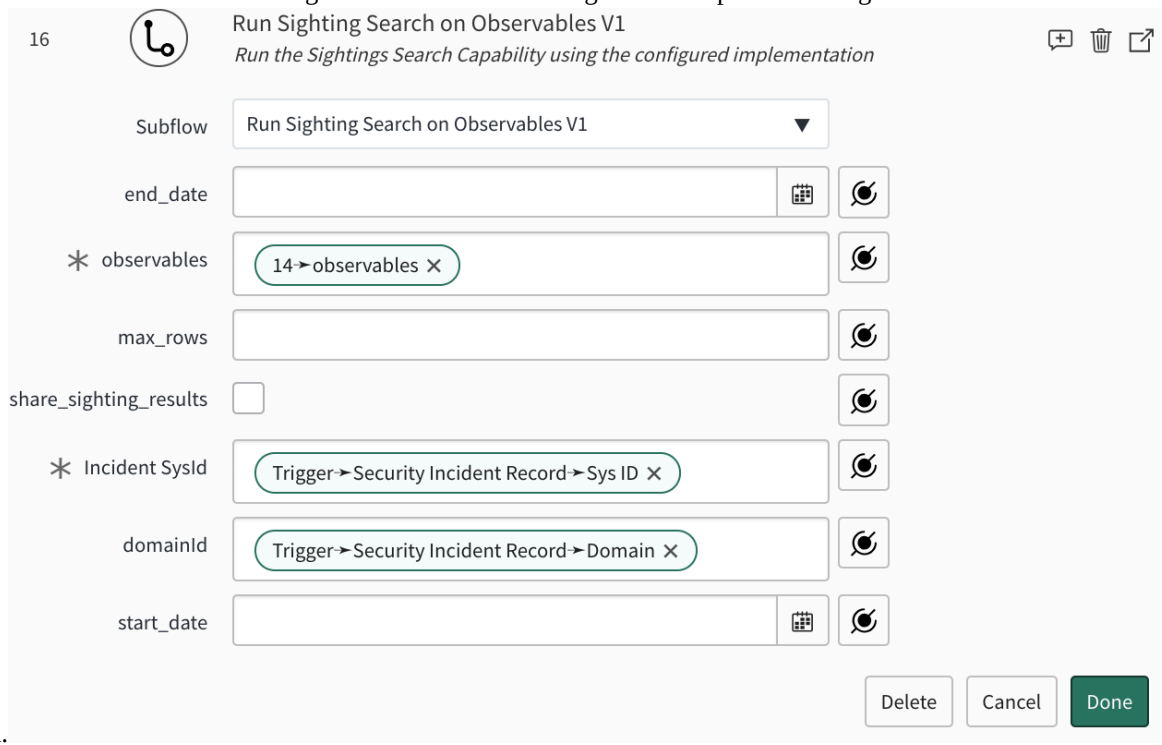


19. Schritt 15 ist eine automatisierte Antwortaufgabe, die den Start und den Abschluss der Sichtungssuche nach erkennbaren Elementen erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

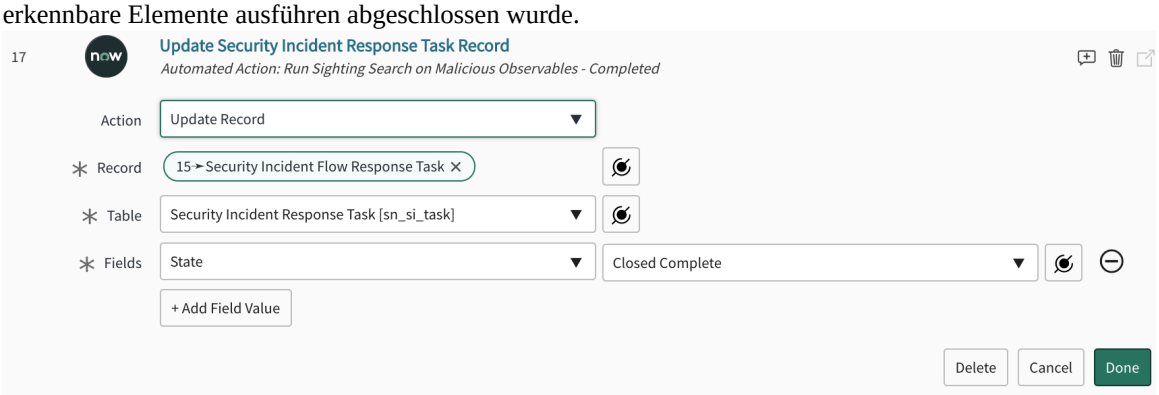


20. In Schritt 16 wird der Subflow „Sichtungssuche für erkennbare Elemente ausführen“ aufgerufen. Dieser Subflow führt eine Sichtungssuche mithilfe der konfigurierten Implementierung



durch.

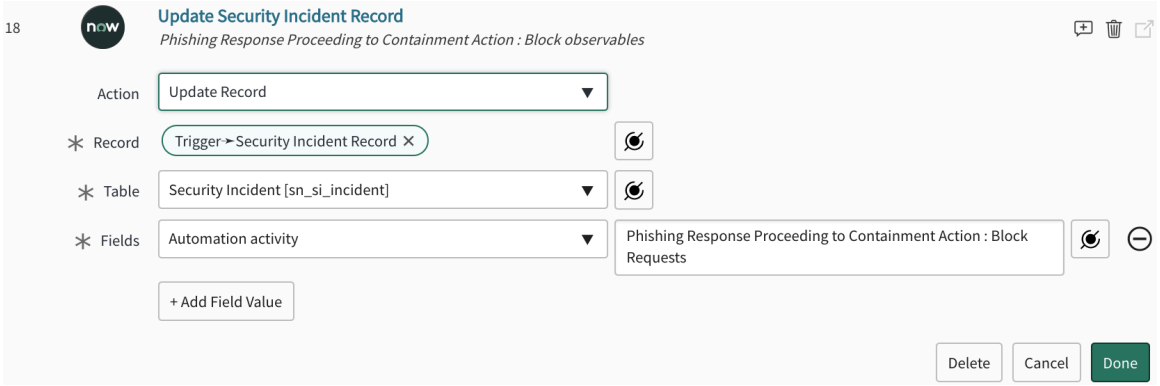
21. In Schritt 17 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow Sichtungssuche für erkennbare Elemente ausführen abgeschlossen wurde.



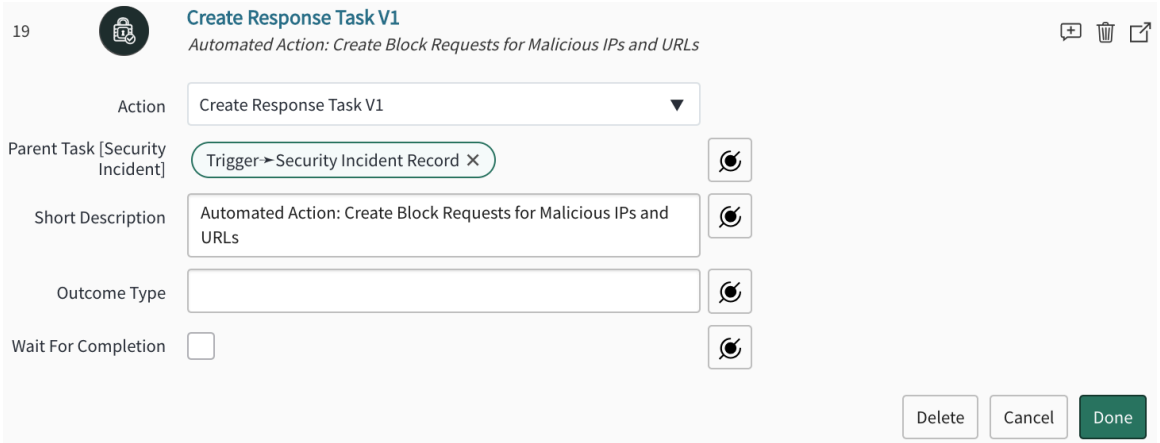
22. Nachdem Sie die schädlichen erkennbaren Elemente identifiziert haben, aktualisieren Sie in Schritt 18 den Security Incident-Datensatz, um anzugeben, dass die Eindämmungsmaßnahmen jetzt beginnen.

Automatische Übersetzung

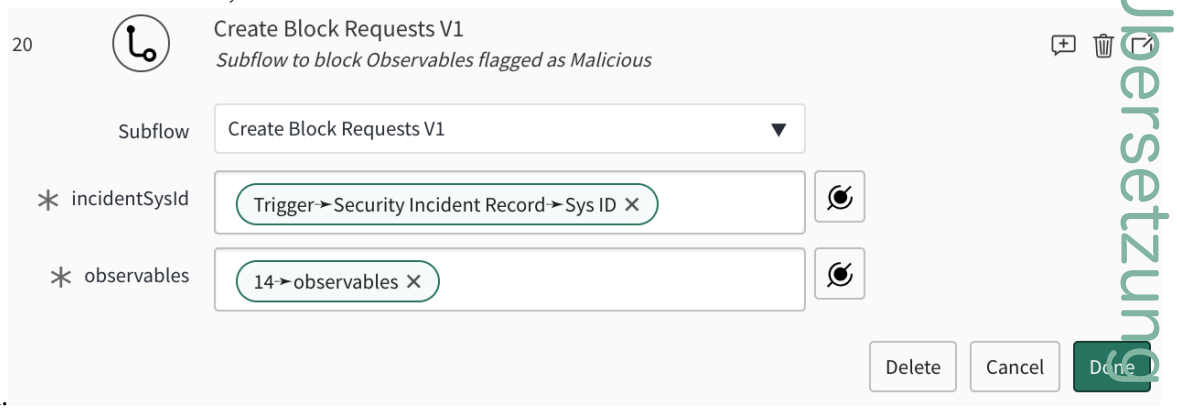
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



23. Schritt 19 ist eine automatisierte Antwortaufgabe, die den Start und den Abschluss der Blockierungsanforderungsaufgabe erfasst.

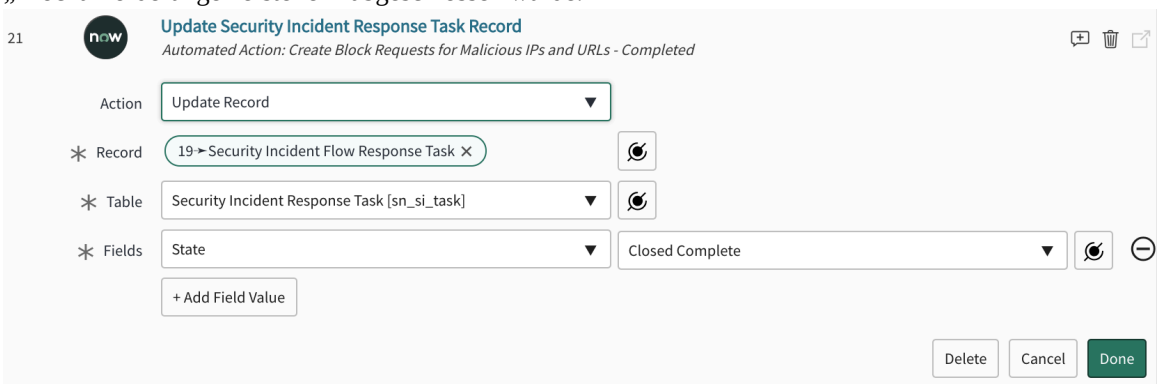


24. In Schritt 20 wird der Subflow „Blockanforderungen erstellen“ aufgerufen. Dieser Subflow wird verwendet, um schädliche erkennbare Elemente zu



blockieren.

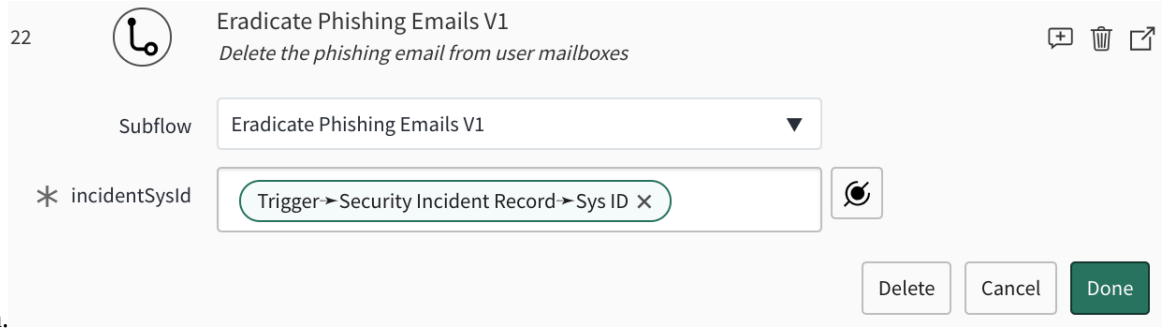
25. In Schritt 21 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow „Blockanforderungen erstellen“ abgeschlossen wurde.



Automatische Übersetzung

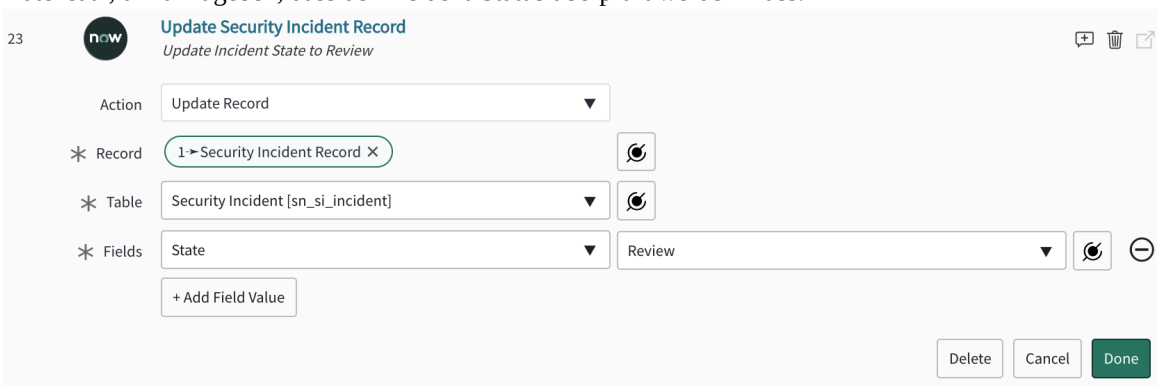
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

26. In Schritt 22 wird der Subflow Phishing-E-Mails beseitigen aufgerufen.
Dieser Subflow wird verwendet, um Phishing-E-Mails aus Anwenderpostfächern zu

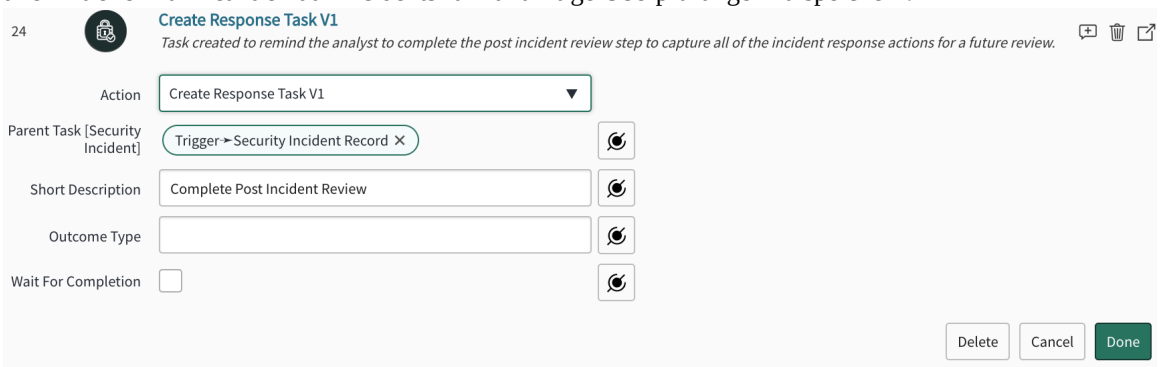


löschen.

27. Nachdem die Phishing-E-Mails gelöscht wurden, aktualisieren Sie in Schritt 23 den Security Incident-Datensatz, um anzugeben, dass der Incident-Status überprüft werden muss.



28. Im letzten Schritt erstellt der Flow eine automatisierte Antwortaufgabe.
Diese Aufgabe wird verwendet, um eine Erinnerung an den Sicherheitsanalysten zu senden, alle Aktionen zur Reaktion auf Incidents für zukünftige Überprüfungen zu speichern.

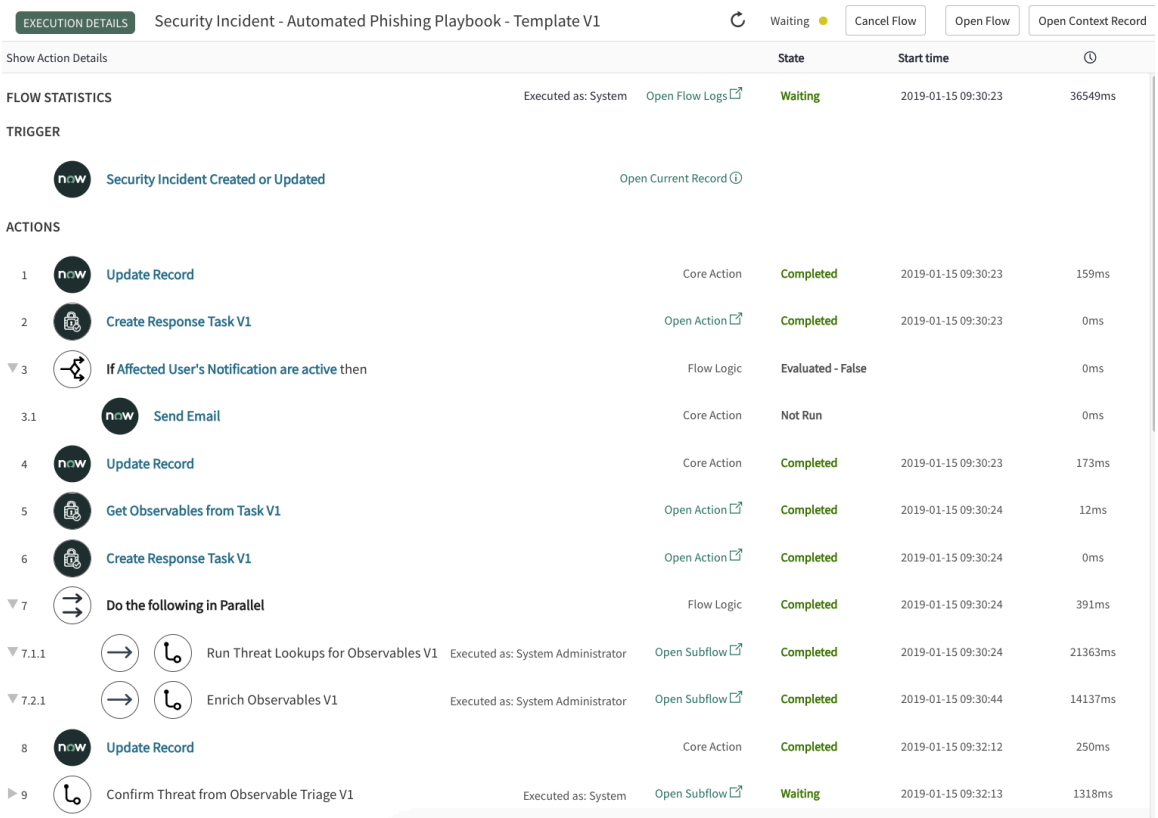


Nächste Maßnahme

Sie können auf **Test** klicken, um die Aktionen im Flow zu simulieren, bevor Sie ihn veröffentlichen. Klicken Sie nach dem Testen des Flows auf **Aktivieren**, um den Flow zu aktivieren und auszuführen.

Klicken Sie auf **Ausführungen**, um die Ausführungsdetails des Flow anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



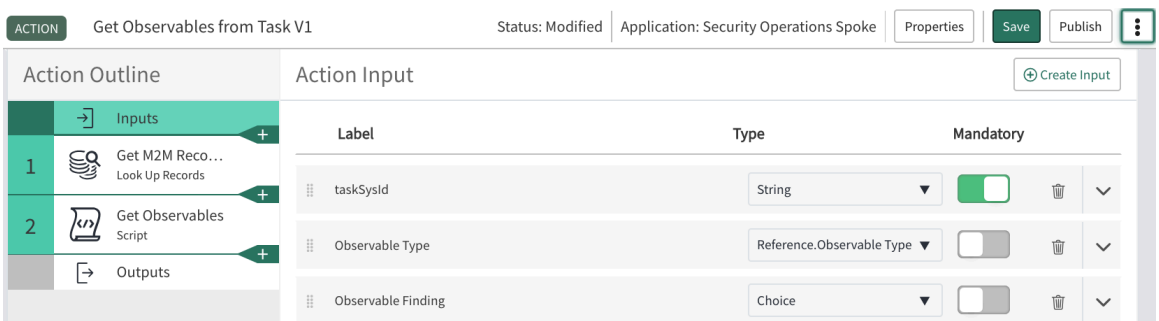
Zeigen Sie den Aktions-Designer des Playbook-Flows für automatisierte Phishing-Antworten an

Sie können einen Drilldown zum Aktionsdesigner durchführen, um detaillierte Informationen zu den Aktionen anzuzeigen, die für einen bestimmten Schritt im Playbook-Flow zur automatisierten Reaktion auf Phishing ausgeführt werden.

Auf dieser Seite wird die Seite „Aktionsdesigner“ für den Schritt „Erkennbare Elemente aus Aufgabe abrufen“ beschrieben. Klicken Sie im Bereich Aktionsgliederung auf eine Aufgabe, um Details anzuzeigen.

Aktionseingabe

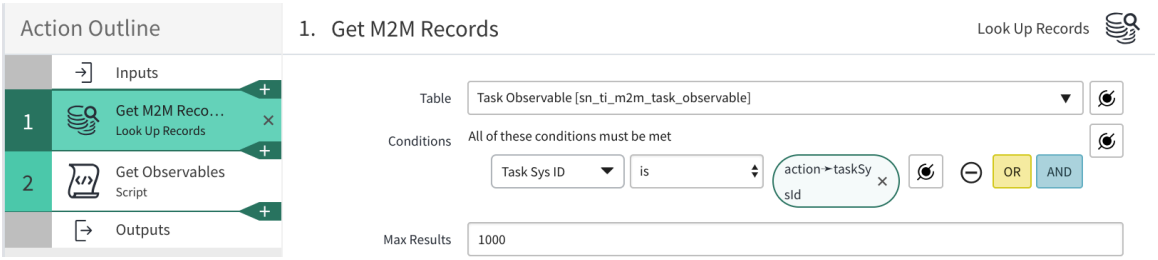
Dieser Abschnitt enthält Details zur Erstellung der Aktion, einschließlich der Incident-ID, des Typs des erkennbaren Elements (Hash oder IP) und des Funds des erkennbaren Elements (nur schädliche E-Mails).



M2M-Datensätze abrufen

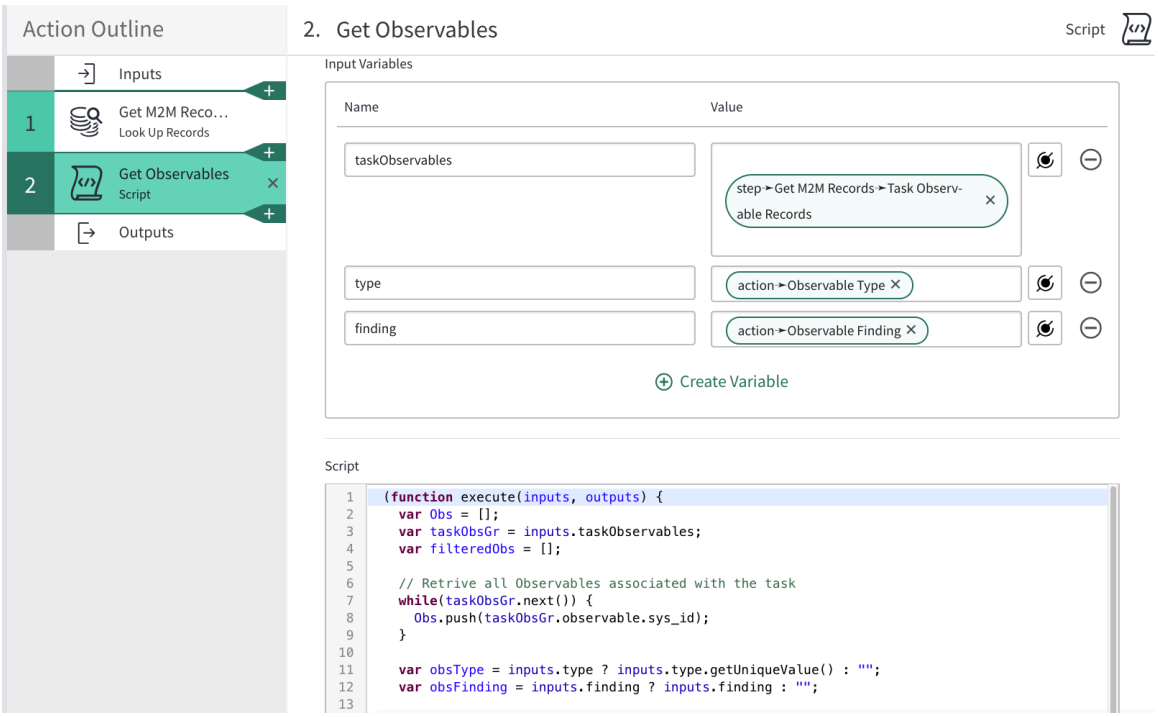
In diesem Abschnitt werden die Bedingungen angezeigt, die für die Suche nach erkennbaren Elementen in einer angegebenen Tabelle definiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erkennbare Elemente abrufen

Dieser Abschnitt zeigt das Skript, das zum Abrufen erkennbarer Elemente basierend auf den angegebenen Filterbedingungen verwendet wird. Schließlich werden die erkennbaren Elemente, die diese Kriterien erfüllen, und die Anzahl der Elemente angezeigt.



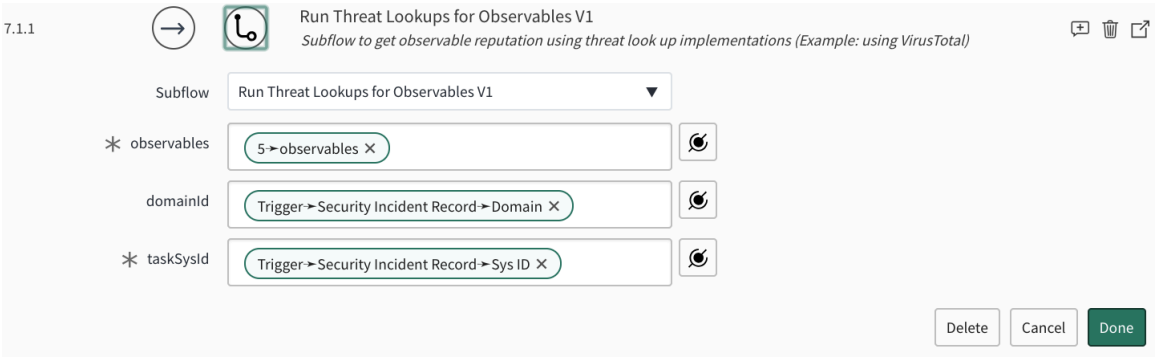
Hinweis:
Alle in diesem Flow definierten Aktionen sind wiederverwendbar und können entsprechend Ihren Anforderungen geändert werden.

Zeigen Sie den Subflow Designer des Playbooks für die automatisierte Reaktion auf Phishing an

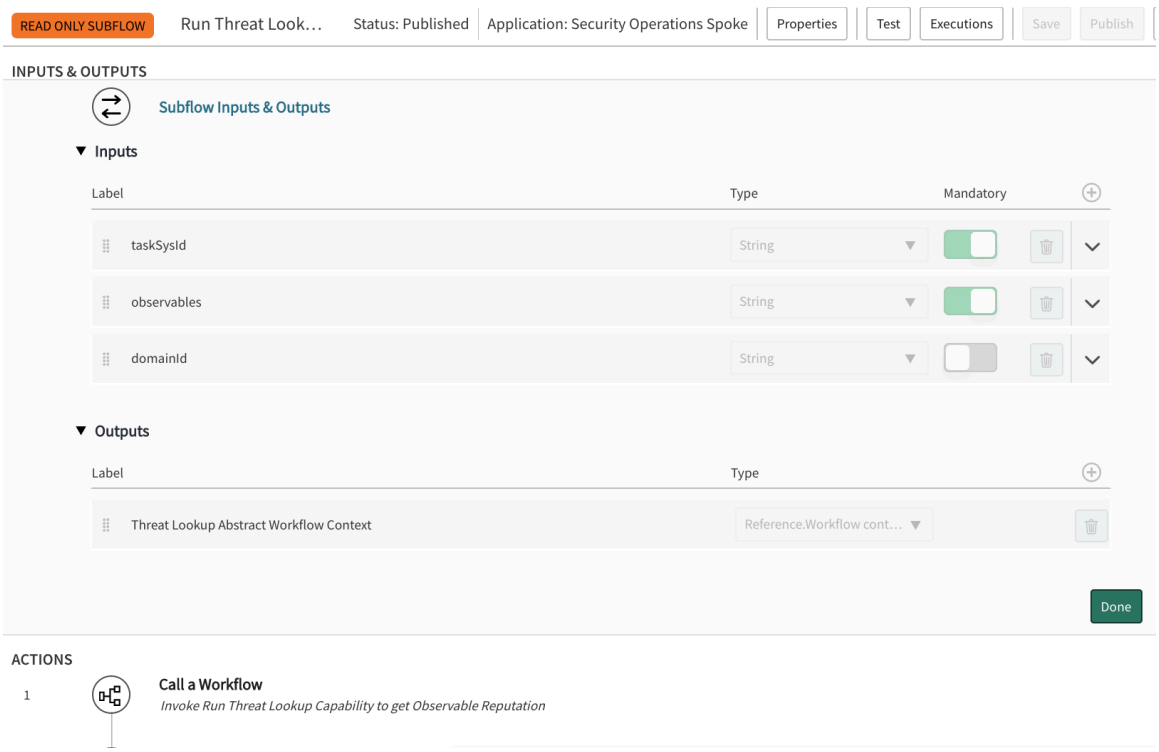
Sie können einen Drilldown zum Subflow-Designer durchführen, um detaillierte Informationen zum Subflow anzuzeigen, der als Teil des Playbook-Flows für die automatisierte Phishing-Antwort ausgeführt wird.

Sie können den Subflow Designer starten, um zusätzliche Details eines Subflow anzuzeigen. Die Seite „Subflow-Designer“ für den Subflow „Bedrohungssuchen für erkennbare Elemente ausführen“ wird hier angezeigt. Klicken Sie in der Abbildung unten auf das Symbol “, um den Subflow-Designer anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Seite „Subflow-Designer“ werden die Eingaben und Ausgaben für diesen Subflow und die zugrunde liegenden Workflow-Aktionen angezeigt, die ausgeführt werden.



Hinweis:
Dieser Subflow ist schreibgeschützt und kann nicht bearbeitet werden. Sie können dem Schritt Subflows hinzufügen oder löschen, aber Sie können den Subflow nicht ändern.

Playbook für automatisierte Malware

Das Automated Malware Playbook bietet eine Reihe von automatisierten Schritten, mit denen Sie Malware-Warnungen schnell und effizient lösen können.

Verwenden Sie den Playbook-Flow für Malware, um die Schritte zur Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk zu automatisieren. Die Flow-Vorlage enthält Auslöserbedingungen, eine Folge von Aktionen und Subflows, die zur besseren Lesbarkeit mit Anmerkungen versehen sind.

Diese Vorlagen enthalten eine Reihe von wiederverwendbaren Aktionen, mit denen auf Phishing-Angriffe reagiert werden kann. Jeder Flow hat einen Auslöser (Bedingung), eine Folge von Aktionen und Subflows, die zur besseren Lesbarkeit mit Anmerkungen versehen sind. Um auf diese Flows zuzugreifen, müssen Sie dieSecurity Operations-Spoke und die App Security Operations Palo Alto Networks - WildFire aus ServiceNow Storeinstallieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie müssen diese Vorlagen aktivieren, bevor Sie sie verwenden können.

Die folgenden Flows und Subflows sind enthalten:

- Security Incident – Automated Malware Playbook Template: Diese Vorlage wurde entwickelt, um die Antworten auf Malware-Warnungen zu automatisieren. Sie enthält eine Folge von Aktionen einschließlich eines Auslösers.
- Security Incident - Malware Manuelle Vorlage: Diese Vorlage ist der vorhandene manuelle Workflow für die Reaktion auf Malware, der aktiviert wird, wenn die Kategorie auf Böswillige Code-Aktivität festgelegt ist.

Subflows

- Bedrohung von erkennbarem Element bestätigen: Überprüft, ob das erkennbare Element schädlich ist und behandelt werden muss.
- Incident-Schweregrad festlegen: Legt einen Schweregradstatus für den Incident fest.
- Ransomware-Playbook: Bestimmt, ob es sich um einen Ransomware-Angriff handelt.

Diese Subflows stellen einen Satz wiederverwendbarer Vorgänge dar, die in mehreren Playbooks verwendet werden können. Sie können diese Subflows verwenden, um anwenderdefinierte Vorlagen (Flows) gemäß Ihren Anforderungen zu definieren.

Um anwenderdefinierte Vorlagen (Flows) zu erstellen, befolgen Sie die Anweisungen unter Flows .

Führen Sie den automatisierten Playbook-Flow für Malware aus

Verwenden Sie diesen Flow, um Aufgaben im Playbook zu automatisieren und Malware-Angriffe auf Ihre Organisation zu analysieren und abzuwehren.

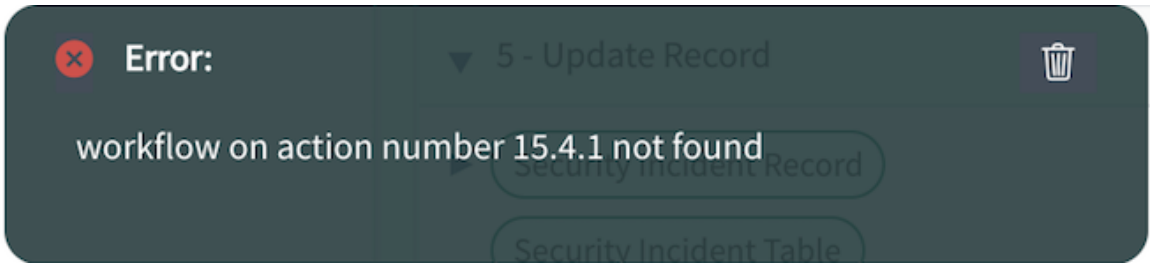
Vorbereitungen

- Erforderliche Rolle: sn_si.admin, flow_designer und action_designer
- Installieren und konfigurieren Sie die folgenden Integrationen mit den richtigen Anmeldeinformationen:
  - Palo Alto Networks WildFire for Security Operations
  - Sichtungssuche (Splunk)
  - Anforderungen blockieren
  - Bedrohungssuche
  - Erkennbare Elemente ergänzen

  Stellen Sie sicher, dass diese Integrationen ordnungsgemäß funktionieren, bevor Sie die Vorlage „Security Incident – Automated Malware Playbook“ aktivieren.

- WildFire-App „Security Operations Palo Alto Networks“: Um auf den automatisierten Playbook-Flow für Malware zuzugreifen, müssen Sie die App „Security Operations Spoke“ und „Security Operations Palo Alto Networks – WildFire“ aus dem ServiceNow Storeinstallieren. Wenn die Palo Alto Networks WildFire-App von Security Operations nicht installiert ist, wird der folgende Fehler angezeigt: „Workflow für Aktionsnummer 15.4.1 nicht gefunden“:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie diese App nicht installieren möchten, löschen Sie die Schritte **15.2, 15.3 und 15.4** aus dem automatisierten Malware-Playbook-Flow.

- Stellen Sie sicher, dass die folgenden Bedingungen erfüllt wurden:
  - Der Security Incident wurde einem Sicherheitsanalysten zugewiesen, der zur entsprechenden Genehmigungsgruppe gehört.
  - Der Sicherheitsanalyst, der den Incident bearbeitet, muss über eine gültige E-Mail-Adresse verfügen.
  - Die erforderlichen Konfigurationselemente und erkennbaren Elemente wurden dem Security Incident hinzugefügt.
- Ändern Sie für **Schritt 21 (Genehmigung anfordern)**die Gruppe von **Security Incident Assignment (Zuweisung des Security Incidents)** zu Ihrer bevorzugten Gruppe.
- Schritt 21 des Flows ist ein obligatorischer Aufgabengenehmigungsschritt, bei dem eine Genehmigungsanforderung an den Administrator gesendet wird. Um die Anforderung zu genehmigen, muss der Administrator zur Seite Aufgabengenehmigungen navigieren und das Feld Status auf **Genehmigt**festlegen. Wenn die Aufgabe nicht genehmigt wird, kann der Flow Designer nicht fortfahren, und der Prozess wird beendet.

Warum und wann dieser Vorgang ausgeführt wird

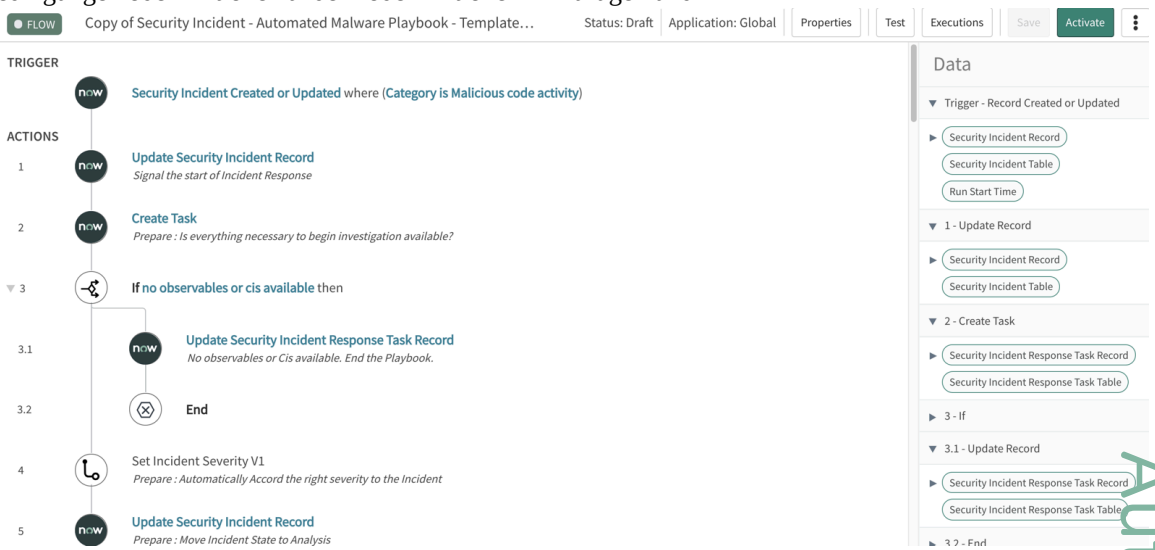
Wenn im Netzwerk eine Aktivität mit schädlichem Code erkannt wird, wird ein Security Incident erstellt und der automatisierte Playbook-Flow für Malware gestartet. Sie können die im automatisierten Malware-Playbook-Flow definierten Aufgaben verwenden, um die Bedrohung zu selektieren, zu analysieren, einzudämmen und zu beseitigen.

Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer** um die mit der Security Operations-Spoke verfügbaren Flows anzuzeigen.
2. Klicken Sie auf den Link **Security Incident – Automated Malware Playbook Template VI (Security Incident – Automated Malware Playbook Template VI)**.
3. Klicken Sie auf der Seite „Flow“ auf das Mehr-Symbol ⋮, erstellen Sie eine Kopie des Flows, und öffnen Sie ihn zur Verwendung.

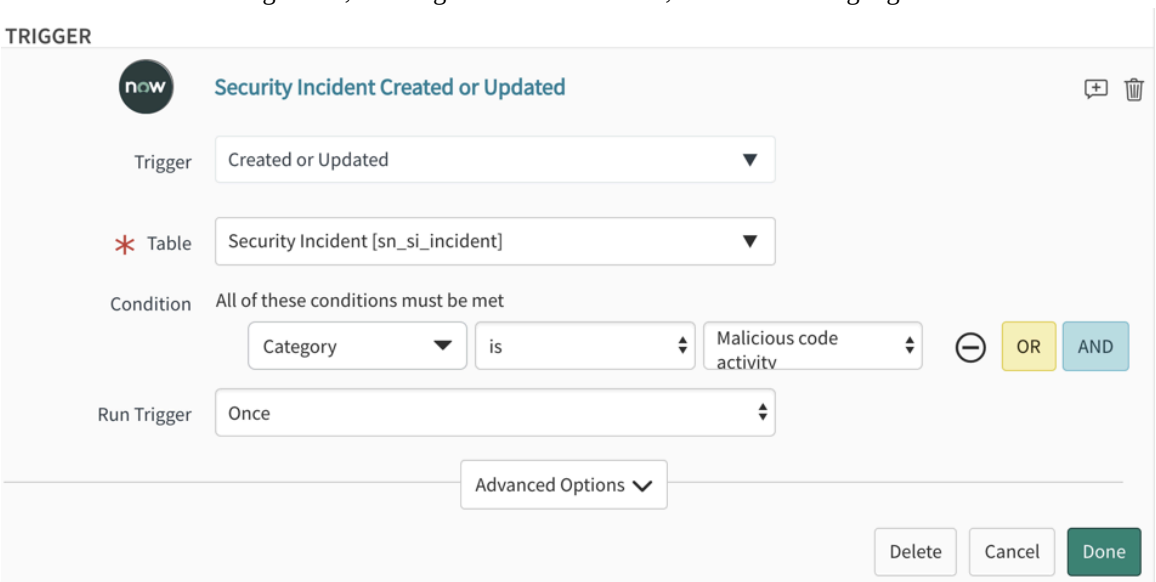
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können jetzt Änderungen an Ihrem Flow vornehmen, z. B. Auslöserbedingungen oder Aktionen ändern oder Aktionen hinzufügen und entfernen.



Dies zeigt den Auslöser und die Schritte, die mit dem Flow ausgeführt werden. Der rechte Bereich zeigt den Datenfluss. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

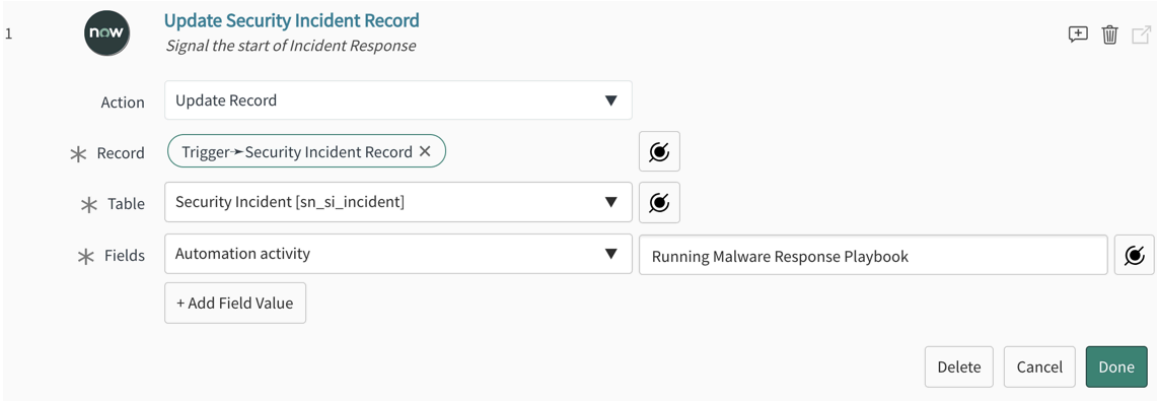
4. Klicken Sie auf das Symbol **Auslöser**.
   Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser und die Aufgabe an, die ausgeführt werden sollen, wenn die Bedingungen erfüllt sind.



Wenn die im Flow definierte Bedingung (Kategorie ist Aktivität von böswilligem Code) im Incident-Datensatz erfüllt ist, werden die Aufgaben im automatisierten Phishing-Flow nacheinander ausgeführt. Sie können den Auslöser ändern, Anmerkungen hinzufügen, Bedingungen hinzufügen oder löschen usw.

5. Der erste Schritt im Flow ist **Security Incident Record aktualisieren**.

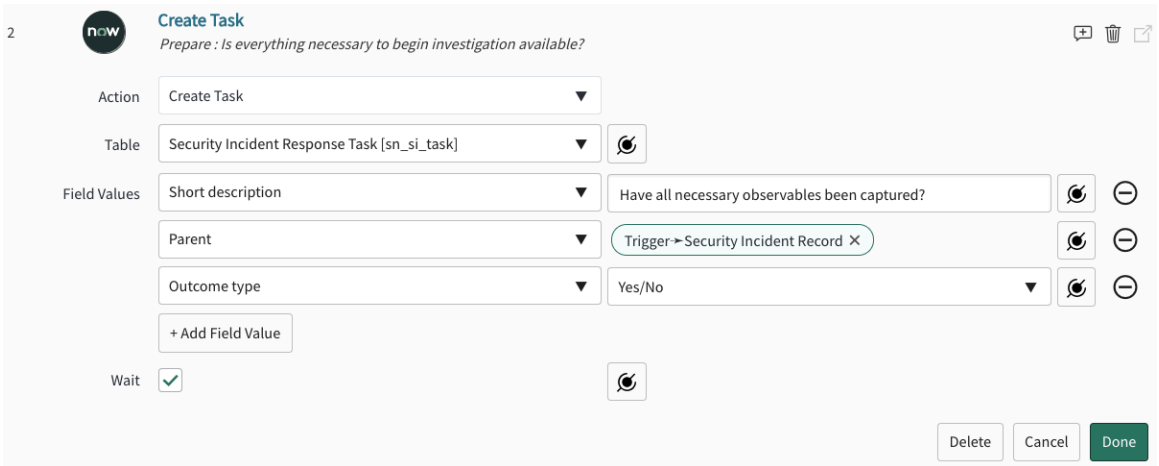
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie auf den Link und dann auf das Anmerkungssymbol , um dem Sicherheitsanalysten eine Notiz hinzuzufügen, dass schädliche Codeaktivitäten aufgetreten sind und die Ausführung des Playbook-Flows zur automatisierten Reaktion auf Malware begonnen hat.

6. Fahren Sie mit Schritt 2 im Flow fort, und klicken Sie auf den Link **Aufgabe erstellen**.

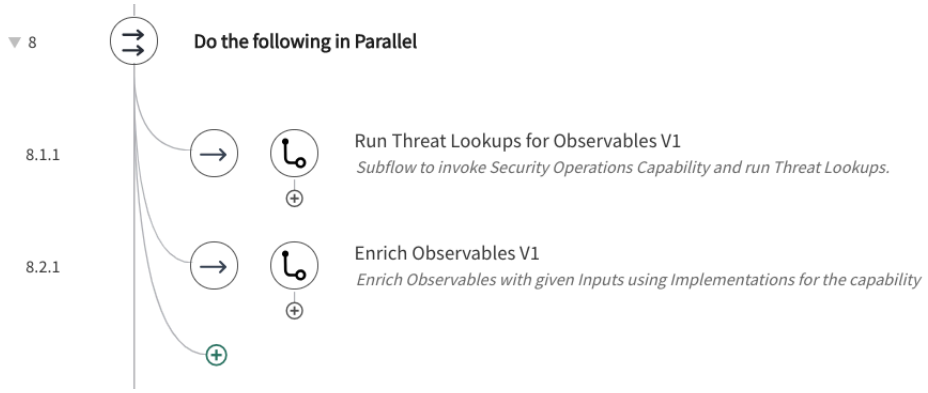
   In diesem Schritt wird eine automatisierte Antwortaufgabe erstellt, um zu überprüfen, ob alle erforderlichen erkennbaren Elemente erfasst wurden und ob die Untersuchung beginnen kann.



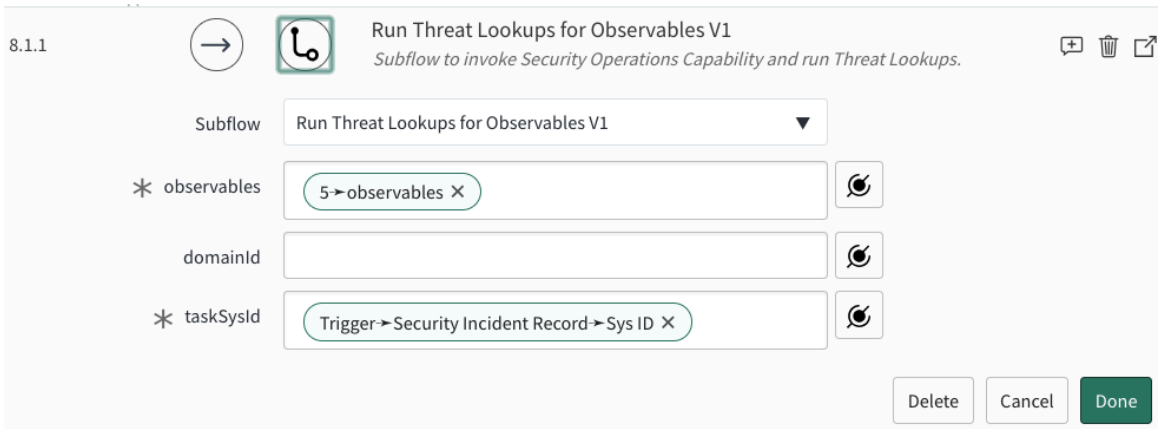
7. Wenn der Ergebnistyp auf **„Nein“**festgelegt ist, gibt dies an, dass keine erkennbaren Elemente und CIs zum Initiieren der Untersuchung verfügbar sind.
   Aktualisieren Sie den Security Incident-Datensatz, um anzugeben, dass das Playbook nicht fortgesetzt werden kann.
8. Wenn der Ergebnistyp auf **Ja**festgelegt ist, weist der Subflow Incident-Schweregrad festlegen dem Security Incident automatisch den richtigen Schweregrad zu.
9. Im nächsten Schritt wird der Security Incident-Datensatz aktualisiert.
10. Im nächsten Schritt werden alle erkennbaren Elemente, die am Incident oder einer ausgewählten Kategorie beteiligt sind, gesammelt, um in den nachfolgenden Playbook-Schritten zusätzliche automatisierte Aktionen auszuführen.
11. Im nächsten Schritt wird eine automatisierte Antwortaufgabe erstellt.
    Diese Aufgabe erfasst den Beginn des Prozesses zum Abrufen der Reputation aller erkennbaren Elemente und zur Ergänzung der Reputation mit konfigurierten Integrationen.
12. In Schritt 8 werden zwei Subflows aufgerufen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bedrohungssuchen für erkennbare Elemente ausführen: Dieser Subflow wird verwendet, um die Reputation aller erkennbaren Elemente mithilfe von Implementierungen der Bedrohungssuche abzurufen.
- Erkennbare Elemente anreichern: Dieser Subflow wird verwendet, um die Anreicherung von erkennbaren Elementen mit konfigurierten Implementierungen durchzuführen.



Beachten Sie die Symbole für diese Aufgabe. Das Symbol für parallele Vorgänge gibt an, dass beide Aufgaben parallel ausgeführt werden, und das Subflow-Symbol gibt an, dass die ausgeführte Aufgabe ein Subflow ist (siehe unten):



Beachten Sie die Zahl 5 im Feld „Erkennbare Elemente“. Dies zeigt an, dass die Bedrohungssuche für erkennbare Elemente ausgeführt wird, die in Schritt 5 abgerufen wurden. Dieser Subflow ruft wiederum vorhandene Workflows und Aktionen auf.

13. Im nächsten Schritt wird die Aktion „Datensätze suchen“ ausgeführt.
Diese Aktion wird verwendet, um nach Workflow-Kontextdatensätzen zu suchen, bei denen die übergeordneten Workflows eine der folgenden sein können.
    - Bedrohungssuche – abstrakter Workflow-Kontext
    - Anreicherung erkennbarer Elemente – abstrakter Workflow-Kontext
14. Im nächsten Schritt werden die Reputation und die Ergänzungsergebnisse für jeweils 8 Datensätze überprüft.
15. Überprüfen Sie die nächsten Schritte weiter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Security Incident-Datensatz aktualisieren: Aktualisiert den Security Incident-Datensatz mit der Angabe, dass die Reputationssuche und die Ergänzungsaktivitäten abgeschlossen wurden.

b. Erkennbare Elemente aus Aufgabe abrufen: Ruft alle schädlichen erkennbaren Elemente ab, die dem Security Incident zugeordnet sind.

c. Aufgabe erstellen: Prüft und bestätigt, ob die Ausführungen der automatisierten Selektierung erfolgreich waren.

16. Wenn erkennbare Elemente vorhanden sind, die als schädlich gekennzeichnet wurden:

a. Security Incident-Datensatz aktualisieren: Veröffentlichen Sie eine Arbeitsnotiz, die angibt, dass eine Bedrohung erkannt wurde.

b. Eingabeabfrage aus erkennbaren Elementen erstellen: Wenn mehr als zehn erkennbare Elemente als schädlich gekennzeichnet wurden, wird der Subflow „Sichtungssuche für erkennbare Elemente“ (in Splunk oder Carbon Black) ausgeführt.

17. Wenn die erkennbaren Elemente nicht als schädlich gekennzeichnet sind, wird der Flow mit den folgenden Schritten fortgesetzt:

a. Security Incident-Datensatz aktualisieren: Veröffentlichen Sie eine Arbeitsnotiz, die angibt, dass keine Bedrohung erkannt wurde

b. Erkennbare Elemente aus Aufgabe abrufen: Identifiziert alle SHA256-Hash-IDs aus dem Incident.

c. Datensätze erkennbarer Elemente suchen: Sucht nach Datensätzen, die diese Kriterien erfüllen.

18. Überprüfen Sie die nächsten Schritte weiter:

a. Für jedes schädliche erkennbare Element wird der Workflow **„Security Operations Palo Alto Networks – WildFire Data Enrichment abrufen“** ausgeführt.

b. Überprüft die Untersuchungsergebnisse, um festzustellen, ob sie zufriedenstellend sind.
Es wird eine Antwortaufgabe erstellt, um zu überprüfen, ob die vermutete Malware ein Ransomware-Angriff ist. Wenn ja, wird der Subflow des Ransomware-Playbooks ausgeführt.

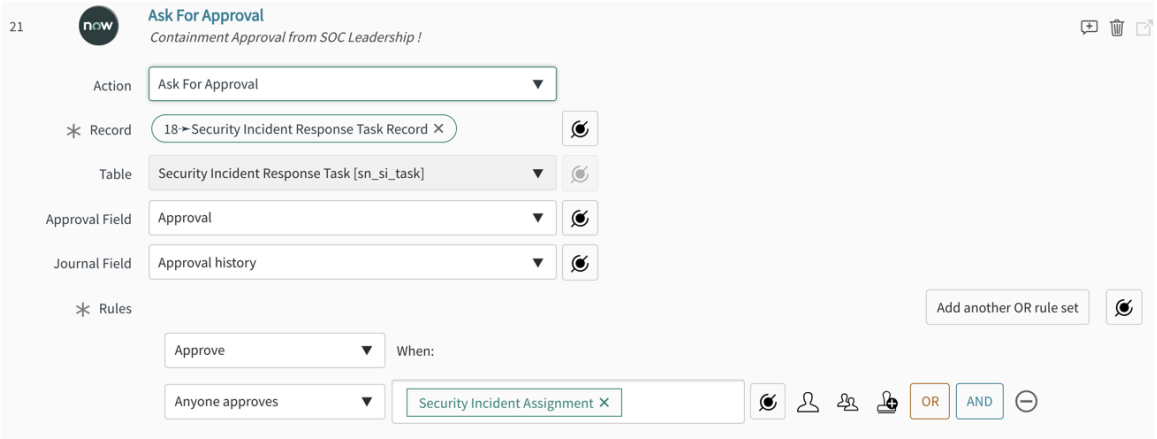
c. Im nächsten Schritt wird eine E-Mail mit einer Zusammenfassung der Analyse gesendet und eine Genehmigung angefordert, um Eindämmungsverfahren zu initiieren.

d. Eine Aufgabe wird erstellt, um Details der angeforderten Genehmigung zu erfassen.

e. Der nächste Schritt besteht in der Aktualisierung des Security Incident-Datensatzes.
Veröffentlichen Sie eine Arbeitsnotiz, die den Sicherheitsanalysten darüber informiert, dass die Genehmigungsanforderung gestellt wurde.

f. Fordert die Genehmigung zur Eindämmung der Malware-Angriffe von Ihrem SOC-Manager an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wenn eine Genehmigungsanforderung vom Flow generiert wird, wird die Arbeitsnotiz mit der folgenden Meldung aktualisiert:

Für wurde eine Genehmigungsanforderung erstellt<task id> Fahren mit Eindämmung fort. Um diese Aufgabe als SOC-Manager zu genehmigen, führen Sie die folgenden Schritte manuell aus:

- Navigieren Sie zur Seite Aufgabengenehmigungen.
- Die Liste der Genehmigungen wird angezeigt. Klicken Sie auf<task id> , der genehmigt werden soll.
- Ändern Sie den Status in **„Genehmigen“**, und speichern Sie das aktualisierte<task id> .

g. Im nächsten Schritt wird der Security Incident-Datensatz aktualisiert, um den Genehmigungsstatus nachzuverfolgen.

h. Als Nächstes wird eine Aufgabe erstellt, um Eindämmungsverfahren zu initiieren.

i. Der Subflow „Create Block Requests for Malicius Observables“ (Anforderungen zum Blockieren von böswilligen erkennbaren Elementen ausführen) wird ausgeführt, und es wird ein Incident-Datensatz mit der Anforderung erstellt, das infizierte Gerät und seine Assets neu zu erstellen.

j. Als Nächstes wird eine Aufgabe erstellt, um die Sichtungssuche auszuführen und zu bestätigen, ob die Umgebung sicher ist.
Die Sichtungssuche wird wiederholt, bis keine Sichtungen gefunden wurden.

k. Als Nächstes wird eine Aufgabe erstellt, um anzuzeigen, dass der Security Incident-Datensatz zur Überprüfung bereit ist.

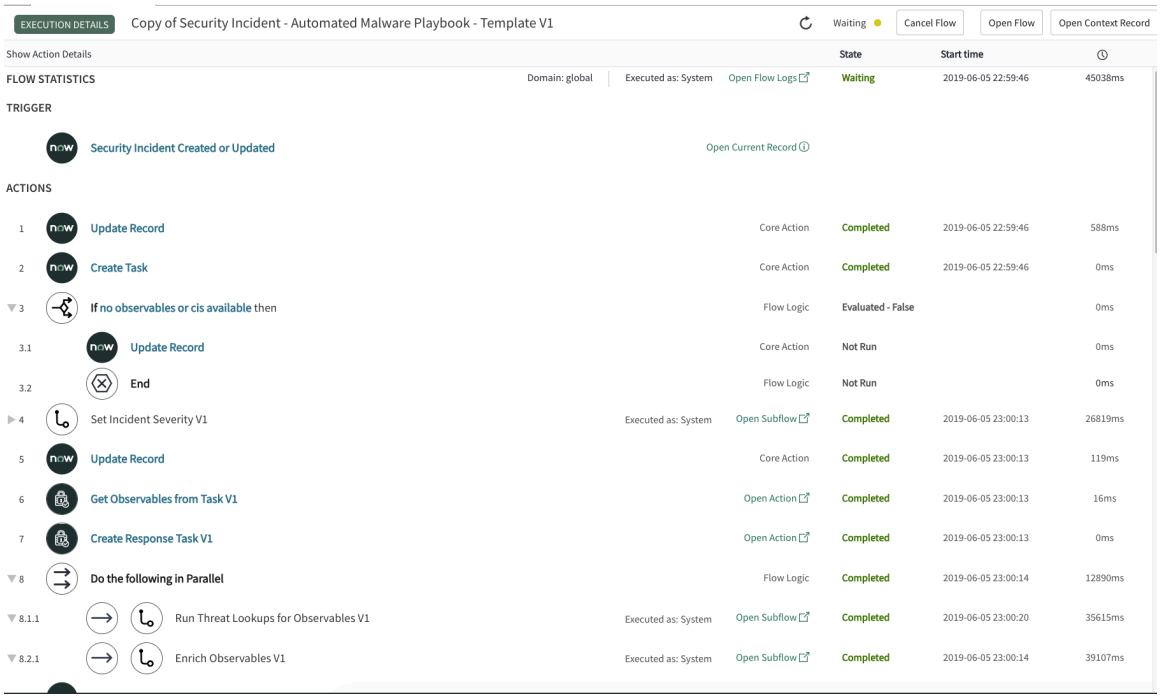
l. Abschließend wird der Datensatz aktualisiert und in die Phase Überprüfen verschoben.

Nächste Maßnahme

Sie können auf **Test** klicken, um die Aktionen im Flow zu simulieren, bevor er veröffentlicht wird. Klicken Sie nach dem Testen des Flows auf **Aktivieren**, um den Flow zu aktivieren, damit er ausgeführt werden kann.

Klicken Sie auf **Ausführungen**, um die Ausführungsdetails des Flow anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Playbook für das Handbuch für fehlgeschlagene Anmeldung

Wenn ein Benutzer bestimmte fehlgeschlagene Anmeldeversuche unternimmt (entsprechend der SIM-Konfiguration), wird ein Security Incident erstellt.

Diese fehlgeschlagenen Anmeldeversuche können entweder falsch positive Meldungen sein oder Versuche von Angreifern, sich Zugriff auf E-Mail-Accounts von Anwendern zu verschaffen. In solchen Szenarien kann das Playbook „Manuelle Fehlgeschlagene Anmeldung“ Anleitung bieten und dazu beitragen, die Untersuchung von Security Incidents mit fehlgeschlagener Anmeldung zu optimieren.

Voraussetzungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Spoke: Security Operations-Spoke installieren (sn_sec_spoke)

Wichtige Funktionen

Das Playbook „Fehlgeschlagene Anmeldung“ umfasst die folgenden Funktionen zur Untersuchung von Security Incidents:

1. Prüft, ob der betroffene Anwender ein aktiver/inaktiver Anwender ist
2. Filtert erkennbare Elemente der zulässigen Liste
3. Ergänzt die erkennbaren Elemente
4. Führt eine automatisierte Bedrohungssuche durch.
5. Sendet eine automatisierte E-Mail an den Anwender, um den fehlgeschlagenen Anmeldeversuch zu bestätigen.
6. Weist dem Analysten Aufgaben zu, um den Benutzerzugriff zu untersuchen
7. Identifiziert schädliche erkennbare Elemente und blockiert IPs und URLs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Setzt das Anwenderpasswort zurück.
9. Aktualisiert den Status des Security Incidents
10. Weist einem Sicherheitsanalysten Aufgaben für die Überprüfung nach Incidents zu.

Erforderliche Fähigkeiten

- Bedrohungssuche (Viren insgesamt, Hybrid-Analyse)
- Anreicherung erkennbarer Elemente (Whist, ReverseWhist)
- Sichtungssuche (Splunk, QRadar)
- Blockierung erkennbarer Elemente (CheckPoint, Palo Alto)

Weitere Informationen finden Sie im ServiceNow Store .

Erfahrung als Sicherheitsanalyst

Anweisungen zur schrittweisen Lösung von Sicherheitsbedrohungen finden Sie unter Beheben Sie Sicherheitsbedrohungen mit dem Playbook.

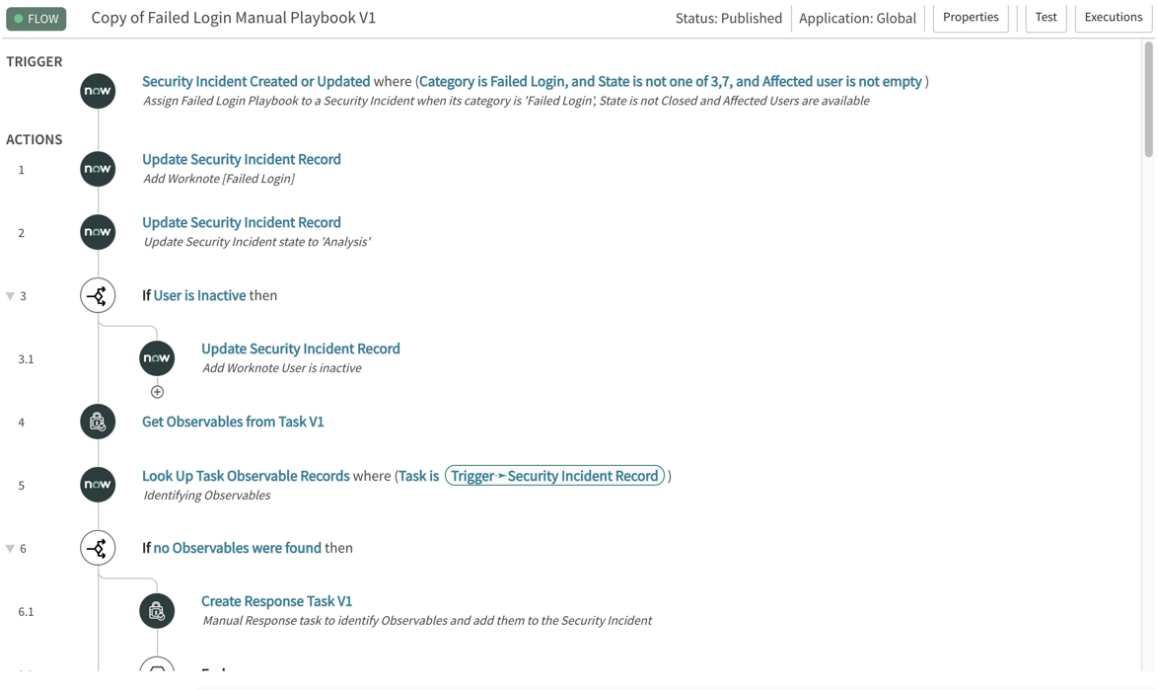
Playbook für fehlgeschlagene Anmeldung mit Flow Designer-Fähigkeiten verwenden

Erste Schritte

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Flow Designer** > **Designer** und klicken Sie auf das Playbook **Fehlgeschlagene Anmeldung**.
3. Erstellen Sie eine Kopie der folgenden Flows, um das Playbook „Fehlgeschlagene Anmeldung“ zu kopieren und die erforderlichen Änderungen vorzunehmen. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen am Flow vorzunehmen.
   - Fehler bei der Anmeldung Manuelles Playbook V1
   - Fehlgeschlagene Anmeldung – Antwort des Anwenders analysieren und Antwortaufgabe aktualisieren V1
4. Nehmen Sie die erforderlichen Änderungen entsprechend Ihrer Anforderung vor. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen am Flow vorzunehmen.
5. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das mit dem Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie Änderungen entsprechend Ihren Anforderungen vorgenommen haben.

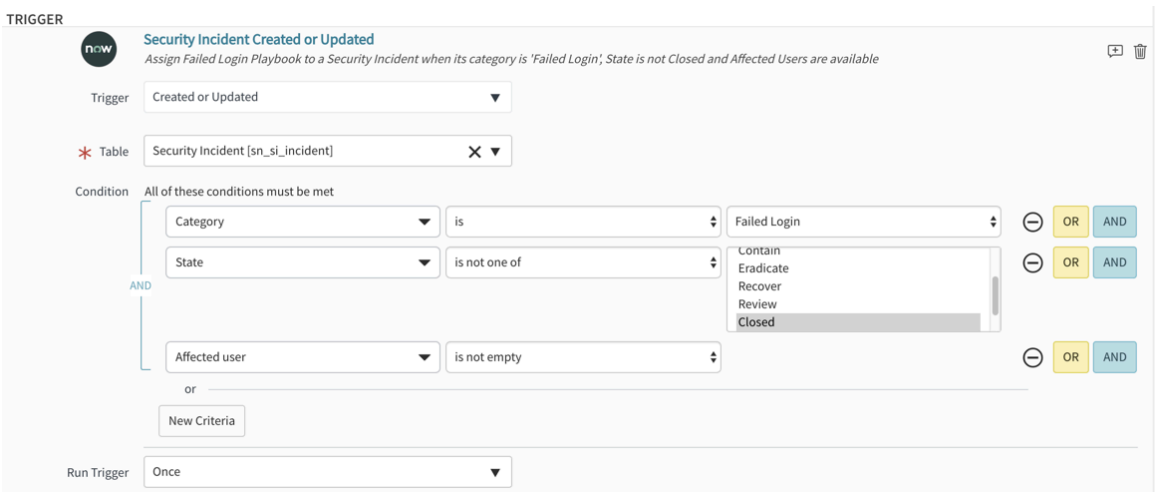
Die folgende Abbildung zeigt eine Kopie des Playbooks „Manuelle Anmeldung fehlgeschlagen“. Überprüfen Sie die folgenden Schritte, um ein Verständnis der verschiedenen Aktionen im Playbook zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

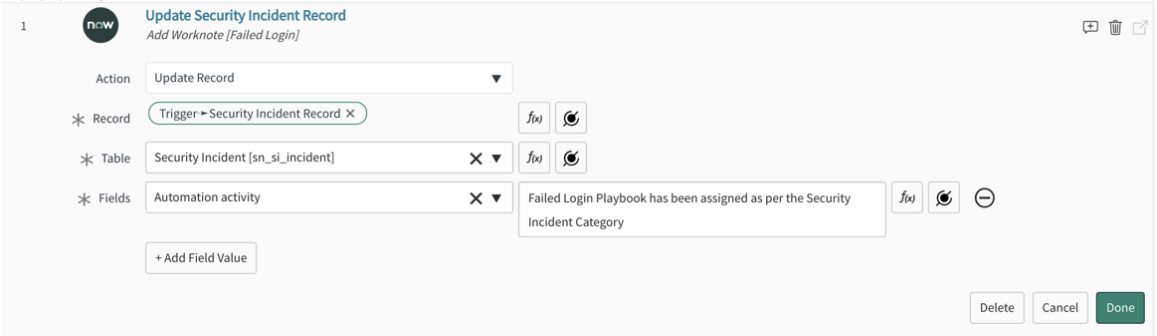
- Kategorie ist „Fehlgeschlagene Anmeldung“.
- Hat mindestens einen betroffenen Anwender
- Security Incident wird nicht geschlossen oder abgebrochen



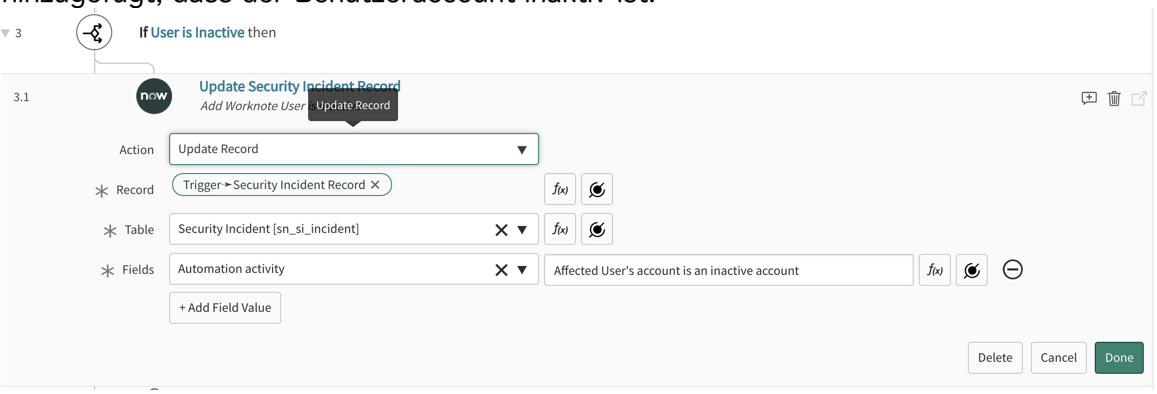
Die folgenden Schritte führen Sie durch die Aktionen, Aufgaben und Subflows, die im Playbook „Manuelle fehlgeschlagene Anmeldung“ verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn die Ausführung des Playbooks in Schritt 1 gestartet wird, wird das Playbook automatisch mit einer Arbeitsnotiz aktualisiert, die zeigt, dass der Security Incident mit der Kategorie „Fehlgeschlagene Anmeldung“ zugewiesen wurde.



2. In Schritt 2 wird das Playbook aktualisiert und in den Status Analyse versetzt.
3. In Schritt 3 prüft das Playbook, ob der betroffene Anwender ein aktiver oder inaktiver Anwender ist. Wenn der Benutzer inaktiv ist, wird dem Security Incident eine Arbeitsnotiz hinzugefügt, dass der Benutzeraccount inaktiv ist.



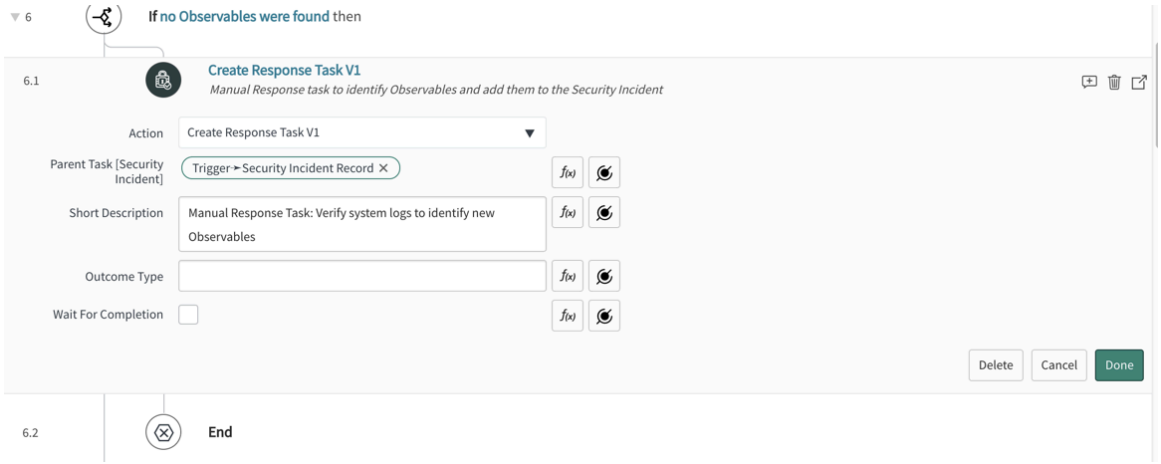
Hinweis:

In Schritt 3 des Flows werden inaktive Benutzer in der Tabelle `sn_si_incident` geprüft, die unter ServiceNowverfügbar ist. Dieser Schritt wird als Leitfaden bereitgestellt und muss für Ihre spezifische Umgebung geändert werden. Wenn Sie diese Funktion verwenden möchten, empfehlen wir die Einrichtung einer Active Directory-Integration in Ihrer Umgebung. Sie können mit Ihrer Active Directory-Integration den Benutzerstatus ermitteln und abhängig von der Antwort die nächsten Schritte für Ihr Playbook entwerfen.

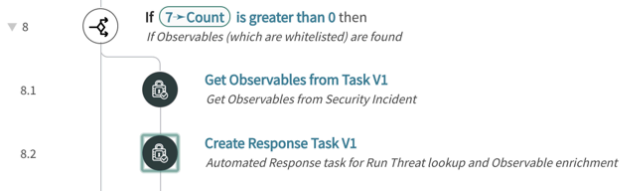
Wenn Sie keine Active Directory-Integration haben, ersetzen Sie diesen Schritt durch eine manuelle Aufgabe für den Sicherheitsanalysten, um mit dem IT-Team zusammenzuarbeiten, um den Anwender zu blockieren und mit den restlichen Schritten im Playbook fortzufahren.

4. In Schritt 4 werden die erkennbaren Elemente für den Security Incident abgerufen.
5. In Schritt 5 werden die erkennbaren Elemente identifiziert.
6. Wenn keine erkennbaren Elemente gefunden werden, wird in Schritt 6 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.

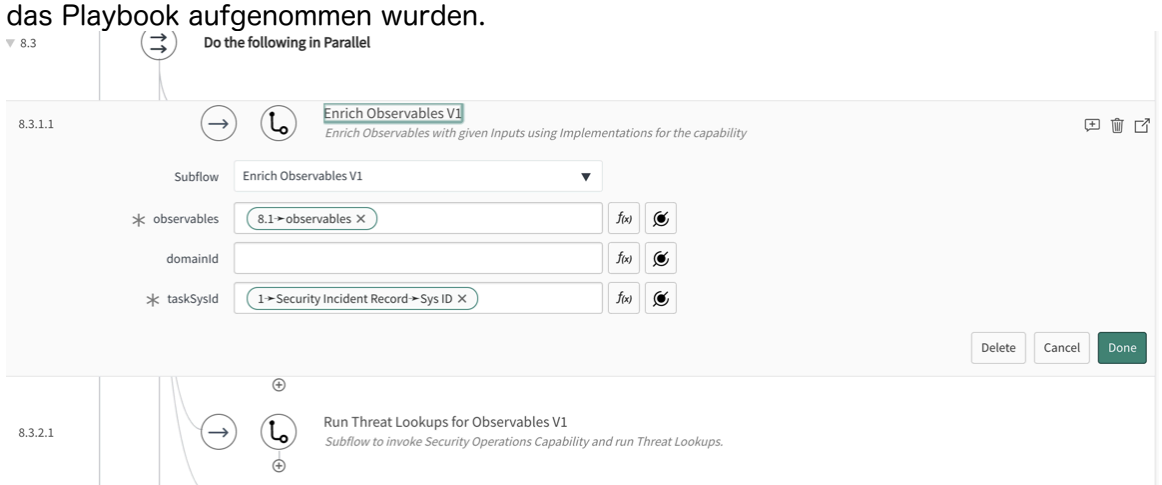
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wenn in Schritt 7 erkennbare Elemente gefunden werden, werden erkennbare Elemente identifiziert, die nicht in die Liste aufgenommen werden dürfen.
8. Wenn mindestens eines der erkennbaren Elemente nicht in die Liste aufgenommen werden kann, werden die folgenden Schritte ausgeführt:
   a. Die Schritte 8.1 und 8.2 werden ausgeführt. Erkennbare Elemente werden abgerufen, und eine automatisierte Antwortaufgabe wird initiiert.



   b. Nachdem die automatisierte Aufgabe erstellt wurde, wird Schritt 8.3 (8.3.1.1 und 8.3.2.1) ausgeführt, und die Integrationen „Erkennbare Elemente anreichern“ und „Bedrohungssuche“ werden ausgeführt. Beachten Sie, dass dies Subflows sind, die in das Playbook aufgenommen wurden.



   c. In Schritt 8.4 wird der Security Incident-Datensatz aktualisiert, nachdem die Integrationen abgeschlossen wurden.
   d. In Schritt 8.5 wird eine neue Antwortaufgabe erstellt, um die nächste automatisierte Aufgabe anzugeben, die ausgeführt wird.
   e. In Schritt 8.6 wird die Integration der Sichtungssuche für die erkennbaren Elemente ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Nachdem der Subflow „Sichtungssuche“ in Schritt 8.7 abgeschlossen wurde, wird der Security Incident aktualisiert.

g. In Schritt 8.8 werden die erkennbaren Elemente auf Schädlichkeit überprüft.

h. Wenn die erkennbaren Elemente nicht schädlich sind und der Benutzeraccount aktiv ist, wird eine automatisierte E-Mail an den Benutzer gesendet, um die fehlgeschlagenen Anmeldeversuche zu bestätigen. Es wird eine manuelle Antwortaufgabe erstellt, um die erkennbaren Elemente zu identifizieren und dem Security Incident hinzuzufügen. Das Playbook endet dann in dieser Phase.

i. Wenn die erkennbaren Elemente schädlich sind, werden drei Antwortaufgaben erstellt:

i. Es wird eine automatisierte E-Mail an den Anwender gesendet, um die fehlgeschlagenen Anmeldeversuche zu bestätigen **(Ja oder Nein)**. Wenn der Benutzer mit „Ja“ antwortet:

1. Der Status des Security Incidents wird auf **„Eindämmen“**aktualisiert.

2. Es wird eine automatisierte E-Mail an den Anwender gesendet, in der er aufgefordert wird, das Passwort zurückzusetzen.

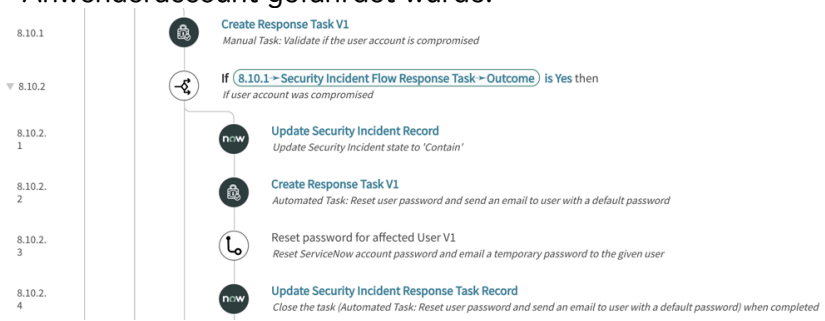
3. Wenn die Aufgabe abgeschlossen wurde, wird der Subflow „Passwort zurücksetzen“ initiiert, und es wird eine E-Mail an den Benutzer gesendet.

Hinweis:
Der Schritt „Passwort zurücksetzen“ dient als Leitfaden. Die Schritte im Flow setzen das Passwort für den Account des Anwenders im ServiceNow-System zurück. Der Vorgang zum Zurücksetzen des Passworts kann jedoch je nach Umgebung unterschiedlich sein. Sie können Ihre Active Directory-Integration überprüfen, um das Passwort von Anwendern automatisch zurückzusetzen. Wenn Sie keine Active Directory-Integration haben, ersetzen Sie diesen Schritt durch eine manuelle Aufgabe für den Sicherheitsanalysten, um mit dem entsprechenden IT-Team zusammenzuarbeiten, um das Passwort der Anwender zurückzusetzen und nach Abschluss des jeweiligen mit den restlichen Schritten im Playbook fortzufahren Aufgabe

ii. Wenn der Benutzer mit Nein antwortet, wird eine automatisierte E-Mail an den Benutzer gesendet, um die Antwort zu bestätigen. Der Sicherheitsanalyst muss manuell entsprechende Maßnahmen ergreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

iii. Wenn der Benutzer nicht auf die automatisierte E-Mail antwortet, muss der Sicherheitsanalyst den Security Incident manuell aktualisieren und eine Antwort geben. Es wird eine manuelle Aufgabe erstellt, um zu überprüfen, ob der Anwenderaccount gefährdet wurde.



9. In Schritt 8.10.3 wird der Status des Security Incident aktualisiert.
10. In Schritt 8.10.4 wird eine automatisierte Aufgabe erstellt, um zu überprüfen, ob die Implementierung der Fähigkeit „Blockierungsanforderungen für schädliche IPs und URLs erstellen“ verfügbar ist. Wenn die Fähigkeitsimplementierung verfügbar ist, wird der Subflow „Blockanforderungen erstellen“ ausgeführt. Wenn nicht verfügbar ist, wird der Security Incident aktualisiert und eine Arbeitsnotiz wird veröffentlicht, um darauf hinzuweisen, dass die Fähigkeitsimplementierung nicht verfügbar ist.
11. In Schritt 9 wird der Security Incident aktualisiert, und der Status wird auf **Überprüfen**festgelegt.
12. In Schritt 10 wird eine Antwortaufgabe erstellt, damit der Benutzer die Überprüfung nach dem Incident abschließen kann, bevor die Aufgabe geschlossen wird.

Playbook für die Automatisierung von untergeordneten Security Incidents

Doppelte Security Incidents werden als untergeordnete Security Incidents kategorisiert und zu den übergeordneten Security Incidents zusammengefasst.

Mit dem Playbook zur Automatisierung von untergeordneten Security Incidents können Sie die Zeit zum Untersuchen und Schließen doppelter Security Incidents reduzieren. Dieses Playbook führt automatisch ein Rollup für bestimmte eindeutige Artefakte des untergeordneten Security Incidents (erkennbare Elemente, betroffene Benutzer, CIs) für den übergeordneten Security Incident durch.

Voraussetzungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Spoke: Security Operations-Spoke installieren (sn_sec_spoke)

Wichtige Funktionen

Das Playbook „Automatisierung untergeordneter Elemente“ deckt die folgenden Funktionen ab:

1. Verschiebt den Security Incident in die **Analysephase**.
2. Er beseitigt Duplikate und fügt die betroffenen Benutzer und CIs dem übergeordneten Security Incident hinzu (Rollup).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Fügt dem übergeordneten Security Incident erkennbare Elemente aus dem untergeordneten Incident hinzu.
4. Schließt den untergeordneten Security Incident oder bricht ihn ab, wenn der übergeordnete Security Incident geschlossen wird.

Erforderliche Fähigkeiten

Weitere Informationen finden Sie im ServiceNow Store .

Erfahrung als Sicherheitsanalyst

Anweisungen zur schrittweisen Lösung von Sicherheitsbedrohungen finden Sie unter Beheben Sie Sicherheitsbedrohungen mit dem Playbook.

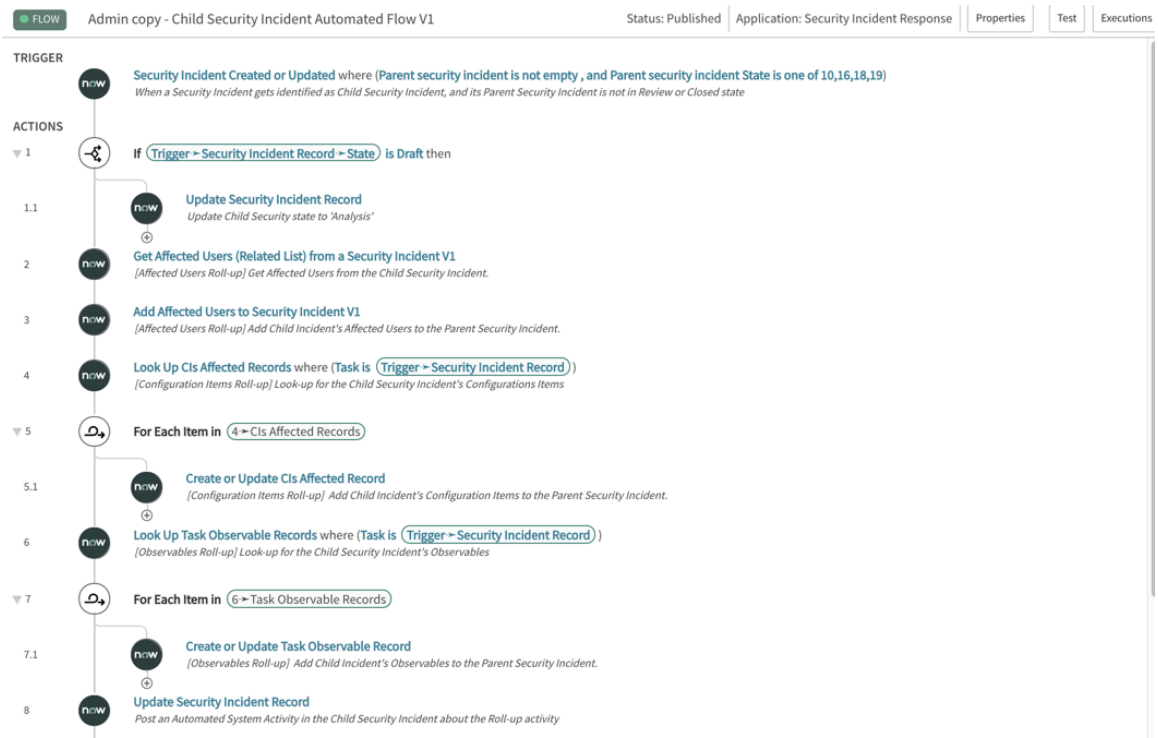
Vertieftes Verständnis des Playbooks „Automatisierung von untergeordneten Security Incidents“ mit Flow Designer-Fähigkeiten

Erste Schritte

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Flow Designer** > **Designer** und klicken Sie auf das Playbook Fehlgeschlagene Anmeldung.
3. Erstellen Sie eine Kopie des Playbooks „Automatisierung von untergeordneten Security Incidents“, und nehmen Sie die erforderlichen Änderungen vor. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen am Flow vorzunehmen.
4. Nehmen Sie die erforderlichen Änderungen entsprechend Ihrer Anforderung vor. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen am Flow vorzunehmen.
5. Aktivieren Sie das Playbook.
   - Aktivieren Sie den Haupt-Flow, um das mit dem Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie den kopierten Flow, nachdem Sie Änderungen entsprechend Ihren Anforderungen vorgenommen haben.

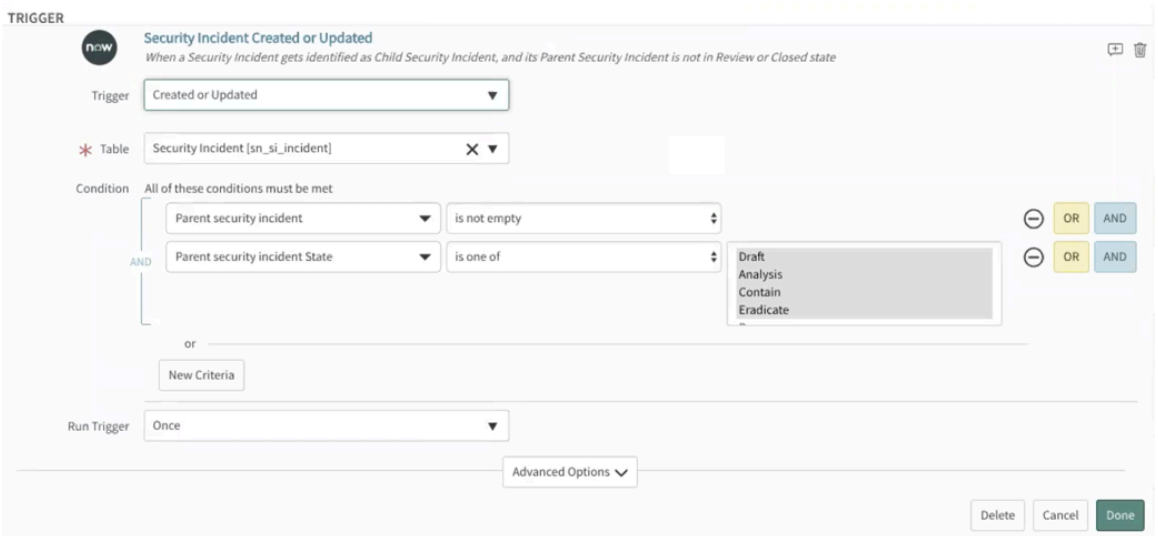
Die folgende Abbildung zeigt eine Kopie des Playbooks „Automatisierung von untergeordneten Security Incidents“. Überprüfen Sie die folgenden Schritte, um ein Verständnis der verschiedenen Aktionen im Playbook zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Playbook wird ausgelöst, wenn:

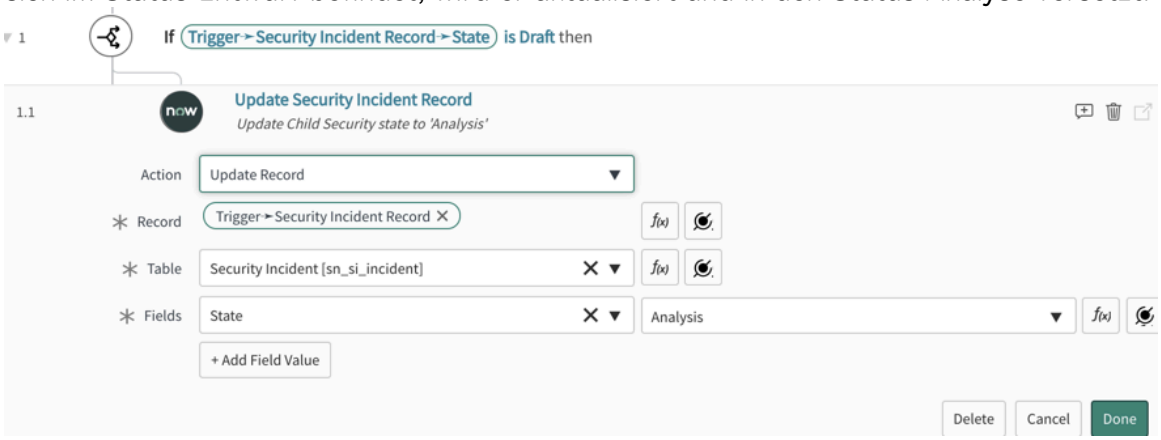
- Das Feld „Übergeordneter Security Incident“ ist nicht leer.
- Der übergeordnete Security Incident befindet sich im Status Entwurf, Analyse, Eindämmen oder Löschen.



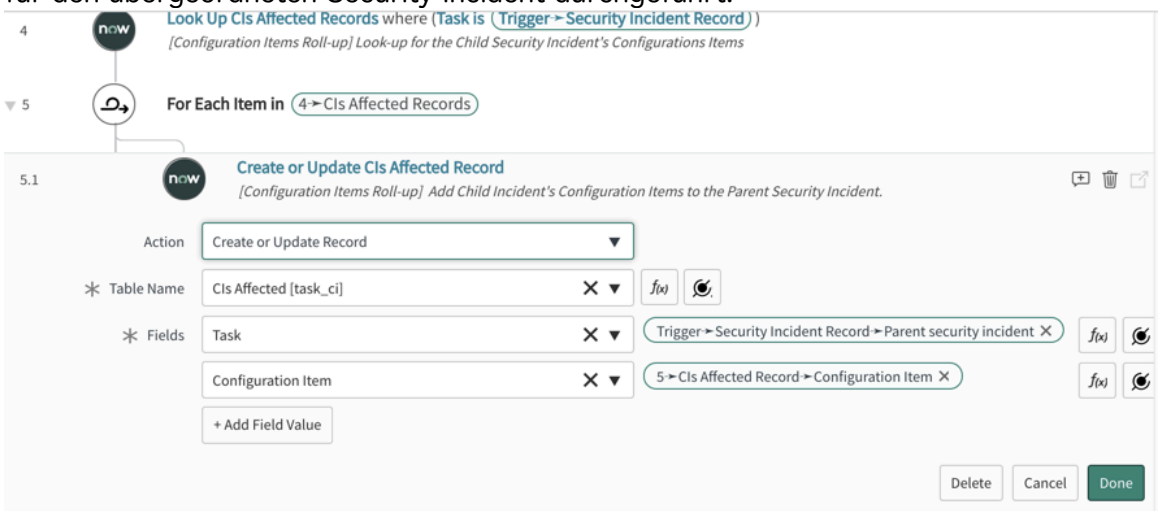
Die folgenden Schritte führen Sie durch die Aktionen und Aufgaben, die im Playbook zur Automatisierung von untergeordneten Security Incidents verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

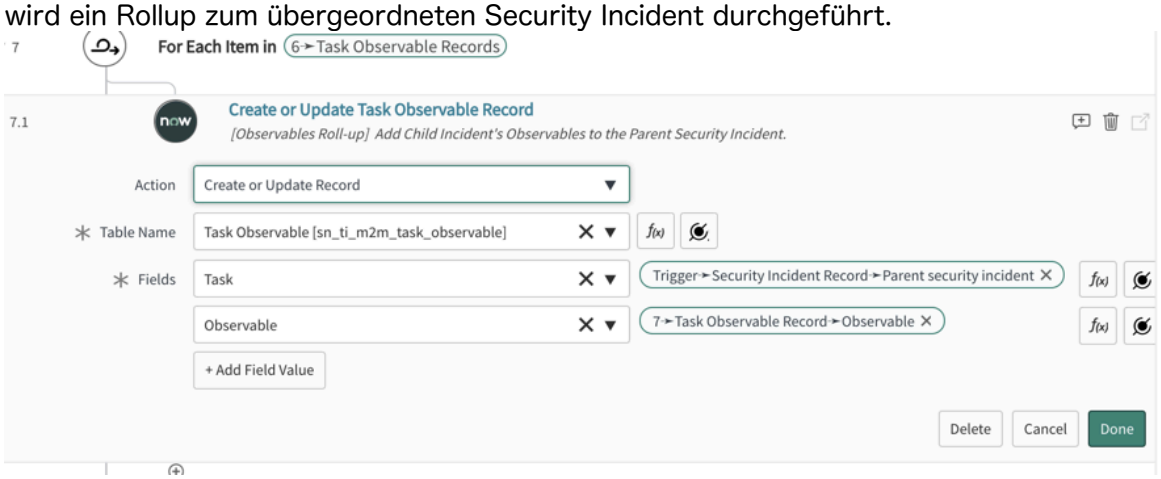
1. Wenn die Ausführung des Playbooks in Schritt 1 gestartet wird und der Security Incident sich im Status Entwurf befindet, wird er aktualisiert und in den Status Analyse versetzt.



2. In den Schritten 2 und 3 werden die betroffenen Anwender für den Security Incident abgerufen und im übergeordneten Security Incident zusammengefasst. Doppelte Benutzer werden eliminiert.
3. In den Schritten 4 und 5 werden die dem untergeordneten Security Incident zugeordneten Konfigurationselemente abgerufen, und für eindeutige CIs wird ein Rollup für den übergeordneten Security Incident durchgeführt.



4. In den Schritten 6 und 7 werden die dem untergeordneten Security Incident zugeordneten erkennbaren Elemente abgerufen, und für eindeutige erkennbare Elemente wird ein Rollup zum übergeordneten Security Incident durchgeführt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. In den Schritten 8 und 9 werden automatisierte Arbeitsnotizen in den übergeordneten und untergeordneten Security Incidents veröffentlicht, die angeben, dass für die betroffenen Anwender, Konfigurationselemente und erkennbaren Elemente ein Rollup vom untergeordneten zum übergeordneten Security Incident durchgeführt wurde.

Playbook für Office 365 – schädliche Datei erkannt

Dieses Playbook bietet systematische Korrekturschritte für die Untersuchung schädlicher Dateien, die in Office 365 erkannt wurden.

Wenn in Office 365 schädliche Dateien erkannt werden, können Sie sich im Flow Designer mit dem Playbook „365 – Böswillige Datei erkannt“ vertraut machen und die Untersuchung dieser schädlichen Dateien optimieren.

Richten Sie das Playbook „Böswillige Office-Datei erkannt“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Böswillige Office-Datei erkannt“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

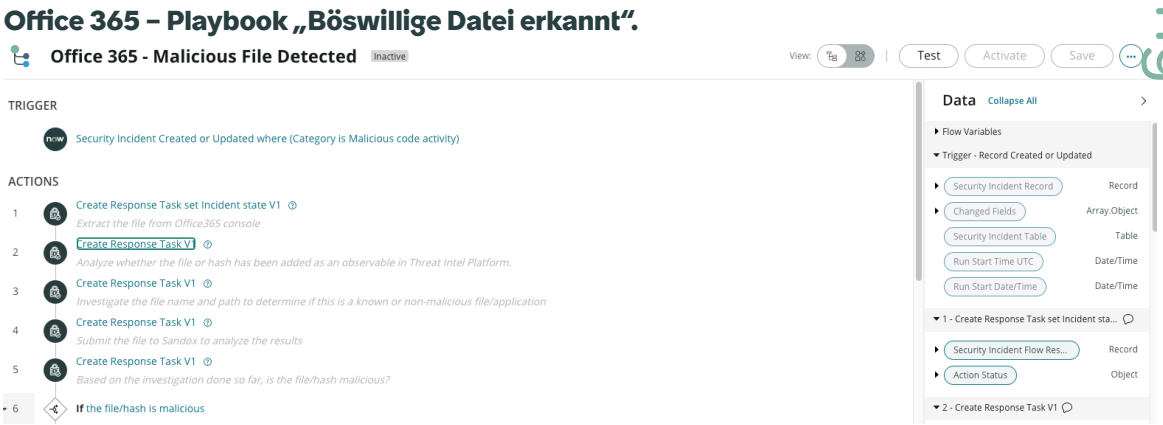
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **Office 365 – Böswillige Datei erkannt aus**.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows „Office 365 – schädliche Datei erkannt“ erstellen und die erforderlichen Änderungen vornehmen.

   Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.



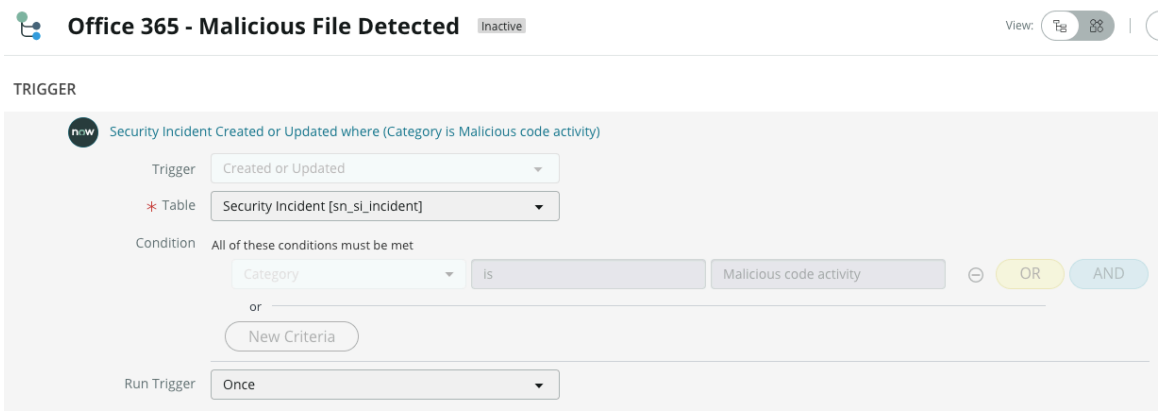
4. Aktivieren Sie die Playbooks.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
- Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieBöswillige Code-Aktivität**lautet.



Verwenden Sie das Playbook „Office 365 Böswillige Datei erkannt“.

Verwenden Sie dieses Playbook, um in Office 365 erkannte schädliche Dateien zu untersuchen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Office 365 Böswillige Datei erkannt“ verfügbar sind.

Vorbereitungen

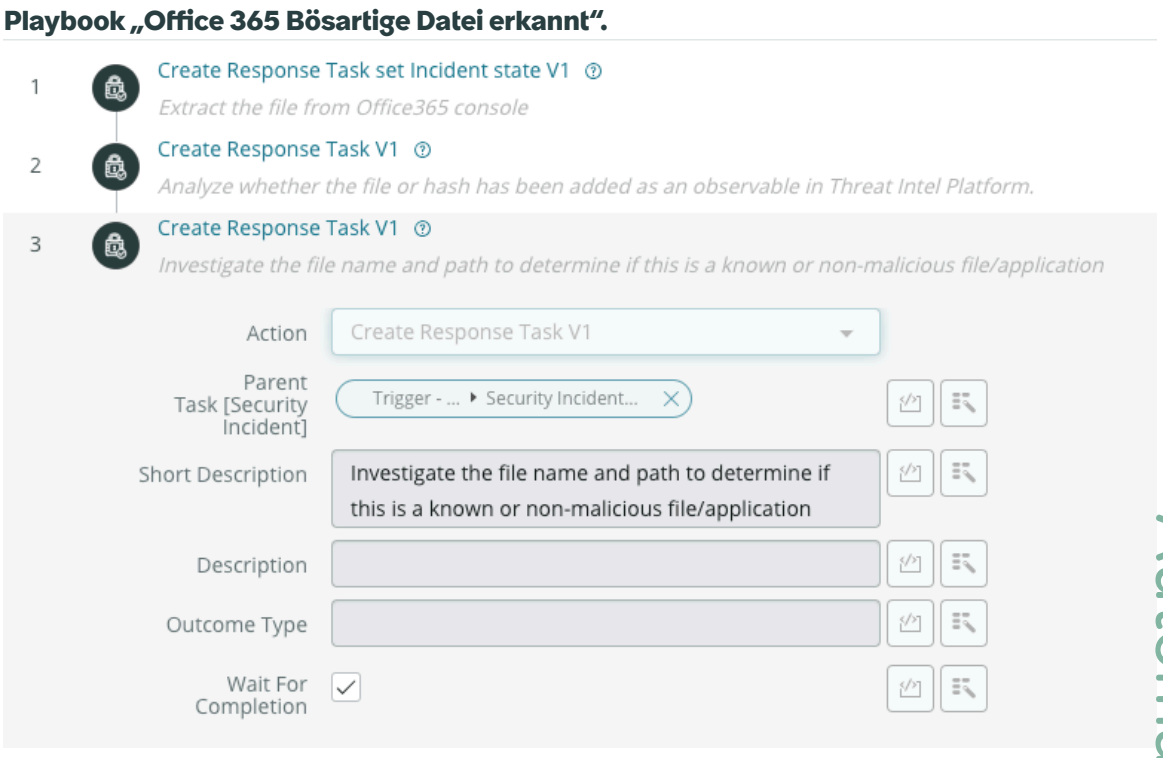
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, müssen Sie in Aktion 1 die schädliche Datei aus der Office 365-Konsole extrahieren.
2. In Aktion 2 müssen Sie analysieren, ob die Datei oder der Hash als erkennbares Element in der Threat Intel Platform hinzugefügt wurde.
3. In Aktion 3 müssen Sie den Dateinamen und Pfad untersuchen, um festzustellen, ob es sich um eine bekannte oder nicht schädliche Datei/Anwendung handelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. In Aktion 4 müssen Sie die Datei zur Analyse der Ergebnisse an die Sandbox übermitteln.
5. In Aktion 5 müssen Sie basierend auf den bisher durchgeführten Untersuchungen überprüfen, ob die Datei oder der Hash schädlich ist oder nicht.
   Wenn die Datei oder der Hash nicht schädlich ist, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.
6. Wenn in Aktion 6 die Datei oder der Hash schädlich ist, werden die Aktionen 7 und 8 ausgeführt.
7. In Aktion 7 müssen Sie beim Endanwender eine stichhaltige geschäftliche Begründung dafür einholen, warum er eine schädliche Datei auf dem Gerät gespeichert hat.
   Wenn die Datei oder der Hash böswillig ist, können Sie die bereits vorhandene E-Mail-Vorlage im Playbook verwenden, um den Endanwender per E-Mail um Klärung zu bitten.
8. In Aktion 8 müssen Sie überprüfen, ob der Endanwender eine gültige geschäftliche Begründung angegeben hat.
   Wenn der Endanwender eine gültige geschäftliche Begründung angegeben hat, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.
9. Wenn der Anwender in Aktion 9 keine stichhaltige geschäftliche Begründung angegeben hat, werden die Aktionen 10, 11 und 12 ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Da in Aktion 10 keine stichhaltigen geschäftlichen Begründungen vorlagen, können Sie die schädliche Datei oder den schädlichen Hash zur Überprüfung an das Threat Intel Team weiterleiten.
11. In Aktion 11 müssen Sie das Skript für den Malware-Bytes-Scanner ausführen, um zu überprüfen, ob die Datei oder der Hash schädlich ist.
12. In Aktion 12 müssen Sie eine forensische Analyse durchführen, um zu überprüfen, ob die Datei oder der Hash schädlich ist.
13. In Aktion 13 wird eine Antwortaufgabe erstellt, damit der Benutzer die Überprüfung nach dem Incident abschließen kann, bevor die Aufgabe geschlossen wird.

Playbook für Wiederholungserkennung

Mit diesem Playbook können Sie feststellen, ob die Incident-Antwort in der Vergangenheit zu einem genauen oder ähnlichen Phishing-Bericht bereitgestellt wurde, und funktioniert automatisch auf den neuen Bericht ähnlich.

Das Playbook zur Wiederholungserkennung überprüft, ob der neu gemeldete Phishing-Incident einem früheren Incident ähnelt. Wenn die Wiederholungserkennung identifiziert wird, werden dem Analysten der entsprechende Security Incident und die Lösungsdetails zur Verfügung gestellt. Er kann sie für den neu gemeldeten Incident verwenden. Dies führt zu einer schnellen Korrektur des Security Incidents.

Richten Sie das Playbook „Wiederholungserkennung“ ein

Führen Sie die folgenden Schritte aus, um das Playbook für die Wiederholungserkennung einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist. Sie können die folgenden Systemeigenschaften ändern:

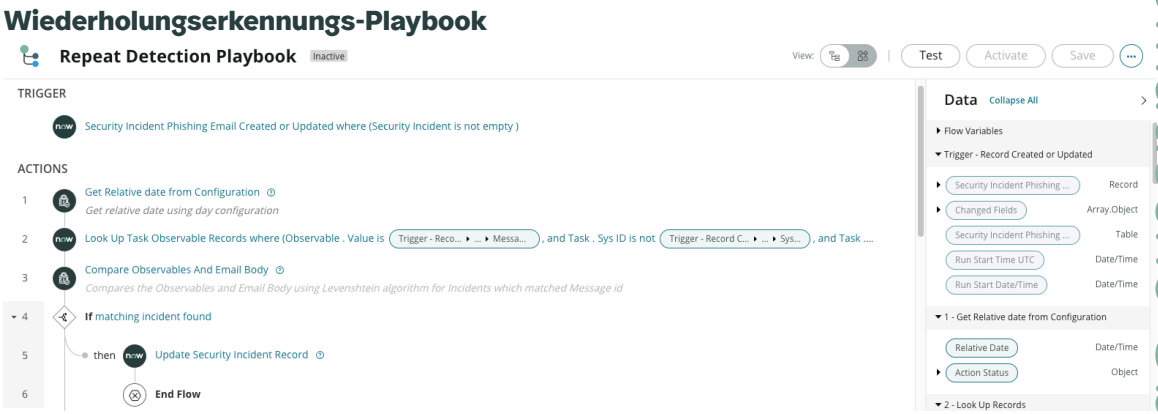
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *sn_sec_spoke.similarphish.earlyterminationscore*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxcomparionsize*
- *sn_sec_spoke.similarphish.minmatchscore*

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Wiederholungserkennungs** -Playbook aus.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows zur Wiederholungserkennung erstellen und die erforderlichen Änderungen vornehmen.

   Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

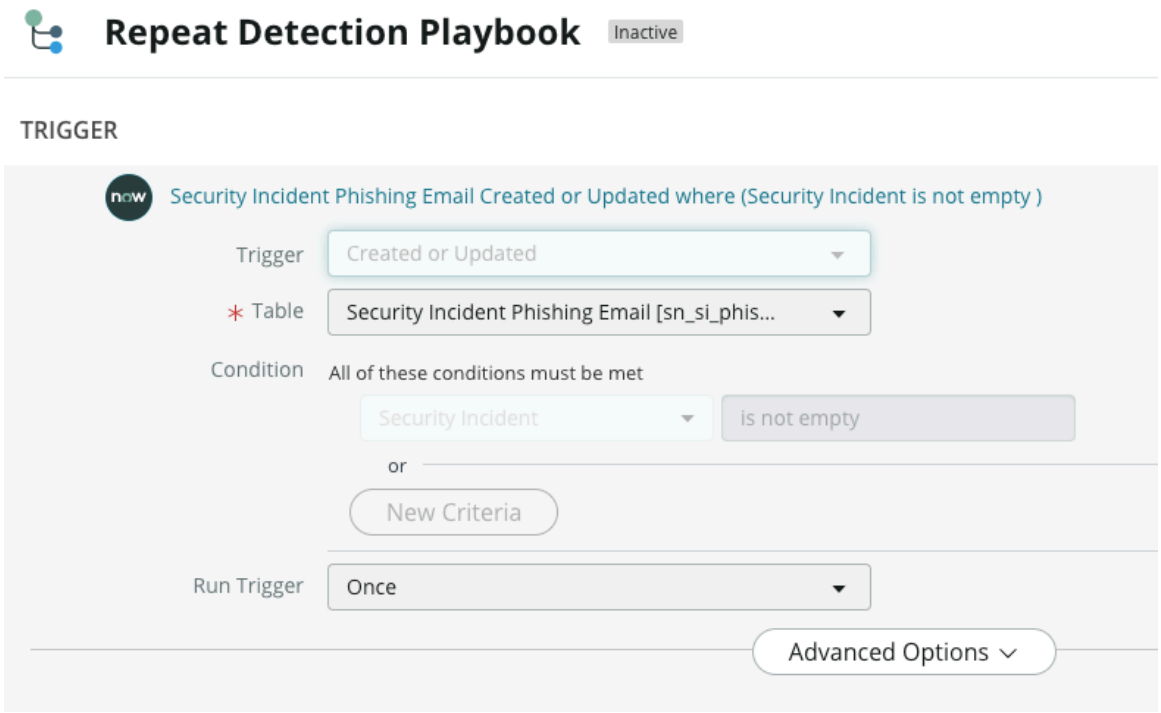


4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst, wenn der **Security Incident nicht leer ist**.



Verwenden Sie das Playbook „Wiederholungserkennung“.

Verwenden Sie dieses Playbook, um zu untersuchen, ob die Incident-Antwort in der Vergangenheit für einen genauen oder ähnlichen Phishing-Bericht bereitgestellt wurde und automatisch für den neuen Bericht in ähnlicher Weise funktioniert. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook für Wiederholungserkennungen verfügbar sind.

Vorbereitungen

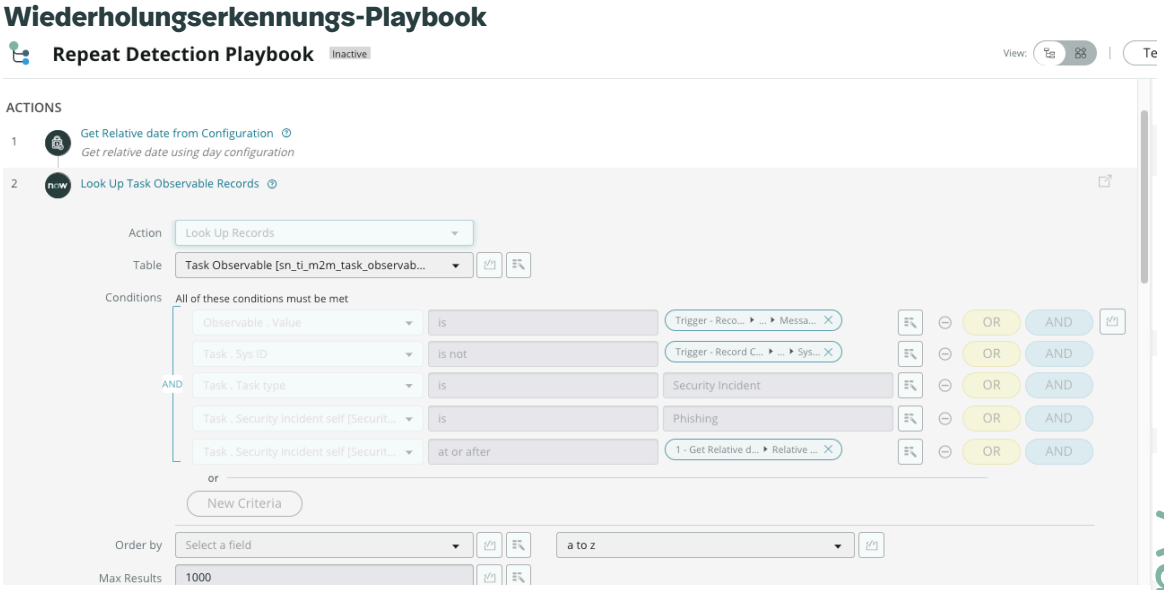
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

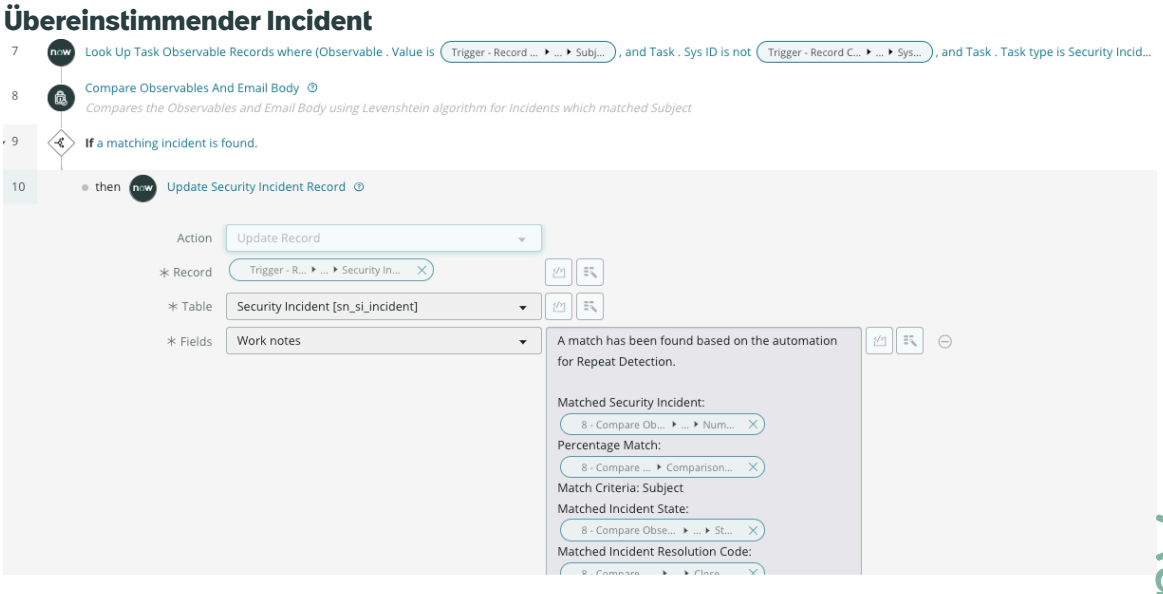
1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, ruft das Playbook in Aktion 1 das relative Datum des Security Incident mithilfe der Tageskonfiguration ab.
2. In Aktion 2 sucht das Playbook in der Tabelle `sn_ti_m2m_task_observable` nach den Datensätzen erkennbarer Aufgabenelemente, die dem Incident entsprechen, basierend auf der Nachrichten-ID.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. In Aktion 3 vergleicht das Playbook die erkennbaren Elemente der Aufgabe und den E-Mail-Text mithilfe des Levenshtein-Algorithmus für Incidents, die der Nachrichten-ID entsprechen.
4. In Aktion 4 prüft das Playbook auf Grundlage der bisher durchgeführten Untersuchungen, ob der übereinstimmende Incident anhand der Nachrichten-ID gefunden wurde oder nicht.
   Wenn in Aktion 5 der übereinstimmende Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz und gibt an, dass basierend auf der Automatisierung für die Wiederholungserkennung eine Übereinstimmung gefunden wurde. In Aktion 6 endet der Flow.
5. Wenn kein passender Incident gefunden wird, sucht das Playbook in Aktion 7 in der Tabelle `sn_ti_m2m_task_observable` nach den Datensätzen erkennbarer Aufgabenelemente, die dem Incident entsprechen, basierend auf dem Betreff.
6. In Aktion 8 vergleicht das Playbook die erkennbaren Elemente der Aufgabe und den E-Mail-Text mithilfe des Levenshtein-Algorithmus für Incidents, die dem Betreff entsprechen.
7. In Aktion 9 überprüft das Playbook, ob der passende Incident gefunden wurde.
   Wenn in Aktion 10 der übereinstimmende Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz und gibt an, dass basierend auf der Automatisierung für die Wiederholungserkennung eine Übereinstimmung gefunden wurde. In Aktion 11 endet der Flow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. In Aktion 12 sucht das Playbook in der Tabelle *sn_ti_m2m_task_observable* nach den Datensätzen erkennbarer Aufgabenelemente, die dem Incident entsprechen, basierend auf der Adresse.
9. In Aktion 13 vergleicht das Playbook die erkennbaren Elemente der Aufgabe und den E-Mail-Text mithilfe des Levenshtein-Algorithmus für Incidents, die mit der Adresse übereinstimmen.
10. In Aktion 14 überprüft das Playbook, ob der übereinstimmende Incident anhand der Adresse gefunden wurde oder nicht.
    Wenn in Aktion 15 der übereinstimmende Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz und gibt an, dass basierend auf der Automatisierung für die Wiederholungserkennung eine Übereinstimmung gefunden wurde. In Aktion 16 endet der Flow.

Playbook für gefälschte E-Mails (mit demselben Anzeigenamen)

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von gefälschten E-Mails, die ausgelöst werden, wenn gefälschte Namen für E-Mails an die Mitarbeiter des Unternehmens gesendet werden.

Richten Sie das Playbook für gefälschte E-Mails ein

Führen Sie die folgenden Schritte aus, um das Playbook für gefälschte E-Mails einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

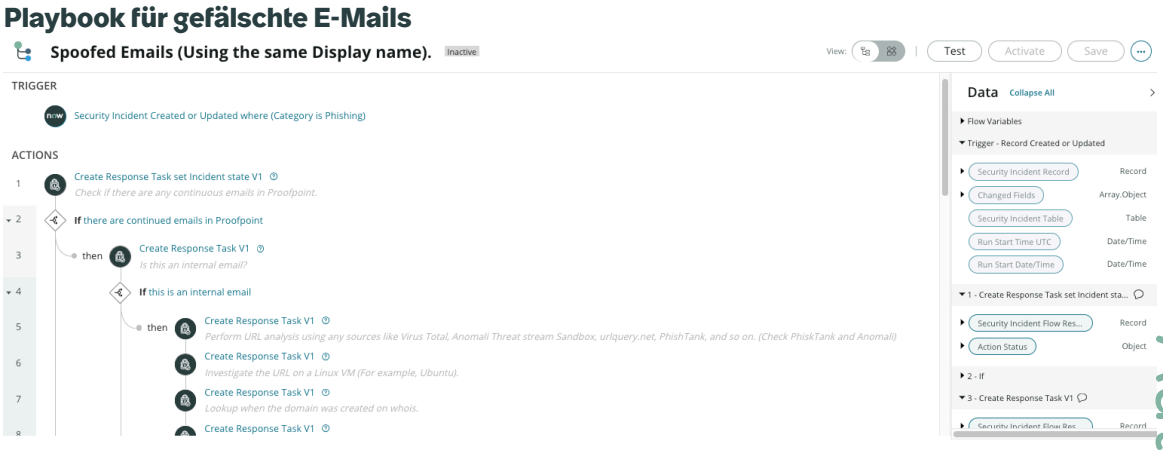
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **Gefälschte E-Mails (mit demselben Anzeigenamen)** aus.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows zur Wiederholungserkennung erstellen und die erforderlichen Änderungen vornehmen.

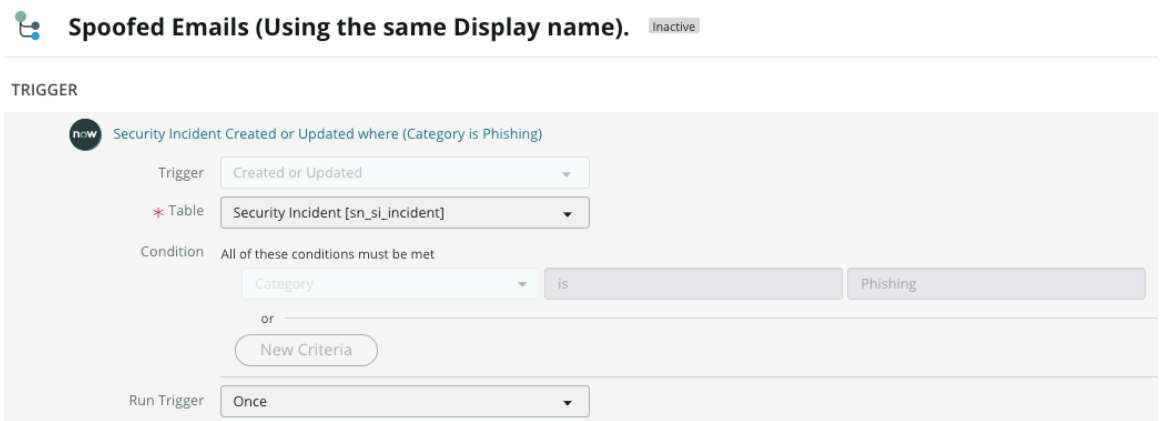
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategoriePhishing**lautet.



Verwenden Sie das Playbook „Gefälschte E-Mails“ (mit demselben Anzeigenamen).

Verwenden Sie dieses Playbook, um gefälschte E-Mails zu untersuchen, die ausgelöst werden, wenn gefälschte Namen für E-Mails an die Mitarbeiter der Organisation gesendet werden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook Gefälschte E-Mails (mit demselben Anzeigenamen) verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_si.admin
- flow_designer

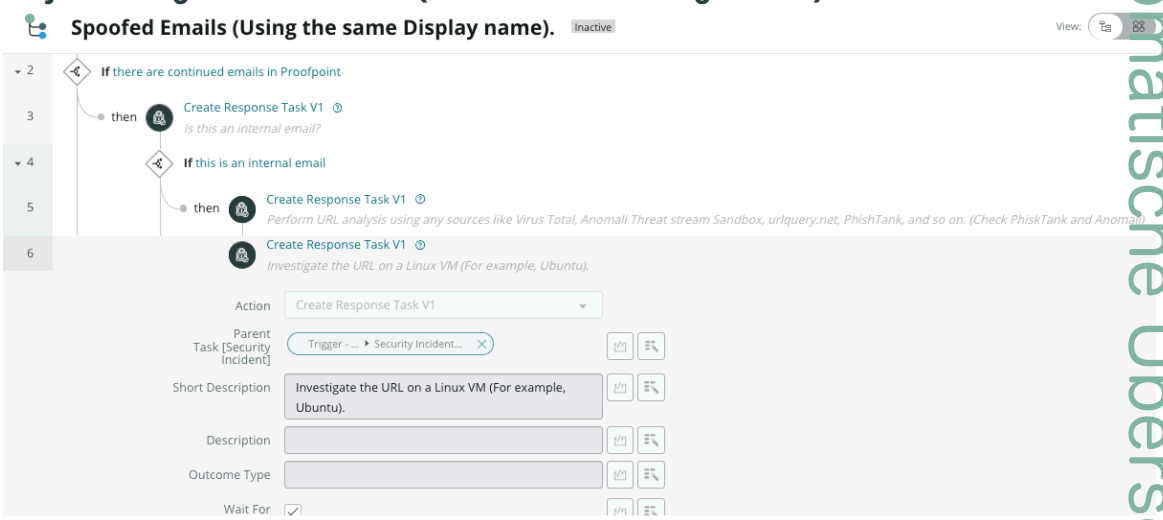
Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob in Proofpoint fortlaufend gefälschte E-Mails vorhanden sind.
2. Wenn in Aktion 2 kontinuierlich E-Mails in Proofpoint vorhanden sind, überprüfen Sie, ob es sich um eine intern gefälschte E-Mail handelt oder nicht.
3. Wenn es sich in Aktion 3 um eine intern gefälschte E-Mail handelt, führen Sie die folgenden Aktionen aus:

   a. In Aktion 5 müssen Sie eine URL-Analyse mit Quellen wie Virus Total, Anomali Threat Stream Sandbox, urlquery.net, PhishTank durchführen (prüfen Sie beispielsweise PhiskTank und Anomali).

   b. In Aktion 6 müssen Sie die URL auf einer Linux-VM (z. B. Ubuntu) untersuchen.

Playbook für gefälschte E-Mails (mit demselben Anzeigenamen).

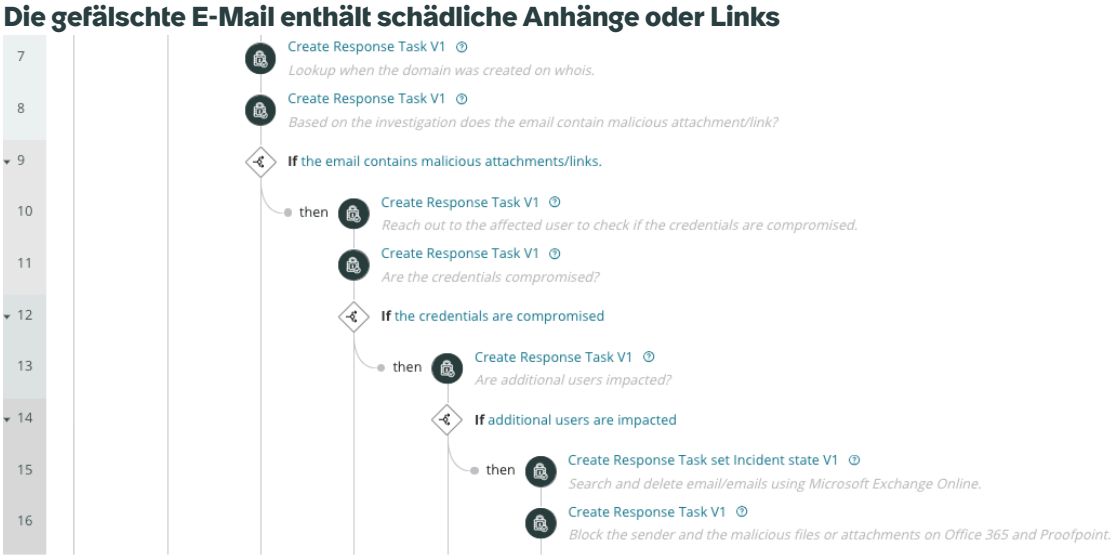


   c. In Aktion 7 müssen Sie suchen, wann die Domäne in WHOIS erstellt wurde.
   Suchen Sie nach kürzlich registrierten Domänen (innerhalb der letzten Woche), die verdächtig sind und eine hohe Wahrscheinlichkeit von Phishing-Angriffen aufweisen.

   d. In Aktion 8 müssen Sie basierend auf der bisher durchgeführten Untersuchung überprüfen, ob diese E-Mail einen schädlichen Anhang oder Link enthält.
   Wenn diese E-Mail keinen schädlichen Anhang oder Link enthält, wird der Flow beendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wenn die E-Mail in Aktion 9 schädliche Anhänge oder Links enthält, führen Sie die folgenden Aktionen aus.

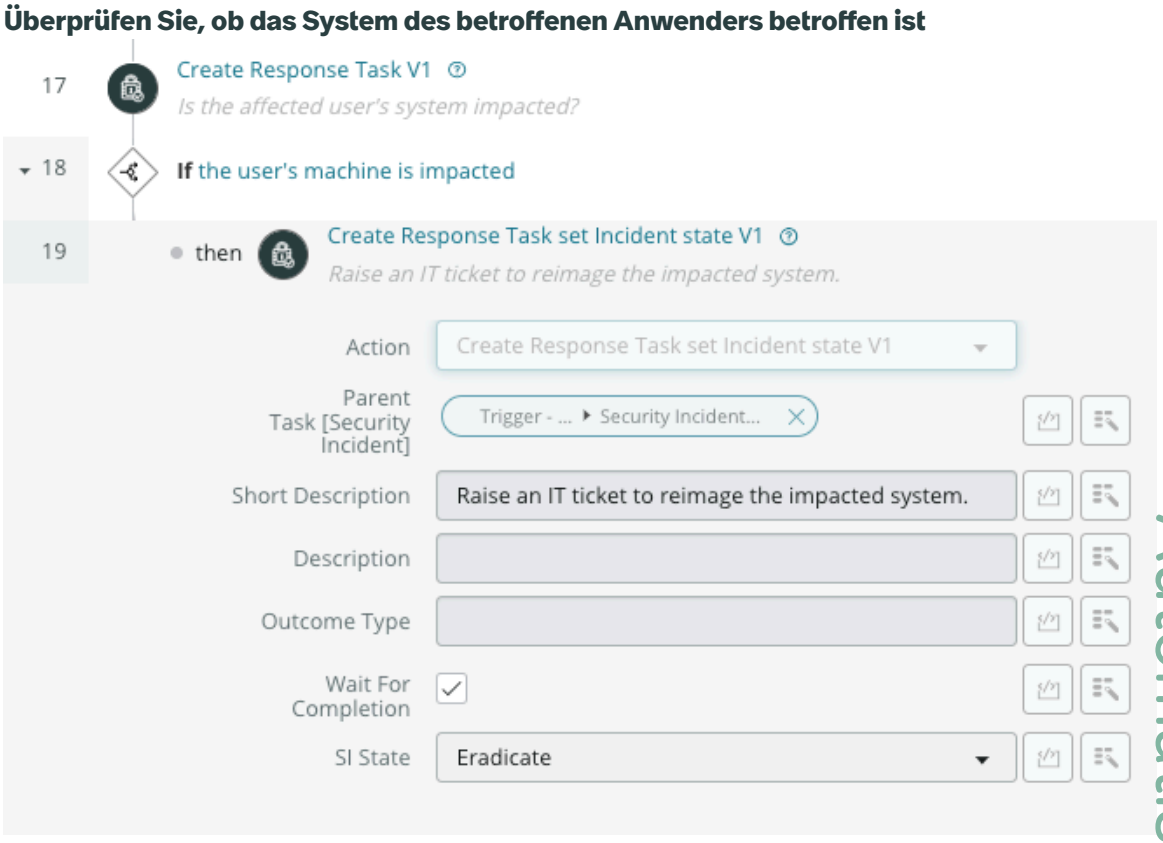
i. In Aktion 10 müssen Sie sich an den betroffenen Anwender wenden, um zu überprüfen, ob die Anmeldeinformationen gefährdet sind. Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den betroffenen Anwender zu kontaktieren.

ii. In Aktion 11 müssen Sie anhand der E-Mail-Antwort überprüfen, ob die Anmeldeinformationen gefährdet sind. Wenn die Anmeldeinformationen nicht gefährdet wurden, wird der Flow beendet.

1. Wenn in Aktion 12 die Anmeldeinformationen gefährdet sind, müssen Sie in Aktion 13 überprüfen, ob weitere Anwender betroffen sind. Wenn keine zusätzlichen Benutzer betroffen sind, wird der Flow beendet.
2. Wenn in Aktion 14 weitere Benutzer betroffen sind, führen Sie die folgenden Aktionen aus:
   a. In Aktion 15 müssen Sie mit Microsoft Exchange Online E-Mails suchen und löschen.
   b. In Aktion 16 müssen Sie den Absender und die schädlichen Dateien oder Anhänge in Office 365 und Proofpoint blockieren.

4. Wenn es sich in Aktion 17 nicht um eine intern gefälschte E-Mail handelt, müssen Sie überprüfen, ob das System des betroffenen Anwenders betroffen ist.
5. Wenn in Aktion 18 das System des Benutzers betroffen ist, lösen Sie in Aktion 19 ein IT-Ticket aus, um ein erneutes Abbild des betroffenen Systems zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. In Aktion 20 wird eine Antwortaufgabe erstellt, damit Sie die Überprüfung nach dem Incident abschließen, bevor die Aufgabe geschlossen wird.

Playbook für Endpunkterkennung

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Malware-Warnungen, die auf einem Host oder Endpunkt ausgelöst werden (z. B. die Erkennung einer schädlichen Datei).

Wenn CrowdStrike-Warnungen auf einem Host oder Endpunkt ausgelöst werden, können Sie das Endpunkterkennungs-Playbook im Flow Designer als Leitfaden verwenden und die Untersuchung dieser schädlichen Dateien optimieren.

Richten Sie das Endpunkterkennungs-Playbook ein

Führen Sie die folgenden Schritte aus, um das Endpunkterkennungs-Playbook einzurichten.

Vorbereitungen
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

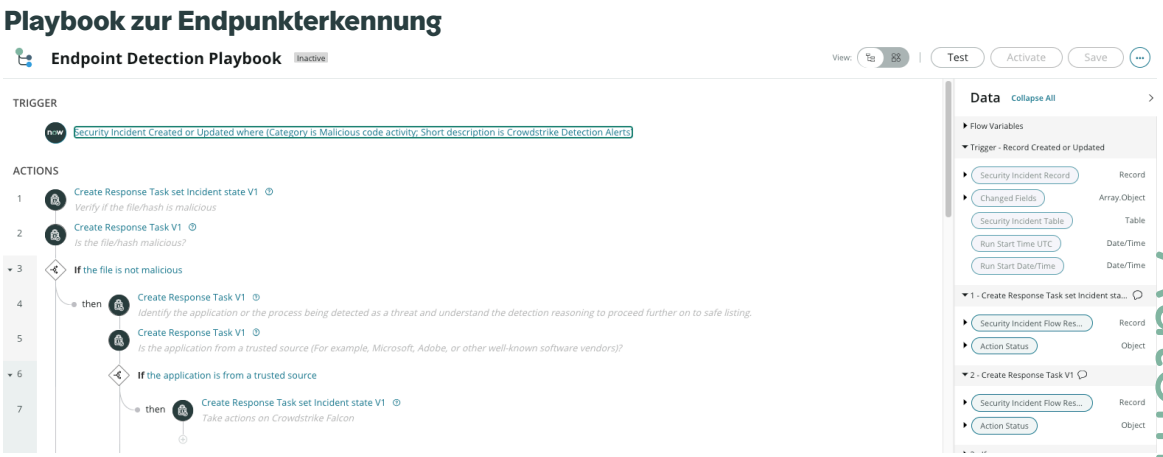
1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Endpunkterkennungs** -Playbook aus.

Automatische Übersetzung

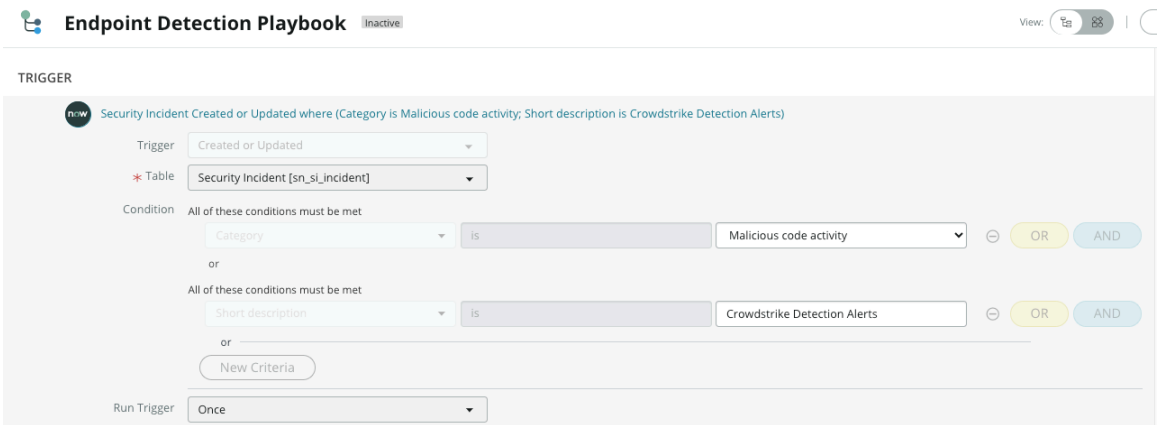
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows zur Endpunkterkennung erstellen und die erforderlichen Änderungen vornehmen.

   Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:
   - **Kategorie** ist **Böswillige Code-Aktivität**.
   - **Kurzbeschreibung** ist **CrowdStrike-Erkennungswarnungen**.



Verwenden Sie das Playbook zur Endpunkterkennung

Verwenden Sie dieses Playbook, um Malware-Warnungen zu untersuchen, die auf einem Host oder Endpunkt ausgelöst werden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Endpoint Detection-Playbook verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

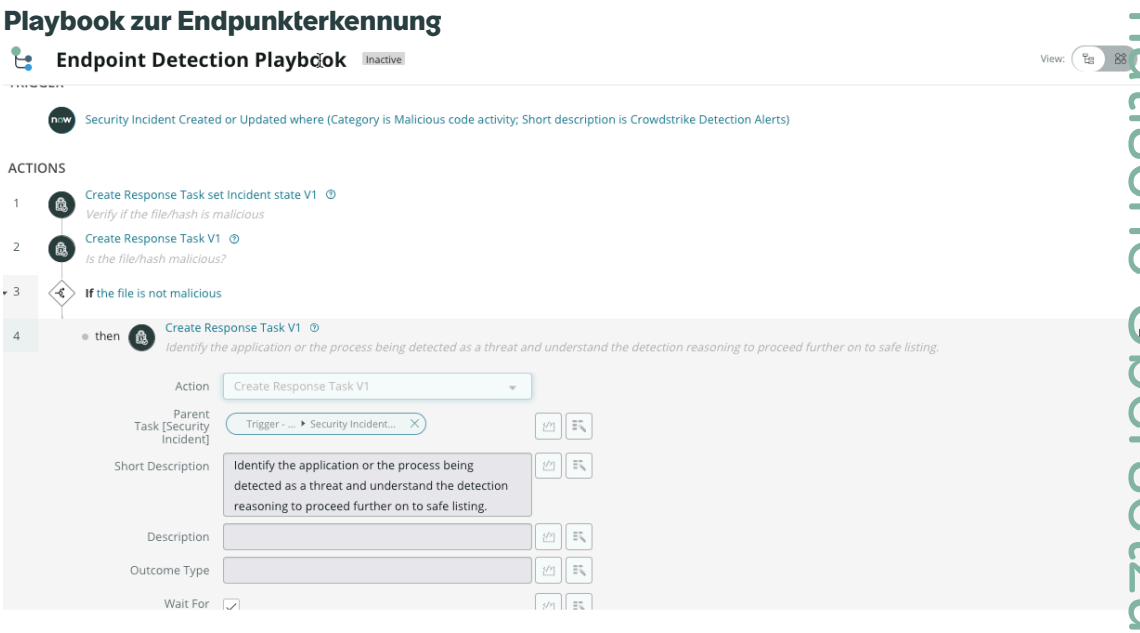
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob die Datei oder der Hash schädlich ist, indem Sie die Ergebnisse der Bedrohungssuche in SIR analysieren und Informationen von VirusTotal, WildFire, ThreatCrowd usw. sammeln.
2. In Aktion 2 müssen Sie überprüfen, ob die Datei oder der Hash schädlich ist oder nicht.
3. Führen Sie in Aktion 3 die folgenden Aktionen aus, wenn die Datei oder der Hash schädlich ist:

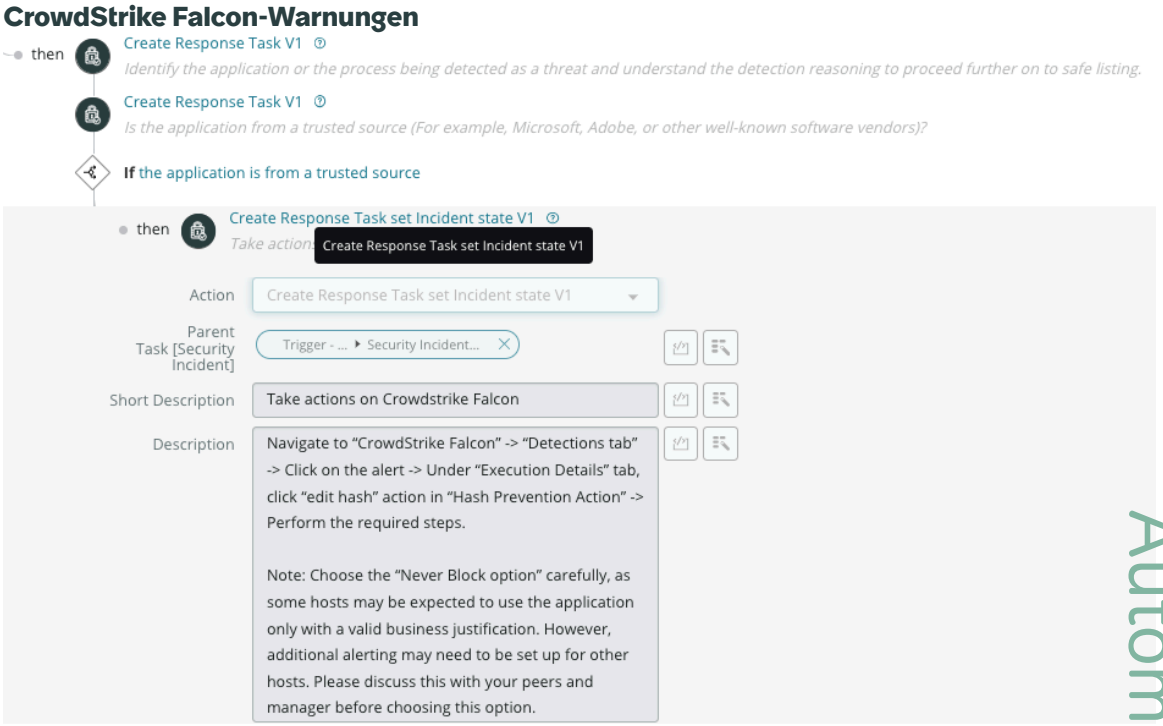
   a. In Aktion 4 müssen Sie die Anwendung oder den erkannten Prozess als Bedrohung identifizieren und Informationen über die Erkennungsgründe sammeln, um mit der sicheren Liste fortzufahren.



   b. In Aktion 5 müssen Sie überprüfen, ob die Anwendung aus einer vertrauenswürdigen Quelle stammt (z. B. Microsoft, Adobe oder andere bekannte Softwareanbieter).

   c. Wenn die Anwendung in Aktion 6 aus einer vertrauenswürdigen Quelle stammt, müssen Sie Maßnahmen für die CrowdStrike Falcon-Warnungen ergreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Führen Sie in Aktion 7 die folgenden Aktionen aus:

i. Navigieren zu **CrowdStrike Falcon** > **Erkennungen** Registerkarte

ii. Klicken Sie auf die CrowdStrike Falcon-Warnung.

iii. Klicken Sie auf der Registerkarte Ausführungsdetails unter **Hash-Verhinderungsaktion auf Hash-Aktion bearbeiten**.

iv. Führen Sie die erforderlichen Schritte aus.

> **Hinweis:**
> Wählen Sie die Option **Nie blockieren** mit Bedacht aus, da möglicherweise nur bestimmte Hosts die Anwendung mit einer gültigen geschäftlichen Begründung verwenden dürfen. Möglicherweise müssen jedoch zusätzliche Warnungen für andere Hosts eingerichtet werden.

e. Wenn die Anwendung in Aktion 8 nicht aus einer vertrauenswürdigen Quelle stammt, müssen Sie auswählen, ob Sie die Datei oder die Anwendung lokal auf dem Gerät speichern möchten.
Wenn Sie in Aktion 10 die Datei oder Anwendung lokal auf dem Gerät speichern möchten, führen Sie die folgenden Aktionen aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Navigieren Sie in Aktion 11 zur Registerkarte **Dateien in Quarantäne**, und filtern Sie den Endpunkt, indem Sie nach dem Gerätenamen suchen.

ii. Wählen Sie die Datei aus, die lokal deaktiviert werden soll, und klicken Sie auf **Freigeben**.

Hinweis:

- Die Datei wird weiterhin an diesem spezifischen Endpunkt ausgeführt. Auf allen anderen Hosts erfolgen Erkennung und Quarantäne jedoch weiterhin.
- Um die Massenfreigabe der Quarantänedatei auf mehreren Hosts durchzuführen, wählen Sie den entsprechenden Dateinamen und Status aus. Klicken Sie auf **Auswählen**und wählen Sie **Release**aus.

Wenn Sie in Aktion 12 die Datei oder Anwendung nicht lokal auf dem Gerät speichern möchten, können Sie den Benutzer an den IT-Support umleiten, um die Installation der genehmigten Anwendungen anzufordern.

4. Führen Sie in Aktion 14 die folgenden Aktionen aus, wenn die Datei oder der Hash nicht schädlich ist:

a. In Aktion 15 müssen Sie basierend auf der Rolle des Anwenders (Abteilung oder Position, die mit vertraulichen Informationen umgeht), dem Typ der Anwendung (Ransomware, Rootkit usw.) und der Auswirkung bestimmen, ob die Datei/der Hash ein hohes Risiko oder ein geringes Risiko aufweist der Anwendung (wie viele Anwender waren betroffen).

b. Wenn es sich bei der Datei um eine Datei mit hohem Risiko handelt, führen Sie in Aktion 16 die folgenden Aktionen aus:

i. Überprüfen Sie in Aktion 17 die Ergebnisse mit dem Threat Intel-Team.

ii. Führen Sie in Aktion 18 den Malware-Byte-Scan für die Datei aus.

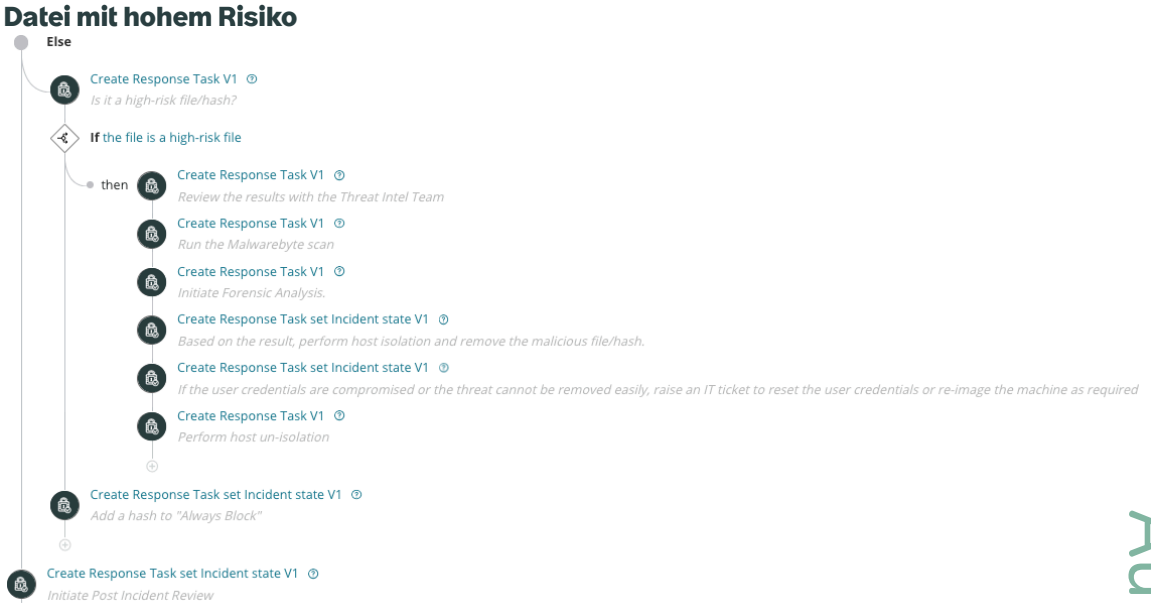
iii. Initiieren Sie in Aktion 19 die forensische Analyse.

iv. In Aktion 20 führen Sie basierend auf dem Ergebnis der forensischen Analyse eine Hostisolierung durch und entfernen die schädliche Datei/den schädlichen Hash.

v. Wenn in Aktion 21 die Anwenderanmeldeinformationen gefährdet sind oder die Bedrohung nicht einfach entfernt werden kann, lösen Sie ein IT-Ticket aus, um die Anwenderanmeldeinformationen zurückzusetzen, oder erstellen Sie ein neues Image des Computers.

vi. Führen Sie in Aktion 22 die Isolierung des Hosts durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Wenn es sich bei der Datei in Aktion 23 nicht um eine Datei mit hohem Risiko handelt, führen Sie die folgenden Aktionen aus:

i. Navigieren zu **CrowdStrike Falcon** > **Konfigurationen** Registerkarte

ii. Navigieren Sie auf der Registerkarte Konfigurationen zu **Verhinderungs-Hashes** > > **Upload-Hash** > **Fügen Sie den Hash hinzu**.

iii. Wählen Sie das erforderliche Betriebssystem und dann **Immer blockieren**aus.

5. In Aktion 24 wird eine Antwortaufgabe erstellt, damit der Benutzer die Überprüfung nach dem Incident abschließen kann, bevor die Aufgabe geschlossen wird.

Playbook für mögliches Passwort-Spray

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Passwort-Spray-Warnungen, die durch mehrere fehlgeschlagene Anmeldungen ausgelöst werden (zu viele Authentifizierungsfehler von mehr als einer IP-Adresse für denselben Anwender).

Richten Sie das Playbook „Mögliches Passwort-Spray“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Mögliches Passwort-Spray“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

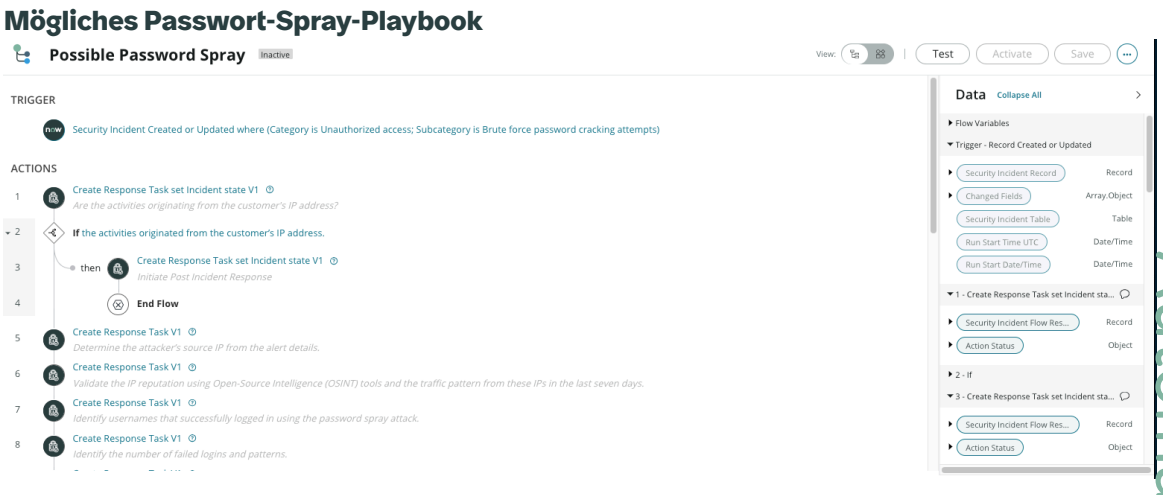
1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.

2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Mögliches Passwort-Spray“**.

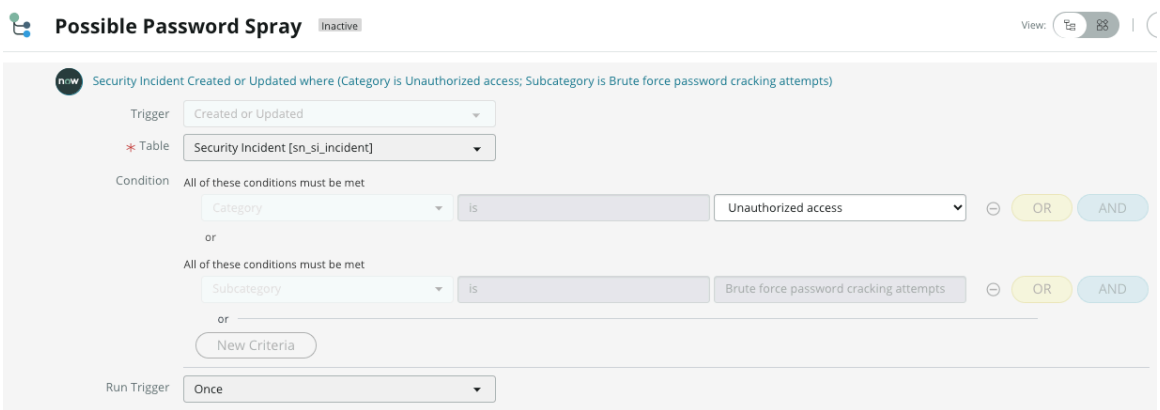
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows „Mögliches Passwort-Spray“ erstellen und die erforderlichen Änderungen vornehmen.

   Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:
   - **Kategorie** ist **„Nicht autorisierter Zugriff“**.
   - **Unterkategorie** ist **Brute-Force-Angriffe auf Passwörter**.



Verwenden Sie das Playbook „Mögliches Passwort-Spray“.

Verwenden Sie dieses Playbook, um Passwort-Spray-Warnungen zu untersuchen, die durch mehrere fehlgeschlagene Anmeldungen ausgelöst wurden (zu viele Authentifizierungsfehler von mehr als einer IP-Adresse für denselben Anwender). Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Mögliches Passwort-Spray“ verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

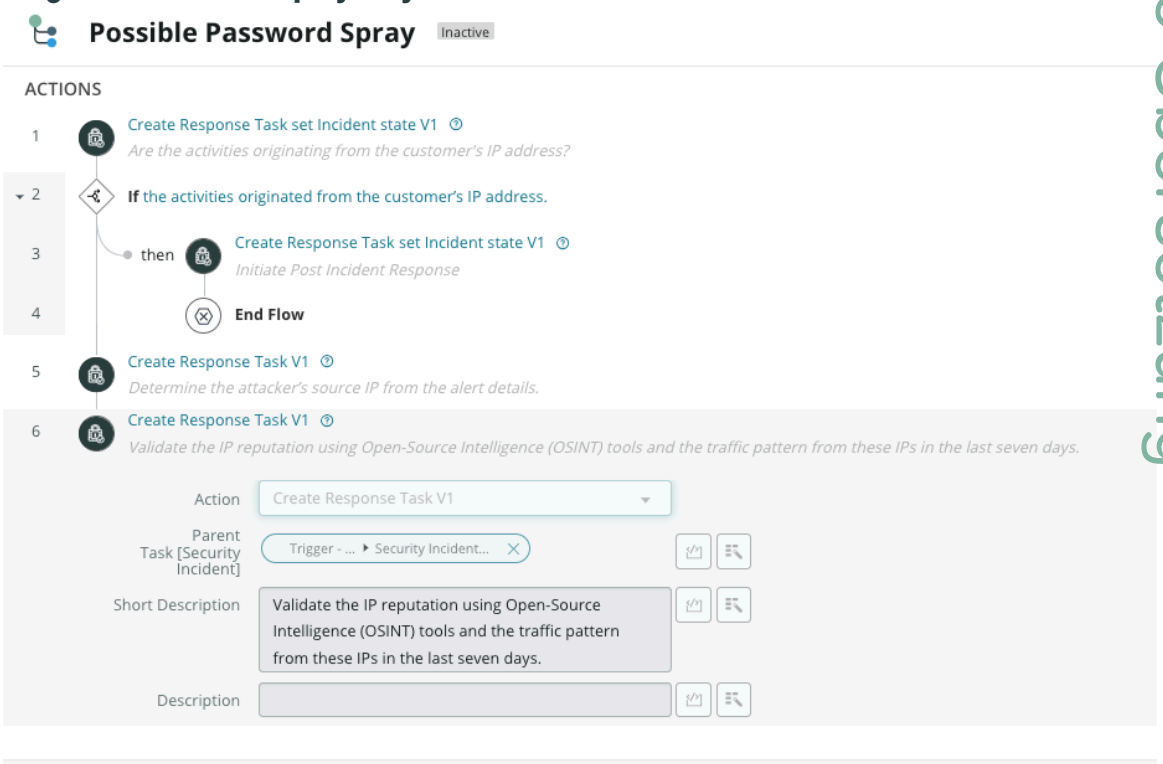
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob die Aktivitäten von der IP-Adresse des Kunden stammen.
   Identifizieren Sie die IP-Adressen, die den Passwort-Spray-Angriff ausführen. Verwenden Sie beispielsweise die TXIDs (Transaktions-IDs) aus der Warnung, und suchen Sie sie in den F5-Protokollen.
2. Wenn in Aktion 2 die Aktivitäten von der IP-Adresse des Kunden stammen, führen Sie die folgenden Aktionen aus:
   a. In Aktion 3 müssen Sie eine Überprüfung des möglichen Passwort-Spray-Angriffs nach einem Incident initiieren.
   b. In Aktion 4 endet der Flow.
3. Wenn die Aktivitäten in Aktion 5 nicht von der IP-Adresse des Kunden stammen, bestimmen Sie die Quell-IP des Angreifers anhand der Warnungsdetails.
4. In Aktion 6 müssen Sie die IP-Reputation mit Open-Source Intelligence-Tools (OSINT) und das Datenverkehrsmuster von diesen IPs in den letzten sieben Tagen validieren.

Mögliches Passwort-Spray-Playbook



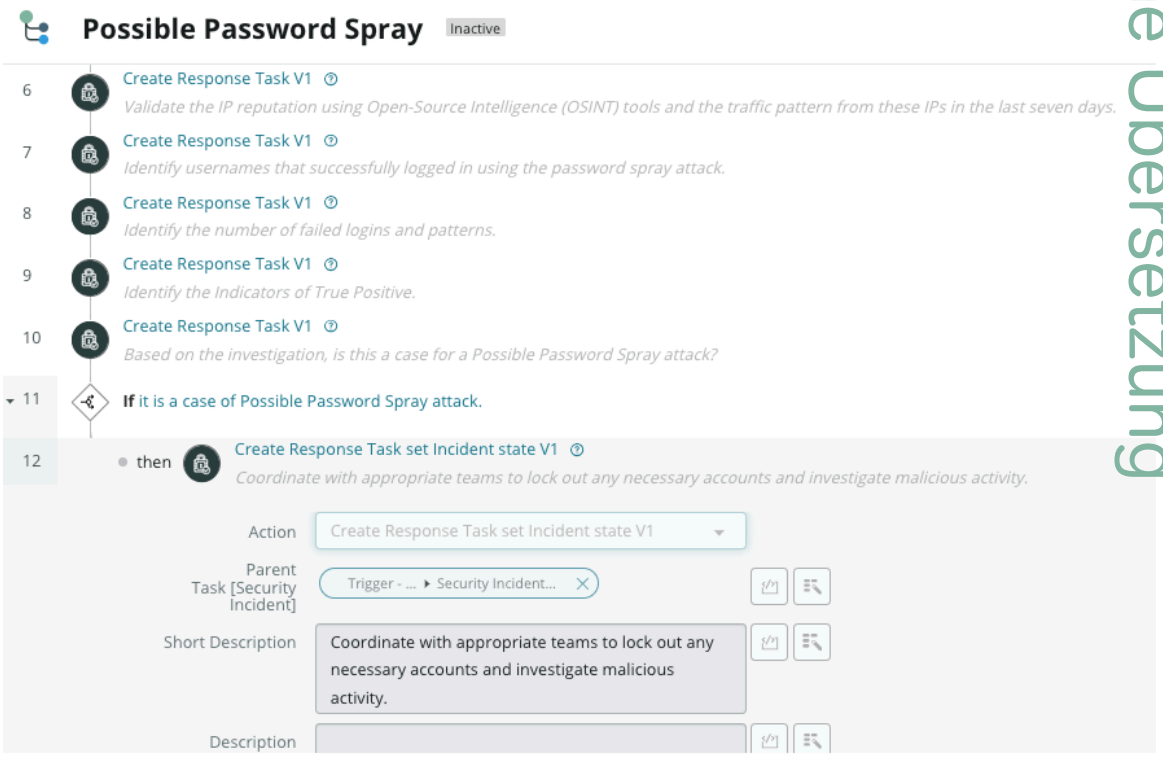
5. In Aktion 7 müssen Sie die Anwendernamen identifizieren, die sich erfolgreich mit dem Passwort-Spray-Angriff angemeldet haben.
6. In Aktion 8 müssen Sie die Anzahl der fehlgeschlagenen Anmeldungen und Muster identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. In Aktion 9 müssen Sie die Indikatoren für wirklich positive Ergebnisse identifizieren.
   - Überprüfen Sie den Datenverkehr von den Quell-IPs in den letzten 60 Tagen. Kein Verlaufsdatenverkehr kann ein Hinweis auf ein wirklich positives Ergebnis sein.
   - Überprüfen Sie die Anwendernamensmuster mit Authentifizierungsfehlern und die Anzahl. Je höher die Anzahl, desto höher die Wahrscheinlichkeit, dass es sich um ein richtig positives Ergebnis handelt.
   - Der Anwendername sieht aus wie ein Wörterbuch (von A bis Z) und enthält möglicherweise allgemeine Administratornamen wie „admin“, „sysadmin“, „root“ usw
   - Derselbe Anwendername kann imSpray-Angriff unterschiedliche Muster aufweisen, z. B. kann dieselbe Warnung Fehler für john.doe, johnd, jdoe, john_doe, jdoe7 usw. aufweisen, was darauf hinweist, dass Angreifer das Anwendernamensmuster basierend auf gängigen Anwendungsfällen erraten.
   - Beachten Sie den Anwenderagent und die URIs aus den F5-Protokollen im obigen Schritt, und prüfen Sie, ob die IoCs mit den Red Kondor-Warnungen zusammenhängen. Wenn sie übereinstimmen, handelt es sich um ein richtig positives Ereignis.
8. In Aktion 10 müssen Sie basierend auf den bisher durchgeführten Untersuchungen überprüfen, ob es sich um einen möglichen Passwort-Spray-Angriff handelt oder nicht.
9. Führen Sie in Aktion 11 im Fall eines möglichen Passwort-Spray-Angriffs die folgenden Aktionen aus:

   a. In Aktion 12 müssen Sie sich mit den entsprechenden Teams abstimmen, um alle erforderlichen Konten zu sperren und böswillige Aktivitäten zu untersuchen.

Mögliches Passwort-Spray-Playbook



   b. In Aktion 13 müssen Sie eine Überprüfung des möglichen Passwort-Spray-Angriffs nach einem Incident initiieren.

   c. In Aktion 14 endet der Flow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. In Aktion 15 müssen Sie überprüfen, ob dies kein Fall eines möglichen Passwort-Spray-Angriffs ist.
11. Wenn es sich in Aktion 16 nicht um einen möglichen Passwort-Spray-Angriff handelt, führen Sie die folgenden Aktionen aus:
    a. In Aktion 17 müssen Sie die bisherigen Ergebnisse dokumentieren.
    b. In Aktion 18 müssen Sie eine Überprüfung des möglichen Passwort-Spray-Angriffs nach einem Incident initiieren.
    c. In Aktion 19 endet der Flow.
12. In Aktion 20 müssen Sie die Kollegen und den GIR-Manager um Rat fragen.
13. In Aktion 21 wird eine Antwortaufgabe erstellt, um die Überprüfung nach dem Incident abzuschließen, bevor die Aufgabe geschlossen wird.

Playbook für T1003 – Tools zum Erkennen von Anmeldeinformations-Dumping

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung eines Incidents im Zusammenhang mit Dumping-Aktivitäten für Anmeldeinformationen.

Richten Sie das Playbook „T1003 – Tools für Anmeldeinformations-Dumping erkennen“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „T1003 – Tools zum Dumping von Anmeldeinformationen erkennen“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

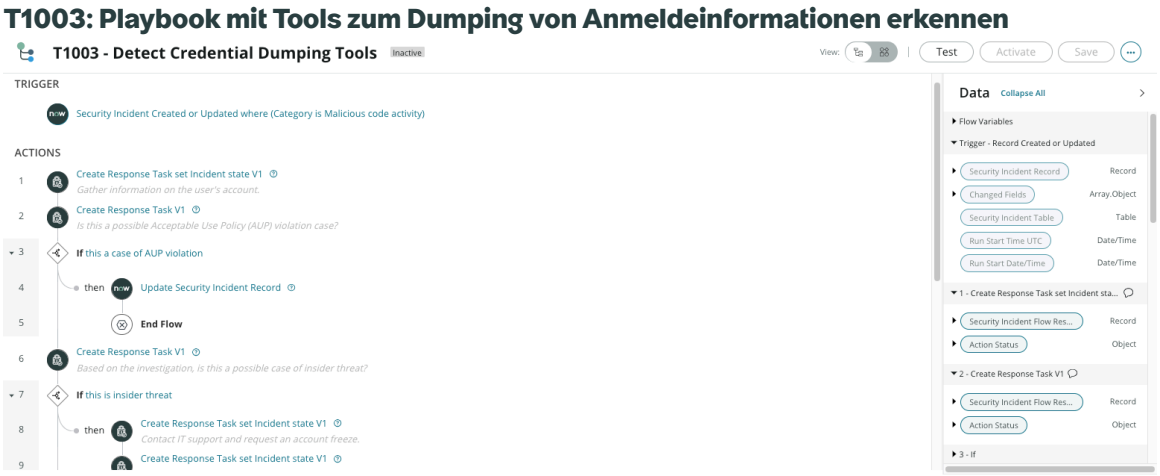
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **T1003 – Tools zum Dumping von Anmeldeinformationen erkennen aus**.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows „T1003 – Detect Credential Dumping Tools“ (T1003 – Erkennungs-Dumping-Tools für Anmeldeinformationen) erstellen und die erforderlichen Änderungen vornehmen.

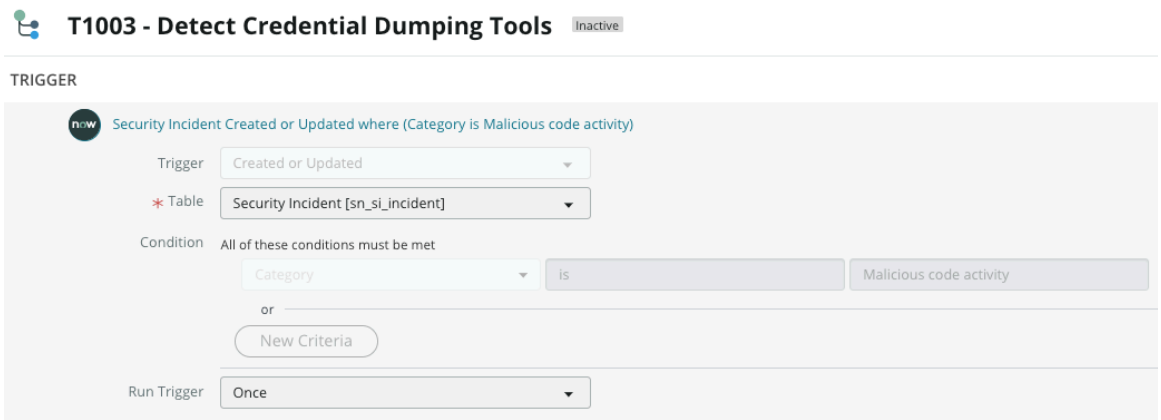
   Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieBöswillige Code-Aktivität**lautet.



Verwenden Sie das Playbook „T1003 – Tools zum Erkennen von Dumping-Anmeldeinformationen“.

Verwenden Sie dieses Playbook, um einen Incident zu untersuchen, der Aktivitäten zum Dumping von Anmeldeinformationen beinhaltet. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Tools für Anmeldeinformations-Dumping erkennen verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

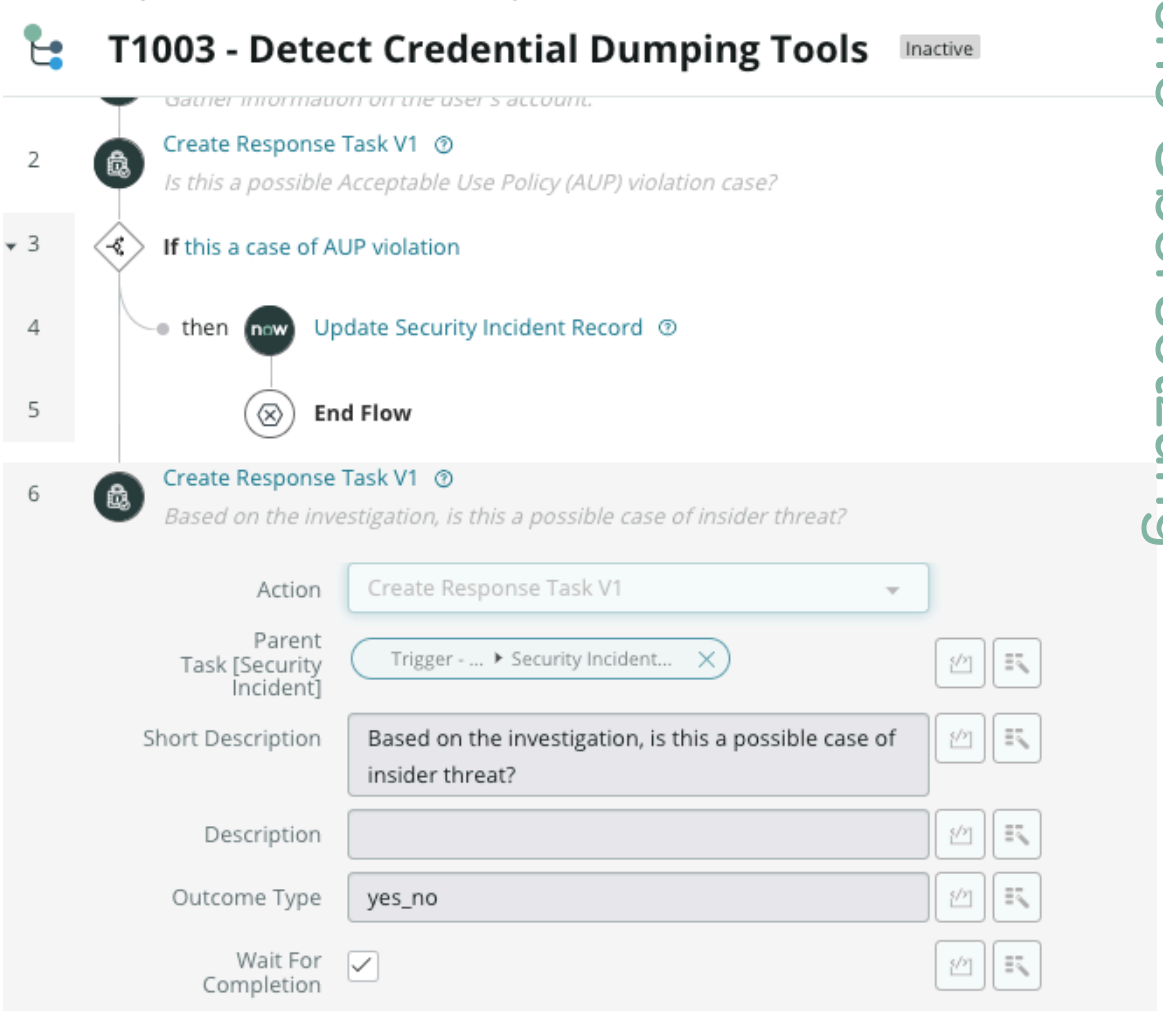
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, müssen Sie in Aktion 1 Informationen zum Account des Anwenders sammeln.
   - Sie müssen die Hostaktivität überprüfen, um nach verdächtigen Aktivitäten zu suchen.
   - Sie müssen den Besitzer des Servers/Endpunkts/der VM identifizieren und die Daten erfassen, die sich auf das Tool beziehen.
   - Sie müssen Informationen zu den anderen Accounts des Benutzers sammeln.
2. In Aktion 2 müssen Sie überprüfen, ob dies ein möglicher Verstoßfall für die Richtlinie zur zulässigen Nutzung (Acceptable Use Policy, AUP) ist.
   Sie können eine Peer-Überprüfung der gesammelten Nachweise durchführen und sich mit Ihrem regionalen Incident Manager beraten, ob Sie den Benutzer kontaktieren sollen.
3. Wenn es sich in Aktion 3 um einen Verstoß gegen die Richtlinie zur zulässigen Nutzung handelt, führen Sie die folgenden Aktionen aus:
   a. In Aktion 4 müssen Sie den Security Incident dahingehend aktualisieren, dass es sich um einen Fall einer AUP-Verletzung handelt
   b. In Aktion 5 endet der Flow.
4. In Aktion 6 müssen Sie basierend auf den bisher durchgeführten Untersuchungen überprüfen, ob dies ein möglicher Fall einer internen Bedrohung ist oder nicht.

T1003: Playbook mit Tools zum Dumping von Anmeldeinformationen erkennen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Führen Sie in Aktion 7 die folgenden Aktionen aus, wenn es sich um eine interne Bedrohung handelt:

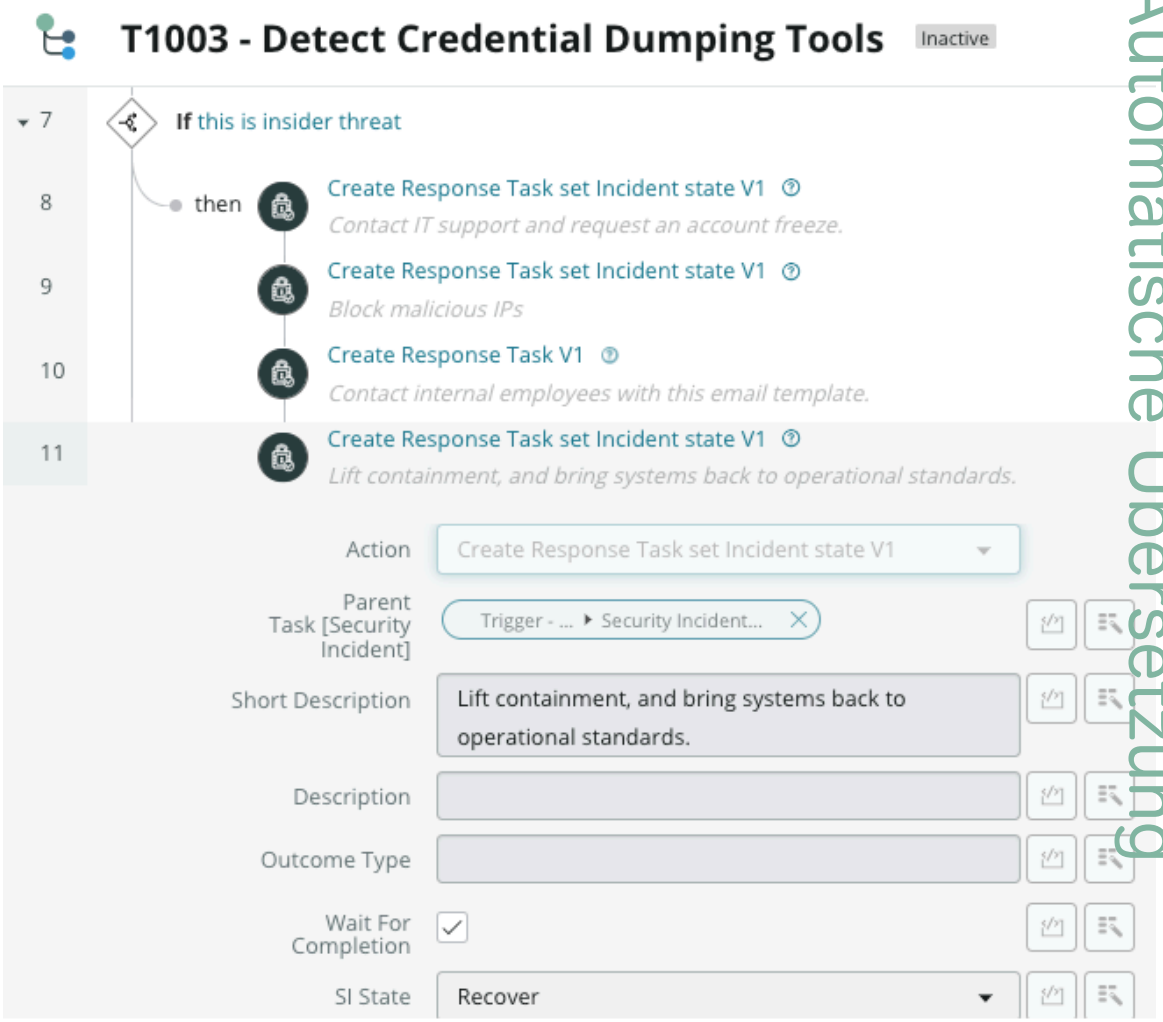
   a. In Aktion 8 müssen Sie sich an den IT-Support wenden und eine Kontosperre anfordern.

   b. In Aktion 9 müssen Sie schädliche IPs blockieren.

   c. In Aktion 10 müssen Sie interne Mitarbeiter per E-Mail kontaktieren.
   Sie können die bereitgestellte E-Mail-Vorlage verwenden, um Ihre internen Mitarbeiter zu kontaktieren.

   d. In Aktion 11 müssen Sie die Eindämmung aufheben und die Systeme wieder auf Betriebsstandard zurücksetzen.
   Der Flow endet.

Antwortaufgaben zum Aufheben des Containments



6. Wenn es sich in Aktion 12 nicht um einen Fall einer internen Bedrohung handelt, müssen Sie in Aktion 13 eine Peer-Überprüfung durchführen, um festzustellen, ob dies der Ausschlussliste hinzugefügt werden muss.
   Der Flow endet.

7. In Aktion 14 wird eine Antwortaufgabe erstellt, um die Überprüfung nach dem Incident abzuschließen, bevor die Aufgabe geschlossen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für Spoofing-Erkennung von E-Mail-Domänen

Dieses Playbook hilft bei der Frühphasen-Selektierung von vom Anwender gemeldeten Phishing-Übermittlungen, indem es den Analysten auf die Möglichkeit einer Look-alike-Domäne in der E-Mail-Adresse des Phishing-Anwenders hinweist.

Das Playbook zur Erkennung von E-Mail-Domänen-Spoofing sucht nach einer Ähnlichkeitsübereinstimmung zwischen der Absender-E-Mail-Domäne des Phishers und einem vertrauenswürdigen Domänennamen, der im Repository für erkennbare Elemente vorhanden ist. Wenn das Playbook eine Übereinstimmung einer gefälschten Absender-E-Mail-Domäne identifiziert hat, werden die Analysten mit einem Tag benachrichtigt.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisorientierte Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

Richten Sie das Playbook „E-Mail-Spoof-Erkennung“ ein

Führen Sie die folgenden Schritte aus, um das Playbook zur Erkennung von E-Mail-Spoof einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

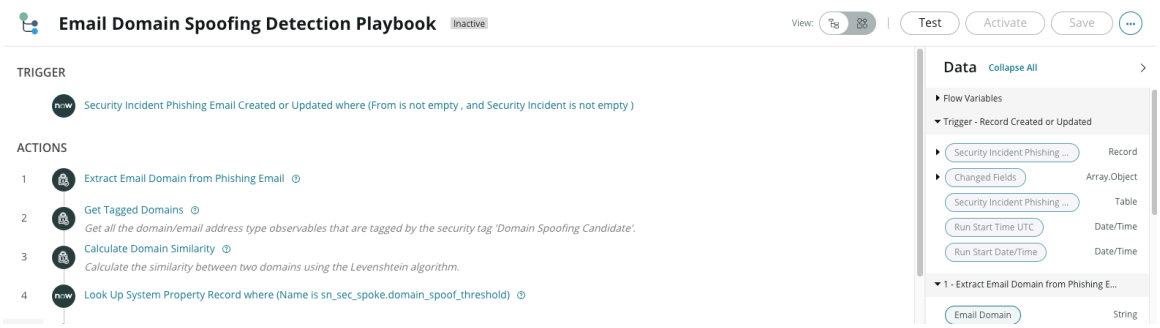
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook Playbook zur Spoofing-Erkennung von E-Mail-Domänen** aus.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows zur Erkennung von E-Mail-Domänen-Spoofing erstellen und die erforderlichen Änderungen vornehmen.

   Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

Playbook zur Erkennung von E-Mail-Domänen-Spoofing

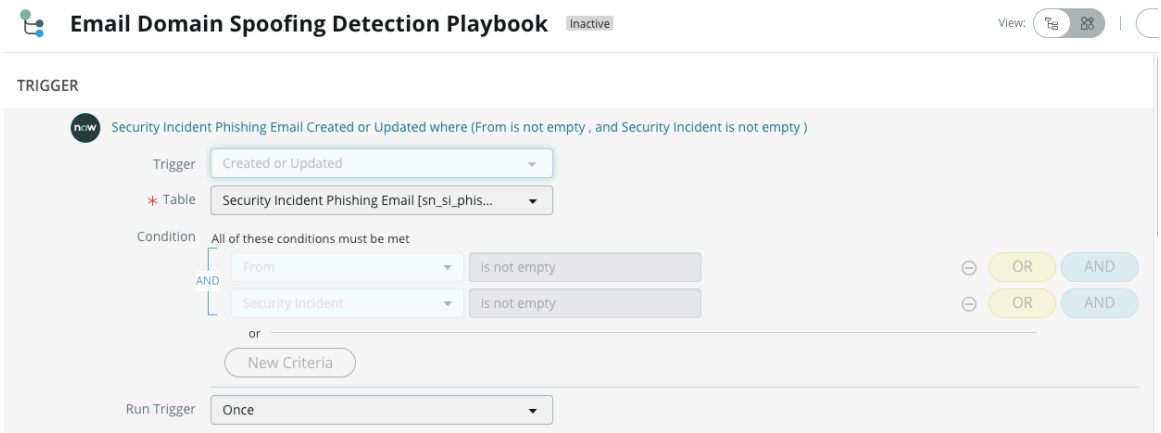


4. Aktivieren Sie die Playbooks.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
- Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:
   - **„Von“** ist nicht **leer**.
   - **Security Incident** ist nicht **leer**.



Verwenden Sie das Playbook zur Erkennung von E-Mail-Domänen-Spoofing

Verwenden Sie dieses Playbook, um eine Ähnlichkeitsübereinstimmung zwischen der Absender-E-Mail-Domäne des Phishers und einem vertrauenswürdigen Domänennamen zu finden, der im Repository für erkennbare Elemente vorhanden ist. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook zur Erkennung von E-Mail-Domänen-Spoofing verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

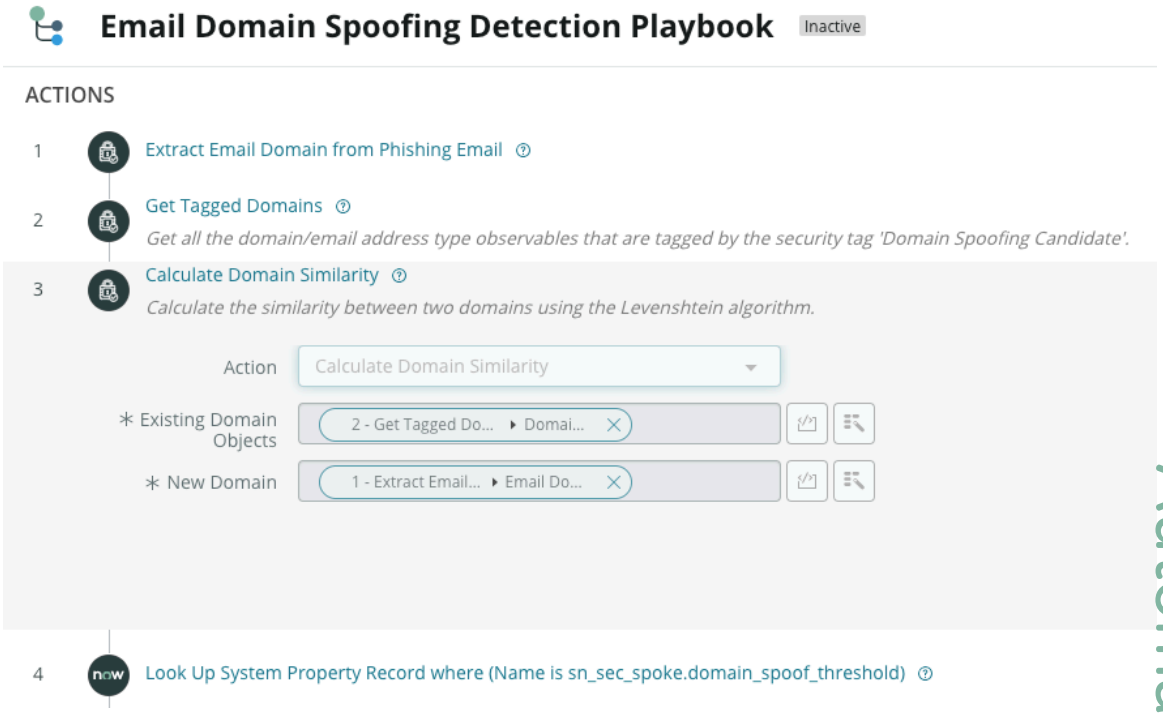
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Wenn das Playbook ausgelöst wird und in Aktion 1 mit der Ausführung beginnt, extrahiert das Playbook die E-Mail-Domäne aus der Phishing-E-Mail.
2. In Aktion 2 ruft das Playbook alle erkennbaren Elemente vom Typ Domäne/E-Mail-Adresse ab, die mit dem Sicherheits-Tag „Domänen-Spoofing-Kandidat“ gekennzeichnet sind.
3. In Aktion 3 berechnet das Playbook die Ähnlichkeit zwischen der getaggten Domäne und der E-Mail-Domäne mithilfe des Levenshtein-Algorithmus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

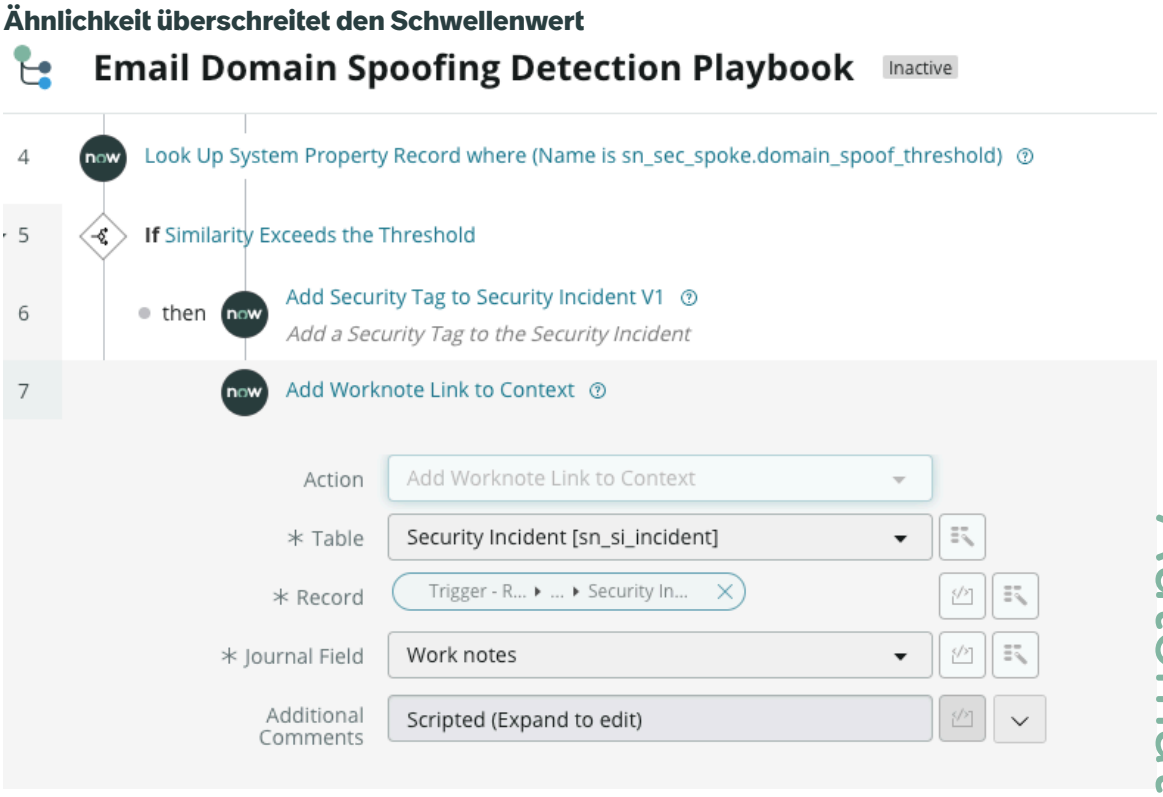
Playbook zur Erkennung von E-Mail-Domänen-Spoofing



4. In Aktion 4 sucht das Playbook basierend auf den folgenden Bedingungen nach dem Systemeigenschaften-Datensatz:
   - Name ist sn_sec_spoke.domain_spoof_threshold, (ODER)
   - Der Name geht von a bis z. Wenn mehrere Datensätze gefunden werden, wird nur der erste zurückgegeben.
5. In Aktion 5 prüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob die Ähnlichkeit der beiden Domänen den Schwellenwert überschreitet oder nicht.
   Wenn die Ähnlichkeit der beiden Domänen den Schwellenwert nicht überschreitet, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet. Wenn die Ähnlichkeit der beiden Domänen den Schwellenwert überschreitet, werden die Aktionen 6 und 7 ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. In Aktion 6 fügt das Playbook dem Security Incident das Sicherheits-Tag „E-Mail-Domänen-Spoofing“ hinzu.
7. In Aktion 7 fügt das Playbook dem Kontext mithilfe der Skriptoption einen Arbeitsnotizlink hinzu.
8. In Aktion 8 endet der Flow.

Playbook für Domäne mit besetzter Tippfehlerdomäne

Dieses Playbook bietet systematische Verfahren für die Untersuchung von falsch geschriebenen Domänen und die Zusammenarbeit mit der Rechtsabteilung des Unternehmens. Bei Domänen mit Tippfehlerbesetzung handelt es sich um absichtlich falsch geschriebene Domänennamen, die echten Domänennamen sehr ähnlich sind. Angreifer nutzen Rechtschreibfehler aus, um auf eine unbeabsichtigte Website zu gelangen, die finanzielle Ausbeutung oder andere böswillige Aktivitäten zur Folge hat.

Die Domänen mit besetztem Tippfehler werden dem Security Operations-Team aus verschiedenen Quellen wie Lösungen zum Schutz vor digitalen Risiken (Digital Schatten) und Threat Intelligence-Plattformen (Anomali Threatstream) gemeldet. Nachdem ein Security Incident erstellt wurde, hilft diese Lösung bei der Identifizierung, ob die Domäne tatsächlich eine Typo-Squartated-Domäne ist. Wenn es sich um einen Tippfehler in der Domäne handelt, kann der Analyst ihn der Rechtsabteilung melden, damit weitere Maßnahmen ergriffen werden können.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisorientierte Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

Richten Sie das Playbook für besetzte Domänen für Tippfehler ein

Führen Sie die folgenden Schritte aus, um das Playbook für Domäne mit besetzter Typo-Gruppe einzurichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

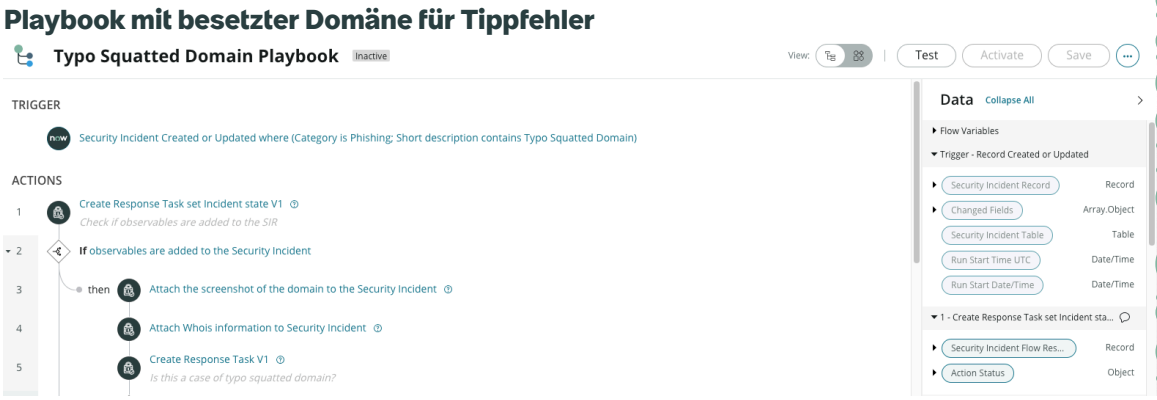
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Tippfehler – Besetzte Domäne“** aus.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows für Typo-Besatzungsdomänen erstellen und die erforderlichen Änderungen vornehmen.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, klicken Sie auf das Menüsymbol , und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.



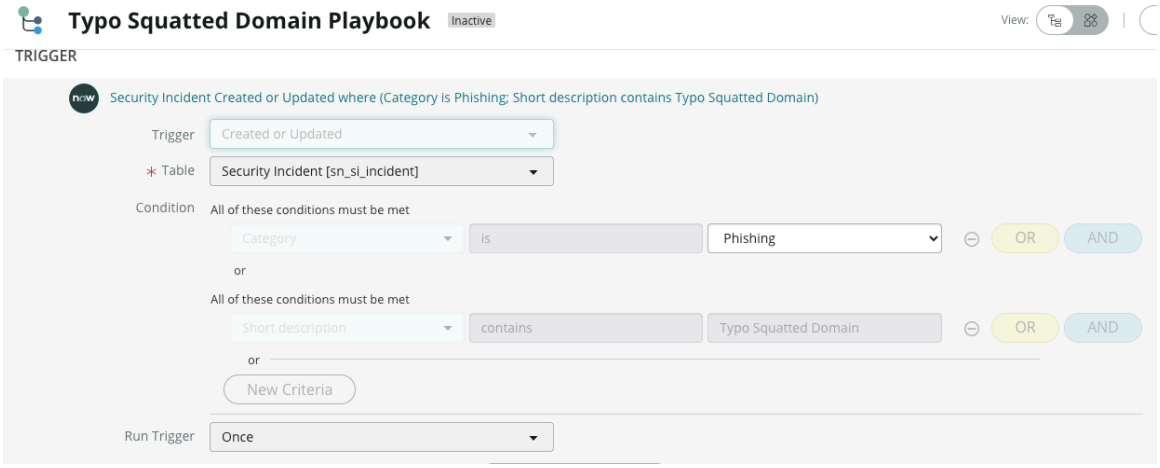
4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kategorie** ist **Phishing**.
- **Kurzbeschreibung** enthält **Tippfehler in Domäne**.



Verwenden Sie das Playbook für besetzte Domänen für Typo

Verwenden Sie dieses Playbook, um falsch geschriebene Domänen zu untersuchen und mit der Rechtsabteilung des Unternehmens zusammenzuarbeiten. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Typo Schatted Domain“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

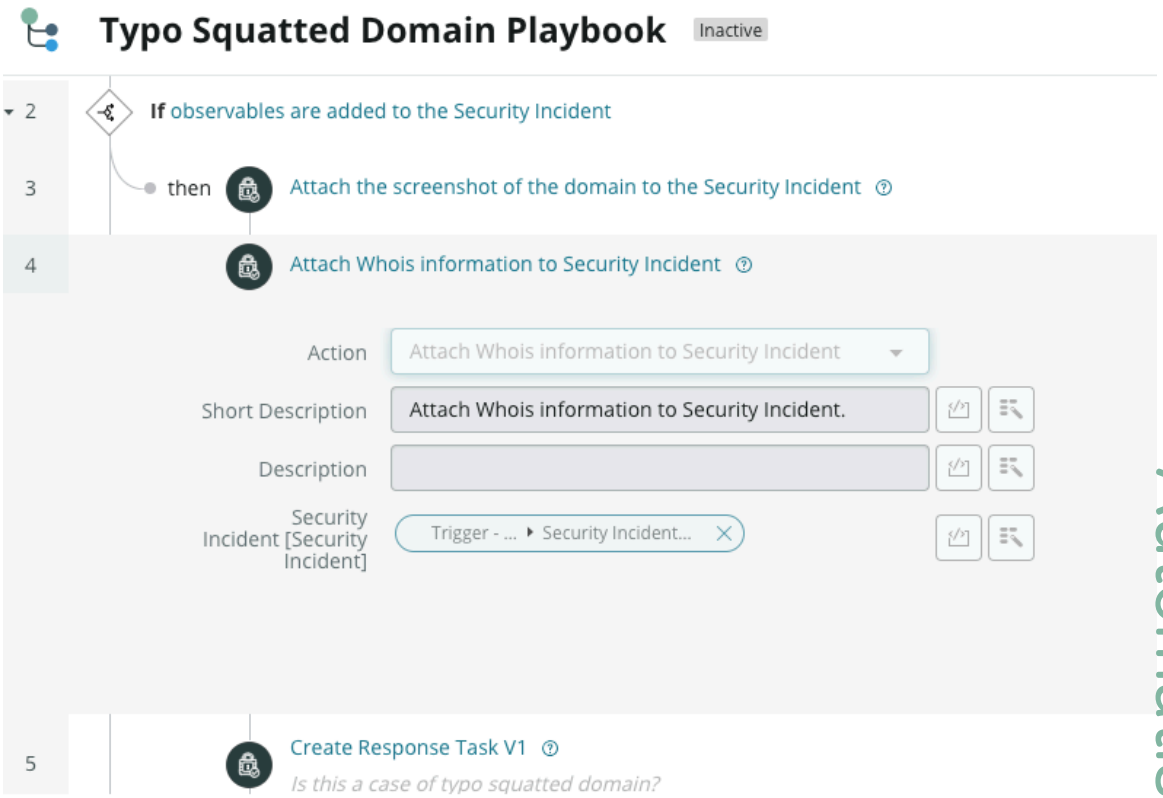
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob die erkennbaren Elemente zu Security Incident Response (SIR) hinzugefügt wurden.
   Wenn die erkennbaren Elemente nicht zu SIR hinzugefügt werden, fügen Sie die erkennbaren Elemente hinzu, bevor Sie fortfahren. Wenn die erkennbaren Elemente nicht verfügbar sind, wird Aktion 10 ausgeführt, und der Security Incident wird geschlossen.
2. Wenn in Aktion 2 dem Security Incident die erkennbaren Elemente hinzugefügt werden, werden die folgenden Aktionen ausgeführt.
3. In Aktion 3 müssen Sie den Screenshot der Domäne „Tippfehler besetzt“ an den Security Incident anhängen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook mit besetzter Domäne für Tippfehler



4. In Aktion 4 müssen Sie dem Security Incident Whois-Informationen anhängen.
5. In Aktion 5 prüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob es sich um einen Fall von „Tippfehler in der Domäne“ handelt oder nicht.
   Wenn es sich nicht um einen Fall von „Tippfehler in Domäne“ handelt, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.
6. Wenn es sich in Aktion 6 um einen Fall von Typo-Besetzungsdomäne handelt, wird Aktion 7 ausgeführt.
7. In Aktion 7 müssen Sie der Rechtsabteilung und anderen erforderlichen Teams eine E-Mail senden und sie darüber informieren, dass es sich um einen Fall von Domäne mit Tippfehler handelt, und die erforderlichen Maßnahmen ergreifen, um den Fehler zu beseitigen.
   Wenn es sich nicht um einen Fall von „Tippfehler in Domäne“ handelt, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall von Tippfehler in Domäne

8. In Aktion 9 wird eine Antwortaufgabe erstellt, damit Sie die Überprüfung nach dem Incident abschließen können, bevor die Aufgabe geschlossen wird.

Playbook für das Sniffing von Anmeldeinformationen

Dieses Playbook bietet Systemkorrekturschritte zur Untersuchung eines Incidents im Zusammenhang mit Sniffing-Aktivitäten für Anmeldeinformationen, die über die Tabelle `sys_installation_exit` in einer ServiceNow-Instanz ausgeführt werden.

Das Playbook „Sniffing von Anmeldeinformationen“ bietet ein Skriptfeld zur Verarbeitung der Datenbankanmeldungen (DB), Single Sign-on (SSO) und LDAP (Lightweight Directory Access Protocol) unter Verwendung der Datensätze in der Tabelle `sys_installation_exit`. Diese privilegierten Skriptfelder ermöglichen das Abhören von Anwenderanforderungen und Parametern bei den Instanzen während der Anmeldung, einschließlich Anmeldeinformationen wie Anwendername und Passwort.

Ein böswilliger Benutzer kann ein Skript erstellen, um die Benutzeranforderungen abzuhören und diese Anforderungen in der Instanz zu protokollieren. Die Tabelle `sys_installation_exit` in einer Instanz definiert die Regeln für die Verarbeitung der An- und Abmeldeaktivitäten aller Benutzer in dieser Instanz.

Richten Sie das Playbook zum Sniffing von Anmeldeinformationen ein

Führen Sie die folgenden Schritte aus, um das Playbook zum Sniffing von Anmeldeinformationen einzurichten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

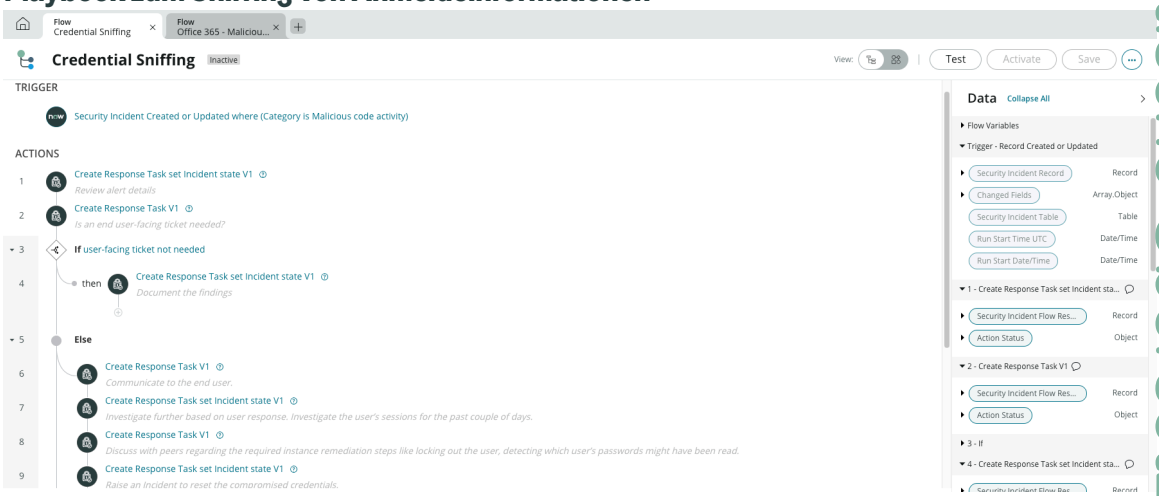
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Sniffing an Anmeldeinformationen“** aus.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows zum Sniffing von Anmeldeinformationen, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

   Playbook zum Sniffing von Anmeldeinformationen

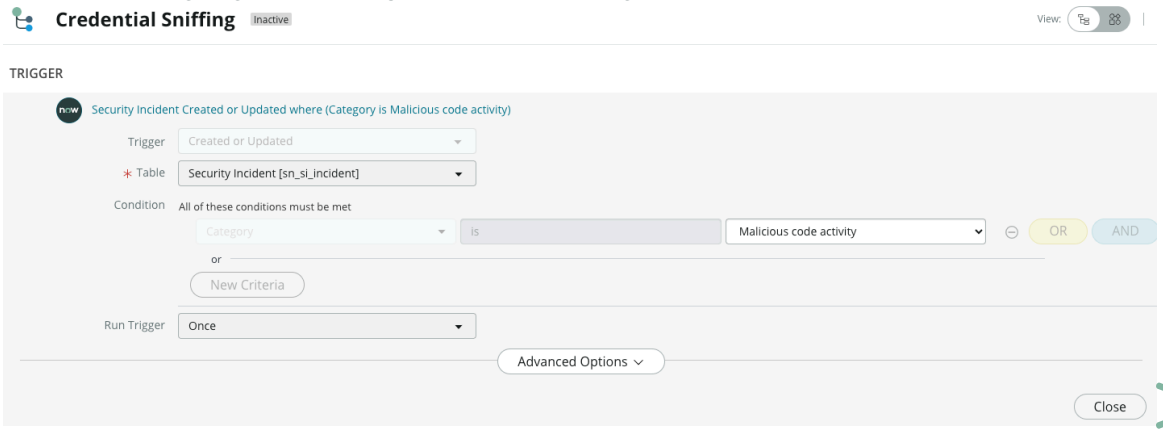
   

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieBöswillige Code-Aktivität**lautet.

Auslösebedingung für das Playbook zum Sniffing von Anmeldeinformationen



Verwenden Sie das Playbook zum Sniffing von Anmeldeinformationen

Verwenden Sie dieses Playbook, um einen Incident zu untersuchen, bei dem Sniffing-Aktivitäten für Anmeldeinformationen über die Tabelle `sys_installation_exit` in einer ServiceNow-Instanz ausgeführt werden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Sniffing von Anmeldeinformationen“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, überprüfen Sie in Aktion 1 die folgenden Warnungsdetails.
   - Instanz
   - Sitzungs-ID
   - Transaktions-ID
   - _raw: Stellt das gesamte Skript bereit.

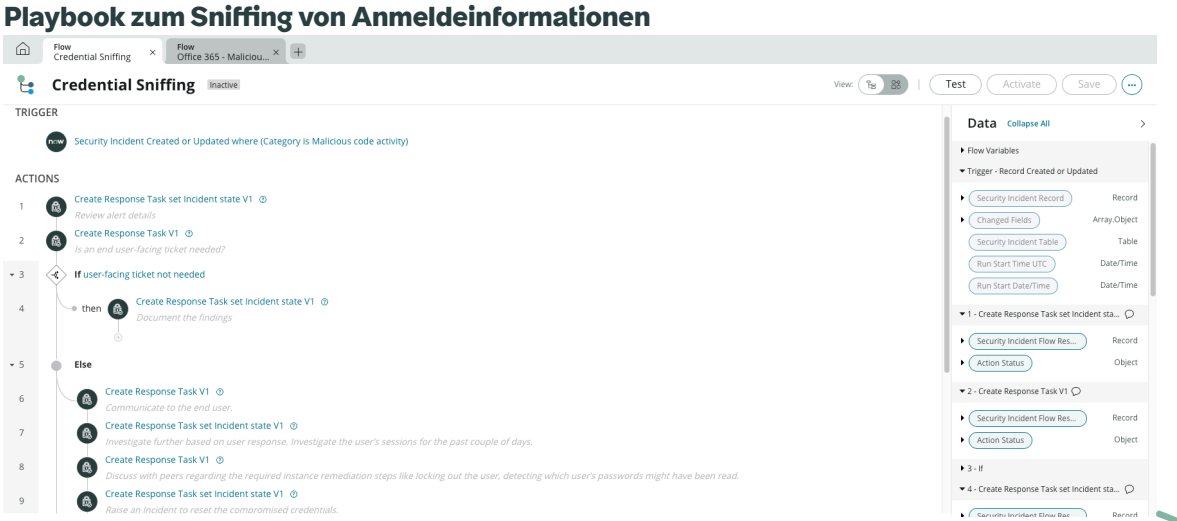
   Beispielskript:

   ```
   Var pass= request.getParameter(“user_password”);
   Gs.log(pass);
   ```

2. Überprüfen Sie in Aktion 2 basierend auf den bisher gesammelten Daten, ob für diese Warnung ein Endanwenderticket erforderlich ist.
3. Wenn in Aktion 3 für die Warnung kein Endbenutzerticket erforderlich ist, dokumentieren Sie in Aktion 4 die bisherigen Ergebnisse.
   Der Flow endet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wenn in Aktion 5 die Warnung ein Endbenutzerticket erfordert, führen Sie die folgenden Schritte aus:

   a. In Aktion 6 informieren Sie den Endanwender darüber, dass für die Warnung ein Endanwenderticket erforderlich ist.

   b. Untersuchen Sie in Aktion 7 basierend auf der Antwort des Anwenders und den Sitzungen des Anwenders in den letzten Tagen weiter.

   c. Diskutieren Sie in Aktion 8 mit Kollegen über die Korrekturschritte für die Instanz, z. B. das Sperren des Anwenders und das Erkennen, welche Anwenderpasswörter möglicherweise gelesen wurden.

   d. Lösen Sie in Aktion 9 einen Incident oder ein Ticket aus, um die gefährdeten Anwenderanmeldeinformationen zurückzusetzen.

   e. Heben Sie in Aktion 10 das Containment auf, und bringen Sie die Systeme wieder in den Betriebszustand Der Flow endet.

5. Schließen Sie in Aktion 11 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für T1070 – Windows-Ereignisprotokolle gelöscht

Dieses Playbook bietet Korrekturschritte zur Untersuchung von Incidents, die Ereignistypen nachverfolgen, bei denen der Anwender Sicherheitsprotokolle entfernt. Jedes Mal, wenn das Sicherheitsprotokoll gelöscht wird, werden die Ereignisse 517 und 1102 unabhängig vom Status der Richtlinie Audit-Systemereignis protokolliert.

Diese Warnung kann die folgenden Ereignistypen nachverfolgen:

- **Ereignis 517**: Die Felder Primärer Anwendername und Client-Anwendername geben den Anwender an, der das Protokoll gelöscht hat. Der primäre Anwendername entspricht dem System, und der Client-Anwendername gibt den Anwender an, der das Protokoll gelöscht hat.
- **Ereignis 1102**: Die Felder „Accountname“ und „Domänenname“ geben den Anwender an, der das Protokoll gelöscht hat. Die Anmelde-ID ermöglicht Ihnen eine Rückwärtskorrelation zum Anmeldeereignis und zu anderen Ereignissen, die während derselben Anmeldesitzung protokolliert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie das Playbook „T1070 – Windows-Ereignisprotokolle gelöscht“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „T1070 – Windows-Ereignisprotokolle gelöscht“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

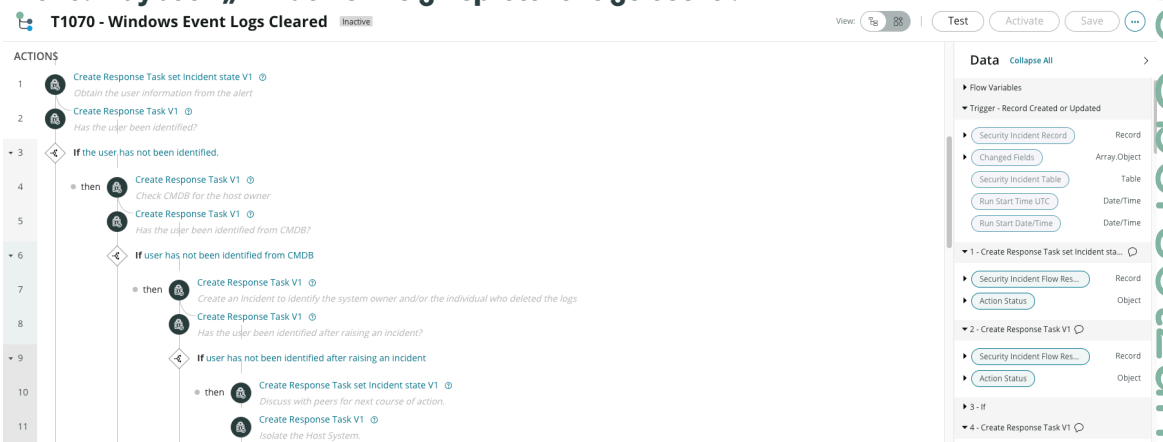
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **T1070 – Windows-Ereignisprotokolle gelöscht aus**.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „T1070 – Windows-Ereignisprotokolle gelöscht“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

   T1070: Playbook „Windows-Ereignisprotokolle gelöscht“.

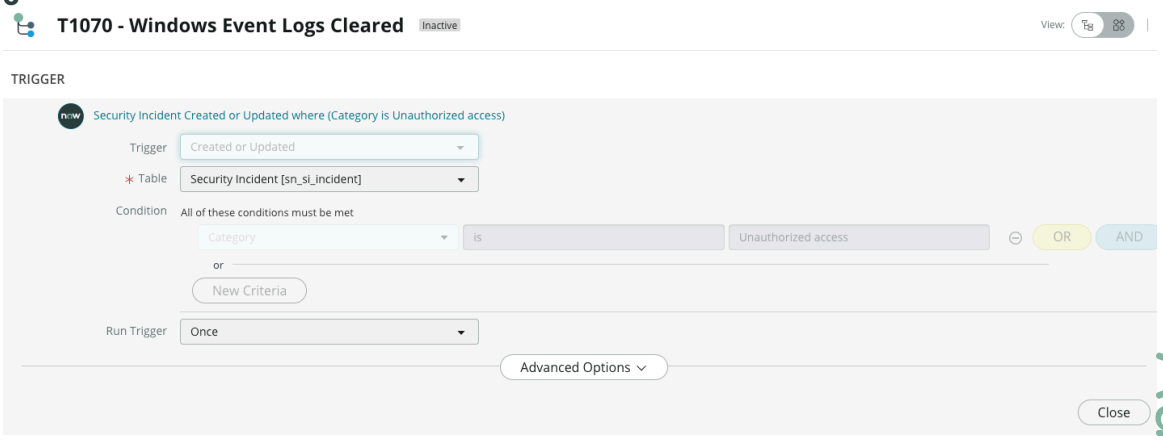
   

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieNicht autorisierter Zugriff**lautet.

T1070 – Playbook-Auslöserbedingung für Playbook-Ereignisprotokolle gelöscht



Verwenden Sie das Playbook „T1070 – Windows-Ereignisprotokolle gelöscht“.

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die Ereignistypen nachverfolgen, bei denen der Anwender Sicherheitsprotokolle entfernt. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „T1070 – Windows-Ereignisprotokolle gelöscht“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, rufen Sie in Aktion 1 die Benutzerdetails aus der Warnung ab.
2. Überprüfen Sie in Aktion 2, ob der Benutzer identifiziert wurde oder nicht.
3. Wenn in Aktion 3 der Benutzer nicht identifiziert wurde, führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie in Aktion 4 die CMDB (Configuration Management Database) auf die Details des Hostbesitzers.

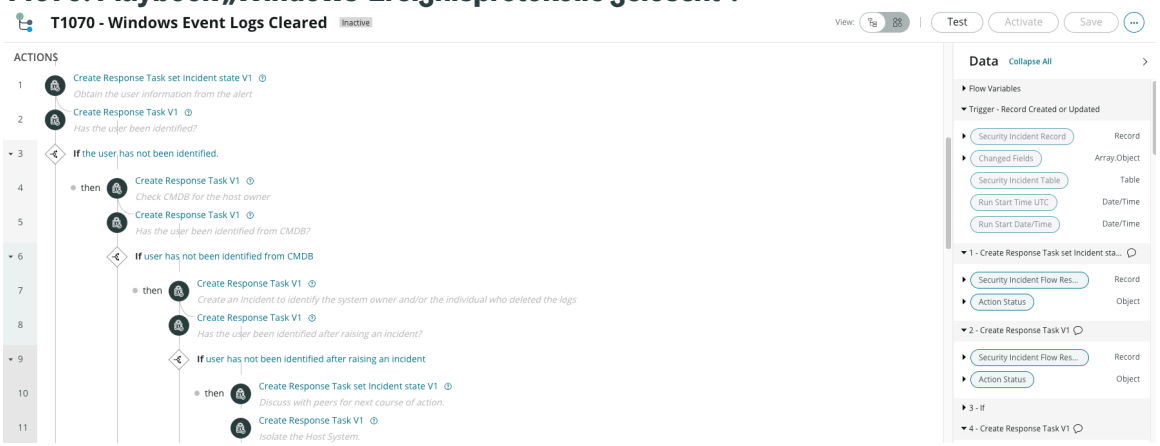
   b. Überprüfen Sie in Aktion 5, ob der Benutzer über die CMDB identifiziert wurde oder nicht.

      Wenn der Benutzer über die CMDB identifiziert wurde, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

T1070: Playbook „Windows-Ereignisprotokolle gelöscht“.



c. Wenn der Benutzer in Aktion 6 nicht über die CMDB identifiziert wurde, führen Sie die folgenden Schritte aus:

i. Erstellen Sie in Aktion 7 einen Incident, um den Systembesitzer und die Person zu identifizieren, die die Protokolle gelöscht hat.

ii. Überprüfen Sie in Aktion 8, ob der Benutzer identifiziert wurde, nachdem ein Incident ausgelöst wurde oder nicht.

Wenn der Benutzer nach dem Auslösen eines incident identifiziert wurde, wird in Aktion 8 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.

iii. Wenn in Aktion 9 der Benutzer nach dem Auslösen eines Incidents nicht identifiziert wurde, führen Sie die folgenden Schritte aus:

1. Besprechen Sie in Aktion 10 mit Kollegen die nächste Vorgehensweise.

2. Isolieren Sie in Aktion 11 das Hostsystem.

3. Entfernen Sie in Aktion 12 alle unerwünschten Dateien, die möglicherweise erstellt wurden, und löschen Sie die nicht autorisierten Accounts.

4. Heben Sie in Aktion 13 das Containment auf, und bringen Sie die Systeme wieder in den Betriebsstandard.

5. Schließen Sie in Aktion 14 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

In Aktion 15 endet der Flow.

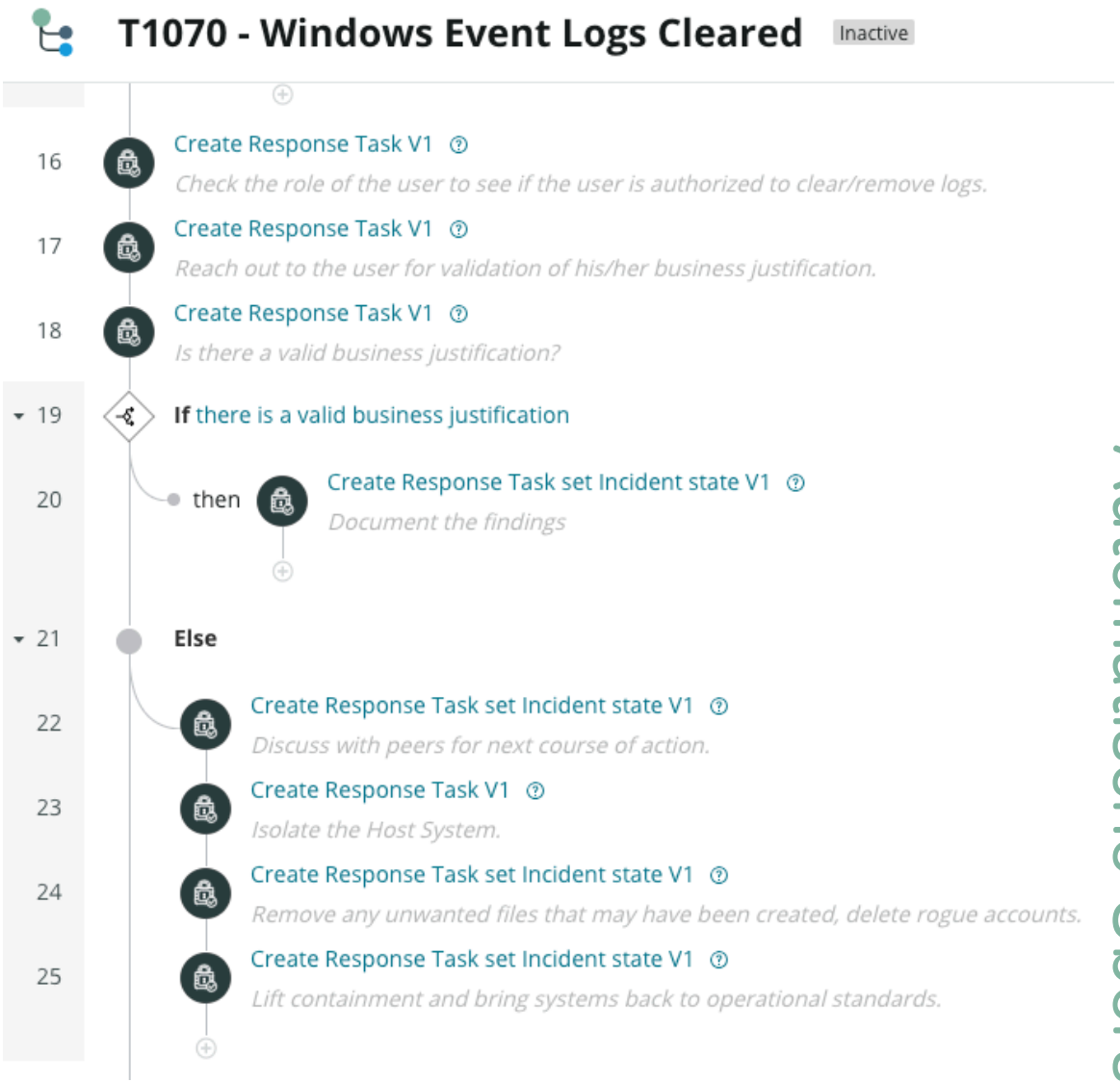
4. Wenn der Benutzer in Aktion 16 identifiziert wurde, überprüfen Sie die Rolle des Benutzers, um zu sehen, ob der Benutzer berechtigt ist, Protokolle zu löschen oder zu entfernen.

5. Wenden Sie sich in Aktion 17 an den Anwender, um seine geschäftliche Begründung zu validieren.
Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Benutzer zu kontaktieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mithilfe des Playbooks „T1070 – Windows-Ereignisprotokolle gelöscht“



6. Überprüfen Sie in Aktion 18, ob eine gültige geschäftliche Begründung angegeben wurde.
7. Wenn in Aktion 19 eine stichhaltige geschäftliche Begründung angegeben wurde, dokumentieren Sie in Aktion 20 die bisherigen Ergebnisse.
   Der Flow endet.
8. Wenn in Aktion 21 keine gültige geschäftliche Begründung angegeben wurde, führen Sie die folgenden Schritte aus:

   a. Besprechen Sie in Aktion 22 die nächste Vorgehensweise mit Kollegen.

   b. Isolieren Sie in Aktion 23 das Hostsystem.

   c. Entfernen Sie in Aktion 24 alle unerwünschten Dateien, die möglicherweise erstellt wurden, und löschen Sie die nicht autorisierten Accounts.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Heben Sie in Aktion 25 das Containment auf, und bringen Sie die Systeme wieder in den Betriebsstandard. Der Flow endet.

9. Schließen Sie in Aktion 26 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für OSquery der externen Adresse in der Datei „/etc/hosts“.

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die darauf hinweisen, dass ein interner Hostname oder eine Domäne einer externen IP-Adresse im lokalen DNS (/etc/hosts) eines Linux-Servers zugewiesen wurde.

Richten Sie die OSquery der externen Adresse im Playbook der Datei „/etc/hosts“ ein

Führen Sie die folgenden Schritte aus, um die OSquery der externen Adresse im Playbook der Datei „/etc/hosts“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

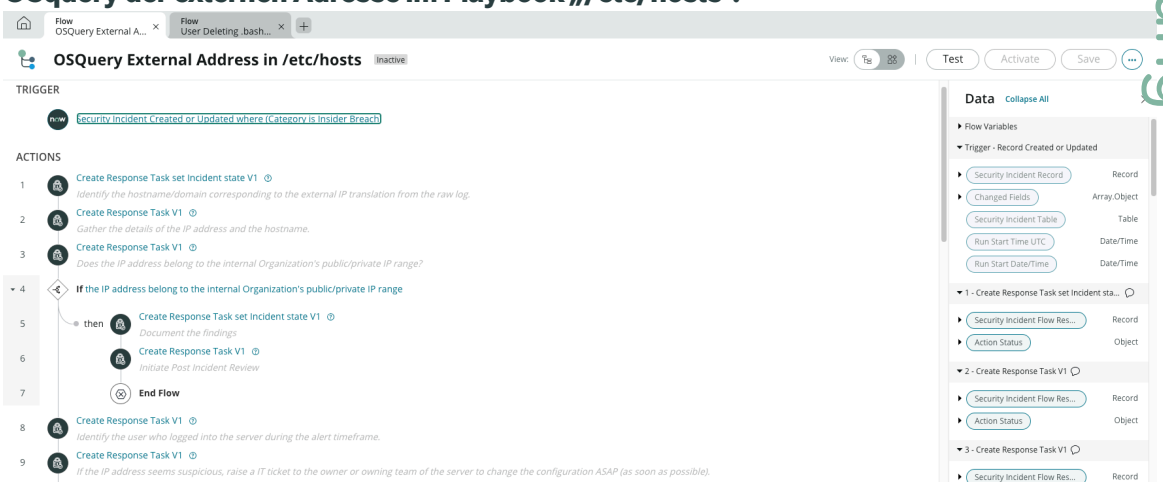
1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.

2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie **im Playbook „/etc/hosts“ die externe OSquery-Adresse** aus.

3. **Wahlweise:** Erstellen Sie eine Kopie der externen OSquery-Adresse im Playbook-Flow „/etc/hosts“, und nehmen Sie die erforderlichen Änderungen vor.

(Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

OSquery der externen Adresse im Playbook „/etc/hosts“.



4. Aktivieren Sie die Playbooks.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

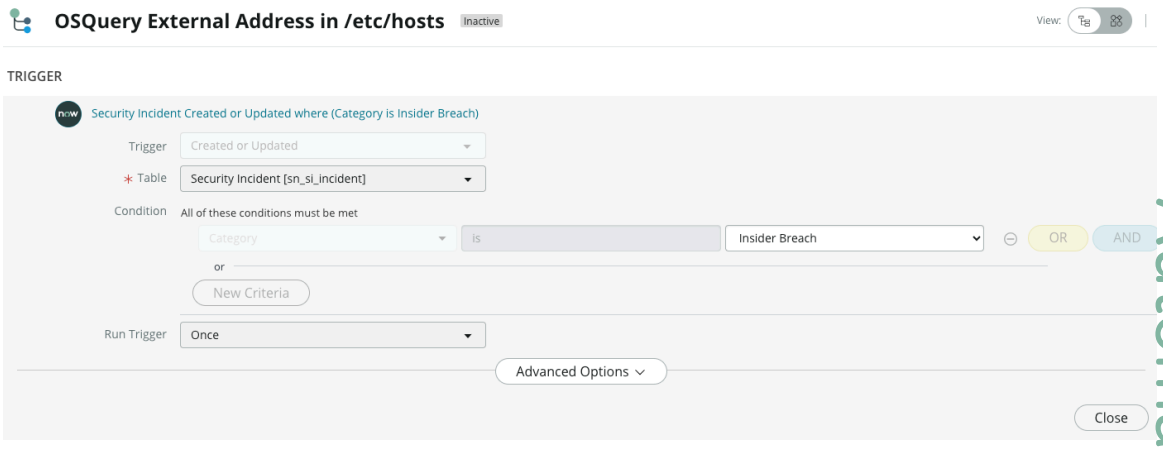
a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.

b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **Kategorie** **Interner Verstoß** lautet.

OSAbfrage der externen Adresse in „/etc/hosts“-Playbook-Auslöserbedingung



Verwenden Sie die OSquery der externen Adresse im Playbook der Datei „/etc/hosts“.

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die darauf hinweisen, dass ein interner Hostname oder eine Domäne einer externen IP-Adresse im lokalen DNS (/etc/hosts) eines Linux-Servers zugewiesen wurde. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die in der OSAbfrage der externen Adresse im Playbook für die Datei „/etc/hosts“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

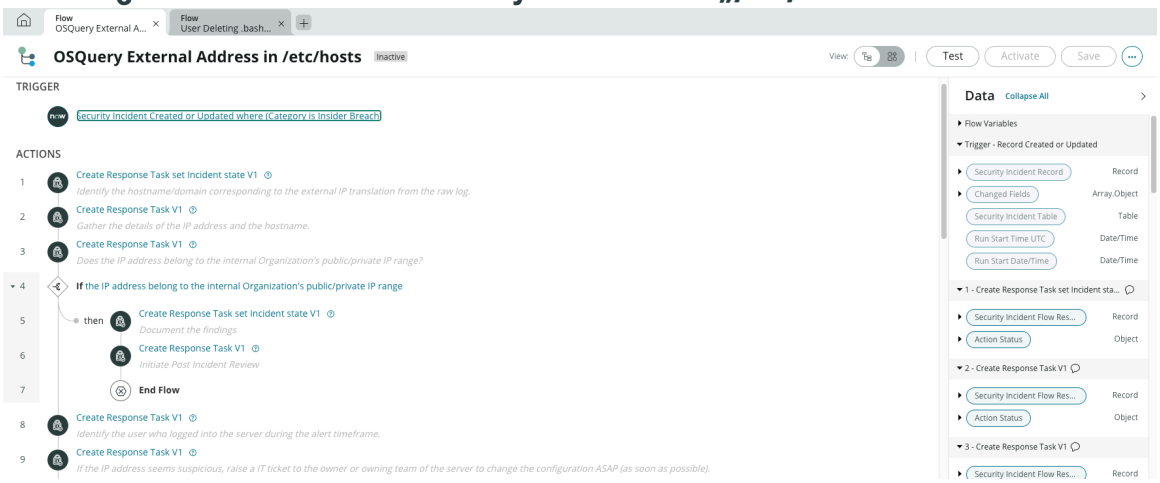
- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, identifizieren Sie in Aktion 1 den Hostnamen oder Domänennamen, der der externen IP-Übersetzung entspricht, aus dem Rohprotokoll.
2. Erfassen Sie in Aktion 2 die Details der IP-Adresse und des Hostnamens.
3. Überprüfen Sie in Aktion 3, ob diese IP-Adresse zum öffentlichen/privaten IP-Bereich der internen Organisation gehört oder nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OSAbfrage der externen Adresse im Playbook der Datei „/etc/hosts“.



4. Wenn die IP-Adresse in Aktion 4 zum öffentlichen/privaten IP-Bereich der internen Organisation gehört, führen Sie die folgenden Schritte aus:

   a. Dokumentieren Sie in Aktion 5 die bisherigen Ergebnisse.

   b. Initiieren Sie in Aktion 6 eine Überprüfung nach Incident.
   In Aktion 7 wird nach der Überprüfung nach Incident der Flow beendet.

5. Wenn die IP-Adresse nicht zum öffentlichen/privaten IP-Bereich der internen Organisation gehört, geben Sie in Aktion 8 den Anwender an, der sich während des Warnungszeitraums beim Server angemeldet hat.
6. Wenn in Aktion 9 die IP-Adresse verdächtig erscheint, lösen Sie ein IT-Ticket beim Besitzer oder beim Team des Servers aus, um die Konfiguration so bald wie möglich zu ändern.
7. Überprüfen Sie in Aktion 10, ob vor und nach dem Hinzufügen des DNS-Eintrags schädliche Aktivitäten auf dem Server aufgetreten sind.
8. Überprüfen Sie in Aktion 11, ob Verbindungen vom Server zur externen IP-Adresse vorhanden sind.
9. Dokumentieren Sie in Aktion 12 die bisherigen Ergebnisse.
10. Überprüfen Sie in Aktion 13, ob die Besitzer- oder Teaminformationen verfügbar sind.
11. Wenn in Aktion 14 Informationen zum Besitzer oder Team verfügbar sind, führen Sie die folgenden Schritte aus:

    a. Wenden Sie sich in Aktion 15 an den Besitzer oder das Team des Servers, um zu erfahren, ob die Aktivität erkannt wird.
    Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Besitzer oder das Team des Servers zu kontaktieren.

    b. Überprüfen Sie in Aktion 16, ob der Besitzer oder das Team eine gültige geschäftliche Begründung angegeben hat.

    c. Wenn in Aktion 17 der angegebene Besitzer oder das angegebene Team keine gültige geschäftliche Begründung angegeben hat, wird der Flow beendet.
    Wenn der Besitzer oder das Team jedoch eine stichhaltige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

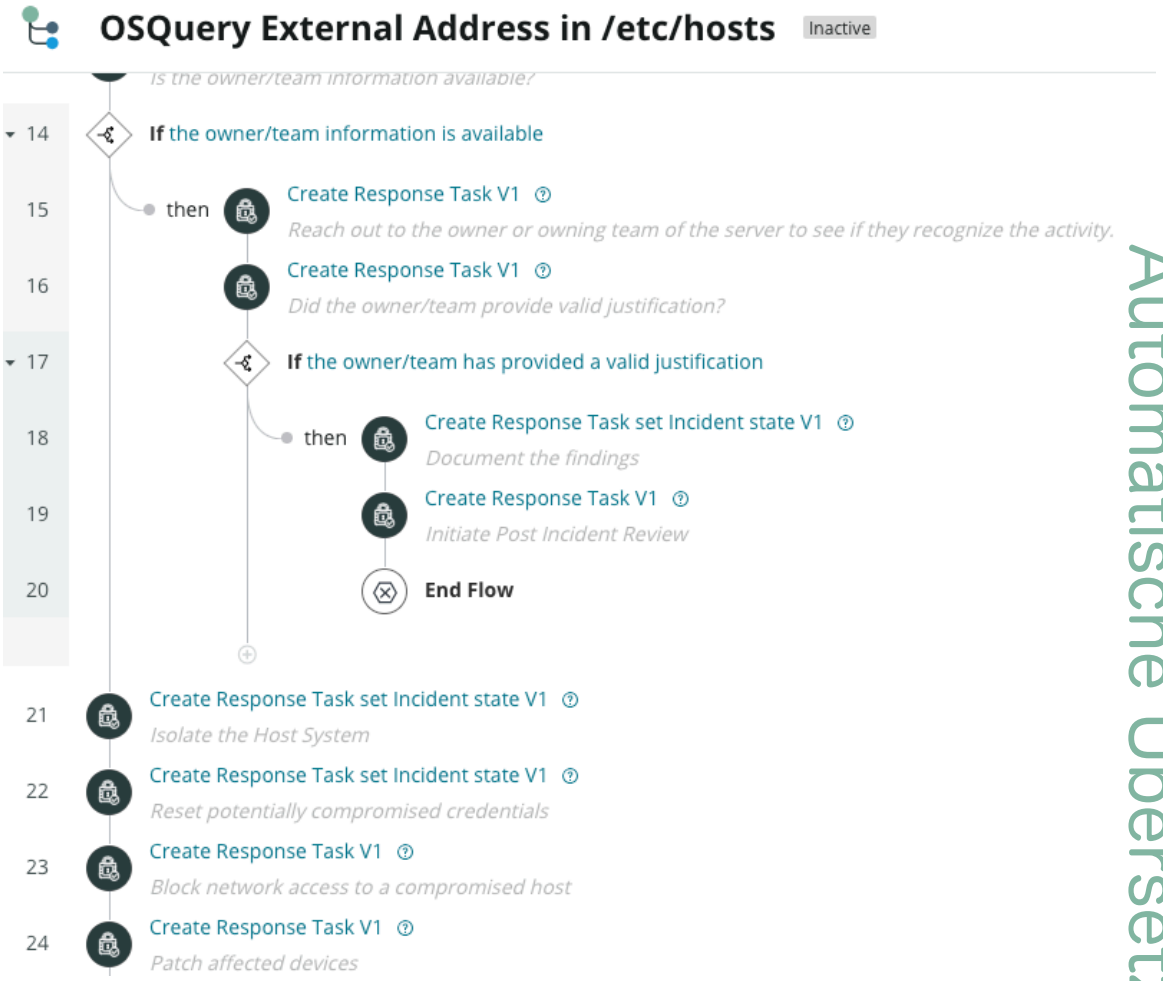
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Dokumentieren Sie in Aktion 18 die bisherigen Ergebnisse.

ii. Initiieren Sie in Aktion 19 eine Überprüfung nach Incident.

In Aktion 20 wird nach der Überprüfung nach Incident der Flow beendet.

Verwenden der OSquery der externen Adresse im Playbook der Datei „/etc/hosts“.



Automatische Übersetzung

12. Wenn in Aktion 21 die Besitzer- oder Teaminformationen nicht verfügbar sind, isolieren Sie das Hostsystem.
13. Setzen Sie in Aktion 22 die potenziell gefährdeten Anmeldeinformationen zurück.
14. Blockieren Sie in Aktion 23 den Netzwerkzugriff auf den gefährdeten Host.
15. Patchen Sie in Aktion 24 die betroffenen Geräte.
16. In Aktion 25: Containment aufheben und Systeme wieder auf Betriebsstandard zurücksetzen.
17. Schließen Sie in Aktion 26 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook zum Löschen des Bash-Verlaufs durch Anwender – Cloud

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die darauf hindeuten, dass jemand versucht hat, die Bash-Verlaufsdatei (`.bash_history`) von einem Linux-Server zu entfernen.

Hinweis:
Sie müssen diese Warnung mit Vorsicht entschärfen, da sie selten ausgelöst wird und möglicherweise auf eine interne Bedrohung hinweist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie das Playbook „Bash-Verlauf für das Löschen von Anwendern“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Bash-Verlauf für das Löschen von Anwendern“ einzurichten.

Vorbereitungen
Erforderliche Rolle:

- sn_si.admin
- flow_designer

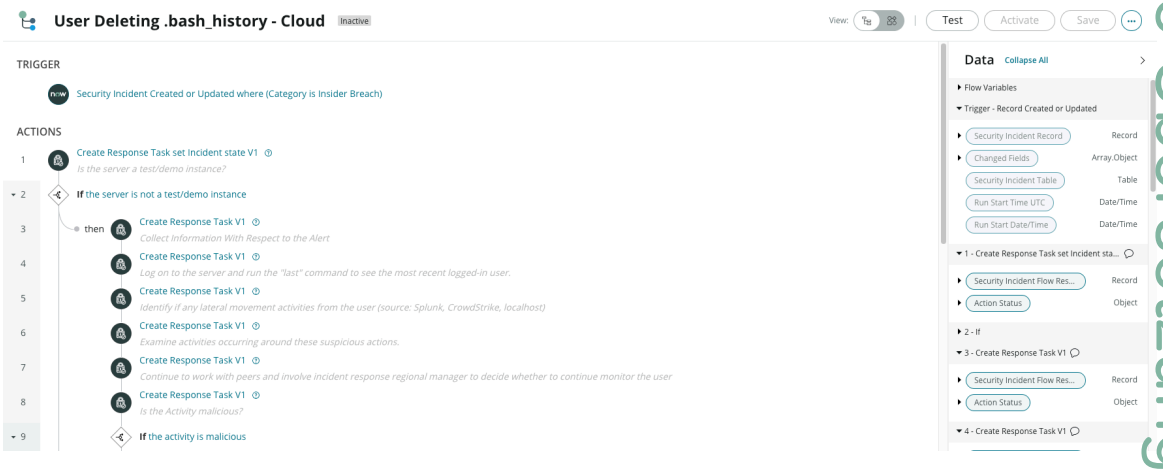
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **Anwenderlöschung .bash_history - Cloud** aus.
3. **Wahlweise:** Erstellen Sie eine Kopie des Flows „User Deleting .bash_history - Cloud Playbook“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

Anwender löscht Bash-Verlauf – Cloud-Playbook

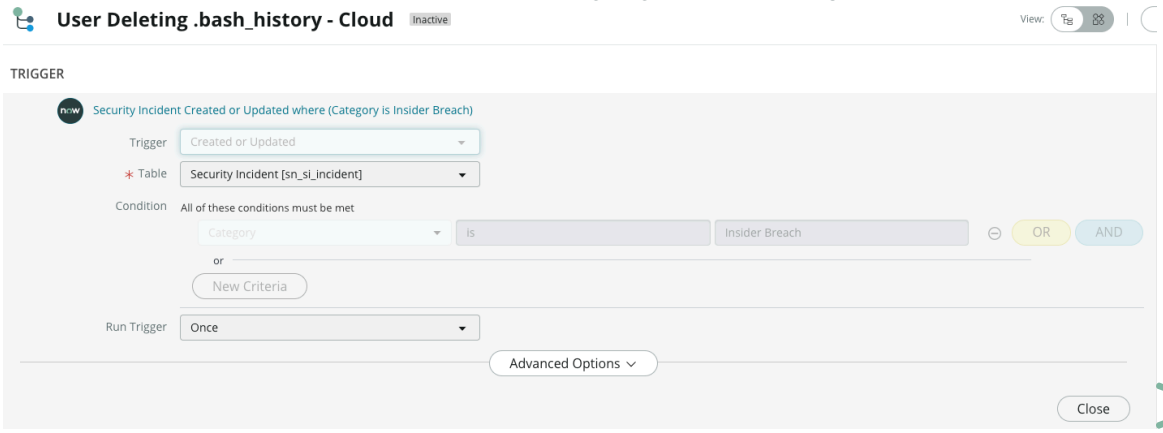


4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **Kategorie** **Interner Verstoß** lautet.

Anwender löscht Bash-Verlauf: Auslösebedingung für Cloud-Playbook



Verwenden Sie das Playbook „Bash-Verlauf zum Löschen von Anwendern“.

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die darauf hinweisen, dass jemand versucht hat, die Bash-Verlaufsdatei von einem Linux-Server zu entfernen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook Anwenderlöschen des Bash-Verlaufs (`.bash_history`) verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, überprüfen Sie in Aktion 1, ob der Server eine Test- oder Demoinstanz ist.
2. Wenn der Server in Aktion 2 keine Test- oder Demoinstanz ist, führen Sie die folgenden Schritte aus:

   a. Erfassen Sie in Aktion 3 die folgenden Informationen für die Warnung:
      - Anwendername
      - IP-Adresse
      - Böswillige Befehle, mit denen versucht wird, den Bash-Verlauf zu löschen
      - Alle vom Anwender ausgeführten Befehle, sofern in den CrowdStrike-Protokollen verfügbar.

   b. Melden Sie sich in Aktion 4 beim Server an, und führen Sie den `letzten` Befehl aus, um den zuletzt angemeldeten Anwender anzuzeigen.

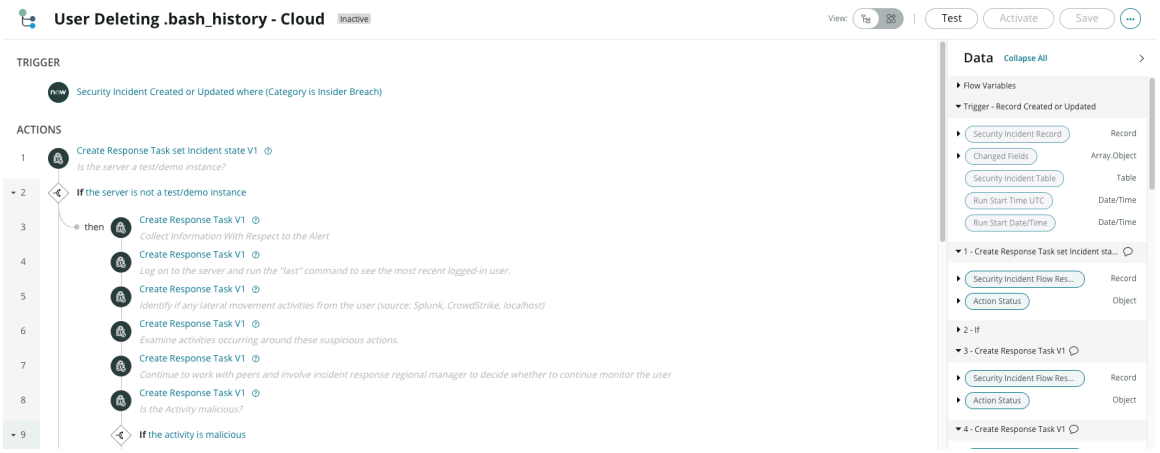
   c. Identifizieren Sie in Aktion 5, ob seitliche Bewegungsaktivitäten vom Anwender aufgetreten sind (Quelle: Splunk, CrowdStrike, localhost).

   d. Überprüfen Sie in Aktion 6 die Aktivitäten im Zusammenhang mit diesen verdächtigen Aktionen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook zum Löschen des Bash-Verlaufs durch Anwender



e. Setzen Sie in Aktion 7 die Arbeit mit Kollegen fort, und beziehen Sie den Regional Manager für die Reaktion auf Incidents in die Entscheidung ein, ob der Benutzer weiterhin überwacht werden soll.

f. Bestimmen Sie in Aktion 8, ob die Aktivität schädlich ist oder nicht.

g. Wenn die Aktivität in Aktion 9 schädlich ist, führen Sie die folgenden Schritte aus:

i. Wenden Sie sich in Aktion 10 während der Untersuchung an den IT-Support, und fordern Sie ein Einfrieren des Accounts an.

ii. Stellen Sie in Aktion 11 sicher, dass die Instanz in einem normalen Zustand ohne schädliche Aktivitäten wiederhergestellt wird.

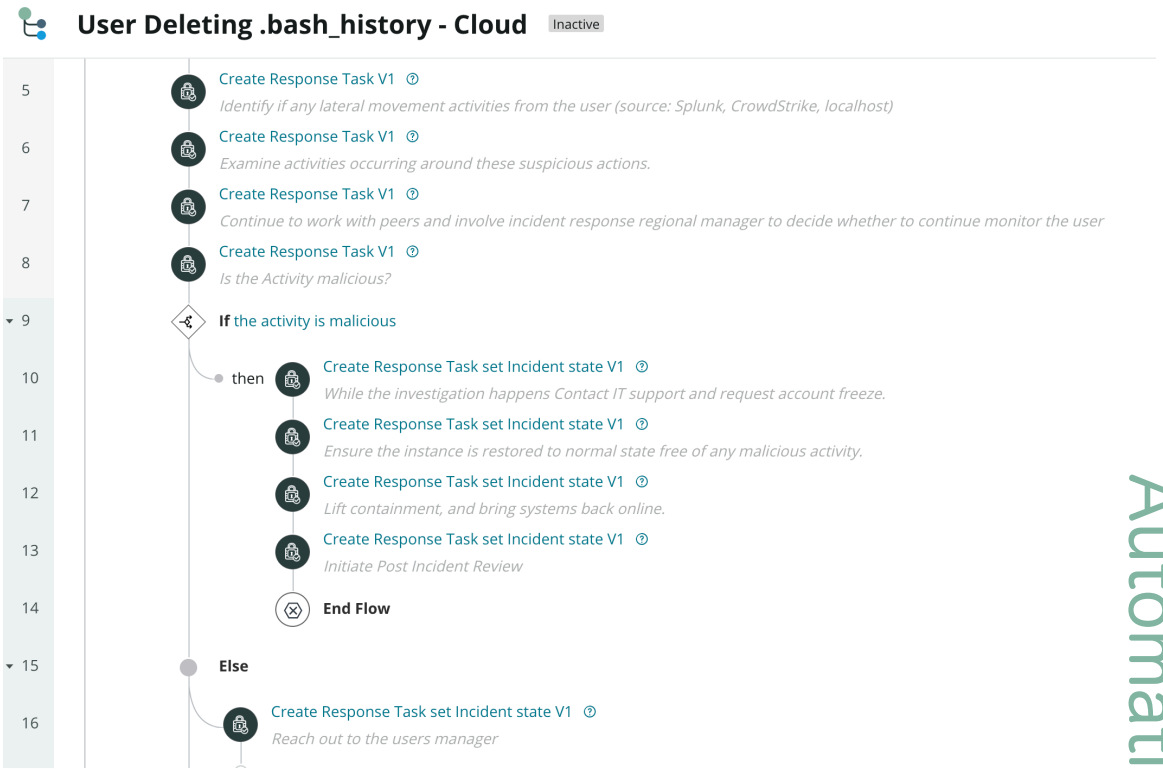
iii. In Aktion 12: Containment aufheben und Systeme wieder auf Betriebsstandard zurücksetzen.

iv. Initiieren Sie in Aktion 13 eine Überprüfung nach Incident.

In Aktion 14 wird nach der Überprüfung nach Incident der Flow beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden des Playbooks zum Löschen des Bash-Verlaufs von Anwendern



h. Wenn in Aktion 15 die Aktivität nicht böswillig ist, wenden Sie sich in Aktion 16 an den Manager des Benutzers.
Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Manager des Benutzers zu kontaktieren und ihn über den empfohlenen Ansatz zu informieren.

3. Dokumentieren Sie in Aktion 17 die bisherigen Ergebnisse.

4. Schließen Sie in Aktion 18 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für erfolgreiche VPN-Versuche von den Servicekonten – Unternehmen/Cloud

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die erfolgreiche Anmeldeversuche von Servicekonten über VPN nachverfolgen. Servicekonten dürfen keine Anmeldeereignisse von einem VPN haben, und solche Ereignisse können Indikatoren für Brute-Force oder eine mögliche Offenlegung der Anmeldeinformationen des Kontos sein.

Richten Sie Erfolgreiche VPN-Versuche über das Playbook für Servicekonten ein

Führen Sie die folgenden Schritte aus, um die Liste „Erfolgreiche VPN-Versuche“ im Playbook für Servicekonten einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Automatische Übersetzung

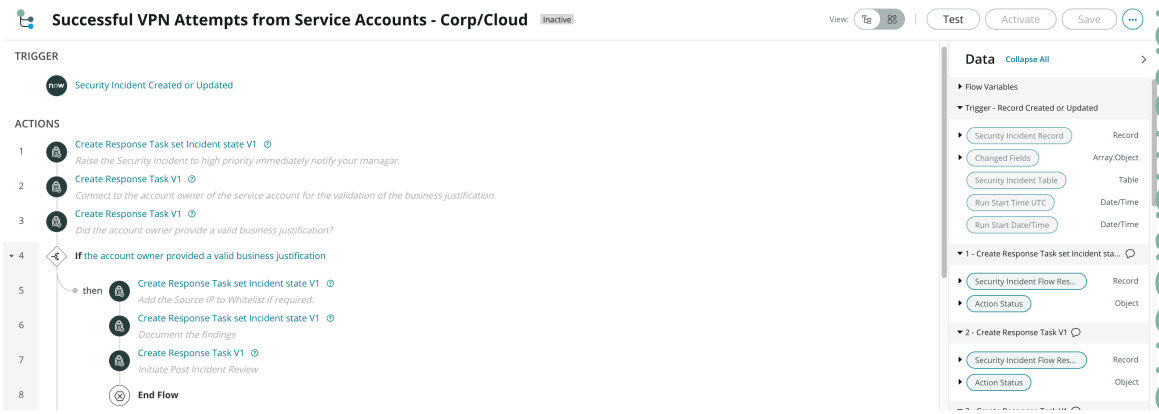
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie **Erfolgreiche VPN-Versuche aus dem Playbook für Servicekonten** aus.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „Erfolgreiche VPN-Versuche“ aus dem Servicekonto, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

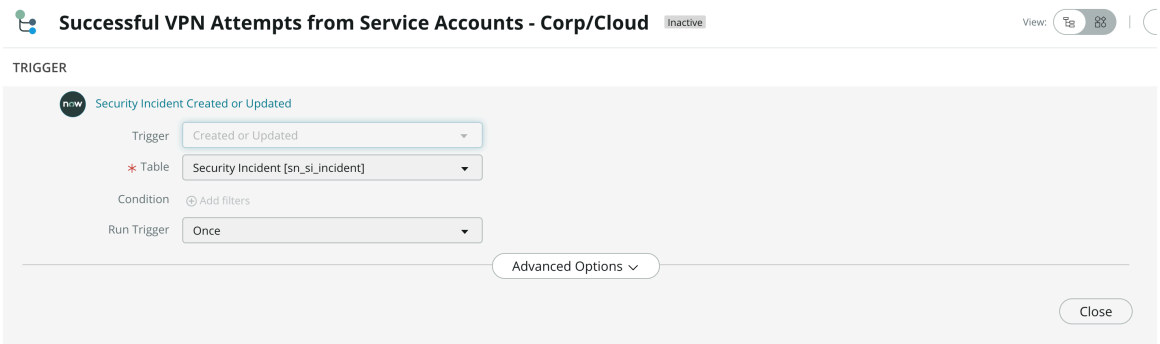
   Erfolgreiche VPN-Versuche aus dem Playbook „Servicekonten – Unternehmen/ Cloud“.

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der Security Incident basierend auf Ihren erforderlichen Bedingungen erstellt oder aktualisiert wird. Zum Beispiel, wenn **die KategorieInsider-Verstoß**lautet.

   Erfolgreiche VPN-Versuche über die Auslösebedingung „Servicekonten – Playbook für Unternehmen/Cloud“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die Erfolgreiche VPN-Versuche aus dem Playbook für Servicekonten

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die erfolgreiche Anmeldeversuche von Servicekonten über VPN nachverfolgen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Erfolgreiche VPN-Versuche aus dem Servicekonten-Playbook“ verfügbar sind.

Vorbereitungen

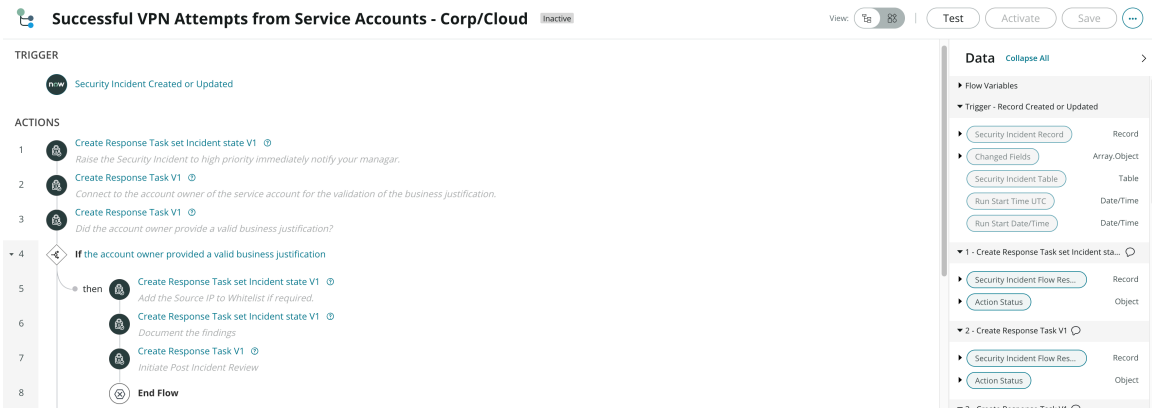
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, erhöhen Sie in Aktion 1 den Security Incident auf eine hohe Priorität, und benachrichtigen Sie sofort Ihren Manager.
2. Wenden Sie sich in Aktion 2 an den Besitzer des Servicekontos, um die geschäftliche Begründung zu validieren.
   Sie können die bereitgestellte E-Mail-Vorlage verwenden, um sich an den Besitzer des Service-Accounts zu wenden und die geschäftliche Begründung zu validieren.
3. Überprüfen Sie in Aktion 3, ob der Service-Account-Besitzer eine stichhaltige geschäftliche Begründung angegeben hat.

Erfolgreiche VPN-Versuche aus dem Playbook „Servicekonten – Unternehmen/ Cloud“.



4. Wenn der Besitzer des Service-Accounts in Aktion 4 eine stichhaltige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

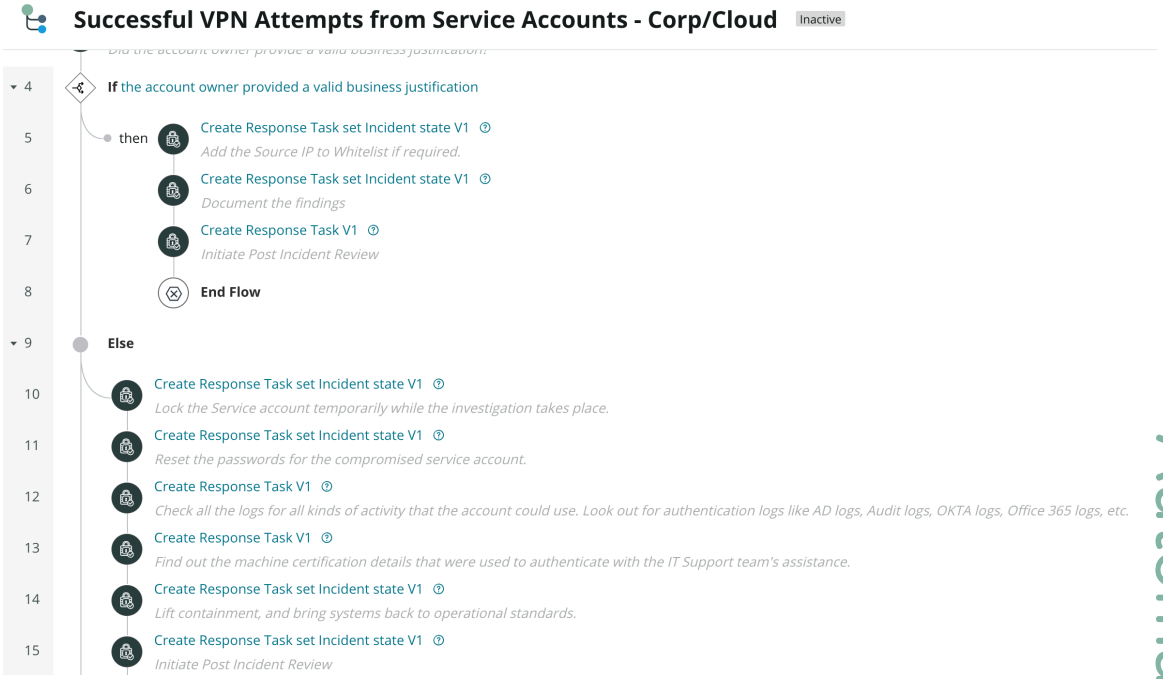
   a. Fügen Sie in Aktion 5 bei Bedarf die Quell-IP der Allow-Liste hinzu.

   b. Dokumentieren Sie in Aktion 6 die bisherigen Ergebnisse.

   c. Initiieren Sie in Aktion 7 eine Überprüfung nach Incident.
   In Aktion 8 wird nach der Überprüfung nach Incident der Flow beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden der erfolgreichen VPN-Versuche aus dem Playbook „Servicekonten – Unternehmen/Cloud“.



5. Wenn der Besitzer des Servicekontos in Aktion 9 keine stichhaltige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

   a. Sperren Sie in Aktion 10 den Serviceaccount vorübergehend, während die Untersuchung stattfindet.

   b. Setzen Sie in Aktion 11 die Passwörter für den gefährdeten Service-Account zurück.

   c. Überprüfen Sie in Aktion 12 die Protokolle auf alle Arten von Aktivitäten, die für den Account verwendet werden könnten.
   Achten Sie auf Authentifizierungsprotokolle wie Active Directory-Protokolle, Audit-Protokolle, Okta-Protokolle, Office 365-Protokolle usw.

   d. Suchen Sie in Aktion 13 nach den Computerzertifizierungsdetails, die zur Authentifizierung mit Unterstützung des IT-Supportteams verwendet werden.

   e. In Aktion 14: Containment aufheben und Systeme wieder auf Betriebsstandard zurücksetzen.

   f. Schließen Sie in Aktion 15 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für versuchten Zugriff auf deaktivierte Accounts

Dieses Playbook wird ausgelöst, wenn ein Mitarbeiter, dessen Account gekündigt, deaktiviert oder getrennt wurde, versucht, sich mit seinen Anmeldeinformationen anzumelden. Der Identitätsstatus des Benutzers in „Sail Point“ wird im Allgemeinen am Datum der Kündigung auf „Deaktiviert“ aktualisiert.

30 Tage ab dem Kündigungsdatum ist der ideale Zeitpunkt, um in einem getrennten Status aktualisiert zu werden. Sie können die Geschäftslogik in Point nutzen, um die RSA-Accounts zu löschen und die Active Directory(AD)-Gruppenmitgliedschaften nach 30 Tagen zu entfernen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie das Playbook für versuchten Zugriff mit deaktiviertem Account ein

Führen Sie die folgenden Schritte aus, um das Playbook für versuchten Zugriff mit deaktiviertem Account einzurichten.

Vorbereitungen

Erforderliche Rolle:

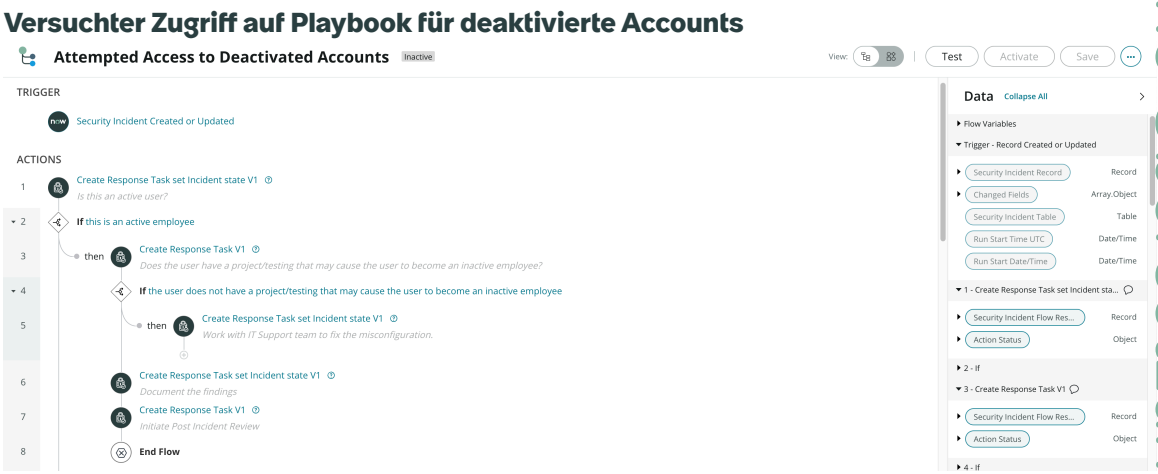
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook „ **Versuchter Zugriff – deaktivierter Account“** aus.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „Versuchter Zugriff – deaktivierter Account“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

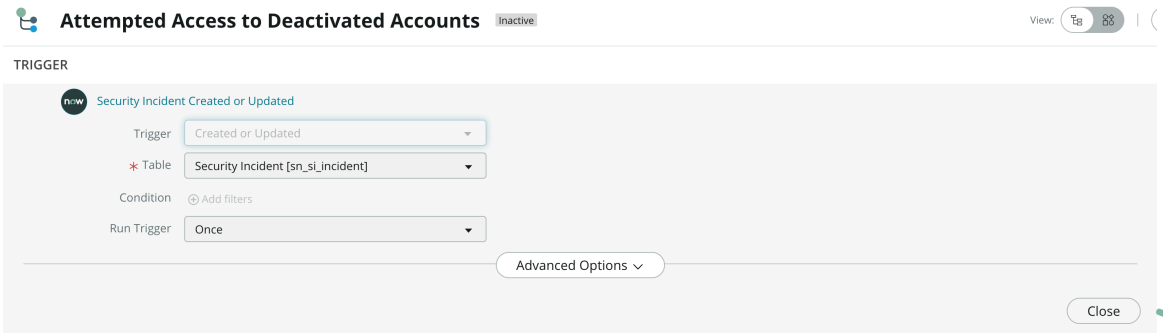


4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst, wenn der Security Incident basierend auf Ihren erforderlichen Bedingungen erstellt oder aktualisiert wird. Beispiel: Wenn **die Kategorie„Insider-Verstoß“**ist

Auslösebedingung für Playbook für versuchten Zugriff auf deaktivierte Accounts



Verwenden Sie das Playbook „Versuchter Zugriff auf deaktivierte Accounts“.

Verwenden Sie dieses Playbook, wenn ein Mitarbeiter, dessen Account gekündigt, deaktiviert oder getrennt wurde, versucht, sich mit seinen Anmeldeinformationen anzumelden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Versuchter Zugriff auf deaktivierte Accounts“ verfügbar sind.

Vorbereitungen

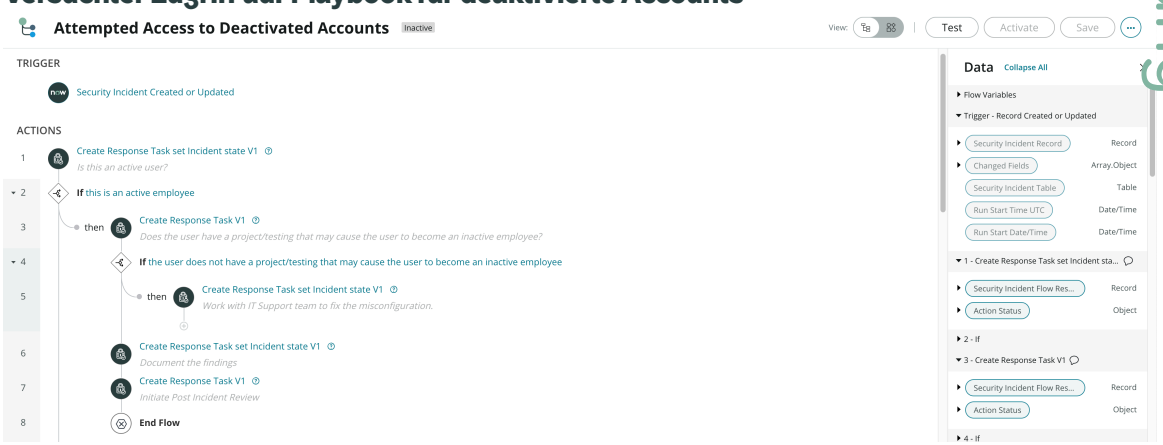
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, überprüfen Sie in Aktion 1, ob der versuchte Zugriff auf die deaktivierten Accounts von einem aktiven Anwender erfolgt ist.
2. Überprüfen Sie in Aktion 2, ob der versuchte Zugriff auf die deaktivierten Accounts von einem aktiven Mitarbeiter erfolgt ist.

Versuchter Zugriff auf Playbook für deaktivierte Accounts



3. Wenn der Zugriffsversuch auf die deaktivierten Accounts von einem aktiven Mitarbeiter erfolgt ist, gehen Sie wie folgt vor:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Überprüfen Sie in Aktion 3, ob der Anwender ein Projekt oder einen Testfall hatte, durch das er zu einem inaktiven Mitarbeiter wurde.

b. Wenn der Benutzer in Aktion 4 kein Projekt oder keinen Testfall hatte, durch den er zu einem inaktiven Mitarbeiter wurde, arbeiten Sie mit dem IT-Supportteam zusammen, um die Fehlkonfiguration zu beheben. Der Flow endet.

c. Wenn der Benutzer in Aktion 5 ein Projekt oder einen Testfall hatte, durch das/den er zu einem inaktiven Mitarbeiter wurde, führen Sie die folgenden Schritte aus:

i. Dokumentieren Sie in Aktion 6 die bisherigen Ergebnisse.

ii. Initiieren Sie in Aktion 7 eine Überprüfung nach Incident.

In Aktion 8 wird nach der Überprüfung nach Incident der Flow beendet.

4. Wenn in Aktion 9 der versuchte Zugriff auf den deaktivierten Account nicht von einem aktiven Mitarbeiter erfolgt ist, führen Sie die folgenden Schritte aus:

a. Überprüfen Sie in Aktion 10, ob sich der Anwender erfolgreich angemeldet hat.

b. Überprüfen Sie in Aktion 11, wann das Offboarding des Mitarbeiters erfolgt ist.

c. Untersuchen Sie in Aktion 12 die Ereignisse in Splunk, um die Aktivitäten des Benutzers während des Zeitraums zu untersuchen.

d. Stellen Sie in Aktion 13 basierend auf der bisherigen Untersuchung fest, ob der Benutzer Daten extrahiert hat.

e. Wenn der Benutzer in Aktion 14 keine Daten extrahiert hat, führen Sie die folgenden Schritte aus:

i. In Aktion 15: Arbeiten Sie mit dem IT-Supportteam zusammen, um alle aktiven Sitzungen zu beenden und die Accounts zu deaktivieren.

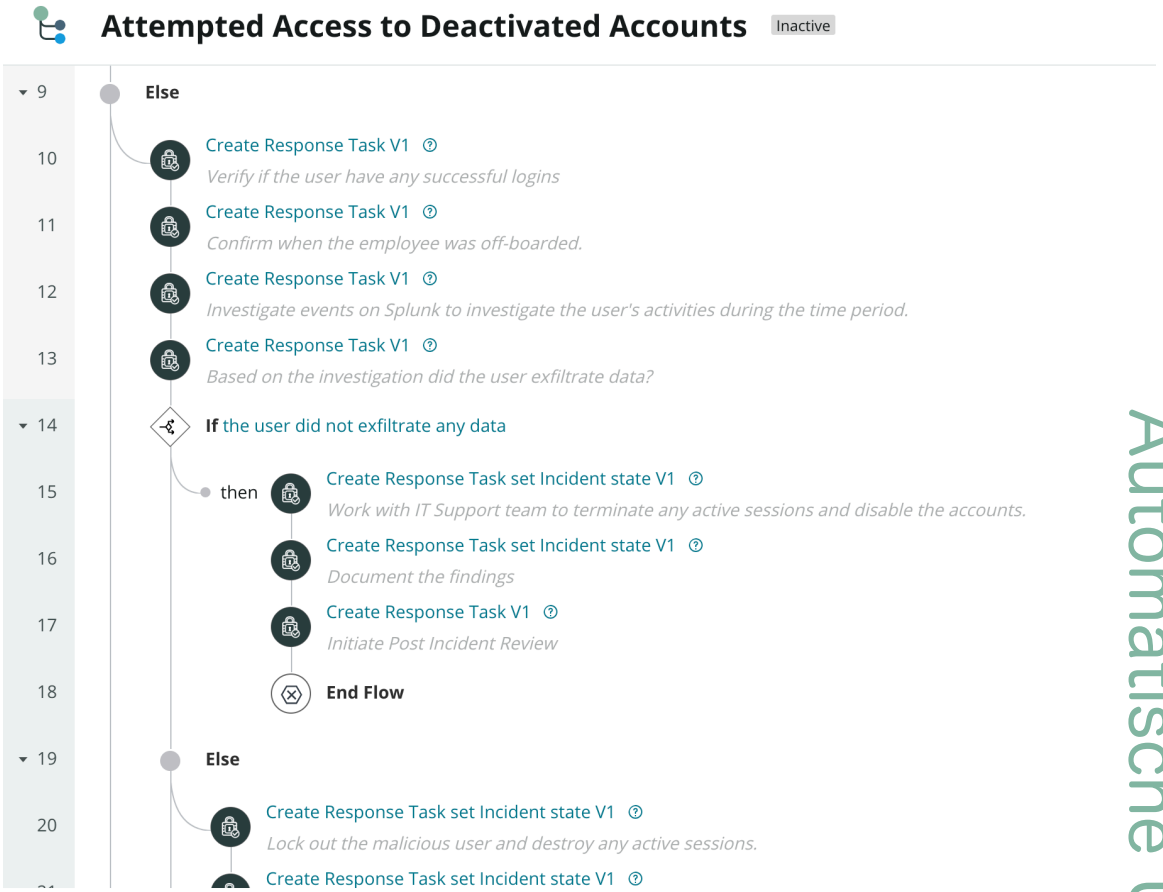
ii. Dokumentieren Sie in Aktion 16 die bisherigen Ergebnisse.

iii. Initiieren Sie in Aktion 17 eine Überprüfung nach Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Aktion 18 wird nach der Überprüfung nach Incident der Flow beendet.

Mithilfe des Playbooks „Versuchter Zugriff auf deaktivierte Accounts“.



5. Wenn der Anwender in Aktion 19 Daten exgefiltert hat, führen Sie die folgenden Schritte aus:

a. Sperren Sie in Aktion 20 den böswilligen Anwender, und löschen Sie alle aktiven Sitzungen.

b. In Aktion 21: Arbeiten Sie mit dem IT-Supportteam zusammen, um alle Konten zu deaktivieren.

c. Stellen Sie in Aktion 22 sicher, dass der normale Status der Ressourcen wiederhergestellt wird und keine schädlichen Aktivitäten mehr vorliegen.
Bei Bedarf können Sie ein erneutes Bild der Ressourcen erstellen.

d. In Aktion 23: Containment aufheben und Systeme wieder auf Betriebsstandard zurücksetzen.

e. Schließen Sie in Aktion 24 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für T1003 – Umgehung der Verteidigung – Mimikatz DCShadow

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, von denen angenommen wird, dass sie durch Mimikatz DCShadow verursacht wurden. DCShadow ist eine Funktion in Mimikatz, die das Verhalten eines Domänencontrollers (eines Servers, der Active Directory steuert) simuliert, um eigene Daten einzuschleusen und die meisten standardmäßigen Sicherheitskontrollen (einschließlich SIEMs) zu umgehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mimikatz DCShadow hilft dem Angreifer, einen nicht autorisierten Domänencontroller (DC) einzurichten, der Teil von Active Directory (AD) wird. Nach der Registrierung kann er als berechtigter DC fungieren und Schaden anrichten.

Richten Sie das Playbook „T1003 – Verteidigungsumgehung – Mimikatz DCShadow“ ein

Führen Sie die folgenden Schritte aus, um das Playbook T1003 - Defence Evasion - Mimikatz DCShadow einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

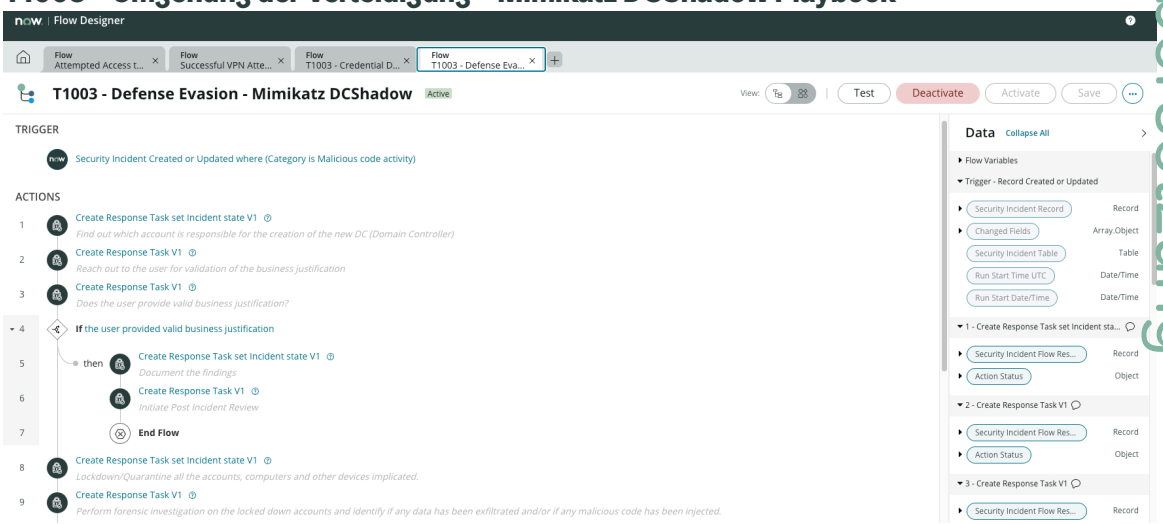
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **T1003 - Defence Evasion - Mimikatz DCShadow** aus.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows T1003 – Defence Evasion – Mimikatz DCShadow, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

   T1003 – Umgehung der Verteidigung – Mimikatz DCShadow Playbook

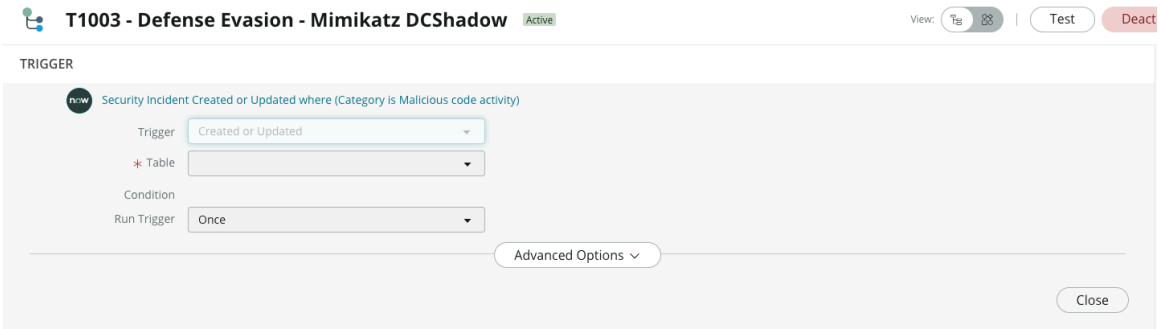
   

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieBöswillige Code-Aktivität**lautet.

T1003 – Umgehung der Verteidigung – Auslöserbedingung für Mimikatz DCShadow-Playbook



Verwenden Sie das Playbook T1003 – Umgehung der Verteidigung – Mimikatz DCShadow

Verwenden Sie dieses Playbook, um Security Incidents zu untersuchen, die mutmaßlich durch Mimikatz DCShadow verursacht wurden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Verteidigungsumgehung – Mimikatz DCShadow verfügbar sind.

Vorbereitungen

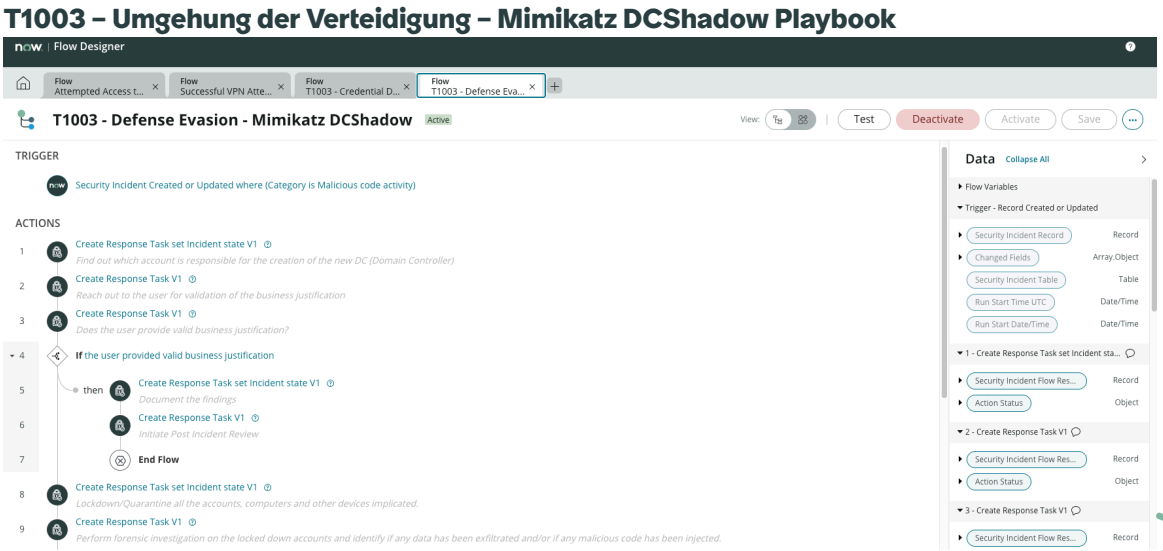
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, finden Sie in Aktion 1 heraus, welcher Account für die Erstellung des neuen DC (Domänencontroller) verantwortlich ist.
2. Wenden Sie sich in Aktion 2 an den Anwender, um die geschäftliche Begründung zu validieren. Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Benutzer zu kontaktieren.
3. Überprüfen Sie in Aktion 3, ob der Anwender eine gültige geschäftliche Begründung angegeben hat.
4. Wenn der Anwender in Aktion 4 eine stichhaltige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. Dokumentieren Sie in Aktion 5 die bisherigen Ergebnisse.

b. Initiieren Sie in Aktion 6 eine Überprüfung nach Incident.
In Aktion 7 wird nach der Überprüfung nach Incident der Flow beendet.

5. Wenn der Anwender in Aktion 8 keine stichhaltige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

a. In Aktion 9 alle beteiligten Konten, Computer und anderen Geräte sperren oder unter Quarantäne stellen.

b. Führen Sie in Aktion 10 eine forensische Untersuchung der gesperrten Accounts durch, und stellen Sie fest, ob Daten extrahiert oder schädlicher Code einschleusen wurden.

c. Erstellen Sie in Aktion 11 ein erneutes Abbild der betroffenen Ressourcen.

d. In Aktion 12: Containment aufheben und Systeme wieder auf Betriebsstandard zurücksetzen.

e. Schließen Sie in Aktion 13 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für T1003 – Dumping von Anmeldeinformationen – Mimikatz DCSync

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, von denen angenommen wird, dass sie durch Mimikatz DCSync verursacht wurden. Dieses Playbook wird ausgelöst, wenn eine der Mimikatz-Funktionen (`lsadump::dcsync`) verwendet wird. Die Funktion wird normalerweise auf angegriffenen Domänencontrollern (DC) verwendet.

Mimikatz ist ein beliebtes Hacking-Tool, mit dem Anwender Befehle eingeben können, um vertrauliche Daten aus dem angegriffenen System abzurufen. Die vertraulichen Daten umfassen Passwörter, deren Hashes und andere.

Hinweis:
Dies ist eine Warnung mit hoher Genauigkeit, von der angenommen wird, dass sie selten ausgelöst wird. Wenn dies ausgelöst wird, benachrichtigen Sie sofort ein leitendes Teammitglied oder einen Manager.

Richten Sie das Playbook „T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync“ ein

Führen Sie die folgenden Schritte aus, um das Playbook T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

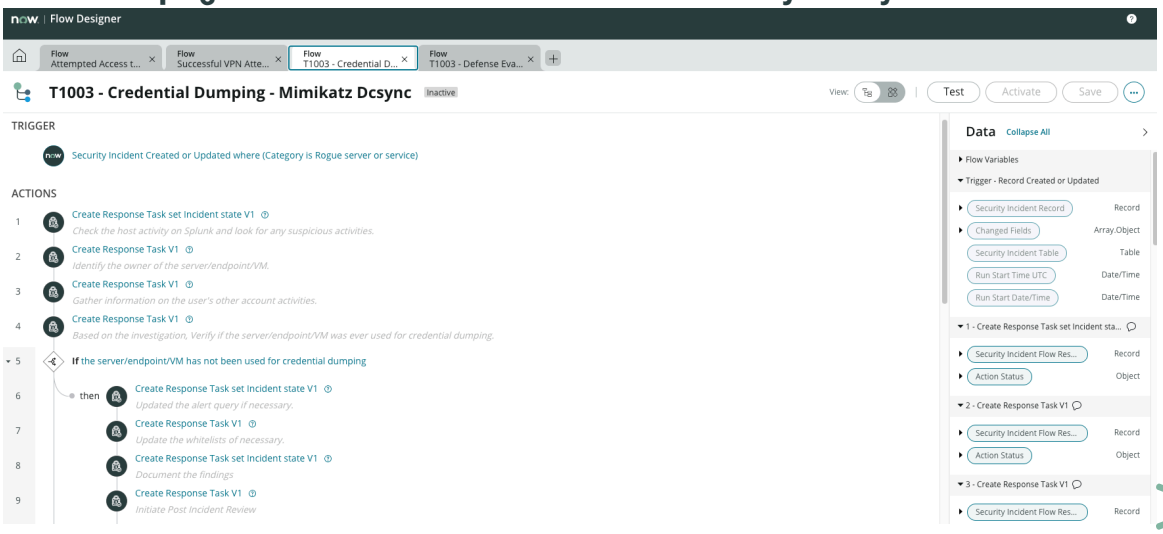
Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync** aus.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

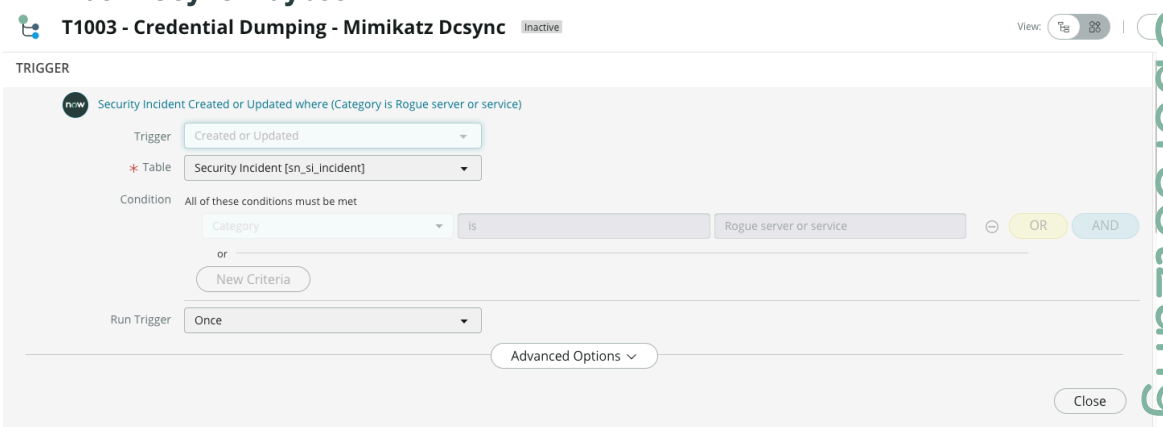
T1003: Dumping von Anmeldeinformationen – Mimikatz DCSync-Playbook



4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **Kategorie** auf **„Nicht autorisierter Server oder Service“**festgelegt ist.

T1003 – Dumping von Anmeldeinformationen – Auslösebedingung für Mimikatz DCSync-Playbook



Verwenden Sie das Playbook T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, von denen vermutet wird, dass sie durch Mimikatz DCSync verursacht wurden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

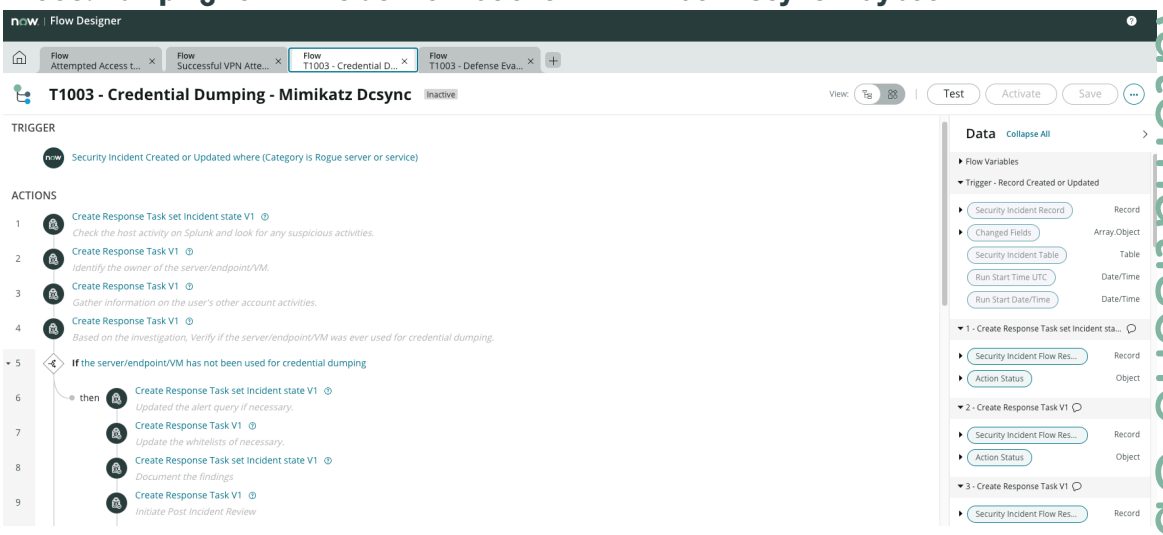
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, überprüfen Sie in Aktion 1 die Hostaktivität in Splunk, und suchen Sie nach verdächtigen Aktivitäten.
2. Identifizieren Sie in Aktion 2 den Besitzer des Servers/Endpunkts/der VM.
   Wenn der Anwender online ist, führen Sie den CrowdStrike EDR aus, um einen besseren Umfang der Systemaktivitäten zu erfassen.
3. Erfassen Sie in Aktion 3 Informationen zu den anderen Kontoaktivitäten des Benutzers.
4. Überprüfen Sie in Aktion 4 basierend auf der Untersuchung, ob der Server/Endpunkt/die VM jemals für das Dumping von Anmeldeinformationen verwendet wurde.
5. Wenn in Aktion 5 der Server/Endpunkt/die VM nicht für die Speicherung von Anmeldeinformationen verwendet wurde, führen Sie die folgenden Aktionen aus:

T1003: Dumping von Anmeldeinformationen – Mimikatz DCsync-Playbook



   a. Aktualisieren Sie in Aktion 6 die Warnungsabfrage, falls erforderlich.

   b. Aktualisieren Sie in Aktion 7 ggf. die Allow-Liste.

   c. Dokumentieren Sie in Aktion 8 die bisherigen Ergebnisse.

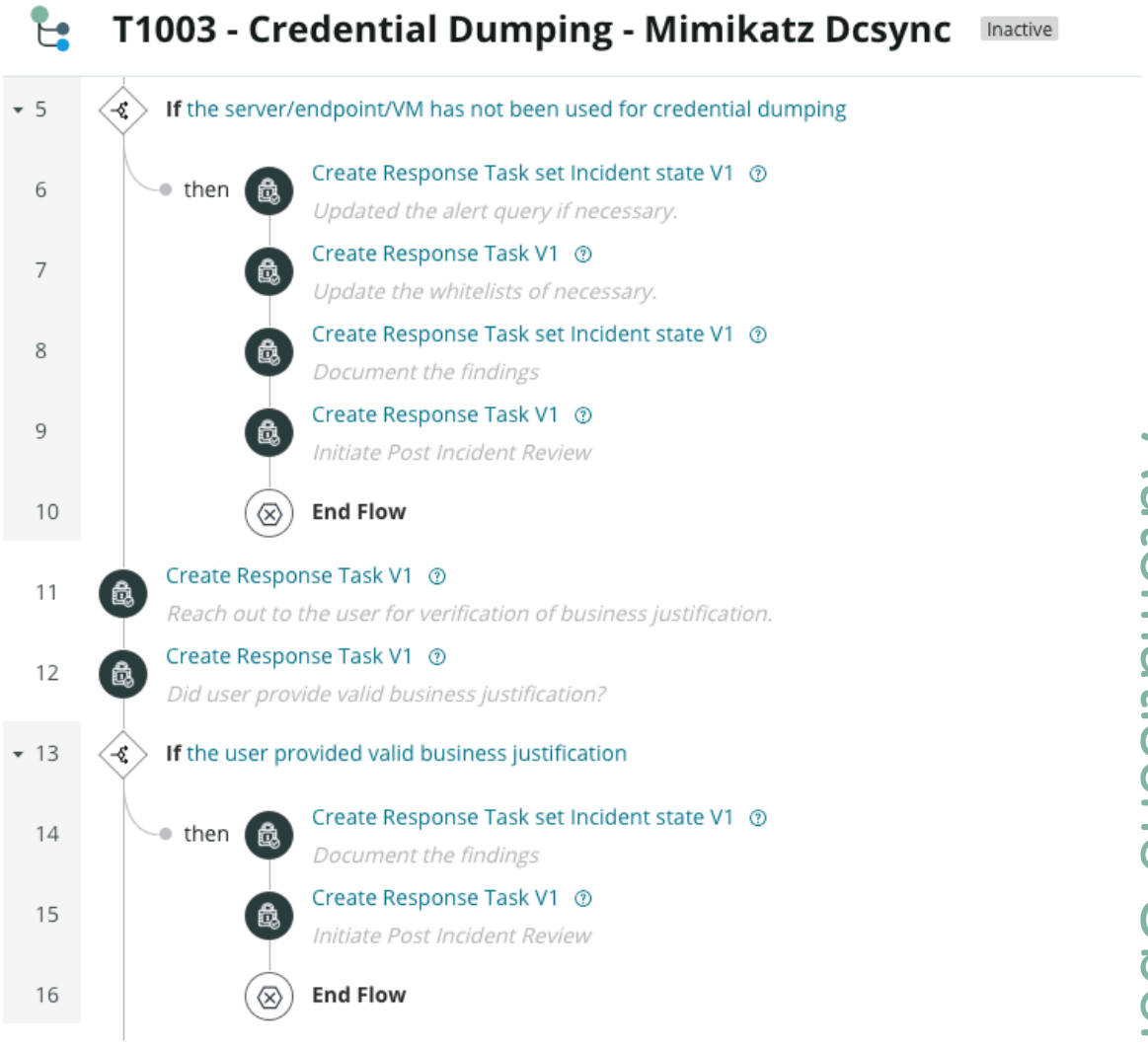
   d. Initiieren Sie in Aktion 9 eine Überprüfung nach Incident.
      In Aktion 10 endet der Flow.

6. Wenn der Server/Endpunkt/die VM für das Dumping von Anmeldeinformationen verwendet wurde, wenden Sie sich in Aktion 11 an den Benutzer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem Playbook „T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync“



7. Wenden Sie sich in Aktion 12 an den Anwender, um die geschäftliche Begründung zu validieren.
8. Wenn der Anwender in Aktion 13 eine stichhaltige geschäftliche Begründung angegeben hat, führen Sie die folgenden Aktionen aus:

   a. Dokumentieren Sie in Aktion 14 die bisherigen Ergebnisse.

   b. Initiieren Sie in Aktion 15 eine Überprüfung nach Incident.
   In Aktion 16 endet der Flow.

9. Wenn der Benutzer keine gültige geschäftliche Begründung angegeben hat, stellen Sie das System in Aktion 17 unter Quarantäne.
10. Entfernen Sie in Aktion 18 alle unerwünschten Dateien, die möglicherweise von den betrügerischen Konten erstellt oder gelöscht wurden.
11. In Aktion 19: Containment aufheben und Systeme wieder auf Betriebsstandard zurücksetzen.
12. Schließen Sie in Aktion 20 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für Okta-Anwenderanmeldung schlägt bei mehreren IPs fehl

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents für Anwenderanmeldungsfehler in Okta.

Das Playbook „Okta-Anwenderanmeldungsfehler bei mehreren IPs“ enthält Anweisungen zur Analyse der Warnung, wenn auf Okta ServiceNow-Kontofehler aufgrund mehrerer Nicht-ServiceNow-IPs erkannt werden. Die Warnung im Zusammenhang mit diesem Playbook überprüft die Okta-Protokolle. Löst eine Warnung aus, wenn innerhalb von 1 Stunde ein Anmeldefehler für ServiceNow-Anwender-IDs aus mehr als drei Nicht-ServiceNow-IP-Bereichen auftritt.

Richten Sie das Playbook „Okta-Anwenderanmeldungsfehler“ über das Playbook „Mehrere IPs“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler bei mehreren IPs“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

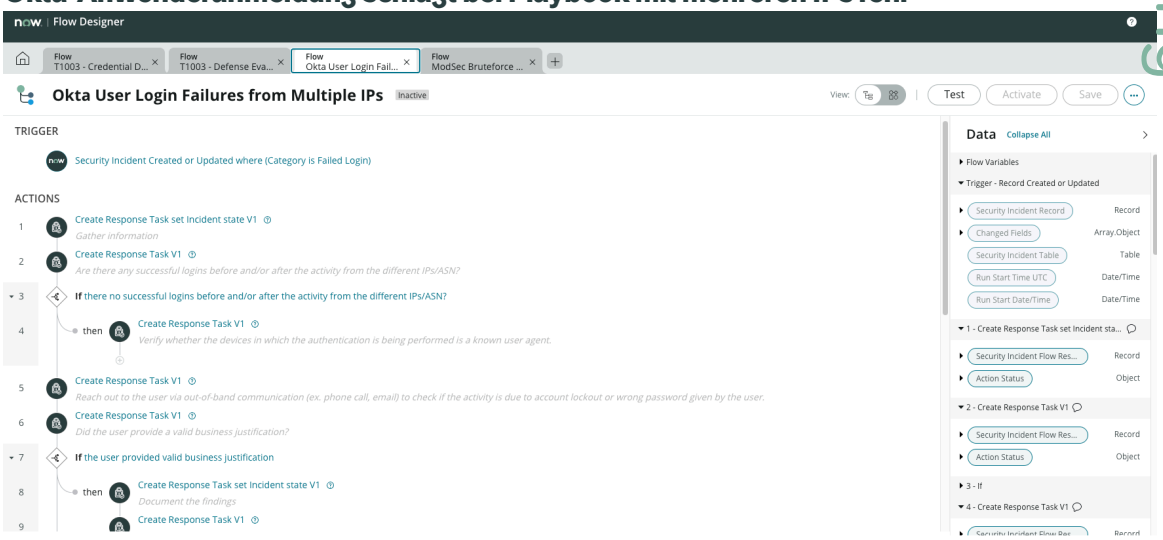
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Okta-Anwenderanmeldung fehlgeschlagen“ im Playbook „Mehrere IPs“ aus**.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „Okta-Anwenderanmeldungsfehler bei mehreren IPs“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol und dann **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

Okta-Anwenderanmeldung schlägt bei Playbook mit mehreren IPs fehl

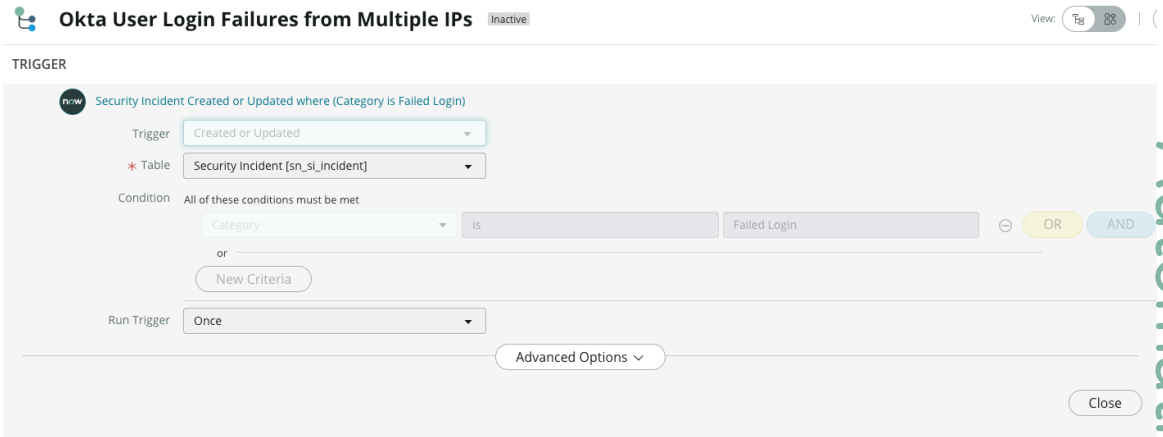


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **Kategorie„Fehlgeschlagene Anmeldung“**lautet.

Fehler bei der Okta-Anwenderanmeldung aufgrund der Playbook-Auslösebedingung für mehrere IPs



Verwenden Sie das Playbook „Okta-Anwenderanmeldungsfehler bei mehreren IPs“.

Verwenden Sie dieses Playbook, um Security Incidents für Anwenderanmeldungsfehler bei Okta zu untersuchen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Okta-Anwenderanmeldung – Fehler bei der Anmeldung mit mehreren IPs“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

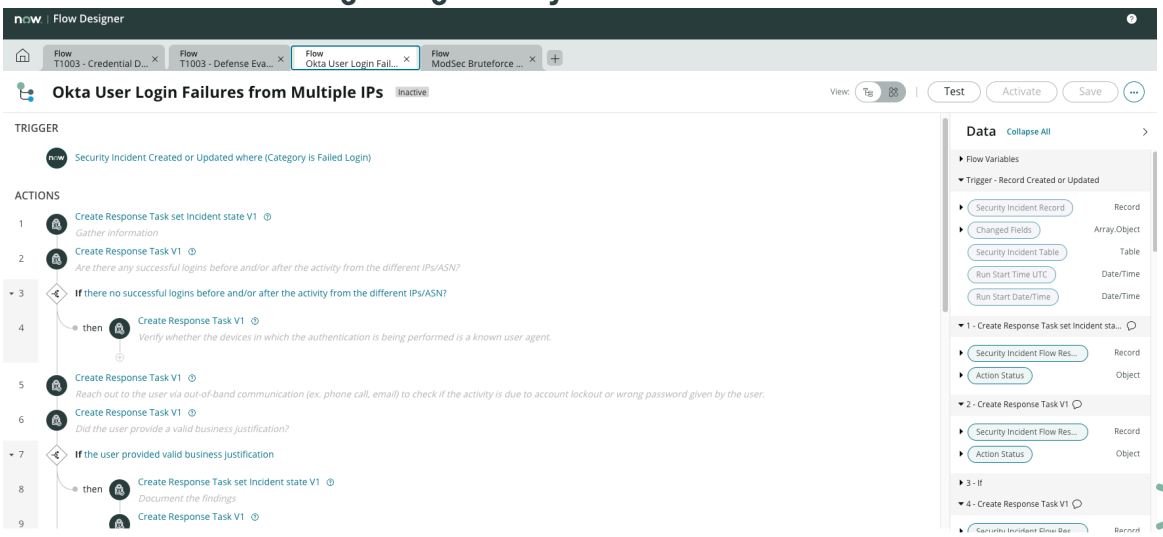
Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, führen Sie in Aktion 1 die folgenden Aufgaben aus:
   - Identifizieren Sie den Anwenderaccount, der als Ziel ausgewählt ist.
   - Verifizieren Sie das IP-Subnetz, und prüfen Sie, ob sie alle demselben Besitzer der autonomen Systemnummer (ASN) gehören.
2. Überprüfen Sie in Aktion 2, ob vor oder nach der Aktivität erfolgreiche Anmeldungen von den verschiedenen IPs/ASNs erfolgt sind.
3. Wenn in Aktion 3 vor oder nach der Aktivität keine erfolgreichen Anmeldungen von den verschiedenen IPs/ASNs stattgefunden haben, überprüfen Sie in Aktion 4, ob die Geräte, auf denen die Authentifizierung durchgeführt wird, bekannte Benutzeragenten sind.
   Wenn die Geräte von bekannten Benutzeragenten authentifiziert werden, wird der Flow beendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Okta-Anwenderanmeldung schlägt bei Playbook mit mehreren IPs fehl



4. Wenden Sie sich in Aktion 5 basierend auf der Untersuchung über Out-of-Band-Kommunikation (z. B. Telefonanruf oder E-Mail) an den Anwender, um zu überprüfen, ob die Aktivität auf eine Kontosperrung oder ein vom Anwender falsch angegebenes Passwort zurückzuführen ist.
5. Überprüfen Sie in Aktion 6, ob der Anwender eine gültige geschäftliche Begründung angegeben hat.
6. Wenn der Anwender in Aktion 7 eine stichhaltige geschäftliche Begründung angegeben hat, führen Sie die folgenden Aufgaben aus.

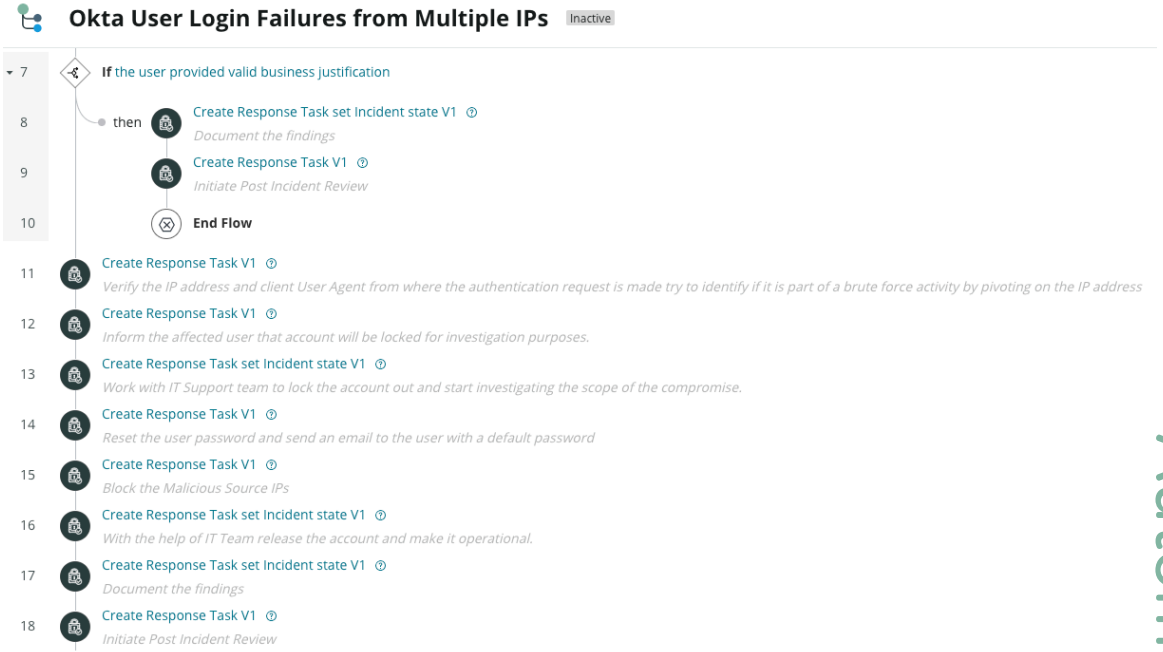
   a. Erstellen Sie in Aktion 8 eine Antwortaufgabe, um die bisherigen Ergebnisse zu dokumentieren.

   b. Erstellen Sie in Aktion 9 eine Antwort, um eine Überprüfung nach Incident zu initiieren.
   In Aktion 10 endet der Flow.

7. Überprüfen Sie in Aktion 11 die IP-Adresse und den Anwenderagenten des Clients, von dem die Authentifizierungsanforderung stammt, und versuchen Sie herauszufinden, ob sie Teil einer Brute-Force-Aktivität ist, indem Sie die IP-Adresse ändern.
8. In Aktion 12 informieren Sie den betroffenen Anwender darüber, dass der Account zu Untersuchungszwecken gesperrt wird.
   Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den betroffenen Anwender zu informieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Verwendung des Playbooks mit mehreren IPs schlägt die Anmeldung bei Okta-Anwendern fehl



9. Arbeiten Sie in Aktion 13 mit dem IT-Supportteam zusammen, um den Account zu sperren und mit der Untersuchung des Umfangs der Gefährdung zu beginnen.
10. Setzen Sie in Aktion 14 das Anwenderpasswort zurück, und senden Sie eine E-Mail mit dem Standardpasswort an den Anwender.
11. Blockieren Sie in Aktion 15 die schädlichen Quell-IPs.
12. Holen Sie in Aktion 16 Hilfe vom IT-Supportteam, um den Account freizugeben und die Betriebsstandards wiederherzustellen.
13. Dokumentieren Sie in Aktion 17 die bisherigen Ergebnisse.
14. Schließen Sie in Aktion 18 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für ModSec Brute-Force nach IP-Burst

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents mit Brute-Force-Versuchen auf den Anmeldeseiten mehrerer von ModSec erkannter IPs. Die Ereignisbedingungen können in der ModSec-Richtlinie selbst festgelegt werden und lösen eine Warnung bei Splunk aus, wenn das Ereignis bei ModSec erstellt wird.

Dieses Playbook hilft bei der Erkennung von abnormalem Datenverkehr auf der Anmeldeseite. In diesem Beispiel sollten zwei aufeinanderfolgende Bursts mit mehr als 50 Treffern/Minute von einer IP an die Anmeldeseite gesendet werden, was auf einen Brute-Force-Anmeldeversuch hinweist.

Richten Sie das Playbook „ModSec Brute-Force nach IP-Burst“ ein

Führen Sie die folgenden Schritte aus, um das ModSec Brute-Force by IP Burst-Playbook einzurichten.

Vorbereitungen
Erforderliche Rolle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_si.admin
- flow_designer

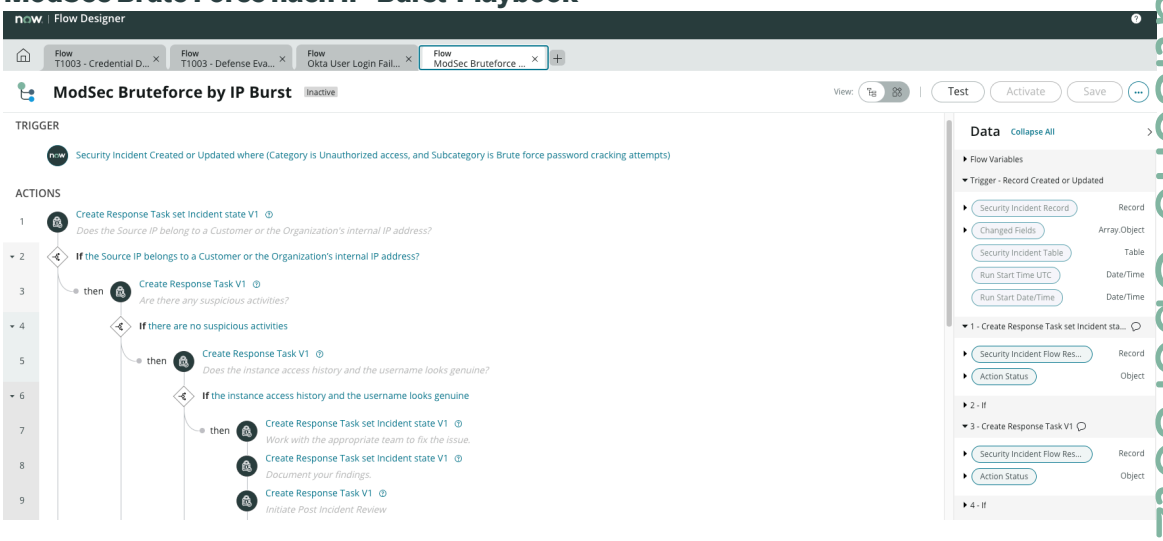
Stellen Sie sicher, dass Security Operations Spoke (*sn_sec_spoke*) installiert ist.

Prozedur

1. Melden Sie sich als -Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„ModSec Bruteforce by IP Burst“ (ModSec Bruteforce by IP-Burst)** aus.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „ModSec Bruteforce by IP Burst“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Flows des Playbooks zu erstellen, wählen Sie das Menüsymbol „Weitere Aktionen“ ( ) und anschließend **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen vornehmen möchten.

   ModSec Brute Force nach IP-Burst-Playbook

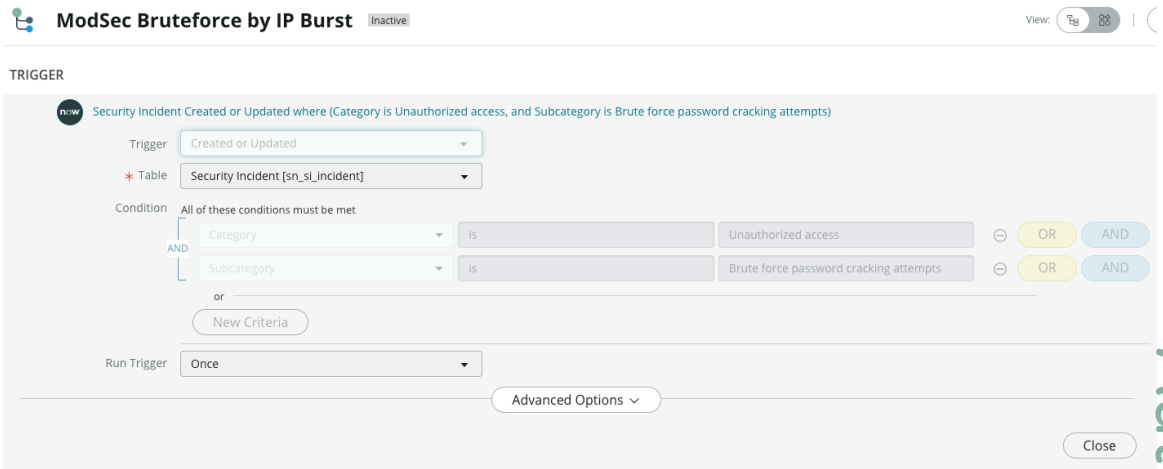
   

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie eine **Auslöserbedingung** für das Playbook fest.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kategorie** ist **„Nicht autorisierter Zugriff“**.
- **Unterkategorie** ist **Brute-Force-Angriffsversuche auf Passwörter**.

ModSec Brute-Force nach IP-Burst-Playbook-Auslösebedingung



Verwenden Sie das ModSec Brute Force by IP Burst Playbook

Verwenden Sie dieses Playbook, um Incidents von Brute-Force-Versuchen auf den Anmeldeseiten von mehreren von ModSec erkannten IPs zu untersuchen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook ModSec Brute-Force by IP Burst verfügbar sind.

Vorbereitungen

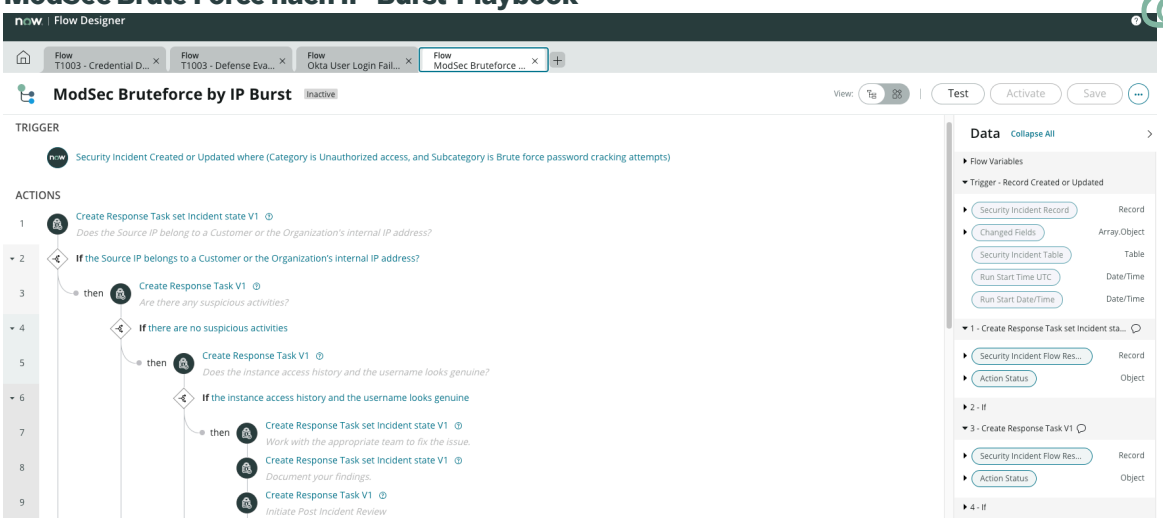
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und seine Ausführung beginnt, überprüfen Sie in Aktion 1, ob die Quell-IP zu einem Kunden oder zur internen IP-Adresse der Organisation gehört.
2. Wenn in Aktion 2 die Quell-IP zu einem Kunden oder zur internen IP-Adresse des Unternehmens gehört, führen Sie die folgenden Schritte aus:

ModSec Brute Force nach IP-Burst-Playbook



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Überprüfen Sie in Aktion 3, ob verdächtige Aktivitäten aufgetreten sind.

- Überprüfen Sie die Aktivität von der Quell-IP in den letzten Tagen. Wenn die IP vernachlässigbaren Datenverkehr aufwies, weist dies auf einen tatsächlichen Angriff hin.
- Überprüfen Sie die Anwendernamen der Anwender. Überprüfen Sie beispielsweise, ob die Anwendernamen in alphabetischer Reihenfolge angeordnet sind.
- Suchen Sie nach beteiligten generischen Accountnamen. Beispiele: admin, sysadmin, root, Administrator und andere Anwendungsaccountnamen.

Wenn keine verdächtigen Aktivitäten vorhanden sind, wird der Flow beendet.

b. Wenn in Aktion 4 verdächtige Aktivitäten vorlagen, überprüfen Sie in Aktion 5, ob der Instanzzugriffsverlauf und der Anwendername echt sind.

Überprüfen Sie die Protokolle *Appnode* auf Anzeichen für einen Fehler. Es könnten SAML-, SSO- oder LDAP-Fehlerereignisse auftreten, die auf ein Betriebsproblem zurückzuführen sein können.

Wenn der Instanzzugriffsverlauf und der Anwendername nicht Original aussehen, wird der Flow beendet.

c. Wenn in Aktion 6 der Instanzzugriffsverlauf und der Anwendername Original aussehen, führen Sie die folgenden Schritte aus:

i. Koordinieren Sie in Aktion 7 mit dem entsprechenden Team, um das Problem zu beheben.

ii. Dokumentieren Sie in Aktion 8 die bisherigen Ergebnisse.

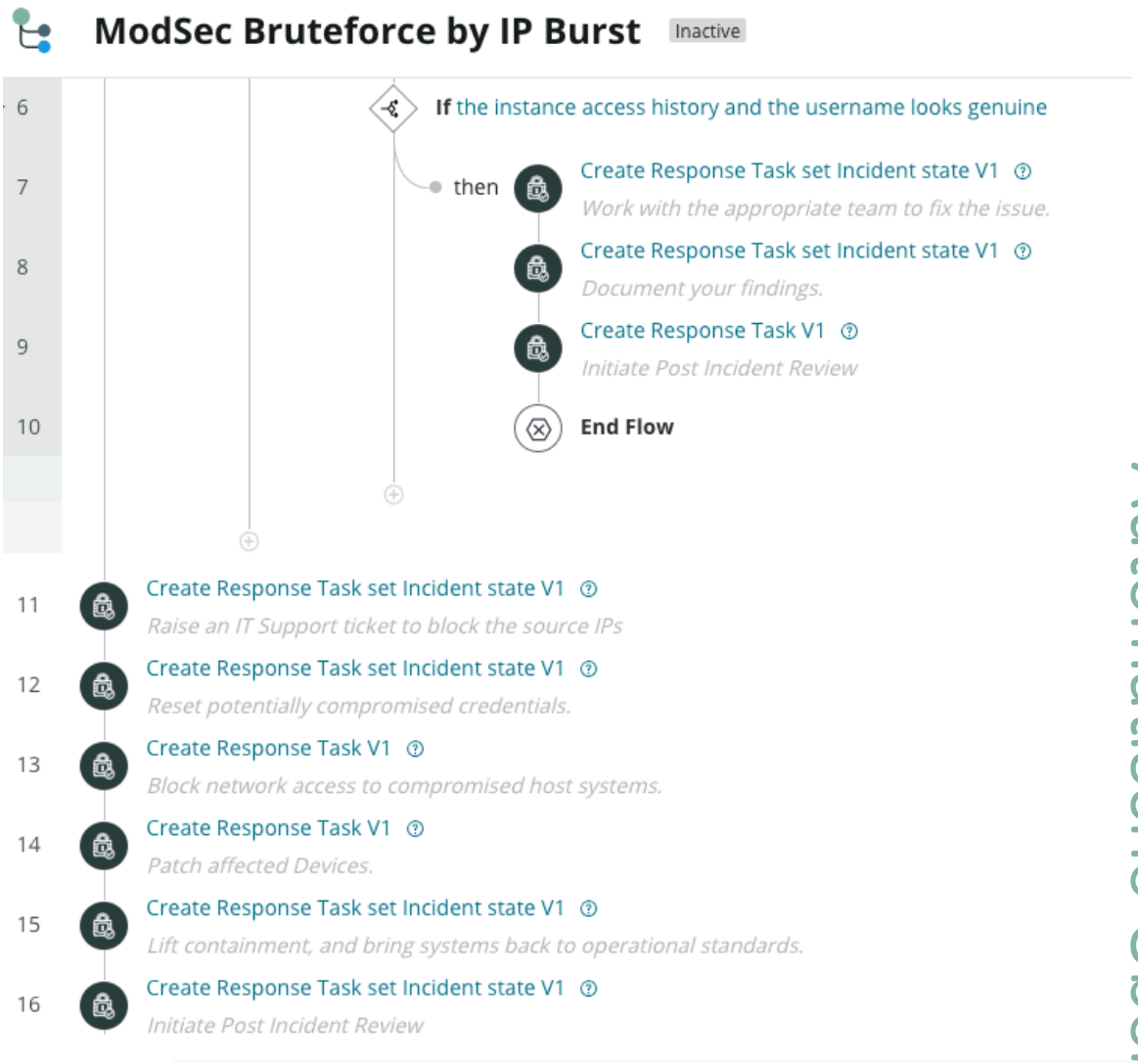
iii. Schließen Sie in Aktion 9 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

In Aktion 10 endet der Flow.

3. Wenn die Quell-IP nicht zu einem Kunden oder zur internen IP-Adresse des Unternehmens gehört, lösen Sie in Aktion 11 ein IT-Support-Ticket aus, um die Quell-IPs zu blockieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem Playbook „ModSec Brute Force by IP Burst“



4. Setzen Sie in Aktion 12 die potenziell gefährdeten Anmeldeinformationen zurück.
5. Blockieren Sie in Aktion 13 den Netzwerkzugriff auf gefährdete Hostsysteme.
6. Patchen Sie in Aktion 14 die betroffenen Geräte.
7. Heben Sie in Aktion 15 das Containment auf, und bringen Sie die Systeme wieder in den Betriebsstandard.
8. Schließen Sie in Aktion 16 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook-Aktionen für Security Incident Response

In diesem Abschnitt werden die in der Flow Designer-Aktionsbibliothek bereitgestellten Aktionen beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
Fügen Sie dem Security Incident ein Sicherheits-Tag hinzu	Diese Aktion verwenden, um automatisch ein Sicherheits-Tag mithilfe der Flow Designer-Logik hinzuzufügen.	Wenn der Flow ein IoC erkennt, kann mit dieser Aktion automatisch das Tag **IoC erkannt** hinzugefügt werden. **Flow**:	• Eingabe: Security Incident, Sicherheits-Tag • Ausgabe: nicht zutreffend
Fügen Sie dem Security Incident erkennbare Elemente hinzu	Diese Aktion verwenden, um einem ausgewählten Security Incident erkennbare Elemente hinzuzufügen. • Standardmäßig wird die Liste der erkennbaren Elemente durch Kommas (,) getrennt, dies kann jedoch geändert werden. Sie können ein anderes einzelnes Sonderzeichen als Trennzeichen angeben. Beim Hinzufügen von erkennbaren Elementen wird der Typ (URL, IP-Adresse, Hash) automatisch festgelegt. • Wenn die erkennbaren Elemente dem Security Incident hinzugefügt werden, wird der Typ (URL, IP-Adresse, Hash) automatisch festgelegt. • Wenn die erkennbaren Elemente hinzugefügt werden, identifiziert die Option „Erkennbare Elemente der zulässigen Liste		• Eingabe: ◦ Security Incident ◦ Erkennbare Elemente ◦ Trennzeichen ◦ Erkennbare Elemente der zulässigen Liste filtern und Aktivitätsnotiz veröffentlichen • Ausgabe: nicht zutreffend

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
	filtern“ die erkennbaren Elemente der zulässigen Liste und fügt sie nicht der zugehörigen Liste der erkennbaren Elemente des Security Incidents hinzu. Eine automatisierte Systemaktivität (Antwort) wird hinzugefügt, um anzuzeigen, dass diese erkennbaren Elemente entfernt wurden.		
Betroffene Anwender (Zugehörige Listen) aus mehreren Security Incidents abrufen V1	Ruft alle betroffenen Anwender ab, die in der zugehörigen Liste „Betroffene Anwender“ für die angegebenen Security Incidents aufgeführt sind.	Sie können übergeordnete Security Incidents mit mehreren untergeordneten Security Incidents haben. Diese Aktion verwenden, um für betroffene Anwender ein Rollup von allen untergeordneten Security Incidents zu den entsprechenden übergeordneten Security Incidents durchzuführen. Nur eindeutig betroffene Anwender werden zusammengefasst, und alle Duplikate werden eliminiert.	• Eingabe: Security Incidents • Ausgabe: ◦ Betroffener Anwender ◦ count
Rufen Sie betroffene Anwender von mehreren Security Incidents ab	Ruft den primären betroffenen Anwender für den angegebenen Security Incident ab. Die betroffenen Benutzer aus der zugehörigen Liste Betroffene Benutzer sind nicht enthalten.	• Senden Sie bei der Untersuchung eines Phishing-Security Incident eine E-Mail an die primär betroffenen Anwender (die den Phishing-Incident gemeldet haben), um zu bestätigen, ob einer der Anwender auf die schädlichen Links in der Phishing-E-Mail geklickt hat.	• Eingabe: Security Incidents • Ausgabe: ◦ Betroffene Anwender ◦ count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
		• Aktualisieren Sie den Schweregrad oder die Risikopunktzahl des übergeordneten Security Incident basierend auf der Anzahl der primär betroffenen Anwender.	
Rufen Sie betroffene Anwender (zugehörige Liste) aus einem Security Incident ab	Ruft alle betroffenen Anwender ab, die in der zugehörigen Liste „Betroffene Anwender“ für einen angegebenen Security Incident aufgeführt sind.		• Eingabe: Security Incidents • Ausgabe: ◦ Betroffene Anwender ◦ count
Fügen Sie dem Security Incident betroffene Anwender hinzu	Fügt alle betroffenen Anwender zu einem Security Incident hinzu.	Angenommen, Sie haben einen übergeordneten Security Incident mit mehreren untergeordneten Security Incidents. Sie können diese Aktion verwenden, um ein Rollup betroffener Anwender aus allen untergeordneten Security Incidents zum entsprechenden übergeordneten Security Incident durchzuführen. Nur eindeutig betroffene Anwender werden zusammengefasst, und alle Duplikate werden eliminiert.	• Eingabe: ◦ Security Incident ◦ user • Ausgabe: nicht zutreffend
Konfigurationselemente der betroffenen Anwender abrufen	Ruft die Configuration Items (CIs) aller betroffenen Anwender ab.	In Phishing- oder Malware-Szenarien können Sie mit dieser Aktion die zugehörige Liste „Betroffene Configuration Items (CI)“ aktualisieren und die CIs untersuchen. Anschließend können Sie den Schweregrad oder die Risikopunktzahl des Security Incidents basierend auf der Anzahl	• Eingabe: users • Ausgabe: ◦ Konfigurationselemente ◦ count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
		der identifizierten CIs aktualisieren.	
Ruft alle untergeordneten Security Incidents für einen Security Incident ab	Ruft alle untergeordneten Security Incidents ab, die sich auf einen bestimmten übergeordneten Security Incident beziehen.	Beispielszenario: Verwenden Sie diese Aktion für Folgendes: • Aktualisieren Sie den Status der untergeordneten Security Incidents, wenn der Status der entsprechenden übergeordneten Security Incidents aktualisiert wird. • Aktualisiert den Schweregrad oder die Risikopunktzahl des Security Incident automatisch basierend auf der Anzahl der untergeordneten Security Incidents.	• Eingabe: ◦ Security Incident ◦ Incident-Status • Ausgabe: ◦ Security Incident untergeordnet ist ◦ count
Konfigurationselemente für die erkennbaren Elemente abrufen (IP-Adresse eingeben)	Ruft alle Configuration Items (CIs) für erkennbare Elemente vom Typ IP-Adresse ab.	Eine erkennbare IP-Adresse kann einem Konfigurationselement zugeordnet werden. Zum Beispiel die IP-Adresse eines Servers. Wenn Sie diese Aktion verwenden, können Sie Informationen für den Server abrufen.	• Eingabe: IP-Adresse des erkennbaren Elements • Ausgabe: ◦ Konfigurationselemente ◦ count
Ist erkennbares Element schädlich	Bestätigt das Vorhandensein eines oder mehrerer schädlicher erkennbarer Elemente in einer Reihe von erkennbaren Elementen.	Nachdem die Bedrohungssuche abgeschlossen wurde und Sie das Vorhandensein schädlicher erkennbarer Elemente identifiziert haben, können Sie den Schweregrad oder die Risikopunktzahl eines Security Incident erhöhen.	• Eingabe: Security Incident • Ausgabe: schädlich (wahr/falsch)
Senden Sie eine E-Mail, um die Anwenderinteraktion zu bestätigen	Sendet eine E-Mail als Antwort auf eine Benutzerantwort.	Wenn ein Benutzer mehrmals versucht, sich bei einer Anwendung anzumelden, und dies fehlschlägt, führt dies zu	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
		einem Anmeldeszenario mit einem Fehler. In diesem Fall wird eine E-Mail an den Benutzer gesendet, um zu bestätigen, ob er versucht hat, sich anzumelden. Je nach Benutzerantwort (Ja oder Nein) können unterschiedliche Aktionen ausgeführt werden. **Flow**: Fehler bei der Anmeldung Manuelles Playbook	
Erkennbare Elemente der zulässigen Liste herausfiltern	Diese Aktion verwenden, um erkennbare Elemente aus einer bestimmten Gruppe von erkennbaren Elementen aufzulisten.	Sie können bestimmte erkennbare Elemente identifizieren, die aus einer Reihe von erkennbaren Elementen ignoriert werden können. Diese erkennbaren Elemente werden bei der Lösung des Security Incidents nicht berücksichtigt.	• Eingabe: Security Incident • Ausgabe: ◦ zulässige Liste erkennbarer Elemente ◦ count
Setzen Sie das Passwort für betroffene Anwender zurück	Diese Aktion verwenden, um das Passwort für betroffene Anwender zurückzusetzen.	Wenn ein Benutzeraccount kompromittiert wurde oder ein Benutzer die Zurücksetzung des Passworts anfordert, wird eine E-Mail an den Benutzer gesendet, um das Passwort zurückzusetzen. **Flow**: Fehler bei der Anmeldung Manuelles Playbook.	
Ruft die Anwendergruppe für den betroffenen Anwender ab	Ruft die Anwendergruppendetails der betroffenen Anwender ab.	Wenn in einer Organisation zwei oder mehr Anwender Phishing-E-Mails melden, können Sie herausfinden, welcher Gruppe sie angehören, und feststellen, ob weitere Anwender betroffen sind	• Eingabe: user • Ausgabe: ◦ Anwendergruppen ◦ count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichterstellung mit Security Incident Response

Sicherheitsmanager können Problembereiche mithilfe allgemeiner grafischer Schnittstellen identifizieren.

Greifen Sie auf den Security Incident Response-Explorer zu

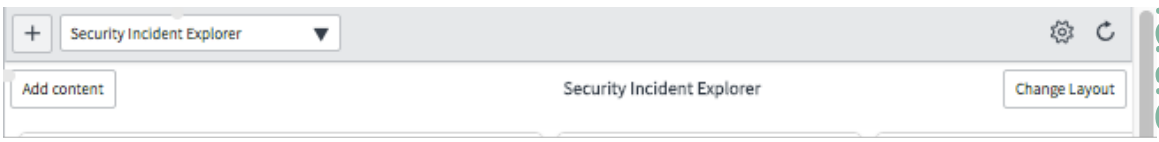
Sie können auf das Security Incident Response Explorer-Dashboard zugreifen, um die Aktivität von Security Incidents anzuzeigen, Problembereiche sofort zu erkennen und Probleme schnell zu lösen.

Vorbereitungen
Erforderliche Rollen:

- sn_si.admin (zum Schreiben)
- sn_si_basic (zum Lesen)

Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Homepage** oder navigieren Sie zu **Selfservice** > **Dashboards**.
2. Wählen Sie in der Berichtsliste Security Incident Explorer aus.

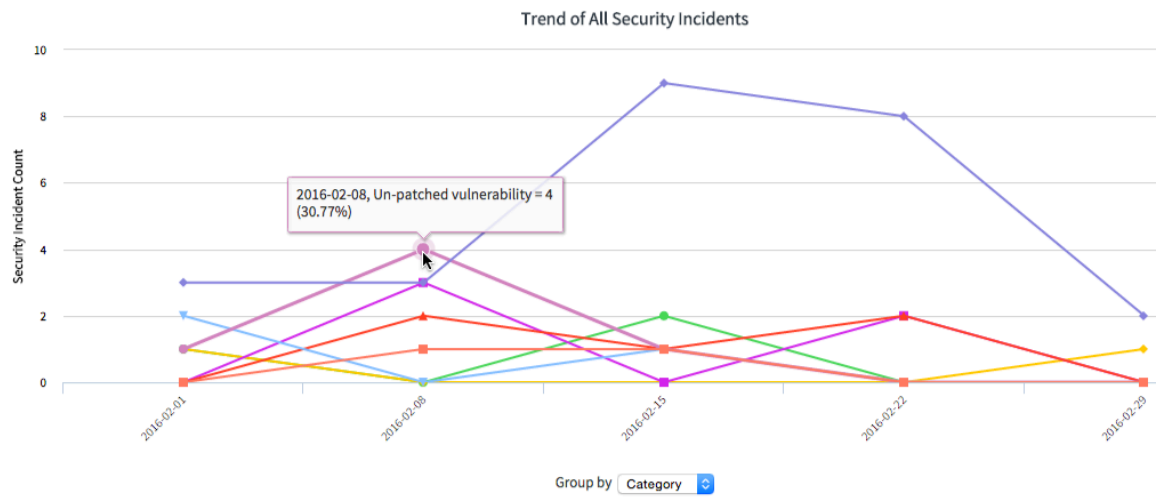


Security Incident Response Übersicht

Die Übersicht Security Incident Response bietet eine leitende Ansicht der Aktivität von Security Incidents und liefert Trends, Berichte und Drilldowns zu bestimmten Daten.

Das Modul „Übersicht“ zeigt Informationen zu Security Incidents an, die auf die Rolle des Benutzers zugeschnitten sind. Sie können auf einen beliebigen Teil eines Diagramms zeigen (Balken, Kreis, Datenpunkt, Heatmap usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Siehe folgende Abbildung. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Trend aller Security Incidents



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsvorfallmanager – Übersicht

Benutzer mit den Rollen „Security Incident-Administrator“ und „Security Incident Manager“ zeigen die Security Incident Manager-Übersicht an. Sie enthält die folgenden Berichte im Basissystem.

Security Incident Manager-Übersichtsberichte

Name	Visuell	Beschreibung
Team Security Incidents mit Priorität „Kritisch“	Einzelne Punktzahl	Anzahl der dem Team zugewiesenen kritischen Security Incidents.
Team Security Incidents mit Priorität „Hoch“	Einzelne Punktzahl	Anzahl der dem Team zugewiesenen Incidents mit hoher Sicherheit.
In 24 Stunden ablaufende SLAs	Einzelne Punktzahl	Die Anzahl der SLAs, die innerhalb der nächsten 24 Stunden ablaufen.
Risiko vs. Schweregrad	Heatmap	Die Verteilung der dem Team zugewiesenen Security Incidents nach Risiko und Schweregrad.
Security Incidents nach CI-Klasse, letzte 3 Monate	Balkendiagramm	Anzahl der Security Incidents, die dem Team nach Configuration Item-Klasse zugewiesen sind.
Trend aller Security Incidents	Trenddiagramm	Stellt die Anzahl der empfangenen Security Incidents nach Kategorie oder Priorität dar.
Security Incidents mit nicht autorisiertem Zugriff	Balkendiagramm	Zeigt die Typen der Security Incident-Kategorien an, die im Laufe der Zeit empfangen wurden.
Durchschnittliche Zeit bis zur Eindämmung	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle kritischen Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Identität	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle Security Incidents zu identifizieren

Sicherheitsanalyst – Übersicht

Benutzer mit der Rolle „Security Incident Analyst“ rufen die Sicherheitsanalystenübersicht auf. Sie enthält die folgenden Berichte im Basissystem.

Übersichtsberichte für Sicherheitsanalysten

Name	Visuell	Beschreibung
Meine Arbeit mit kritischer Priorität	Einzelne Punktzahl	Anzahl der mir zugewiesenen kritischen Security Incidents.
Meine Arbeit mit hoher Priorität	Einzelne Punktzahl	Anzahl der mir zugewiesenen Incidents mit hohem Sicherheitsstatus.
Meine in 24 Stunden ablaufenden SLAs	Einzelne Punktzahl	Anzahl der mir zugewiesenen SLAs, die innerhalb der nächsten 24 Stunden ablaufen.
Mir zugewiesene Security Incidents	Balkendiagramm	Mir zugewiesene Security Incidents nach Incident-Status oder Kategorie.
Mir zugewiesene Arbeit nach Typ	Balkendiagramm	Mir zugewiesene Sicherheitsaufgaben (Incidents, Aufgaben oder Anforderungen) nach Typ oder Priorität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichtsberichte für Sicherheitsanalysten (Fortsetzung)

Name	Visuell	Beschreibung
Mir zugewiesene Security Incidents, Anforderungen, Aufgaben	Liste	Eine Liste aller mir zugewiesenen Security Incidents, Sicherheitsanforderungen und Aufgaben.
Ort des Security Incidents	Karte	Regionaler Standort der Security Incidents.
Anzahl	Karte	Anzahl der Security Incidents pro Region.
Min./Max. Anzahl	Farbspektrum-Balken	Die minimale und maximale Anzahl von Security Incidents pro Region, dargestellt durch einen Farbraumbalken.
Prozentsatz der Anzahl	Karte	Prozentsatz der Gesamtzahl der Incidents pro Region.

CISO-Übersicht über Security Incidents bei aktivierter Analyse von Security Incidents

Wenn das Plugin Security Incident Analytics aktiviert ist, können Benutzer mit den Rollen „Security Incident CISO“ und „Systemadministrator“ die Security Incident CISO-Übersicht anzeigen. Die folgenden CISO-Berichte werden im Basissystem bereitgestellt.

CISO-Übersichtsberichte für Security Incidents (mit aktivierten Analytics für Security Incidents)

Name	Visuell	Beschreibung
Neue Security Incidents diese Woche	Einzelne Punktzahl	Anzahl der neuen Security Incidents, die in der aktuellen Woche empfangen wurden.
Diese Woche geschlossene Security Incidents	Einzelne Punktzahl	Anzahl der in der aktuellen Woche geschlossenen Security Incidents.
Neue Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Anzahl der Security Incidents, die in den letzten 7 Tagen geöffnet wurden.
Geschlossene Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Anzahl der Security Incidents, die innerhalb der letzten 7 Tage geschlossen wurden.
Tägliche neue Security Incidents im Vergleich zu geschlossenen Security Incidents	Trenddiagramm	Anzahl neuer und geschlossener Security Incidents im Zeitverlauf nach Tag.
Wöchentliche neue Security Incidents im Vergleich zu geschlossenen Security Incidents	Trenddiagramm	Neue und geschlossene Security Incidents im Zeitverlauf nach Woche.
Lösungscode für Security Incident	Trenddiagramm	Vollständige Anzahl der Abschlusscodes im Zeitverlauf.
Security Incident – Geschäftsauswirkung	Verzeichnisübersicht	Business-Services mit Security Incidents mit verfügbaren Gruppierungen nach Geschäftsrelevanz.
Durchschnittliche Zeit bis Eindämmung (wöchentlich)	Trenddiagramm	Die durchschnittliche Zeit von 7 Tagen, die benötigt wird, um einen Security Incident im Laufe der Zeit einzudämmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CISO-Übersichtsberichte für Security Incidents (mit aktivierten Analytics für Security Incidents) (Fortsetzung)

Name	Visuell	Beschreibung
Durchschnittliche Zeit bis Beseitigung (wöchentlich)	Trenddiagramm	Die durchschnittliche Zeit von 7 Tagen, die benötigt wird, um einen Security Incident im Laufe der Zeit zu beseitigen.
Durchschnittliche Zeit bis Identifizierung (wöchentlich)	Trenddiagramm	Die durchschnittliche 7-Tage-Zeit, die benötigt wird, um einen Security Incident im Laufe der Zeit zu identifizieren.
Ort des Security Incidents	Karte	Regionaler Standort der Security Incidents.
Anzahl	Karte	Anzahl der Security Incidents pro Region.
Min./Max. Anzahl	Farbspektrum-Balken	Die minimale und maximale Anzahl von Security Incidents pro Region, dargestellt durch einen Farbraumbalken.
Prozentsatz der Anzahl	Karte	Prozentsatz der Gesamtzahl der Incidents pro Region.

CISO-Übersicht über Security Incidents ohne aktivierte Security Incident Analytics

Wenn das Plugin Security Incident Analytics nicht aktiviert ist, können Benutzer mit den Rollen „Security Incident CISO“ und „Systemadministrator“ die Übersicht über das Security Incident CISO-Reporting anzeigen. Die folgenden CISO-Berichte werden im Basissystem bereitgestellt.

CISO-Übersichtsberichte zu Security Incidents (ohne aktivierte Security Incident Analytics)

Name	Visuell	Beschreibung
Neue Security Incidents diese Woche	Einzelne Punktzahl	Anzahl der neuen Security Incidents, die in der aktuellen Woche geöffnet wurden.
Diese Woche geschlossene Security Incidents	Einzelne Punktzahl	Anzahl der in der aktuellen Woche geschlossenen Security Incidents.
Neue Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Anzahl der Security Incidents, die in den letzten 7 Tagen geöffnet wurden.
Geschlossene Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Anzahl der Security Incidents, die innerhalb der letzten 7 Tage geschlossen wurden.
Wöchentliche neue Security Incidents	Trenddiagramm	Die neuen Security Incidents, die wöchentlich geöffnet werden.
Wöchentliche geschlossene Security Incidents	Trenddiagramm	Die Security Incidents werden wöchentlich geschlossen.
Lösungscodes für Security Incident	Trenddiagramm	Abschlusscodes für Security Incidents im Zeitverlauf.
Business Services mit Sicherheitsvorfällen – Geschäftsauswirkung	Verzeichnisübersicht	Business-Services mit Security Incidents mit verfügbaren Gruppierungen nach Geschäftsrelevanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CISO-Übersichtsberichte zu Security Incidents (ohne aktivierte Security Incident Analytics) (Fortsetzung)

Name	Visuell	Beschreibung
Durchschnittliche Zeit bis zur Eindämmung	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle kritischen Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Identität	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle Security Incidents zu identifizieren

Hinweis:
Das -Basissystem Security Incident Response enthält Performance Analytics-Lösungen zum Anzeigen vorkonfigurierter Best Practice-Dashboards. Die Dashboards enthalten wichtige Metriken für die Analyse Ihres Prozesses in Security Incident Response, z. B. neue Sicherheitsvorfälle oder das durchschnittliche Alter offener Sicherheitsvorfälle. Weitere Informationen und Installationsanweisungen finden Sie unter Security Incident Response Platform Analytics-Lösungen.

Zuordnung des Security Incidents

Die Security Incident-Karte enthält Daten nach geografischem Standort. Jeder Bereich, in dem ein Incident auftritt, wird auf der Weltkarte hervorgehoben. Wenn das Plugin Security Incident Analytics „ aktiviert ist, können Sie die Security Incident-Zuordnung der Übersicht Security Incident Response hinzufügen. Nachdem es hinzugefügt wurde, können Sie die Zuordnung konfigurieren, indem Sie die Zuordnungsfilter ändern.

Zuordnung zur Übersicht Security Incident Response hinzufügen

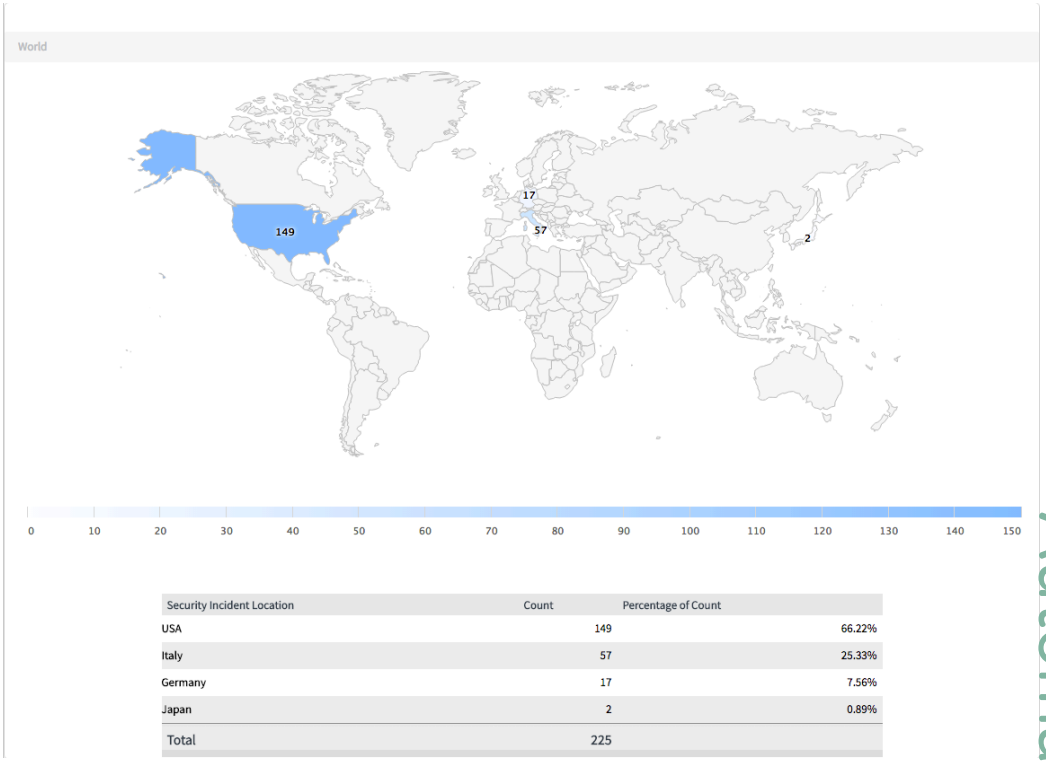
Sie können die Zuordnung der Übersicht Security Incident Response hinzufügen, um Daten zu Security Incidents nach geografischem Standort anzuzeigen. Mit einer Zuordnung können Sie Detailinformationen zu Security Incidents nach Standort anzeigen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Übersicht**.
2. Klicken Sie oben links auf der Seite **auf Inhalt hinzufügen,** um das Steuerelement für die Widget-Auswahl zu öffnen.
3. Klicken Sie im ersten Auswahlfeld auf **Berichte**.
4. Klicken Sie im zweiten Auswahlfeld auf **Security Incident**.
5. Klicken Sie im dritten Auswahlfeld auf **Security Incident Map**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. Klicken Sie unten auf dem Bildschirm auf die Stelle im Bildschirm, die Sie dem Bericht hinzufügen möchten.
7. Schließen Sie das Feld **Inhalt hinzufügen**.

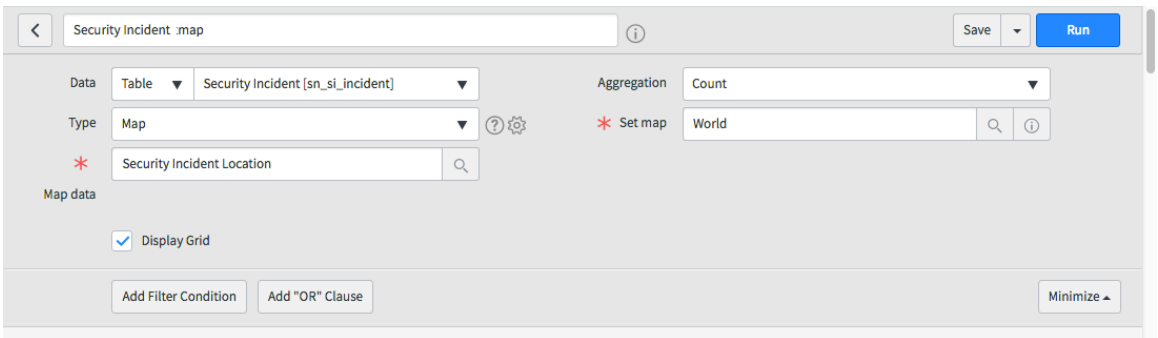
Ändern Sie die Security Incident-Zuordnung

Administratoren in der globalen Domäne können mithilfe von Filtern ändern, wie die Security Incident-Zuordnung Security Incidents behandelt.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Berichte** > **Administration** > **Alle**.
2. Suche nach **Security Incident-Zuordnung**.
3. Klicken Sie auf **Bericht bearbeiten**.



4. Klicken Sie auf **Filterbedingung hinzufügen,** um Filter hinzuzufügen oder zu bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Ausführen**, um die angewendeten Änderungen anzuzeigen.
6. Klicken Sie auf **Speichern**.

Verzeichnisübersichten zu Security Incidents

Wenn das Plugin Security Incident Analytics aktiviert ist, können Sie die Echtzeit-Treemaps „Security Incident – Serviceauswirkung“ und „Security Incident – Echtzeit“ der Übersicht Security Incident Response hinzufügen. Nachdem sie hinzugefügt wurden, können Sie die Verzeichnisübersichten konfigurieren, indem Sie die Verzeichnisübersichtskategorien und -indikatoren ändern.

Fügen Sie der Übersicht über Security Incident Response Treemaps hinzu

Treemaps zeigen hierarchische Daten (baumstrukturierte Daten) als Satz verschachtelter Rechtecke an. Jede Verzweigung der Struktur erhält ein Rechteck, das dann mit kleineren Rechtecken gekachelt wird, die Unterverzweigungen darstellen. Mit Verzeichnisübersichten können Sie Informationen zu Security Incidents auf dynamische und ansprechende Weise anzeigen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

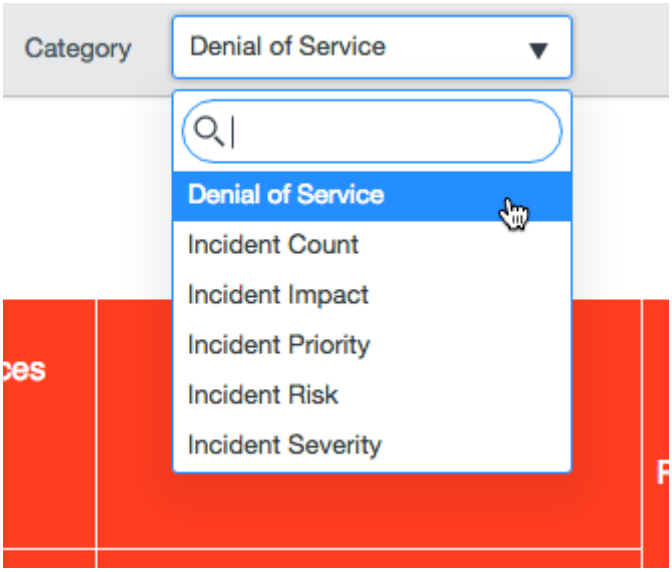
1. Navigieren zu **Alle** > **Security Incident** > **Übersicht**.
2. Klicken Sie oben links auf der Seite **auf Inhalt hinzufügen,** um das Steuerelement für die Widget-Auswahl zu öffnen.
3. Klicken Sie im ersten Auswahlfeld auf **Verzeichnisübersicht**.
4. Wählen Sie im zweiten Auswahlfeld die Verzeichnisübersicht, die Sie einfügen möchten, aus der folgenden Liste aus:
   - Security Incident – Serviceauswirkung
   - Security Incident – Echtzeit
   - Security Incident – Geschäftsauswirkung
   - Bedeutung der Schwachstelle

   Hinweis:
   Die Geschäftsauswirkungs-Treemap wird standardmäßig auf der Homepage Security Incident Response angezeigt. Für die Serviceauswirkungs- und Echtzeit-Treemaps muss das Plugin „Security Incident Analytics“ aktiviert sein.

5. Wählen Sie im dritten Auswahlfeld den Granularitätsgrad der Informationen aus, die Sie für die ausgewählte Verzeichnisübersicht abrufen möchten.

   Hinweis:
   Wählen Sie für die Treemap „Security Incident – Service Impact“ im dritten Auswahlfeld **Security Incident** aus. Diese Auswahl stellt eine Dropdown-Liste mit mehreren Datenkategorien bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie unten auf dem Bildschirm auf die Stelle auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
7. Schließen Sie das Feld **Inhalt hinzufügen**.

Erstellen oder aktualisieren Sie eine Verzeichnisübersichtskategorie

Sie können die vordefinierten Kategorien für die Security Incident-Treemaps ändern oder bei Bedarf Kategorien neu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Die Verzeichnisübersichten verwenden Performance Analytics als Datenquelle. Das Performance Analytics-Modul erfordert ein separates Plugin.

Warum und wann dieser Vorgang ausgeführt wird

Im Basissystem sind Verzeichnisübersichtskategorien wie Incident-Risiko, Denial of Service und Incident-Schweregrad enthalten. Sie können diese Kategorien ändern oder nach Bedarf weitere Kategorien definieren.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration**, und öffnen Sie die Verzeichnisübersichts-Definition, für die Sie Kategorien konfigurieren möchten:
   - **Servicerelevanz-Reportingdefinition**
   - **Echtzeitdefinition**
2. **Wahlweise:** Ändern Sie den Namen der Treemap-Definition.
   Im Basissystem lautet der Standardname für die Treemap-Definition für die Serviceauswirkung **Security Incident**. Der Standardname für die Echtzeit-Treemap-Definition lautet **Security Incident – Echtzeit**.
3. Ändern Sie den Wert der **PA-Indikatorgruppe** nicht, es sei denn, Sie verwenden eine anwenderdefinierte Verzeichnisübersicht.
4. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um die Verzeichnisübersichtsdefinition zu deaktivieren.
   Wenn Sie beispielsweise die Kategorie „Denial of Service“ im Dashboard für die Systemauswirkungen deaktivieren, ist diese Verzeichnisübersichts-Kategorie nicht verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie in der zugehörigen Liste **„Treemap-Kategorien“** eine Kategorie aus, die Sie ändern möchten, oder klicken Sie auf **Neu**, um eine neue Kategorie zu erstellen.
6. Füllen Sie die Felder aus.

Formular „Kategorie der Verzeichnisübersicht“.

Feld	Beschreibung
Name	Der Name, der für die Kategorie in der Liste **Kategorien** über der Verzeichnisübersicht angezeigt wird.
Bestellung	Die Reihenfolge, in der die Kategorie in der Liste **Kategorien** über der Verzeichnisübersicht angezeigt wird.
Verzeichnisübersicht	Der Name der Verzeichnisübersicht, die diese Kategorie verwendet.
Farbe	Die Farbe, die für diese Kategorie in der Verzeichnisübersicht angezeigt wird.
Aktiv	Auswählen, um diese Kategorie zu aktivieren.
Beschreibung	Eine Beschreibung der Kategorie.
Für alle Rollen sichtbar	Wählen Sie diese Option aus, um diese Kategorie für alle Anwender unabhängig von ihrer Rolle sichtbar zu machen.
Rollen	Wenn Sie das Kontrollkästchen **Für alle Rollen sichtbar** nicht aktiviert haben, wählen Sie die Rollen aus, die diese Kategorie anzeigen können.

7. Klicken Sie auf **Absenden** oder **Aktualisieren**.

Erstellen oder aktualisieren Sie einen Verzeichnisübersichts-Indikator

Sie können die vordefinierten Indikatoren für eine Verzeichnisübersichtskategorie ändern oder neue Indikatoren erstellen. Für jeden Indikator können Sie die zugehörige Datenquelle konfigurieren und angeben, wie Listen von Security Incidents in Verzeichnisübersichten geöffnet werden, die mit dem Indikator angezeigt werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Die Verzeichnisübersichten verwenden Performance Analytics als Datenquelle. Das Performance Analytics-Modul erfordert ein separates Plugin.

Prozedur

1. Öffnen Sie die Verzeichnisübersichts-Definition, für die Sie Indikatoren konfigurieren möchten.
2. Wählen Sie in der zugehörigen Liste **Treemap-Kategorien** die Kategorie aus, für die Sie Indikatoren konfigurieren möchten.
3. Wählen Sie in der zugehörigen Liste **„Treemap-Indikatoren“** einen Indikator aus, den Sie ändern möchten, oder klicken Sie auf **Neu,** um einen neuen Indikator zu erstellen.
4. Füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Treemap-Indikator“.

Feld	Beschreibung
Name	Der Name, der für den Indikator in der Liste **„Indikatoren“** im Serviceeinfluss-Dashboard angezeigt wird.
Kurzbeschreibung	Eine Beschreibung, die für den Indikator in der Liste **„Indikatoren** “ oberhalb der Verzeichnisübersicht angezeigt wird.
Ergebnisgrenzwert	Die maximal zulässige Anzahl von Ergebnissen. Die Obergrenze ist 100.
Ergebnispräzision	Die Anzahl der Stellen, die nach dem Dezimalkomma angezeigt werden sollen. Dieses Feld wird nur für die Echtzeit-Treemap-Definition angezeigt.
Aktiv	Aktivieren Sie die Checkbox, um diesen Indikator zu aktivieren.
Kategorie	Der im vorherigen Bildschirm eingegebene Kategoriename.
Richtung	Gibt an, ob die Kachel in der Verzeichnisübersicht minimiert oder maximiert ist. Dieses Feld wird nur für die Echtzeit-Treemap-Definition angezeigt.
Einheit	Die für die Metrik zu verwendende Maßeinheit. Dieses Feld wird nur für die Echtzeitdefinition angezeigt.
Automatisches Aktualisierungsintervall	Wie häufig die Verzeichnisübersicht aktualisiert werden soll.
Bestellung	Die Reihenfolge, in der der Indikator in der Liste **der Indikatoren** über der Verzeichnisübersicht angezeigt wird.

5. Klicken Sie auf die Registerkarte **Datenquellenkonfiguration**, und konfigurieren Sie eine der folgenden Datenquellenoptionen für den Indikator.

6. Klicken Sie auf die Registerkarte **Click-Through**, und geben Sie an, wie Listen mit Security Incidents in der Verzeichnisübersicht geöffnet werden.
   a. Wählen Sie im Feld **Navigationstyp der Klickaktion-URL** aus, ob die Liste der Security Incidents in einem neuen Fenster, im selben Fenster oder in einem Dialogfeld geöffnet werden soll.
   b. **Wahlweise:** Ändern Sie im Feld **Click-Through-URL-Skript** das Beispielskript bei Bedarf.
7. Klicken Sie auf **Absenden** oder **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einer Übersicht Schwachstellen-Bedeutungsdiagramme hinzu

Wenn das Plugin Vulnerability Response aktiviert ist, können Sie der Übersicht Diagramme zur Definition der Bedeutung der Schwachstelle und andere Visualisierungen hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren Sie zur Seite Übersicht, der Sie die Anzeige für die Bedeutung der Schwachstelle hinzufügen möchten.
2. Klicken Sie oben links auf der Seite **auf Inhalt hinzufügen,** um das Steuerelement für die Widget-Auswahl zu öffnen.
3. Treffen Sie in den drei Auswahlfeldern die Auswahl je nach Anzeige (Baumkarte oder Punktzahlbericht), die Sie hinzufügen möchten:
   - Um die Strukturzuordnung für die Schwachstellenbedeutung hinzuzufügen, treffen Sie diese Auswahl:
     - Verzeichnisübersicht
     - Bedeutung der Schwachstelle
     - Bedeutung der Schwachstelle
   - Um den Bericht zur Bedeutung der Schwachstelle hinzuzufügen, treffen Sie diese Auswahl:
     - Performance Analytics
     - Punktzahl
     - Services mit Bedeutung für Schwachstellen
4. Klicken Sie auf die Position auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
5. Schließen Sie das Feld **Inhalt hinzufügen**.

Management schwerwiegender Sicherheits-Incidents

Die Anwendung ServiceNow® Management schwerwiegender Sicherheits-Incidents verfolgt den Fortschritt von Major Security Incident (MSI) von der Discovery über die Analyse, das Vorschlagen, Heraufstufen und Verknüpfen von Security Incidents bis zum Abschluss.

Management schwerwiegender Sicherheits-Incidents

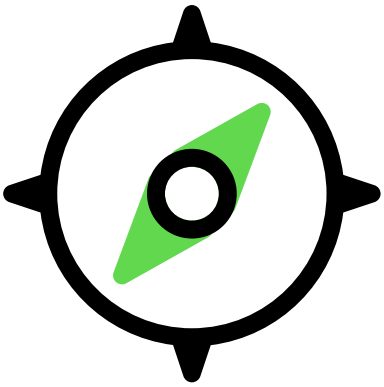
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

servicenow

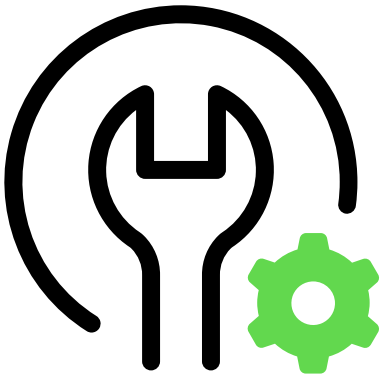
Automatische Übersetzung

Untersuchen



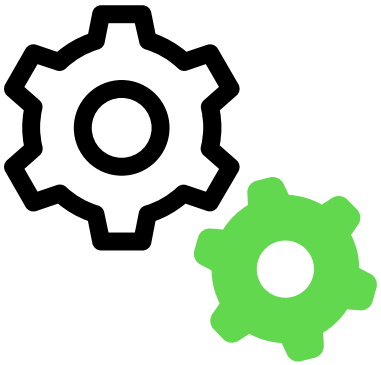
Erfahren, wie Analysten, Administratoren und Manager das Management schwerwiegender Sicherheits-Incidents (Major Security Incident Management, MSIM) verwenden

Konfigurieren



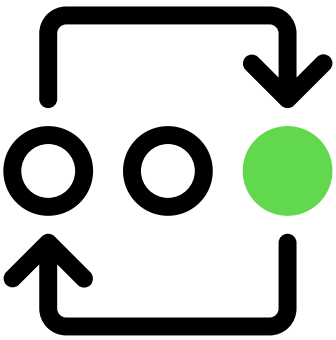
Planen und konfigurieren Sie Ihre -Implementierung

integrieren



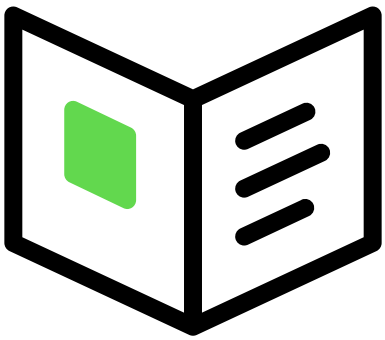
Erweitern Sie die MSIM-Fähigkeiten durch die Integration mit anderen MicrosoftMicrosoft Azure Event Hubs -Anwendungen

Verwalten



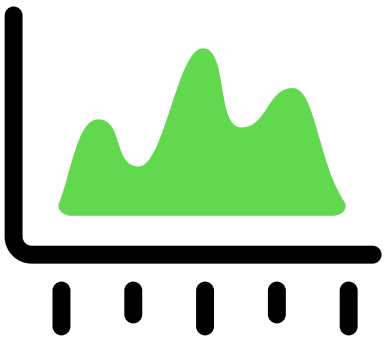
Administrationsaufgaben zum Taggen von Incident-Datensätzen und zum Konfigurieren von Bezeichnungen

Verwenden



Über die Verwaltung des Arbeitsbereichs können Sie Datensätze schwerwiegender Security Incidents vorschlagen, heraufstufen, verknüpfen und ablehnen

Statusberichte



Überwachen Sie Incident-bezogene Aufgaben, und verbessern Sie Prozesse mithilfe von Metriken, Trenddiagrammen und Berichten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Fähigkeiten		
Konfigurieren Sie Informationen, um Datensätze zusammenzufassen		

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Security Operations-Apps im Store anfordern

Wenn Sie ein neuer Security Operations -Kunde auf Rome oder höher sind, besuchen Sie die ServiceNow Store Website, um die verfügbaren Apps und Informationen zum Senden von Anforderungen an den Store anzuzeigen.

Problembehandlung und Hilfe

- Management schwerwiegender Sicherheits-Incidents Forum auf ServiceNow Community.
- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Management schwerwiegender Sicherheits-Incidents

Erkunden Sie Management schwerwiegender Sicherheits-Incidents, um zu verstehen, wie die Anwendung kritische Security Incidents mit hoher Priorität nachverfolgt, die als Bedrohung für das Unternehmen identifiziert werden.

Verwenden Sie diesen Abschnitt, um die wichtigsten Funktionen und verschiedenen Rollen kennen zu lernen, die bei der Arbeit mit Datensätzen schwerwiegender Security Incidents erforderlich sind. Dieser Abschnitt enthält auch Informationen zu den ersten Schritten mit der Anwendung, den Voraussetzungen und den Plugins, die für die Arbeit mit der Anwendung erforderlich sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Management schwerwiegender Sicherheits-Incidents

Verfolgen und verwalten Sie verschiedene Aktivitäten, die normalerweise zur Lösung eines schwerwiegenden Security Incident gehören, über Management schwerwiegender Sicherheits-Incidentsnach. Über einen intuitiven Arbeitsbereich können Incident-Manager und andere, die an einem Incident arbeiten, Incidents zu schwerwiegenden Incidents hochstufen, Aktivitäten zu schwerwiegenden Security Incidents nachverfolgen und problemlos mit Kollegen zusammenarbeiten.

Übersicht

Die Funktionen zur Verwaltung schwerwiegender Security Incidents werden mit den vorhandenen Funktionen des Security Incident Response-Produkts kombiniert. Dies beinhaltet die Möglichkeit für einen Sicherheitsanalysten, einen Standard-Security Incident zu einem schwerwiegenden Security Incident zu eskalieren, sodass die neuen Produktfunktionen zur Unterstützung des Nachbesserungsprozesses verfügbar sind.

Nach der Installation von in Ihrer Instanz ServiceNow kann ein Security Incident-Analyst:

- Schlagen Sie dem Kandidaten für einen schwerwiegenden Security Incident einen Security Incident vor, um einen Überprüfungsprozess für die Erstellung eines schwerwiegenden Security Incident zu initiieren.
- Sie können einen Security Incident ohne zusätzlichen Überprüfungsprozess zu einem schwerwiegenden Security Incident heraufstufen.
- Lehnen Sie einen Security Incident ab, der als schwerwiegender Security Incident (Major Security Incident, MSI) vorgeschlagen wird.
- Verknüpfen Sie einen Security Incident als untergeordneten Incident mit dem schwerwiegenden Security Incident (MSI), damit alle Security Incidents bearbeitet werden können.

Schlüsselfunktionen

Major Security Incident Management (MSIM) verbessert den Nachbesserungsprozess für schwerwiegende Security Incidents durch folgende Funktionen:

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents für die Anwenderrolle „Manager schwerwiegender Security Incidents“.
- Organisieren Sie Antwortaufgaben über mehrere „untergeordnete“ Security Incidents hinweg.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chatkommunikationskanälen nach der Erstellung eines schwerwiegenden Security Incident sowie die Archivierung als Teil des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien) im Zusammenhang mit dem schwerwiegenden Security Incident über eine Microsoft SharePoint -Integration.
- Chatkanalmanager und Aktivitätenstromkomponenten zur Verwaltung der Kommunikation zwischen mehreren Sicherheits-, IT- und Funktionsgruppen über eine Microsoft Teams -Integration.

Arbeitsbereichskomponenten

Das Produkt Management schwerwiegender Sicherheits-Incidents enthält mehrere neue Arbeitsbereichskomponenten und Anwenderoberflächenseiten, die folgende wichtige Funktionen bereitstellen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für die Anwenderrolle „Manager für schwerwiegende Security Incidents“ entwickelt wurde.
- Organisieren Sie Antwortaufgaben über mehrere untergeordnete Security Incidents hinweg.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chatkommunikationskanälen nach der Erstellung eines schwerwiegenden Security Incident sowie die Archivierung als Teil des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien) im Zusammenhang mit dem schwerwiegenden Security Incident über eine Microsoft SharePoint -Integration.
- Chatkanalmanager und Aktivitätenstromkomponenten zur Verwaltung der Kommunikation zwischen mehreren Sicherheits-, IT- und Funktionsgruppen über eine Microsoft Teams -Integration.

Unterstützte Versionen von Major Security Incident Management

Management schwerwiegender Sicherheits-Incidents (MSIM) erfordert die Version Now Platform® Rome.

Diese Funktion unterstützt Microsoft Teams, einen chatzentrierten Arbeitsbereich in der Suite Microsoft Office 365. Vor Microsoft Teams war eine separate Installation der Anwendungen Microsoft Office 365.

Unterstützte Versionen Now Platform.

Diese Funktion wird ab Rome und späteren Releases unterstützt.

Die folgenden Security Operations -Anwendungen sind die Standard- Security Incident Response - Plugins, die wahrscheinlich für die meisten Benutzer installiert werden, wenn sie bereits Security Incident Response (SIR) verwenden. Wenn nicht installiert, müssen Sie über ServiceNow Storeinstallieren und aktivieren. Installieren Sie jeweils eine Anwendung in der angegebenen Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten:

1. Security Incident Response: com.snc.si_dep ist das abhängige Plugin. Durch die Installation dieses Plugins werden die anderen Security Operations-Anwendungen aktiviert.
2. Security Integration Framework
3. Security Support Common
4. Security Support Common Orchestration

Erste Schritte mit MSIM

Lesen Sie sich die folgenden Informationen durch, bevor Sie die Arbeit mit Management schwerwiegender Sicherheits-Incidentsbeginnen.

Erforderliche Rolle: sn_msi.workspace_admin.

Für eine einfache Installation und Konfiguration der Anwendung Management schwerwiegender Sicherheits-Incidents müssen Sie möglicherweise überprüfen, ob die folgenden Plugins aktiviert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Im Schnellstarthandbuch für das Management schwerwiegender Sicherheits-Incidents ist ein Update Set (KB1289784) verfügbar, das Anwendern bei der Einrichtung einer einfachen Konfiguration hilft. Sie müssen das Update Set importieren, nachdem Sie die Installation der Anwendung abgeschlossen haben. Befolgen Sie die Anweisungen im Schnellstarthandbuch (Schritt 2) im Abschnitt „Begleitende Dokumente“ in der Anwendung MSIM im ServiceNow Store.

Voraussetzung

Aufgabe	Beschreibung
Bevor Sie mit der Anwendung beginnen, vergewissern Sie sich, dass Sie über die erforderlichen abhängigen Plugins verfügen.	Als ersten Schritt installieren Sie: • ServiceNow IntegrationHub-Installationsprogramm (com.glide.hub.integrations) • ServiceNow® IntegrationHub Laufzeit (com.glide.hub.integration.runtime) • ServiceNow® IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) • ServiceNow® IntegrationHub Aktionsvorlage – Datenstrom (com.glide.hub.action_type.datastream) • ServiceNow® IntegrationHub Flow Designer – Dynamische Eingaben (com.glide.hub.dynamic_inputs) **Hinweis:** Wenn Sie nicht über die erforderlichen Berechtigungen für eines der aufgeführten ServiceNow® IntegrationHub -Plugins verfügen, erstellen Sie ein Supportticket, um diese erforderlichen Anwendungen zu installieren.
Stellen Sie sicher, dass Sie über den erforderlichen Zugriff zum Installieren von Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke verfügen. **Hinweis:** Die oben aufgeführten sind die primären abhängigen Anwendungen für die ersten Schritte mit Management schwerwiegender Sicherheits-Incidents.	Bevor Sie Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke installieren, vergewissern Sie sich, dass Sie über den erforderlichen Zugriff auf die Anwendungen ServiceNow IntegrationHub verfügen. **Hinweis:** Microsoft SharePoint -Spoke und Microsoft Teams Graph -Spoke sind abhängige Anwendungen von ServiceNow® IntegrationHub -Anwendungen.

Prüfliste für Setup MSIM

Bevor Sie die Anwendung ServiceNow® Management schwerwiegender Sicherheits-Incidents (MSIM) verwenden, laden Sie die Anwendung aus dem ServiceNow® Storeherunter.

Verfolgen Sie Ihren Fortschritt bei Setup, Installation und Konfiguration anhand der folgenden Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die der Anwendung Management schwerwiegender Sicherheits-Incidents zugewiesenen Rollen sind in den weiteren folgenden Abschnitten aufgeführt. Weitere Informationen finden Sie unter Management schwerwiegender Sicherheits-Incidents Rollen.

Verwenden Sie die folgende Prüfliste, um sich durch die End-to-End-Schritte zum Installieren und Konfigurieren der Anwendung Management schwerwiegender Sicherheits-Incidents führen zu lassen.

Prüfliste

Setupaufgabe	Beschreibung
Vergewissern Sie sich, dass die Anwendung Management schwerwiegender Sicherheits-Incidents über ServiceNow® Storeinstalliert und aktiviert ist.	Management schwerwiegender Sicherheits-Incidents v1.1.1 ist unter ServiceNow® Storeverfügbar. Befolgen Sie diese Anweisungen: Herunterladen einer Anwendung aus dem ServiceNow Store.
Stellen Sie sicher, dass die folgenden Anwendungen in der angegebenen Reihenfolge installiert sind.	Die folgenden Anwendungen werden standardmäßig installiert, nachdem Sie die Anwendung Management schwerwiegender Sicherheits-Incidents in der aktuellen Anwendungs-Release-Version installiert haben: • File Explorer Core for Security Operations v1.1.1 • Microsoft SharePoint File Explorer Connector für Security Operations v1.1.1 • File Explorer Komponente für Security Operations v1.0.0 • Microsoft Teams Chat Connector für Security Operations v1.0.0 • Chat Core für Security Operations v1.0.0 • Major Security Incident Antwort v1.1.1 • EVAM-Karte für Zusammenarbeitschat für MSIM Arbeitsbereich v1.0.0 (Diese Anwendung wird nur für die UI-Visualisierungen im Anwendungshintergrund für Management schwerwiegender Sicherheits-Incidents den Arbeitsbereich eingerichtet) • Task Organizer UI Component for Management schwerwiegender Sicherheits-Incidents workspace 1.0.0 • Security Incident Response v12.8.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Major Security Incident je nach Bedarf Anwenderrollen zugewiesen sind.	Im Folgenden sind die Rollen aufgeführt, die während des gesamten Incident-Lebenszyklus des Nachbesserungsprozesses für Major Security Incident beteiligt sind: • MSI-Administrator [sn_msi.workspace_admin] • MSI-Manager [sn_msi.workspace_manager] • MSI-Responder [sn_msi.workspace_responder]. Ausführliche Informationen zu den einzelnen Rollen finden Sie unter Management schwerwiegender Sicherheits-Incidents Rollen.
Vergewissern Sie sich, dass die Konfiguration Microsoft SharePoint v1.0.0 erfolgreich eingerichtet wurde.	Microsoft SharePoint verwaltet Sites, Ordner, Dateien, Gruppen und Benutzer in Microsoft SharePoint. Fügen Sie Microsoft SharePoint -Daten zu Ihrer Instanz ServiceNow® hinzu. Dazu müssen Sie Graph- und REST-Verbindungen einrichten. Informationen zum Einrichten der Konfiguration von REST- und Graph-Verbindungen finden Sie in der Dokumentationzur Microsoft SharePoint-Spoke v1.1.2. Richten Sie eine Graph- und eine REST-Verbindung ein, um von Microsoft SharePointaus eine Verbindung zu Ihrer Instanz ServiceNow® herzustellen.
Stellen Sie sicher, dass Sie eine Website Microsoft SharePoint erstellt haben, um eine Dokumentbibliothek zu erstellen.	Erstellen Sie bei Bedarf eine Microsoft SharePoint -Website, oder verwenden Sie eine vorhandene Website, um unsere Dokumentbibliothek zu erstellen.
Stellen Sie sicher, dass Sie eine Dokumentbibliothek unter der Website Microsoft SharePoint erstellt haben.	Erstellen Sie eine dedizierte Dokumentbibliothek unter einer neuen oder vorhandenen Microsoft SharePoint -Website.
Stellen Sie sicher, dass die erforderlichen Berechtigungen für die Benutzer bereitgestellt und den erforderlichen	Verwalten Sie den Zugriff von der Site Microsoft SharePoint auf verschiedene Benutzer und Benutzergruppen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
Benutzergruppen im Microsoft SharePointzugewiesen werden.	
Vergewissern Sie sich, dass das Laufwerk Microsoft SharePoint und die erforderlichen Konfigurationseinstellungen erstellt und konfiguriert wurden.	Um die Laufwerkskonfigurationen zu überprüfen, richten Sie Microsoft SharePoint File Explorer Connector, Ordner- und Dateiaktionen und Ordnervorlagen ein: • Konfigurieren Sie das Laufwerk des Datei-Explorers Repository: Erstellt eine Verbindung von der Instanz Microsoft SharePoint zur Instanz ServiceNow®. • Konfigurieren Sie die Aktionseinstellungen für Ordner und Dateien: Konfigurieren und steuern Sie die einzelnen Ordner- und Dateiaktionen, die in der Datei-Explorer-Komponente angezeigt werden. • Erstellen Sie Ordnervorlagen: Konfigurieren Sie, um eindeutige Ordner für verschiedene Typen von schwerwiegenden Security Incidents zu erstellen.
Stellen Sie sicher, dass Sie erfolgreich eine Verbindung zur Microsoft Teams Chat Connector-Anwendung hergestellt haben.	Um eine Verbindung der Microsoft Teams Chat Connector-Anwendung mit der Instanz ServiceNow® herzustellen, führen Sie das hier erläuterte Verfahren aus: Stellen Sie eine MS Teams Graph-Verbindung her auf Now Platform.
Stellen Sie sicher, dass Sie Microsoft Teams mit der Instanz Now Platform® konfiguriert und Konfigurationen für Verbindungen und Anmeldeinformationen erstellt haben.	Um die Konfiguration Microsoft Teams von mit der Instanz ServiceNow® zu überprüfen, gehen Sie wie folgt vor: • Stellen Sie eine MS Teams Graph-Verbindung her auf Now Platform • Erstellen Sie eine Chatkanalvorlage
Vergewissern Sie sich, dass die Konfigurationseinstellungen für Administration schwerwiegender Security Incidents erfolgreich sind.	Als MSI-Administrator müssen Sie in der Lage sein: • bestimmen, ob Sicherheitsanalysten den Incident vorschlagen und hochstufen und andere Security Incidents verknüpfen können. • Aktivieren oder deaktivieren Sie die Benachrichtigungen, wenn ein Incident vorgeschlagen oder heraufgestuft wird. Möglichkeit zum Bearbeiten von Standardvorlagennachrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	• Konfigurieren Sie Sicherheits-Tags, die auf der Anwenderoberfläche für Sicherheitsanalysten angezeigt werden, um die Incidents zu unterscheiden, die als Kandidaten für schwerwiegende Security Incidents vorgeschlagen oder zu schwerwiegenden Security Incidents heraufgestuft wurden.
Vergewissern Sie sich, dass die Einstellungen für Administration schwerwiegender Security Incidents – Benachrichtigungen erfolgreich sind.	Lösen Sie als MSI-Administrator E-Mail-Benachrichtigungen aus, wenn ein Security Incident vorgeschlagen wird und an alle Benutzer und Gruppen gesendet wird, die für die Benachrichtigungsliste konfiguriert sind. Weitere Informationen finden Sie unter Legen Sie Benachrichtigungseinstellungen für fest MSIM.

Management schwerwiegender Sicherheits-Incidents Rollen

Weisen Sie Rollen zu, um sicherzustellen, dass Benutzer alle erforderlichen Aktionen innerhalb der MSIM-Anwendung ausführen können.

Rollen für Management schwerwiegender Incidents

Rollentyp	Rolle	Beschreibung
MSI-Administrator	sn_msi.workspace_admin	Kann ich Management schwerwiegender Incidents installieren und konfigurieren und die abhängigen Anwendungen wie File Explorer (FE), Microsoft Teams- und Chatkanalkonfiguration, Setup des Arbeitsbereichs und MSI-Administration: Setup für Konfigurationen und Benachrichtigungen einrichten? So richten Sie ein: • File Explorer-Komponente (FE): ◦ Konfigurieren Sie das Datei-Repository. ◦ Konfigurieren Sie Datei- und Ordneraktionen, die in der Komponente „Datei-Explorer“ der Registerkarte „Zusammenarbeit“ im Arbeitsbereich „Major Security

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen für Management schwerwiegender Incidents (Fortsetzung)

Rollentyp	Rolle	Beschreibung
		Incident Management“ bereitgestellt werden. ○ Erstellen Sie die Stammordner und Unterordner, und gewähren Sie Zugriff auf die Unterordner. • Verwaltung von Chatkanälen ○ Aktivieren und konfigurieren Sie Microsoft Teams, indem Sie die Verbindung Microsoft Teams validieren. ○ Erstellen Sie Chat-Teams und Chat-Kanäle, fügen Sie Anwender hinzu, und weisen Sie Anwender den verschiedenen Anwendergruppen zu. • MSI-Administration: ○ Konfigurationen: Konfigurieren Sie die Aktionen der Sicherheitsanalysten, die Benachrichtigungen, die gesendet werden, wenn Incidents vorgeschlagen und heraufgestuft werden, und die Anzeige von Tags für Security Incidents. ○ Benachrichtigungen: Automatisieren Sie den E-Mail-Benachrichtigungsprozess und die Benutzerbenachrichtigung, wenn ein Security Incident als schwerwiegender Security Incident vorgeschlagen oder heraufgestuft wird.
MSI-Manager	sn_msi.workspace_manager	• Zeigen Sie den Zugriff auf die Seite mit den Konfigurationseinstellungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen für Management schwerwiegender Incidents (Fortsetzung)

Rollentyp	Rolle	Beschreibung
		für das Management schwerwiegender Security Incidents an. Das Ändern einer der Konfigurationseinstellungen ist eingeschränkt. • Zeigen Sie Incident-Datensatzdaten auf den Registerkarten **Details**, **Zusammenarbeit**und **Aufgabenorganisator** des Arbeitsbereichs Management schwerwiegender Incidents an, und bearbeiten Sie sie. • Stufen Sie den Security Incident zu einem schwerwiegenden Security Incident herauf. • Konfigurieren Sie Datei- und Ordneraktionen, die in der Datei-Explorer-Komponente auf der Registerkarte **Zusammenarbeit** des Arbeitsbereichs Management schwerwiegender Incidents verfügbar sind. • Verknüpfen und Aufheben der Verknüpfung von Datensätzen mit schwerwiegenden Security Incidents aus dem -Arbeitsbereich.
MSI-Responder	sn_msi.workspace_responder	• Optionale Rolle zum Anzeigen, Bearbeiten und Reagieren auf schwerwiegende Security Incidents im **Details** und **Aufgaben** Registerkarten des Arbeitsbereichs Management schwerwiegender Incidents. • Verknüpfen und Aufheben der Verknüpfung von Datensätzen mit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen für Management schwerwiegender Incidents (Fortsetzung)

Rollentyp	Rolle	Beschreibung
		schwerwiegenden Security Incidents aus dem -Arbeitsbereich.

Integration von Management schwerwiegender Sicherheits-Incidents

Erweitern Sie die Fähigkeiten von Management schwerwiegender Sicherheits-Incidents, und stellen Sie durch die Integration mit den Anwendungen MicrosoftMicrosoft Azure Event Hubs eine Verbindung zur Instanz Now Platform her.

Wichtig:
Im Schnellstarthandbuch für das Management schwerwiegender Sicherheits-Incidents ist ein Update Set (KB1289784) verfügbar, das Anwendern bei der Einrichtung einer einfachen Konfiguration hilft. Sie müssen das Update Set importieren, nachdem Sie die Installation der Anwendung abgeschlossen haben. Befolgen Sie die Anweisungen im Schnellstarthandbuch (Schritt 2) im Abschnitt „Begleitende Dokumente“ in der Anwendung MSIM im ServiceNow Store.

Richten Sie die Microsoft SharePoint -Dokumentbibliothek ein

Überprüfen Sie die erforderliche Einrichtung, die in Microsoft SharePointdurchgeführt werden muss.

Vorbereitungen

Vergewissern Sie sich, dass das folgende Konfigurationsverfahren abgeschlossen wurde.

Erforderliche Rolle: Systemadministrator, sn_msi.workspace_admin

Prozedur

1. Erstellen Sie eine neue Dokumentbibliothek unter einer neuen oder vorhandenen Site Microsoft SharePoint, und verwenden Sie dieselbe Site, während Sie die Datei-Repository-Konfiguration Management schwerwiegender Sicherheits-Incidents konfigurieren.
2. Registrieren Sie eine Anwendung bei MicrosoftMicrosoft Azure Event Hubs, um eine Verbindung herzustellen und mit Microsoft SharePoint über die Microsoft SharePoint REST API zu kommunizieren. Durch das Registrieren der Anwendung wird eine Verbindung zwischen der App und Microsoft hergestellt. Weitere Informationen finden Sie unter Nur-App-Zugriff auf SharePoint im Portal „docs.microsoft.com“ einrichten .

   Es gibt zwei Möglichkeiten, eine Anwendung bei Microsoft SharePointzu registrieren:

   a. Zugriff wird nur über Azure AD-App gewährt

   b. Zugriff wird mithilfe von gewährt Microsoft SharePoint Nur App

   Wichtig:
   Das Gewähren des Zugriffs nur über Microsoft SharePoint App ist ein veralteter Ansatz, aber sehr relevant und einfach zu konfigurieren.

   Verwenden Sie die Client-ID und den geheimen Clientschlüssel, die im obigen Schritt generiert wurden, während Sie die REST-Verbindung für den Datei-Explorer Microsoft SharePoint -Connector konfigurieren.

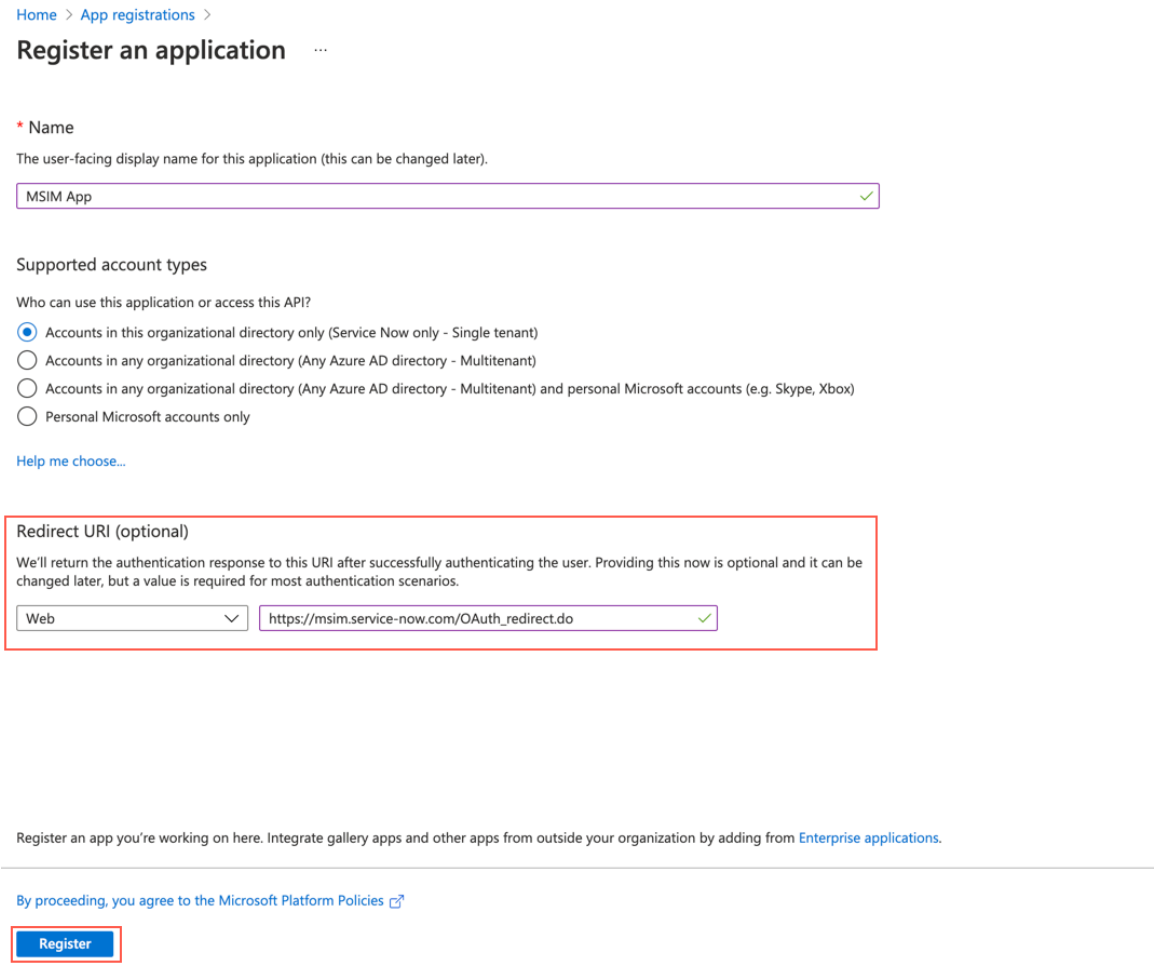
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Registrieren Sie eine weitere App bei MicrosoftMicrosoft Azure Event Hubs, um mit Microsoft SharePoint über Microsoft Graph APIs zu kommunizieren.
   Weitere Informationen hierzu finden Sie unter Anwendungen bei Microsoft Identity Platform registrieren
   Registrieren Sie eine neue Anwendung in Azure mit der Now Platform-Instanz

   a. Melden Sie sich mit dem Konto MicrosoftMicrosoft Azure Event Hubs beim Azure -Portal an.

   b. Folgen Sie den Anweisungen im Microsoft-Portal.

   c. Geben Sie im Feld „Zulässige Umleitungs-URL“ die Umleitungs-URL für die Instanz Now Platform® an.
   Beispiel: `msim.service-now.com/OAuth_redirect.do`



   d. **Registrieren** der Anwendung.

   e. Navigieren Sie zum Abschnitt **Zertifikate und Geheimnisse**, und erstellen Sie ein neues Clientgeheimnis.

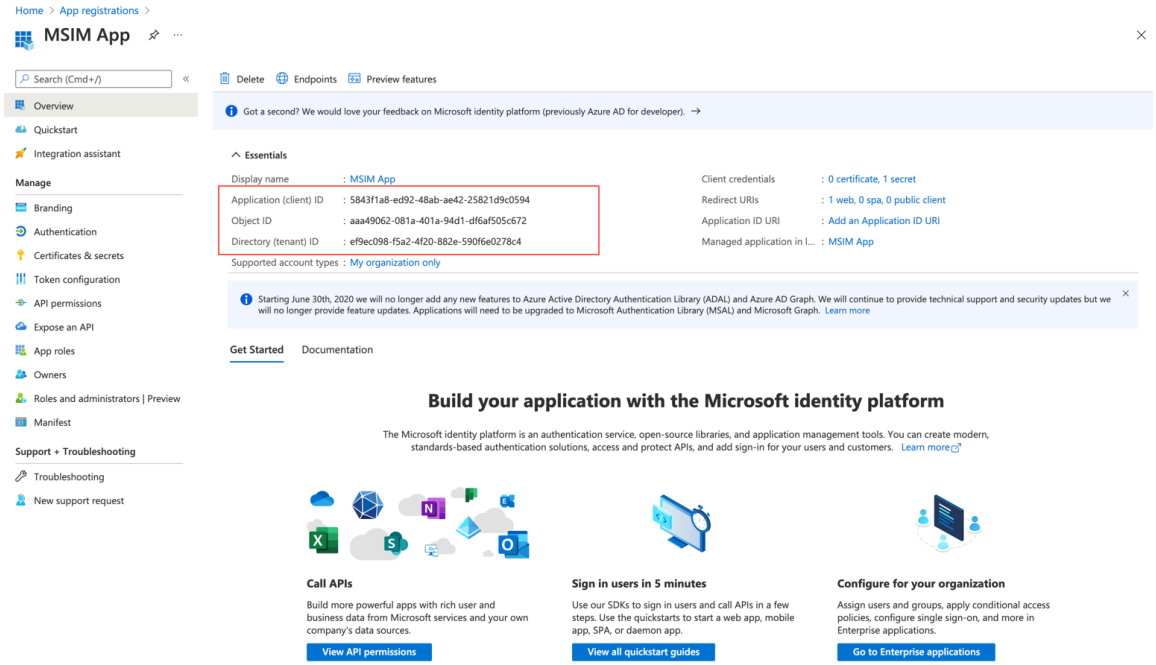
   > **Hinweis:**
   > Sie können auch ein Client-Zertifikat hochladen und den generierten Fingerabdruckwert kopieren und speichern.

   f. Kopieren Sie den generierten geheimen Clientschlüssel, und speichern Sie ihn, da er bei der Konfiguration der OAuth-Anwendungsregistrierung in der Instanz ServiceNow® erforderlich ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Fügen Sie unter **API-Berechtigungen**die Microsoft Graph-Berechtigung hinzu:
   a. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
   b. Wählen Sie **Microsoft Graph** aus.
   c. Wählen Sie **Delegierte Berechtigungen**aus.
   d. Wählen Sie in der **Sites** -Liste die Berechtigung **Sites.ReadWrite.All (Sites.LesenSchreiben.Alle)** aus.
   e. Wählen Sie in der Liste **Benutzer** die Option **Benutzer.Leseberechtigung** aus.
   f. Klicken Sie auf **Berechtigungen hinzufügen**.
5. Fügen Sie unter **API-Berechtigungen**die SharePoint-Berechtigung hinzu:
   a. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
   b. Wählen Sie **SharePoint**aus.
   c. Wählen Sie **Anwendungsberechtigungen**aus.
   d. Wählen Sie in der Liste **Sites** die Berechtigung **Sites.FullControl.All** aus.
   e. Klicken Sie auf **Berechtigungen hinzufügen**.
6. Klicken Sie nach dem Hinzufügen von Berechtigungen **auf Administratorzustimmung erteilen**.
7. Verwenden Sie dieselben Werte für die Client-ID und den geheimen Clientschlüssel, die aus dieser Anwendungsregistrierung generiert wurden (verfügbar im Abschnitt „Übersicht“), während Sie den Connector Graph Connection für Datei-Explorer Microsoft Teams konfigurieren.



Stellen Sie Graph- und REST-Verbindungen her in Now Platform

Konfigurieren Sie Graph- und REST-Verbindungen in der Instanz Now Platform für die Kommunikation mit Microsoft SharePoint.

Integrieren Sie die Instanz Now Platform und Microsoft SharePoint, indem Sie in Microsoft SharePoint eine anwenderdefinierte OAuth-Anwendung erstellen, um Now Platform -Anforderungen zu authentifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die REST-Verbindung für MS SharePoint

REST-Verbindung in Instanz Now Platform für die Kommunikation mit Microsoft SharePointkonfigurieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Konfigurieren Sie einen neuen Mandantendatensatz, und wählen Sie **MicrosoftSharepointOnline** als Aliasdatensatz aus.
   Weitere Informationen finden Sie unter Microsoft SharePoint-Mandanten definieren.
2. So konfigurieren Sie den Alias **für MicrosoftSharepointOnline** -Verbindungen und -Anmeldeinformationen .
3. Wählen Sie den in Schritt 2 oben erstellten Mandantendatensatz wie folgt aus: **REST-Verbindung** beim Ausfüllen des Formulars **„Datei-Repository-Konfiguration“**.

Graph-Verbindung für MS SharePoint konfigurieren

Konfigurieren Sie die Graph-Verbindung in der Instanz Now Platform für die Kommunikation mit Microsoft SharePoint.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Informationen zum Konfigurieren des Alias für Graph-Verbindungen und Anmeldeinformationen mithilfe des Client-Geheimnisses finden Sie unter .
   Führen Sie die folgenden Schritte aus, um den Alias für Graph-Verbindungen und Anmeldeinformationen mithilfe eines Client-Zertifikats zu konfigurieren.

   Hinweis:
   Standardmäßig werden der JWT-Provider, der JWT-Schlüssel und das Zertifikat, die in der vorherigen REST-Verbindung konfiguriert sind, hier in diesem Verfahren verwendet. Weitere Informationen finden Sie unter Konfigurieren Sie die REST-Verbindung für MS SharePoint.

   a. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.

   b. Öffnen Sie den Datensatz **MicrosoftSharePointGraph**.

   c. Klicken Sie auf den zugehörigen Link **Neue Verbindung und Anmeldeinformationen erstellen**.

   d. Füllen Sie diese Details im Formular aus.

Feld	Beschreibung
OAuth-Entitätsname	Name zur Identifizierung des OAuth-Anwendungsregistrierungsdatensatzes.
OAuth-Client-ID	Client-ID
OAuth-Client-Geheimnis	Sie können einen beliebigen Wert eingeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Dies ist nicht wichtig, da Sie die zertifikatbasierte Authentifizierung verwenden.
OAuth-Autorisierungs-URL	Autorisierungs-URL in diesem Format: `https://login.microsoftonline.com/<tenant-id> /oauth2/v2.0/authorize?response_mode=query`
OAuth-Token-URL	Token-URL in diesem Format: `https://login.microsoftonline.com/<tenant-id> /oauth2/v2.0/token`
Token-Sperr-URL	Tokenwiderruf-URL in diesem Format: `https://login.microsoftonline.com/<tenant-id> /oauth2/v2.0/token` .
OAuth-Umleitungs-URL	ServiceNow -Umleitungs-URL in diesem Format: `https://empipaas.service-now.com/oauth_redirect.do`

Hinweis:
Sie können die Standardwerte entsprechend Ihren Anforderungen ändern.

e. Klicken Sie auf **OAuth-Token erstellen und abrufen**.
Es wird eine Fehlermeldung mit der Meldung „401 – nicht autorisiert“ angezeigt.

f. Laden Sie das Formular neu, und öffnen Sie den Datensatz in der zugehörigen Liste **„Verbindungen“**.

g. Geben Sie den Base64-codierten **Fingerabdruckwert** im Attribut **Codierter Fingerabdruckwert** im Abschnitt **„Attribute“** ein.

Hinweis:
Der **Fingerabdruckwert** ist ein hexadezimaler Wert. Sie können ein Hexadezimal-toBase64-Konvertierungstool (Hex in Base64) verwenden, um den **Fingerabdruckwert** in einen Base64-Wert zu codieren.

h. Navigieren zu **System-OAuth** > **Applikationsregistrierung**.

i. Öffnen Sie den Datensatz, der den gleichen Namen wie **OAuth-Entitätsname**hat. Dies ist der Schritt d in diesem Verfahren.

j. Ändern Sie das OAuth-API-Skript in: **OAuthUtilJWTFESPGraph**

k. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.

l. Öffnen Sie den folgenden Datensatz: **Microsoft SharePoint Graph-Anmeldeinformationen**.

m. Klicken Sie im Abschnitt „Zugehörige Links“ **auf OAuth-Token abrufen**.

2. Aktualisiert den OAuth-Entitätsbereich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **System-OAuth** > **Applikationsregistrierung**.

b. Öffnen Sie den in Schritt 1 generierten OAuth-Anwendungsregistrierungsdatensatz.

c. Wählen Sie die zugehörige Liste **OAuth-Entitätsbereiche** aus.

d. Ersetzen Sie das Feld **OAuth-Bereich** durch den folgenden Wert **offline_access** :

```
https://graph.microsoft.com/Sites.ReadWrite.All
```

Hinweis:
Sie können Schritt 2 ignorieren und mit dem nächsten Schritt fortfahren, wenn Sie ein Client-Zertifikat hinzufügen.

3. Konfigurieren Sie einen neuen Mandantendatensatz, und wählen Sie den Aliasdatensatz wie in Schritt 1 erstellt aus.
   Weitere Informationen finden Sie unter Microsoft SharePoint-Mandanten definieren.
4. Wählen Sie den in Schritt 3 erstellten Mandantendatensatz als: **Graph-Verbindung** beim Ausfüllen des Formulars „Datei-Repository-Konfiguration“.

Stellen Sie eine MS Teams Graph-Verbindung her auf Now Platform

Integrieren Sie die Instanz Now Platform und den Account Microsoft Teams, indem Sie eine Verbindung Microsoft Teams Graph herstellen.

Vorbereitungen
Wenn Sie möchten, können Sie dieselbe Anwendung verwenden, die Sie für SharePoint erstellt haben, um die Microsoft Teams Graph-Verbindung herzustellen.

Erforderliche Rolle: admin, Azure-Administrator

Registrieren Sie eine neue Anwendung in Azure für Microsoft Teams Graph Connection

Prozedur

1. Melden Sie sich mit dem Konto MicrosoftMicrosoft Azure Event Hubs beim Azure -Portal an.
2. Navigieren zu **Azure-Services** > **Anwendungsregistrierung** > **Neue Registrierung**.
3. Geben Sie den Namen der Anwendung ein.
   Beispiel: Microsoft Teams Graph.
4. Wählen Sie die entsprechende Option **Unterstützte Kontotypen** aus, die für Ihre Organisation zutreffend ist.
   Wählen Sie beispielsweise **Accounts in diesem Organisationsverzeichnis (Nur ServiceNow – Einzelner Mandant)** aus.

Hinweis:
Informationen zu unterstützten Kontotypen finden Sie unter Anwendungen bei Microsoft Identity Platform registrieren .

5. Wählen Sie in der Dropdown-Liste unter der Umleitungs-URL die Option **Webtyp** aus.
6. Geben Sie im Feld „Zulässige Umleitungs-URL“ die Umleitungs-URL für Instanz Now Platform ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: https://<<InstanceName> >.service-now.com/oauth_redirect.do

7. Klicken Sie auf **Registrieren**, um Ihre neue Anwendung zu registrieren und sicherzustellen, dass die Seite mit dem Abschnitt **Übersicht** angezeigt wird.

Verwendung von Zertifikaten für die Authentifizierung

Fordern Sie ein Zugriffstoken mit den Anmeldeinformationen eines Zertifikats an.

Vorbereitungen

1. Sie können entweder ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgestelltes Zertifikat verwenden. Sie können ein selbstsigniertes Zertifikat erstellen, indem Sie das PowerShell-Skript ausführen (siehe Azure AD-App für Nur-App-Zugriff einrichten) . Das Skript generiert zwei Dateien: PFX-Datei und cer-Datei.

   Hinweis:
   Stellen Sie sicher, dass Sie das Passwort kennen, das zum Verschlüsseln des privaten Schlüssels zum Generieren der PFX-Datei und der .cer-Datei verwendet wird.

2. Verwenden Sie die PFX-Datei, um eine JKS-Datei (Java Key Store) zu erstellen.

   Hinweis:
   Stellen Sie sicher, dass Sie das Passwort kennen, das zum Generieren einer JKS-Datei aus der PFX-Datei verwendet wird.

Erforderliche Rolle: Administrator

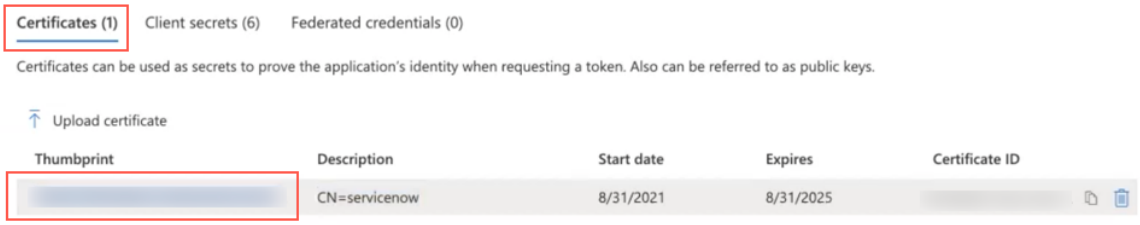
Prozedur

1. Navigieren Sie im Azure AD-Portal zu **App-Registrierungen**.
2. Klicken Sie im Abschnitt **Verwaltenauf Zertifikate und Geheimnisse**.
3. Klicken Sie auf der Registerkarte **Zertifikateauf Zertifikat hochladen**.
4. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Laden Sie ein Zertifikat (öffentlicher Schlüssel) mit einem der folgenden Dateitypen hoch: .cer, .pem, .crt	.cer-Datei, die Sie mit dem PowerShell-Skript generiert haben.
Beschreibung	Beschreibung des Zertifikats.

5. Klicken Sie auf **Hinzufügen**.
   Das Zertifikat wird hochgeladen, und die zugehörigen Details werden unter der Registerkarte **Zertifikate** angezeigt.
6. Kopieren Sie den **Fingerabdruckwert** des hochgeladenen Zertifikats.
   Der **Fingerabdruckwert** ist ein hexadezimaler Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Codieren Sie den **Fingerabdruckwert** in einen Base64-Wert, und zeichnen Sie den Wert zur späteren Verwendung auf.

Hinweis:
Sie können ein Hexadezimal-zu-Base64-Konvertierungstool (Hex-zu-Base64) verwenden, um den **Fingerabdruckwert** in einen Base64-Wert zu codieren.

Hängen Sie ein Java Key Store-Zertifikat für MS Teams an

Aktivieren Sie die JWT-Bearer-Grant-Token-Authentifizierung, indem Sie ein gültiges JKS-Zertifikat (Java Key Store) anfügen.

Vorbereitungen

Melden Sie sich bei Ihrer ServiceNow-Instanz an, um das folgende Verfahren auszuführen.

- Gültiges Java Key Store-Zertifikat
- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Systemdefinition** > **Zertifikate**.
2. Öffnen Sie den Datensatz **Microsoft Teams Connector-Zertifikat**.
   Stellen Sie sicher, dass Sie nur das **Microsoft Teams Connector-Zertifikat** des Standarddatensatzes verwenden.
3. Geben Sie unter **Schlüsselspeicher-Passwort**das Passwort ein, das der JKS-Datei zugeordnet ist.
4. Klicken Sie auf das Anhangsymbol ( ), und hängen Sie das generierte JKS-Zertifikat an.
   Weitere Informationen finden Sie unter .
5. Klicken Sie auf **Speicher/Zertifikate validieren**.
6. Klicken Sie auf **Aktualisieren**.

Konfigurieren Sie den JWT-Signaturschlüssel für MS Teams

Erstellen Sie einen JSON Web Token (JWT)-Signaturschlüssel, um ihn Ihrem Java Key Store-Zertifikat zuzuweisen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **System-OAuth** > **JWT-Schlüssel**.
2. Öffnen Sie den Datensatz **Microsoft Teams Connector JWT**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie im **Feld Signaturschlüssel-Passwort**das Passwort ein, das zum Verschlüsseln des privaten Schlüssels zum Generieren der PFX-Datei und der .cer-Datei verwendet wird.
4. Klicken Sie auf **Aktualisieren**.

Konfigurieren Sie den JWT-Provider für MS Teams

Fügen Sie Ihrer ServiceNow-Instanz einen JSON Web Token (JWT)-Anbieter hinzu.

Vorbereitungen

- Kopieren Sie den Wert der **Anwendungs-ID (Client)** und **der Verzeichnis-ID (Mandant)** der Anwendung, die Sie im Azure-Portal registriert haben, und notieren Sie sie.

- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **System-OAuth** > **JWT-Anbieter**.
2. Öffnen Sie den Datensatz **MS Teams-Connector – JWT-Anbieter**.
3. Geben Sie in der zugehörigen Liste „Standardansprüche“ Werte für **„iss“**, **„sub“**und **„aud“** ein.

Feld	Wert
aud	Microsoft Online-URL in diesem Format: https://login.microsoftonline.com/<tenant-id> /oauth2/token . Ersetzen<tenant-id> mit dem Wert der Verzeichnis-ID (Mandant) Ihrer Anwendung wurde im Azure-Portal registriert.
iss	**Anwendungs-ID (Client)** der Anwendung, die Sie im Azure-Portal registriert haben.
sub	**Anwendungs-ID (Client)** der Anwendung, die Sie im Azure-Portal registriert haben.

4. Klicken Sie auf **Aktualisieren**.

Stellen Sie mithilfe von Zertifikaten eine Verbindung her

Stellen Sie mithilfe von Zertifikaten eine Verbindung zwischen der neu erstellten Microsoft Teams-Graph-Anwendung her.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Öffnen Sie **die Microsoft Teams-Spoke**.
3. Ändern Sie den Feldwert **Configuration Template: MSIM Microsoft Teams ConnectorAuthorization Code Template (Vorlage für Autorisierungscode)**, und speichern Sie das Formular.

   Hinweis:
   Diese Vorlage enthält die delegierte API-Berechtigung, die für die MSTeams-Integration erforderlich ist.

4. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Neue Verbindung und Anmeldeinformationen**erstellen.
5. Klicken Sie auf **OAuth-Token erstellen und abrufen**.
   Es wird eine Fehlermeldung mit der Meldung „401 – nicht autorisiert“ angezeigt.
6. Laden Sie das Formular neu, und öffnen Sie den Datensatz in der zugehörigen Liste „Verbindungen“.
7. Geben Sie den Wert des Base64-codierten **Fingerabdrucks** im Attribut **Fingerabdruck des codierten Zertifikats** im Abschnitt **Attribute** ein.

   Hinweis:
   Der Fingerabdruckwert ist ein hexadezimaler Wert. Sie können ein Hexadezimal-toBase64-Konvertierungstool (Hex in Base64) verwenden, um den Fingerabdruckwert in einen Base64-Wert zu codieren.

8. Navigieren zu **System-OAuth** > **Applikationsregistrierung**
9. Öffnen Sie den Datensatz **mit dem Autorisierungscode des MSIM Microsoft Teams-Connectors**.
10. Ändern Sie das OAuth-API-Skript: **OAuthUtilJWTMSTeamsConnector**.
11. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.
12. Öffnen Sie den Datensatz **Anmeldeinformationen für MSIM Microsoft Teams-Connector**.
13. Klicken Sie unter Zugehörige Links **auf OAuth-Token abrufen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Erfolg werden der Azure-Anwendung die folgenden API-Berechtigungen hinzugefügt.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Wert des Clientgeheimnisses wird verwendet

Verwenden Sie den Wert des geheimen Clients, um den Registrierungsdatensatz der Graph-Anwendung zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie im Azure AD-Portal zu **App-Registrierungen**.
2. Klicken Sie im Abschnitt **Verwaltenauf Zertifikate und Geheimnisse**.
3. Klicken Sie auf **New client secret** (Neuer geheimer Clientschlüssel).
4. Kopieren und notieren Sie den erstellten geheimen Clientschlüssel aus dem Feld **Wert**.

Stellen Sie eine Verbindung mit dem geheimen Clientschlüssel her

Stellen Sie eine Verbindung zwischen der neu erstellten Microsoft Teams-Graph-Anwendung und der Instanz Now Platform her.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Öffnen Sie **die Microsoft Teams-Spoke**.
3. Ändern Sie den Feldwert **Configuration Template: MSIM Microsoft Teams ConnectorAuthorization Code Template (Vorlage für Autorisierungscode)**, und speichern Sie das Formular.

Hinweis:
Diese Vorlage enthält die delegierte API-Berechtigung, die für die MSTeams-Integration erforderlich ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Neue Verbindung und Anmeldeinformationen**erstellen.

5. Klicken Sie auf **OAuth-Token erstellen und abrufen**.
   Bei Erfolg werden der Azure-Anwendung die folgenden API-Berechtigungen hinzugefügt.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Aktivieren Sie den MS Teams Chat-Connector für den MS Teams Graph Spoke-Benutzer

Wenn Sie ein vorhandener Benutzer sind, befolgen Sie das Verfahren in diesem Abschnitt, um den Microsoft Teams-Chat-Connector zu aktivieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

Wenn Sie bereits Microsoft Teams Graph-Spoke-Anwender sind, führen Sie die folgenden Schritte aus:

- Navigieren Sie im Azure-Portal zu Ihrer registrierten Anwendung, die von der Microsoft Teams Graph-Spoke verwendet wird.
- Navigieren Sie zum Abschnitt **API Permissions (API-Berechtigungen)**, um die erforderlichen API-Berechtigungen zu konfigurieren.
- Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
- Wählen Sie **Microsoft Graph** aus.
- Um die Anwendung Microsoft Teams Connector zu verwenden, müssen Sie Ihrer Anwendung zwei weitere delegierte Berechtigungen aus dem Azure-Portal hinzufügen: „ChannelMember.ReadWrite.All“ und „TeamMember.ReadWrite.All“.
- Nachdem Sie die oben genannten erforderlichen Berechtigungen hinzugefügt haben, klicken Sie auf **Administratorzustimmung erteilen**.

Konfigurieren Sie MS Teams in der Now Platform-Instanz für einen vorhandenen Anwender:

- Navigieren Sie zu **Aliasse für Verbindungen und Anmeldeinformationen**.
- Wählen Sie **den Microsoft Teams-Spoke-** Datensatz aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie den Anmeldeinformationsdatensatz aus, der der Microsoft Teams-Spoke zugeordnet ist.
- Klicken Sie auf **OAuth-Token abrufen**. In einer Bestätigungsmeldung wird angezeigt, dass das OAuth-Aktualisierungstoken verfügbar ist.

Als bestehender Anwender haben Sie jetzt die Integration der Microsoft Teams-Chat-Connector-Anwendung in die Microsoft Teams Graph API abgeschlossen.

Management schwerwiegender Sicherheits-Incidents Integration mit Telefonkonferenzen

Mit der Integration von Management schwerwiegender Sicherheits-Incidents -Telefonkonferenzen können Sie mit Ihren Kunden und Kollegen zusammenzuarbeiten, um Kundenprobleme mithilfe der Video- und Bildschirmfreigabeoptionen in Microsoft Teams, Cisco Webexoder Zoom in der Anwendung MSIM zu lösen.

Mit der Management schwerwiegender Sicherheits-Incidents -Telefonkonferenz können Sie den Konferenzkommunikationskanal mit dem Notify -Kommunikationskanal integrieren, indem Sie ein Microsoft Teams- , Cisco Webex- oder Zoom -Meeting direkt in der Anwendung Management schwerwiegender Sicherheits-Incidents verwalten und initiieren.

Als MSI-Manager können Sie die MSIM-Konferenzanrufintegration verwenden, um Microsoft Teams- , Cisco Webex - oder Zoom -Besprechungen zu initiieren. Integrieren Sie die Telefonkonferenz Management schwerwiegender Sicherheits-Incidents mit Drittpartei-Service Providern als Kommunikationskanal, um sich mit den Stakeholdern zu treffen und schwerwiegende Security Incidents zu lösen.

Schlüsselfunktionen

Die Integration der Major Security Incident Management-Telefonkonferenz bietet die folgenden wichtigen Funktionen:

- MSI-Manager können -Konferenzanrufe vom Microsoft TeamsTyp , Cisco Webexoder Zoom direkt von einem schwerwiegenden Security Incident aus initiieren.
- Laden Sie weitere Teilnehmer zum Anruf ein.
- Zeigen Sie Anrufaufzeichnungen und Chatdetails an.
- Sendet Einladungen per E-Mail und Microsoft Teams -Chat an Teilnehmer.

Konferenzanruf starten

Starten Sie eine Telefonkonferenz über eine Aufgabe oder einen schwerwiegenden Sicherheitsrisiko, indem Sie einen oder mehrere Benutzer zur Teilnahme an der Telefonkonferenz einladen. Die Telefonkonferenz wird nur gestartet, wenn mindestens zwei Teilnehmer beitreten.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

Stellen Sie sicher, dass Sie in der Instanz ServiceNow® Folgendes getan haben:

- Das Plugin Notify (com.snc.notify) muss installiert und aktiviert sein.
- Die App Notify UI Components for Configurable Workspaces wurde installiert.
- Das Plugin „Visuelle Aufgabentafel“ (com.devsnc.snb_vtb) ist installiert und aktiviert.

Weitere Informationen finden Sie unter IntegrationHub anfordern .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

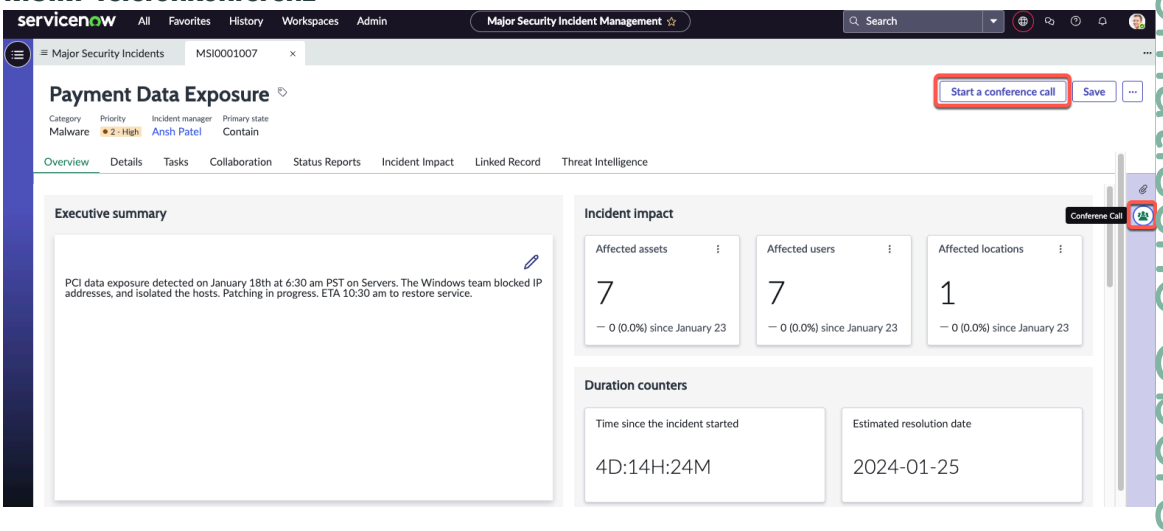
Die Teilnehmer des Anrufs können sein:

- Benutzer, denen bestimmte Verantwortlichkeiten zugewiesen wurden.
- Ad-hoc- oder On-Demand-Kontakte
- Andere Drittparteikontakte

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste Schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Wählen Sie die Aktion **Eine Telefonkonferenz starten aus**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü das Symbol und dann das Symbol + auswählen.
   Das Popup-Fenster Telefonkonferenz starten wird angezeigt.

MSIM-Telefonkonferenz



5. Wählen Sie im Feld Konferenzbrücke eine **Konferenzbrücke** aus, über die Sie eine Verbindung herstellen möchten.
   Zum Beispiel Microsoft Team, Zoom oder Cisco Webex.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Telefonkonferenz beschreibt.
7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Telefonkonferenz aus.
   Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der **Empfehlungsliste** auswählen, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.

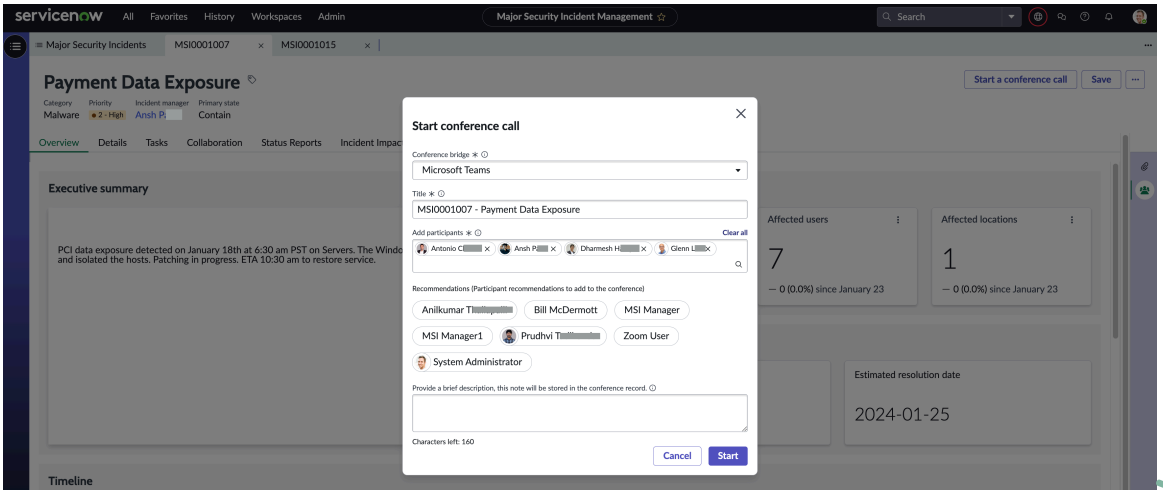
   Der Benutzer (Host), der die Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Benutzer, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig in der **Empfehlungsliste** verfügbar.

Hinweis:
Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer eine gültige E-Mail-Adresse haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konferenzanruf starten



8. Nachdem Sie die Teilnehmer ausgewählt haben, beschreiben Sie im Feld Beschreibung kurz den Grund für den Start der Telefonkonferenz.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie **Start**aus.
   Die Telefonkonferenz beginnt in der ausgewählten Konferenzbrücke. Alle Teilnehmer werden per E-Mail benachrichtigt und werden auch über die jeweils ausgewählte Konferenzbrücke benachrichtigt.
10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz teilzunehmen.
    Die Teilnehmer können den Link in der E-Mail-Benachrichtigung oder die Benachrichtigung in der ausgewählten Konferenzbrücke verwenden, um an der Konferenz teilzunehmen.
11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident, um die Details der Telefonkonferenz anzuzeigen.
    Wenn der letzte Teilnehmer die Konferenz verlässt, wird die Telefonkonferenz beendet, oder Sie wählen **Anruf beenden**, um sie zu beenden.

Einer Telefonkonferenz Teilnehmer hinzufügen

Fügen Sie einer Telefonkonferenz mithilfe der Suchoption im **Popup-Fenster Telefonkonferenz starten** Teilnehmer hinzu, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen. Sie können Teilnehmer auch hinzufügen, indem Sie die Teilnehmer aus der Empfehlungsliste auswählen, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Warum und wann dieser Vorgang ausgeführt wird

Der Benutzer (Host), der die Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Benutzer, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig in der Empfehlungsliste verfügbar.

Die Teilnehmer des Anrufs können sein:

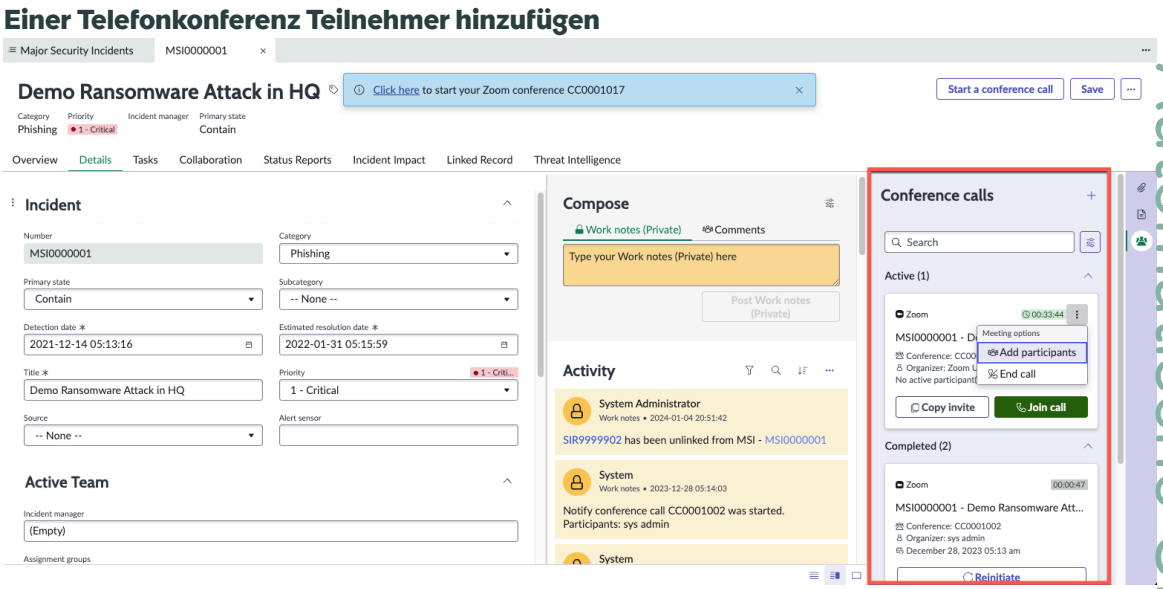
- Benutzer, denen bestimmte Verantwortlichkeiten zugewiesen wurden.
- Ad-hoc- oder On-Demand-Kontakte
- Andere Drittparteikontakte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie im Kontextmenü mit der rechten Maustaste das Symbol aus, um die Detailinformationen zu den Telefonkonferenzen anzuzeigen.
   Dies umfasst Details wie Name der Konferenzbrücke, Name des Organisators, Datum, Uhrzeit, Dauer des Anrufs, aktive und inaktive Teilnehmer.
4. Wählen Sie neben der aktiven Telefonkonferenz und anschließend **Teilnehmer hinzufügen**.



5. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der **Empfehlungsliste** auswählen, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.
6. Nachdem Sie die Teilnehmer ausgewählt haben, beschreiben Sie im Feld Beschreibung kurz den Grund für den Start der Telefonkonferenz.
   Alle Teilnehmer werden per E-Mail benachrichtigt und werden auch über die jeweils ausgewählte Konferenzbrücke benachrichtigt. Die Teilnehmer können den Link in der E-Mail-Benachrichtigung oder die Benachrichtigung in der ausgewählten Konferenzbrücke verwenden, um an der Konferenz teilzunehmen.
7. Alternativ können Sie Teilnehmer hinzufügen, indem Sie im Abschnitt „Telefonkonferenzen“ im rechten Kontextmenü die Option **Einladung kopieren** auswählen, und Sie können die Freigabe für die erforderlichen Teilnehmer freigeben.

Schalten Sie Teilnehmer in einer Telefonkonferenz stumm

Als MSI-Manager oder Host einer Telefonkonferenz haben Sie die Möglichkeit, einen bestimmten Teilnehmer oder alle Teilnehmer der Telefonkonferenz stummzuschalten.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Stellen Sie vor dem Starten dieses Verfahrens sicher, dass eine aktive Telefonkonferenz mit mindestens einem Teilnehmer vorhanden ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie im Kontextmenü mit der rechten Maustaste das Symbol aus, um die Detailinformationen zu den Telefonkonferenzen anzuzeigen.
4. Wählen Sie auf der aktiven Konferenzbrücke **Anruf beitreten** aus.
5. Nachdem Sie der Telefonkonferenz beigetreten sind, wählen Sie einen Teilnehmer aus, den Sie stummschalten möchten, und wählen Sie auf der Konferenzbrücke **Stumm**.
6. Um alle Teilnehmer der Telefonkonferenz stummzuschalten, wählen Sie in den Besprechungssteuerelementen **Teilnehmer** und dann **Alle stummschalten**aus.

Zeigen Sie Details zur Telefonkonferenz an

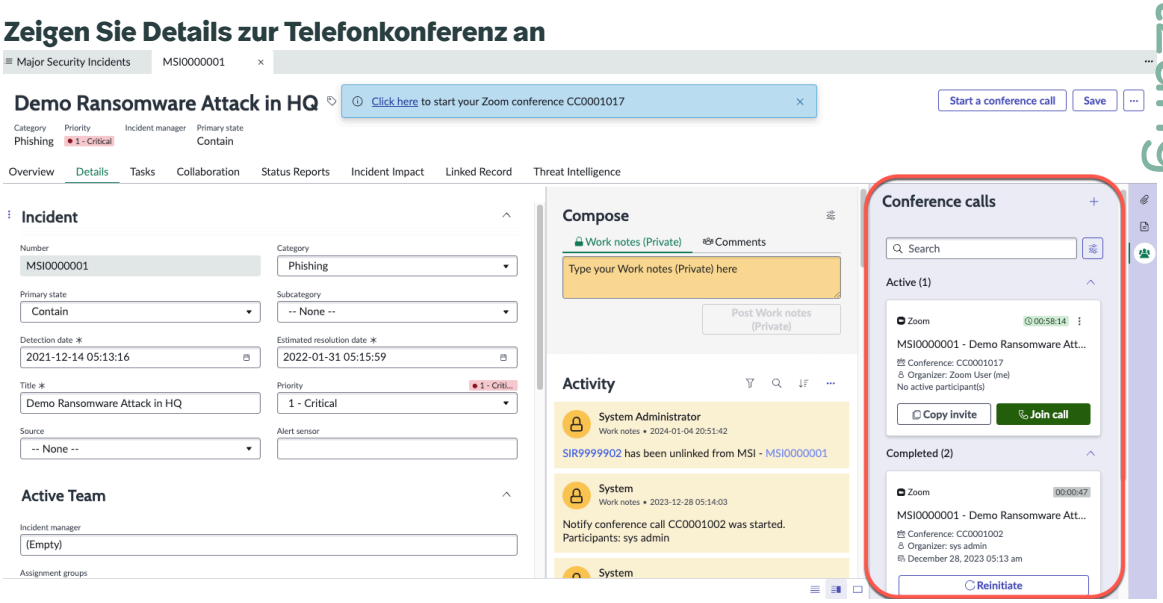
Telefonkonferenzen werden als Systemaktivitäten im Abschnitt „Aktivität“ des schwerwiegenden Security Incident und auch in der zugehörigen Liste „Telefonkonferenzen“ aufgeführt. Sie können Details wie Name der Konferenzbrücke, Name des Organisators, Datum, Uhrzeit, Dauer des Anrufs sowie aktive und inaktive Teilnehmer anzeigen.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie im Kontextmenü mit der rechten Maustaste das Symbol aus, um die Detailinformationen zu den Telefonkonferenzen anzuzeigen.
   Dies umfasst Details wie Name der Konferenzbrücke, Name des Organisators, Datum, Uhrzeit, Dauer des Anrufs, aktive und inaktive Teilnehmer.



4. Mit der Suchoption können Sie nach einer bestimmten Telefonkonferenz suchen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es kann mehrere Anrufe für denselben schwerwiegenden Security Incident geben.

5. Um einer Telefonkonferenz Teilnehmer hinzuzufügen, wählen Sie neben der aktiven Telefonkonferenz und anschließend die Option **Teilnehmer hinzufügen** aus.
6. Sie können Teilnehmer auch hinzufügen, indem Sie die Option **Einladung kopieren** verwenden und den Link für die erforderlichen Teilnehmer freigeben.
7. Um an einer Telefonkonferenz teilzunehmen, navigieren Sie zum Abschnitt „Aktiv“, und wählen Sie die Option **An Anruf teilnehmen** für die gewünschte Telefonkonferenz aus.
8. Um eine Telefonkonferenz zu beenden, wählen Sie neben der aktiven Telefonkonferenz und dann die Option **Anruf beenden** aus.
9. Um eine Telefonkonferenz neu zu starten, navigieren Sie zum Abschnitt Abgeschlossen und wählen Sie die Option **Erneut initiieren** für die gewünschte Telefonkonferenz aus.

Integrieren Sie MSIM-Telefonkonferenzen in Microsoft Teams

Mit der Telefonkonferenz Microsoft Teams -Integration können Sie eine Microsoft Teams -Telefonkonferenz direkt in einem schwerwiegenden Security Incident verwalten und initiieren.

Schlüsselfunktionen

- Starten und beenden Sie Telefonkonferenzen Microsoft Teams direkt über schwerwiegende Security Incidents oder Aufgaben in der Workbench für schwerwiegende Security.
- Verwalten Sie eine Microsoft Teams -Telefonkonferenz durch Hinzufügen oder Entfernen von Teilnehmern.

Voraussetzungen

Vergewissern Sie sich, dass die folgenden IntegrationHub -Plugins in Ihrer ServiceNow -Instanz installiert sind.

- Notify Plugin (com.snc.notify)
- Microsoft Teams Kommunikations-Spoke-Plugin (sn_msteams_com_spk).
- Azure Active Directory User Mapping-Plugin (sn_now_azure).
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Weitere Informationen finden Sie unter IntegrationHub anfordern .

Konfiguration

- Informationen zur Konfiguration der MSIM-Telefonkonferenz Microsoft Teams -Integration mit der vorkonfigurierten App finden Sie unter Integrate Notify connector pre-published app with Microsoft Teams .
- Informationen zur Konfiguration der MSIM-Telefonkonferenz Microsoft Teams -Integration mit der selbstkonfigurierten App finden Sie unter Integrating Notify connector self-configured app with Microsoft Teams .

Verwenden Sie die MSIM-Telefonkonferenz Microsoft Teams -Integration

Die folgenden Schritte zeigen Ihnen, wie Sie eine Telefonkonferenz Microsoft Teams direkt von einem schwerwiegenden Security Incident aus verwalten und initiieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

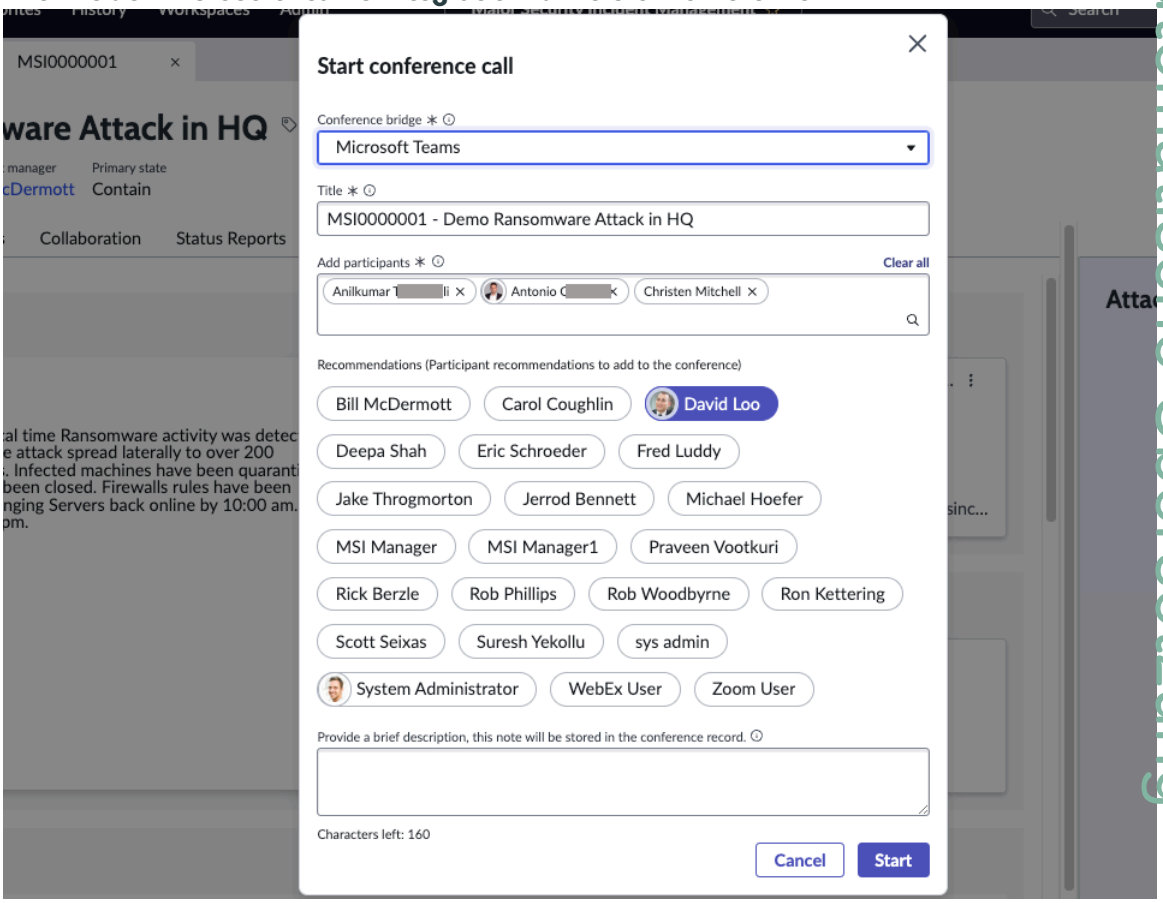
Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste Schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Wählen Sie die Aktion **Eine Telefonkonferenz starten aus**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü das Symbol und dann das Symbol + wählen.
   Das Popup-Fenster Telefonkonferenz starten wird angezeigt.
5. Wählen Sie **Microsoft Teams** als Konferenzbrücke aus, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Microsoft Teams-Telefonkonferenz beschreibt.

Mithilfe der Microsoft Teams-Integration für Telefonkonferenzen



7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Microsoft Teams-Telefonkonferenz aus. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der **Empfehlungsliste** auswählen, die Teilnehmerempfehlungen zum Hinzufügen zur Microsoft Teams-Telefonkonferenz enthält.

   Der Benutzer (Host), der die Microsoft Teams-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Benutzer, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig in der **Empfehlungsliste** verfügbar.

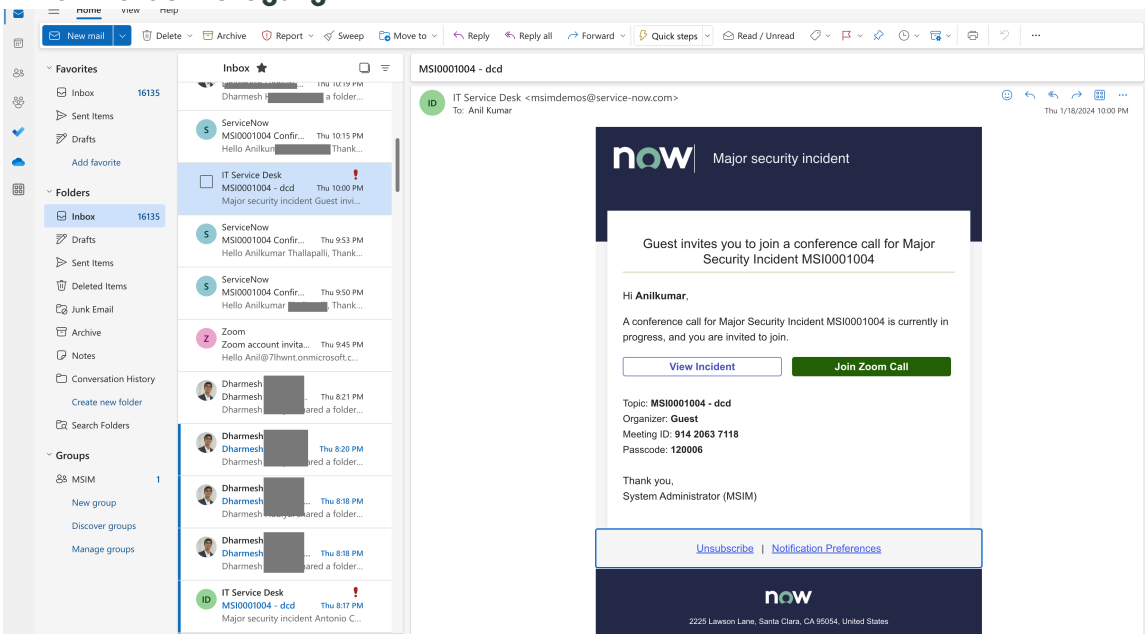
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer eine gültige E-Mail-Adresse haben.

8. Nachdem Sie die Teilnehmer ausgewählt haben, beschreiben Sie im Feld Beschreibung kurz den Grund für den Start der Telefonkonferenz.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie **Start**aus.
   Die Telefonkonferenz wird in der Microsoft Teams-App gestartet. Alle Teilnehmer werden per E-Mail von der MSIM-App benachrichtigt, und die andere Benachrichtigung wird über einen Bot in der Microsoft Teams-App gesendet.
10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz in der Microsoft Teams-App teilzunehmen.
    Die Teilnehmer können den Link in der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung in der Microsoft Teams-App verwenden, um an der Konferenz teilzunehmen.

E-Mail-Benachrichtigung



11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Details der Telefonkonferenz anzuzeigen.

    Wenn der letzte Teilnehmer den Anruf verlässt, wird der Konferenzanruf beendet, oder Sie wählen **Anruf beenden** im Abschnitt Telefonkonferenz, um den Konferenzanruf zu beenden.

Integrieren Sie MSIM-Telefonkonferenzen in Zoom

Mit der Telefonkonferenz Zoom -Integration können Sie eine Zoom -Telefonkonferenz direkt in einem schwerwiegenden Security Incident verwalten und initiieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

- Starten und beenden Sie Zoom Meetings direkt in einem beliebigen Aufgabendatensatz, z. B. bei einem schwerwiegenden Security Incident oder einem Change, oder sogar in der Workbench für schwerwiegende Incidents.
- Verwalten Sie Zoom Meetings durch Hinzufügen oder Entfernen von Teilnehmern.
- Verfolgen und melden Sie Besprechungsdetails wie Besprechungsdauer und Teilnehmer zur weiteren Analyse.

Voraussetzungen

Vergewissern Sie sich, dass die folgenden IntegrationHub -Plugins in Ihrer ServiceNow -Instanz installiert sind.

- Notify Plugin (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)
- Notify Zoom (sn_notify_zoom)
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Weitere Informationen finden Sie unter IntegrationHub anfordern .

Konfiguration

Informationen zur Konfiguration der MSIM-Telefonkonferenz Zoom -Integration über den Kommunikationskanal Notify finden Sie unter Configure Notify Zoom connector in Notify .

Verwenden Sie die MSIM-Telefonkonferenz Zoom -Integration

Die folgenden Schritte zeigen Ihnen, wie Sie eine Telefonkonferenz Zoom direkt von einem schwerwiegenden Security Incident aus verwalten und initiieren können.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

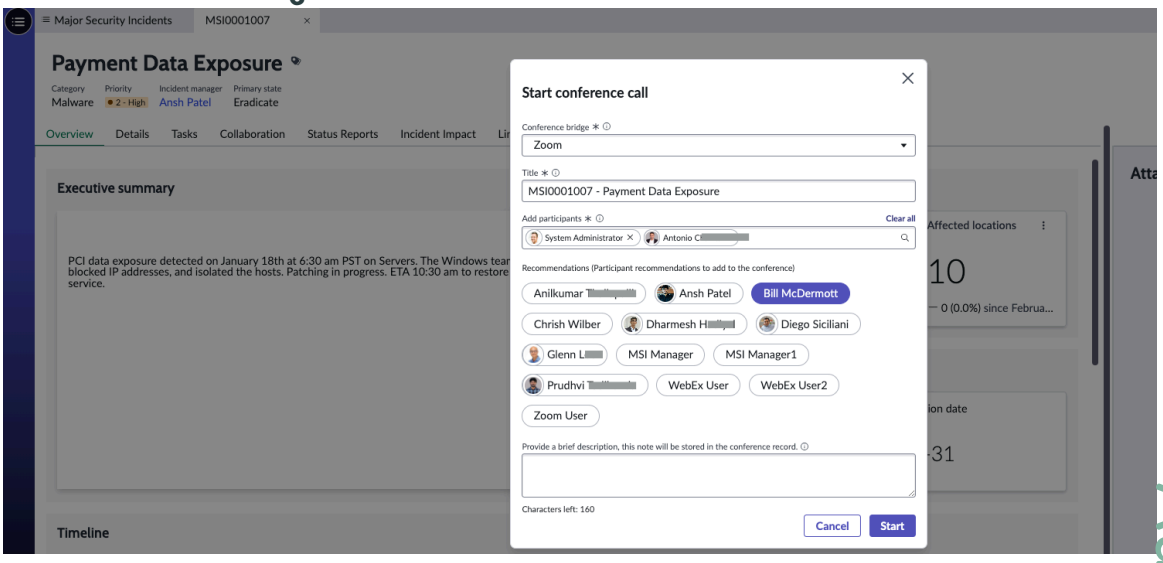
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste Schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Klicken Sie auf **die Aktion Telefonkonferenz starten**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü auf das Symbol klicken und das Symbol + auswählen.
   Das Popup-Fenster Telefonkonferenz starten wird angezeigt.
5. Wählen Sie **Zoom** als Konferenzbrücke aus, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Zoom-Telefonkonferenz beschreibt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mithilfe der Zoom-Integration für Telefonkonferenzen



7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Zoom-Telefonkonferenz aus.
   Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der **Empfehlungsliste** auswählen, die Teilnehmerempfehlungen zum Hinzufügen zur Zoom-Telefonkonferenz enthält.

   Der Benutzer (Host), der die Zoom-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Benutzer, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig in der **Empfehlungsliste** verfügbar.

   Hinweis:
   Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer eine gültige E-Mail-Adresse haben.

8. Nachdem Sie die Teilnehmer ausgewählt haben, beschreiben Sie im Feld Beschreibung kurz den Grund für den Start der Telefonkonferenz.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.

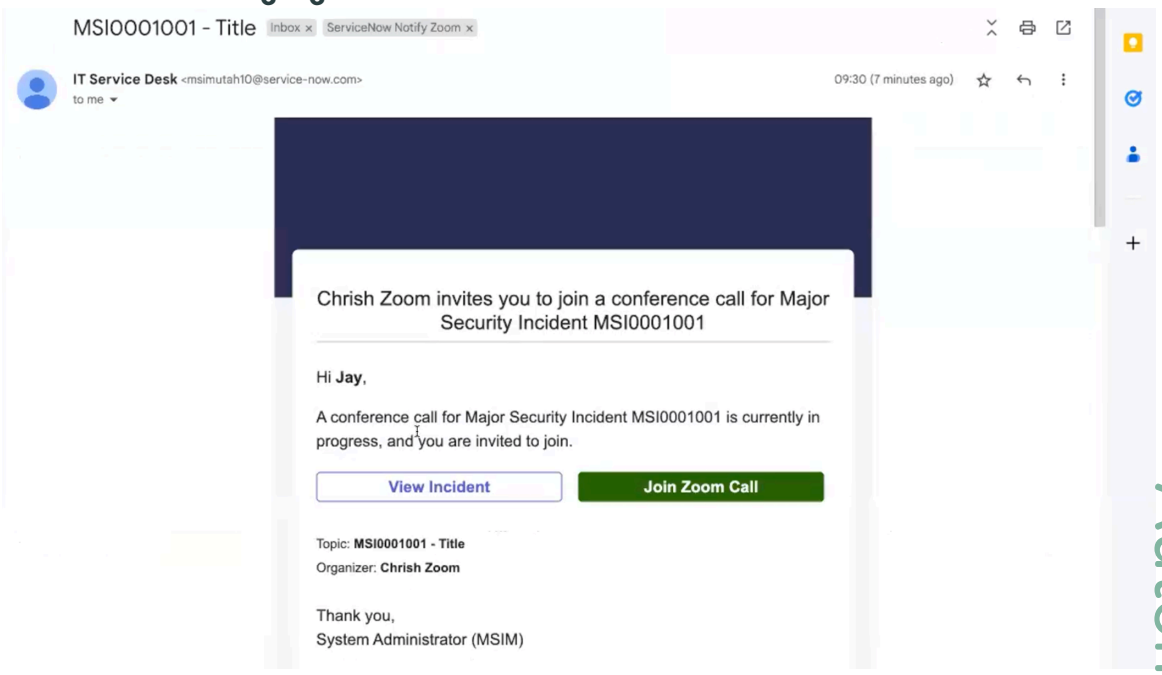
9. Nachdem die Teilnehmerliste abgeschlossen wurde, klicken Sie auf **Start**.
   Die Telefonkonferenz wird in der Zoom-App gestartet. Alle Teilnehmer werden durch zwei E-Mails benachrichtigt: Eine E-Mail wird über die MSIM-App an die Teilnehmer gesendet und die andere E-Mail wird von der Zoom-Konferenzbrücke gesendet.

10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz in der Zoom-App teilzunehmen.
    Die Teilnehmer können den Link in der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung in der Zoom-App verwenden, um an der Konferenz teilzunehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Benachrichtigung



11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Details der Telefonkonferenz anzuzeigen.

    Wenn der letzte Teilnehmer den Anruf verlässt, wird der Konferenzanruf beendet, oder Sie wählen **Anruf beenden** im Abschnitt Telefonkonferenz, um den Konferenzanruf zu beenden.

    Wenn die Telefonkonferenz aufgezeichnet wurde, ist die Aufzeichnung nach einiger Zeit im Abschnitt Telefonkonferenz des zugehörigen schwerwiegenden Security Incident verfügbar.

Integrieren Sie MSIM-Telefonkonferenzen in Cisco Webex

Mit der MSIM-Telefonkonferenz Cisco Webex -Integration können Sie eine Cisco Webex -Telefonkonferenz direkt in einem schwerwiegenden Security Incident verwalten und initiieren.

Schlüsselfunktionen

- Starten und beenden Sie Cisco Webex Meetings direkt in schwerwiegenden Security Incidents.
- Verwalten Sie ein Meeting Cisco Webex durch Hinzufügen oder Entfernen von Teilnehmern.

Voraussetzungen

Vergewissern Sie sich, dass die folgenden IntegrationHub -Plugins in Ihrer ServiceNow -Instanz installiert sind.

- Notify Plugin (com.snc.notify)
- Notify Cisco Webex Connector (sn_notify_webex)
- Cisco Webex Teams-Spoke (sn_cisco_teams_spk)
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter IntegrationHub anfordern .

Konfiguration

Informationen zur Konfiguration der MSIM-Telefonkonferenz Cisco Webex -Integration über den Kommunikationskanal Notify finden Sie unter Configure Notify Cisco Webex Connector .

Verwenden Sie die -Telefonkonferenzen -Integration Cisco Webex .

Die folgenden Schritte zeigen Ihnen, wie Sie eine Telefonkonferenz Cisco Webex direkt von einem schwerwiegenden Security Incident aus verwalten und initiieren können.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

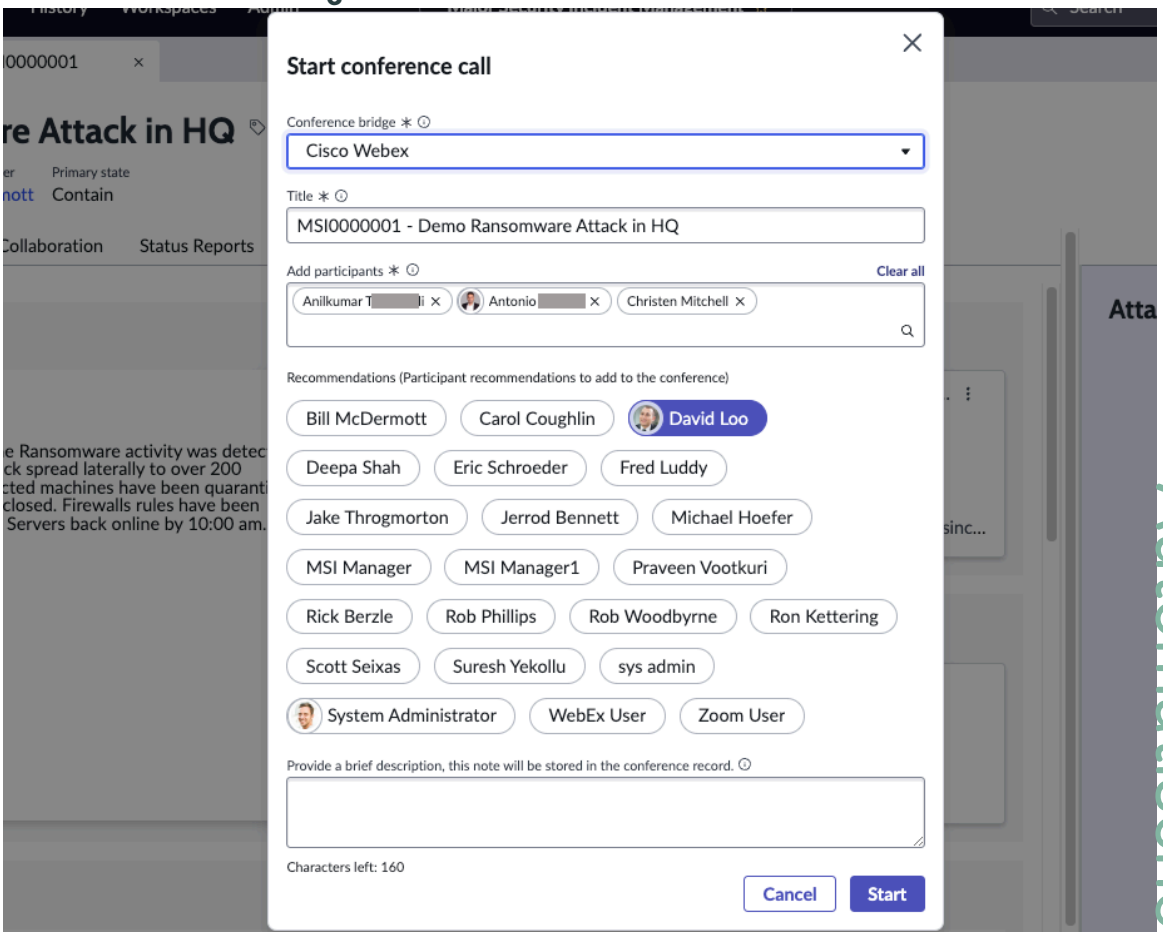
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste Schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Wählen Sie die Aktion **Eine Telefonkonferenz starten aus**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü das Symbol und dann das Symbol + auswählen.
   Das Popup-Fenster Telefonkonferenz starten wird angezeigt.
5. Wählen Sie **Cisco Webex** als Konferenzbrücke aus, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Cisco Webex-Telefonkonferenz beschreibt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit der Cisco Webex-Integration für Telefonkonferenzen



7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Cisco Webex-Telefonkonferenz aus. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der **Empfehlungsliste** auswählen, die Teilnehmerempfehlungen zum Hinzufügen zur Cisco Webex-Telefonkonferenz enthält.

   Der Benutzer (Host), der die Cisco Webex-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Benutzer, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig in der **Empfehlungsliste** verfügbar.

   Hinweis:
   Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer eine gültige E-Mail-Adresse haben.

8. Nachdem Sie die Teilnehmer ausgewählt haben, beschreiben Sie im Feld Beschreibung kurz den Grund für den Start der Telefonkonferenz.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.

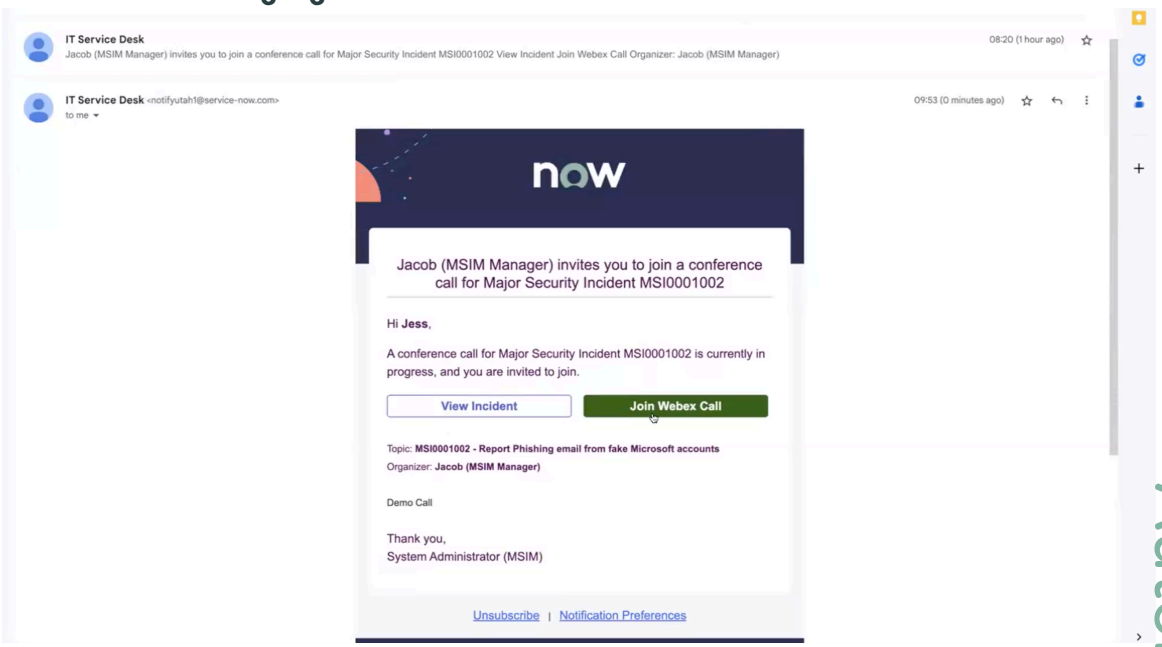
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie **Start**aus.
   Die Telefonkonferenz wird in der Cisco Webex-App gestartet. Alle Teilnehmer werden durch zwei E-Mails benachrichtigt: Eine E-Mail wird über die MSIM-App an die Teilnehmer gesendet und die andere E-Mail wird von der Cisco Webex-Konferenzbrücke gesendet.

10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz in der Cisco Webex-App teilzunehmen.
    Die Teilnehmer können den Link in der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung in der Cisco Webex-App verwenden, um an der Konferenz teilzunehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Benachrichtigung



11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Details der Telefonkonferenz anzuzeigen.

    Wenn der letzte Teilnehmer den Anruf verlässt, wird der Konferenzanruf beendet, oder Sie wählen **Anruf beenden** im Abschnitt Telefonkonferenz, um den Konferenzanruf zu beenden.

    Wenn die Telefonkonferenz aufgezeichnet wurde, ist die Aufzeichnung nach einiger Zeit im Abschnitt Telefonkonferenz des zugehörigen schwerwiegenden Security Incident verfügbar.

Management schwerwiegender Sicherheits-Incidents konfigurieren

Installieren und konfigurieren Sie die Anwendung Management schwerwiegender Sicherheits-Incidents.

Wichtig:

- Um schnell mit der Konfiguration von Management schwerwiegender Sicherheits-Incidents zu beginnen, lesen Sie den Schnellstartleitfaden für Major Security Incident Management (MSIM) im ServiceNow Store.
- Stellen Sie nach der Installation der App Management schwerwiegender Sicherheits-Incidents sicher, dass Sie das Update Set in KB1289784 importieren, um die teilweise vorkonfigurierten Dateien zu laden.

In diesem Abschnitt erfahren Sie, wie Sie die erforderlichen Konfigurationen einrichten, die für die Arbeit mit Major Security Incident -Datensätzen durch die Integration mit anderen externen MicrosoftMicrosoft Azure Event Hubs -Anwendungen erforderlich sind, um Verbindungen mit der Instanz ServiceNow herzustellen.

Konfigurieren Sie die Datei-Explorer-Komponente

Die Komponente „File Explorer-Arbeitsbereich“ organisiert und verfolgt die Sammlung von Artefakten (Dateien), die sich auf einen schwerwiegenden Security Incident beziehen. Es

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

unterstützt die Integration mit jedem Dateihosting-Anbieter einer Drittpartei, z. B. Microsoft SharePoint im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents.

- File Explorer Komponente: Stellt eine grafische Anwenderoberfläche zum Anzeigen des Dateisystems bereit und ermöglicht den Anwendern das Ausführen von Dateivorgängen.
- File Explorer Core: Stellt eine Abstraktionsschicht bereit, die es der Datei-Explorer-Komponente ermöglicht, das Dateisystem anzuzeigen und verschiedene Dateivorgänge auszuführen, ohne etwas über den zugrunde liegenden Connector zu wissen, der für die Kommunikation mit externen Repositorys verwendet wird.
- File Explorer Microsoft SharePoint Connector-Anwendung: Stellt die Implementierungsmodule bereit, die zum Nachverfolgen und Abrufen von Dateien/Ordnermetadaten aus einer Microsoft SharePoint -Dokumentbibliothek und zum Ausführen von Dateivorgängen erforderlich sind.

Die Komponente File Explorer Core bietet eine Basisinfrastruktur, die für die verschiedenen Connector-Anwendungen für die Dateifreigabe erforderlich ist, um ihre Verbindungseigenschaften zu definieren.

Sie müssen das Datei-Repository-Laufwerk und den Datei-Repository-Provider installieren und konfigurieren, indem Sie die Verbindungseigenschaften hinzufügen, um die Datei-Metadaten von einem Datei-Hosting-Provider-Speicherort abzurufen.

Für die aktuelle Version von File Explorerumfassen diese Anweisungen das Konfigurieren und Abonnieren einer Datei zum Abrufen von -Metadaten wie z. B. Microsoft SharePoint Datei- und Ordneraktualisierungen, Dateivorgänge und Protokollierung der Dateiaktivität. Eine bestimmte Microsoft SharePoint -Dokumentbibliothek und eine zugehörige Laufwerkskonfiguration sind erforderlich, um einzelne Ordner zu erstellen, die für schwerwiegende Security Incidents spezifisch sind.

File Explorer ermöglicht auch Connector-Anwendungen wie Microsoft SharePoint. Sie können dieses Beispiel verwenden, um die Implementierungen von Dateivorgängen zu konfigurieren, z. B. **Herunterladen** oder **Umbenennen** Ordner- und Dateiaktionen werden in der Komponente des Datei-Explorer-Arbeitsbereichs aktiviert. Diese Aktionen werden mit den integrierten Flow Designer-Subflows aktiviert und ausgeführt. Weitere Informationen finden Sie unter Einstellungen für Ordner- und Dateiaktionen.

File Explorer Die -Konfiguration enthält das folgende Setup:

- Konfigurieren Sie das Laufwerk des Datei-Explorers Repository
- Konfigurieren Sie die Aktionseinstellungen für Ordner und Dateien
- Erstellen Sie Ordnervorlagen

Erste Schritte mit dem Datei-Explorer

Lesen Sie sich die folgenden Informationen durch, bevor Sie die Arbeit mit der Komponente File Explorer beginnen.

Lesen Sie sich die folgenden Informationen durch, bevor Sie die Verbindung mit Microsoft SharePointherstellen, Ordner- und Dateiaktionen erstellen und Ordnervorlagen für die Datei-Explorer-Komponente erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Name	Beschreibung
Microsoft SharePoint -Spoke, Version 2.0.2 für ServiceNow® IntegrationHub.	Verwenden Sie die Plugin-ID **sn_sp_spoke**, um Microsoft SharePoint die -Spoke zu suchen und zu installieren. Durch die Installation dieses Plugins werden Flows und Aktionen zur Automatisierung der Zusammenarbeit, der Dokumentenverwaltung und von Anwenderzugriffsrechten in Microsoft SharePointbereitgestellt.
Datei-Explorer-Komponente v1.1.0	Verwenden Sie die Plugin-ID **sn_file_explorer**, um die Datei-Explorer-Komponente v1.1.0 zu suchen und zu installieren Wenn Sie dieses Plugin installieren, wird eine grafische Benutzeroberfläche zum Durchsuchen des Dateisystems bereitgestellt, das im Datei-Explorer-Core verfügbar ist.
File Explorer Core for Security Operations v1.1.1	Verwenden Sie die Plugin-ID **sn_fe**, um Datei-Explorer Core zu suchen und zu installieren. Durch die Installation dieses Plugins wird eine Basisinfrastruktur für die Integration mit jedem Datei-Hosting-Drittanbieter bereitgestellt.
Microsoft SharePoint File Explorer Connector for Security Operations v1.1.1	Verwenden Sie die Plugin-ID **sn_fe_sharepoint**, um Microsoft SharePoint den File Explorer Connector zu suchen und zu installieren. Durch die Installation dieses Plugins werden die Microsoft SharePoint -Dateien/-Ordner mit dem Datei-Explorer verwaltet.

Konfigurieren Sie das Laufwerk des Datei-Explorers Repository

Der Connector Microsoft SharePoint bietet verschiedene Funktionen, die in den Datei-Explorer-Funktionen Microsoft SharePoint von implementiert werden, indem die Dateimetadaten verwaltet und nachverfolgt werden.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Schwerwiegender Security Incident** > **Dateiexplorer** > **Datei-Repository-Konfiguration**.
2. Füllen Sie die folgenden Felder wie in der folgenden Tabelle beschrieben aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

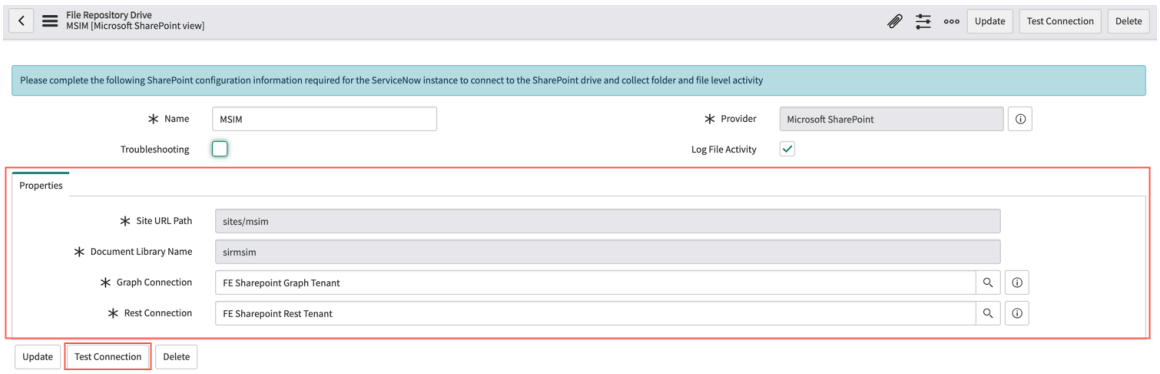
Feldname	Feldbeschreibung
Name	Name des Datei-Repository-Datensatzes, der die Verwendung identifiziert. Beispiel: MSIM.
Anbieter	Name des Anbieters, der die Drittpartei-Datei-Hosting-Repository-Anbieter ist. Beispiel:Microsoft SharePoint.
Eigenschaften	
Website-URL-Pfad	Geben Sie eine URL Microsoft SharePoint mit einem bestimmten Websitepfad ein. Geben Sie nur den relativen Pfad zur Site an. Eine vollständige Site-URL ist möglicherweise nicht erforderlich. Beispiel: Sites/MSIM.
Name der Dokumentbibliothek	Erstellen Sie eine Dokumentbibliothek unter der Website Microsoft SharePoint, und geben Sie hier den Namen der gleichen Dokumentbibliothek an. Dies ist dieselbe Dokumentbibliothek, die Sie im Setup des Microsoft SharePoint Connector-Laufwerks erstellt haben.
Graph-Verbindung	Wählen Sie den Datensatz des Datei-Explorer-Graph-Mandanten aus. Weitere Informationen zur Konfiguration der Mandantenverbindung finden Sie unter Microsoft SharePoint-Spoke.
REST-Verbindung	Wählen Sie den REST-Mandantendatensatz des Datei-Explorers aus. Weitere Informationen zur Konfiguration der Mandantenverbindung finden Sie unter Microsoft SharePoint-Spoke.

3. Wählen Sie **Speichern**.
4. Klicken **Testverbindung** Registerkarte zum Testen der Verbindung und Validieren der Konfigurationseigenschaften des Datei-Repository-Laufwerks.

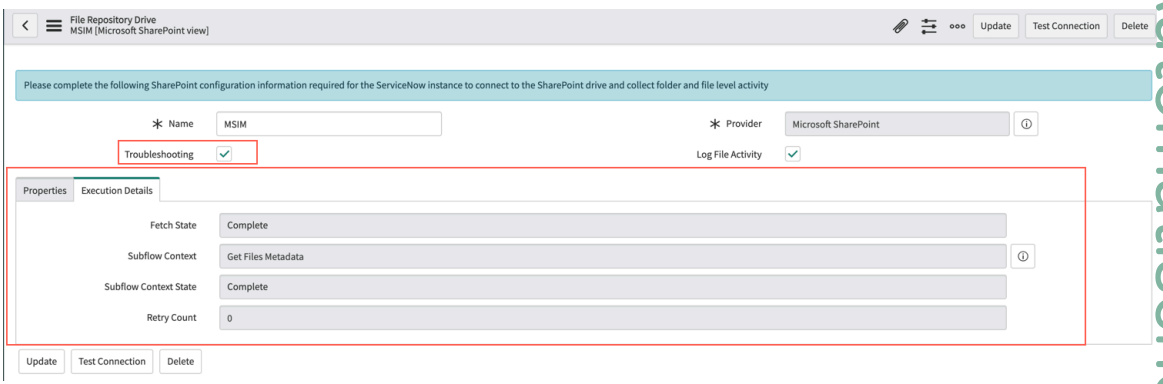
   Hinweis:
   Stellen Sie vor **der Aktivierung** des Datei-Repositorys sicher, dass die entsprechende Dokumentbibliothek unter Microsoft SharePoint keine Ordner- oder Dateidaten enthält.

5. Klicken Sie auf **Aktivieren**, um das Datei-Repository zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Aktivieren Sie das Kontrollkästchen **Problembehandlung**, um die **Ausführungsdetails** des Datei-Repositorys zu überprüfen, und überprüfen Sie **Status abrufen** ist abgeschlossen. Stellen Sie sicher, dass die Laufwerksabonnements Microsoft SharePoint erstellt wurden und der Status „Abgeschlossen“ lautet.



Hinweis:
Mit der Schaltfläche **„Verbindung testen“** kann entweder der MSI-Administrator oder der MSI-Manager nur die Datei-Repository-Konfiguration validieren.

Konfigurieren Sie die Aktionseinstellungen für Ordner und Dateien

Ckonfigurieren die Aktionen für Ordner und Dateien, die aktiviert werden sollen, über die Komponente „Datei-Explorer“ im Arbeitsbereich „Major Security Incident Management“über die Setup-Seite „Einstellungen für Ordner- und Dateiaktionen“ . Als MSI-Administrator können Sie die einzelnen Ordner- und Dateiaktionen steuern, die in der Datei-Explorer-Komponente angezeigt werden.

Vorbereitungen

Im Folgenden finden Sie die implementierten Dateivorgangsfunktionen in der Datei-Explorer-Komponente mit dem Flow Designer ServiceNow® :

Funktionen für Dateivorgänge

Dateivorgang	Beschreibung
Öffnen Sie in Microsoft SharePoint	Öffnet eine neue Browserregisterkarte, um die Dateiansicht der Dokumentbibliothek Microsoft SharePoint anzuzeigen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen für Dateivorgänge (Fortsetzung)

Dateivorgang	Beschreibung
Ordner erstellen	Möglichkeit, zusätzliche Ad-hoc-Ordner zu erstellen, nachdem der schwerwiegende Security Incident erstellt wurde.
Ordner umbenennen	Möglichkeit zum Umbenennen der erstellten Ordner.
Datei verschieben	Ermöglicht das Verschieben von Dateien zwischen Ordnern in der Datei-Explorer-Komponente des Arbeitsbereichs, was zu einer Verschiebung von Dateien in führt Microsoft SharePoint
Datei suchen	Zeigt den Ordnerspeicherort bei Verwendung von an **Letzte** Ansicht des Datei-Explorers.
Datei löschen	Löschen Sie die Datei.
Ordner löschen	Löschen Sie den Ordner.
Datei herunterladen	Lädt die Datei auf der vorhandenen Browserregisterkarte des MSIM-Arbeitsbereichs herunter, um sie schnell anzuzeigen.
Datei umbenennen	Benennt die Datei um.

Hinweis:

1. Alle aufgelisteten Aktionen sind derzeit standardmäßig aktiviert. Sie müssen bearbeiten **Einstellungen für Dateiaktionen** wenn bestimmte Aktionen nicht angezeigt werden sollen. Alle Einstellungen sind derzeit für alle Anwender global, , was bedeutet, dass Aktionen für eine Teilmenge der Anwender mit einer bestimmten Rolle nicht aktiviert werden können.
2. **Anwenderzugriff widerrufen** und **Berechtigungen hinzufügen** -Aktionen sind systembezogene Aktionen. Es wird empfohlen, diese Dateiaktionen nicht zu ändern.

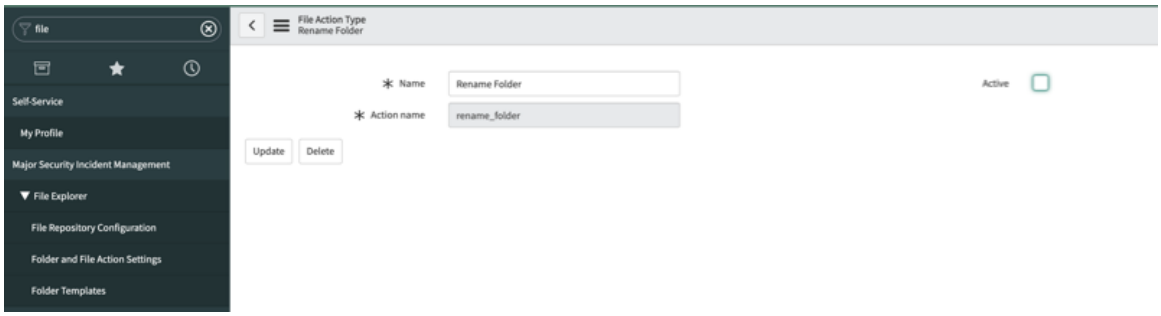
Das folgende Beispielverfahren beschreibt eine der Dateivorgänge-Funktionen mit denen] bestimmte Ordner- und Dateiaktionen während der Konfiguration des Datei-Explorer-Repositorys deaktivieren kann. Dieses Verfahren gilt für alle anderen Aktionen, die möglicherweise bearbeitet werden müssen:

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Dateiexplorer** > **Einstellungen für Ordner- und Dateiaktionen**.
2. Wählen Sie den gewünschten Datensatz aus, um die Ordner- bzw. Dateiaktion zu aktivieren bzw. zu deaktivieren.
3. Heben Sie die Auswahl von auf **Aktiv** Kontrollkästchen zum Deaktivieren der Ordner- und Dateiaktion.

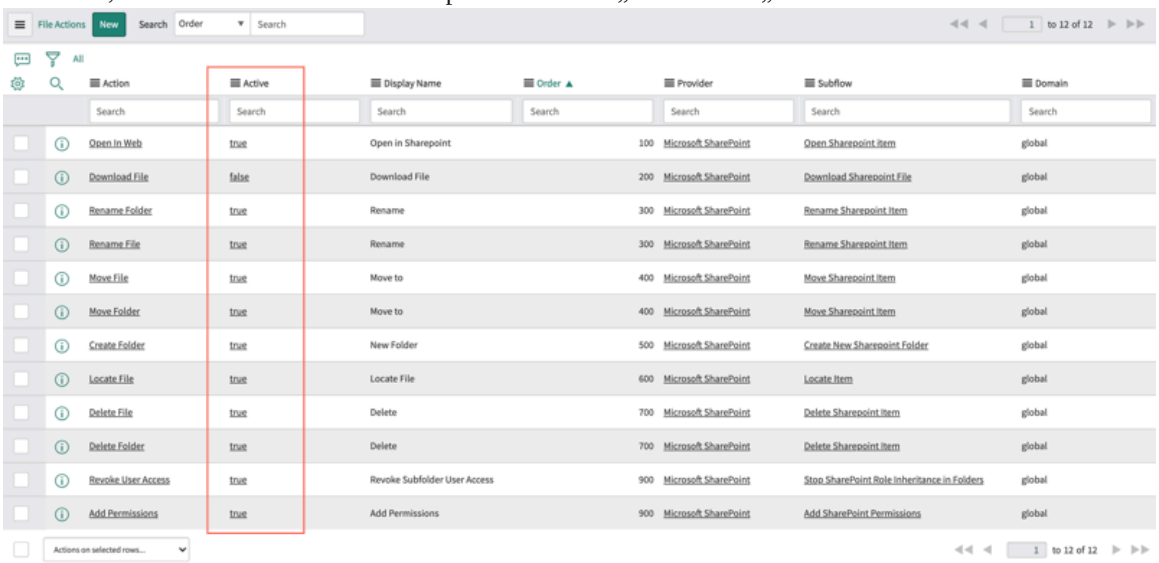
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



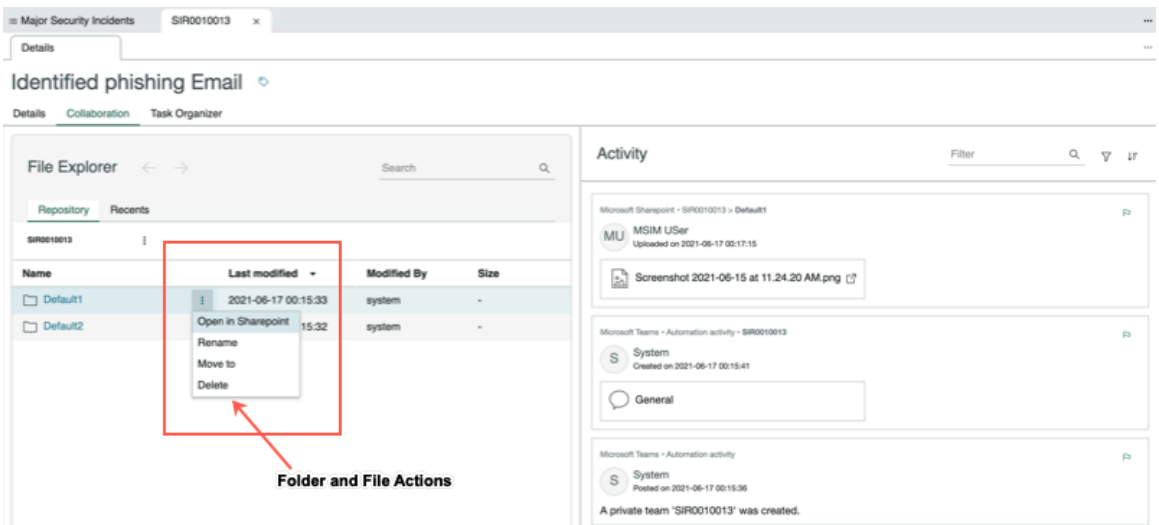
4. **Aktualisieren Sie** den Laufwerksdatensatz.

Hinweis:

Sie können die Dateiaktion auch direkt aus der Liste der angezeigten Dateivorgänge ausführen, indem Sie auswählen **Aktiv** Spaltenwerte auf „Wahr“ oder „Falsch“.



Wenn die ausgeführte Dateiaktion deaktiviert ist, wird die Aktion nicht unter angezeigt **Kollaborationen** Registerkarte von **Management schwerwiegender Sicherheits-Incidents** -Arbeitsbereich



Erstellen Sie Ordnervorlagen

Verwenden Sie Ordnervorlagen, um automatisch eindeutige Ordner für verschiedene Typen von schwerwiegenden Security Incidents zu erstellen. Die Ordnervorlagen in der Datei-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Explorer-Komponente werden verwendet, um eine Basisordnerstruktur für den Security Incident in Microsoft SharePointzu erstellen.

Vorbereitungen

Als MSI-Administrator definieren Sie die anfängliche Ordnerstruktur, die für die Zusammenarbeit zwischen verschiedenen Incident-Responder-Gruppen erforderlich ist, und weisen die entsprechenden Zugriffsrechte auf Unterordnerebene zu. Mehrere Konfigurationen können für verschiedene Major Security Incident -Typen mithilfe eines Bedingungsgenerators für bestimmte Major Security Incident -Feldwerte erstellt werden, einschließlich des Zugriffs für verschiedene Anwender und Anwendergruppen auf jeder Unterordnerebene.

Hinweis:
Diese Ordnervorlagen werden von allen schwerwiegenden Security Incidents verwendet, die die im Bedingungsgenerator angegebenen Bedingungen erfüllen. Es wird empfohlen, Incident-Feldvariablen zu verwenden, z. B. Incident-Nummer oder Kategorie, um eindeutige Stammordnernamen zu erstellen, die einen Satz von Unterordnern mit allgemeinen Ordnernamen für einen schwerwiegenden Security Incident von ähnlichen Ordnern mit diesen Namen unterscheiden, die Teil von sind einen anderen schwerwiegenden Security Incident.

Die definierte Konfiguration für Ordnervorlagen wird nur dann auf den schwerwiegenden Security Incident angewendet, wenn die Bedingung erfüllt ist.

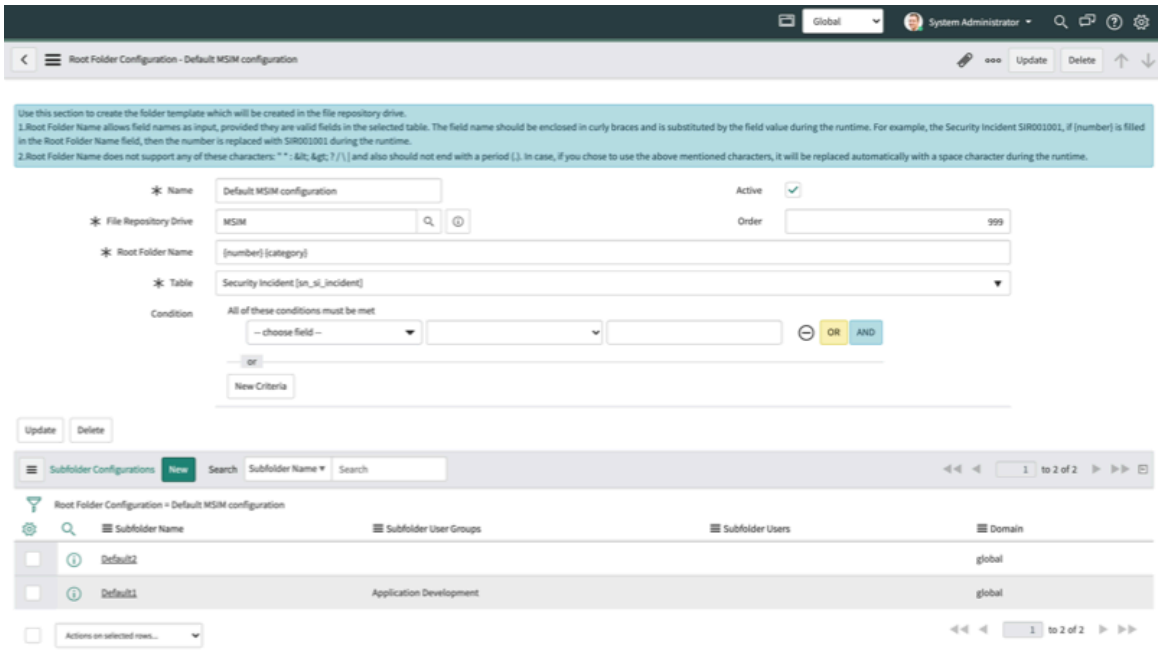
Hinweis:
Eine Basissystemkonfiguration (ohne Unterordner) wird auf alle Security Incidents angewendet. Sie können entweder diese Standardkonfiguration bearbeiten, um bestimmte Unterordner einzubeziehen, oder eine neue Konfiguration basierend auf einem angegebenen Satz von Feldwerten für schwerwiegende Security Incidents erstellen. Beispiel: Kategorie = Aktivität böswilliger Codes.

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

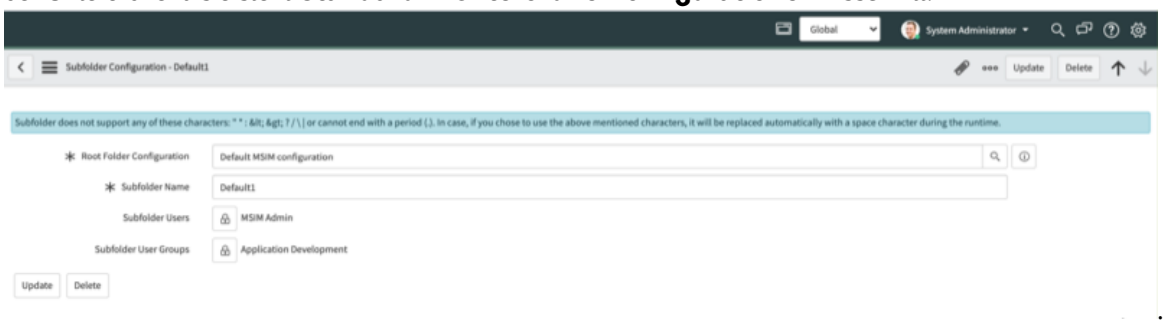
1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Dateiexplorer** > **Ordnervorlagen**.
2. Klicken **Neu** für die Stammordnerkonfiguration.
3. Füllen Sie die Felder im Formular aus.
4. Definieren Sie den Security Incident **Bedingung** Werte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. **Aktualisieren** den Datensatz.
   Die Unterordner werden mit den definierten Werten erstellt.

6. Klicken Sie auf den gewünschten **Unterordner**.
   Wenn Sie keinen Unterordner mit einem entsprechenden Namen erstellen, werden die Namen der Unterordner als erstellt **Standard** in **Unterordnerkonfigurationen** Abschnitt.



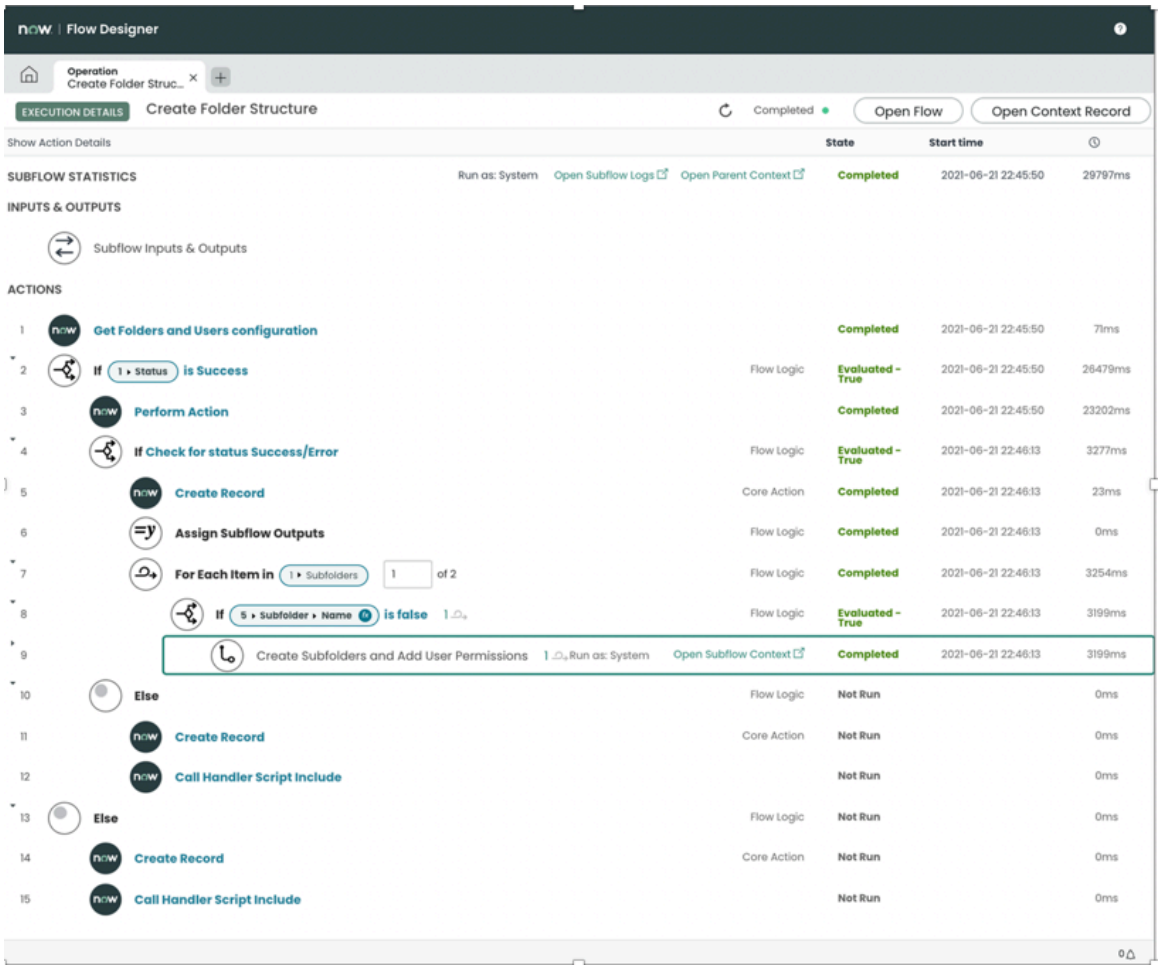
Dieselbe Ordnerstruktur wird automatisch in Microsoft SharePoint mit denselben Zugriffsrechten erstellt, die im konfiguriert sind **Ordnervorlagen** Seite.

Hinweis:

- **Stammordnername** ermöglicht Feldvariablennamen als Eingabe, sofern es sich um gültige Felder in der ausgewählten Tabelle handelt. Der Feldname muss in geschweifte Klammern eingeschlossen werden und wird während der Laufzeit der Flow-Ausführung durch den Feldwert ersetzt. Beispiel: Security Incident SIR001001: Wenn die Variable {number} im Feld **Stammordnername** konfiguriert ist, wird die Nummer während der Laufzeit durch SIR001001 ersetzt.
- **Stammordnername** unterstützt keines der folgenden Zeichen: " * : < > ? / \ | und darf auch nicht mit einem Punkt (.) enden. Wenn Sie die oben genannten Zeichen verwenden, werden sie während der Laufzeit automatisch durch ein Leerzeichen ersetzt.
- Wenn der **Stammordner-** und **Unterordnername** den definierten Grenzwert (256 Zeichen) überschreiten, wird der Ordnername gekürzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden finden Sie die Ausführung des Subflows „Ordnerstruktur erstellen“ zur Laufzeit:



File Explorer Aktivitätenstrom im Arbeitsbereich

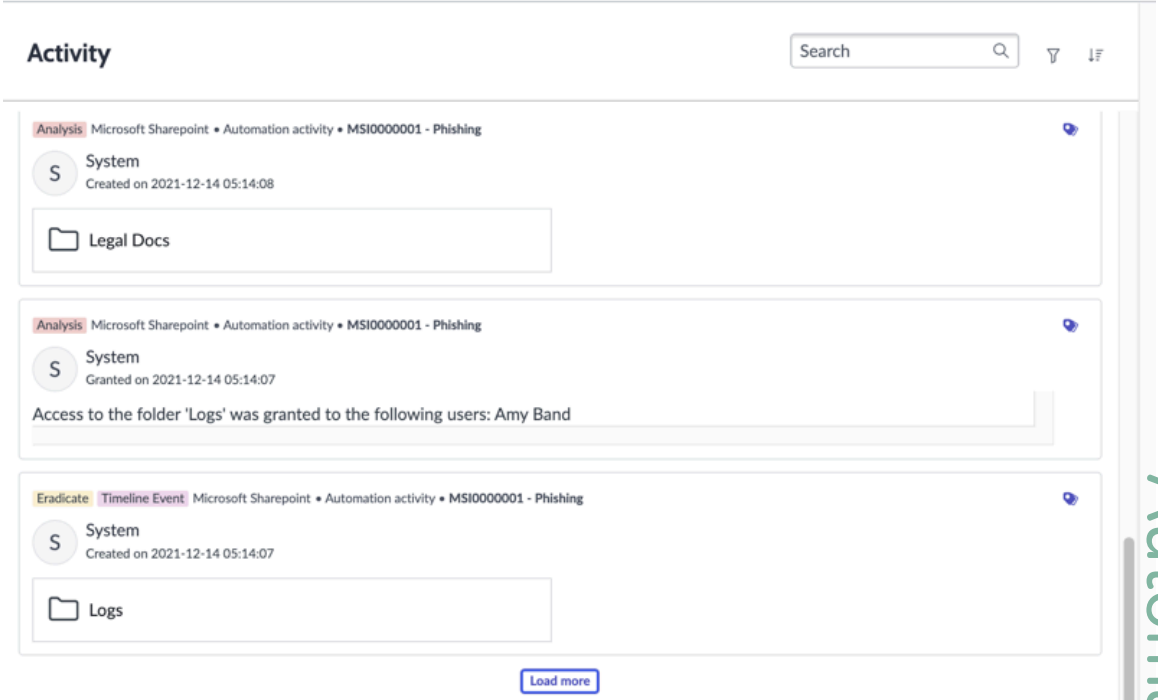
Verwenden Sie den Abschnitt „Datei-Explorer“ im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents, um die Ordner und Dateien in der Reihenfolge anzuzeigen, in der sie in der Dokumentbibliothek Microsoft SharePoint erstellt wurden.

Der Aktivitätenstrom listet alle Automatisierungsaktivitätsveröffentlichungen bei jeder Ordner- und Dateiaktivität oder Protokolle auf, die während der Lösung Major Security Incident auftreten. Die Struktur des Aktivitätenstroms ist im gleichen Format wie die Bibliothek Microsoft SharePoint ausgerichtet, die die Ordner anzeigt, die erstellt wurden und welche Anwender oder Anwendergruppen diesen Ordnern zugewiesen wurden.

Der Aktivitätenstrom ermöglicht es Arbeitsbereichs-Managern und anderen Anwendern oder Anwendergruppen effektiv zu kommunizieren und zusammenzuarbeiten, die Aktivitäten aufzulisten, die für Microsoft SharePoint Ordner und Dateien ausgeführt wurden, den Status von Incidents zu überwachen, Notizen zu veröffentlichen oder zusätzliche Kommentare hinzuzufügen im Incident-Datensatz haben. Die Manager des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereichs können basierend auf der zuletzt aktualisierten Aktivität aufnehmen und



arbeiten.

File Explorer-Problembehandlung

Der Abschnitt zur Problembehandlung kann Ihnen helfen, einige der technischen Probleme zu beheben, die beim Einrichten der Komponente File Explorer auftreten können.

Im folgenden Abschnitt erfahren Sie mehr über die geplanten Aufgaben, die Systemeigenschaften und die Flow Designer-Subflows File Explorer.

Geplante Aufgaben für File Explorer

Geplante Aufgaben sind automatisierte Aufgaben, die ausgeführt werden, um die Benachrichtigungen von Microsoft SharePointzu verarbeiten, die Dateimetadaten in der Instanz ServiceNow aufzunehmen und die Datei-Repository-Abonnements nach einem wiederkehrenden Zeitplan zu verlängern.

Geplante Aufgaben sind automatisierte Aufgaben, die im Hintergrund ausgeführt werden, um:

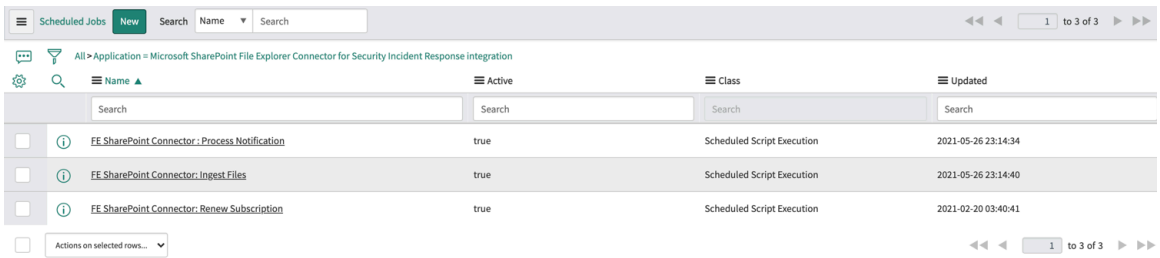
- die Benachrichtigungen von Microsoft Microsoft SharePointverarbeiten.
- Nehmen Sie die Dateimetadaten in der Instanz Now Platform auf.
- Verlängern Sie das Abonnement mit der Dokumentbibliothek Microsoft SharePoint, um Benachrichtigungen zu erhalten.

Auftrag	Beschreibung
Microsoft SharePoint File Explorer Connector: Benachrichtigung verarbeiten	Wird alle 30 Sekunden ausgeführt und ist für das Lesen der Benachrichtigungen verantwortlich, die auf Änderungen in der abonnierten Dokumentbibliothek hinweisen und den Status von Laufwerken (sn_fe_file_repo_drive) als ausstehend markieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auftrag	Beschreibung
Microsoft SharePoint File Explorer Connector: Dateien erfassen	Wird alle 30 Sekunden ausgeführt und ist in erster Linie für die Verarbeitung der Laufwerke (sn_fe_file_repo_drive) verantwortlich, die sich im Status „Ausstehend“ befinden. Außerdem werden die Delta-Datei-Changes seit dem letzten Abruf aus der konfigurierten Dokumentbibliothek Microsoft SharePoint abgerufen.
Microsoft SharePoint File Explorer: Abonnement verlängern	Wird alle 10 Minuten ausgeführt und ist für die Verlängerung des Abonnements der Dokumentbibliothek Microsoft SharePoint einen Tag vor dem Ablaufdatum verantwortlich. Normalerweise laufen diese Abonnements in 30 Tagen ab.



Verfügbare Systemeigenschaften für Datei-Explorer

Im Folgenden finden Sie die verfügbaren Systemeigenschaften für den Microsoft SharePoint Datei-Explorer-Connector.

Systemeigenschaften

Eigenschaftsname	Beschreibung
sn_fe_sharepoint.max_retry_count	Steuert die Häufigkeit der Versuche der Connector-Anwendung Microsoft SharePoint, das fehlerhafte Laufwerk abzurufen oder das fehlerhafte Abonnement zu verlängern. Der Standardwert für die Häufigkeit ist auf 50 festgelegt.
sn_fe_sharepoint.retry_after_seconds	Zeitintervall zwischen jedem Versuch, das fehlgeschlagene Laufwerk abzurufen oder das Abonnement zu verlängern. Der Standardwert ist auf 900 Sek. oder 15 Minuten festgelegt.
sn_fe_sharepoint.max_subscription_expiration_time	Maximaler Abonnementablaufzeitraum in Tagen für Microsoft SharePoint. Der Standardablaufzeitraum ist auf 30 Tage festgelegt.

File Explorer Flow Designer-Subflows

Im Folgenden finden Sie die Flow Designer-Subflows, die mit dem Connector Microsoft SharePoint File Explorer installiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows

Name	Beschreibung
Fügen Sie Berechtigungen Microsoft SharePoint hinzu	Erteilt bestimmten Anwendern Bearbeitungsberechtigungen für einen bestimmten Ordner.
Laufwerksabonnement erstellen	Abonniert mit einer konfigurierten Microsoft SharePoint -Dokumentbibliothek, um Benachrichtigungen über alle Aktualisierungen in der Dokumentbibliothek zu erhalten.
Neuen Ordner Microsoft SharePoint erstellen	Erstellt einen neuen Ordner Microsoft SharePoint unter einem bestimmten übergeordneten Ordner.
Löschen Sie das Element Microsoft SharePoint	Löscht Microsoft SharePoint Dateien und Ordner.
Laden Sie die Datei Microsoft SharePoint herunter	Gibt die Download-URL von Microsoft SharePoint -Dateien zurück
Ruft Datei-Metadaten ab	Abonniert die Änderungen aus der Dokumentbibliothek Microsoft SharePoint und ruft sie ab.
Microsoft SharePoint Element verschieben	Verschiebt die Dateien/Ordner Microsoft SharePoint in den Zielordner
Öffnen Sie Microsoft SharePoint Element	Gibt die Web-URL der Datei/des Ordners Microsoft SharePoint zum Öffnen in einem Browser zurück.
Verlängern Sie das Laufwerksabonnement	Verlängert das Abonnement mit der Dokumentbibliothek Microsoft SharePoint.
Erstellen Sie eine Ordnerstruktur	Verfolgt die Konfigurationen der Ordnervorlage und erstellt die Ordnerstruktur in der Dokumentbibliothek Microsoft SharePoint.

Microsoft Teams konfigurieren

Einfache Integration von und Zusammenarbeit mit Microsoft Teams, um Major Security Incident zu lösen und Zusammenarbeits-Chat-Aktivitäten anzuzeigen und zu filtern.

Das Konfigurieren und Abonnieren einer Chat-Umgebung Microsoft Teams, das Abrufen von Chat-Konversationen aus angegebenen Kanälen und das Archivieren des Teams und der zugehörigen Kanäle sind Teil des Prozesses zum Schließen von Incidents. Eine bestimmte Microsoft Teams -Umgebung und eine zugehörige Microsoft Teams Graph -API-Konfiguration sind erforderlich, um einzelne Kanäle zu erstellen, die für einen Major Security Incidentspezifisch sind.

Aktivieren Sie zum Konfigurieren von Microsoft Teams Teams als Chat-Anbieter. Anschließend können Sie Chatkanäle für die verschiedenen Stakeholder und Gruppen erstellen, die über Aktivitäten kommunizieren, und Chatunterhaltungen nachverfolgen, um das Problem Major Security Incidentzu lösen. Die Konfiguration der Microsoft Teams- und Microsoft Graph API umfasst:

- Stellen Sie eine MS Teams Graph-Verbindung her auf Now Platform
- Aktivieren Sie MS Teams als Chat-Anbieter
- Erstellen Sie eine Chatkanalvorlage
- Chatnachrichtenaktivität anzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit Microsoft Teams

Lesen Sie sich die folgenden Informationen durch, bevor Sie Microsoft Teams als Connector-Anwendung verwenden.

Stellen Sie sicher, dass die folgenden Plugins installiert sind, bevor Sie mit dem Herstellen, Aktivieren und Validieren Microsoft Teams von Setup-Verbindungen beginnen.

Benötigte Plugins

Name	Beschreibung
Chat integration with Security Incident Management	Verwenden Sie die Plugin-ID **sn_chat_collab_core**, um Microsoft Teams Chat zu suchen und zu installieren. Durch die Installation dieses Plugins können Sie die Chataktivität für Anwendungen von Drittanbietern wie Microsoft Teams (oder Slack und andere Chat-Anwendungen von Drittanbietern) nachverfolgen.
Microsoft Teams Chat Connector for Security Incident Management	Verwenden Sie die Plugin-ID **sn_ms_teams_connector**, um Microsoft Teams Chat Connector for Major Security Incident Management zu suchen und zu installieren. Wenn Sie dieses Plugin installieren, können Sie die Chataktivitäten mit der für Microsoft Teamsspezifischen Zusammenarbeitskomponente nachverfolgen.
Microsoft Teams Graph-Spoke	Durch die Installation dieses Plugins wird eine Graph-Spoke-Verbindung mit Microsoft Teamshergestellt. Weitere Informationen finden Sie unter Microsoft Teams Graph-Spoke

Aktivieren Sie MS Teams als Chat-Anbieter

Aktivieren Sie Microsoft Teams, indem Sie die Verbindung Microsoft Teams validieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Sobald die Verbindung aktiviert und validiert wurde, wird eine Informationsmeldung angezeigt, dass die Anbieterverbindung erfolgreich validiert wurde. Sie können die Kanalkonfiguration ändern, indem Sie Benutzer hinzufügen und entfernen und möglicherweise weitere Kanäle hinzufügen oder vorhandene Kanäle umbenennen.

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Konfiguration des Chat-Providers**.
2. Wählen Sie **den Microsoft Teams-Datensatz**aus.
3. Klicken Sie auf **Verbindung validieren**.
   In einer Bestätigungsmeldung wird angezeigt, dass die Anbieterverbindung erfolgreich validiert wurde.
4. Aktivieren Sie das Kontrollkästchen **Aktiv**, um den Anbieterdatensatz zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Bestätigungsmeldung zeigt an, dass die Anbieterverbindung erfolgreich validiert wurde.

5. **Speichern Sie** das Formular, nachdem Sie die Konfiguration des Chat-Providers aktiviert haben.
   Womit wurde die Verbindung zwischen Microsoft Teams und Now Platform Instanz erfolgreich hergestellt.

Erstellen Sie eine Chatkanalvorlage

Konfigurieren Sie Chat-Teams und Kanalvorlagen, um Chat-Teams und Kanäle für die Zusammenarbeit zu erstellen, Chatunterhaltungen nachzuverfolgen und diesen Chatkanälen Anwender und Anwendergruppen hinzuzufügen. Diese Kanalvorlagen werden in Microsoft Teams erstellt, wenn ein schwerwiegender Security Incident heraufgestuft wird.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

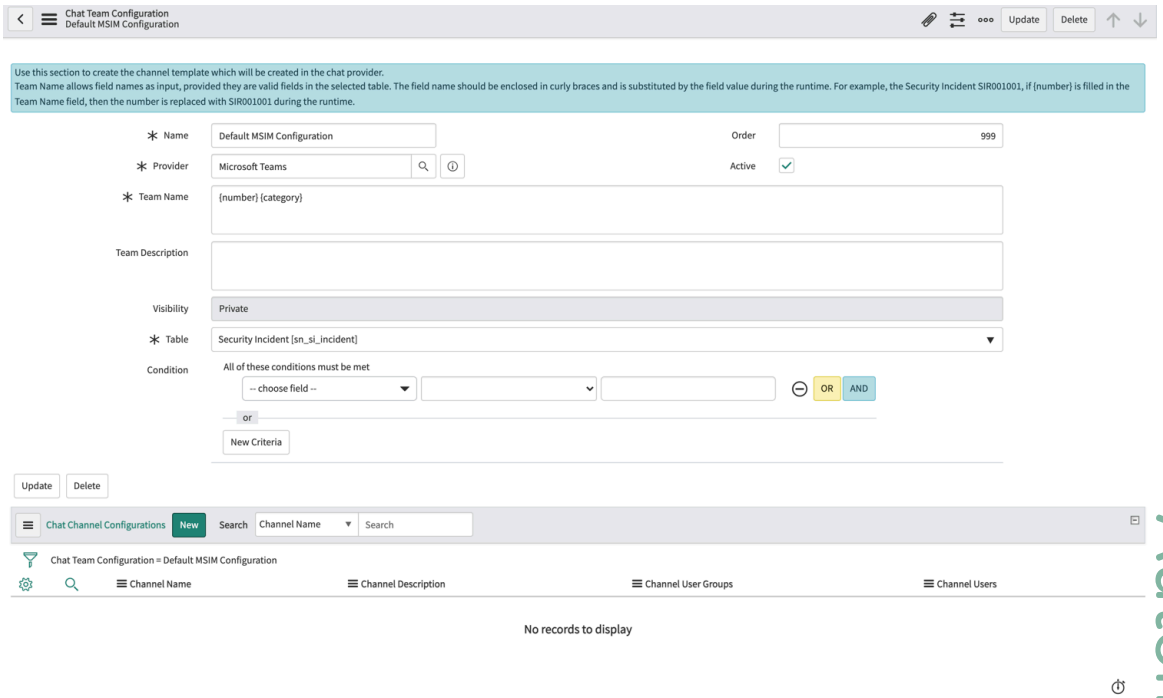
1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Kanalvorlagen**.
2. Klicken Sie im Formular „Konfiguration des Chat-Kanals“ im Header des Formulars **auf Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Konfiguration des Chat-Teams“.

Feld	Beschreibung
Name	Name des Ordners.
Anbieter	Microsoft Teams
Teamname	Name für das Team, z. B. im Format {Nummer}-{Kategorie}. **Hinweis:** Der hier angegebene Teamname wird für alle Datensätze für schwerwiegende Security Incidents verwendet. Um sicherzustellen, dass der tatsächliche Microsoft Team-Name in der MS Teams-Anwendung angezeigt wird und einen eindeutigen Namenswert für verschiedene schwerwiegende Security Incidents aufweist, wird empfohlen, einen eindeutigen Incident-Feldwert zu verwenden, z. B. die Incident-Nummer – {number}. Wie im Screenshot-Beispiel gezeigt, geben {number}, gefolgt von einem Trennzeichen '-' und die Feldvariable {category} eine eindeutige Nummer und Beschreibung des schwerwiegenden Security Incidents zurück, für den Microsoft Teams erstellt wurde, z. B. {number} {Kategorie}.
Teambeschreibung	Optionale Beschreibung des Teams.
Tabelle	Schwerwiegender Security Incident (sn_msi_incident).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



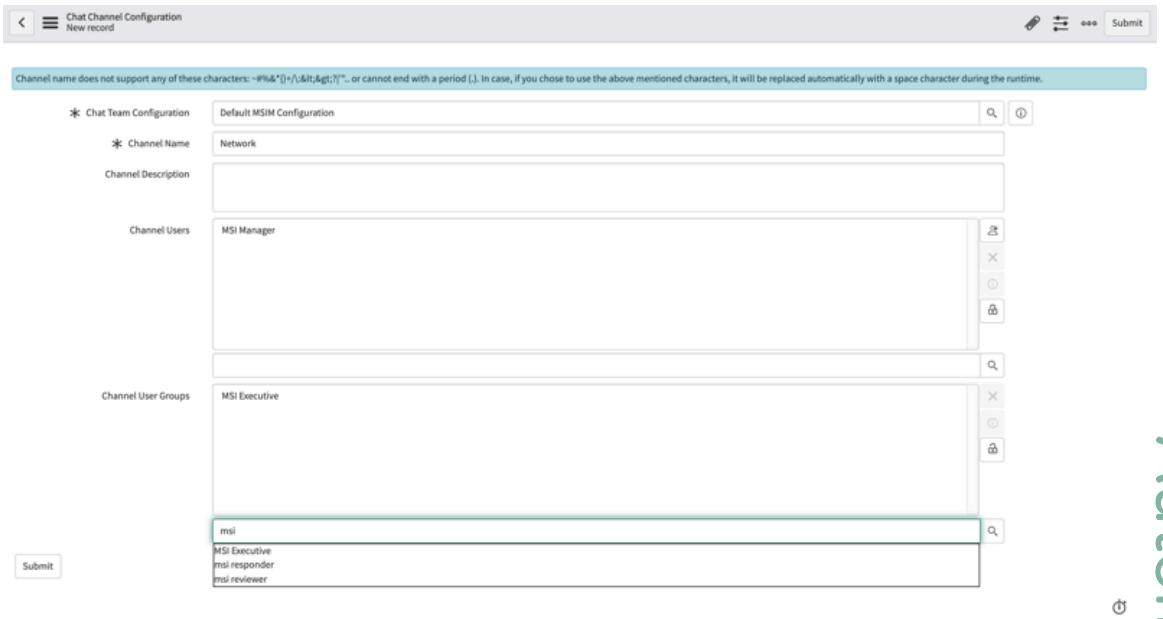
4. Klicken Sie auf **Absenden**.
5. Navigieren Sie zum Abschnitt Chatkanalkonfiguration.
6. Klicken **Neu** um eine neue Chatkanalkonfiguration zu erstellen.
7. Geben Sie ein **Konfiguration des Chat-Teams** und **Kanalname**.

   Hinweis:
   Der neue Kanal, den Sie hier erstellt haben, ist auch Ihr Kanalname in Microsoft Teams. Sie können nach demselben Kanal suchen und Ihre Konversationen hinzufügen.

8. Fügen Sie die Systemeigenschaft **Kanalanwender** und **Kanalanwendergruppen** aus der Nachschlageliste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Absenden den neuen Konfigurationsdatensatz des Chatkanals.



Ergebnisse

Der Chatkanal ist jetzt erstellt, und die Anwender sind diesen Chatkanalgruppen zugewiesen. Sie können die Zusammenarbeits-Chat-Aktivitäten sowohl in Microsoft Teams als auch im Aktivitätenstrom für Zusammenarbeit des MSIM-Arbeitsbereichs mit der organisierten Chatkanal-Hierarchiestruktur anzeigen, die in der Konfiguration des Chatkanal-Anbieters konfiguriert ist.

Chatnachrichtenaktivität anzeigen

Die Aktivität Chat-Nachrichten wird aufgezeichnet und auf der Registerkarte Zusammenarbeit des Arbeitsbereichs „Major Security Incident Management“ angezeigt.

Die Aktivität „Chatnachricht“ umfasst alle Chatunterhaltungen, die zwischen den Teilnehmern und verschiedenen Benutzergruppen stattgefunden haben.

Problembehandlung für MS Teams-Chat-Connector für MSIM

Im Abschnitt zur Fehlerbehebung bei Microsoft Teams-Chat-Connectors finden Sie Informationen zu geplanten Aufgaben, Systemeigenschaften und Microsoft Teams-Flow Designer-Subflows.

Überprüfen Sie, ob der Chat-Connector in jedem Fall geplante Aufgaben verarbeitet, wenn Sie nicht sehen, dass die Nachrichten des Zusammenarbeits-Chats in Microsoft Team und im externen Aktivitätenstrom für Zusammenarbeit des MSIM-Arbeitsbereichs veröffentlicht werden.

Geplante Aufgaben für Microsoft Teams

Geplante Aufgaben sind automatisierte Aufgaben, die ausgeführt werden, um die Benachrichtigungen vom Chat-Connector Microsoft Teams zu verarbeiten und die Microsoft Teams-Abonnements nach einem wiederkehrenden Zeitplan zu verlängern.

Erforderliche Rolle: admin.

- **MS Teams-Chat-Connector: Benachrichtigung verarbeiten**

  Für jedes Chatnachrichtenereignis wird eine Benachrichtigung empfangen, bei der die Ressourcen-ID und die Benachrichtigung in einer Tabelle gespeichert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle 30 Sekunden wird eine geplante Aufgabe ausgeführt, um unverarbeitete Benachrichtigungen auszuwählen und die Microsoft Teams-API abzufragen, um die tatsächlichen Nachrichteninhalte zu erhalten, die weiter in einer anderen Tabelle gespeichert werden.

- **MS Teams-Chat-Connector: Abonnements verlängern**

  Für jeden Kanal im Team werden Abonnements erstellt, um über die erstellten, aktualisierten und gelöschten Ereignisse benachrichtigt zu werden. Dieses Abonnement ist nur 60 Minuten lang aktiv. Die Abonnements werden alle 25 Minuten über die geplante Aufgabe „Microsoft Teams Connector: Benachrichtigung verlängern“ verlängert.

Microsoft Teams Funktions-Flow des Chat-Connectors

Sehen Sie sich diesen Abschnitt an, um die Microsoft Teams zugehörigen Flow Designer-Subflows zu verstehen, die zur Verwaltung der Erstellung von Chatkanälen und des Benutzerzugriffs von schwerwiegenden Security Incidents verwendet werden.

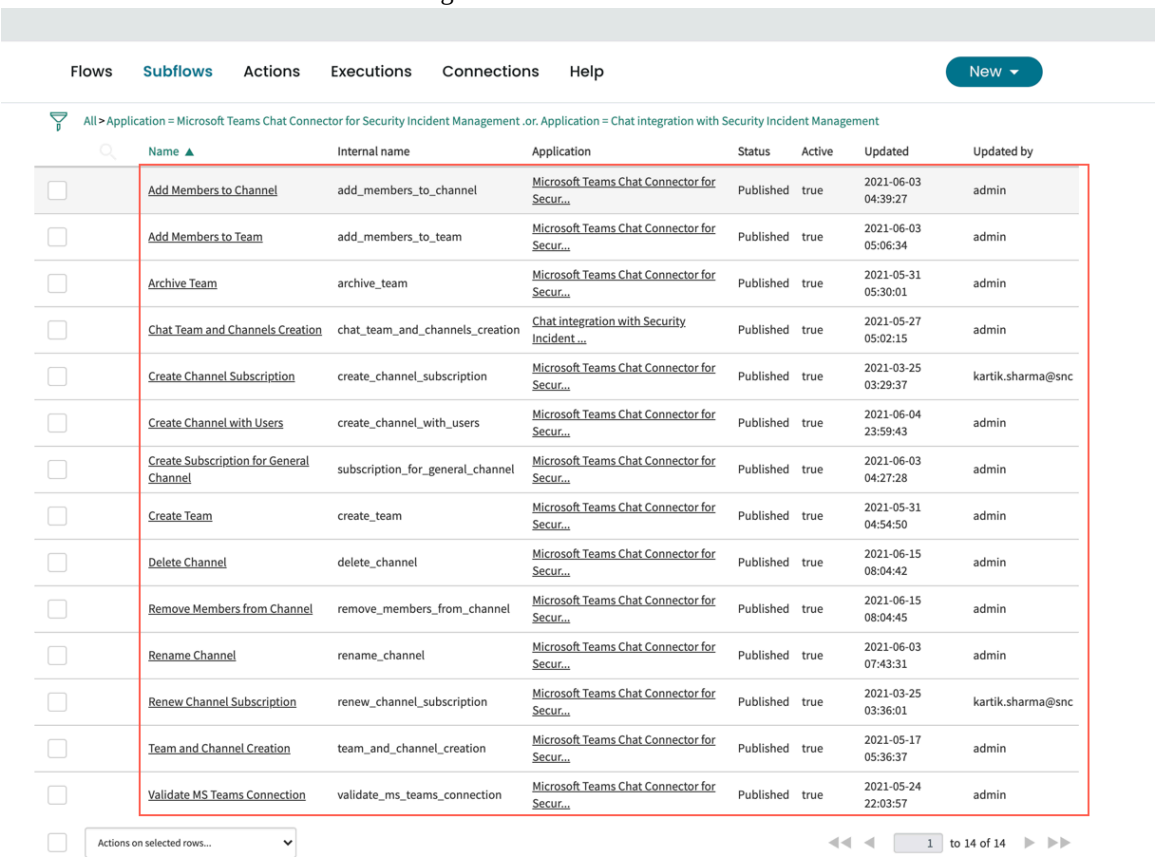
Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Flow Designer**.
2. Mitglieder zu Kanal hinzufügen
3. Fügen Sie dem Team Mitglieder hinzu
4. Team archivieren
5. Erstellung von Chat-Teams und -Kanälen
6. Erstellen Sie ein Kanalabonnement
7. Erstellen Sie einen Kanal mit Anwendern
8. Erstellt ein Abonnement für den allgemeinen Kanal
9. Team erstellen
10. Kanal löschen
11. Entfernen Sie Mitglieder aus dem Kanal
12. Benennen Sie Kanal um
13. Verlängern Sie das Kanalabonnement
14. Team- und Kanalerstellung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

15. Validieren Sie die MS Teams-Verbindung



Konfigurieren Sie den Slack-Chat-Connector für schwerwiegende Security Incidents

Integrieren Sie und arbeiten Sie mit Slack zusammen, um schwerwiegende Security Incidents zu lösen und Zusammenarbeits-Chat-Aktivitäten anzuzeigen und zu filtern.

Das Konfigurieren und Abonnieren einer Chat-Umgebung Slack, das Abrufen von Chat-Konversationen aus angegebenen Kanälen und das Archivieren von Slack und zugehörigen Kanälen sind Teil des Prozesses zum Schließen von Incidents. Eine bestimmte Slack -Umgebung und eine zugehörige Slack -API-Konfiguration sind erforderlich, um einzelne Kanäle zu erstellen, die für einen Major Security Incidentspezifisch sind.

Um Slack zu konfigurieren, aktivieren Sie Slack als Chat-Anbieter. Anschließend können Sie Chatkanäle für die verschiedenen Stakeholder und Gruppen erstellen, die über Aktivitäten kommunizieren, und Chatunterhaltungen nachverfolgen, um das Problem Major Security Incidentzu lösen. Die API-Konfiguration Slack und Slack umfasst:

- Erste Schritte mit der Konfiguration des Slack-Chat-Connectors
- Aktivieren Sie Slack als Kanalanbieter
- Erstellt eine Chat-Kanalvorlage für Slack
- Zeigen Sie Chatnachrichtenaktivitäten in Slack an

Erste Schritte mit der Konfiguration des Slack-Chat-Connectors

Lesen Sie sich die folgenden Informationen durch, bevor Sie Slack als Connector-Anwendung verwenden.

Stellen Sie sicher, dass die folgenden Plugins installiert sind, bevor Sie mit dem Herstellen, Aktivieren und Validieren Slack von Setup-Verbindungen beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benötigte Plugins

Name	Beschreibung
Slack Chat Connector für Security Incident Management	Verwenden Sie die Plugin-ID **sn_slack_connector**, um Slack Connector for Major Security Incident Management zu suchen und zu installieren. Wenn Sie dieses Plugin installieren, können Sie die Chataktivitäten mit der für Slackspezifischen Zusammenarbeitskomponente nachverfolgen.
Slack-Spoke	Durch die Installation dieses Plugins wird eine Spoke-Verbindung mit Slackhergestellt. Weitere Informationen finden Sie unter Slack Spoke

Erstellt eine Chat-Kanalvorlage für Slack

Konfigurieren Sie Chat-Teams und Kanalvorlagen, um Chat-Teams und Kanäle für die Zusammenarbeit zu erstellen, Chatunterhaltungen nachzuverfolgen und diesen Chatkanälen Anwender und Anwendergruppen hinzuzufügen. Diese Kanalvorlagen werden in Slack erstellt, wenn ein schwerwiegender Security Incident heraufgestuft wird.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_admin

Warum und wann dieser Vorgang ausgeführt wird
Der neue Kanal, den Sie erstellen, ist auch Ihr Kanalname in Slack. Sie können nach demselben Kanal suchen und Ihre Konversationen hinzufügen.

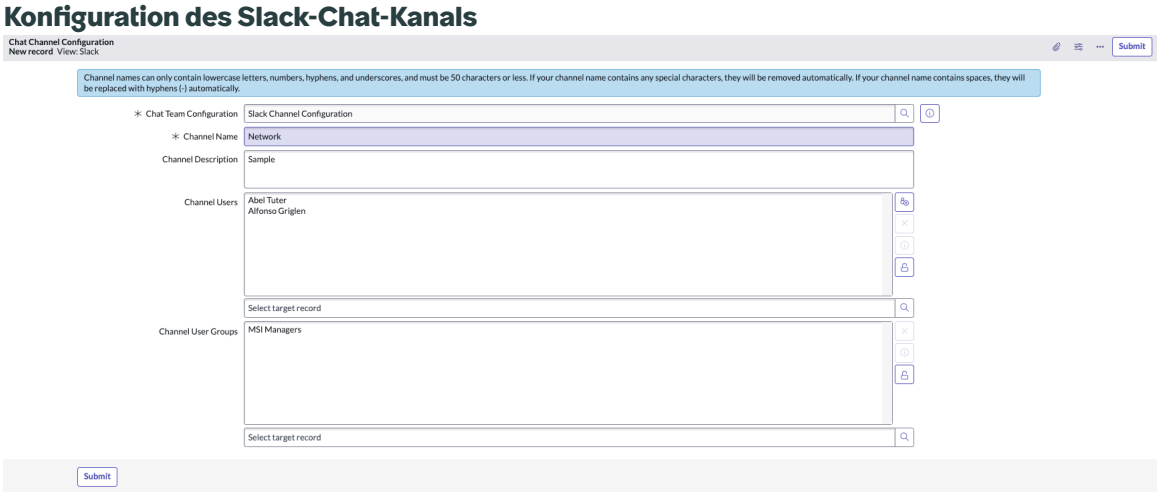
Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Kanalvorlagen**.
2. Wählen Sie **Slack-Kanalkonfiguration** aus, um die Slack-Konfigurationsdetails anzuzeigen.
3. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Konfiguration des Slack-Chat-Kanals zu aktivieren.
4. Geben Sie im Feld Teamname die MSI-Nummer und den Codenamen an.

   Standardmäßig wird allen Slack-Kanälen die Incident-Nummer vorangestellt. Beispiel: `MSI000000 - {Kanalname}`. Sie können das Präfix für ein beliebiges Feld Ihrer Wahl in diesem Format ändern: `{field_name}`.

   Hinweis:
   Der hier angegebene Teamname wird für alle Datensätze für schwerwiegende Security Incidents verwendet. Um sicherzustellen, dass Slack in der Anwendung Slack angezeigt wird und einen eindeutigen Namenswert für verschiedene schwerwiegende Security Incidents aufweist, wird empfohlen, einen eindeutigen Incident-Feldwert zu verwenden, z. B. `MSI000000 - {Kanalname}`.
5. Klicken Sie mit der rechten Maustaste auf die Konfiguration, und wählen Sie **Speichern**aus.
6. Navigieren Sie zum Abschnitt Chatkanalkonfiguration.
7. Auswahlvorgang **Neu** um eine neue Chatkanalkonfiguration zu erstellen.
8. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Wählen Sie **Absenden**.

Ergebnisse

Der Chatkanal ist jetzt erstellt, und die Anwender sind diesen Chatkanalgruppen zugewiesen. Sie können die Zusammenarbeits-Chat-Aktivitäten sowohl in Slack als auch im Aktivitätenstrom für Zusammenarbeit des MSIM-Arbeitsbereichs mit der organisierten Chatkanal-Hierarchiestruktur anzeigen, die in der Konfiguration des Chatkanal-Anbieters konfiguriert ist.

Aktivieren Sie Slack als Kanalanbieter

Aktivieren Sie Slack, indem Sie die Verbindung Slack validieren.

Vorbereitungen

Erforderliche Rolle:

- sn_msi.workspace_admin: Schreiben
- sn_msi.chat_collab_provider: Lesen

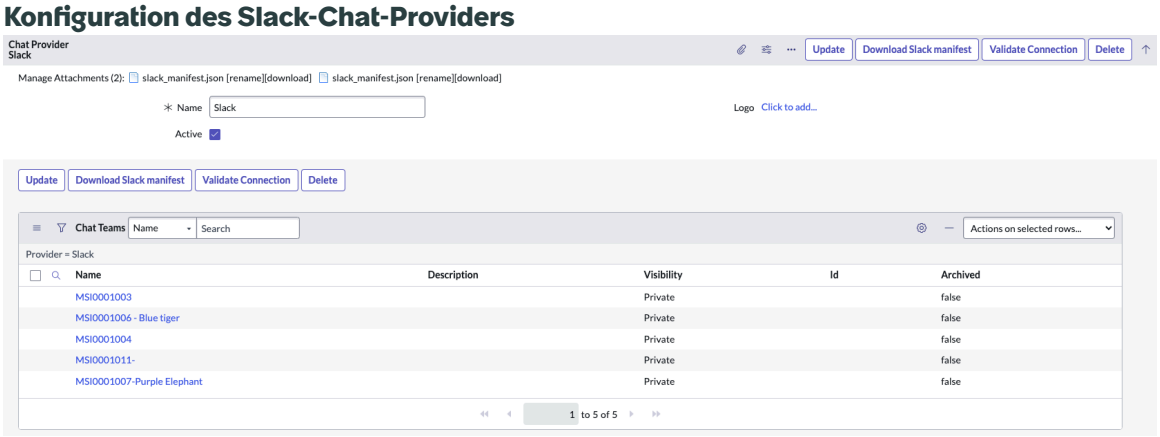
Sobald die Verbindung aktiviert und validiert wurde, wird eine Informationsmeldung angezeigt, dass die Anbieterverbindung erfolgreich validiert wurde. Sie können die Kanalkonfiguration ändern, indem Sie Benutzer hinzufügen und entfernen und möglicherweise weitere Kanäle hinzufügen oder vorhandene Kanäle umbenennen.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Konfiguration des Chat-Providers**.
2. Wählen Sie **Slack** aus, um die Konfiguration des Slack-Chat-Providers zu öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie **Slack-Manifest herunterladen**, um die Datei slack_manifest.json herunterzuladen. Die Datei slack_manifest.json enthält die vollständige Konfiguration für das Slack-Setup und ermöglicht Ihnen die automatische Konfiguration von Slack. Sie müssen diese JSON-Datei in die Slack-Konfiguration hochladen.
4. Öffnen Sie die Datei slack_manifest.json, und führen Sie die folgenden Schritte aus:
   a. Rufen Sie in Ihrem Webbrowser die URL api.slack.com/apps auf.
   b. Wählen Sie die Aktion **Neue App erstellen aus**.
   c. Wählen Sie im Popup-Fenster „App erstellen“ die Option **Aus einem App-Manifest**.
   d. Wählen Sie im Popup-Fenster „Arbeitsbereich für die Entwicklung Ihrer App auswählen“ einen Arbeitsbereich aus der Liste aus, und wählen Sie **Weiter**.
   Beispiel: MSIM Slack-Arbeitsbereich.
   e. Wählen Sie im Popup-Fenster „App-Manifest eingeben unten“ die Registerkarte **JSON** aus, und kopieren Sie den Code aus der Datei slack_manifest.json, und fügen Sie ihn ein.
   f. Wählen Sie **Weiter**.
   g. Wählen Sie im Popup-Fenster Zusammenfassung überprüfen und App erstellen die Option **Erstellen aus**. Jetzt wurde Ihre App erstellt.
   h. Wählen Sie auf der Seite „Basisinformationen **“ Install to Workspace (In Arbeitsbereich installieren**).
   Der Slack-Integrations-Bot fordert Ihre Berechtigung zum Zugriff auf den MSIM Slack-Arbeitsbereich an.
   i. Wählen Sie **Genehmigen** aus.
   j. Füllen Sie im Abschnitt „App-Anmeldeinformationen“ die Details aus, indem Sie zurück zur ServiceNow-Instanz navigieren.
   k. Auswahlvorgang **Alle** > **Slack-Konfigurationen**.
   Für diese Aktion benötigen Sie die Rolle sn_msi.workspace_admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

l. Wählen Sie eine Eigenschaft **für das Signier-Secret** aus.

m. Kopieren Sie das Signier-Secret, und fügen Sie es in Slack im Abschnitt „App-Anmeldeinformationen“ ein.

n. Navigieren Sie in der ServiceNow-Instanz zu **Alle** > **Flow Designer**.

o. Navigieren zu **Verbindungen** > **Slack** > **Details anzeigen** > **Konfigurieren**.

p. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Verbindungsname	Name dieser Verbindung. Beispiel: Slack.
Verbindungs-URL	URL dieser Verbindung. Beispiel: https://slack.com
Anmeldeinformationsname	Name der Anmeldeinformationen Beispiel: Slack-Anmeldeinformationen.
OAuth-Name	Name von OAuth Beispiel: Slack OAuth.
OAuth-Client-ID	Die Client-ID, die für den von Ihnen in Slack erstellten Account generiert wurde.
OAuth-Client-Geheimnis	Der geheime Clientschlüssel für den Account, den Sie in Slack erstellt haben.
OAuth-Umleitungs-URL	Name der OAuth-Umleitungsinstanz. Beispiel: msimslack.service-now.com/oauth_redirect.do

q. Wählen Sie **Konfigurieren und OAuth-Token abrufen aus**.
Der Slack-Integrations-Bot fordert Ihre Berechtigung zum Zugriff auf den MSIM Slack-Arbeitsbereich an.

r. Wählen Sie **Genehmigen** aus.
Das OAuth-Zugriffstoken ist verfügbar und läuft am ab<YYYY-MM-DD><HH:MM:SS> .

5. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Konfiguration des Chat-Providers**.
6. Aktivieren Sie das Kontrollkästchen **Aktiv**, um den Chat-Provider-Datensatz zu aktivieren.
7. Wählen Sie **Verbindung validieren** aus, um die Verbindung zu testen.
Eine Bestätigungsmeldung zeigt an, dass die Anbieterverbindung erfolgreich validiert wurde.
8. Klicken Sie mit der rechten Maustaste auf den Datensatz, und wählen Sie **Speichern**aus.
Danach wurde die Verbindung zwischen Slack und der Instanz Now Platform erfolgreich hergestellt.
9. Navigieren zu **api.slack.com/apps** > **Funktionen** > **OAuth und Berechtigungen**.

a. Überprüfen Sie, ob alle Umfänge korrekt sind.

b. Navigieren zu **Funktionen** > **Ereignisabonnements**.

c. Wählen Sie im Feld Anforderungs-URL **die Option Wiederholen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können eine verifizierte Nachricht sehen.

d. Wählen Sie **Speichern**.

Zeigen Sie Chatnachrichtenaktivitäten in Slack an

Die Aktivität Chat-Nachrichten wird aufgezeichnet und auf der Registerkarte Zusammenarbeit des Arbeitsbereichs „Major Security Incident Management“ angezeigt.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Aktivität „Chatnachricht“ umfasst alle Chatunterhaltungen, die zwischen den Teilnehmern und verschiedenen Benutzergruppen stattgefunden haben. Weitere Informationen finden Sie unter Verwalten Sie die Kommunikation von Chat-Kanälen mit Slack.

Management schwerwiegender Sicherheits-Incidents – Administration

Planen und konfigurieren Sie Ihre Management schwerwiegender Sicherheits-Incidents-Implementierung.

Sie können die folgenden Aspekte der Management schwerwiegender Sicherheits-Incidents -Administration konfigurieren:

Ermöglichen Sie die Empfehlung, Heraufstufung und Verknüpfung von schwerwiegenden Security Incidents

Ermöglichen Sie Anwendern, zu entscheiden, ob Incidents als schwerwiegende Security Incidents vorgeschlagen oder hochgestuft werden sollen. Verfolgen Sie ganz einfach alle Incidents im Zusammenhang mit einem schwerwiegenden Security Incident, indem Sie die Verknüpfung von Security Incidents mit dem übergeordneten oder untergeordneten Incident aktivieren.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Ermöglichen Sie Anwendern, einen Security Incident für einen schwerwiegenden Security Incident vorzuschlagen, indem Sie das Kontrollkästchen **Schwerwiegenden Security Incident vorschlagen** im Abschnitt „Aktionen des SIR-/VR-Arbeitsbereichs“ aktivieren.
3. Ermöglichen Sie Anwendern, einen Security Incident zu einem schwerwiegenden Security Incident heraufzustufen, indem Sie das Kontrollkästchen **Zu schwerwiegendem Security Incident heraufstufen** aktivieren.
4. Aktivieren Sie die Verknüpfung eines Security Incident mit einem schwerwiegenden Security Incident, damit beide gemeinsam nachverfolgt werden können, indem Sie das Kontrollkästchen **Mit schwerwiegendem Security Incident verknüpfen** aktivieren.
5. Wählen Sie **Aktualisieren**.

Markieren Sie Security Incidents als schwerwiegende Security Incidents

Markieren Sie Security Incidents oder angreifbare Datensätze mit einem Tag oder kennzeichnen Sie sie als schwerwiegenden Security Incident, wenn der Incident vorgeschlagen oder heraufgestuft wird. Wenn ein Security Incident vorgeschlagen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird, wird der Incident-Datensatz als Kandidat für schwerwiegenden Security Incident bezeichnet. Wenn ein Wertpapier heraufgestuft wird, wird der Incident-Datensatz als schwerwiegender Security Incident mit dem Status „Akzeptiert“ bezeichnet.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Aktivieren Sie das Kontrollkästchen **Bezeichnungen anzeigen**, um den vorgeschlagenen Incident-Kandidaten als schwerwiegenden Security Incident zu kennzeichnen, indem Sie das **Suchfeld Bezeichnungsname – Als Kandidat vorschlagen** auswählen und im Abschnitt **„Bezeichnungen des SIR/VR-Arbeitsbereichs“** die Option Kandidat für schwerwiegenden Security Incident auswählen.
3. Aktivieren Sie das Kontrollkästchen **Bezeichnungen anzeigen**, um den heraufgestuften Incident-Kandidaten als schwerwiegenden Security Incident zu kennzeichnen, indem Sie das **Suchfeld Bezeichnungsname – Heraufstufung zu schwerwiegendem Security Incident** auswählen und im Abschnitt **„Bezeichnungen des SIR/VR-Arbeitsbereichs“ die** Option Schwerwiegender Security Incident auswählen.
4. Wählen Sie **Aktualisieren**.

Bezeichnungen für schwerwiegende Security Incidents konfigurieren

Konfigurieren Sie Bezeichnungen in der Verwaltung schwerwiegender Security Incidents, um anwenderdefinierte Bezeichnungen zu erstellen und die externen Zusammenarbeitsaktivitäten und -aufgaben im Aktivitätenstrom zu filtern. Die verschiedenen Arten von implementierten Bezeichnungen sind Statusbezeichnungen und Zeitleistenbezeichnungen.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Kontrollkästchen **„Bezeichnungen anzeigen** “ aktivieren, um die Beschriftung verschiedener Incident-Status wie Analyse, Eindämmen, Löschen, Wiederherstellen, Überprüfen, Zeitleistenereignis im Abschnitt **„Bezeichnungen“ des MSIM-Arbeitsbereichs (Anzeige bei Zusammenarbeitsaktivitäten und -aufgaben)** zu aktivieren.
3. Wählen Sie **Aktualisieren**.

Bezeichnungen für schwerwiegende Security Incidents konfigurieren

Konfigurieren Sie verschiedene Arten von Bezeichnungen, um die Incident-Status besser zu filtern und auch anzugeben. Bezeichnungen schwerwiegender Security Incidents bieten die Flexibilität, die Zusammenarbeitsaktivitäten und -aufgaben der Incident-Datensätze zu kennzeichnen.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Bezeichnungen mithilfe des Bezeichnungssymbols aktivieren oder deaktivieren, das im Abschnitt „Aktivitätenstrom“ des Abschnitts „Zusammenarbeit und Aufgabenorganisator“ des MSIM-Arbeitsbereichs verfügbar ist.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **MSI-Bezeichnungen**.
2. Klicken Sie auf **Neu**, um eine neue Bezeichnung zu erstellen.
3. Füllen Sie das Formular mit **Bezeichnungsname** und **Bezeichnungsfarbe**aus.
4. Klicken Sie auf **Bezeichnung erstellen**.
5. Als Teil des Basissystems sind für jeden Incident-Status folgende Bezeichnungen konfiguriert. Sie können den Bezeichnungsnamen oder die Farbe nicht ändern:
   - Analyse
   - Beinhalten
   - Beseitigen
   - Prüfung
   - Wiederherstellen
   - Zeitleistenereignis

Hinweis:
Sie können die anwenderdefinierten Bezeichnungen und ihre Eigenschaften ändern.

Konfigurieren Sie Zeitleistenkategorien für schwerwiegende Security Incidents

Konfigurieren Sie Zeitleistenkategorien wie Bedrohung, Antwort oder Anwenderdefiniert, und weisen Sie sie Ihren schwerwiegenden Security Incidents im Abschnitt „Zeitleiste“ auf der Registerkarte Übersicht zu.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Zeitleistenkategorien**.
   Die folgenden Zeitleistenkategorien werden als Teil des Basissystems bereitgestellt:
   - **Anwenderdefiniert**.
   - **Antwort**.
   - **Bedrohung**.
2. Um eine vorhandene Zeitleisten-Ereigniskategorie zu ändern, gehen Sie wie folgt vor:
   a. Wählen Sie eine Zeitleisten-Ereigniskategorie aus der Liste aus.
   b. Sie können den Namen der Ereigniskategorie der Zeitleiste ändern.
   c. Sie können die Ereignisfarbe ändern und eine andere Farbe für die Kategorie des Zeitleisten-Ereignisses auswählen.
   d. Wählen Sie **Aktualisieren**.
3. Um eine neue Ereigniskategorie auf der Zeitleiste zu erstellen, gehen Sie wie folgt vor:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie **Neu**.

b. Geben Sie im Feld Name einen Namen für die Ereigniskategorie der Zeitleiste ein.

c. Wählen Sie im Feld Ereignisfarbe mithilfe der Dropdown-Liste eine Farbe für die Kategorie der Ereigniszeitleiste aus.

d. Wählen Sie **Absenden**.

Legen Sie Benachrichtigungseinstellungen für fest MSIM

Automatisieren Sie den E-Mail-Benachrichtigungsprozess und benachrichtigen Sie die Anwender, wenn ein Security Incident entweder vorgeschlagen oder zu einem Kandidaten für schwerwiegenden Security Incident hochgestuft wird.

Erforderliche Rolle: sn_msi.workspace_admin.

Die Benachrichtigungen werden nur ausgelöst, wenn ein Security Incident vorgeschlagen und an alle Benutzer und Gruppen gesendet wird, die für die Benachrichtigungsliste konfiguriert sind. Standardmäßig erhält der Benutzer die E-Mail-Benachrichtigung, der den Security Incident als Kandidaten für einen schwerwiegenden Security Incident vorgeschlagen hat.

Benachrichtigung: Security Incident vorgeschlagen (SI) als schwerwiegender Security Incident (MSI)

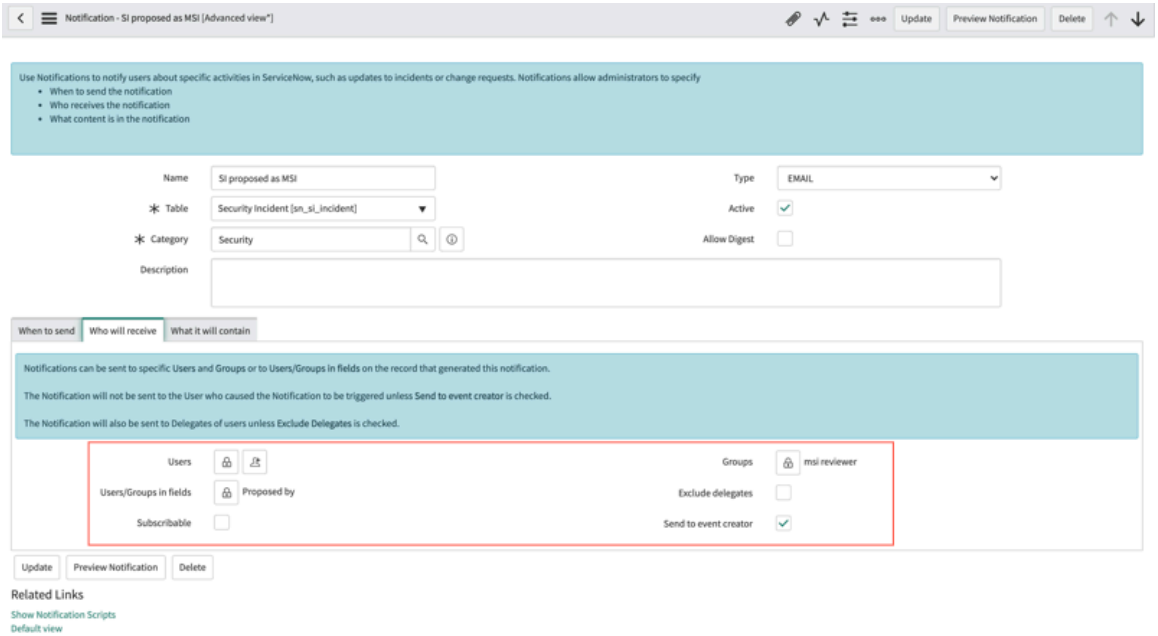
Empfänger:

- Standardmäßig **MSI-Prüfer** Gruppenname wird erstellt, und jeder Anwender, der dieser Gruppe hinzugefügt wird, erhält das Recht, ein zu sein **MSIM-Manager** und die Benutzer in dieser Gruppe erhalten die Benachrichtigungs-E-Mails.
- Jeder bestimmte Benutzer, der hinzugefügt wird **Anwender** Liste erhält auch die Benachrichtigungs-E-Mails.

Inhalt:

Wenn Sie den E-Mail-Inhalt ändern möchten, z. B. den Textkörper der E-Mail, der den Betreff oder den Nachrichten-HTML enthält, müssen Sie über Systemadministratorrollenzugriff verfügen oder als Systemadministrator und nicht als MSI-Administrator zugewiesen sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Benachrichtigung: Security Incident heraufgestuft (SI) als schwerwiegender Security Incident (MSI)

Diese Benachrichtigung wird ausgelöst, wenn ein Security Incident hochgestuft wird und wenn der Datei-Explorer und die Basisstruktur Microsoft Teams erstellt werden. Standardmäßig wird diese Benachrichtigung von dem Benutzer empfangen, der den Security Incident zu einem schwerwiegenden Incident hochgestuft hat.

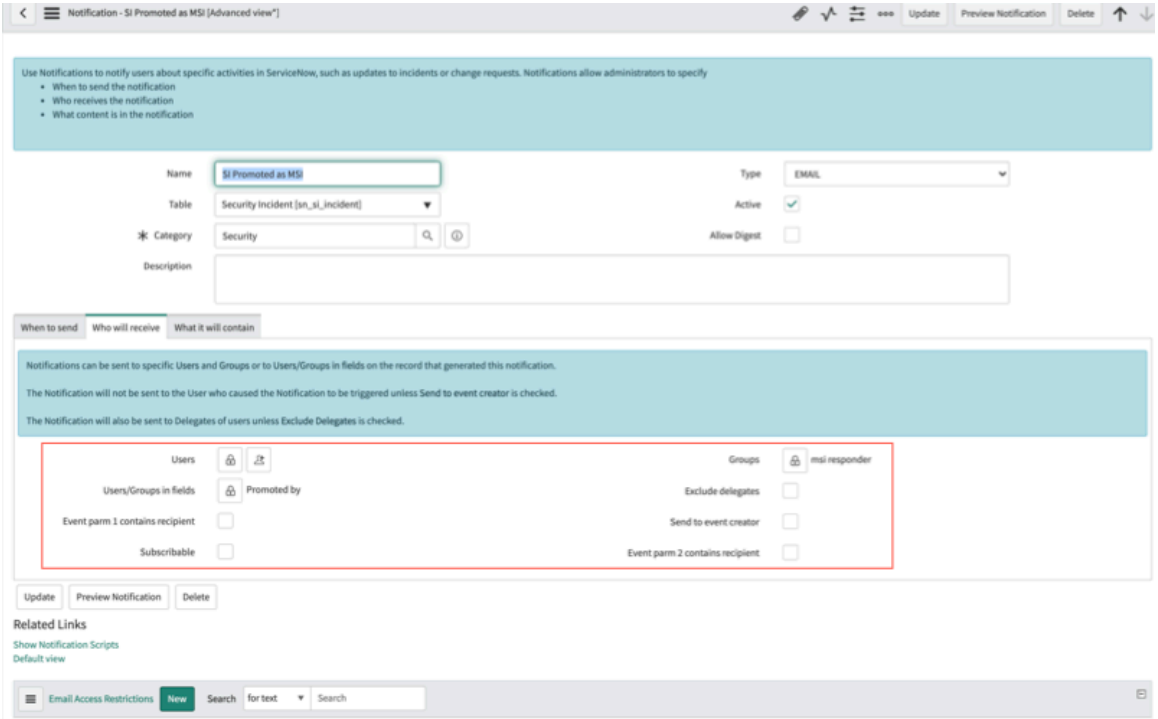
Empfänger

- Standardmäßig a **Gruppe** nach Namen **MSI-Responder** wird erstellt, und jeder Anwender, der dieser Gruppe hinzugefügt wird, hat die Berechtigung **MSIM-Responder** Rolle und alle Benutzer in dieser Gruppe erhalten die Benachrichtigungs-E-Mail.
- Jeder bestimmte Benutzer, der hinzugefügt wird **Anwender** Liste erhält auch die Benachrichtigungs-E-Mails.

Was enthalten sein wird

Wenn Sie E-Mail-Inhalte wie den E-Mail-Text ändern möchten, der den Betreff oder Nachrichten-HTML enthält, müssen Sie über die Systemadministratorrolle verfügen oder als Systemadministrator und nicht als MSI-Administrator zugewiesen sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Konfigurieren Sie MSI-Abschlussaktivitäten

Richten Sie Aktionen ein, die automatisch ausgeführt werden, wenn ein schwerwiegender Security Incident geschlossen wird. Erhöhen Sie die Sicherheit, indem Sie den Zugriff auf Ordner mit Lösungsinformationen automatisch archivieren und entfernen.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Archivieren Sie Chatkommunikation im Zusammenhang mit der Lösung des Incidents, indem Sie das Kontrollkästchen **Zusammenarbeitskanäle archivieren** im Abschnitt Automatisierte Abschlussaktionen aktivieren.
3. Entfernen Sie Ordner, die Material im Zusammenhang mit der Lösung des Incidents enthalten, indem Sie das Kontrollkästchen **Zusammenarbeitsordner entfernen** aktivieren.
4. Wählen Sie **Aktualisieren**.

Management schwerwiegender Sicherheits-Incidents-Arbeitsbereich

Management schwerwiegender Sicherheits-Incidents bietet einen dedizierten Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für den Major Security Incident -Manager entwickelt wurde.

Einfache Zusammenarbeit bei Aktivitäten, die zur Lösung schwerwiegender Security Incidents beitragen, indem Sie Dateien und Ordner freigeben und anzeigen, Incident-Aufgaben anzeigen und aktualisieren und über dedizierte Chatkanäle mit denjenigen kommunizieren, die an dem Incident arbeiten.

Major Security Incident Management (MSIM) bietet einen Mechanismus zur Nachverfolgung und Lösung schwerwiegender Security Incidents. MSIM arbeitet mit den vorhandenen Produktfunktionen für Security Incidents und Vulnerability Response zusammen und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verbessert den Nachbesserungsprozess für schwerwiegende Security Incidents durch folgende Funktionen:

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für die Anwenderrolle „Manager schwerwiegender Security Incidents“ entwickelt wurde.
- Organisieren Sie Aufgaben zur Reaktion auf schwerwiegende Security Incidents, einschließlich Aufgaben, die für verknüpfte Security Incidents und Schwachstellen-Gruppen nachverfolgt werden.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chatkommunikationskanälen, sobald ein schwerwiegender Security Incident erstellt wurde, sowie die Archivierung als Teil des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien) im Zusammenhang mit dem schwerwiegenden Security Incident über eine Microsoft SharePoint -Integration.
- Chatkanalmanager und Aktivitätenstromkomponenten zur Verwaltung der Kommunikation zwischen mehreren Sicherheits-, IT- und Funktionsgruppen über eine Microsoft Teams -Integration.
- Zusammenfassende Berichte über die Auswirkung und den Fortschritt von schwerwiegenden Security Incidents, einschließlich Rollup der betroffenen Assets, Anwender, Standorte und Teamressourcen sowie Zeitleiste der wichtigsten Incident-Meilensteine.

Verwenden Sie den MSIM-Arbeitsbereich, um schwerwiegende Security Incidents nachzuverfolgen und zu beheben:

1. Zeigen Sie die Trenddiagramme und den Fortschritt des schwerwiegenden Security Incident an.
2. Verfolgen und organisieren Sie Microsoft SharePoint-Dateiaktivitäten über den MSIM-Arbeitsbereich.
3. Verfolgen und organisieren Sie Microsoft Teams-Chataktivitäten über den MSIM-Arbeitsbereich.
4. Zeigen Sie Incident-Details über den MSIM-Arbeitsbereich an, und aktualisieren Sie sie.
5. Filtern Sie Zusammenarbeitsaktivitäten im Aktivitätenstrom des MSIM-Arbeitsbereichs.

Management schwerwiegender Sicherheits-Incidents verwenden

Manager können den -Arbeitsbereich Management schwerwiegender Sicherheits-Incidents verwenden, um die vorgeschlagenen, heraufgestuften, verknüpften und abgelehnten Incident-Datensätze anzuzeigen und die zugehörigen Aktivitäten nachzuverfolgen.

Incident-Datensätze vorschlagen, hochstufen und verknüpfen

Sie können Security Incidents als schwerwiegende Security Incidents vorschlagen oder heraufstufen, wenn Incidents als kritische Bedrohung für das Unternehmen identifiziert werden.

Sobald das Management schwerwiegender Sicherheits-Incidents in Ihrer Instanz ServiceNow installiert ist, können Sie den Übergang von Security Incidents zu schwerwiegenden Incidents wie folgt handhaben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schlagen Sie dem Kandidaten für einen schwerwiegenden Security Incident einen Security Incident vor, um einen Überprüfungsprozess zu initiieren.
- Sie können einen Security Incident ohne Überprüfungsprozess direkt zu einem schwerwiegenden Security Incident heraufstufen.
- Lehnen Sie einen als schwerwiegenden Security Incident vorgeschlagenen Security Incident ab.

Sie können einen Security Incident auch als untergeordneten Incident mit einem schwerwiegenden Security Incident verknüpfen, um alle zugehörigen Security Incidents gemeinsam nachzuverfolgen.

Vorschlagen als Major Security Incident

Schlagen Sie einem schwerwiegenden Security Incident einen Security Incident vor.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Listen**.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie als schwerwiegenden Security Incident vorschlagen möchten.
3. Wählen Sie das Symbol **Weitere Aktionen** und dann **Als schwerwiegenden Security Incident vorschlagen**aus.
4. Füllen Sie im Dialogfeld „Als schwerwiegenden Security Incident vorschlagen“ die Felder aus.
   a. **Erkennungsdatum**: Datum, an dem der schwerwiegende Security Incident zum ersten Mal erstellt oder vorgeschlagen wurde.
   b. **Begründung**: Geben Sie eine Begründung für das Vorschlagen des incident an.
   c. **Potenzielle Auswirkung**: Geben Sie die Auswirkung des incident an.
5. Wählen Sie **Vorschlagen**aus.

Ergebnisse

Der Incident wird vorgeschlagen, und die folgenden Aktionen werden ausgeführt:

- Im Security Incident-Datensatz wird eine Bannermeldung zur Verifizierung angezeigt, und das definierte Tag für schwerwiegende Security Incidents wird angezeigt.
- Der Datensatz wird in der zugehörigen Liste „Schwerwiegender Security Incident“ im Incident-Datensatz mit dem Status „Vorgeschlagen“ und in der Liste der Kandidaten für den MSIM-Arbeitsbereich angezeigt.
- Im Abschnitt „Aktivität“ im MSIM-Arbeitsbereich wird angezeigt, dass der Security Incident als schwerwiegender Security Incident heraufgestuft wurde.
- An alle Personen in der definierten Benachrichtigungsliste wird eine Nachricht gesendet, die einen Link zum Incident-Datensatz und die Registerkarte Details für den Incident enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Heraufstufen zu einem Major Security Incident

Heraufstufen Sie einen -Security Incident zu einem schwerwiegenden -Security Incident, oder lehnen Sie vorgeschlagene Vorschläge über den -Arbeitsbereich Management schwerwiegender Sicherheits-Incidents (MSIM) ab.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Listen**.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie als schwerwiegenden Security Incident heraufstufen möchten.
   Überprüfen Sie die Details des Security Incident im Abschnitt Details, oder zeigen Sie erweiterte Details im Incident-Datensatz auf einer separaten Registerkarte an, indem Sie **auf Weitere Details anzeigen**klicken.
3. Wählen Sie das Symbol **Weitere Aktionen** und **dann Zu schwerwiegendem Security Incident hochstufen**aus.
4. Füllen Sie im Dialogfeld „Heraufstufen des schwerwiegenden Security Incident“ die Felder aus.
   a. **Erkennungsdatum**: Datum, an dem der schwerwiegende Security Incident zum ersten Mal erstellt oder vorgeschlagen wurde.
   b. **Geschätztes Lösungsdatum**: Das geschätzte Lösungsdatum, bis zu dem der schwerwiegende Security Incident gelöst werden soll.
   c. **Codename**: Wählen Sie den Codenamen für den schwerwiegenden Security Incident aus.
   Beispiel: Bluetiger.
   d. **Kategorie**: Wählen Sie die Kategorie für den schwerwiegenden Security Incident aus.
   Beispiel: Fehlkonfiguration.
   e. **Begründung**: Geben Sie eine Begründung für das Vorschlagen des incident an.
   f. **Potenzielle Auswirkung**: Geben Sie die Auswirkung des incident an.
5. Wählen Sie **Vorschlagen**aus.
6. Heraufstufen Sie den Security Incident, oder lehnen Sie den Heraufstufungsvorschlag ab.
   - Um den Incident hochzustufen, klicken Sie auf **Zu schwerwiegendem Security Incident heraufstufen**.
   - Um den Heraufstufungsvorschlag abzulehnen, klicken Sie auf **Als schwerwiegenden Security Incident ablehnen**.
7. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

- Wenn Sie den Heraufstufungsvorschlag abgelehnt haben, wird der Incident nicht heraufgestuft, und der Incident-Eintrag wird in die Registerkarte Abgelehnt verschoben.
- Wenn Sie den Incident hochgestuft haben, wird der Incident-Eintrag auf die Registerkarte Öffnen verschoben, und im Sicherheitsdatensatz wird ein Tag angezeigt, das angibt, dass es sich um einen schwerwiegenden Security Incident handelt.
- Die Entscheidung wird im Abschnitt „Aktivität“ des MSIM-Arbeitsbereichs aufgeführt.

Sobald ein Incident heraufgestuft wurde, wird die Standardkonfiguration angewendet.

- Eine Ordnerstruktur wird basierend auf der Konfiguration der Ordnervorlage erstellt.
- Chatkanäle werden basierend auf der Konfiguration der Kanäle erstellt.
- An die angegebenen Benutzer wird eine E-Mail-Nachricht gesendet. Die Standardbenachrichtigung enthält einen Link zum schwerwiegenden Security Incident und Details zum Incident. Die festgelegten Benutzer haben jetzt auch Zugriff auf die Zusammenarbeitsressourcen, sodass die Benachrichtigung auch den Namen des Microsoft-Teams und einen Link zu Microsoft SharePoint-Ordnern enthält, die sich auf den Incident beziehen.

Verknüpfen mit Major Security Incident

Verknüpfen Sie Security Incidents mit einem schwerwiegenden Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie mit dem schwerwiegenden Security Incident verknüpfen möchten.
3. Wählen Sie das Symbol **Zusätzliche Aktionen** und dann **Mit schwerwiegendem Security Incident verknüpfen**aus.
4. Wählen Sie den schwerwiegenden Security Incident aus, zu dem Sie eine Verknüpfung herstellen möchten.
   a. Wählen Sie im Dialogfeld das Symbol „Nachschlagen mit Liste“.
   b. Wählen Sie den schwerwiegenden Security Incident aus, zu dem Sie einen Link erstellen möchten.
   c. Wählen Sie **OK**.
5. Wählen Sie **Vorschlagen**aus.

Ergebnisse

Der Vorschlag wird übermittelt, und die folgenden Aktionen werden ausgeführt:

- Im Datensatz des Security Incidents wird eine Bannermeldung zur Verifizierung angezeigt, und neben dem Feld **Sicherheits-Tag auswählen** das definierte Tag für schwerwiegenden Security Incident angezeigt.
- Auf der Registerkarte **Details** für den schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidentsenthält die Dropdown-Liste mit der Datensatznummer beide Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Datensatz wird in der zugehörigen Liste „Schwerwiegender Security Incident“ des Incident-Datensatzes angezeigt, wobei der Status als „Vorgeschlagen“ aufgeführt wird.
- An alle Personen in der definierten Benachrichtigungsliste wird eine Nachricht gesendet, die einen Link zum Incident-Datensatz und die Registerkarte Details für den Incident enthält.
- Im Abschnitt **„Aktivität“** im MSIM-Arbeitsbereich wird angezeigt, dass der Security Incident als untergeordneter Security Incident dem schwerwiegenden Security Incident mit einem Link hinzugefügt wurde.

Verwenden der MSI-Listenansicht im MSIM-Arbeitsbereich

Mit der Listenansicht im MSIM-Arbeitsbereich können Sie vorgeschlagene, heraufgestufte und abgelehnte schwerwiegende Security Incidents anzeigen.

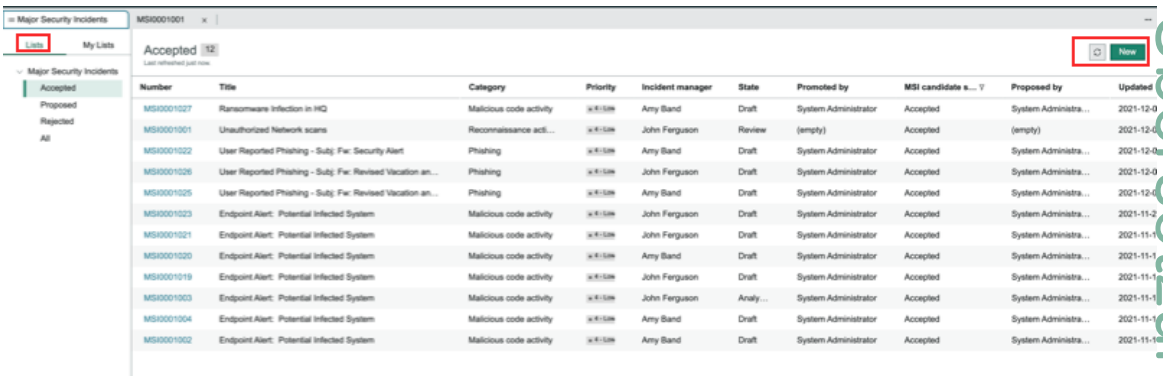
Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Sie können neue Incidents auch über die Schaltfläche **Neu** in der oberen rechten Ecke des Arbeitsbereichs erstellen.

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSIM-Arbeitsbereich**.
2. Wählen Sie die Registerkarte Listen aus, um die Listenansicht anzuzeigen.



3. Wählen Sie **Meine Listen** aus, um eine eigene Liste schwerwiegender Security Incidents zu erstellen.
4. Der folgenden Tabelle können Sie entnehmen, welche Aktionen Sie in der Listenansicht ausführen können:

Aufgabe	Beschreibung
Meine Listen	Erstellen Sie neue MSI-Datensatzlisten, und zeigen Sie die von Ihnen erstellten Listen an.
Legen Sie Filter für eine Spalte in einer Liste fest	Wählen Sie eine Spalte aus, und erweitern Sie das Menü mit vertikalen Punkten, um Optionen anzuzeigen, mit denen die Daten in der Spalte weiter gefiltert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
Filtern Sie Elemente heraus, oder gleichen Sie Elemente aus einer Zeile in einer Spalte ab	Wählen Sie eine Zelle in einer Spalte aus, und verfeinern Sie die angezeigten Daten, indem Sie eine auswählen: ○ Übereinstimmungen anzeigen: Zeigt nur Elemente an, die dem ausgewählten Element in der Spalte entsprechen. ○ Herausfiltern – Filtert die Elemente aus der Spalte heraus, die dem ausgewählten Element in der jeweiligen Spalte entsprechen.
Liste neu laden	Aktualisieren Sie die Listen, und zeigen Sie alle aktualisierten Listen an.
Neu	Erstellen Sie einen neuen MSI-Datensatz.

Zeigen Sie die Auswirkungsmetriken für Major Security Incident an

Stellt aktuelle zusammenfassende Berichte zu Auswirkungen und Fortschritt schwerwiegender Security Incidents bereit. Dies ist ein wichtiger Aspekt bei der Verwaltung schwerwiegender Security Incidents mit dem neuen Arbeitsbereich.

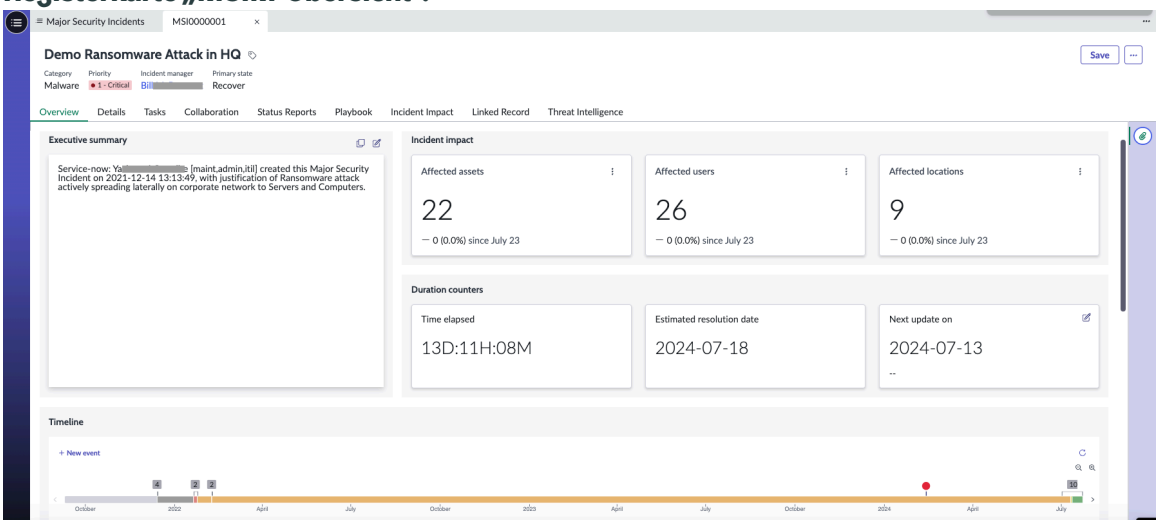
Die Registerkarte **„Übersicht“** enthält die relevanten Metriken zur Verwaltung des Umfangs und Fortschritts des incident, einschließlich eines Rollups der betroffenen Assets, Benutzer, Standorte und Teamressourcen sowie der Zeitleiste der wichtigen Incident-Meilensteine.

Die Zeitleiste bietet eine horizontale Ansicht der wichtigsten Ereignisse und Meilensteine, die im Rahmen der Lösung eines bestimmten schwerwiegenden Security Incident aufgetreten sind. Die Zeitleistenkomponente wird über allen Registerkarten des Arbeitsbereichs für das Management schwerwiegender Sicherheits-Incidents angezeigt und kann bei Bedarf ein- und ausgeklappt werden. Die dargestellten Ereignisdaten werden aktualisiert, wenn bestimmte Meilensteinereignisse oder Meilensteine hinzugefügt oder aktualisiert werden.

Jedes Ereignis oder jeder Meilenstein wird mit einer anderen Option für den Ereignistyp auf der Zeitleiste angezeigt, um die Anzahl und den Typ der Ereignisse oder Meilensteine zu identifizieren. Zum Beispiel NOW-Datensatzaktualisierungen, Zusammenarbeitsaktivitäten. Darüber hinaus wird der Zeitraum für den Zeitraum für die verschiedenen Status schwerwiegender Security Incidents automatisch nachverfolgt und mithilfe von farbcodierten Bereichen zusammen mit der Dauer jedes Incident-Status angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „MSIM-Übersicht“.



Kurzzusammenfassung und Incident-Auswirkung

Aufgabe	Beschreibung
Kurzübersicht	Kurze Zusammenfassung des schwerwiegenden Security Incident mit Anwendername, Anwenderrolle und Zeitstempeldetails. • Sie können die Kurzzusammenfassung ändern, indem Sie auf das Symbol **„Bearbeiten“** klicken. Nachdem Sie die erforderlichen Änderungen vorgenommen haben, wählen Sie die Option **Aktualisieren** aus. • Um die Kurzzusammenfassung zu kopieren und in einen schwerwiegenden Security Incident einzufügen, wählen Sie das Symbol **Kopieren** und fügen die Zusammenfassung in den gewünschten schwerwiegenden Security Incident ein.
Incident Impact	Diese Komponenten zeigen die betroffenen Ressourcen basierend auf einem Rollup aller aktiven Aufgaben und verknüpften Incidents mit identifizierten Assets, Benutzern, Standorten und zugewiesenen Teammitgliedern an. Die betroffenen Ressourcen sind: • **Betroffene Assets** • **Betroffene Anwender** • **Betroffene Standorte** Wenn Sie die Zahlenwerte auswählen, können Sie Detailinformationen zu den betroffenen Assets, Benutzern und Standorten anzeigen und zu den betroffenen Assets, Benutzern und Standorten navigieren. Außerdem werden

Automatische Übersetzung

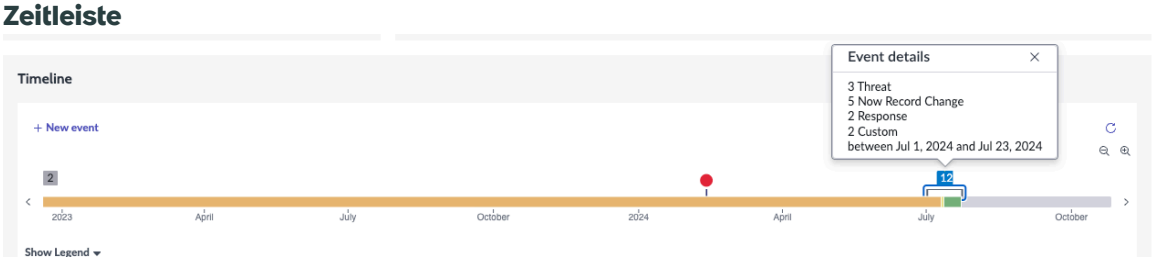
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kurzzusammenfassung und Incident-Auswirkung (Fortsetzung)

Aufgabe	Beschreibung
	die zugehörigen Aufgaben auf der Registerkarte **Incident Impact (Incident-Auswirkung)** des -Arbeitsbereichs angezeigt. Basierend auf dem von Ihnen ausgewählten Link für den Incident-Auswirkungstyp werden im die zugehörigen Incident-Details angezeigt, z. B. Aufgabentyp und dessen Beschreibung, Zuweisungsgruppe und Incident-Status **Incident Impact** Registerkarte des MSIM-Arbeitsbereichs.
Dauerzähler	Diese Komponenten zeigen die Dauer des schwerwiegenden Security Incident an. Die betroffenen Ressourcen sind: • **Verstrichene Zeit**: Zeigt die Zeit an, die seit der Erkennung des schwerwiegenden Security Incidents verstrichen ist. • **Geschätztes Lösungsdatum**: Zeigt das geschätzte Lösungsdatum an, bis zu dem der schwerwiegende Security Incident gelöst werden soll. • **Nächstes Update am**: Datum und Uhrzeit des nächsten Updates zur Behebung des schwerwiegenden Security Incidents. Beispiel: 17:00 Uhr EST am 25. März 2024. Sie können **Nächste Aktualisierung am** ändern, indem Sie das Symbol **Bearbeiten** wählen. Wählen Sie das neue Datum und die neue Uhrzeit und anschließend **Aktualisieren**aus.

Sie können die Anzeige bestimmter Ereignistypen für Zeitleistenindikatoren und Zeitleistenbereiche entsprechend mit den Filter-Umschaltflächen aktivieren oder deaktivieren.

Zeitleiste



In der folgenden Tabelle finden Sie zusätzliche Funktionen, die mit der Zeitleistenkomponente verfügbar sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Funktionen der Zeitleistenkomponente

Aufgabe	Beschreibung
Neues Ereignis	Erstellt neue anwenderdefinierte Ereignisse und ordnet diese Ereignisse dem MSI-Datensatz zu. Dies hilft beim Erstellen von Ereignissen für vergangene und zukünftige Daten, die andernfalls möglicherweise nicht über eine beschriftete Aufgabe, eine Datensatzstatusänderung oder eine beschriftete Zusammenarbeitsaktivität erfasst werden, die standardmäßig auf der Zeitleiste angezeigt werden.
Neu laden	Aktualisiert die Zeitleisten-Ereignisse, um die neuesten Aktualisierungen anzuzeigen.
Zeitleistenindikatoren	Listet die verschiedenen Ereignistypen auf, z. B. Änderungen am Feld „Now Record“, „Beschriftete Zusammenarbeitsaktivitäten“ und „Andere (anwenderdefiniert)“, zusammen mit den Symbolen und der Gesamtzahl der Ereignisse, die für jeden Ereignistypindikator aufgetreten sind. Mit dem Schiebeindikator können Sie alle Ereignisse für einen bestimmten Ereignistyp aktivieren oder deaktivieren.
Legende anzeigen	Wählen Sie diese Option aus, um die Dropdown-Legende mit verschiedenen Arten von Zeitleistenindikatoren anzuzeigen.
Fortschrittsbalken auf der Zeitleiste	Zeigt den Gesamtfortschritt des incident über festgelegte Zeitleistenereignisse oder Meilensteine an, die innerhalb der verschiedenen angezeigten Zeitleistenbereiche aufgetreten sind. Sie können einen Ereignistyp auch mit einer Ereigniskategorie verknüpfen. Nachdem Sie es verknüpft haben, werden die Ereignisdetails an beiden Stellen der Zeitleiste aktualisiert.
Zeitleistenbereiche	Zeigt verschiedene Arten von Incident-Status und deren Dauer an, während der Incident während des gesamten Lebenszyklus eines schwerwiegenden Security Incident fortschreitet. Aktivieren oder deaktivieren Sie ein bestimmtes Ereignis basierend auf dem Incident-Status.

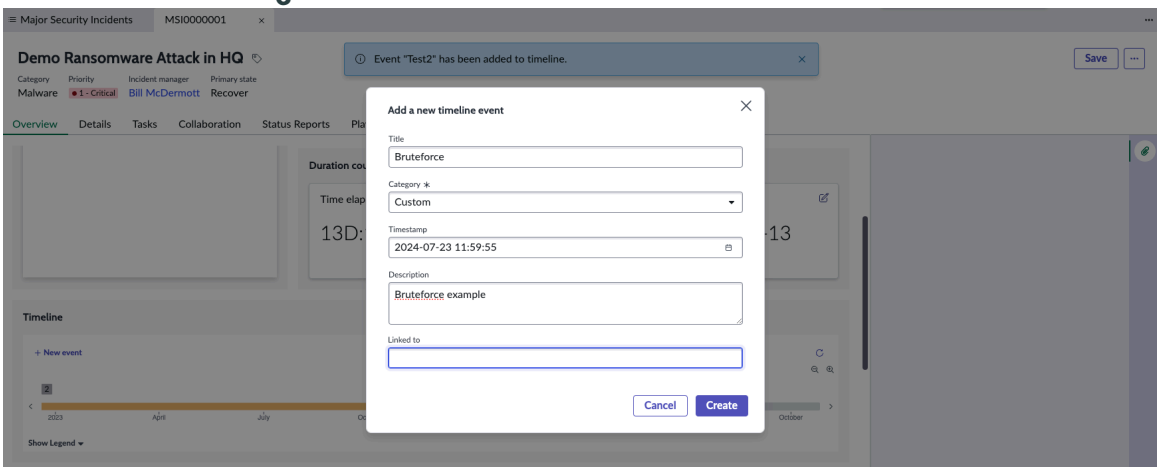
Erstellen Sie ein Zeitleistenereignis

Um ein neues Zeitleisten-Ereignis zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie auf der Registerkarte Übersicht zum Abschnitt **Zeitleiste**.
2. Auswahlvorgang **+ Neues Ereignis**.
3. Füllen Sie die Felder im Popup-Fenster „Neues Zeitleisten-Event hinzufügen“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neues Zeitleistenereignis



Aufgabe	Beschreibung
Titel	Geben Sie den Titel für das Zeitleistenereignis ein.
Kategorie	Wählen Sie eine Kategorie für das Zeitleistenereignis aus. Die folgenden Kategorien werden als Teil des Basissystems bereitgestellt, und Sie können eine entsprechend Ihren Anforderungen auswählen. ○ **Anwenderdefiniert**. ○ **Antwort**. ○ **Bedrohung**. Informationen zum Hinzufügen oder Konfigurieren einer Zeitleisten-Ereigniskategorie finden Sie unter Konfigurieren Sie Zeitleistenkategorien für schwerwiegende Security Incidents.
Zeitstempel	Wählen Sie das Datum und die Uhrzeit des Zeitleistenereignisses mithilfe des Zeitstempel-Kalenders aus. Sie können der Zeitleiste vor und nach dem Startdatum Ereignisse hinzufügen.
Beschreibung	Geben Sie eine kurze Beschreibung des Zeitleistenereignisses an.
Verknüpft mit	Option zum Verknüpfen des Zeitleistenereignisses mit einem Datensatz für schwerwiegende Security Incidents.

4. Auswahlvorgang **Erstellen**.
5. Sie können die Symbole **„Vergrößern“** und **„Verkleinern“** verwenden, um den Fortschrittsbalken der Zeitleiste zu vergrößern oder zu verkleinern. Er umfasst die Anzeige einzelner Ereignisse, während Zahlen angezeigt werden, um mehrere Ereignisse in unmittelbarer zeitlicher Nähe darzustellen.

   Sie können auch die Standardzoomstufe hinzufügen, um alle Ereignisse anzuzeigen.
6. Wählen Sie das **Aktualisieren** -Symbol, um die neuesten Zeitleistenereignisse anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

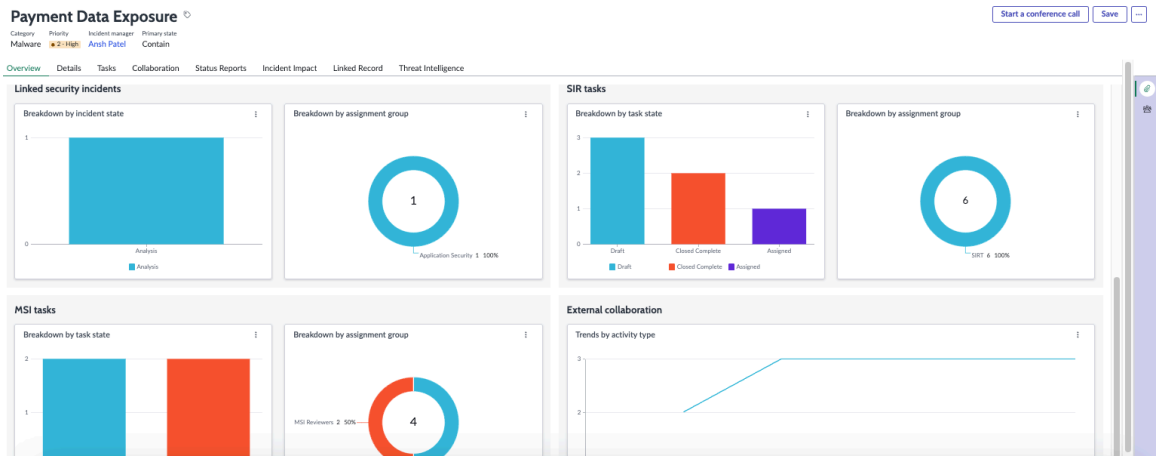
Zeigen Sie Major Security Incident Trenddiagramme an

Zeigen Sie die Metriken zum Fortschritt schwerwiegender Security Incident-Auswirkungen in Form von Balkendiagrammen und Diagrammen an.

Zusätzlich zur Visualisierungen der Incident-Zeitleiste und des Fortschrittstrenddiagramms bietet **Übersicht** Die Registerkarte enthält relevante Auswirkungsmetriken, um den sich ändernden Umfang des incident zu verwalten, einschließlich Rollup der betroffenen Assets, Benutzer, Standorte und Teamressourcen.

Die in den Visualisierungskomponenten angezeigten Anzahlen basieren auf aktiven Aufgaben für verknüpfte Security Incident Response-Incidents (SIR). Beim Öffnen und Schließen von Aufgaben ändern sich diese Anzahlen in Bezug auf Art und Umfang der verbleibenden Aktivitäten, die für den schwerwiegenden Security Incident geplant sind, um die in den Komponenten der Trenddiagramm-Visualisierung angezeigten Trends darzustellen.

Auswirkungsmetriken der Registerkarte „MSIM-Übersicht“.



In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie über ausführen können **Übersicht** Abschnitt:

Übersichts-UI-Abschnitte

Titel	Beschreibung
Zeit	Zeigt den Zeitraum in Gesamtanzahl von Tagen ab dem Zeitpunkt an, ab dem der schwerwiegende Security Incident aktiv ist. Die Zeit wird basierend auf berechnet **Erkennungsdatum** wurde in eingegeben **Details** Registerkarte des -Arbeitsbereichs. Das Erkennungsdatum wird häufig anfänglich erfasst, wenn der schwerwiegende Security Incident zum ersten Mal erstellt oder vorgeschlagen wurde. Bei jeder Änderung dieses Datums wird die Uhrzeit automatisch berechnet, aktualisiert und im Format „Tage:Stunden:Minuten“ angezeigt, z. B. 20T: 13 Uhr: 58 M.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichts-UI-Abschnitte (Fortsetzung)

Titel	Beschreibung
	Geschätztes Lösungsdatum: Das Datum, bis zu dem das Lösungsdatum des incident geschätzt wird. Dieses Datum wird häufig zu Beginn der Erstellung oder Heraufstufung des schwerwiegenden Security Incident erfasst. Das Datum wird basierend auf dem in angegebenen geschätzten Datum aktualisiert **Details** Registerkarte des -Arbeitsbereichs. Wenn das geschätzte Datum im Abschnitt „Details“ nicht angegeben ist, wird in diesem Abschnitt „Himmelstrich“ ohne Datumswert angezeigt.
Aktives Team	Zeigt die verschiedenen Antwortteams und Teammitglieder jedes Teams an, die aktiv an dem schwerwiegenden Security Incident und den zugehörigen Aufgaben arbeiten. **Aktives Team** Trend: Zeigt das Trenddiagramm jedes Teams und seiner Teammitglieder an, die in regelmäßigen Abständen aktiv an dem schwerwiegenden Security Incident und den zugehörigen Aufgaben arbeiten. **Hinweis:** Zeigen Sie die zugewiesenen aktiven Gruppen aus dem an **Details** Registerkarte des -Arbeitsbereichs.
Verknüpfte SIR-Incidents	**Nach Incident-Status**: Zeigen Sie die Verteilung verknüpfter Security Incidents basierend auf einem Incident-Status wie Analyse, Eindämmen, Beseitigen, Wiederherstellen oder Überprüfen an. **Trends nach Incident-Status**: Zeigt außerdem in der Trendansicht den Fortschritt der Anzahl verknüpfter Incidents basierend auf dem Incident-Status an. Wenn Sie die einzelnen Incident-Statuslinks auswählen, können Sie navigieren und die Details der verknüpften Security Incidents direkt im anzeigen **Verknüpftes SI/VI** Registerkarte des -Arbeitsbereichs. Dieser Abschnitt wird automatisch aktualisiert, wenn Änderungen an den zugrunde liegenden Incidents auftreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichts-UI-Abschnitte (Fortsetzung)

Titel	Beschreibung
SIR-Aufgaben	Zeigt die Gesamtzahl aktiver Aufgaben an, die über SIR-Incidents mit dem MSI-Datensatz verknüpft sind. • **Nach Aufgabenstatus**: Zeigen Sie die Incident-Antwortaufgaben basierend auf dem Incident-Status an, z. B. Entwurf, Zugewiesen, In Arbeit, Abgeschlossen. Dieses Verteilungsdiagramm ermöglicht eine weitere Aufgliederung der Verteilung nach Zuweisungsgruppen. Wenn Sie die einzelnen Aufgabenstatus auswählen, können Sie im eine nach Incident-Aufgabenstatus gefilterte Liste anzeigen **Aufgaben** Registerkarte des -Arbeitsbereichs. In der gefilterten Ansicht können Sie einzelne Aufgabendetails anzeigen und aktualisieren. • **In Bearbeitung befindliche Aufgaben nach Incident-Statusbezeichnung**: Zeigt aktive Aufgaben und Gruppen basierend auf der Incident-Statusbezeichnung an, die in den Komponenten des Aufgabenorganisators angewendet werden muss. Diese Standardbezeichnungen haben Werte wie „Analyse“, „Eindämmen“, „Beseitigen“, „Wiederherstellen“ oder „Überprüfen“, um die Art der betreffenden Aufgabe anzugeben. • **Überfällig**: Zeigt die Security Incident Response-Aufgaben an, die aktiv sind und das Fälligkeitsdatum überschritten haben. Sie können die Details aller überfälligen Aufgaben anzeigen, indem Sie die Gesamtanzahl der Überfälligen auswählen und automatisch zur Registerkarte Aufgaben navigieren lassen. • **Trends nach Aufgabenstatus**: Zeigen Sie den Fortschrittstrend von in Arbeit und von geschlossenen Antwortaufgaben über die Incident-Dauer an. **Hinweis:** Das Trenddiagramm ruft die neuesten Daten basierend auf der geplanten Aufgabe ab. Sie können das Zeitintervall für den Datenabruf nach Bedarf konfigurieren oder ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichts-UI-Abschnitte (Fortsetzung)

Titel	Beschreibung
MSI-Aufgaben	Zeigt insgesamt aktive Aufgaben an, die direkt im MSI-Datensatz erstellt wurden (und keine verknüpften Antwortaufgaben sind): **Nach Aufgabenstatus:** Zeigen Sie die erstellten schwerwiegenden Security Incidents, die zugewiesenen Aufgaben und die zugehörigen Informationen an. Wenn Sie die einzelnen Aufgabenstatus auswählen, können Sie im eine nach Incident-Aufgabenstatus gefilterte Liste anzeigen **Aufgaben** Registerkarte des -Arbeitsbereichs. In der gefilterten Ansicht können Sie einzelne Aufgabendetails anzeigen und aktualisieren.
Externe Zusammenarbeit	Zeigt Zusammenarbeitsaktivitäten für alle gekennzeichneten Zusammenarbeitsaktivitäten aus dem Aktivitätenstrom Zusammenarbeit an: • **Nach Incident-Statusbezeichnung:**Zeigen Sie auf der Registerkarte **Zusammenarbeit** des -Arbeitsbereichs die Daten der Zusammenarbeitsaktivitäten für Incidents an, die mit den Dateien und Ordnern Microsoft Teams und Microsoft SharePoint koordiniert sind und mit Incident-Statusbezeichnungen wie Analyse, Eindämmen, Beseitigen oder Wiederherstellen gekennzeichnet sind. • **Trends nach Aktivitätstyp**: Zeigen Sie das Trenddiagramm für die Anzahl der Datei- und Ordneraktivitäten von Microsoft Teams und Microsoft SharePoint über die Incident-Dauer an.

Automatische Übersetzung

Aktualisieren Sie Major Security Incident Details

Zeigen Sie bestimmte Details im Zusammenhang mit dem schwerwiegenden Security Incident an, und aktualisieren Sie sie, z. B. Details zum Incident-Datensatz, aktive Teammitglieder und das entsprechende Aktivitätsprotokoll.

Alle zugehörigen Details des schwerwiegenden Security Incident werden mit verschiedenen Formularabschnitten auf der Registerkarte **Details** des -Arbeitsbereichs angezeigt. Zeigt Detailinformationen wie Incident-Datensatzdetails, aktive Teammitglieder und das entsprechende Aktivitätsprotokoll an. Sie können auch die verknüpften SIR-Incidents und Datensatzdetails zu Schwachstellengruppen anzeigen und eine Aktivitätsveröffentlichung an alle verknüpften Incident-Datensätze übertragen.

Die Registerkarte „Details“ enthält primär:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Felder des Formulars für schwerwiegende Security Incidents und UI-Abschnitte im Zusammenhang mit Incidents.
2. Aktivitätenstrom

Die folgende Tabelle enthält die Details der Felder des Formulars für schwerwiegende Security Incidents:

Formularabschnitte „Schwerwiegender Security Incident“.

Feld	Beschreibung
Incident	
Nummer	Datensatznummer des schwerwiegenden Security Incidents.
Primärer Status	Primärer Status des Datensatzes für schwerwiegenden Security Incidents
Erkennungsdatum	Das Datum, an dem der schwerwiegende Security Incident zum ersten Mal erstellt oder vorgeschlagen wurde. Wenn Sie das Erkennungsdatum auf der Registerkarte Details ändern, werden Datum und Uhrzeit des MSI automatisch berechnet, aktualisiert und im angezeigt **Zeit** > **Zeit seit Beginn des Incidents** Abschnitt im Abschnitt **„Übersicht“** des Arbeitsbereichs.
Titel	Titel des schwerwiegenden Security Incidents.
Codename	Codename für den schwerwiegenden Security Incident Beispiel: Bluetiger.
Nächstes Update am	Datum und Uhrzeit des nächsten Updates zur Lösung schwerwiegender Security Incidents. Beispiel: 17:00 Uhr EST am 25. März 2024.
Kategorie	Kategorie des schwerwiegenden Security Incidents.
Unterkategorie	Unterkategorietyp des schwerwiegenden Security Incident.
Geschätztes Lösungsdatum	Das geschätzte Datum, bis zu dem der Incident gelöst werden soll. Der Standardwert ist 7 Tage ab dem Zeitpunkt der Erstellung des schwerwiegenden Security Incidents.
Priorität	Priorität des schwerwiegenden Security Incident.
Warnungssensor	Warnungssensor des schwerwiegenden Security Incidents. Beispiel: Vom Anwender gemeldetes Phishing.
Quelle	Quelle des schwerwiegenden Security Incidents.
Aktives Team	
Incident-Manager	Name des Incident-Managers.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularabschnitte „Schwerwiegender Security Incident“. (Fortsetzung)

Feld	Beschreibung
Zuweisungsgruppen	Gibt die verschiedenen Antwortteams und die Teammitglieder jedes Teams an, die aktiv an dem schwerwiegenden Security Incident arbeiten.
Kandidat	
MSI-Kandidatenstatus	Gibt den Status des Kandidaten für schwerwiegenden Security Incident an, z. B. „Vorgeschlagen“ oder „Heraufgestuft“. Wenn der Incident hochgestuft wird, wird der Status als Akzeptiert angezeigt.
Heraufgestuft durch	Benutzer, der den schwerwiegenden Security Incident heraufgestuft hat.
Heraufgestuft	Datum, an dem der schwerwiegende Security Incident heraufgestuft wurde.
Begründung	Begründung für den schwerwiegenden Security Incident. Die Begründung muss die MSI-Nummer und den Codenamen enthalten.
Potenzieller Impact	Potenzielle Auswirkung und Schweregrad des schwerwiegenden Security Incidents. Die „Potenzielle Auswirkung“ sollte die MSI-Nummer und den Codenamen enthalten.
Beschränkung	
Beschränkung erzwingen	Wählen Sie diese Option aus, um Einschränkungen für bestimmte schwerwiegende Einschränkungen für Security Incidents zu erzwingen. Sie können Einschränkungen erzwingen, um den Ansichts- oder Änderungszugriff nur auf bestimmte Benutzer oder Gruppen zu beschränken. Weitere Informationen finden Sie unter Beschränken Sie den Zugriff auf bestimmte schwerwiegende Security Incidents.
Zulässige Mitglieder	Liste der Benutzer, die auf den schwerwiegenden Security Incident zugreifen können.
Zulässige Gruppen	Liste der Gruppen, die auf den schwerwiegenden Security Incident zugreifen können.
Andere Aktionen	
Anhang	Alle Anhänge im Zusammenhang mit dem schwerwiegenden Security Incident. Wählen Sie die Option Option **auswählen** aus, um dem Incident Anhänge hinzuzufügen.
Telefonkonferenz	Nutzen Sie Telefonkonferenzen mit Drittpartei-Service Providern als Kommunikationskanal, um sich mit den Stakeholdern zu treffen und schwerwiegende Security Incidents zu lösen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularabschnitte „Schwerwiegender Security Incident“. (Fortsetzung)

Feld	Beschreibung
	Weitere Informationen finden Sie unter Management schwerwiegender Sicherheits-Incidents Integration mit Telefonkonferenzen

Aktivität:

Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und bei Bedarf zusätzliche Kommentare hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügte Aktivität oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

Hinweis:
Wählen Sie den Link **Weitere Details anzeigen**, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, die diesem schwerwiegenden Security Incident zugeordnet sind.

Legen Sie Ihre Einstellungen fest, um die zugehörigen Aktivitäten anzuzeigen, z. B.:

1. **Filter**: Wählen Sie das Symbol **Filtersätze**, um Filter festzulegen.

   Legen Sie Filter fest, um die Aktivitätskonversationen anzuzeigen, z. B. Aktivitäten, die in den Arbeitsnotizen, der E-Mail, der Zeitleiste und zusätzlichen Kommentaren hinzugefügt wurden.

2. **Gekennzeichnet**: Wählen Sie das Symbol **„Gekennzeichnet“** aus, um die Aktivitäten zu kennzeichnen.

   Markieren Sie wichtige Aktivitätskonversationen, damit Sie sie immer zur Hand haben.

Beschränken Sie den Zugriff auf bestimmte schwerwiegende Security Incidents

Verwalten Sie, wer schwerwiegende Security Incidents anzeigen oder ändern kann, die vertrauliche Informationen enthalten. Sie können Einschränkungen schwerwiegender Security Incidents erzwingen, um zu bestimmen, wer Zugriff auf das Anzeigen oder Ändern bestimmter Datensätze schwerwiegender Security Incidents und zugehöriger Listen hat, und den Lese- oder Schreibzugriff auf bestimmte Benutzer oder Gruppen beschränken.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

Warum und wann dieser Vorgang ausgeführt wird
Mit Einschränkungen für schwerwiegende Security Incidents können Sie verhindern, dass kritische schwerwiegende Security Incidents von allen Benutzern oder Gruppen in einer bestimmten Organisation aufgerufen oder geändert werden. Mit diesen Einschränkungen können Sie die schwerwiegenden Security Incidents, die ein Benutzer oder eine Gruppe anzeigen oder ändern kann, präziser steuern. Sie können eine Einschränkung für schwerwiegende Security Incidents erzwingen, indem Sie das Kontrollkästchen **Einschränkung erzwingen** aktivieren und die Benutzer oder Gruppen auswählen, die den jeweiligen schwerwiegenden Security Incident anzeigen oder ändern dürfen.

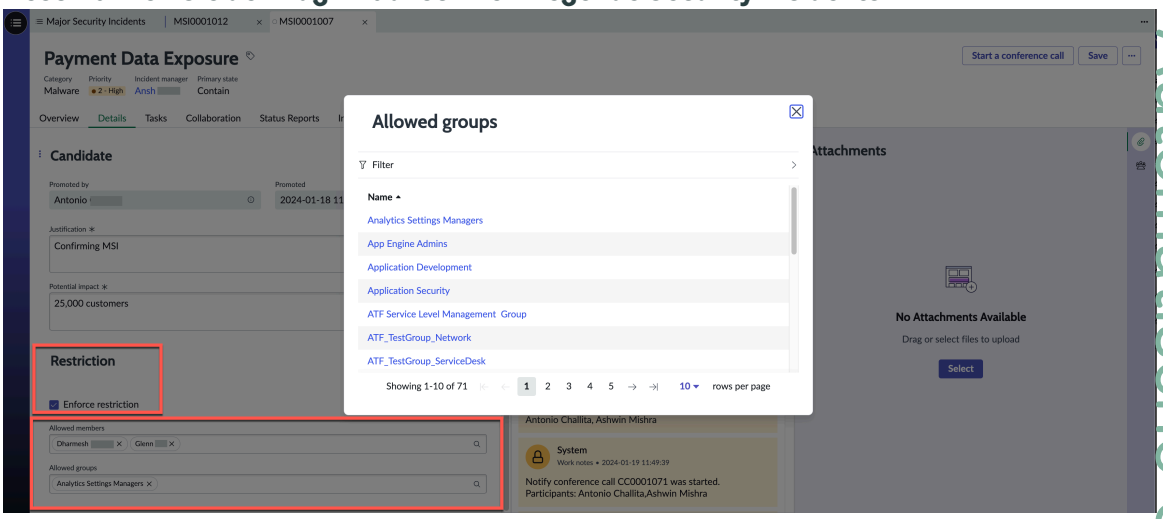
Nachdem Sie die Einschränkung für schwerwiegende Security Incidents oder zugehörige Listen auf bestimmte Anwender oder Gruppen erzwungen haben, können alle verbleibenden Anwender oder Gruppen in Ihrer Organisation diese schwerwiegenden Security Incidents oder zugehörigen Listen nicht mehr anzeigen oder ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.
3. Wählen Sie den gewünschten Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Details** aus.
5. Scrollen Sie nach unten, und wählen Sie den Abschnitt **Einschränkung** aus.
6. Aktivieren Sie das Kontrollkästchen **Einschränkung erzwingen**, um die Einschränkung des schwerwiegenden Security Incident zu aktivieren.

Beschränken Sie den Zugriff auf schwerwiegende Security Incidents



7. Wählen Sie im Feld Zulässige Mitglieder die Benutzer aus, die den schwerwiegenden Security Incident mithilfe der Suchoption anzeigen oder ändern können.
8. Wählen Sie im Feld Zulässige Gruppen mithilfe der Suchoption die Gruppen aus, die den schwerwiegenden Security Incident anzeigen oder ändern können.

Hinweis:
Nachdem das Kontrollkästchen **Einschränkung erzwingen** für den schwerwiegenden Security Incident aktiviert ist, können nur der sn_msi.workspace_manager und die zugehörigen Mitglieder oder Gruppen den schwerwiegenden Security Incident anzeigen oder ändern.

9. Wählen Sie **Speichern**.

Zusätzliche Datensätze mit verknüpfen Major Security Incident

Verwenden Sie im -Arbeitsbereich die Funktion zum Verknüpfen von Datensätzen, um alle zugehörigen Security Incident-Datensätze und die zugehörigen untergeordneten Security Incidents, Korrekturaufgaben aus Vulnerability Response und Sicherheitsfälle aus Threat Intelligence mit einem Datensatz Major Security Incident (MSI) zu verknüpfen.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager und sn_msi.workspace_responder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Major Security Incident Response** > **MSIM-Arbeitsbereich**.
2. Navigieren Sie zur Ansicht **Listen**, die im linken Bereich des Arbeitsbereichs angezeigt wird.
3. Klicken Sie auf **Akzeptiert**, um die heraufgestuften Datensätze für schwerwiegende Security Incidents auszuwählen.
4. Wählen Sie aus der Liste der heraufgestuften Datensätze den Incident-Datensatz aus, der verknüpft werden muss und sich nicht im Status „Geschlossen“ befindet.
5. Klicken Sie auf die Registerkarte **Verknüpfte Datensätze**.
   Eine Dropdown-Liste zur Auswahl anderer verknüpfter Datensatztabellen wird bereitgestellt.
   Im Abschnitt „Verknüpfte Datensätze“ werden die verknüpften Datensätze und die zugehörigen Datensätze angezeigt, die mit dem schwerwiegenden Security Incident verknüpft wurden.
6. Wählen Sie in der Liste die gewünschte Tabellenansicht aus, z. B. „Security Incidents“, „Korrekturaufgaben“ (angreifbare Elemente) oder „Sicherheitsfall“.
   Basierend auf der Ansicht der Datensatztabelle für den Auswahltyp werden die verknüpften Datensätze angezeigt, die mit den Datensätzen für schwerwiegende Security Incidents verknüpft sind.
7. Verknüpfen Sie einen Datensatz, der mit keinem MSI-Datensatz verknüpft ist und sich im Status „ **Offen** “ befindet, indem Sie den Datensatz auswählen und oben rechts auf der Seite **auf Datensatz verknüpfen** klicken.

   Hinweis:
   Sie können einen Incident-Datensatz nicht mit einem MSI-Datensatz verknüpfen, wenn er sich im Status „ **Geschlossen** “ befindet.

8. Wählen Sie den zu verknüpfenden Datensatz aus, und klicken Sie auf **Link**.
   In einer Bestätigungsmeldung wird angezeigt, dass der Datensatz erfolgreich verknüpft wurde und das Rollup zugehöriger Datensätze im Hintergrund verarbeitet wird.

   Hinweis:
   Nachdem ein Datensatz verknüpft wurde, wird die Listenansicht automatisch aktualisiert, und zeigt die aktualisierte Liste der Incident-Datensätze an.

Zugehörige Informationen

Verknüpfung von Datensätzen mit aufheben Major Security Incident

Verknüpfung von Datensätzen mit aufheben Major Security Incident

Heben Sie im Arbeitsbereich „Major Security Incident Management“ die Verknüpfung der Datensätze zu schwerwiegenden Security Incidents im Abschnitt Verknüpfte Datensätze auf.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager und sn_msi.workspace_responder

Hinweis:
Sie können jeweils nur die Verknüpfung eines Datensatzes aufheben. Nachdem Sie die Verknüpfung eines Datensatzes aufgehoben haben, werden die zugehörigen Rollup-Informationen aus den Abschnitten „Auswirkung von Incidents“ und „Threat Intelligence“ im Arbeitsbereich entfernt, und die Aktion kann nicht rückgängig gemacht werden.

Weitere Informationen zum Rollup von Datensätzen finden Sie unter Rollup-Framework für MSIM.

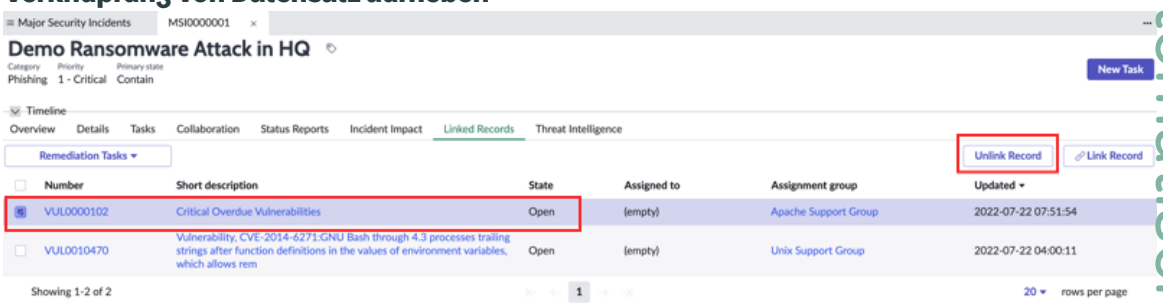
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

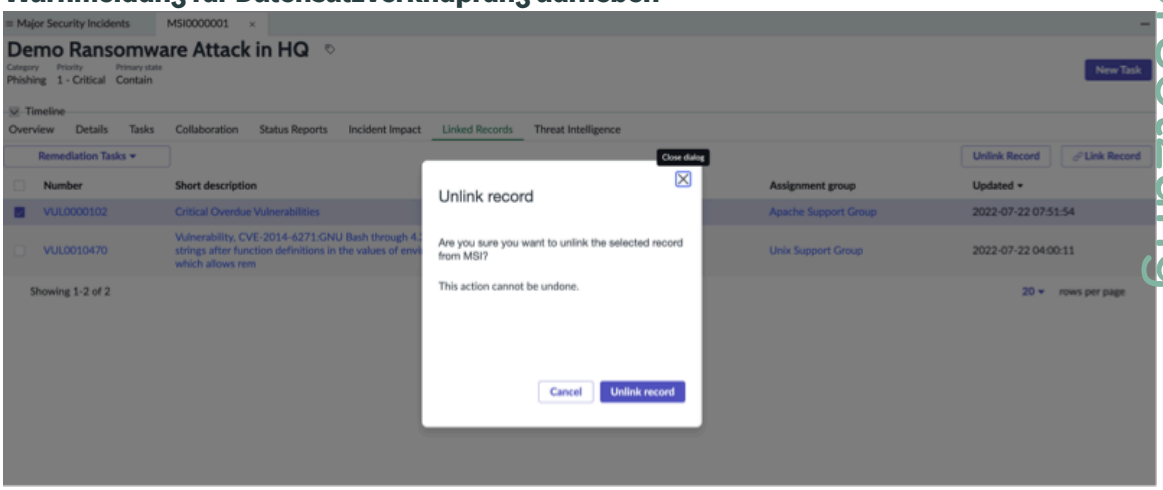
1. Navigieren zu **Major Security Incident Response** > **MSIM-Arbeitsbereich**.
2. Navigieren Sie zur Ansicht **Listen**, die im linken Bereich des Arbeitsbereichs angezeigt wird.
3. Klicken Sie auf **Akzeptiert**, um die heraufgestuften Datensätze für schwerwiegende Security Incidents auszuwählen.
4. Klicken Sie auf die Registerkarte **Verknüpfte Datensätze**.
   In diesem Abschnitt werden die verknüpften Datensätze und die zugehörigen Datensätze angezeigt, die mit dem schwerwiegenden Security Incident verknüpft sind.
5. Wählen Sie die gewünschte Tabellenansicht aus, z. B. Security Incidents, Korrekturaufgaben (angreifbare Elemente) oder Sicherheitsfall.
6. Wählen Sie den Datensatz aus, um die Verknüpfung mit der Listenansicht der Datensätze aufzuheben.
7. Klicken Sie auf **Verknüpfung aufheben für Datensatz aufheben**.

Verknüpfung von Datensatz aufheben



8. Es wird eine Warnmeldung angezeigt, in der Sie gefragt werden, ob Sie die Verknüpfung des ausgewählten Datensatzes mit MSI aufheben möchten.

Warnmeldung für Datensatzverknüpfung aufheben



9. Klicken Sie auf **Verknüpfung aufheben für Datensatz aufheben**.
   Der Datensatz ist nicht verknüpft. Sobald die Verknüpfung aufgehoben wurde, können die Änderungen nicht mehr rückgängig gemacht werden. Die Listenansicht der verknüpften Datensätze wird nach dem Aufheben der Verknüpfung aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurieren Sie verknüpfte Datensätze in Management schwerwiegender Sicherheits-Incidents

Rollup-Datensätze in konfigurieren Management schwerwiegender Sicherheits-Incidents

Verwalten Sie Aufgaben in einem Major Security Incident

Auf der Registerkarte Aufgabe können Sie alle Aufgaben im Zusammenhang mit schwerwiegenden Security Incidents über den MSIM-Arbeitsbereich nachverfolgen und verwalten. Sie können die verschiedenen Aufgaben mithilfe des standardmäßigen visuellen Taskboards (Kanban-Ansicht) oder der Listenansicht anzeigen.

sn_msi.workspace_manager kann auf der Registerkarte Aufgaben:

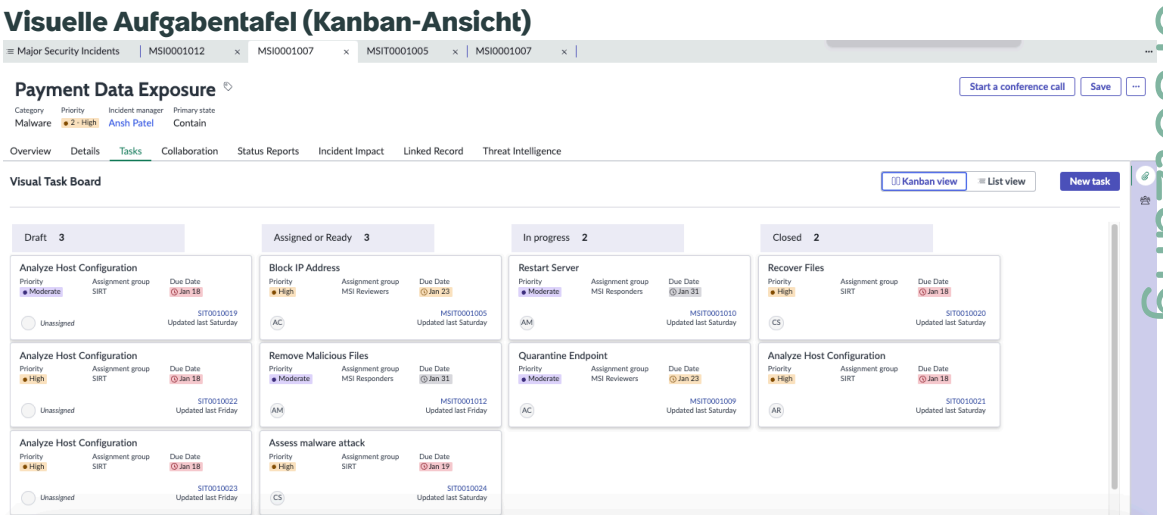
- Eine Aufgabe erstellen
- Aufgaben ändern
- Aufgaben anzeigen und sich selbst oder anderen zuweisen
- Löschen Sie Aufgaben

Hinweis:
Stellen Sie sicher, dass Sie die App **„MSIM-VTB-Aufgabenkarte: 1.0.1v“** separat nach der Installation der MSIM-App installiert haben.

Auf der Registerkarte Aufgaben werden die Details aller Aufgaben angezeigt, die einem schwerwiegenden Security Incident zugeordnet sind. Die Registerkarte „Aufgabe“ unterstützt zwei Ansichten:

- **Visuelle Aufgabentafel (Kanban-Ansicht)**:

  Zeigen Sie mehrere Aufgabendatensätze an, und aktualisieren Sie sie. Sie werden auf dem visuellen Taskboard als Karten angezeigt und können basierend auf dem Status der Aufgaben im schwerwiegenden Security Incident zwischen Spuren verschoben werden.



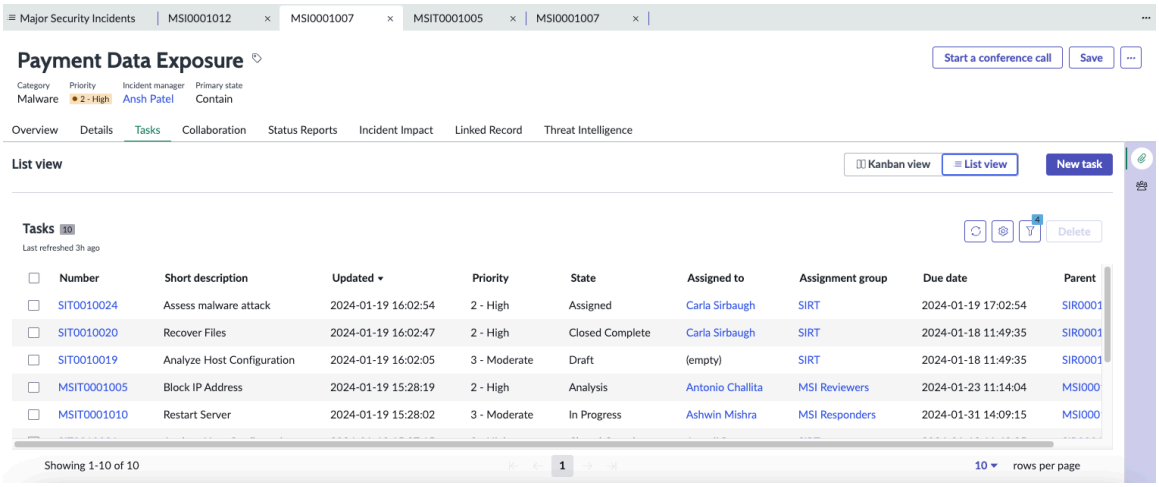
- **Listenansicht**:

  Zeigen Sie mehrere Aufgabendatensätze an, und aktualisieren Sie sie mithilfe von in Form von Listen. Mit diesen Listenkategorien und Filtern können Sie schnell die Aufgaben finden und nachverfolgen, an denen Sie bei einem schwerwiegenden Security Incident arbeiten müssen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listenansicht



Die gekennzeichneten Aktivitäten werden zusammengefasst und im Abschnitt Übersicht des schwerwiegenden Security Incident angezeigt. Im Abschnitt „Übersicht“ ist ein Trenddiagramm verfügbar, um den Status der konsolidierten Aufgabenaktivitäten anzuzeigen.

Verwalten Sie Aufgaben mit dem visuellen Taskboard

Verfolgen und verwalten Sie alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind, mithilfe des visuellen Taskboards (Kanban-Ansicht).

Sie können das visuelle Taskboard verwenden, um die Karten je nach Status der Aufgaben Schritt für Schritt zwischen Spuren wie Entwurf, Zugewiesen oder Bereit, In Bearbeitung und Geschlossen zu verschieben. Ein Aktivitätenstrom auf der Tafel zeigt die letzten Aktivitäten an, um Aufgabenänderungen einfach nachzuverfolgen. Sie können Aufgabenkarten aus jeder Tabelle hinzufügen, die Aufgabe erweitert, um Updates schnell nachzuverfolgen und schwerwiegende Security Incidents direkt über die Tafel zu bearbeiten.

Erstellen Sie eine Aufgabe mit dem visuellen Taskboard

Erforderliche Rolle: sn_msi.workspace_manager.

Hinweis:
Stellen Sie sicher, dass Sie die App **„MSIM-VTB-Aufgabenkarte: 1.0.1v“** separat nach der Installation der MSIM-App installiert haben.

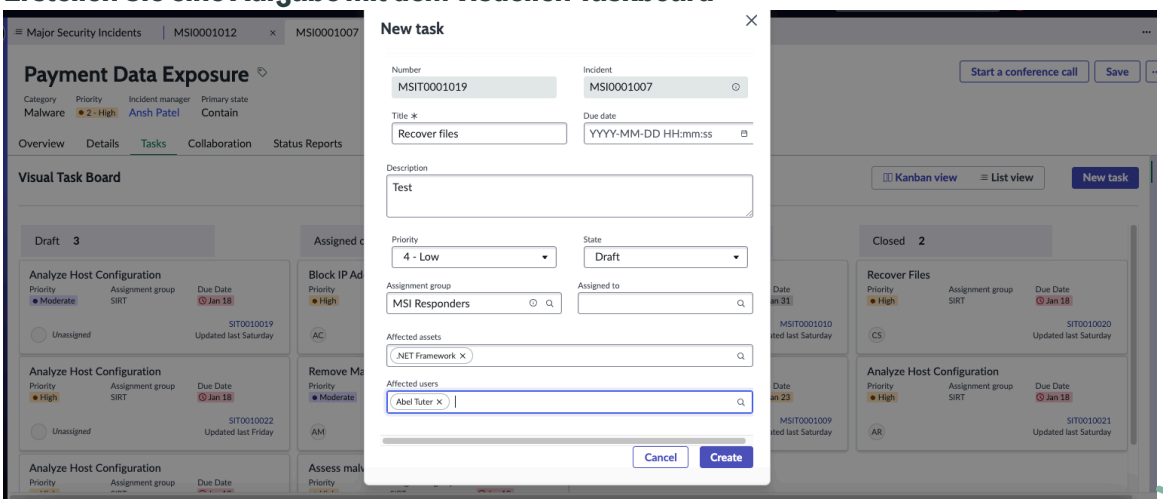
Gehen Sie wie folgt vor, um eine Aufgabe auf dem visuellen Taskboard zu erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.
3. Wählen Sie den gewünschten Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Aufgaben**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Aufgabe mit dem visuellen Taskboard



5. Wählen Sie **Kanban-Ansicht**und dann **Neue Aufgabe**aus.

6. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Nummer	Eine eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie mithilfe der Option **Kalender** ein Datum aus, und geben Sie im Abschnitt Zeit auswählen die **Uhrzeit** an.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein: ○ **Keine** ○ **1 – Kritisch** ○ **2 – Hoch** ○ **3 – Mittel** ○ **4 – Niedrig** ○ **5: Planung**
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen.
Zugewiesen an	Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll.
Betroffene Assets	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Assets aus.
Betroffene Anwender	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Anwender aus.

7. Wählen Sie **Erstellen** aus, um die Aufgabe zu erstellen.

Zeigen Sie eine Aufgabe mit dem Visual Task Board an, und ändern Sie sie

Erforderliche Rolle: sn_msi.workspace_manager.

> **Hinweis:**
> Stellen Sie sicher, dass Sie die App **„MSIM-VTB-Aufgabenkarte: 1.0.1v“** separat nach der Installation der MSIM-App installiert haben.

MSI-Manager können die Details einer Aufgabe und Aktivitätsinformationen aus den MSI-Respondern anzeigen und eine Aufgabe im visuellen Taskboard mithilfe der folgenden Schritte ändern:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.
3. Wählen Sie den gewünschten Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Aufgaben** und dann **Kanban-Ansicht**.
5. Wählen Sie die gewünschte Aufgabenkarte in einer der Spuren aus, um die Details der Aufgabe anzuzeigen.

   Die Aufgabenkarte kann sich in einer der folgenden Spuren befinden: Entwurf, Zugewiesen oder Bereit, In Bearbeitung oder Geschlossen.
6. Im Abschnitt Aufgabeninformationen können Sie die folgenden Details ändern:

Feld	Beschreibung
Nummer	Eine eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

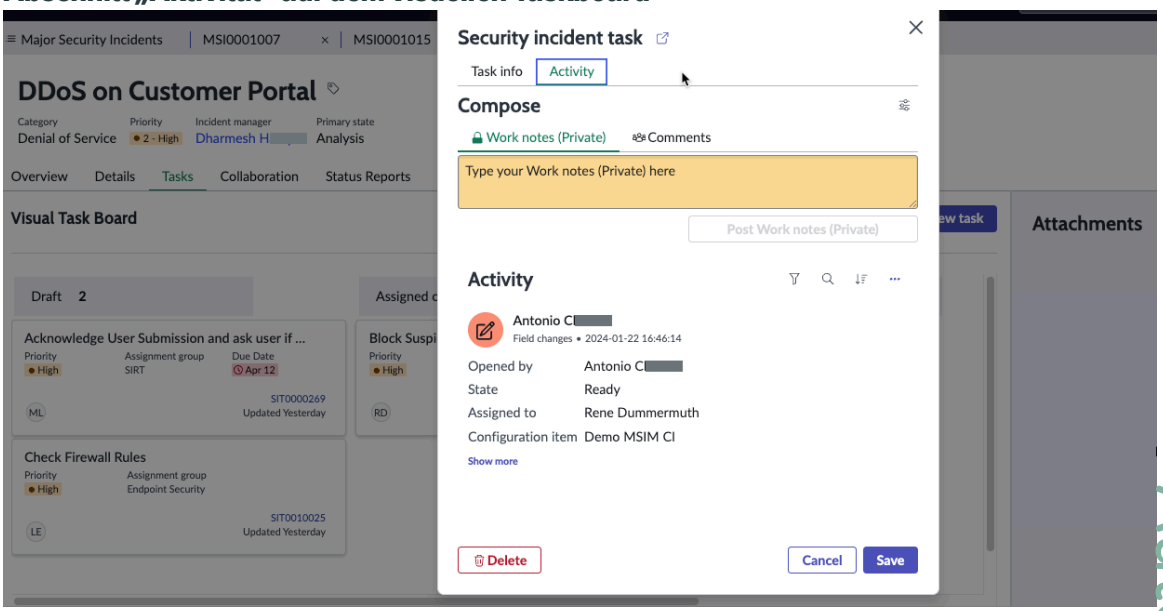
Feld	Beschreibung
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie mithilfe der Option **Kalender** ein Datum aus, und geben Sie im Abschnitt Zeit auswählen die **Uhrzeit** an.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein: ○ **Keine** ○ **1 – Kritisch** ○ **2 – Hoch** ○ **3 – Mittel** ○ **4 – Niedrig** ○ **5: Planung**
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse** ○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen.
Zugewiesen an	Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll.
Betroffene Assets	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Assets aus.
Betroffene Anwender	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Anwender aus.

7. Wählen Sie den Abschnitt **„Aktivität“** aus, um die Aktivitätsdetails aus den MSI-Respondern anzuzeigen.

   Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und bei Bedarf zusätzliche Kommentare hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügten Aktivitäten oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Aktivität“ auf dem visuellen Taskboard



Hinweis:
Wählen Sie den Link **Weitere Details anzeigen** aus, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, der diesem schwerwiegenden Security Incident zugeordnet ist.

8. Wählen Sie **Speichern**, um die Aufgabeninformationen zu aktualisieren.

   Die Aufgabeninformationen werden sofort aktualisiert.

Löschen Sie eine Aufgabe mit dem visuellen Taskboard

Erforderliche Rolle: sn_msi.workspace_manager.

Hinweis:
Stellen Sie sicher, dass Sie die App **„MSIM-VTB-Aufgabenkarte: 1.0.1v“** separat nach der Installation der MSIM-App installiert haben.

Der MSI-Manager kann eine Aufgabe im visuellen Taskboard wie folgt löschen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.
3. Wählen Sie den gewünschten Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Aufgaben** und dann **Kanban-Ansicht**
5. Wählen Sie die Aufgabenkarte aus, die Sie löschen möchten.
6. Wählen Sie im Popup-Fenster „Aufgabe für schwerwiegenden Security Incident“ die Option **Löschen** aus.

   Das Popup-Fenster „Aufgabe löschen“ wird angezeigt, in dem Sie aufgefordert werden, das Löschen der Aufgabe zu bestätigen.
7. Wählen Sie **Löschen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Aufgaben mithilfe der Listenansicht

Verfolgen und verwalten Sie mithilfe der Listenansicht alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind.

Die Listenansicht zeigt die Details aller Aufgaben an, die dem schwerwiegenden Security Incident zugeordnet sind, z. B. Aufgabennummer, Priorität, aktueller Status, Zugewiesen an, Zugewiesene Gruppe. Mit diesen Listenkategorien und Filtern können Sie schnell die erforderlichen Aufgaben finden und nachverfolgen, an denen Sie bei einem schwerwiegenden Security Incident arbeiten müssen.

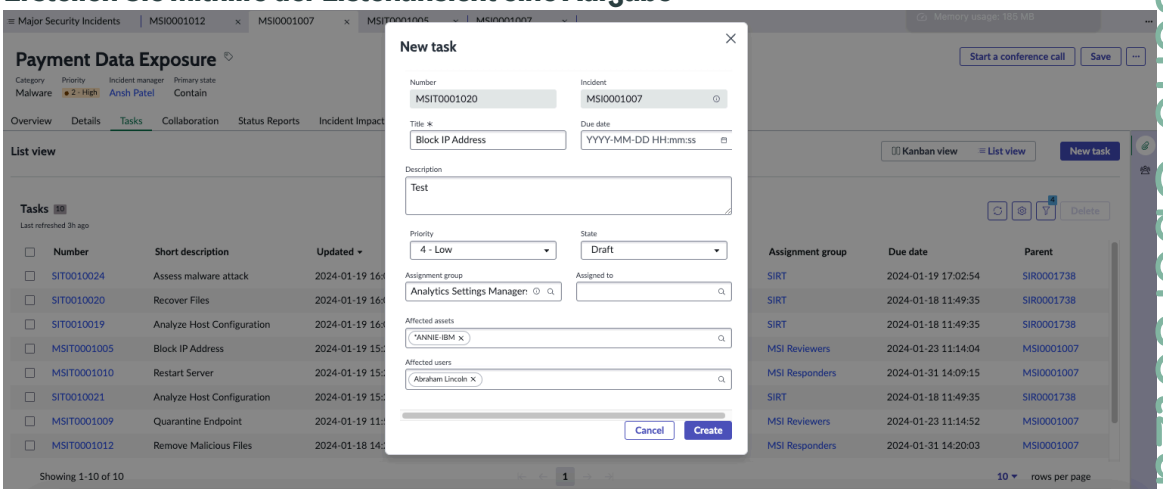
Erstellen Sie mithilfe der Listenansicht eine Aufgabe

Erforderliche Rolle: sn_msi.workspace_manager.

Gehen Sie wie folgt vor, um eine Aufgabe in der Listenansicht von MSI-Managern zu erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.
3. Wählen Sie den gewünschten Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Aufgaben**.

Erstellen Sie mithilfe der Listenansicht eine Aufgabe



5. Wählen Sie **Listenansicht**und dann **Neue Aufgabe**aus.
6. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Nummer	Eine eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie mithilfe der Option

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Kalender ein Datum aus, und geben Sie im Abschnitt Zeit auswählen die **Uhrzeit** an.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein: ○ **Keine** ○ **1 – Kritisch** ○ **2 – Hoch** ○ **3 – Mittel** ○ **4 – Niedrig** ○ **5: Planung**
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse** ○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen.
Zugewiesen an	Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll.
Betroffene Assets	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Assets aus.
Betroffene Anwender	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Anwender aus.

7. Wählen Sie **Erstellen** aus, um die Aufgabe zu erstellen.

Sie können eine Aufgabe mithilfe der Listenansicht anzeigen und ändern

Erforderliche Rolle: sn_msi.workspace_manager.

MSI-Manager können die Details einer Aufgabe und Aktivitätsinformationen aus den MSI-Respondern anzeigen und eine Aufgabe in der Listenansicht wie folgt ändern

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.
3. Wählen Sie den gewünschten Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Aufgaben** und dann **Listenansicht**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie die gewünschte Aufgabe in der Listenansicht aus, um die Details der Aufgabe anzuzeigen.
6. Im Abschnitt „Aufgabeninformationen“ können Sie die folgenden Details ändern:

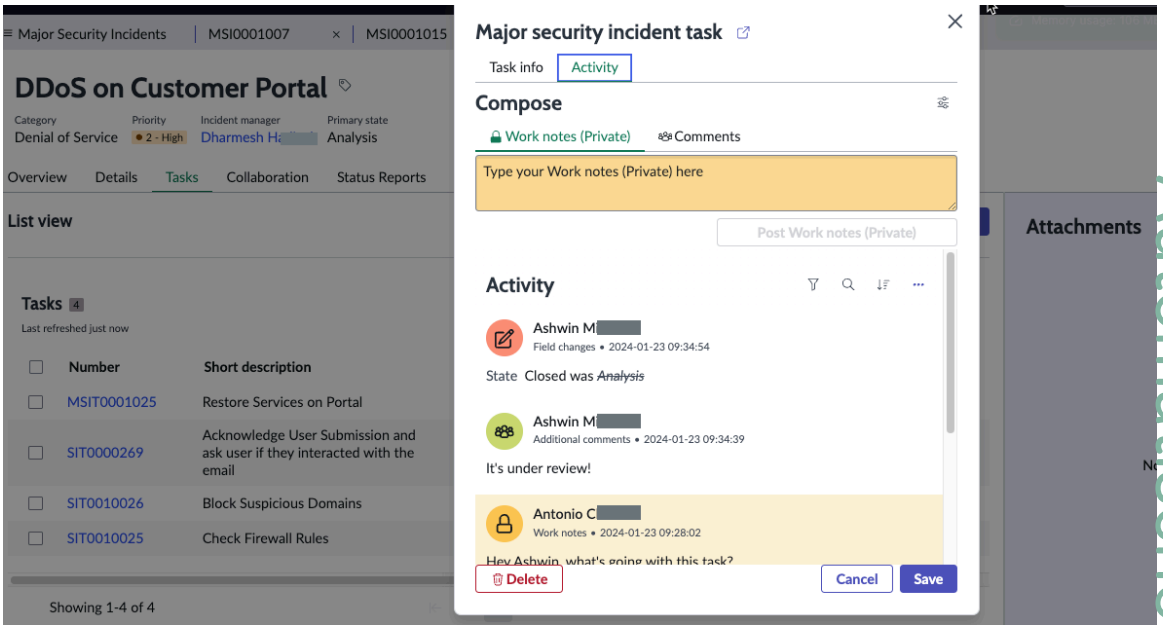
Feld	Beschreibung
Nummer	Eine eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie mithilfe der Option **Kalender** ein Datum aus, und geben Sie im Abschnitt Zeit auswählen die **Uhrzeit** an.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein: ○ **Keine** ○ **1 – Kritisch** ○ **2 – Hoch** ○ **3 – Mittel** ○ **4 – Niedrig** ○ **5: Planung**
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse** ○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen.
Zugewiesen an	Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll.
Betroffene Assets	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Assets aus.
Betroffene Anwender	Wählen Sie mithilfe der Suchoption die von der Aufgabe betroffenen Anwender aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie den Abschnitt **„Aktivität“** aus, um die Aktivitätsdetails aus den MSI-Respondern anzuzeigen.

   Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und bei Bedarf zusätzliche Kommentare hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügten Aktivitäten oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

Abschnitt „Aktivität“ in der Listenansicht



Hinweis:
Wählen Sie den Link **Weitere Details anzeigen** aus, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, der diesem schwerwiegenden Security Incident zugeordnet ist.

8. Wählen Sie **Speichern**, um die Aufgabeninformationen zu aktualisieren.

   Die Aufgabeninformationen werden sofort aktualisiert.

9. Sie können in der Listenansicht auch die folgenden Aktionen ausführen:
   a. Wählen Sie das **Aktualisieren** -Symbol, um die Liste der Aufgaben in der Listenansicht zu aktualisieren.
   b. Wählen Sie das Symbol **Einstellungen**, und verwenden Sie die Option **Spalten bearbeiten,** um die Liste der Spalten zu ändern, die in der Listenansicht angezeigt werden. Verwenden Sie die Option **Breiten zurücksetzen**, um die Breite der Spalten zurückzusetzen.

Löschen Sie eine Aufgabe mithilfe der Listenansicht

Erforderliche Rolle: sn_msi.workspace_manager.

Der MSI-Manager kann eine Aufgabe in der Listenansicht wie folgt löschen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie den gewünschten Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Aufgaben**.
5. Wählen Sie **Listenansicht**aus.
6. Wählen Sie in der Liste die Aufgabe aus, die Sie löschen möchten.
7. Wählen Sie im Popup-Fenster „Aufgabe für schwerwiegenden Security Incident“ die Option **Löschen** aus.

   Das Popup-Fenster „Aufgabe löschen“ wird angezeigt, in dem Sie aufgefordert werden, das Löschen der Aufgabe zu bestätigen.
8. Wählen Sie **Löschen**.

Verfolgen Sie die Zusammenarbeitsaktivität über den Arbeitsbereich MSIM .

Verfolgen Sie Chat- und Dateiaktivitäten im Zusammenhang mit der Lösung schwerwiegender Security Incidents über den MSIM-Arbeitsbereich.

Aktivitäten werden mithilfe des Chats Microsoft Teams und der Dateien und Ordner Microsoft SharePoint von koordiniert und dann über -Integrationen an den Major Security Incident zurückgesendet.

Sobald Microsoft Teams und Microsoft SharePoint in Management schwerwiegender Sicherheits-Incidentsintegriert sind, können Sie den Arbeitsbereich MSIM verwenden, um die Zusammenarbeit zwischen Incident-Responder-Benutzern und anderen Gruppen nachzuverfolgen, die zur Lösung schwerwiegender Security Incidents beitragen. Alle Aktualisierungen von Zusammenarbeitsordnern und -dateien in Microsoft SharePoint werden mit dem MSIM -Arbeitsbereich File Explorer synchronisiert und werden auch in den Komponenten des Aktivitätenstroms berücksichtigt.

Wenn ein Security Incident als schwerwiegender Incident heraufgestuft wird:

1. Eine Ordnerstruktur wird in Microsoft SharePoint basierend auf der Konfiguration der Ordnervorlage erstellt. Dieselbe Ordnerstruktur wird in der Komponente File Explorer des Arbeitsbereichs angezeigt.
2. Ein Team mit mehreren Kanälen wird unter der Anwendung Microsoft Teams erstellt, und dasselbe wird in der Komponente „Chat-Management“ des Arbeitsbereichs angezeigt.

Erforderliche Rolle: sn_msi.workspace_manager.

Interagieren Sie mit Dateien und Ordnern

Der Datei-Explorer zeigt das Dateisystem an, sodass Sie Dateien und Ordner im Zusammenhang mit der Lösung des incident anzeigen und mit ihnen interagieren können.

Zeigt die Datei und die Ordner an, die in Microsoft SharePoint für einen bestimmten Security Incident erfasst wurden. Diese Ordner werden in Microsoft SharePoint für diesen schwerwiegenden Security Incident automatisch erstellt. Sie können diese standardmäßig erstellten Ordner verwenden, um bei Bedarf unterstützende Dateien hochzuladen. Sie können diese Dateien und Ordner nach Bedarf umbenennen, verschieben oder löschen.

Außerdem wird jedes Mal, wenn Sie eine Datei in einen der Ordner hochladen, die Aktivität, die diesen Ordnern entspricht, automatisch den Datei-Explorer-Ordnern auf der Registerkarte „Zusammenarbeit“ zugeordnet, und die Aktivität wird aufgezeichnet und im Abschnitt „Aktivität“ von „Major Security Incident Management“ angezeigt Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Auf der Registerkarte **Zusammenarbeit** wird der Incident-Datensatz mit einer eindeutigen Incident-Nummer und Incident-Kategorie an die übergeordnete Datei in SharePoint angehängt.

1. **Repository-Ansicht**: Listet die Dateien und Ordner auf, die in Microsoft SharePoint für diesen bestimmten Security Incident aufgeführt sind. Für jede Datei oder jeden Ordner werden in der Repository-Ansicht Name, Geändert von, Zuletzt geändert und Größe angezeigt.

Repository-Ansicht

Feld	Beschreibung
In SharePoint öffnen	Wählen Sie diese Option neben Ihrem schwerwiegenden Security Incident aus. Klicken Sie auf den Link, um die Ordnerstruktur in Microsoft SharePoint auszuwählen und anzuzeigen.
Neuer Ordner	Wählen Sie diese Option aus, um nach Bedarf einen neuen Ordner zu erstellen. Nachdem Sie einen neuen Ordner erstellt haben, wird standardmäßig derselbe neue Ordner erstellt und in Ihrem Microsoft SharePoint zugeordnet.

2. **Letzte**: Zeigt alle aktuellen Aktivitätsprotokolle an. Diese Protokolle enthalten sowohl Ihre SharePoint- als auch Ihre Datei-Explorer-Aktivitäten. Die letzten Aktivitäten sind normalerweise Ihre unterstützenden Dateien, einschließlich des übergeordneten Ordners.

   Im Folgenden finden Sie das Verfahren zum **Auffinden einer Protokolldatei:**

   a. Wählen Sie die entsprechende Datei aus, um die Details anzuzeigen.

   b. Klicken Sie auf **Datei suchen**.

   Hinweis:
   Die Navigation und die Details der übergeordneten Datei und der übergeordneten Ordner werden im Abschnitt **Zuletzt** verwendete Listenansicht angezeigt. Sie können dieselbe Datei in SharePoint öffnen. Wenn Sie die zugehörigen Protokolldateien oder Aktivitäten hochladen, werden alle diese Dateien und Aktivitäten sowohl in SharePoint als auch im Datei-Explorer angezeigt.

Verwalten Sie die Kommunikation über Chat-Kanäle mit Microsoft Teams

Der Chatkanalmanager zeigt Microsoft Teams mit mehreren Kanälen an, die in der Microsoft Teams-Anwendung basierend auf einer Konfigurationsvorlage erstellt wurden.

Diese konfigurierten Kanäle werden zusammen mit den ihnen zugewiesenen Anwendern und Anwendergruppen in der Komponente „Chat-Management“ angezeigt. Mit dem Chatkanalmanager können Sie:

- **Chat-Kanäle verwalten**
- **Team umbenennen**
- **Teammitglieder verwalten**

Das Team und die Kanäle werden basierend auf der Konfiguration des Chat-Kanals in Microsoft Teams erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Chatkanäle verwalten

Mit dem Chatkanal-Manager können Sie Chatkanäle erstellen, bearbeiten oder löschen. Um einen Chatkanal in Microsoft Teams zu verwalten, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Registerkarte **Zusammenarbeit**.
2. Navigieren zu **Chatkanalmanager** > **Neuen Kanal erstellen**.
3. Fügen Sie einen neuen **Kanalnamen**und **eine Beschreibung**hinzu, und wählen Sie die **Mitglieder** für den Kanal aus.
4. Wählen Sie **Erstellen** aus.

Hinweis:
Im Abschnitt „Microsoft Teams-Kanäle“ der Microsoft Teams-Anwendung wird ein neuer Kanaldatensatz erstellt, und derselbe Datensatz wird in MSIM wiedergegeben.

5. Um einen Chatkanal zu bearbeiten, wählen Sie einen Chatkanal in der Liste Chatkanal-Manager aus.
6. Sie können den Kanalnamen, die Mitgliederliste und die Gruppenmitgliederliste basierend auf Ihren Anforderungen ändern.
7. Wählen Sie **Speichern**.
8. Um einen Chatkanal zu löschen, wählen Sie einen Chatkanal in der Liste „Chatkanal-Manager“ aus.
9. Wählen Sie **Kanal löschen aus**.

Team umbenennen

Um ein Team in Microsoft Teams umzubenennen, gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Zusammenarbeit**.
2. Navigieren zu **Chatkanalmanager** > **Team umbenennen**.
3. Benennen Sie im Feld Teamname das Team entsprechend Ihren Anforderungen um.
4. Wählen Sie **Speichern**.

Hinweis:
Durch das Umbenennen des Teamnamens wird auch der Teamname in Microsoft Teams umbenannt.

Teammitglieder verwalten

Mit dem Chatkanalmanager können Sie Teammitglieder in Microsoft Teams hinzufügen oder entfernen. Sie können Mitglieder auch über Gruppen hinzufügen. Um Teammitglieder in Microsoft Teams zu verwalten, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Registerkarte **Zusammenarbeit**.
2. Navigieren zu **Chatkanalmanager** > **Teammitglieder verwalten**.
3. Fügen Sie im Feld Mitglieder je nach Anforderungen Teammitglieder hinzu, oder entfernen Sie sie.
4. Wählen Sie im Feld Mitglieder über Gruppen hinzufügen die Gruppen aus, die Sie in Microsoft Teams hinzufügen möchten.

Hinweis:
Wenn die Gruppenmitglieder bereits im Team sind, werden sie nicht hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Speichern**.

   Der Chatkanalmanager zeigt die Details zur Gesamtzahl der Teammitglieder und die Anzahl der neuen Mitglieder an, die hinzugefügt werden.

Verwalten Sie die Kommunikation von Chat-Kanälen mit Slack

Der Chatkanalmanager zeigt Slack mit mehreren Kanälen an, die in der Anwendung Slack basierend auf einer Konfigurationsvorlage erstellt wurden.

Diese konfigurierten Kanäle werden zusammen mit den ihnen zugewiesenen Anwendern und Anwendergruppen in der Komponente „Chat-Management“ angezeigt. Mit dem Chatkanalmanager können Sie **Chatkanäle verwalten**. Das Team und die Kanäle werden basierend auf der Konfiguration des Chat-Kanals in Slack erstellt.

Chatkanäle verwalten

Mit dem Chatkanal-Manager können Sie Chatkanäle in Slack erstellen, bearbeiten oder löschen. Um einen Chatkanal zu verwalten, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Registerkarte **Zusammenarbeit**.
2. Navigieren zu **Chatkanalmanager** > **Neuen Kanal erstellen**.
3. Fügen Sie einen neuen **Kanalnamen**und **eine Beschreibung**hinzu, und wählen Sie die **Mitglieder** für den Kanal aus.
4. Wählen Sie **Erstellen** aus.

   Hinweis:
   Im Abschnitt „Slack-Kanäle“ der Slack-Anwendung wird ein neuer Kanaldatensatz erstellt, und derselbe Datensatz wird in MSIM wiedergegeben.

5. Um einen Chatkanal zu bearbeiten, wählen Sie einen Chatkanal in der Liste Chatkanal-Manager aus.
6. Sie können den Kanalnamen, die Mitgliederliste und die Gruppenmitgliederliste basierend auf Ihren Anforderungen ändern.
7. Wählen Sie **Speichern**.
8. Um einen Chatkanal zu löschen, wählen Sie einen Chatkanal in der Liste „Chatkanal-Manager“ aus.
9. Wählen Sie **Kanal löschen aus**.

Verwalten Sie Aktivitätenstrom-Konversationen

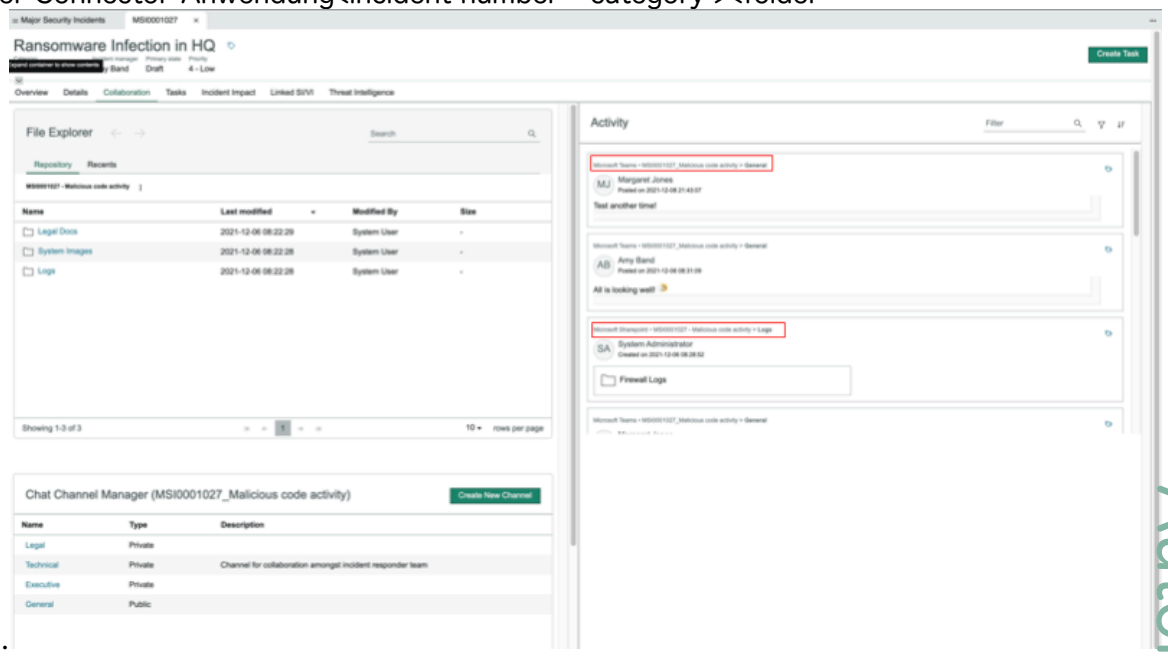
Zeigt alle Aktivitäten, Protokolle und Status an, die für Microsoft SharePoint, den Datei-Explorer und Microsoft Teamsausgeführt wurden.

Wenn Sie eine bestimmte Aktivität anzeigen oder die Details der Zusammenarbeitsaktivität suchen möchten, mit der zwischen verschiedenen Dateien und Ordnern sowie in Microsoft Teams interagiert wurde, können Sie die Filterfunktion verwenden, die oben rechts im Abschnitt „Aktivitätenstrom“ angezeigt wird, und das gewünschte suchen Aktivitätsdetails.

Für „Major Security Incident Management“ freigegebene Ordner und Chatunterhaltungen werden als Breadcrumbs mit der folgenden Struktur angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

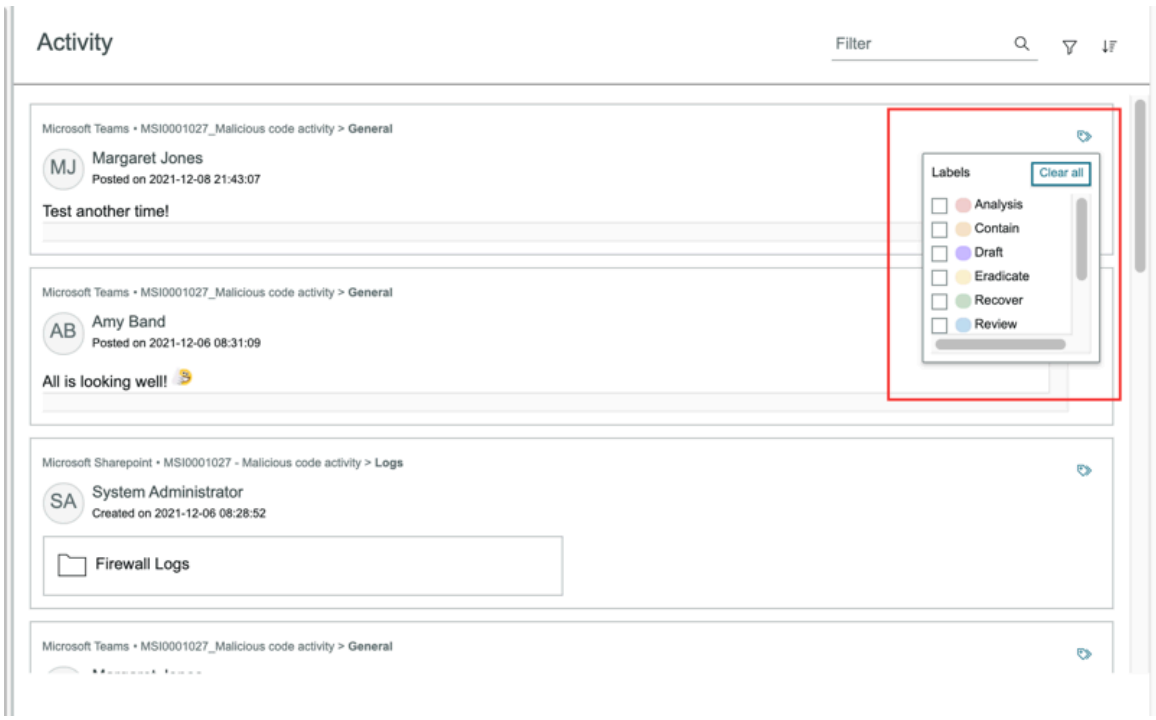
Name der Connector-Anwendung<incident number – category ><folder



name>).

Beschriften Sie die Aktivitäten mit:

1. Klicken Sie auf das **Symbol** Bezeichnung.
2. Aktivieren Sie das entsprechende Kontrollkästchen für die Incident-Aktivitätsbezeichnung (siehe Screenshot unten).



3. Die gekennzeichneten Aktivitäten sind farbcodiert und werden als Fortschrittstrenddiagramm im Abschnitt **„Externe Zusammenarbeit“** des Arbeitsbereichs dargestellt.

Erstellen und verteilen Sie MSIM Statusberichte

Als Major Security Incident -Manager können Sie basierend auf der konfigurierten Berichtsvorlage oder einem vorherigen Statusbericht im Verlauf der Lösung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

schwerwiegender Security Incidents verschiedene Statusberichte zu unterschiedlichen Intervallen erstellen und an verschiedene Stakeholder verteilen.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Sie können eine Vorschau der zuvor konfigurierten Datenelemente des Zusammenfassungsberichts anzeigen, zusätzlichen Text oder eine Zusammenfassung hinzufügen, einzelne Berichtskomponenten nach Bedarf entfernen und die Richtigkeit und Vollständigkeit des Berichts überprüfen, bevor Sie ihn an andere Stakeholder verteilen.

Erstellen Sie die Statusberichte, indem Sie die gewünschte Berichtsvorlage auswählen, die ursprünglich auf der Setup-Seite für MSI-Berichtsvorlagen konfiguriert wurde.

Prozedur

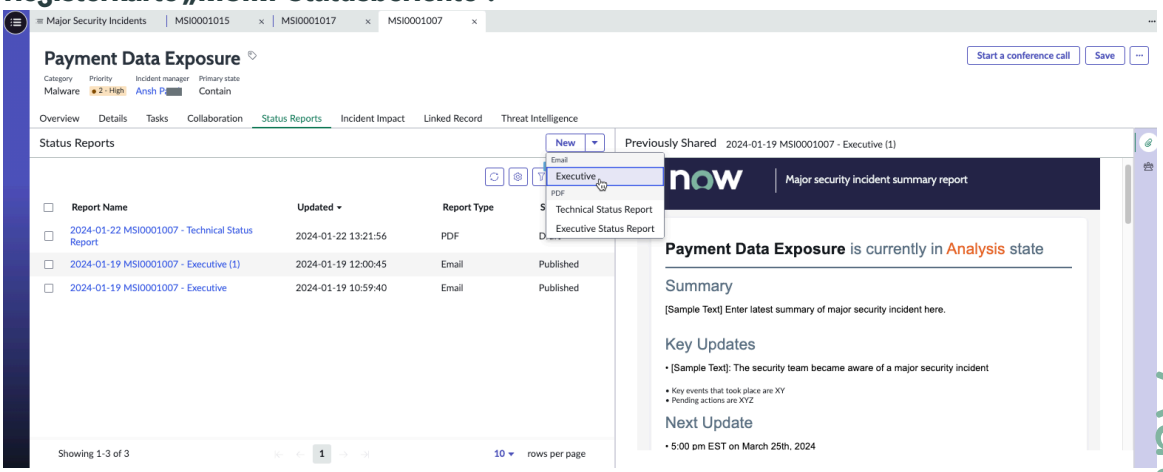
1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die Ansicht **Listen** aus.
3. Wählen Sie den entsprechenden heraufgestuften MSI-Datensatz aus.
4. Wählen Sie die Registerkarte **Statusberichte**.
   Die Registerkarte „Statusberichte“ enthält drei verschiedene Arten von Unterabschnitten wie unten dargestellt.

Feld	Beschreibung
Berichtname	Name der Statusberichtvorlage. **Hinweis:** In der Ansicht „Statusberichte“ werden die vorhandenen vordefinierten Berichtsvorlagen aufgelistet, die als Teil des Basissystems für die betroffene Persona verfügbar sind. Zum Beispiel Managerstatusberichte per E-Mail (für Mobilgeräte optimiert), technische Statusberichte und Managerstatusberichte als PDFs.
Aktualisiert	Das Datum, an dem die Berichtsvorlage zuletzt aktualisiert wurde.
Berichtstyp	Art des Statusberichts. Der Statusbericht kann einen der folgenden Typen aufweisen: ○ PDF ○ E-Mail
Status	Status der Statusberichte. Die Statusberichte können einen der folgenden Status aufweisen: ○ Entwurf ○ In Warteschlange ○ Veröffentlicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie den Typ des Statusberichts aus, den Sie anzeigen möchten, oder wählen Sie **Neu,** um einen Statusbericht zu erstellen.

Registerkarte „MSIM-Statusberichte“.



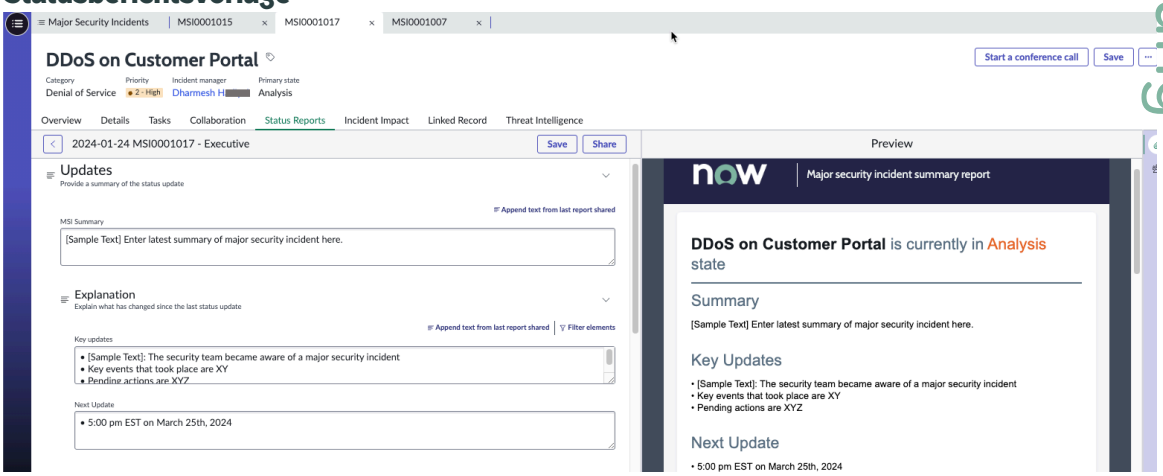
6. Wählen Sie einen der folgenden Statusberichtstypen aus der Liste aus.
   - E-Mail-Statusberichte**für Führungskräfte**, die für Mobilgeräte optimiert sind.
   - **Technischer Statusbericht** (PDF)
   - **Statusbericht für Führungskräfte** (PDF)

Hinweis:
Wenn Sie eine beliebige Berichtsvorlage auswählen, wird im rechten Bereich sofort eine Vorschau des ausgewählten Berichts generiert. Sie können den ausgewählten Statusbericht des MSI anzeigen.

7. Füllen Sie in der Vorlage „E-Mail-Statusbericht für Führungskräfte“ die Abschnitte mit den Details des Statusberichts aus.

Hinweis:
Die Optionen, die Sie im Abschnitt „Statusberichte“ ausgewählt haben, sind die gleichen Optionen, die im Vorschaubericht gerendert werden.

Statusberichtsvorlage



8. Wählen Sie **Speichern** aus, um die Aktualisierungen zu speichern, die Sie am Statusbericht vorgenommen haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie **Freigeben** aus, um den Statusbericht für interne und externe Stakeholder freizugeben.
   Das Dialogfeld „Freigeben“ wird angezeigt.

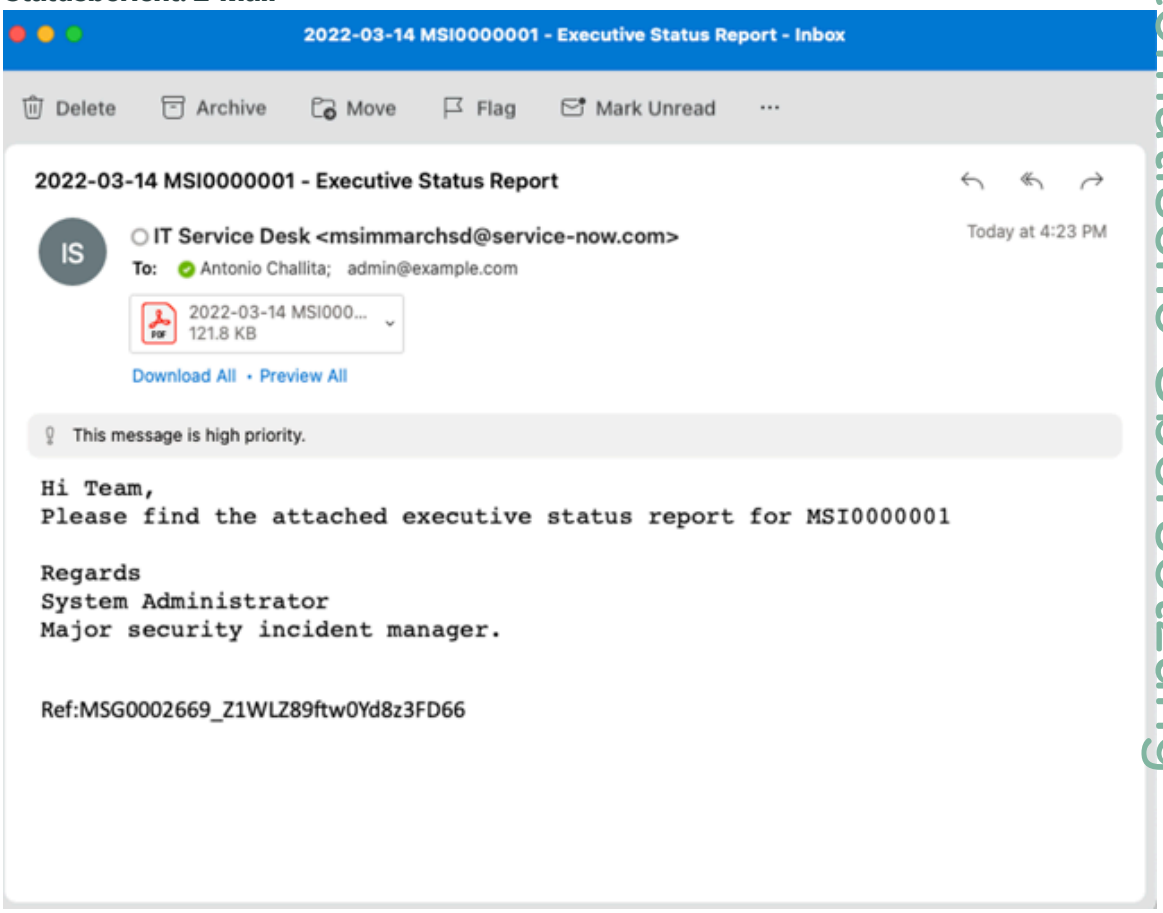
   a. Geben Sie im Feld Betreff den Betreff für den E-Mail-Bericht ein.

   b. Geben Sie im Feld Interne Empfänger hinzufügen die Empfänger für den E-Mail-Bericht ein, und wählen Sie sie aus.

   c. Geben Sie im Feld Externe Empfänger hinzufügen die E-Mail-Adresse der Empfänger oder DL für den E-Mail-Bericht ein.
   Sie können mehrere E-Mail-IDs mit einem Komma oder Semikolon hinzufügen.

10. Wählen Sie **E-Mail-Bericht**aus.
    Eine E-Mail mit dem angehängten PDF-Statusbericht wurde zur Überprüfung erfolgreich an den betroffenen Empfänger gesendet.

Statusbericht: E-Mail



11. Auf der Registerkarte Statusberichte können Sie auch die folgenden Aktionen ausführen:

    a. Verwenden Sie die Aktion **Aktualisieren** in der Ansicht Statusberichte, um die Liste der Statusberichte zu aktualisieren.

    b. Verwenden Sie die Aktion **Listenaktionen** in der Ansicht Statusberichte, um Spalten zu bearbeiten oder die Breite der Liste der Statusberichte zurückzusetzen.

    c. Verwenden Sie die Aktion **Filter** in der Ansicht Statusberichte, um die Statusberichte anhand bestimmter Bedingungen zu filtern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurieren Sie Major Security Incident Statusberichte

MSIM -Statusberichte werden verwaltet

Statusberichte bieten vorkonfigurierte Trenddiagramme mit umsetzbaren Datenvisualisierungen, um Security Operations-Prozesse zu verbessern und die Lösungszeitleiste, die Anzahl der überfälligen Fälle und den Status jeder zugewiesenen Aufgabe zu messen und zu analysieren.

Konfigurieren Sie Major Security Incident Statusberichte

Konfigurieren Sie Berichte zu schwerwiegenden Security Incidents, um die Berichte während des gesamten Lebenszyklus des Korrekturprozesses für Datensätze schwerwiegender Security Incidents entsprechend Ihren Geschäftsanforderungen einzurichten und herunterzuladen.

Sie können die Berichtsvorlagen mit einem bestimmten Format und Layout erstellen und diese Berichte mit der Funktion „Statusberichte“ im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents an Ihre spezifischen Anforderungen anpassen.

Ein Anwender mit der Rolle sn_msi.workspace_manager kann die Berichtsvorlagen erstellen und konfigurieren, die die Art der Berichtsinformationen beschreiben, die zum Generieren aller Statusberichte verwendet werden können. Sie können für bestimmte Anwender wie Stakeholder in der Geschäftsführung und Rechtsabteilungen freigegeben werden Vorlagen für die Datensätze schwerwiegender Security Incidents.

Um Ihre MSI-Statusberichte anzupassen, müssen Sie zuerst die Berichtsvorlagen mithilfe von **Berichtsvorlagen**einrichten. Mithilfe von Berichtsvorlagen können Sie Berichtsvorlagentypen erstellen, die Berichtskomponenten für diese Berichtsvorlagen definieren, zusätzliche Informationen hinzufügen, visualisierte Daten erstellen, um Umfang und Fortschrittsmetriken nachzuverfolgen, zugehörige Listendaten hinzufügen und Statusberichte generieren.

Im Folgenden werden die Standardfelder beschrieben, die in allen Berichtsvorlagentypen enthalten sind. Sie können die Berichtsvorlage mithilfe von Abschnitten, Unterabschnitten und deren Elementen entsprechend Ihren Anforderungen konfigurieren und formatieren:

Statusberichtkomponenten

Komponententyp	Beschreibung
Berichtstitel	Titel des Berichtstyps. Das Standardformat des Berichtstyps lautet beispielsweise: {MSI-Nummer} – {Stakeholder-Bericht der Geschäftsleitung}, dargestellt als MSI0001001: Stakeholder-Bericht der Geschäftsleitung.
Name	Zeigt den Namen des Benutzers an, der den Bericht im Abschnitt „Statusberichte“ des Arbeitsbereichs „Major Security Incident Management“ generiert hat.
Zusammenfassung	Zeigt eine kurze Zusammenfassung des Berichts an.
Datum	Zeigt das Datum an, an dem der Bericht für den betroffenen Empfänger freigegeben wird.
Fortschritt	Zeigt die Umfangs- und Fortschrittsmetriken an, z. B. die verknüpften SIR-Incidents, Antwortaufgaben, ergänzenden Aufgaben, externe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Statusberichtkomponenten (Fortsetzung)

Komponententyp	Beschreibung
	Zusammenarbeit, Zeitleistenkomponenten und aktuelle Zeitleistenereignisse.
Herausforderungen	Dieser Abschnitt enthält eine kurze Beschreibung der Herausforderungen, die während des Nachbesserungsprozesses für schwerwiegende Security Incidents auftreten.
Nächste Schritte	In diesem Abschnitt wird eine kurze Beschreibung der nächsten Schritte angezeigt, die zur Behebung eines schwerwiegenden Security Incident erforderlich sind. Beispielsweise enthält der Unterabschnitt „Aktives Team“ im Stakeholder-Bericht für Führungskräfte mit dem nächsten Schritt die Informationen zur Teamzuweisung, die an der weiteren Analyse des Datensatzes für schwerwiegende Security Incidents beteiligt ist.
Andere Anpassungen	Die Berichtsvorlage bietet Ihnen auch die Möglichkeit, das Logo hochzuladen und die Kopf- und Fußzeilen des Berichts anzupassen.

Die folgenden Berichtskategorien können eingerichtet und angezeigt werden:

- E-Mail-Adresse**des Vorstands**
- **Technischer Statusbericht** (PDF)
- **Vorstandsstatusbericht** (PDF)

Die obigen Berichte sind konfiguriert und stehen dem Anwender zur Verfügung, um den Bericht im „Major Security Incident Management“-Arbeitsbereich auszuwählen, anzuzeigen und zu generieren.

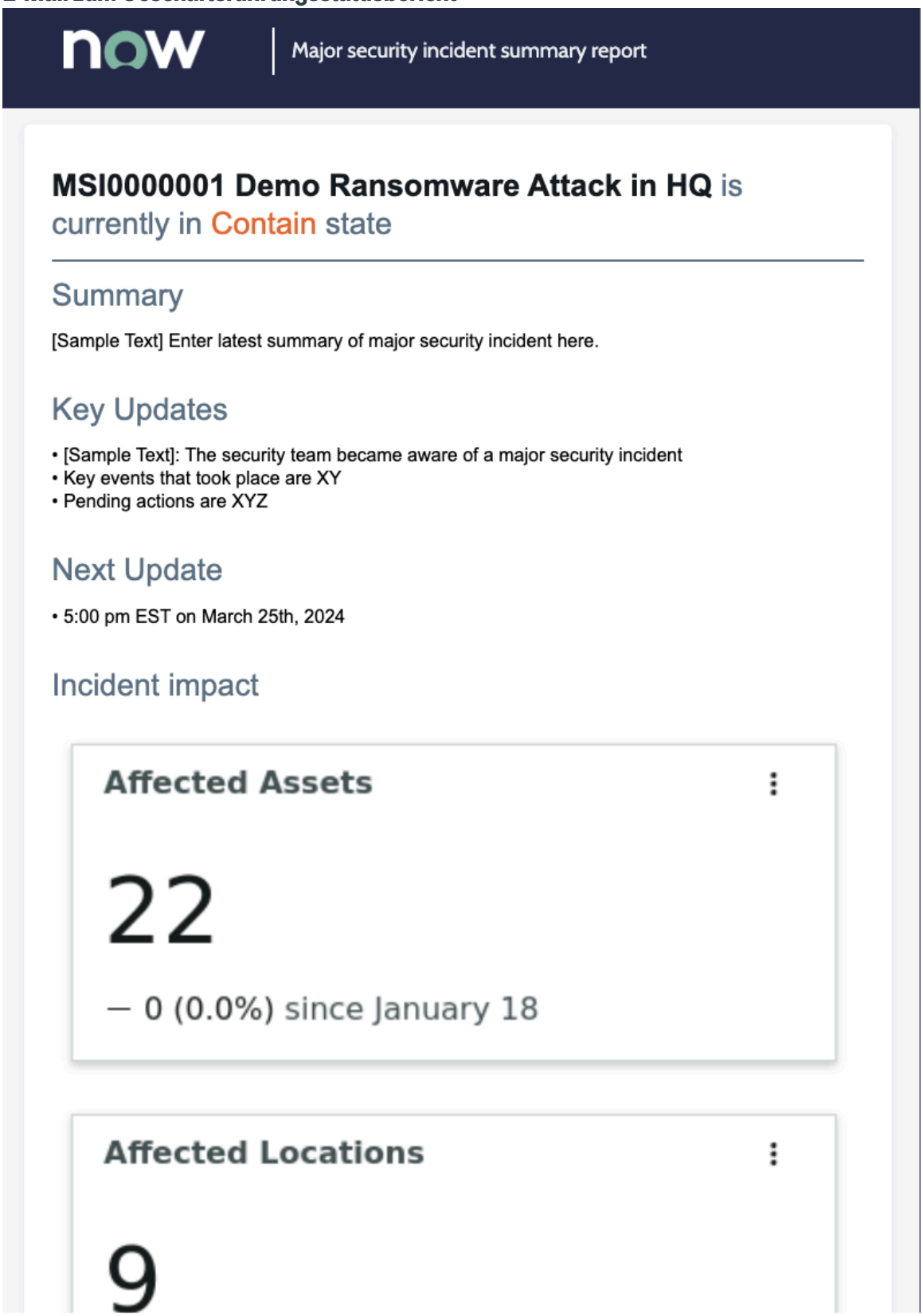
Für Mobilgeräte optimierte Statusberichte für Führungskräfte – E-Mail

Die Statusberichte für Führungskräfte – E-Mail sind für Mobilgeräte optimiert und werden im E-Mail-Format generiert. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, eine MSI-Dauerspalte, Incident-Umfang/Auswirkung, aktive Teammetriken, Fortschrittsmetriken und Zeitleistenkomponenten, z. B. die neuesten Zeitleistenereignisse für diesen bestimmten Datensatz für schwerwiegende Security Incidents.

Passen Sie die folgenden Berichtsvorlagenfunktionen an, und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Unten finden Sie ein Beispiel für einen E-Mail-Statusbericht für Führungskräfte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail zum Geschäftsführungsstatusbericht



Automatische Übersetzung

Statusberichte von Führungskräften – PDF

„Statusberichte für Führungskräfte – PDF“ sind Statusberichte, die im PDF-Format generiert werden. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, eine MSI-Dauerspalte, Incident-Umfang/Auswirkung, aktive Teammetriken, Fortschrittsmetriken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und Zeitleistenkomponenten, z. B. die neuesten Zeitleistenereignisse für diesen bestimmten Datensatz für schwerwiegende Security Incidents.

Passen Sie die folgenden Berichtsvorlagenfunktionen an, und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Unten finden Sie ein Beispiel für einen Geschäftsleitungsbericht.

Statusbericht für Führungskräfte (PDF)

MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

In progress tasks by incident state label

Figure 3. Response Tasks

Technische Statusberichte – PDF

Die technischen Statusberichte – PDF sind Statusberichte, die im PDF-Format generiert werden. Der Abschnitt „Bericht“ enthält eine Zusammenfassung des Berichts, eine Spalte für die MSI-Dauer, den Umfang/die Auswirkung des Incidents, Metriken für aktive Teams, Fortschrittsmetriken und Zeitleistenkomponenten wie die neuesten Zeitleistenereignisse für diesen bestimmten Datensatz für schwerwiegende Security Incidents, gekennzeichnete Aufgabenaktualisierungen und gekennzeichnete Aktivitäten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

basierend auf der Zuweisungsgruppe und der ausgewählten Tag-Bezeichnung seit der Generierung des letzten Statusberichts sowie zusätzlichen Informationen wie Auswirkung auf Incidents und verknüpfte Incidents.

Sie können die Berichtsvorlage anpassen und konfigurieren, um dem Bericht zusätzliche Informationen hinzuzufügen. Ein technischer Beispielbericht, der zusätzliche Informationen enthält, z. B. die Auswirkungen auf Incidents, ist unten als Referenz abgebildet. Der verbleibende Teil der Berichtsinformationen ähnelt den Berichten der Führungskräfte.

Technischer Statusbericht – PDF

MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

Die Abschnitte der Berichtsvorlagen enthalten verschiedene Unterabschnitte, in denen beschrieben wird, wie Sie die Berichtsunterabschnitte und ihre Elemente erstellen können, z. B.:

1. Branding: Fügen Sie Ihren Berichtsvorlagen Branding hinzu
2. Vorlagenskripts: Verwenden Sie Vorlagenskripts in Ihren Berichtsvorlagen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

3. Verwenden Sie Visualisierungen in Berichtsvorlagen
4. Verwenden Sie Berichtslisten in Berichtsvorlagen

Erstellt eine Berichtsvorlage

Erstellen Sie verschiedene Berichtsvorlagen, die auf schwerwiegende Security Incidents angewendet werden können, und generieren Sie einen Statusbericht. Sie können der Berichtsvorlage standardmäßige und anwenderdefinierte Formularfelder für die Reaktion auf schwerwiegende Security Incidents hinzufügen, die für Dot-Walking geeignet sind. Darüber hinaus können Sie den Bericht mithilfe von Abschnitten, Unterabschnitten und deren Elementen entsprechend Ihren Anforderungen formatieren und konfigurieren.

Vorbereitungen

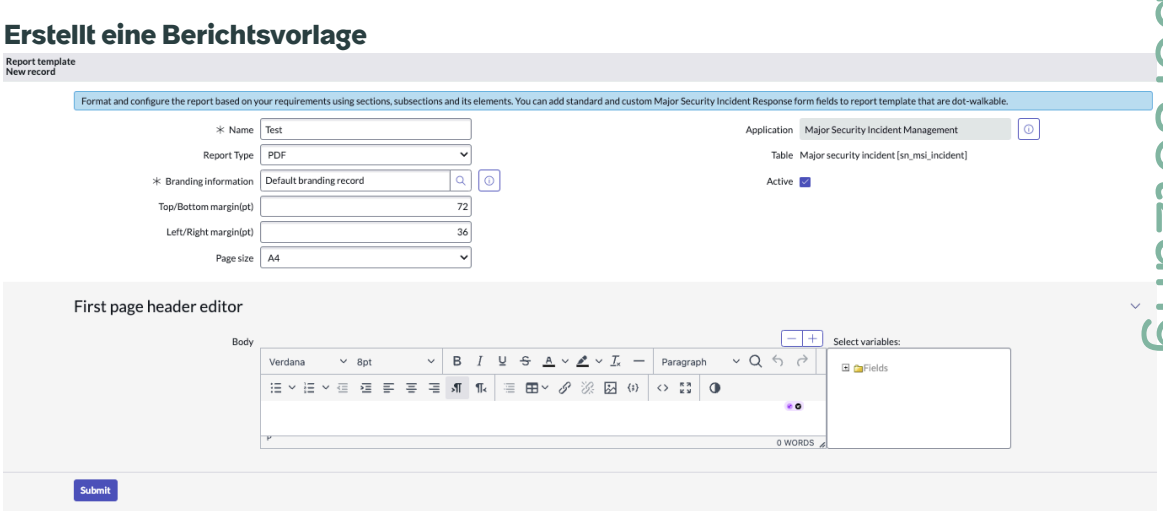
Erforderliche Rolle: sn_msi.workspace_manager

Warum und wann dieser Vorgang ausgeführt wird

Sie können Berichtskomponenten für Ihre Berichtsvorlagen definieren und zusätzliche Informationen bereitstellen. Erstellen Sie visualisierte Daten, um Umfang und Fortschrittsmetriken nachzuverfolgen, zugehörige Listendaten hinzuzufügen, Vorschauen anzuzeigen und die Statusberichte zu generieren oder freizugeben.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Wählen Sie **Neu** aus, um eine Berichtsvorlage zu erstellen.
4. Füllen Sie die Felder im Formular „Berichtsvorlage“ aus.



5. **Senden Sie** den neuen Berichtsvorlagendatensatz.
   Auf der Seite „Berichtsvorlagen“ wird eine neue Berichtsvorlage erstellt.

Zugehörige Informationen

Erstellen und verteilen Sie MSIM Statusberichte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Ihren Berichtsvorlagen Branding hinzu

Fügen Sie Ihren Berichten Branding hinzu. Sie können Kopf- und Fußzeilenbilder sowie Kopf- und Fußzeilentext hinzufügen. Sie können diese Branding-Informationen in jeden der Berichtsvorlagentypen aufnehmen, die Sie mit Ausnahme der beiden vordefinierten Berichte erstellen möchten.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

Warum und wann dieser Vorgang ausgeführt wird
Beim Hinzufügen von Branding zu Ihren Berichtsvorlagen sind folgende Punkte zu berücksichtigen:

- Laden Sie das Kopf- und Fußzeilenbild hoch, und richten Sie die Bildposition aus.
- Die maximale Größe für Kopf- und Fußzeilenbilder beträgt 5 MB. Wenn die Größe den angegebenen Grenzwert überschreitet, wird im schwerwiegenden Security Incident die Fehlermeldung „Bildformat kann nicht erkannt werden“ angezeigt.
- Passen Sie die Höhe des Kopf- und Fußzeilenbilds an.
- Die Länge des Fußzeilentexts ist auf 100 Zeichen beschränkt.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
2. Drilldown zu **Berichtsvorlage** > **Branding**.
3. Wählen Sie **Konfigurieren**.
4. Wählen Sie **Neu** aus, um Ihrer Berichtsvorlage ein Branding hinzuzufügen.
5. Füllen Sie die Felder im Formular „Branding-Vorlage“ aus.
6. Wählen Sie **Absenden**.
   Auf der Seite „Branding-Vorlagen“ wird eine neue Branding-Vorlage erstellt.

Verwenden Sie Visualisierungen in Berichtsvorlagen

Verwenden Sie Bericht-Widgets, um User Interface Builder-Elemente (UIB) wie Datenvisualisierungen zu definieren und in die MSIM-Statusberichte aufzunehmen.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Drilldown zu **Berichtsvorlage** > **Visualisierungen**.
3. Wählen Sie **Konfigurieren**.
   Im Folgenden finden Sie die vordefinierten UIB-Visualisierungen als Teil des Basissystems, die Sie zum Konfigurieren und Ändern Ihrer Statusberichte verwenden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellt ein Visualisierungstypelement

Verwenden Sie Berichtslisten in Berichtsvorlagen

Verwenden Sie Berichtslisten, um die zugehörigen Listenartefakte zu definieren und einzubeziehen, um auf Grundlage Ihrer konfigurierten MSI-Listendatensätze Listen im PDF zu generieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Drilldown zu **Berichtsvorlage** > **Listen**.
3. Wählen Sie **Konfigurieren**.
   Im Abschnitt „MSI-Statusberichtslisten“ wird beschrieben, wie sich die Erstellung des incident auf die einzelnen spezifischen zugehörigen Listen auswirkt. Im Folgenden finden Sie die vordefinierten MSI-Berichtslisten als Teil des Basissystems, die Sie zum Konfigurieren und Ändern Ihrer Statusberichte verwenden können.

Zugehörige Informationen

Erstellen Sie ein Listentypelement

Verwenden Sie Vorlagenskripts in Ihren Berichtsvorlagen

Erstellen Sie ein Skript, um die zugehörigen Listendaten, Datumsvorgänge und alle anderen Daten einzubeziehen, die nicht direkt Dot-Walk-fähig sind.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Warum und wann dieser Vorgang ausgeführt wird

Sie können dieses vordefinierte Vorlagenskript in Ihren Berichtsvorlagen verwenden, um zugehörige Daten aufzunehmen, nachdem die Berichtsvorlagen konfiguriert und angepasst wurden.

Erstellen Sie ein Vorlagenskript, um die zugehörigen Listendaten in der Berichtsvorlage anzuzeigen. Wenn Sie ein Vorlagenskript verwenden und ausfüllen möchten, müssen Sie das Tag-Vorlagenskript-Tag wie folgt hinzufügen: `${template_script:script name}`.

Beispiel: `${template_script:msi_collab_cards}`

Hinweis:
Sie können die vordefinierten Vorlagenskripts nicht löschen. Eine Fehlermeldung wird angezeigt, wenn ein Benutzer mit Administratorrolle versucht, einen Vorlagenskript-Datensatz zu löschen, der einer Berichtsvorlage zugeordnet ist.

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Drilldown zu **Berichtsvorlage** > **Vorlagenskripts**.
3. Wählen Sie **Konfigurieren**.
   Im Folgenden finden Sie die vordefinierten Vorlagenskripts als Teil des Basissystems, die Sie zum Konfigurieren und Ändern Ihrer Statusberichte verwenden können.

> **Hinweis:**
> Sie können auch ein eigenes Vorlagenskript erstellen, um zusätzlich zu den aufgeführten Vorlagenskripts die zugehörigen Listendaten, Datumsvorgänge und alle anderen Daten einzubeziehen, die nicht direkt Dot-Walk-fähig sind.

Zeigen Sie eine Vorschau der Berichtsvorlage an

Verwenden Sie die Vorschaufunktion, um eine Vorschau Ihrer Berichtsvorlage zur Entwurfszeit anzuzeigen, um den Bericht zur Laufzeit über den Arbeitsbereich Management schwerwiegender Sicherheits-Incidents zu generieren und für andere Stakeholder freizugeben.

Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Wählen Sie die gewünschte Berichtsvorlage aus.
4. Wählen Sie als Berichtstyp je nach Anforderung **E-Mail** oder **PDF** aus.
5. Wählen Sie die Aktion **Bericht speichern und in der Vorschau anzeigen aus**.

   Das Dialogfeld Vorschaubericht wird angezeigt.
6. Wählen Sie mithilfe der Suchoption einen schwerwiegenden Security Incident aus, um eine Vorschau eines Berichts mit der ausgewählten Vorlage anzuzeigen.
7. Wählen Sie **Vorschaubericht**aus.
   Der Bericht generiert eine Vorschau entsprechend der ausgewählten Vorlagenkonfiguration. Wenn Sie als Berichtstyp **E-Mail**ausgewählt haben, erfolgt die Vorschau im E-Mail-Vorlagenformat. Die Statusberichte im E-Mail-Format sind für Mobilgeräte optimiert.

Erstellen Sie eine Berichtsabschnittsvorlage

Ein Bericht kann außerdem in verschiedene Abschnitte unterteilt werden. Verwenden Sie den Abschnitt „Bericht“, um den Bericht in mehrere Abschnitte aufzuteilen und sie der Reihe nach neu zu organisieren.

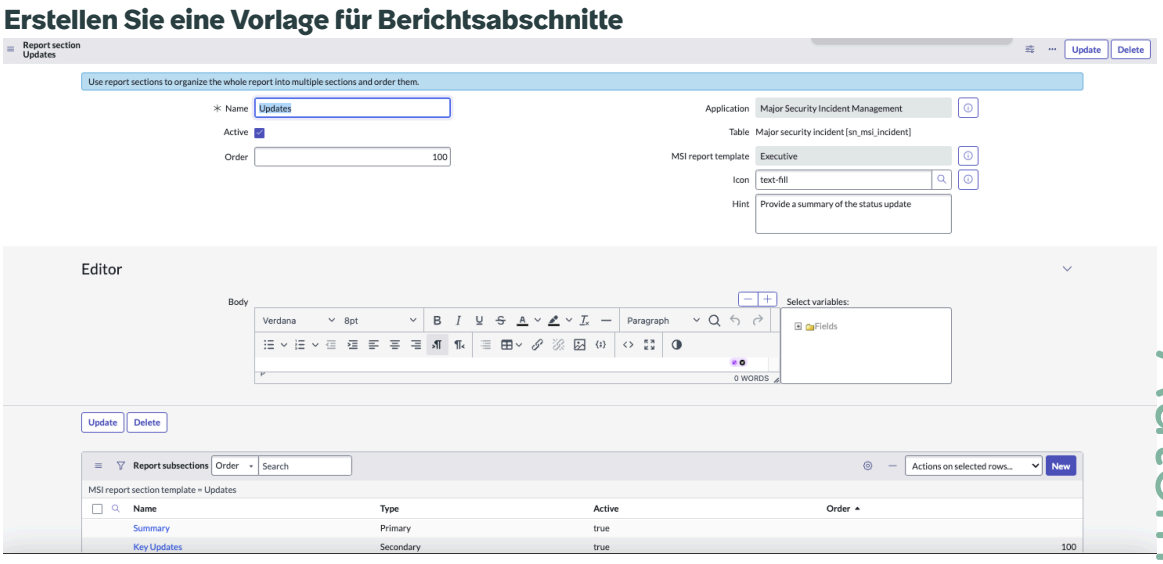
Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie eine vorhandene Berichtsvorlage.
4. Navigieren zu **Berichtsabschnitte** > **Neu**.
   Die neue Berichtsabschnittsseite wird angezeigt.



5. Füllen Sie die Felder im Formular „Berichtsabschnittsvorlage“ aus.
6. Speichern und **übermitteln Sie** den neuen Berichtsvorlagenabschnitt.

Erstellt eine Berichtsunterabschnittsvorlage

Verwenden Sie den Berichtunterabschnitt, um den Abschnitt weiter in mehrere Unterabschnitte zu organisieren und deren Ausrichtung und Position mithilfe der verfügbaren Typen wie Textseitenbereich, Primär und Sekundär zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

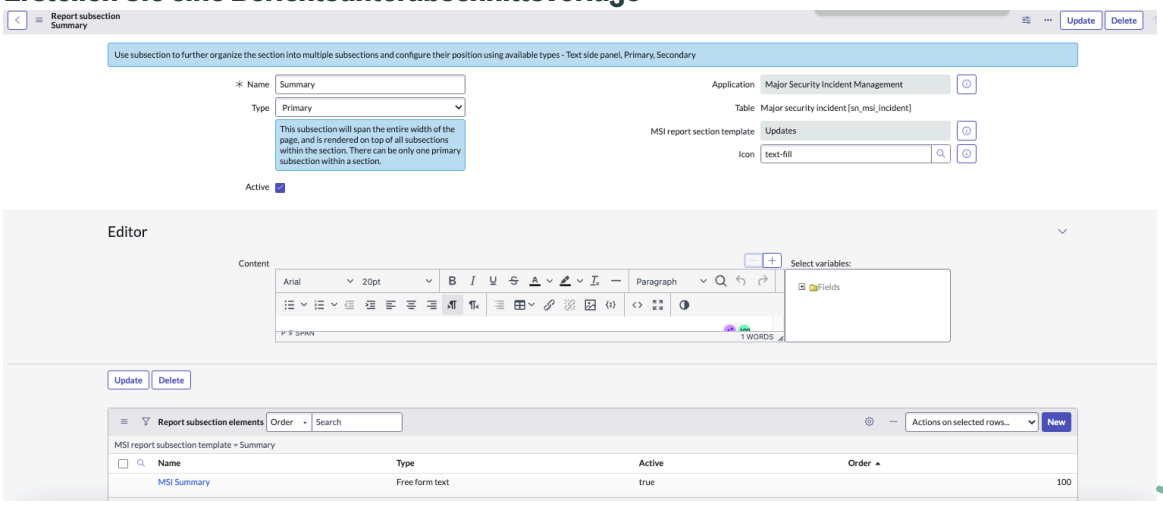
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste der Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Navigieren zu **Berichtsunterabschnitte** > **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Berichtsunterabschnittsvorlage



6. Füllen Sie die Felder im Formular „Berichtsunterabschnitt“ aus.

7. Speichern und **übermitteln Sie** den neuen Berichtsvorlagenabschnitt.

Elementvorlage für Berichtsunterabschnitt erstellen

Verwenden Sie Unterabschnittselemente, um einen Unterabschnitt weiter in mehrere Elemente zu organisieren. Unterabschnittselemente helfen dabei, Visualisierungen, Listen und Freiformtext mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

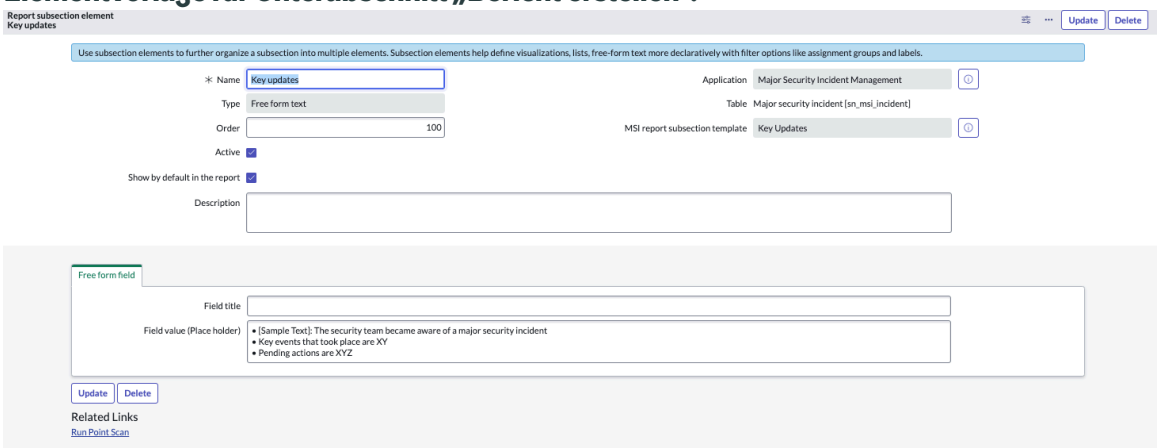
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste der Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elementvorlage für Unterabschnitt „Bericht erstellen“.



7. Füllen Sie die Felder im Formular „Berichtsunterabschnittselemente“ aus.

8. Speichern und **aktualisieren Sie** den neuen Berichtsvorlagenabschnitt.

Erstellen Sie ein Freiform-Typelement

Erstellen Sie einen Freiformelementtyp, um Freiformtext mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste der Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Elementvorlage für Berichtsunterabschnitt erstellenerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Freiformfeld** aus.
   Dadurch wird der Abschnitt **Freiformfeld** angezeigt.
9. Füllen Sie die Felder auf der Registerkarte Freiform aus.

Erstellt ein Visualisierungstypelement

Erstellen Sie einen Visualisierungselementtyp, um die Visualisierungselemente mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

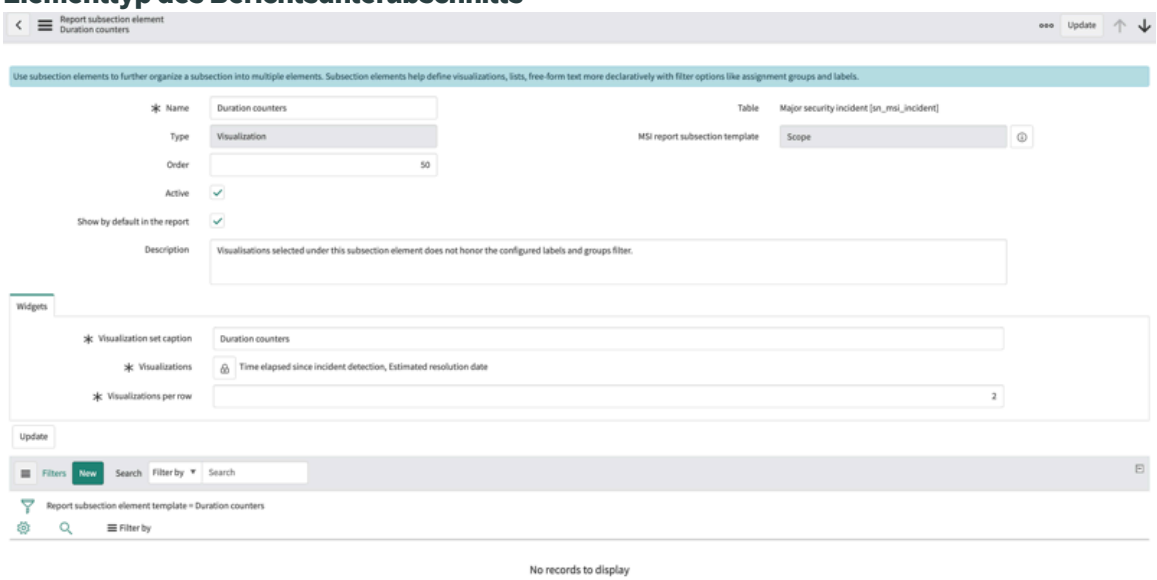
Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Setup-Seite für den MSI-Statusbericht wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste der Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Elementvorlage für Berichtsunterabschnitt erstellenerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Visualisierung** aus.
   Dadurch wird der Abschnitt **„Visualisierung“** angezeigt.
9. Füllen Sie die Felder im Formular „Visualisierung“ aus.
10. Wählen Sie **Absenden**.

Example: Elementtyp des Unterabschnitts der Berichtsvorlage für einen technischen Statusbericht

Elementtyp des Berichtsunterabschnitts



Erstellen Sie ein Listentypelement

Erstellen Sie ein Listentypelement, das die zugehörigen Listenelemente mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer definiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste der Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Elementvorlage für Berichtsunterabschnitt erstellenerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Liste** aus.
   Dadurch wird der Abschnitt **Listen** angezeigt.
9. Füllen Sie die Felder des Listenformulars aus.

Erstellen Sie ein anwenderdefiniertes Typelement

Erstellen Sie ein Listentypelement, das die zugehörigen Listenelemente mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer definiert.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

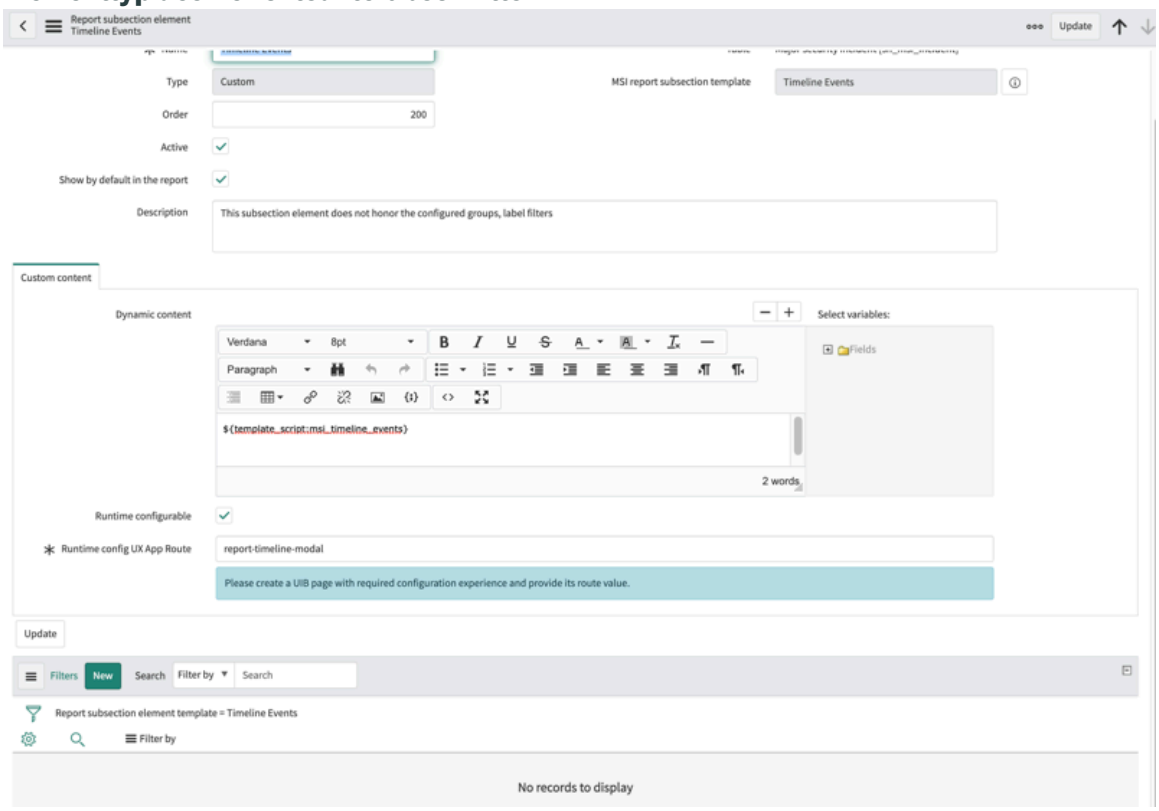
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite „MSI-Statusbericht-Setup“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage **die Option Konfigurieren aus**.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste der Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Elementvorlage für Berichtsunterabschnitt erstellenerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Anwenderdefiniert** aus.
   Dadurch wird der Abschnitt **„Anwenderdefinierter Inhalt“** angezeigt.
9. Füllen Sie die Felder im Formular „Anwenderdefinierter Inhalt“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Im Folgenden finden Sie ein Beispiel für den Unterabschnittselementtyp der Berichtsvorlage für einen technischen Statusbericht

Elementtyp des Berichtsunterabschnitts



Fügen Sie Systemeigenschaften hinzu

Fügen Sie Systemeigenschaften hinzu, um das MSIM-Anwendungsverhalten zu steuern. Im Folgenden sind die Standardsystemeigenschaften aufgeführt, die als Teil der Management schwerwiegender Sicherheits-Incidents -Statusberichte eingeführt werden.

Systemeigenschaften

Eigenschaftsname	Beschreibung
sn_msi.export_img	Verwenden Sie diese Eigenschaft, um den Export von Bildern zu steuern. Der Standardwert ist auf EIN festgelegt.
sn_msi.export_img_log	Verwenden Sie diese Eigenschaft, um die Anmeldung bei der Browserkonsole zu aktivieren. Der Standardwert ist auf AUS festgelegt.
sn_msi.export_img_parallel_threshold	Verwenden Sie diese Eigenschaft, um die maximale Anzahl paralleler Anforderungen zum Generieren der Bilder aus Bericht-Widget-Konfigurationen zu steuern. Der Standardwert ist 14.
sn_msi.img_export_log	Verwenden Sie diese Eigenschaft, um die Konsolenprotokolle im Browser zu aktivieren.
sn_msi.img_export_poll_interval	Verwenden Sie diese Eigenschaft, um den Zeitabstand zwischen Abfragen zu steuern, der überprüft, ob das

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften (Fortsetzung)

Eigenschaftsname	Beschreibung
	Bild generiert wird oder nicht. Die standardmäßige Abfrageintervallzeit ist auf 3000 Millisekunden festgelegt.
sn_msi.export_poll_request_timeout	Verwenden Sie diese Eigenschaft, um die maximale Zeit zu steuern, die das System exportierte Bilder abfragen kann. Der Standardwert beträgt 120.000 Millisekunden.
sn_msi.msi_report_uib_element_js_path	Verwenden Sie diese Eigenschaft, um den generischen Pfad zu steuern, um das Bild aus dem UIB-Seitenteil zu erfassen.
sn_msi.report_default_style_objects	Verwenden Sie diese Eigenschaft, um das CSS der generierten PDFs zu ändern, z. B. Schriftgröße, Schriftfarbe oder Feldwert. Wenn sn_msi.workspace_manager beispielsweise die Schriftfarbe des linken Bereichs des generierten PDF-Statusberichts ändern möchte, kann der Arbeitsbereichsmanager die Schriftfarbe der Systemeigenschaft ändern und die PDF-Datei in einer gewünschten Ansicht rendern.

Playbooks zur Verwaltung schwerwiegender Sicherheits-Incidents

Sie können den Playbook-Flow zur Verwaltung schwerwiegender Sicherheits-Incidents automatisch oder manuell aufrufen.

Ein Playbook ist nur sichtbar, wenn einem Security Incident mindestens ein Playbook zugeordnet ist. Die Playbook-Komponente wird nur für den Process Automation Designer (PAD) unterstützt, der erstellt wurde. „Major Security Incident Management“ stellt mit dem Basissystem das Playbook für Anfragen an die Rechtsabteilung bereit.

Playbook für Anfragen an die Rechtsabteilung

Das Playbook „Rechtsanforderung“ enthält eine Schritt-für-Schritt-Anleitung, wie Sie die Rechtsabteilung über die aktuelle Zusammenfassung eines MSI informieren können, damit die SEC innerhalb des für wesentliche Verstöße erforderlichen Zeitraums von vier Tagen benachrichtigt werden kann.

Übersicht

Als Incident-Manager können Sie das Playbook für Anfragen an die Rechtsabteilung verwenden, um das Rechtsteam über die aktuelle Zusammenfassung eines MSI zu informieren, damit es die SEC über wesentliche Verstöße benachrichtigen kann. Sie können die Vorlagen des Prozessautomatisierungs-Designers (PAD) verwenden, um die Schritte im Playbook für Anfragen an die Rechtsabteilung auszuführen und das Team der Rechtsabteilung entsprechend zu informieren.

Dieses Playbook kann verwendet werden, wenn ein schwerwiegender Security Incident erstellt oder aktualisiert wird. Sie müssen das Playbook für Anfragen an die Rechtsabteilung in PAD aktivieren und dann alle Aufgaben ausführen, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

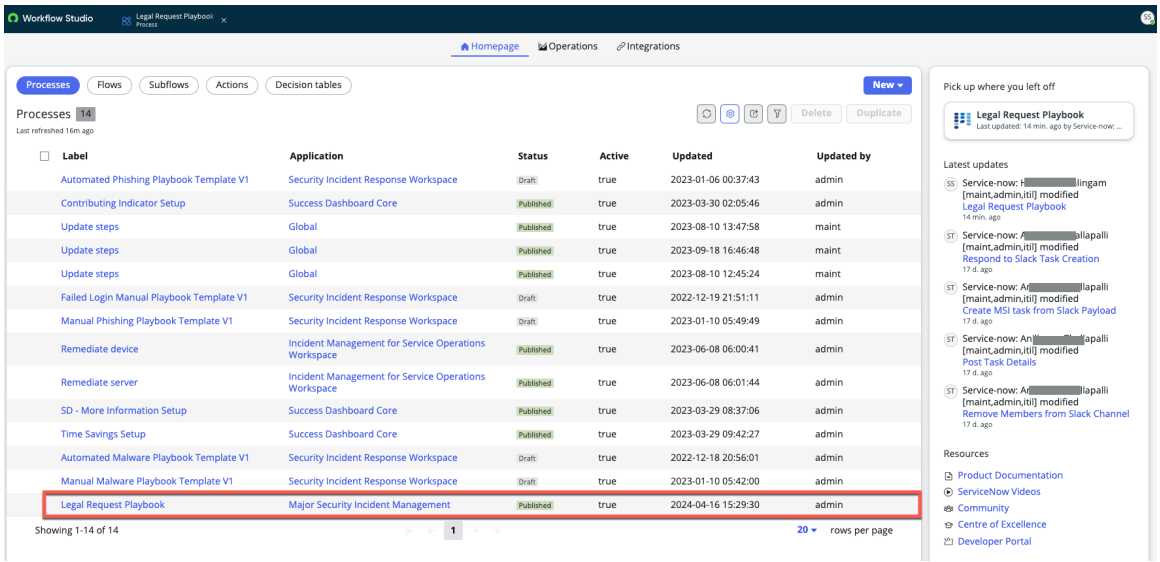
Die folgenden Spalten der Prozessdefinition entsprechen dem Status des schwerwiegenden Security Incident:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Spalte enthält bestimmte Aktivitäten.

Playbook für Anfragen an die Rechtsabteilung



Sobald Sie eine Aufgabe in einer Spur als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt (Datum und Uhrzeit) zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Spur abgeschlossen haben, können Sie zur nächsten Spur wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weitere Aufgaben und Spuren abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für die jeweilige Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die Details zu überprüfen, die Sie in allen Spuren eingegeben haben. Sie können jedes Feld bearbeiten oder **Fertigstellen** wählen, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für das Playbook für Anfragen an die Rechtsabteilung

Führen Sie diese Schritte aus, um Prozesse für das Playbook für Anfragen an die Rechtsabteilung im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager.

Prozedur

1. Klicken **ALLE** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**.

   Beispiel: Playbook für Anfragen an die Rechtsabteilung.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie auf **Auslöser auswählen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Eigene Bedingungen für die Ausführung Ihres Prozesses definieren aus**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken Sie auf **Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
7. Klicken Sie auf **Zum Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwerfen Ihres automatisierten Prozesses zu beginnen, klicken Sie **auf Neue Spalte hinzufügen**.
   Das Feld Spalteneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich Spalteneigenschaften die folgenden Details ein: **Name**, **Beschreibung**, **Ausführungsbedingung**und **Startzeitpunkt angeben**.
   Die Felder **Ausführungsbedingung** und **Startzeitpunkt angeben** geben an, wann die Spalte ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Spalte hinzuzufügen, klicken Sie auf **Weitere Spalte hinzufügen**.
    Ebenso können Sie beliebig viele Spuren erstellen. In diesem Beispiel können Sie eine Spalte für „Analyse“, „Eindämmen“, „Beseitigen“ und „Überprüfen“ erstellen. Im folgenden Beispiel startet **die Analysespalte** sofort und weist keine Ausführungsbedingung auf. Die Spalte**„Contain“** beginnt, nachdem die vorherige Spalte abgeschlossen wurde, und verfügt über eine Ausführungsbedingung, die auf dem Ergebnis einer Aktivität in der vorherigen Spalte basiert.
    Nachdem Sie die Spuren hinzugefügt haben, müssen Sie für jede Spur Prozessaktivitäten hinzufügen.
12. Klicken Sie auf **Weitere Prozessaktivität hinzufügen** unter einer bestimmten Spalte (z. B. Spalte „Analyse“).
    Das Popup-Fenster „Aktivität hinzufügen“ wird geöffnet.
    a. Wählen Sie im Popup-Fenster „Aktivität hinzufügen“ die gewünschte Aktivitätsdefinition aus.
13. Klicken Sie auf **Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Spuren konfiguriert werden. Auf ähnliche Weise können Sie auch andere Prozessaktivitäten unter jeder Spalte erstellen.
14. Fügen Sie im Bereich Aktivitätseigenschaften eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) wird angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie **auf Alle Eigenschaften anzeigen** und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mithilfe des Playbooks für Anfragen an die Rechtsabteilung

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook für Anfragen an die Rechtsabteilung im MSIM-Arbeitsbereich und seine Funktionen verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager.

Prozedur

1. Öffnen Sie im MSIM-Arbeitsbereich einen schwerwiegenden Security Incident.
2. Wählen Sie die Registerkarte **Playbook** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Playbooks anzeigen, die für den schwerwiegenden Security Incident aktiviert wurden.

Hinweis:
Wenn die Playbooks nicht aufgelistet sind, müssen Sie zu PAD wechseln und sie auf der Registerkarte **„Playbook“** aktivieren, damit sie angezeigt werden.

3. Wählen Sie das **Playbook für Anfragen an die Rechtsabteilung**aus.
4. Klicken Sie auf jede Spur, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen. Sie haben die Möglichkeit, dies entsprechend Ihren Anforderungen zu ändern.
6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase durchgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn Sie noch Aktivitäten oder Anwenderaktionen ausführen müssen, werden sie in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch Aktivitäten oder Anwenderaktionen erforderlich sind, klicken Sie auf die entsprechende Phase und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Rollup-Framework für MSIM

Erweitert die Fähigkeit zum Verknüpfen der Quelldatensätze aus dem Arbeitsbereich Management schwerwiegender Sicherheits-Incidents.

Übersicht

Mit dem Rollup-Framework ist der Rollup-Flow konfigurierbar und erweiterbar. Verwenden Sie dieses Framework-Modell, um die Informationen zu konfigurieren, die zu einem schwerwiegenden Security Incident zusammengefasst werden können.

Zuvor konnte sn_msi.workspace_manager die Security Incidents und angreifbaren Elemente verknüpfen, die als MSIvorgeschlagen oder heraufgestuft wurden. Nach der Verknüpfung des Security Incidents oder des angreifbaren Elements wurden die Informationen zu einem schwerwiegenden Security Incident zusammengefasst. Die Art der Informationen, die für das Rollup erforderlich sind, war in den Skripts hartcodiert.

Sie können das Framework-Modell zum Konfigurieren des Rollup-Flows verwenden, der die folgenden Funktionen unterstützt und auch die vorhandenen Probleme in der Anwendung behandelt:

Das Rollup-Framework-Modell bietet sn_msi.workspace_manager mit den folgenden Vorteilen:

- Fügen Sie die Datensatzfähigkeiten „Verknüpfen“ in jeder Tabelle hinzu, oder entfernen Sie sie, oder schlagen Sie MSI vor, oder stufen Sie sie herauf, wodurch die Aufgabentabelle erweitert wird.
- Steuern Sie die Art der Informationen, für die ein Rollup auf MSI durchgeführt werden soll, während Aktionen wie Verknüpfen/Vorschlagen/Heraufstufen für die Incident-Datensätze ausgeführt werden.
- Unterstützen Sie das Verknüpfen, Vorschlagen oder Heraufstufen von Security Incidents, Korrekturaufgaben und sofort einsatzbereiten Security Cases (OOTB) sowohl in der klassischen Umgebung als auch im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents.

Das Rollup-Framework weist die in der folgenden Tabelle erläuterten Konfigurationen auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationen des Rollup-Frameworks

Name	Beschreibung
Konfiguration verknüpfter Datensätze	Speichert die Informationen von Aufgabentabellen, die zum Verknüpfen/Heraufstufen/Vorschlagen mit Major Security Incidentverwendet werden können.
Konfiguration von Rollup-Datensätzen	Erfasst die Informationen, die aus der Aufgabentabelle zusammengefasst werden können, wenn Verknüpfungs-/Heraufstufungs-/Vorschlagsaktionen ausgeführt werden.
Listenlayoutkonfiguration	Steuert die Bezeichnungen und das Listenlayout für verschiedene Tabellen, wie auf den Registerkarten des Arbeitsbereichs Management schwerwiegender Sicherheits-Incidents angezeigt, z. B. Incident-Auswirkung, Verknüpfte Datensätze und Threat Intelligence.

Konfigurieren Sie verknüpfte Datensätze in Management schwerwiegender Sicherheits-Incidents

Verwenden Sie die Konfiguration verknüpfter Datensätze, um die Informationen von Aufgabentabellen zu speichern, die zum Verknüpfen/Heraufstufen/Vorschlagen mit Major Security Incidentverwendet werden können.

Erforderliche Rolle: admin und sn_msi.workspace_admin.

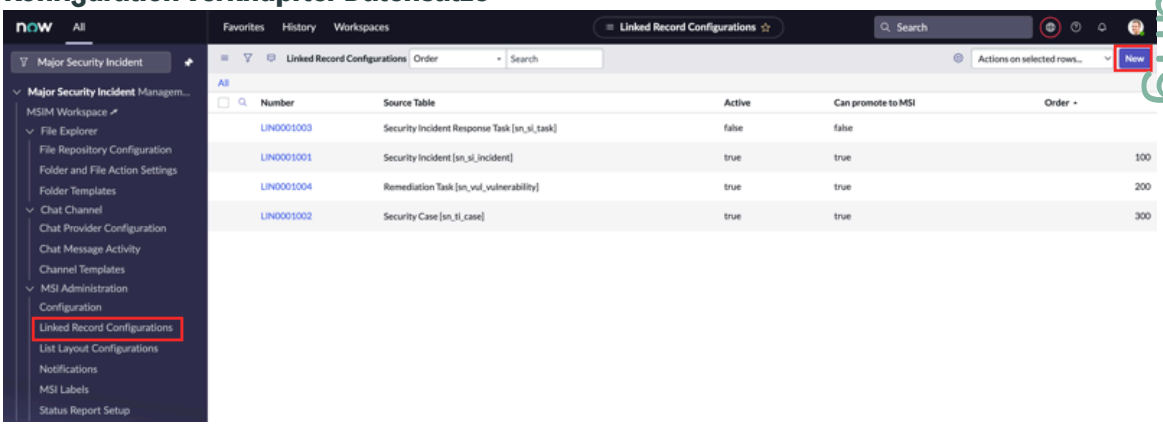
Hinweis:
Der Administrator kann den Datensatz erstellen, und der Administrator des Arbeitsbereichs MSIM kann den Datensatz aktualisieren.

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Konfigurationen verknüpfter Datensätze**.

   Die Seite „Konfiguration verknüpfter Datensätze“ wird angezeigt.

Konfiguration verknüpfter Datensätze

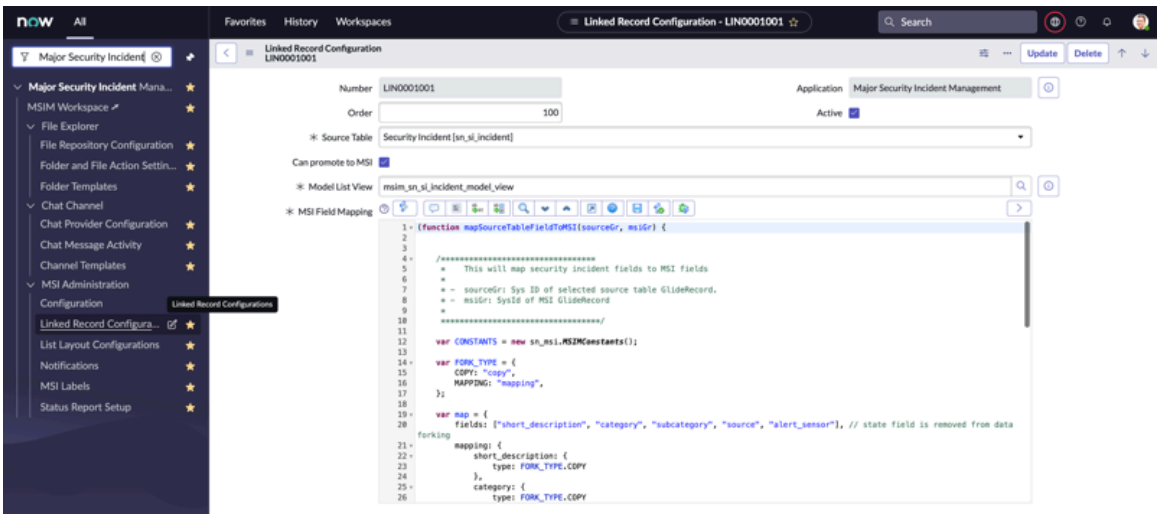


2. Klicken Sie auf der Seite „Konfiguration verknüpfter Datensätze“ auf **Neu**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Stellen Sie sicher, dass sich die Anwendung im Bereich Management schwerwiegender Sicherheits-Incidents befindet.



3. Füllen Sie die Felder des Formulars für die Datensatzkonfiguration aus.

Feldbeschreibungen für verknüpfte Datensätze

Feld	Beschreibung
Quelltabelle	Gibt die Aufgabentabelle an, die verknüpft und per Rollup mit Major Security Incidentverknüpft werden muss.
Bestellung	Ermöglicht es Ihnen, die Reihenfolge der aktuellen Quelltabelle in der Dropdownliste des MSIM-Arbeitsbereichs zu steuern. Nachfolgend finden Sie ein Beispiel für die **Reihenfolge**. Siehe Abbildung 1 unten, die nach dieser Tabelle bereitgestellt wird.
Modell ListView	Wählen Sie eine Ansicht aus, die das Listenlayout steuern kann, das in der modalen Liste für verknüpfte Datensätze angezeigt wird.
Kann heraufstufen auf MSI	Aktivieren Sie dieses Kontrollkästchen, um zu bestätigen, ob der Datensatz ein primärer Datensatz ist. Nachfolgend finden Sie ein Beispiel für die Auswahl der Option **„Kann zu MSI heraufstufen“**. Sehen Sie sich die folgende Abbildung 2 an, die nach dieser Tabelle bereitgestellt wird. Wenn dieses Kontrollkästchen aktiviert ist und der Wert „true“lautet, gilt: ○ können Sie einen Quelldatensatz mithilfe der klassischen Umgebungsaktionen mit zusätzlichen Konfigurationen direkt zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Major Security Incident vorschlagen und heraufstufen. ○ können Sie Quelldatensätze sowohl in der klassischen Umgebung als auch im Arbeitsbereich MSIM mit schwerwiegenden Security Incidents verknüpfen. ○ Management schwerwiegender Sicherheits-Incidents Auf der verknüpften Datensatzseite des Arbeitsbereichs werden die Datensätze der verknüpften Quelltabelle angezeigt. **Hinweis:** Wenn ein Datensatz direkt als Major Security Incidentvorgeschlagen/ heraufgestuft werden kann, ist dieser Datensatz ein primärer Datensatz. In der Konfiguration der Tabellenkonfiguration für Sicherheitsantwortaufgaben ist beispielsweise der Wert von **Kann zu MSI heraufstufen** gleich „false“, da Sie die Sicherheitsantwortaufgabe nicht direkt zu Major Security Incidentheraufstufen können. Daher wird es nicht in der Dropdown-Liste der verknüpften Datensatzregisterkarten des Arbeitsbereichs MSIM angezeigt.
MSI Feldzuordnung	Schreiben Sie ein Skript, um die Quelldatensatzfelder einem neu erstellten schwerwiegenden Security Incident zuzuordnen, wenn der Quelltabellendatensatz gerade vorgeschlagen oder heraufgestuft wird. Dieses Skript wird nur ausgeführt, wenn für **„Kann zu MSI heraufstufen“** der Wert „wahr“ festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abbildung 1: Listenansichtsreihenfolge der verknüpften Datensätze

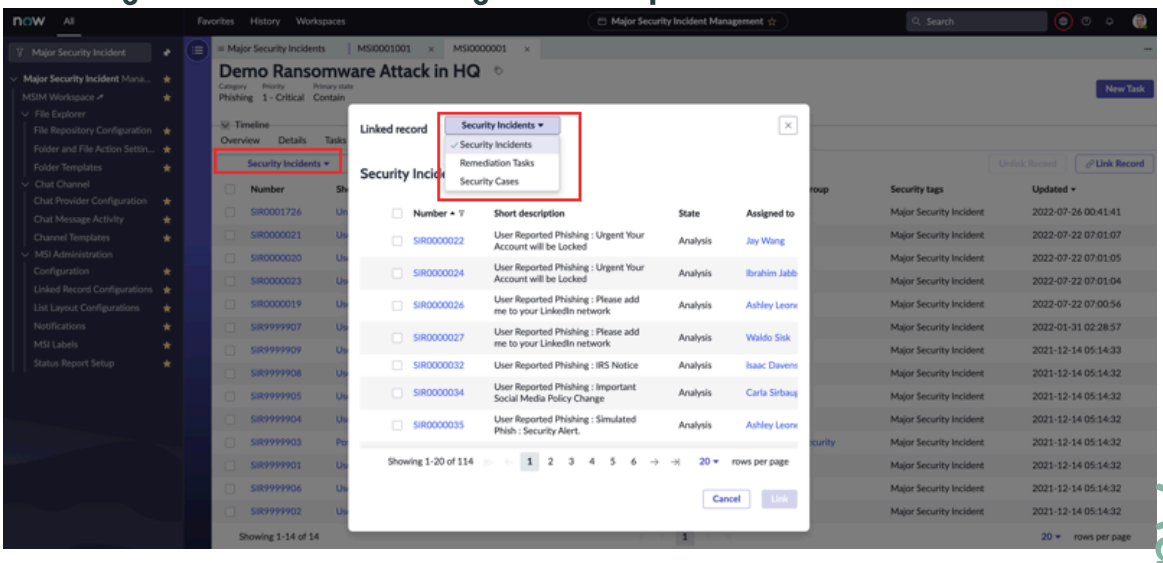
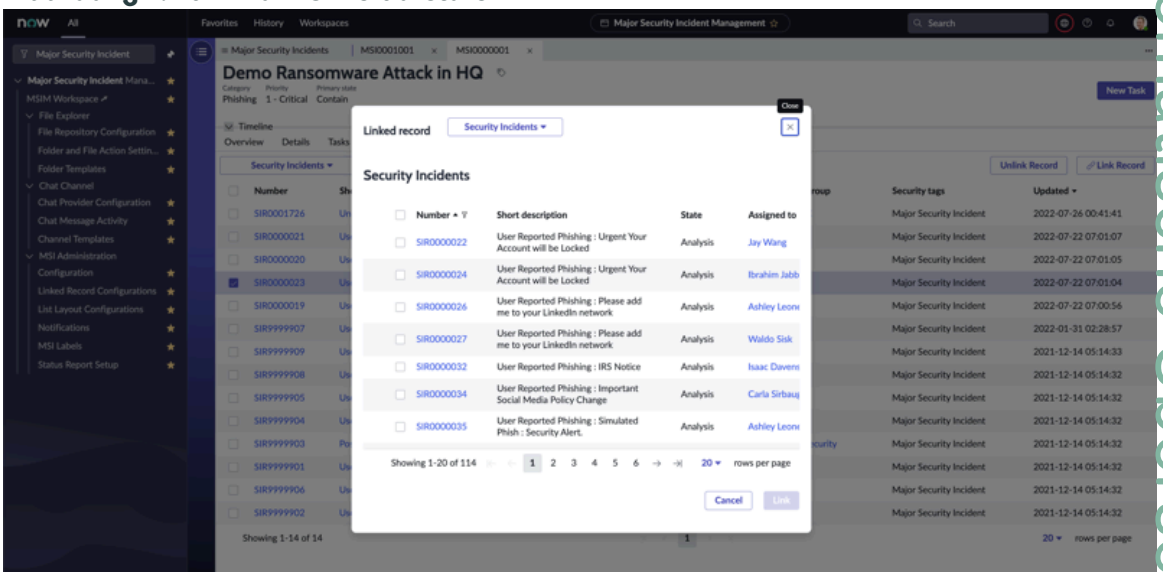


Abbildung 2: Kann zu MSI heraufstufen



Automatische Übersetzung

Rollup-Datensätze in konfigurieren Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents, um die Informationen zu steuern, für die ein Rollup durchgeführt wird, wenn der Quelldatensatz als schwerwiegender Security Incident verknüpft/vorgeschlagen/heraufgestuft wird.

Erforderliche Rolle: admin und sn_msi.workspace_admin.

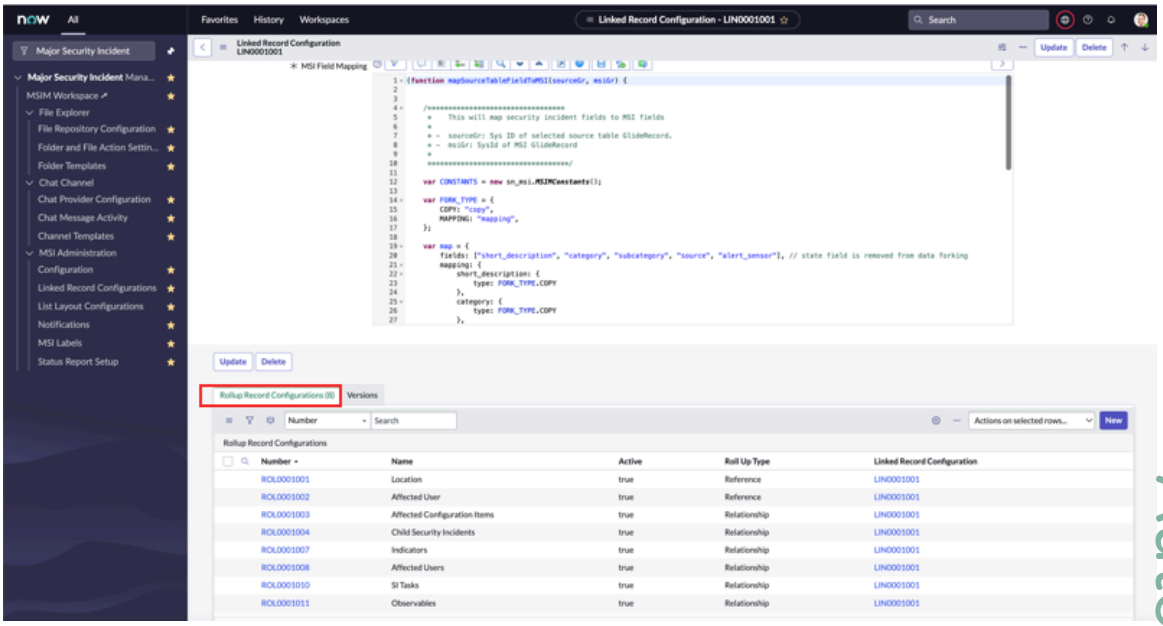
Hinweis:
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

Prozedur

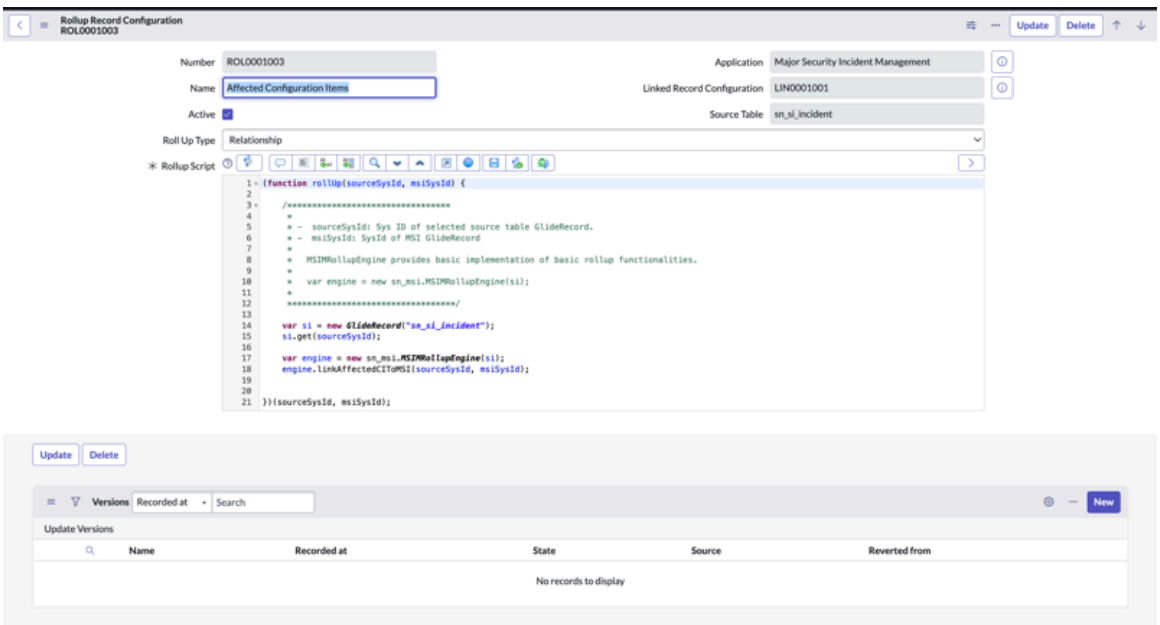
1. Navigieren zu **Major Security Incident Response** > **Konfiguration verknüpfter Datensätze**. Die Seite „Konfigurationen verknüpfter Datensätze“ wird angezeigt.
2. Wählen Sie einen neuen verknüpften Datensatz aus, oder erstellen Sie einen neuen, und navigieren Sie auf derselben Seite zum Abschnitt **„Rollup-Datensatzkonfiguration“**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Rollup-Datensatzkonfiguration“.



3. Klicken Sie auf **Neu**.



4. Füllen Sie auf der Konfigurationsseite die Details aus.

Konfiguration von Rollup-Datensätzen

Feldname	Feldbeschreibung
Name	Gibt den Namen des Rollup-Datensatzes an.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die aktuelle Konfiguration zu implementieren, wenn das Rollup des Quelldatensatzes stattfindet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Feldbeschreibung
Konfiguration verknüpfter Datensätze	Gibt eine eindeutige Nummer an, die sich auf die Konfiguration Ihrer übergeordneten verknüpften Datensätze bezieht und schreibgeschützt ist.
Quelltabelle	Der schreibgeschützte Quelltabellenname, der in der Konfiguration des verknüpften Datensatzes verwendet wird.
Rollup-Typ	Beschreibt die Art der Informationen, für die ein Rollup durchgeführt werden soll ○ **Beziehung**: Wählen Sie diese Option aus, wenn die Daten als zugehörige Liste vorhanden sein müssen. ○ **Referenz**: Wählen Sie diese Option aus, wenn die Daten als Referenzfeld im Quelltabellenformular vorhanden sind.
Rollup-Skript	Wenn der Rollup-Typ auf **Beziehung**festgelegt ist, ist das Feld **Rollup-Skript** aktiviert, das Ihnen das Schreiben von Skripts ermöglicht und zum Rollup von Informationen verwendet werden kann. Hier empfängt das Skript die Eingaben, die Informationen zum Quelldatensatz und zum schwerwiegenden Security Incident enthalten. Das Skript sollte in der Lage sein, die Informationen aus den Beziehungstabellen und dem Rollup in der Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_child) zu finden.
Quellfeld	Wenn der Rollup-Typ **Referenz**ist, ist das **Quellfeld** verfügbar. Dadurch können Sie das Referenzfeld Quelltabelle auswählen, das die Informationen enthält, für die ein Rollup durchgeführt werden musste.
Zielfeld	Wenn der Rollup-Typ **Referenz**ist, ist das **Zielfeld** verfügbar. Dadurch können Sie auf ein Referenzfeld aus der Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_child) verweisen und die Daten speichern, die im ausgewählten Quellfeld und im Quelltabellendatensatz vorhanden sind.

Skript für Rollup schreiben

Name	Beschreibung
Eingaben	• sourceSysId: Sys-ID des Quelltabellendatensatzes, der entweder verknüpft/vorgeschlagen/heraufgestuft wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

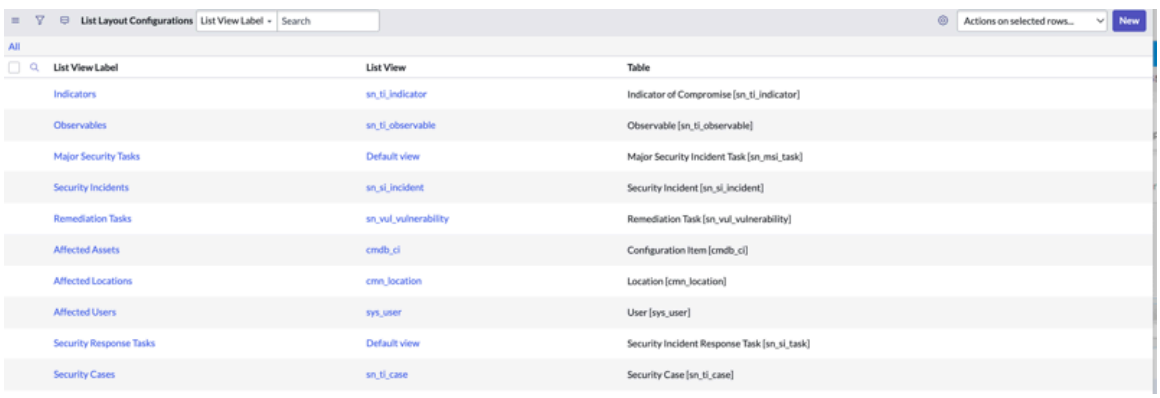
Name	Beschreibung
	• msiSysId: Sys-ID des schwerwiegenden Security Incidents, mit dem der Quelldatensatz verknüpft/vorgeschlagen/ heraufgestuft wird.
Ausgabe	Kein Ausgaberückgabewert.
Verantwortlichkeit	Das Skript sollte Informationen in der Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_child) zusammenfassen. • Verwenden Sie sourceSysID, um Daten aus ServiceNow -Beziehungstabellen abzufragen. • Nachdem die Daten abgerufen wurden, führen Sie ein Rollup der Daten in einem verknüpften Datensatz (sn_msi_m2m_child) mit dem Dienstprogramm MSIRollupEngine durch, um Daten zusammenzufassen.

Konfigurieren Sie das Listenlayout in Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie das Listenlayout, um das Layout und die verwendeten Bezeichnungen im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents anzupassen, z. B. die Registerkarten „Auswirkung auf Incidents“, „Verknüpfte Datensätze“ und „Threat Intelligence“.

Erforderliche Rolle: admin und sn_msi.workspace_admin.

Hinweis:
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

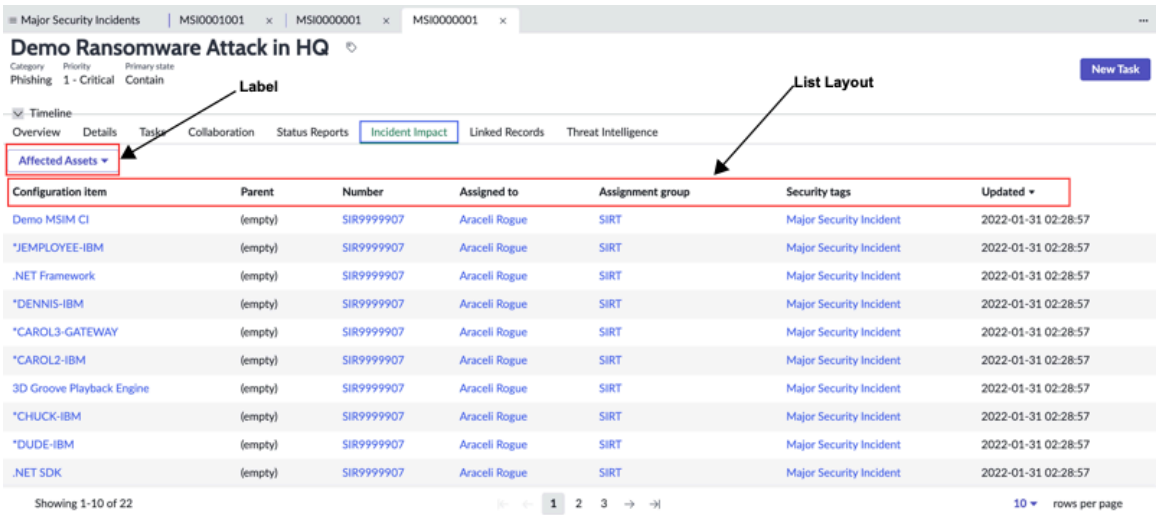


Die Listenlayoutkonfigurationen wurden bereits für vorhandene bekannte Tabellen geliefert, die im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Sie die anwenderdefinierte Ansicht für die vorhandenen Tabellen rendern möchten, können Sie den jeweiligen Tabellendatensatz in der Listenlayoutkonfiguration mit der anwenderdefinierten Listenansicht aktualisieren.
- Für neue Aufgabentabellen können Sie eine neue Listenlayoutkonfiguration erstellen, um die anwenderdefinierte Listenansicht und Bezeichnungen zu rendern. Ein detaillierteres Verfahren finden Sie unter Vorgehensweise Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte für verknüpfte Datensätze für einen Sicherheitsfall



Rollup-Beispiel-Anwendungsfallimplementierung für einen Sicherheitsfall

In den folgenden Schritten wird ein Beispielanwendungsfall erläutert, in dem erläutert wird, wie in der Tabelle „Schwerwiegender Security Incident“ für eine Sicherheitsfall-Tabelle Unterstützung für das Verknüpfen/Vorschlagen/Heraufstufen hinzugefügt wird.

- Schritt 1. Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall
- Schritt 2. Erstellen Sie eine Ansicht für ein modales Fenster für einen Sicherheitsfall
- Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall
- Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte für verknüpfte Datensätze für einen Sicherheitsfall
- Schritt 5. Fügen Sie Zugriffssteuerungslisten (ACLs) für Management schwerwiegender Sicherheits-Incidents -Arbeitsbereichsbenutzer hinzu
- Schritt 6. Erstellen Sie Geschäftsregeln für einen Sicherheitsfall
- Schritt 7. Erstellen Sie Rollup-Datensatzkonfigurationen

Schritt 1. Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall

Erstellt eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall.

Vorbereitungen
Erforderliche Rolle: admin und sn_msi.workspace_admin

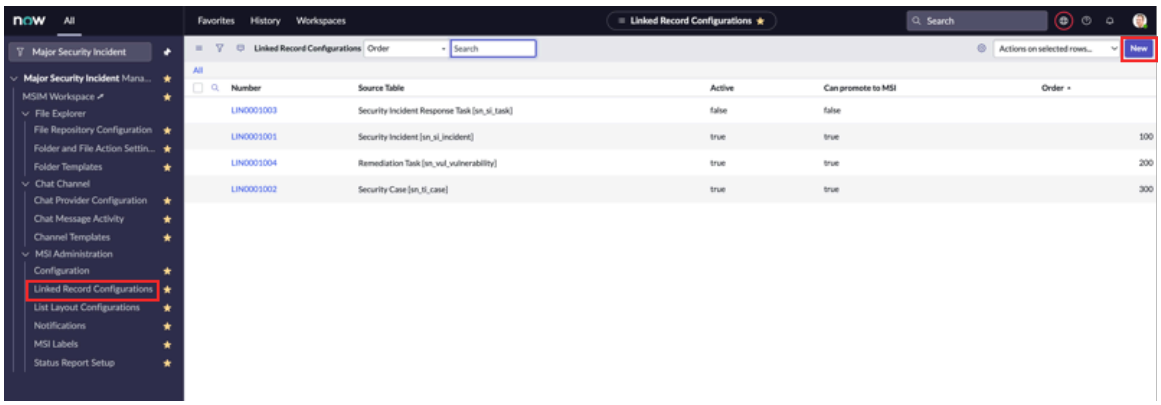
Hinweis:
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

Automatische Übersetzung

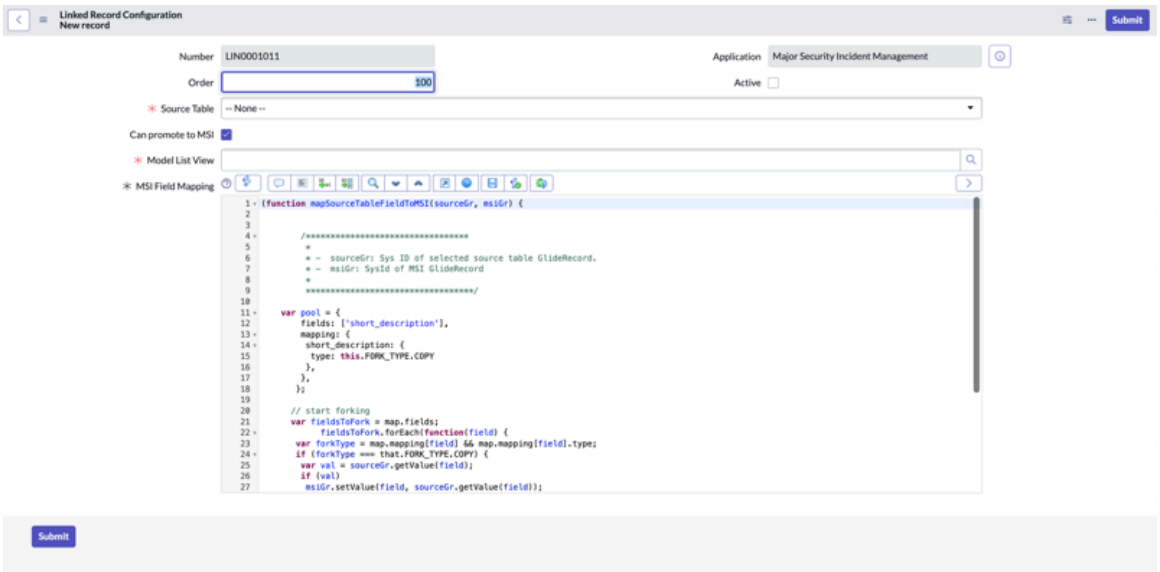
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Suchen Sie in der linken Navigation nach der Konfiguration verknüpfter Datensätze.
2. Klicken Sie auf **Neu**.



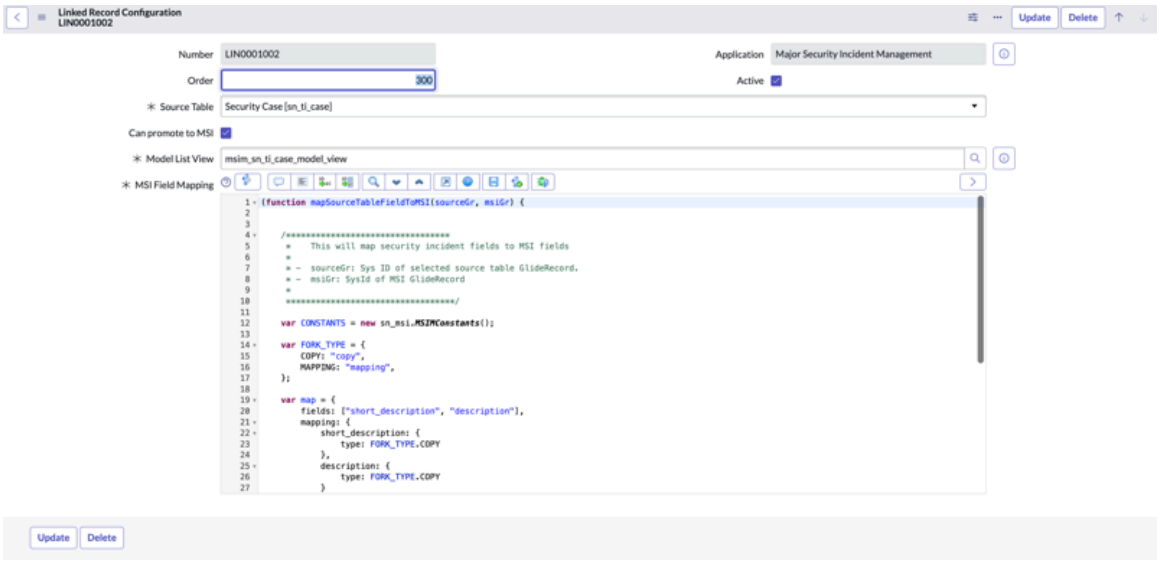
3. Füllen Sie das Formular mit den erforderlichen Spalten aus, und schreiben Sie ein Feldzuordnungsskript.



4. Sie haben jetzt eine verknüpfte Datensatzkonfiguration für den Sicherheitsfall erstellt, indem Sie die Werte wie in der folgenden Tabelle beschrieben hinzugefügt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Name	Beschreibung
Quelltabelle	Sicherheitsfall (sn_ti_case). Hier in diesem Beispiel wird ein Sicherheitsfall als MSI verknüpft/heraufgestuft/vorgeschlagen.
Bestellung	Eingabewert: 300 **Hinweis:** Ein niedrigerer Wert hat Vorrang vor höheren Werten. Da ein Security Case eine höhere Reihenfolge hat als der Security Incident und die Korrekturaufgabe, wird er in der letzten Sequenz angezeigt.
Hochstufen zu MSI möglich	„Wahr“. Aktivieren Sie dieses Kontrollkästchen, um den Sicherheitsfall zu MSI heraufzustufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: ○ Verknüpfung von Sicherheitsfalldatensätzen mit schwerwiegenden Security Incidents im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents automatisch herstellen bzw. aufheben. Außerdem ist die Funktion „Datensatzverknüpfung aufheben“ nur für die verknüpften Datensätze sichtbar. ▪ Dadurch wird das Verknüpfen von Sicherheitsfällen mit schwerwiegenden Security Incidents mithilfe klassischer Umgebungsaktionen ermöglicht, das Heraufstufen und Vorschlagen von zu Sicherheitsfällen möglich, diese UI-Aktionen sind jedoch nicht sofort einsatzbereit. Jede UI-Aktion muss manuell erstellt werden. Weitere Informationen finden Sie unter Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall. ▪ Die UI-Aktion „Linken/Heraufstufen/Vorschlagen“ ist für Security Incidents, Korrekturaufgaben und Sicherheitsfälle standardmäßig verfügbar. ○ Auf der Seite mit dem verknüpften Datensatz des MSIM-Arbeitsbereichs werden die verknüpften Sicherheitsfalldatensätze angezeigt. Sehen Sie sich die folgende Abbildung 1 an, um die Optionen anzuzeigen, die nach Aktivierung dieses Kontrollkästchens verfügbar sind.
Modale Listenansicht	msim_sn_ti_case_model_view

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: Diese Ansicht enthält Felder und deren Reihenfolge, die in der Listenansicht des modalen Elements „Linkdatensatz“ im MSIM-Arbeitsbereich angezeigt werden. Weitere Informationen finden Sie unter Schritt 2. Erstellen Sie eine Ansicht für ein modales Fenster für einen Sicherheitsfall Sehen Sie sich die folgende Abbildung 2 für die Ansicht von der Seite **„Verknüpfte Datensätze“** an.
Feldzuordnungsskript	Dieses Skript beschreibt die Felder aus dem Quelltabellen-Datensatz, die einem neu erstellten schwerwiegenden Security Incident zugeordnet werden, wenn der Quelltabellen-Datensatz vorgeschlagen oder heraufgestuft wird. die Eingaben empfangen: ○ sourceGr: Glide-Datensatzobjekt für Sicherheitsfall ○ msiGr: Glide-Datensatzobjekt für schwerwiegenden Security Incident Das Skript liest aus der Kurzbeschreibung des Sicherheitsfalls und kopiert sie als Titel für den schwerwiegenden Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abbildung 1: Kann zu MSI heraufstufen

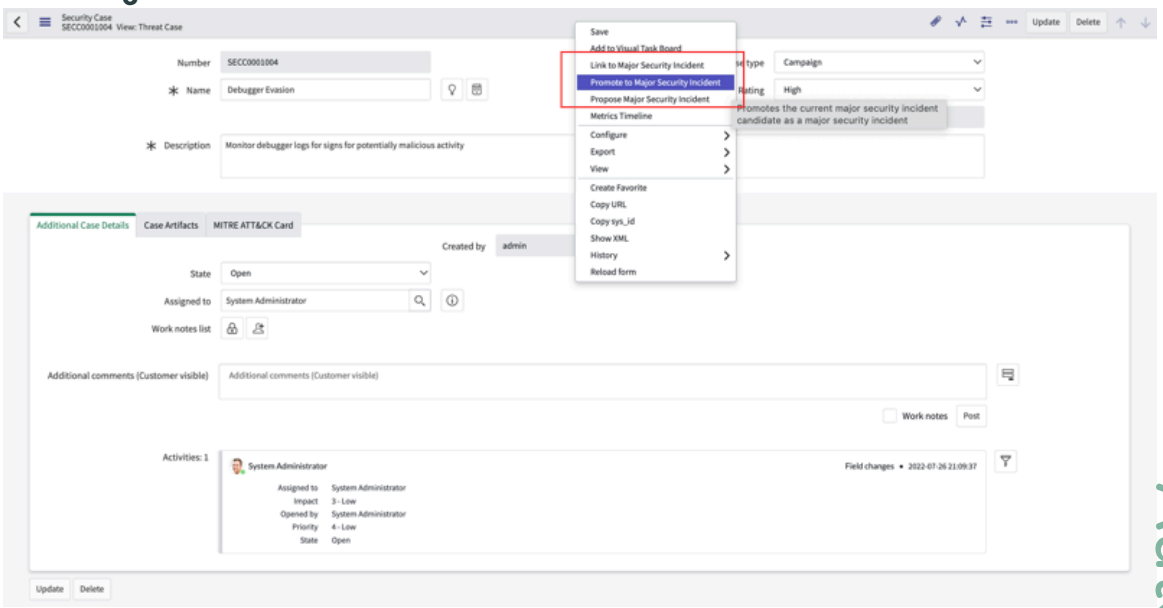
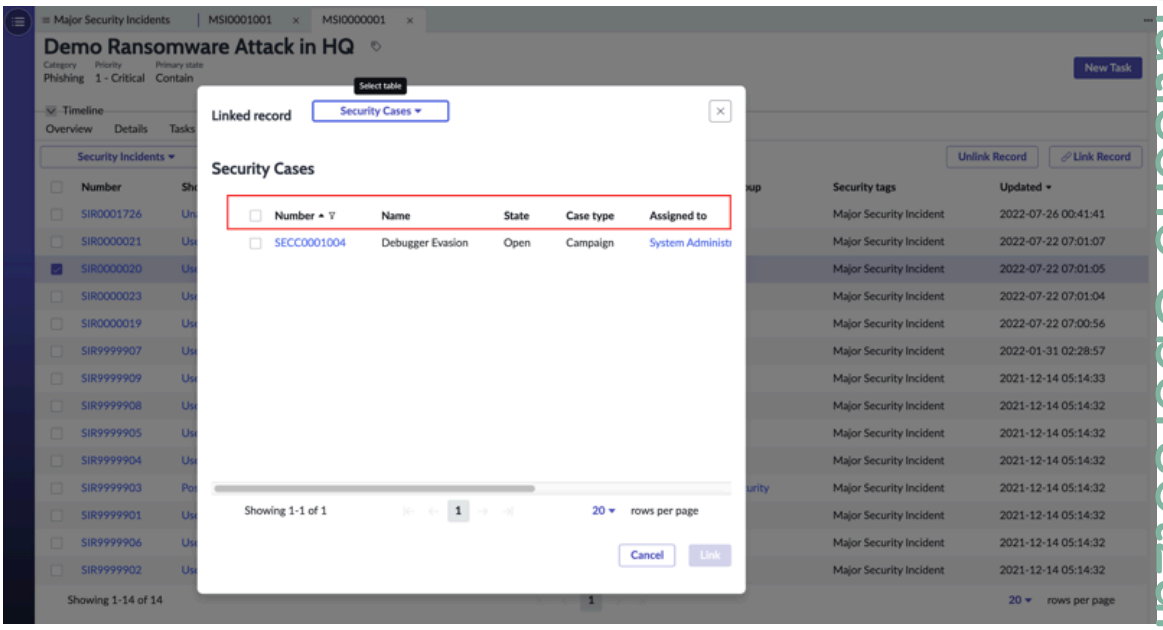


Bild 2. Modalansicht



Schritt 2. Erstellen Sie eine Ansicht für ein modales Fenster für einen Sicherheitsfall

Erstellt eine Ansicht für ein modales Fenster für einen Sicherheitsfall.

Vorbereitungen

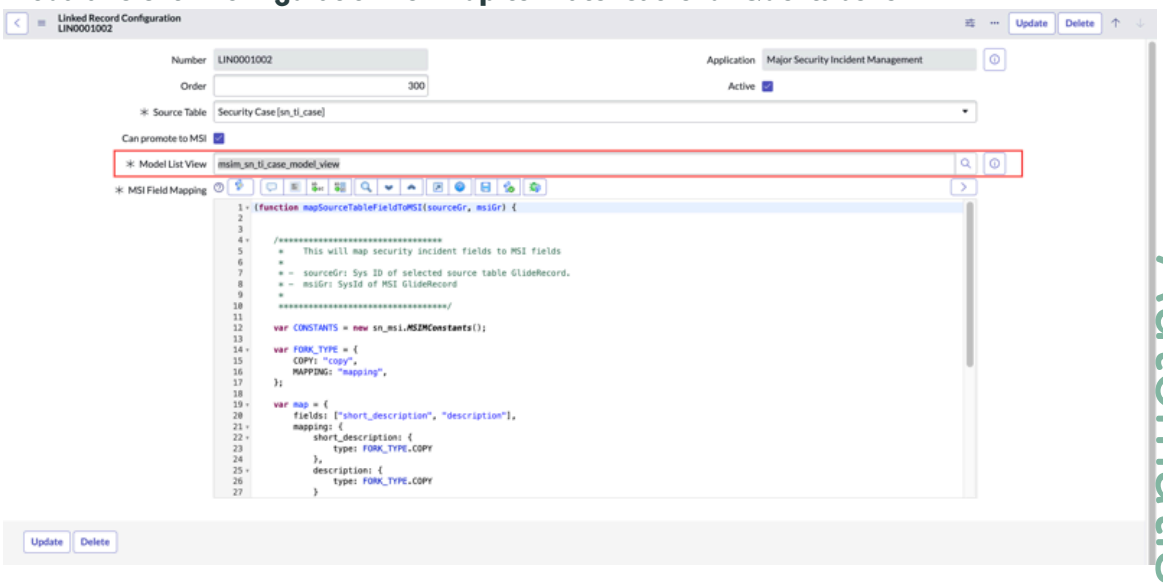
Wichtige Überlegung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Standardmäßig zeigt die modale Liste des verknüpften Datensatzes nur das **Standardlistenlayout** an. Wenn Sie das Listenlayout anpassen möchten, können Sie in der Quelltabelle **die anwenderdefinierte Ansicht** verwenden.
- Wenn Sie die anwenderdefinierte Ansicht rendern möchten, muss sie auch in der Konfiguration verknüpfter Datensätze für Quelltabelle ausgewählt werden.

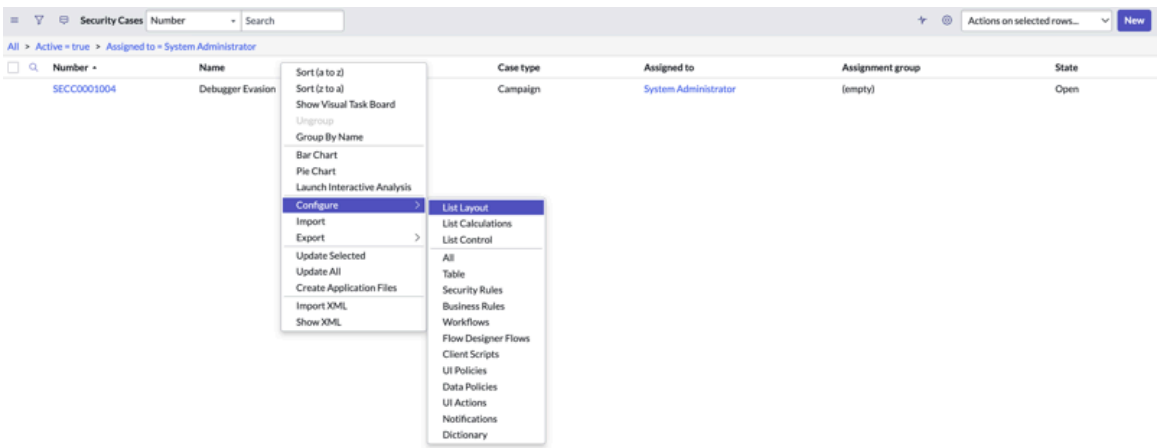
Modalansicht – Konfiguration verknüpfter Datensätze für Quelltabelle



Erforderliche Rolle: Administrator

Prozedur

1. Wechseln Sie zur Quelltabelle, und klicken Sie auf **Konfigurieren** > **Listenlayout**.



2. Gehe zu **Listenansicht** > **Name anzeigen**.
3. Klicken Sie in der Dropdown-Liste Ansichtsname **auf Neu**, und erstellen Sie eine neue Ansicht, z. B. msim_sn_ti_case_modal_view.
4. Wählen Sie die neu erstellte Ansicht aus.
   Nach der Auswahl können Sie die erforderlichen Felder aus der Liste Verfügbar auswählen.
5. Klicken Sie auf **Speichern**.
6. Navigieren zu **Menü** > **Aufrufe** um zu überprüfen, ob die Ansicht ordnungsgemäß gerendert wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall

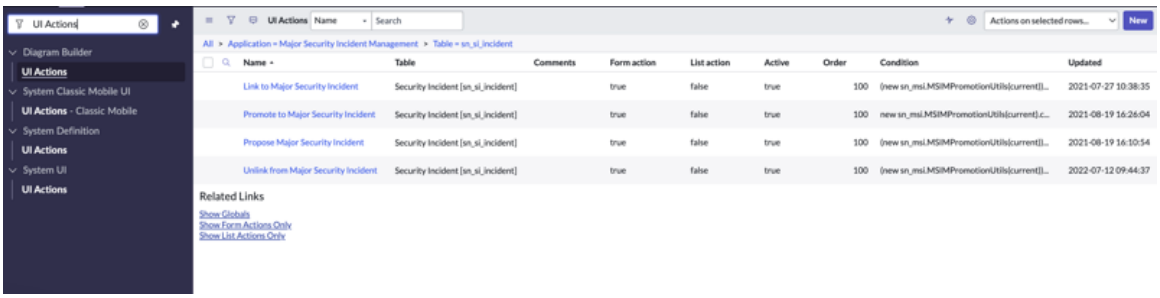
Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall.

Vorbereitungen

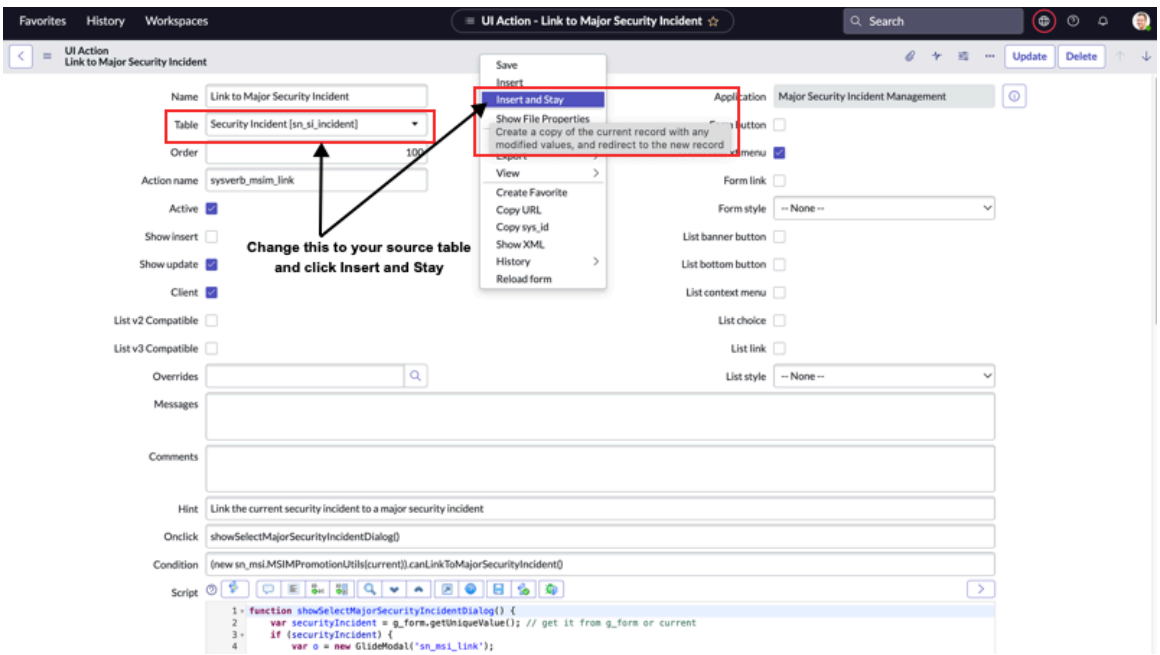
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Systemdefinition** > **UI-Aktionen**.
2. Führen Sie die Option Filter aus, um die Liste nach **Anwendung**: Major Security Incident Management und **Tabelle**: sn_si_incident zu filtern.



3. Wählen Sie jede UI-Aktion nacheinander aus, und speichern Sie die Details für die Quelltabelle.



4. Wiederholen Sie die gleichen Schritte wie oben für die folgenden UI-Aktionen:
   - Link zu schwerwiegendem Security Incident
   - Vorgeschlagener schwerwiegender Security Incident
   - Verknüpfung mit schwerwiegendem Security Incident aufheben
   - Zu schwerwiegendem Security Incident heraufstufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

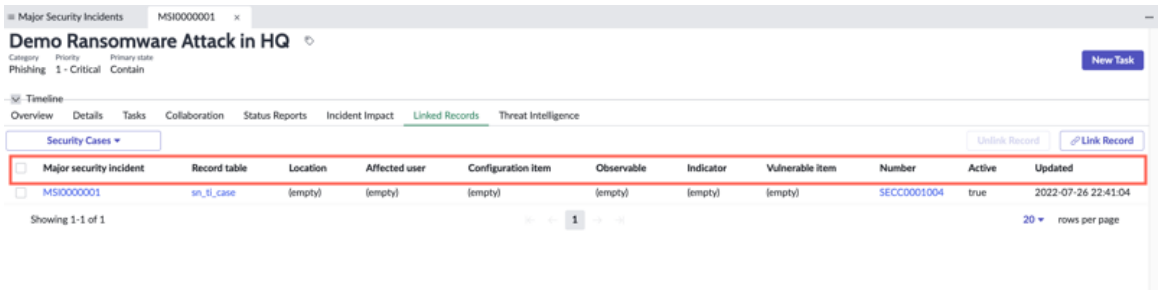
Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte für verknüpfte Datensätze für einen Sicherheitsfall

Passen Sie das Listenlayout für eine Sicherheitsfalltabelle an, wenn sie auf der Seite „Datensätze mit dem Arbeitsbereich Management schwerwiegender Sicherheits-Incidents verknüpfen angezeigt wird.

Vorbereitungen

Voraussetzungen:

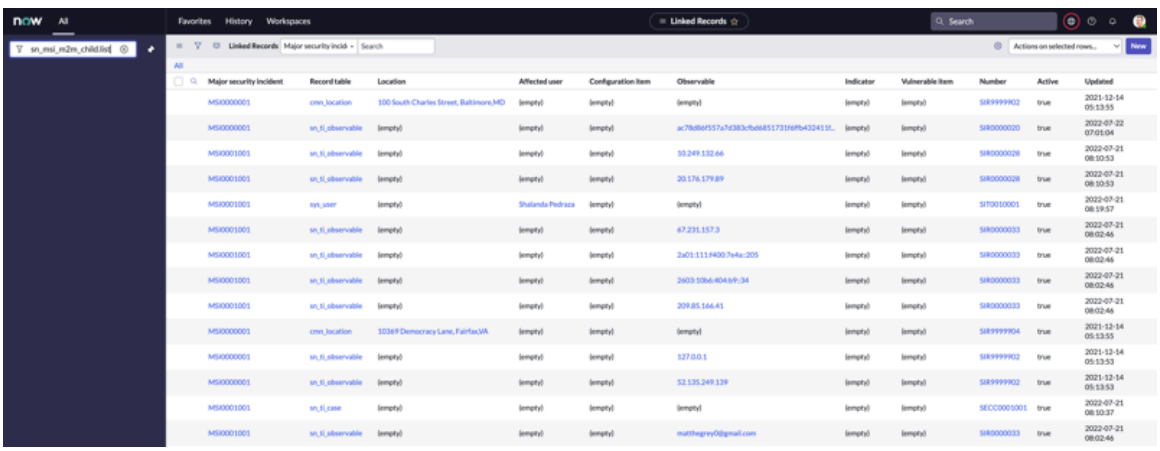
- Wählen Sie die Spalte aus, die sichtbar sein soll, wenn eine Liste für eine Sicherheitsfalltabelle gerendert wird.
- Wählen Sie die Reihenfolge der Felder aus, die in der Dropdown-Liste angezeigt werden sollen.



Erforderliche Rolle: Administrator

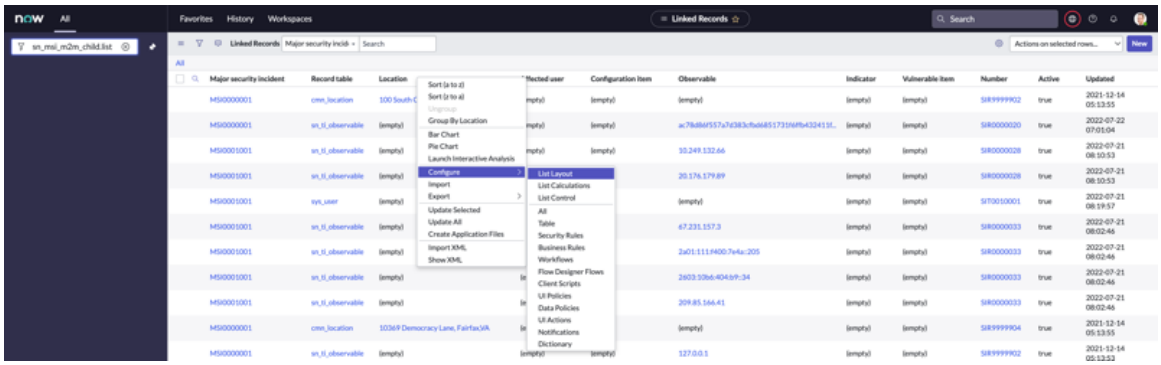
Prozedur

1. Suchen Sie mithilfe der linken Navigation **nach sn_msi_m2m_child.list**.
   Die Tabelle Verknüpfte Datensätze wird angezeigt.

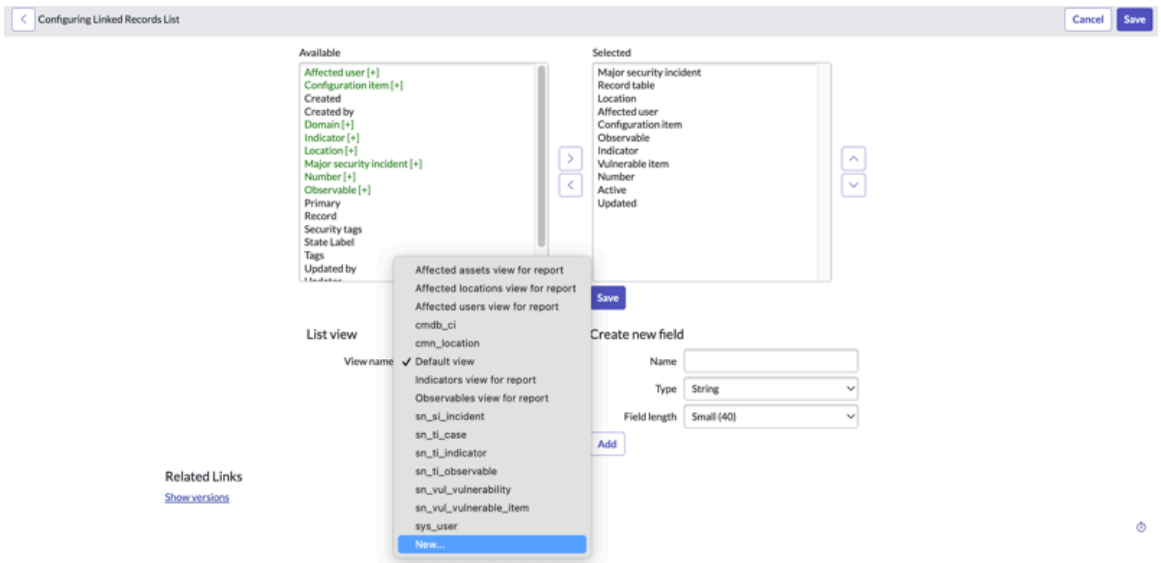


2. Klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie **Konfigurieren** > **Listenlayout**.
   Die Seite Konfiguration verknüpfter Datensätze wird angezeigt.

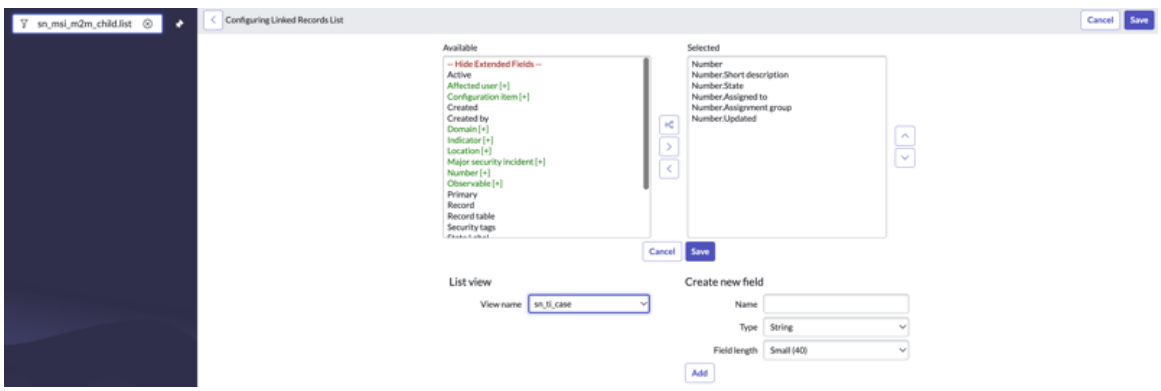
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Gehe zu **Listenansicht** > **Name anzeigen**.
4. Wählen Sie in der Dropdown-Liste Ansichtsname die **Option Neu** aus.



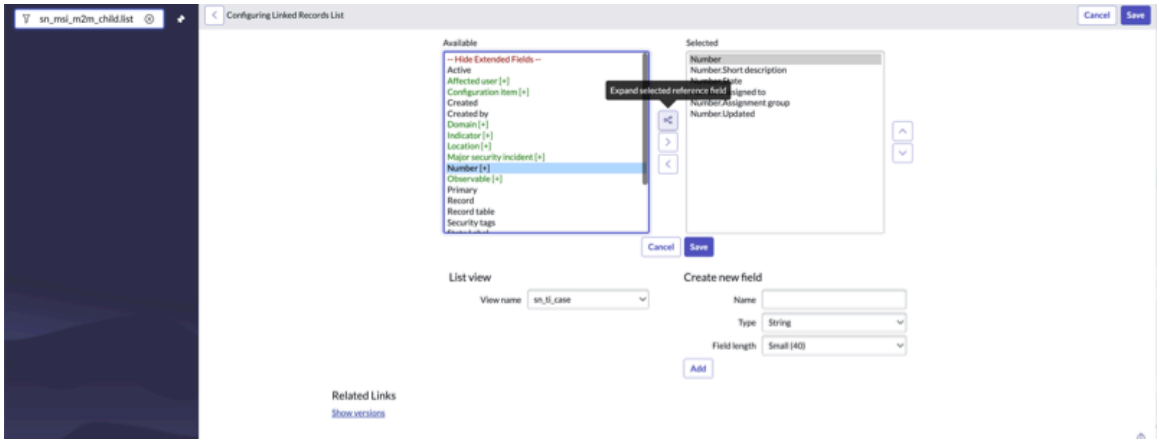
5. Wählen Sie die Spalten aus, die in der Listenansicht des Arbeitsbereichs gerendert werden.
   Der Sicherheitsfalldatensatz wird in der Spalte **Nummer** gespeichert. Um Informationen aus einem Sicherheitsfall zu rendern, müssen Sie in der **Nummernspalte** einen Dot-Walking durchführen.



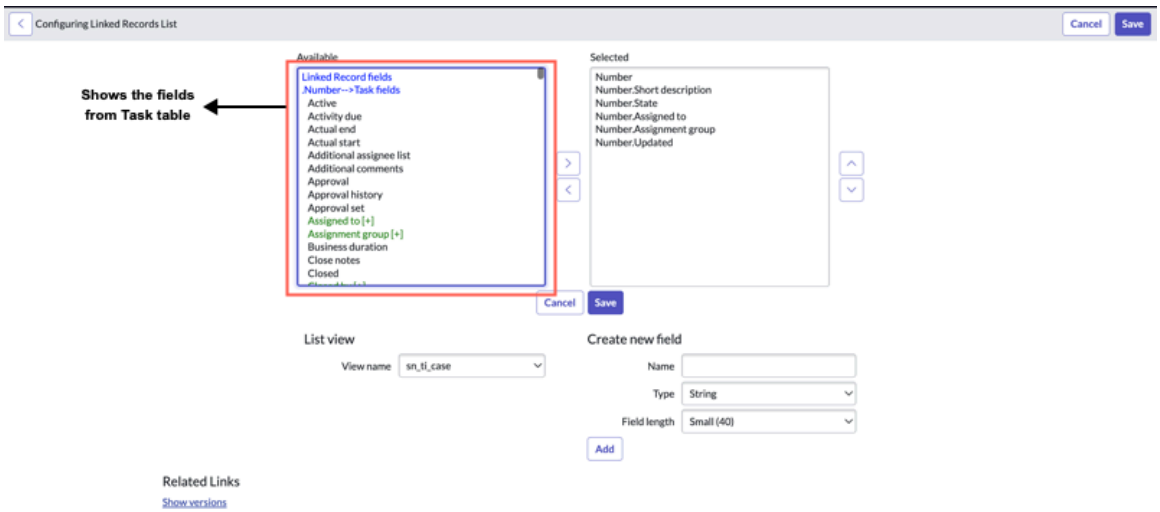
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Für Dot-Walking wählen Sie zuerst die Spalte **Nummer** aus der Liste Verfügbar aus, und klicken Sie dann auf **Ausgewähltes Referenzfeld erweitern**.



b. Erweitern Sie die Spalten unter **Anzahl**, um sie auszuwählen und in die Liste Ausgewählt zu verschieben.



c. Klicken Sie auf **Speichern**, um zu speichern und eine Ansicht zu erstellen.

6. Der nächste Schritt besteht darin, die erstellte Ansicht im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents zu rendern. Sie müssen eine **Listenlayoutkonfiguration**erstellen.

a. Suchen Sie mithilfe der linken Navigation nach der **Listenlayoutkonfiguration**.

b. Klicken **MSI-Administration** > **Listenlayoutkonfigurationen**.

c. Klicken Sie auf **Neu**, um eine neue Konfiguration zu erstellen.

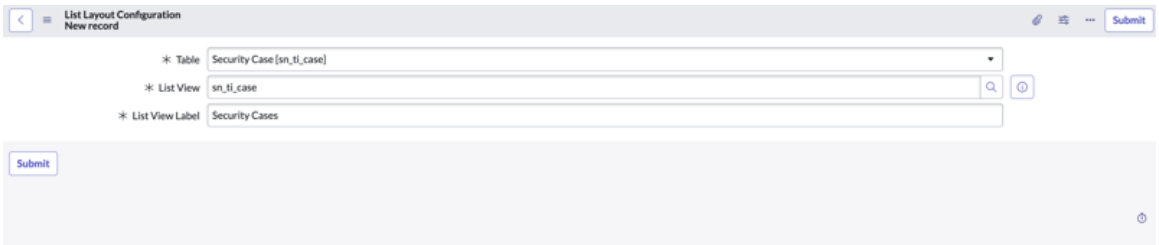
d. Wählen Sie die Quelltabelle aus der Spalte Tabelle und anschließend die neu erstellte Ansicht aus dem Feld Listenansicht aus.

e. Mit der Bezeichnung **„Listenansicht“** können Sie Bezeichnungen steuern, wenn dieselbe Quelltabelle im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents gerendert wird.

f. Speichern Sie den Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Navigieren Sie nach dem Speichern des Datensatzes zum Arbeitsbereich Management schwerwiegender Sicherheits-Incidents, um die gerenderte Listenansicht und die Bezeichnung im Arbeitsbereich anzuzeigen.



Schritt 5. Fügen Sie Zugriffssteuerungslisten (ACLs) für Management schwerwiegender Sicherheits-Incidents -Arbeitsbereichsbenutzer hinzu

Fügen Sie Zugriffssteuerungslisten (ACLs) für Benutzer des Arbeitsbereichs Management schwerwiegender Sicherheits-Incidents hinzu.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis:
Welche Berechtigungen zum Verknüpfen und Aufheben von Verknüpfungen erforderlich sind, wird von der Rolle sn_msi.linkedsivi_read gesteuert.

Management schwerwiegender Sicherheits-Incidents Persona enthält die Rolle „sn_msi.linkedsivi_read“.

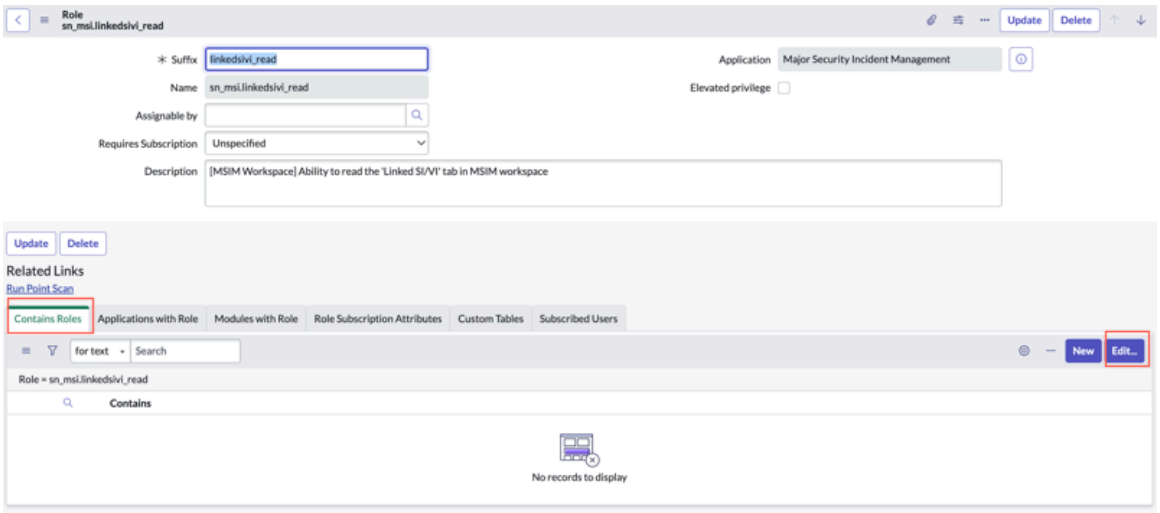
1. sn_msi.workspace_admin (MSIM-Arbeitsbereichsadministrator)
2. sn_msi.workspace_manager (MSIM-Arbeitsbereichsmanager)
3. sn_msi.workspace_responder (MSIM-Arbeitsbereich-Beantworter)

Hinweis:
Für jede -Quelltabelle müssen Sie sicherstellen, dass die erforderlichen -Rollen der Rolle „sn_msi.linkedsivi_read“ hinzugefügt werden.

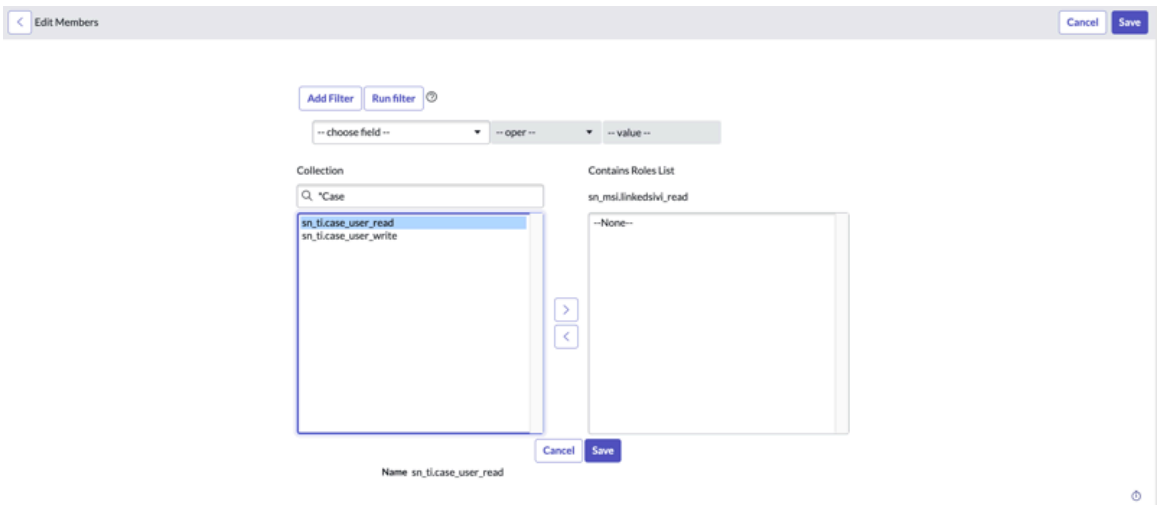
Prozedur

1. Navigieren zu **Anwenderadministration** > **Rollen** und suchen Sie nach der Rolle **sn_msi.linkedsivi_read**.
2. Klicken Sie im Abschnitt Enthält Rollen der zugehörigen Liste **auf Bearbeiten**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Stellen Sie sicher, dass Ihre Quelltabellenrollen im Abschnitt „Enthält Rollen“ hinzugefügt werden.
   Die Seite „Mitglieder bearbeiten“ wird angezeigt, um die für einen Sicherheitsfall erforderlichen Rollen zu konfigurieren.



4. Suchen Sie im Abschnitt Sammlungen nach den Quelltabellenrollen.
   Wählen Sie die erforderlichen Rollen aus, die Lese- und Schreibzugriff auf die Quelltabelle für einen Sicherheitsfall ermöglichen.

   Hinweis:

   - Für einen Sicherheitsfall sind zwei separate Rollen für Lesen und Schreiben erforderlich.
   - Schreibzugriff auf Tabellen für die Möglichkeit, den Quelldatensatz aus dem mit dem Arbeitsbereich Management schwerwiegender Sicherheits-Incidents verknüpften Datensatz-Modal auszuwählen.

5. Klicken Sie auf **Speichern**, um Rollen hinzuzufügen.
6. Stellen Sie sicher, dass die Rollen erfolgreich zum Abschnitt **„Enthält Rollen“** der zugehörigen Liste hinzugefügt wurden.

Schritt 6. Erstellen Sie Geschäftsregeln für einen Sicherheitsfall

Erstellen Sie die erforderlichen Business-Regeln für einen Sicherheitsfall.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Erstellen Sie die folgenden drei Geschäftsregeln für die neue Quelltabelle Security Case (sn_ti_case). Diese Business-Regeln sind erforderlich, um die Konsistenz des Verhaltens mit einer sofort einsatzbereiten Quelltabelle wie „Security Incident“ (sn_si_incident) zu gewährleisten.

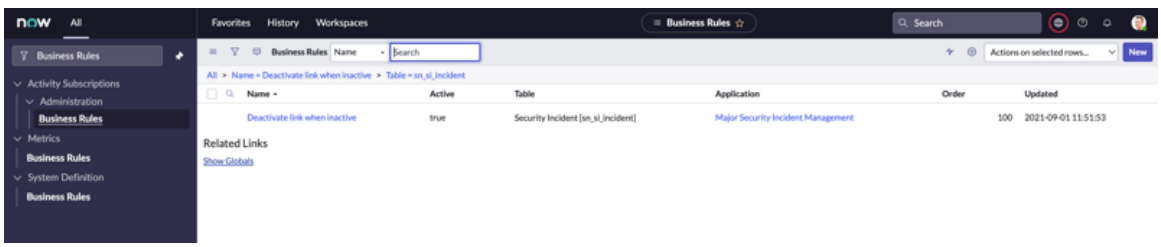
Business-Regeln für die neue Quelltabelle:

1. **Link deaktivieren, wenn inaktiv**: Sobald der Sicherheitsfall geschlossen ist, werden zugehörige Informationen auf der Seite des Arbeitsbereichs Management schwerwiegender Sicherheits-Incidents nicht mehr angezeigt.
2. **Teaminformationen beim Aktualisieren synchronisieren**: Die Registerkarte mit den Details zu schwerwiegenden Security Incidents zeigt Informationen zu allen aktiven Teams und Anwendern, die an verschiedenen Aufgaben arbeiten. Sobald Sie „Zugewiesen an“ aktualisiert haben oder die Zuweisungsgruppe im Sicherheitsfall geändert wurde, müssen Sie die Informationen zum Sicherheitsfall-Team im Abschnitt „Aktives Team für schwerwiegenden Security Incident“ aktualisieren. Diese Business-Regeln aktualisieren den Anwender im Feld „Zugewiesen an“ und die Zuweisungsgruppe im Abschnitt „Aktives Team“.
3. **Teaminformationen beim Löschen synchronisieren**: Die Registerkarte mit den Details zu schwerwiegenden Security Incidents zeigt Informationen zu allen aktiven Teams und Anwendern, die an verschiedenen Aufgaben arbeiten. Sobald der Sicherheitsfall geschlossen wurde, müssen im Abschnitt „Aktives Team des schwerwiegenden Security Incident“ keine Informationen mehr zum Sicherheitsfallteam angezeigt werden. Diese Business-Regeln entfernen den „Zugewiesen an“-Anwender und die Zuweisungsgruppe aus dem aktiven Team.

Business-Regeln für neue Quelltabelle erstellen:

Prozedur

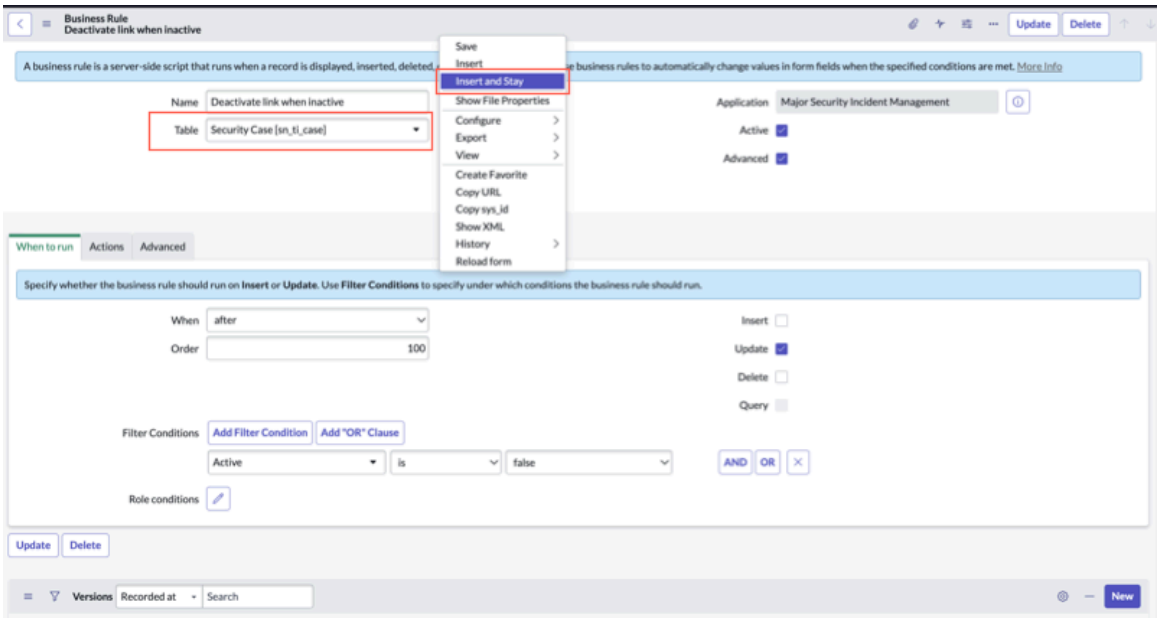
1. Navigieren zu **Systemdefinition** > **Business-Regeln**.
2. Führen Sie die Filteroption aus, um Business-Regelkriterien mit den folgenden Informationen zu filtern:
   - **Name**: Link deaktivieren, wenn inaktiv
   - **Tabelle**: sn_si_incident



3. Öffnen Sie den Datensatz, und ändern Sie den Tabellennamen in eine neue Quelltabelle: sn_ti_case.
4. Klicken Sie mit der rechten Maustaste auf das Menü auf der Seite, und klicken Sie auf **Einfügen und bleiben,** um den Datensatz zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wiederholen Sie den Vorgang für zwei weitere Geschäftsregeln.
   - Teaminformationen beim Löschen synchronisieren
   - Teaminformationen beim Aktualisieren synchronisieren

Schritt 7. Erstellen Sie Rollup-Datensatzkonfigurationen

Erstellen Sie eine Rollup-Datensatzkonfiguration, um zusätzliche Datensätze mit MSI zu verknüpfen und die Verknüpfung aufzuheben.

Vorbereitungen

Erforderliche Rolle: admin und sn_msi.workspace_admin

Hinweis:
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

Um ein Rollup für Informationen wie Konfigurationselemente, erkennbare Elemente und Kompromittierungsindikatoren im Zusammenhang mit einem Sicherheitsfall durchzuführen, erstellen Sie eine Rollup-Datensatzkonfiguration.

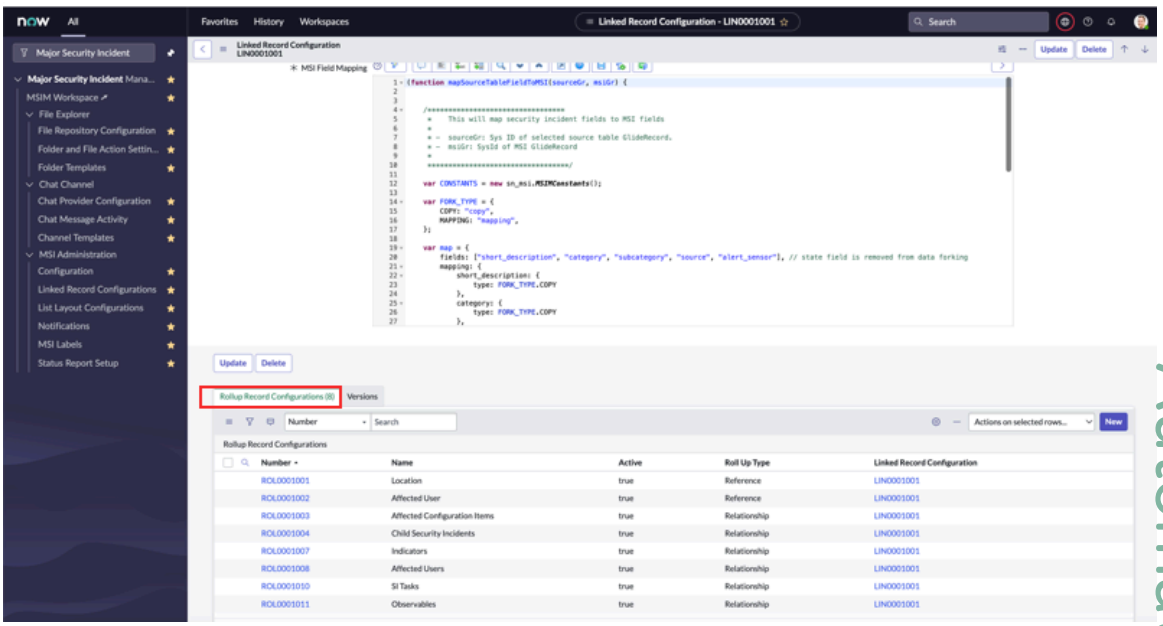
Prozedur

1. Navigieren zu **Major Security Incident Response** > **Konfiguration verknüpfter Datensätze**.
   Die Seite „Konfigurationen verknüpfter Datensätze“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie einen neuen verknüpften Datensatz aus, oder erstellen Sie einen neuen, und navigieren Sie auf derselben Seite zum Abschnitt **„Rollup-Datensatzkonfiguration“**.

Abschnitt „Rollup-Datensatzkonfiguration“.



Nächste Maßnahme

- Ausführlichere Informationen finden Sie unter Rollup-Datensätze in konfigurieren Management schwerwiegender Sicherheits-Incidents
- Ein Beispiel für einen Sicherheitsfall finden Sie unterSkript für einen Sicherheitsfall schreiben

Skript für einen Sicherheitsfall schreiben

Schreiben eines Skripts für einen Sicherheitsfall zum Rollup der Datensatzkonfiguration.

Vorbereitungen
Erforderliche Rolle: admin und sn_msi.workspace_admin

Hinweis:
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

Prozedur

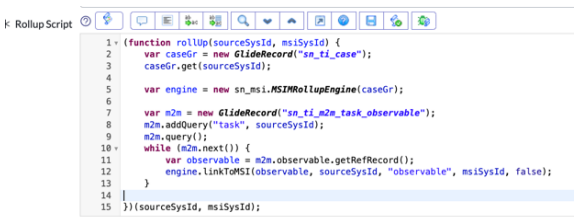
1. Suchen Sie mithilfe der linken Navigation nach Konfigurationen für verknüpfte Datensätze.
2. Navigieren zu **MSI-Administration** > **Konfiguration verknüpfter Datensätze**.
3. Öffnen Sie den Konfigurationsdatensatz, der für einen Sicherheitsfall erstellt wurde.
4. Die Konfiguration des Rollup-Datensatzes wird im Abschnitt „Zugehörige Liste“ angezeigt.
5. Klicken Sie auf **Neu**, um eine neue Rollup-Datensatzkonfiguration zu erstellen.

Nachfolgend finden Sie einen Beispieldatensatz, der für ein Rollup von Daten erkennbarer Elemente im Zusammenhang mit dem Sicherheitsfall erstellt wurde, für den ein Rollup mit den Feldwerten durchgeführt wird:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Rollup-Typ	Beziehung **Hinweis:** Die Informationen des erkennbaren Elements sind in einem zugehörigen Listenformat verfügbar.

Rollup-Skript	Eingabe „sourceSysId“ enthält die Sys-ID des Sicherheitsfalls, und „msiSysId“ enthält die Sys-ID des schwerwiegenden Security Incidents.
	
	 
	Rollup Script
	1 (function rollUp(sourceSysId, msiSysId) {
	2 var caseGr = new GlideRecord("sn_ti_case");
	3 caseGr.get(sourceSysId);
	4
	5 var engine = new sn_msi.MSIMRollupEngine(caseGr);
	6
	7 var m2m = new GlideRecord("sn_ti_m2m_task_observable");
	8 m2m.addQuery("task", sourceSysId);
	9 m2m.query();
	10 while (m2m.next()) {
	11 var observable = m2m.observable.getRefRecord();
	12 engine.linkToMSI(observable, sourceSysId, "observable", msiSysId, false);
	13 }
	14
	15 })(sourceSysId, msiSysId);
	
	○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table.
	
	○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case.
	
	○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method:
	
	`MSIMRollupEngine.linkToMSI("entityGr","sourceSy`

Atomic Rollup bei Bedarf durchführen

Das Rollup-Framework kann keine Aktualisierungen der vorhandenen verknüpften Datensätze verarbeiten. In solchen Fällen sollte ein atomares Rollup für verknüpfte Datensätze bei Bedarf erfolgen, was über Business-Regeln erreicht werden kann.

Um Aktualisierungen der verknüpften Datensätze zu erfassen, müssen in der Quelltabelle Geschäftsregeln erstellt werden.

Diese Business-Regeln gelten für Einfüge-, Aktualisierungs- und Löschvorgänge. Wenn Sie eine Einfügung oder Aktualisierung durchführen, müssen Sie Rollup-Informationen zu MSIhinzufügen oder aktualisieren. Wenn Sie löschen, werden die aufgerollten Informationen aus MSIentfernt.

Beispiel: Sobald ein Security Incident mit MSIverknüpft ist, werden die zugehörigen Informationen automatisch zusammengefasst MSI. Wenn Sie jedoch später ein neues erkennbares Element zu einem MSIhinzufügen, wird auch für das neu hinzugefügte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erkennbare Element ein Rollup zu MSIdurchgeführt. Hier erfasst die Business-Regel **„Rollup für erkennbares Element synchronisieren“** die Aktualisierung und führt ein Rollup des aktualisierten Datensatzes zu MSIdurch. In ähnlicher Weise handhabt dieselbe Geschäftsregel auch die Entfernung der vorhandenen aufgerollten erkennbaren Elemente, wenn sie aus dem Security Incident entfernt werden.

Vordefinierte Geschäftsregeln

Im Folgenden finden Sie einige vordefinierte Geschäftsregeln, die Ihnen dabei helfen, den Umgang mit atomaren Rollups zu verstehen

Regel	Beschreibung
Rollup-Indikator für Synchronisierung (sn_ti_m2m_task_indicator)	Verwenden Sie diese Business Rule, um das Rollup und die Entfernung des Kompromittierungsindikators aus einem Security Incident, einem Sicherheitsfall und einer Korrekturaufgabe zu verarbeiten.
Rollup für erkennbares Element synchronisieren (sn_ti_m2m_task_observable)	Mit dieser Business-Regel werden das Rollup und die Entfernung verknüpfter erkennbarer Elemente aus Security Incidents, Sicherheitsfällen und Korrekturaufgaben verarbeitet.
Rollup des betroffenen Anwenders synchronisieren (sn_si_m2m_task_affected_user)	Mit dieser Business-Regel werden das Rollup und die Entfernung verknüpfter betroffener Anwender aus Security Incidents, Sicherheitsfällen und Korrekturaufgaben verarbeitet.
Rollup der betroffenen CI synchronisieren (task_ci)	Mit dieser Business-Regel werden das Rollup und die Entfernung zugehöriger Konfigurationselemente aus Security Incidents, Sicherheitsfällen und Korrekturaufgaben verarbeitet.

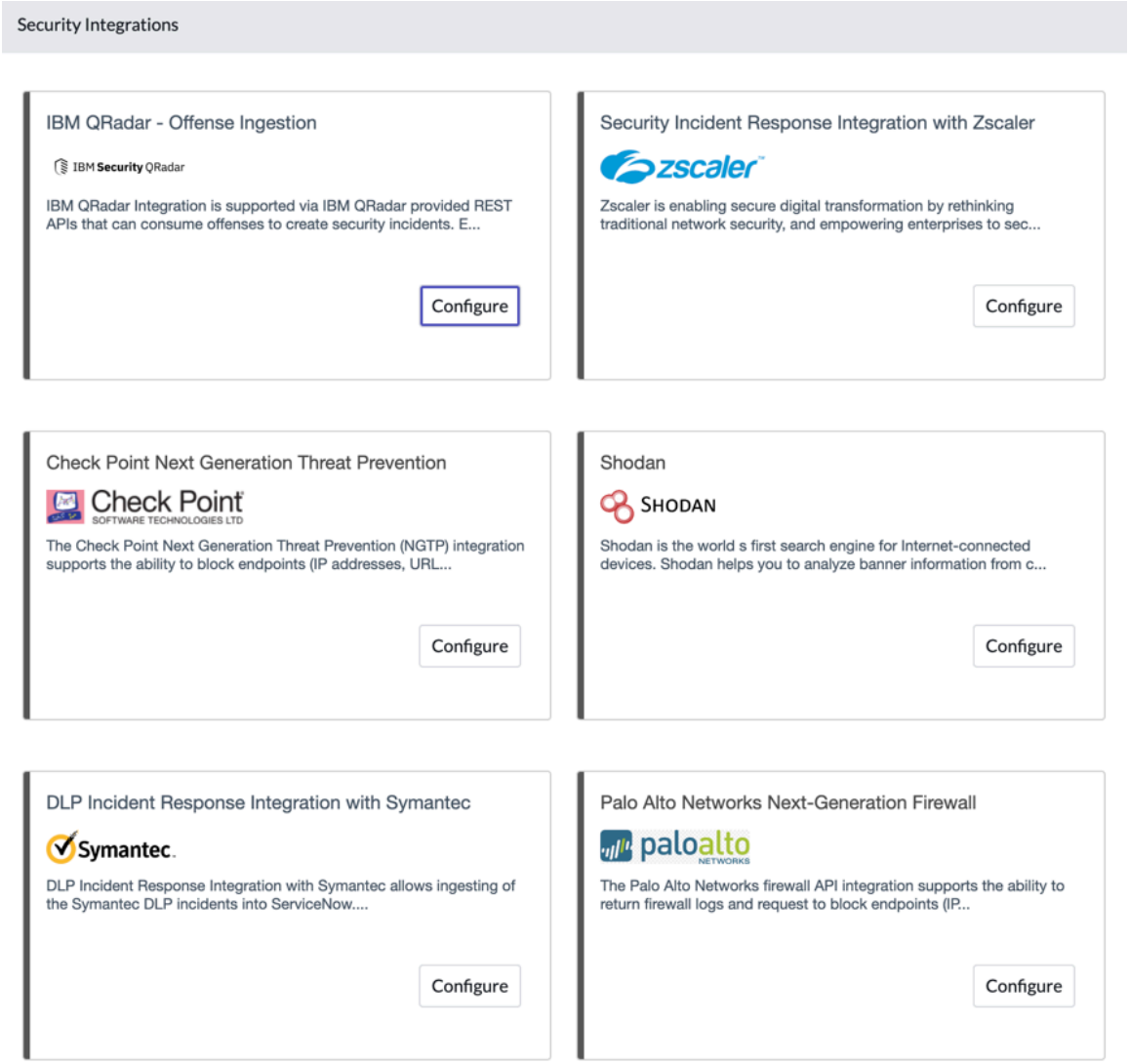
Security Incident Response-Integrationen

Alle Security Operations -Core-Anwendungen und Nicht-Core-Drittparteiintegrationen sind über den ServiceNow Storeverfügbar. Dieser Abschnitt enthält Anweisungen zum Aktivieren der Integrationen und zum Konfigurieren von ServiceNow und Drittanbieterintegrationen. Außerdem enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten im Basissystem enthaltenen Integrationen.

Integrationskonfigurationen

Das Basissystem enthält eine Reihe von „Karten“ für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von Plugins Security Operations aufweisen. Die Integrationskarten können durch Auswahl von angezeigt werden **Security Operations** > **Integrationskonfigurationen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die sichtbaren Integrationen mithilfe des Dropdown-Menüs **Kategorie** filtern. Im Dropdown-Menü **Konfigurationen anzeigen** werden mehrere Instanzen von Implementierungen angezeigt, die deren Erstellung ermöglichen.

Schaltflächen auf Integrationskarten

Je nach Status der Integration und Quelle der Karte werden auf Integrationskarten unterschiedliche Schaltflächen angezeigt.

Schaltfläche	Beschreibung
Plugin installieren	Klicken Sie auf diese Schaltfläche, um das entsprechende Plugin zu installieren und die Integration zu aktivieren. Nachdem das Plugin installiert ist, ändert sich die Schaltfläche in **Konfigurieren**.
Konfigurieren	Klicken Sie auf diese Schaltfläche, um Informationen zum Konfigurieren der Integration einzugeben. Für einige Integrationen müssen Sie möglicherweise API-Schlüssel oder URLs eingeben, die Sie auf der Website der Drittanbieterintegration erworben haben.
Neu	Bei bestimmten Integrationen (z. B. Carbon Black und IBM QRadar) können Sie mehrere Implementierungen derselben Integration definieren. Klicken Sie bei diesen Integrationen auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schaltfläche	Beschreibung
	Neu, nachdem das Plugin aktiviert wurde. Mit den Karten können Sie Plugins installieren (falls zutreffend) und die zu verwendenden Implementierungen konfigurieren.
Seite öffnen	Im Basissystem führt Ihre Instanz von eine Abfrage an den ServiceNow Store für alle Anwendungen durch, die von den Plugins Security Operations abhängig sind. Wenn diese Anwendungen gefunden wurden und die zugehörigen Anwendungs-Plugins aktiviert sind, werden Integrationskarten für sie zusammen mit den anderen Sicherheitsintegrationskarten angezeigt. Klicken Sie **auf Seite öffnen**, um auf die Website der Drittanbieteranwendung zuzugreifen und die Integration zu konfigurieren. Nachdem Sie die Konfiguration abgeschlossen haben, ändert sich die Schaltfläche **Seite öffnen** in **Konfigurieren**.

ArcSight ESM Ereigniserfassung für Security Operations Integration

Die Integration der ArcSight ESM -Ereigniserfassung mit dem Produkt Security Incident Response ermöglicht es Security Incident-Analysten, korrelierte Ereignisse zu sammeln und die Erstellung von Security Incidents mit der Plattform ServiceNow zu automatisieren. Daten werden kontinuierlich basierend auf einem konfigurierten Abfragezeitplan erfasst und von Analysten verwendet, um potenzielle Cybersicherheitsbedrohungen zu identifizieren und darauf zu reagieren.

Mit dieser Integration können korrelierte Ereignisse, die Kandidaten für Security Incidents sind, regelmäßig erfasst werden. Sie können Felder in korrelierten Ereignissen zu Security Incident-Feldern zuordnen, eine Vorschau der Einrichtung eines Ereignisses als Security Incident anzeigen und die geplante Erfassung von Ereignissen einrichten, um automatisch laufend Security Incidents zu erstellen.

Übersicht

Diese Integration bietet einem SOC-Analysten (Security Operations Center) Einblick in die Korrelation von Ereignissen in ArcSight ESM. Diese Daten können zur weiteren Untersuchung und Behebung in Security Incidents Now Platform von Security Incident Response (SIR) integriert werden. In Ihrer Instanz Now Platform werden Profile erstellt, um verschiedene Typen von Korrelationsereignissen zu verarbeiten, die über Korrelationsabfrage-Viewers in ArcSight ESMerstellt und verfügbar gemacht werden. Diese Profile passen an, wie verschiedene ArcSight ESM Felder für korrelierte Ereignisse in SIR-Security Incidents angezeigt werden.

Schlüsselfunktionen

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Erstellen Sie mehrere Ereigniserfassungsprofile, um SIR Security Incidents für bestimmte Arten von Bedrohungen wie Malware und nicht autorisierte Zugriffsversuche zu erstellen.
- Drag-and-Drop-Zuordnung von ArcSight ESM -Werten des Korrelationsereignisfeldes zu zugehörigen SIR -Security-Incident-Feldern.
- Eine Vorschau des Security Incident-Layouts SIR basierend auf Beispielkorrelationsereignissen, um die Details der Ereigniszuordnung zu validieren.
- Erfassung historischer Korrelationsereignisse sowie neuer beachtenswerter Ereignisse in konfigurierbaren Intervallen.
- Filtern Sie Korrelationsereignisse heraus, die die Kriterien für die SIR Incident-Generierung nicht erfüllen, z. B. Ereignisse mit niedriger Priorität

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fassen Sie Ereignisse basierend auf übereinstimmenden Feldwerten für vorhandene SIR Security Incidents zusammen, um doppelte Security Incidents zu vermeiden.
- Aktualisieren Sie Korrelationsereignisse basierend auf SIR Bedingungen für die Incident-Erstellung und/oder -Abschluss über eine bidirektionale Schnittstelle.

Unterstützte Versionen Now Platform.

Diese Integration unterstützt die Releases New York Patch 6 und Orlando Now Platform.

Die folgenden Security Operations-Anwendungen müssen über ServiceNow Storeinstalliert und aktiviert werden. Installieren Sie eine Anwendung nach der anderen in der unten aufgeführten Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response
4. Event and Alert Ingestion for Security Operations
5. Integration Hub-Plugins
   a. ServiceNow Integration Hub Runtime
   b. Aktionsschritt für ServiceNow Integration Hub – REST

Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

ArcSight ESM unterstützte Versionen

Diese Integration wurde mit Version 7.0.0.2436 des ArcSight ESM Managers getestet. Die -Integration unterstützt sowohl lokale ArcSight ESM als auch Cloud-/gehostete Serviceumgebungen.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrer Instanz Now Platform®, um eine Verbindung zum Service ArcSight ESM herzustellen, wenn der Server ArcSight ESM innerhalb Ihres Unternehmensnetzwerks bereitgestellt wird. Wenn Sie den Cloud-Service ArcSight ESM verwenden, ist kein MID-Server erforderlich. Weitere Informationen zu MID-Servern finden Sie auf der Website der ServiceNow-Produktdokumentation .

Referenzen

Referenz	Dokumentbezeichner	Dokumententitel
1	ArcSight ESM Produktdokumentation	ArcSight-Produktdokumentation .
2	ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Ihre Instanz Now Platform® für die Integration der Ereigniserfassung ArcSight ESM ein

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in der Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung von ServiceNow Storeinstallieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Sehen Sie sich die folgende Tabelle an, und vergewissern Sie sich, dass Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben.	Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Instanz Now Platform® von erforderlich. • Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Ein Benutzer mit der Rolle sn_si.admin überwacht die folgenden Aufgaben in Now Platform®: ◦ Benennt, erstellt und bearbeitet Ereignisprofile. ◦ Wählt Werte aus ArcSight ESM Korrelationsereignissen aus und ordnet sie Security Incidents zu. ◦ Zeigt eine Vorschau der Details von Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird. ◦ Plant die laufende Erfassung korrelierter Ereignisse. ◦ Aktiviert die Aktualisierung korrelierter Ereignisse, wenn ein SIR-Incident erstellt und geschlossen wird. ◦ Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu. ◦ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Rollen auf der Website der ServiceNow-Produktdokumentation .
Stellen Sie sicher, dass Sie Version 7.0.0.2436 oder höher des ArcSight ESM Managers verwenden. Frühere Versionen werden nicht unterstützt.	Wenn Sie Zugriff auf den Abfrage-Viewer ArcSight ESM haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Richten Sie den Abfrage-Viewer in ArcSight ESMein.	Bevor Sie Korrelationsereignisse erfassen können, müssen Sie den Abfrage-Viewer in der Konsole ArcSight ESM konfigurieren. Details siehe Richten Sie den Abfrage-Viewer ArcSight ESM ein.
Optional Erstellen Sie anwenderdefinierte Phasen in ArcSight ESM für Aktualisierungen von Korrelationsereignissen.	Ein Korrelationsereignis durchläuft viele Phasen in seinem Lebenszyklus, bevor es geschlossen wird. ArcSight ESM bietet Standardphasen wie „Anfänglich“, „Überwachung“, „In Warteschlange“ und „Geschlossen“. Einige dieser Phasen erfordern Benutzereingaben, andere werden jedoch automatisch ohne Benutzereingriff auf das Ereignis angewendet (das Feld **Vom Anwender erforderlich** ist in der Konsole ArcSight ESM deaktiviert). Sie können anwenderdefinierte Phasen erstellen, für die keine Benutzereingriffe erforderlich sind, und sie in Ihrer Instanz Now Platform® verwenden. Details siehe Zusätzliche Optionen: Automatisieren Sie die Aktualisierung und den Abschluss korrelierter Ereignisse basierend auf dem Incident-Status SIR ..
Stellen Sie sicher, dass Sie eine MID-Serveranwendung installiert und konfiguriert haben.	Konfigurierte MID-Server-Anwendung Ein MID-Server in Ihrer Instanz Now Platform® ist erforderlich, um eine Verbindung zum Service ArcSight ESM herzustellen, wenn der Server ArcSight ESM innerhalb Ihres Unternehmensnetzwerks bereitgestellt wird. Anweisungen zum Konfigurieren einer MID-Server-Anwendung finden Sie unter Installieren und konfigurieren Sie die ServiceNow-Anwendung für die ArcSight ESM Event Ingestion-Integration. Informationen zu MID-Servern finden Sie unter MID-Server. Wenn Sie einen gehosteten oder Cloud-Service verwenden, der über das Internet zugänglich ist, ist ein MID Server nicht erforderlich.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Event and Alert Ingestion for Security Operations: Diese Anwendung benötigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST **5.** Threat Core Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Nächste Maßnahme

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht in der Installation der Anwendung ArcSight ESM Security Event Ingestion for Security Operations aus dem ServiceNow Store für die -Integration.

Richten Sie den Abfrage-Viewer ArcSight ESM ein

Erstellen Sie einen Abfrage-Viewer, und definieren Sie Filter, die kürzlich erstellte Korrelationsereignisse enthalten, die erfasst werden ServiceNow.

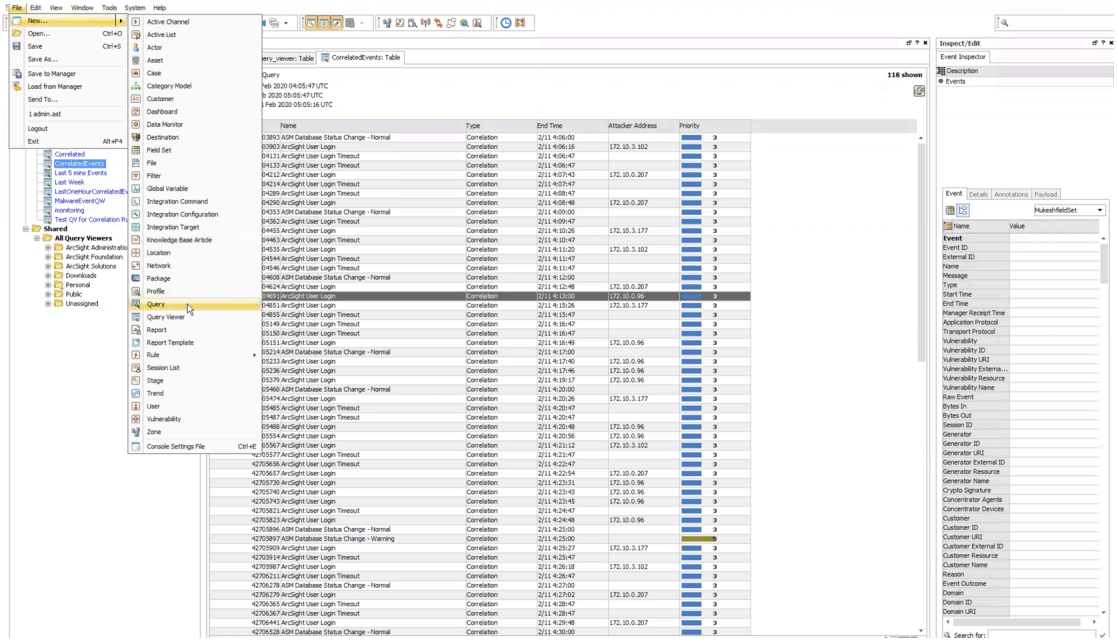
Vorbereitungen

Erforderliche Rolle: ArcSight-Administrator

Prozedur

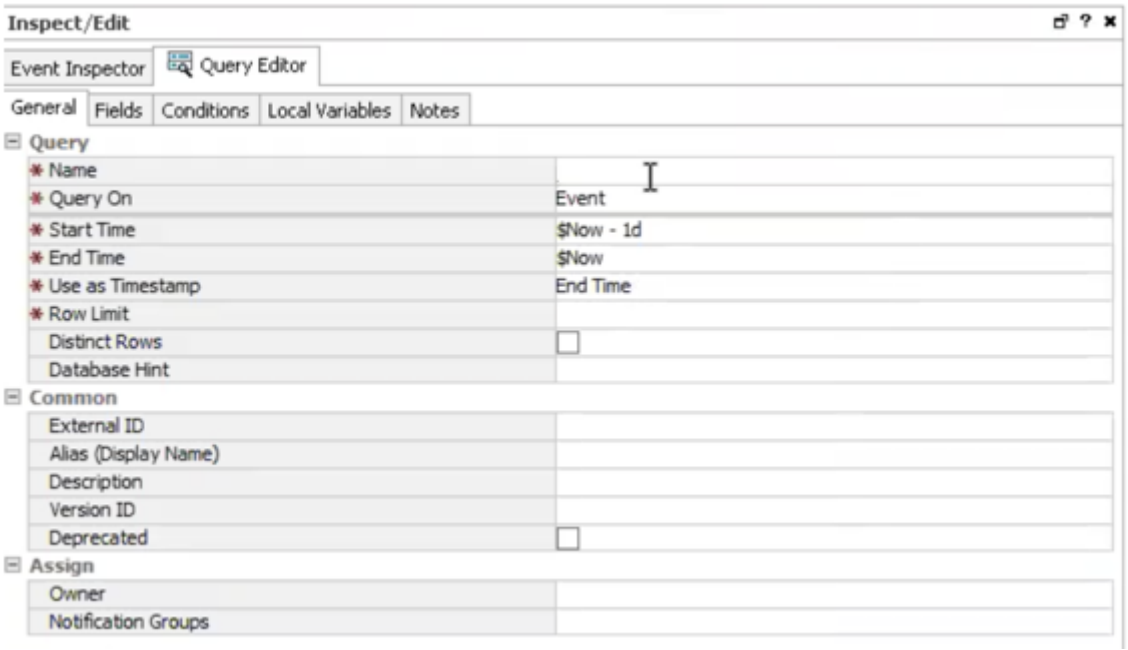
1. Melden Sie sich bei der -Konsole ArcSight ESM an, um einen Abfrage-Viewer zu erstellen.

2. Um eine neue Abfrage zu erstellen, navigieren Sie zu **Datei** > **Neu** > **Abfrage**.



3. Definieren Sie Bedingungen für den Abfrage-Viewer im Bereich **„Untersuchen/Bearbeiten“**.

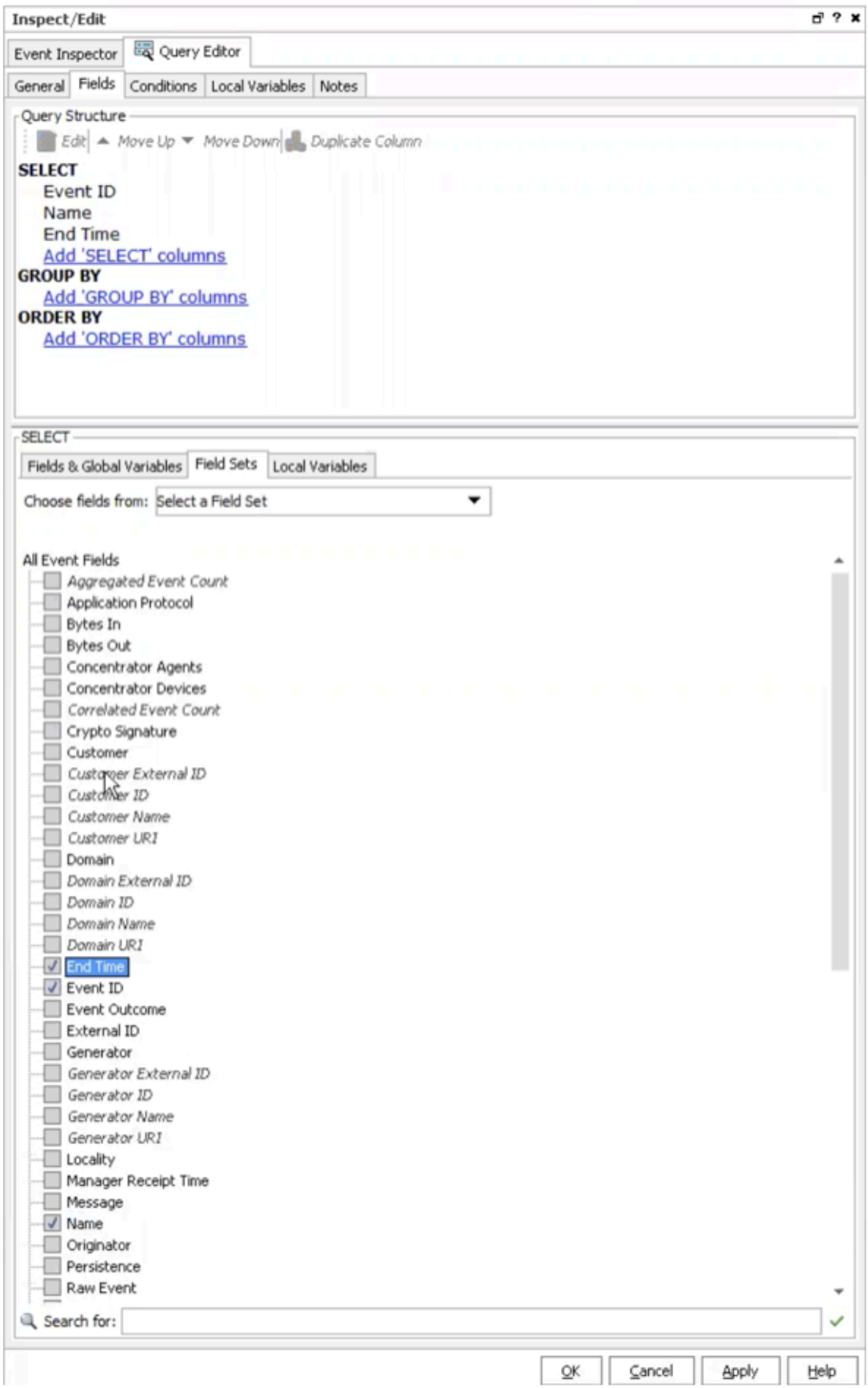
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf die Registerkarte **Felder**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

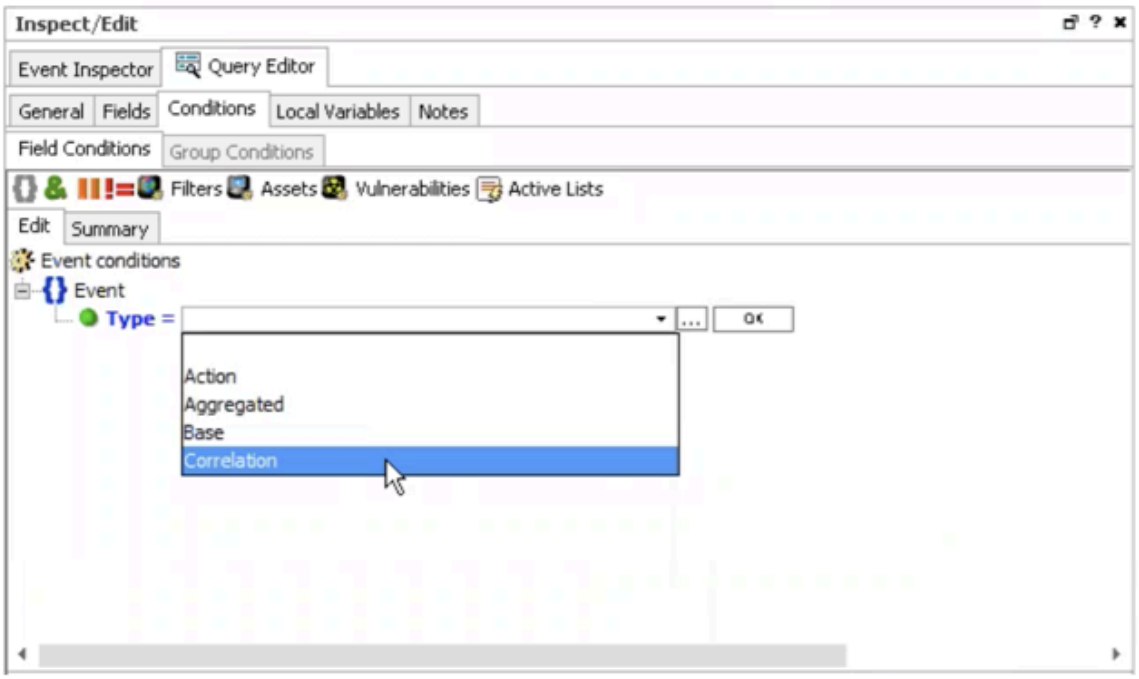


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

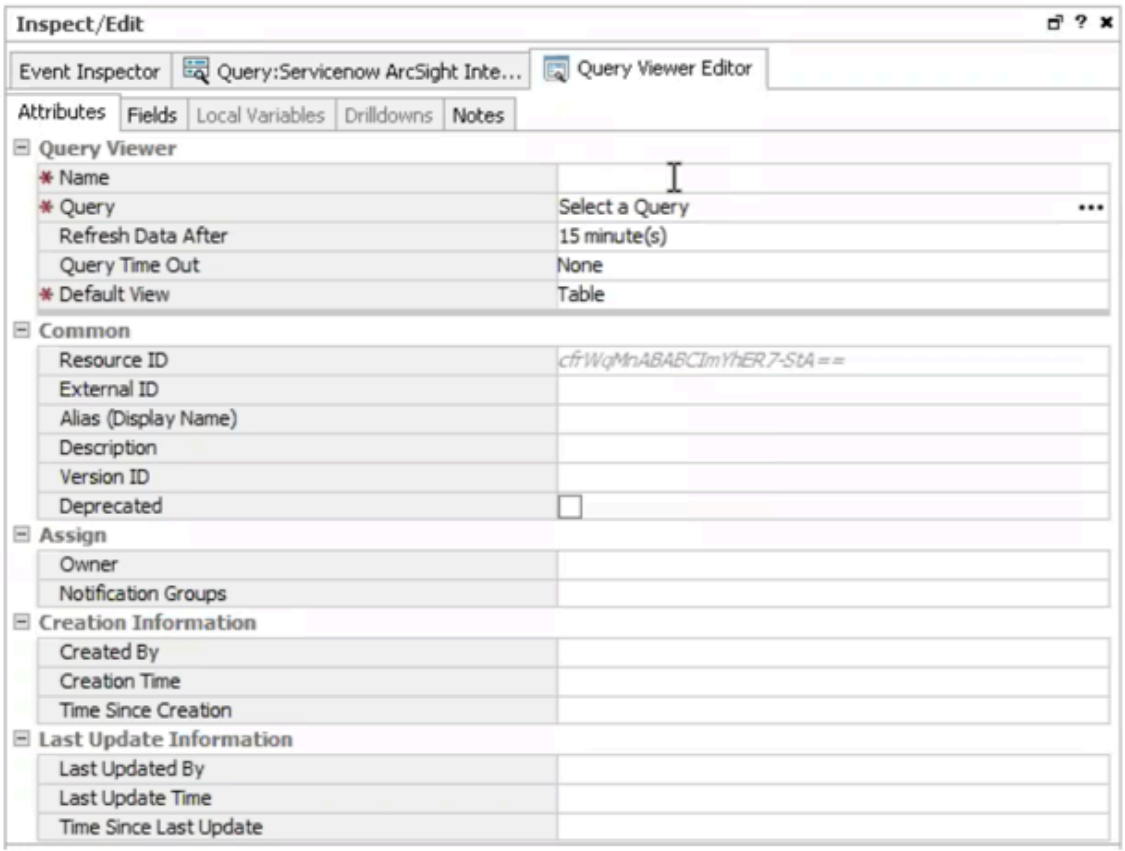
5. Wählen Sie die Felder aus, die bei der Erfassung einbezogen werden müssen.
   Sie müssen die Felder *Ereignis-ID*, *Name*und *Endzeit* auswählen, damit die Erfassung erfolgreich ist.
6. Klicken Sie auf den Link **„SORTIEREN NACH"-Spalten hinzufügen**, wählen Sie das Feld **Ereignis-ID** aus, und geben Sie **Absteigend** als Sortierreihenfolge an, um sicherzustellen, dass die neuesten Ereignisse erfasst werden.
7. Klicken Sie auf die Registerkarte **Bedingungen**.
8. Klicken Sie mit der rechten Maustaste auf **Ereignis** unter **Ereignisbedingungen** im Abschnitt **Zusammenfassung**.
9. Klicken **Neue Bedingung** > **Stamm** > **Typ** und wählen Sie als Ereignistyp **Korrelation**aus.

Wichtig:
Nur Korrelationsereignisse werden abgerufen. Basisereignisse für Korrelationen werden nicht abgerufen.



10. Klicken Sie auf **OK**, um die Abfrage zu speichern.
    Der nächste Schritt besteht darin, einen Abfrage-Viewer für diese Abfrage zu erstellen.
11. Navigieren zu **Datei** > **Neu** > **Abfrage-Viewer**.

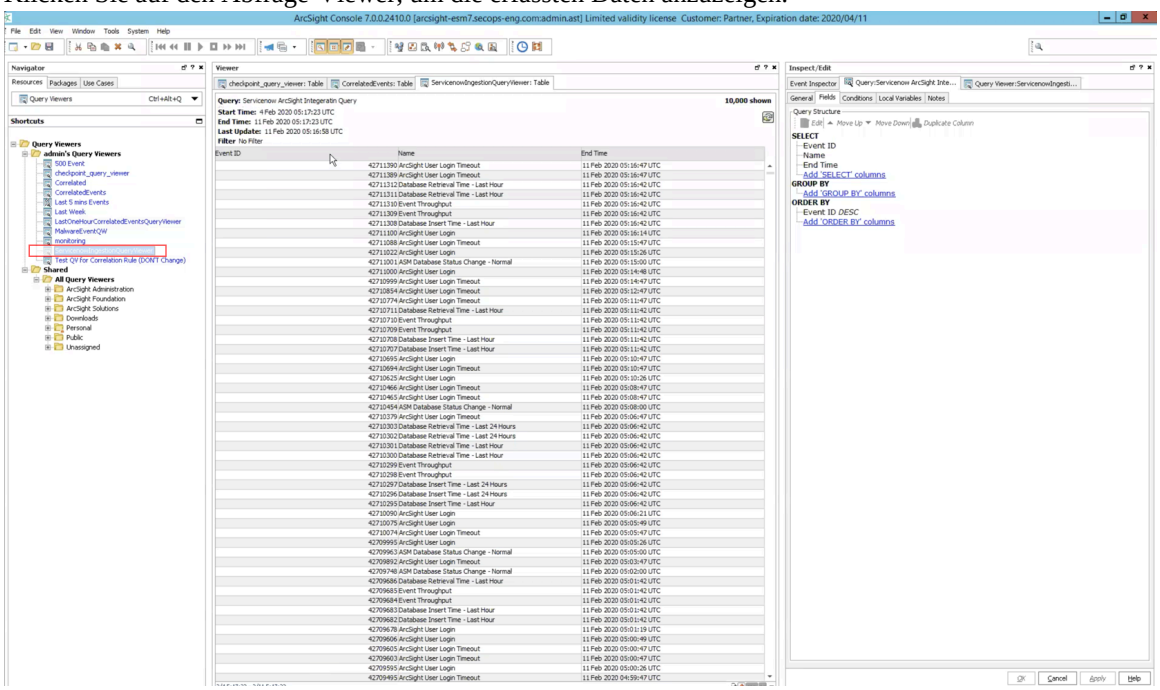
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



12. Klicken Sie auf die Registerkarte **Felder**, und vergewissern Sie sich, dass die in der Abfrage angegebenen Pflichtfelder (`Ereignis-ID, Name, Endzeit`) ausgewählt sind.

13. Klicken Sie **auf Übernehmen**, um den Abfrage-Viewer zu speichern.
Der von Ihnen neu erstellte Abfrage-Viewer wird im Abschnitt „Query Viewers“ (Abfrage-Viewers) aufgeführt.

14. Klicken Sie auf den Abfrage-Viewer, um die erfassten Daten anzuzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie die ServiceNow-Anwendung für die ArcSight ESM Event Ingestion-Integration

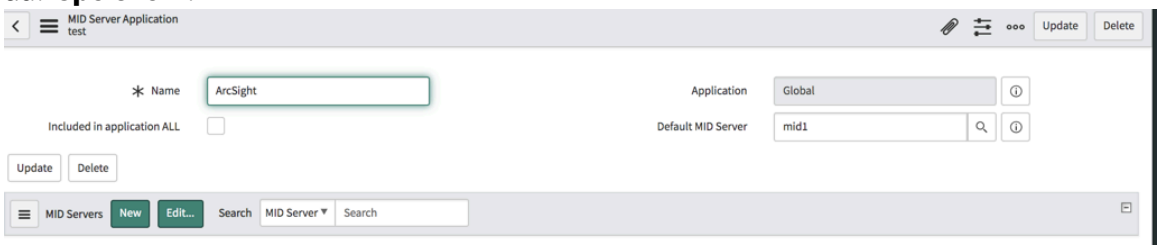
Bevor Sie die -Integration in Ihrer Instanz Now Platform® ausführen, führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in die -Produkte Security Incident Response und Security Operations in Ihrer Instanz Now Platform integriert werden kann.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn Sie die Anwendung ArcSight ESM für die Integration nicht aus ServiceNow Store installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel ArcSight ESM.
3. Klicken Sie zum Konfigurieren der Anwendung auf **Neu**.
4. Alternativ: Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, können Sie darauf klicken, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie die Felder des Formulars aus.
   Um eine neue MID-Server-Anwendung zu erstellen, gehen Sie wie folgt vor:
   a. Navigieren zu **MID-Server** > **Anwendungen** und klicken Sie auf **Neu**.
   b. Geben Sie einen Namen für die MID-Server-Anwendung ein, und wählen Sie einen MID-Server aus, der als Standard verwendet werden soll.
   c. Deaktivieren Sie das Kontrollkästchen In Anwendung ALLE enthalten, und klicken Sie auf **Speichern**.

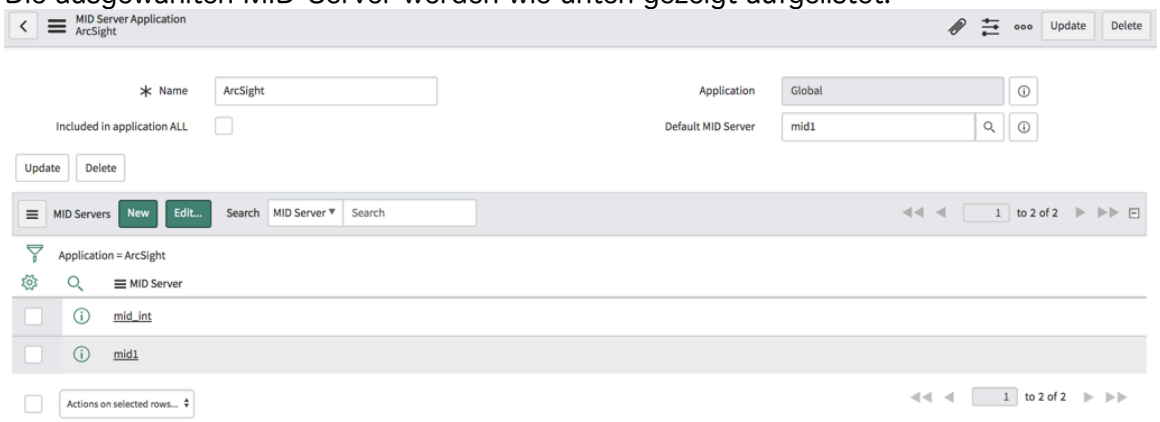


   d. Klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **„Mitglieder bearbeiten“** alle verfügbaren MID-Server aus, verschieben Sie sie in die Liste der MID-Server, und klicken Sie auf **Speichern**.

Automatische Übersetzung

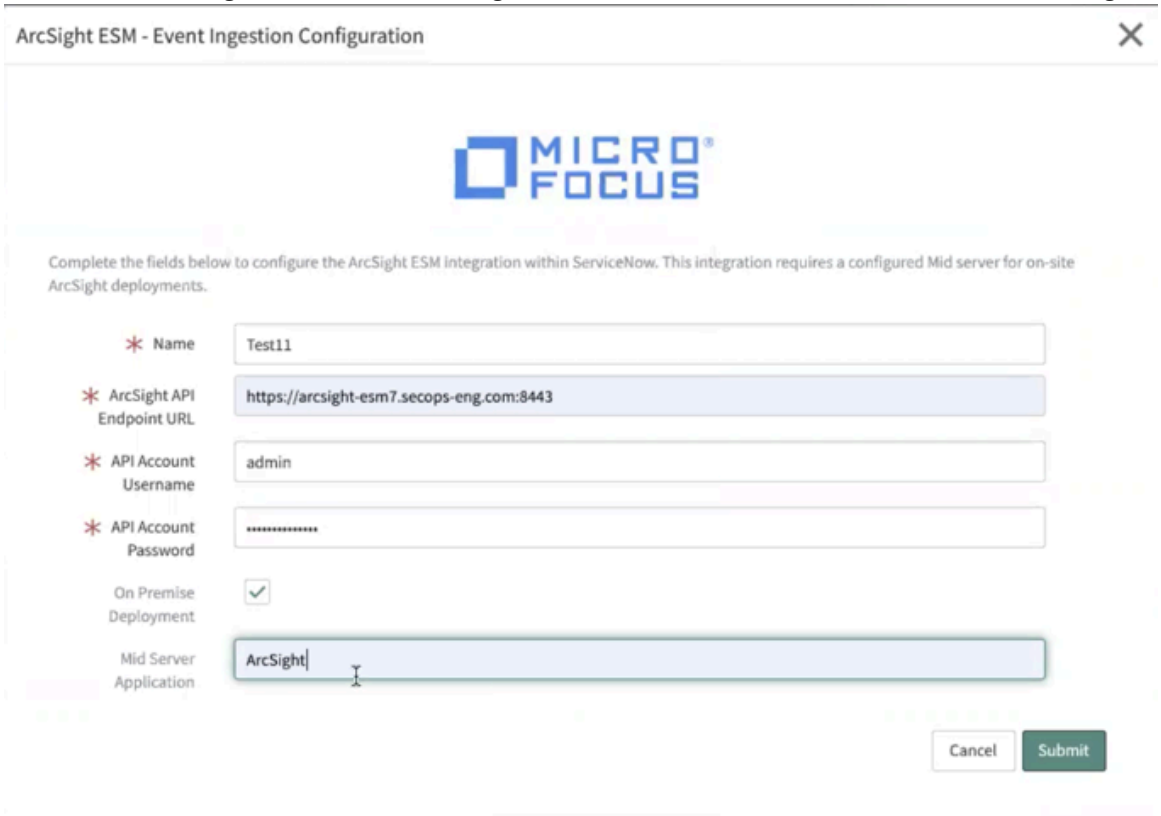
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Die ausgewählten MID-Server werden wie unten gezeigt aufgelistet.



Je nach Verfügbarkeit wird einer der mit der MID Server-Anwendung konfigurierten MID Server verwendet.

6. Geben Sie die Konfigurationsdetails ein, und geben Sie die von Ihnen erstellte MID-Server-Anwendung an.



Jedes Korrelationsereignis, das Sie über Ihre ArcSight ESM Manager-Konsole erfassen, erfordert ein eindeutiges Ereignisprofil in Ihrer Instanz. Die Quelle ArcSight ESM, die Sie im Formular „Konfiguration der Ereigniserfassung“ konfigurieren, kann jedoch für mehrere Profile wiederverwendet werden, solange jedes Profil eindeutige Korrelationsereignistypen erfasst.

7. Klicken Sie auf **Absenden**.
Nach erfolgreicher Validierung und Übermittlung wird jede ArcSight ESM -Serverkonfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite mit den Sicherheitsintegrationen angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.

Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht im Erstellen eines Ereignisprofils.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Profil für die Integration der Korrelationsereigniserfassung ArcSight ESM .

Als Benutzer mit der Rolle sn_si.admin erstellen Sie ein Profil in Ihrer Instanz Now Platform und bestimmen, welche Korrelationsereignisse Security Incidents verursachen. Bevor Security Incidents Now Platform Security Incident Response (SIR) aus Korrelationsereignissen erstellt werden, werden die Feldwerte aus Ereignissen in einem Layout eines Now Platform -Security Incidents angezeigt, sodass Sie eine Vorschau auf die Erstellung des tatsächlichen Security Incidents anzeigen können.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Korrelationsereignisse werden je nach definiertem Profiltyp automatisch in der Umgebung Security Operations Ihrer Instanz Now Platform erfasst. Ein Profil ist eine Kapselung einer Art von Korrelationsereignis wie nicht autorisierter Zugriffsversuche oder Malware.

Nachdem ein Korrelationsereignis erfasst wurde, können Sie einzelne Korrelationsereignisfelder den entsprechenden Feldern im Security Incident zuordnen. Sie können Korrelationsereignisse filtern, um anzugeben, welche Ereignisse Security Incidents erstellen. Beispielsweise können Sie Filter bevorzugen, die Security Incidents nur für Korrelationsereignisse erstellen, die als hoch riskant identifiziert wurden. Sie können auch zusätzliche Kriterien für die Zusammenfassung von Ereignissen definieren, sodass eingehende doppelte Korrelationsereignisse zu einem offenen Security Incident zusammengefasst werden. Schließlich können Sie einen Aufnahmezeitplan definieren und das Profil aktivieren.

Namen für die Ereignisprofile in Ihrer Instanz Now Platform müssen eindeutig sein und können jeweils nur einem aktiven Ereignisprofil zugeordnet werden.

Erstellen und benennen Sie das Profil für die ArcSight ESM Integration zur Ereigniserfassung

Sie können ein Profil einrichten, um Korrelationsereignisse zu erfassen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

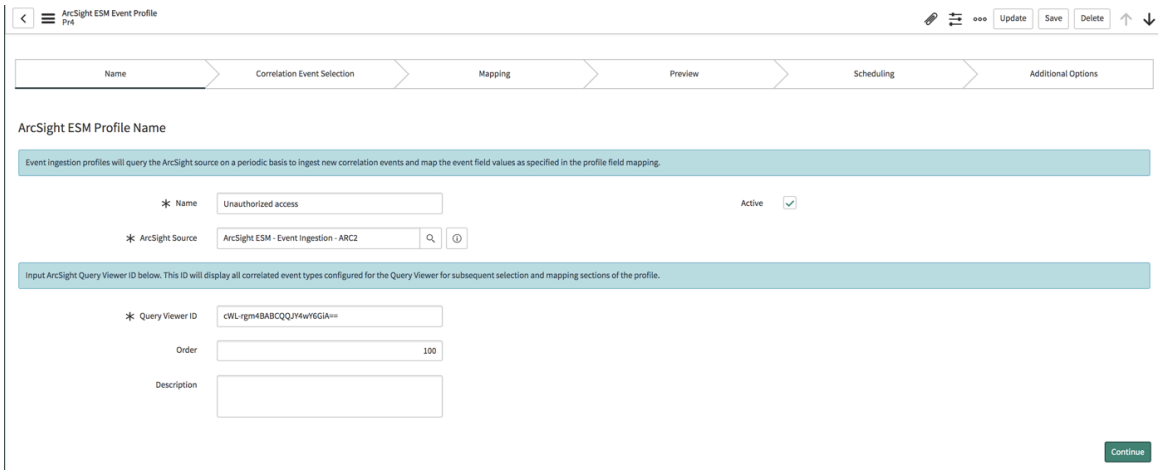
Prozedur

1. Um ein Ereignisprofil für ein Korrelationsereignis in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **ArcSight ESM Integration** > **ArcSight ESM Ereignisprofil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

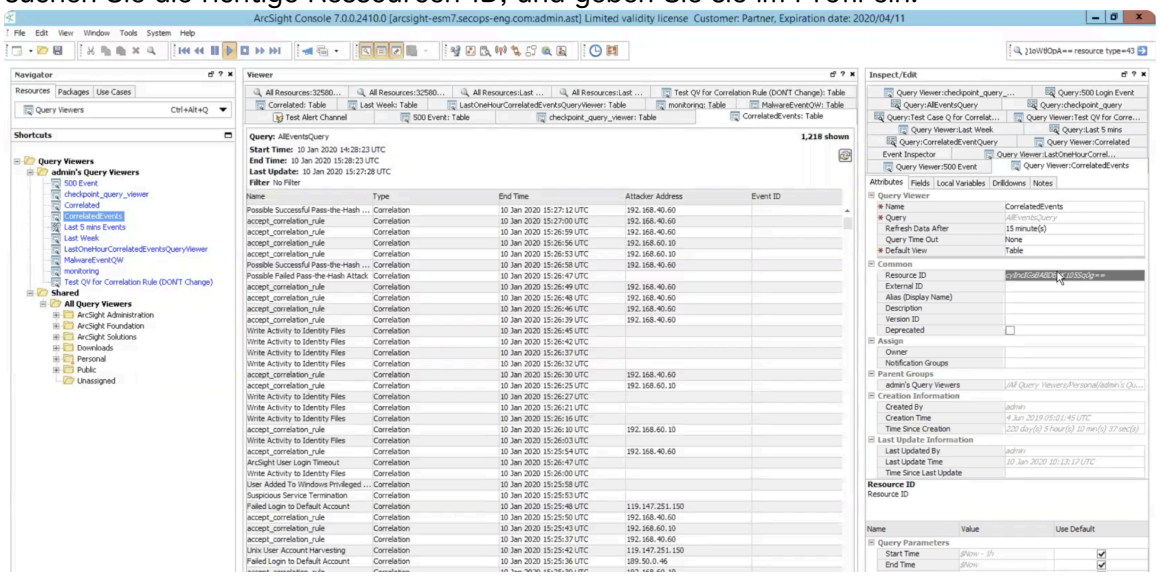
   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem Sie die Profildetails eingegeben haben, klicken Sie auf **Fortsetzen**. Die ID des Abfrage-Viewers wird validiert. Wenn im Abfrage-Viewer ArcSight ESM eine entsprechende Ressourcen-ID vorhanden ist, wird der Name des Abfrage-Viewers wie unten gezeigt zurückgegeben. Wenn die Validierung fehlschlägt, überprüfen Sie, ob die Ressourcen-ID in der -Konsole ArcSight ESM vorhanden ist. Wenn die Ressourcen-ID nicht gefunden wird, suchen Sie die richtige Ressourcen-ID, und geben Sie sie im Profil ein.



Nächste Maßnahme

Der nächste Schritt besteht in der Auswahl der Korrelationsereignistypen für die Erfassung aus dem Abfrage-Viewer, der im vorherigen Schritt ausgewählt wurde.

Wählen Sie Korrelationsereignisse für die Integration der Ereigniserfassung ArcSight ESM aus

Wählen Sie basierend auf der Quelle ArcSight ESM und dem konfigurierten Abfrage-Viewer eine Korrelationsereignisregel für das Profil aus.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Korrelationsereignisse an, die in der Auswahl der Korrelationsereignisse in Ihrer Now Platform-Instanz aufgeführt sind, damit Sie bestimmen können, welche Korrelationsereignisse Sie erfassen und Security Incidents erstellen möchten. Sie können für jedes Profil nur einen Korrelationsregeltyp aus der Liste auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Abfrage-Viewer-ID und der Abfrage-Viewer-Name werden angezeigt, wie im Formular „Abfrage-Viewer“ angegeben. Wählen Sie ein Korrelationsereignis aus der Liste aus, das Sie verwenden können, um eine Konfigurationszuordnung für das erfasste korrelierte Ereignis zu erstellen.

Klicken Sie auf die Dropdown-Liste im Feld Liste der Korrelationsereignisse. Eine Liste der Korrelationsereignisse, die in der Abfrage-Viewer-Konsole ArcSight ESM vorhanden sind, wird angezeigt.

Klicken Sie auf **„Fortsetzen“**, um mit dem nächsten Schritt im Assistenten fortzufahren.

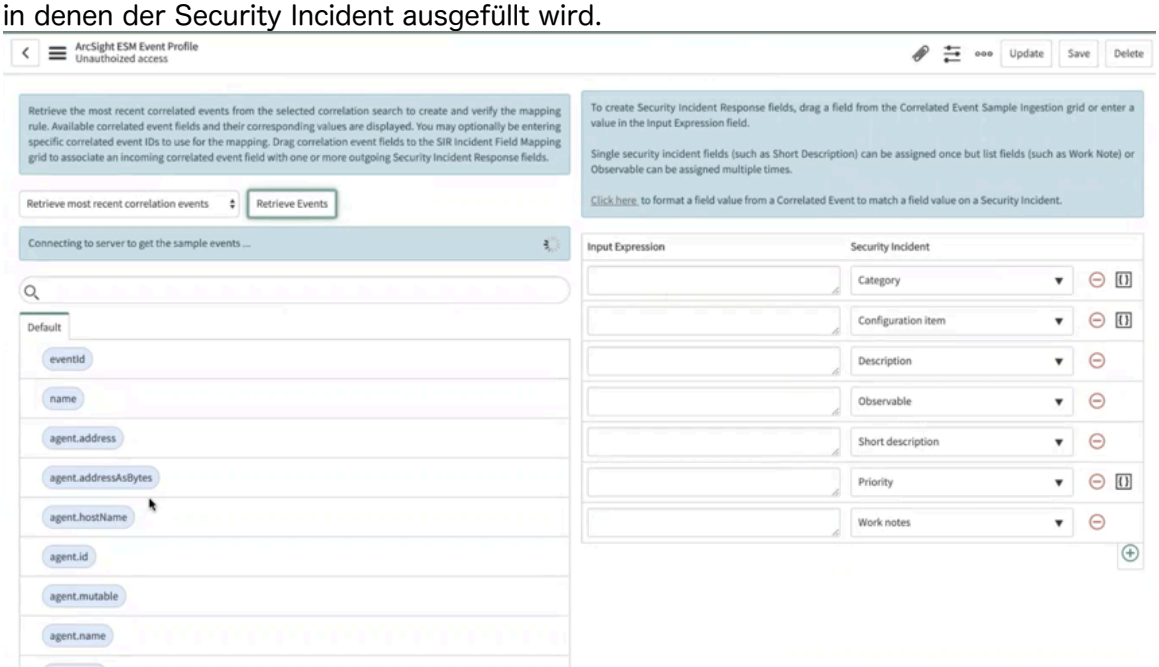
Zuordnung von Korrelationsereignisfeldern für die ArcSight ESM -Ereigniserfassungsintegration

Nachdem Sie die spezifische Korrelationsereignisregel aus der Liste identifiziert haben, besteht der nächste Schritt darin, Korrelationsereignisfelder den Feldern im Formular „Security Incident“ zuzuordnen.

Übersicht

Für den Zuordnungsschritt können Sie Beispiele für Korrelationsereignisse für die ausgewählte Korrelationsregel erfassen. Während dieser Zuordnungsphase können Sie sicherstellen, dass alle relevanten Daten des Korrelationsereignisfeldes an der entsprechenden Stelle im Incident-Formular SIR zugeordnet sind, und dann den Incident SIR im Vorschaubereich visualisieren.

Die folgende Abbildung zeigt die standardmäßige Zuordnungskonfiguration, die zum Erstellen des Korrelationsereignisprofils bereitgestellt wird. Sie können die Felder anpassen, in denen der Security Incident ausgefüllt wird.



Wenn Sie **auf Ereignisse abrufen**klicken, werden die Feldnamen des Korrelationsereignisses und die entsprechenden Werte auf der linken Seite des Formulars ausgefüllt. Dies sind die Korrelationsereignisfelder ArcSight ESM, die für die Zuordnung zu den Feldern für Security Incidents verfügbar sind.

Möglicherweise möchten Sie einige Beispiele für Korrelationsereignisse in Ihrer Konsole überprüfen, um sie für den Konfigurationsschritt der Feldzuordnung zu erfassen. Dieser Schritt wird auf dem Fortschrittsbalken als Zuordnung bezeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**. Sie können bis

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu fünf Beispielekorrelationsereignisse vom Manager ArcSight ESM für die ausgewählte Korrelationsregel erfassen, um den Feldzuordnungsprozess zu unterstützen. Es gibt Optionen, um entweder die fünf neuesten Korrelationsereignisse für das ausgewählte Korrelationsereignis oder bis zu fünf spezifische Korrelationsereignisse basierend auf den Ereignis-IDs zu erfassen.

Nachfolgend finden Sie eine Zusammenfassung der Schritte, die zum Zuordnen von Korrelationsereignissen erforderlich sind:

- Feldzuordnung: Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Korrelationsereignisfelder aus der linken Seite in den Abschnitt SIR Incident-Zuordnung auf der rechten Seite ziehen. Die Zuordnung auf der rechten Seite ordnet das eingehende Korrelationsereignisfeld einem ausgehenden Security Incident-Feld zu.
- Zuordnungs-Experience: Passen Sie das Zuordnungsraster an, indem Sie Felder über das Symbol + unten im Abschnitt „SIR-Incident-Feldzuordnung“ hinzufügen oder entfernen. Verfolgen Sie übersehene oder zuvor zugeordnete Felder mit der angegebenen Farbcodierung (zugeordnete Felder sind ausgegraut, blaue Felder sind nicht zugeordnet).
- Bedingungen für Incident-Generierung: Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen definieren, um zu filtern, welche Korrelationsereignisse Security Incidents erstellen und welche Korrelationsereignisse herausgefiltert werden sollen, z. B. Korrelationsereignisse mit niedriger Priorität. Dies geschieht im Abschnitt „Bedingungen für Incident-Generierung“, der sich unter dem Abschnitt „Beispielerfassung für Korrelationsereignis“ befindet.
- Kriterien für Ereigniszusammenfassung: Definieren Sie zusätzliche Kriterien für Ereigniszusammenfassung, die ein eingehendes Korrelationsereignis zu einem vorhandenen Security Incident SIR zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Daten zu wichtigen Sicherheitsereignissen in einem einzigen Security Incident zusammengefasst werden.
- Formatfeldübersetzung: In bestimmten Fällen werden Ereignisfeldwerte im Korrelationsereignis ArcSight ESM möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten.

  Beispielsweise können mit dem Skript-Editor die Kategoriewerte „Malware-Warnung“ und „Virusinfizierung“ unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mithilfe von in eine gemeinsame böswillige Code-Aktivität im Feld „Kategorie“ des Security Incident SIR übersetzt werden Formatfeldübersetzungsfunktion.

Der nächste Schritt besteht darin, Beispiele für Korrelationsereignisse zu erfassen und Werte den Security Incident-Feldern SIR zuzuordnen.

Erstellen Sie Zuordnungen für die Ereigniserfassungsintegration ArcSight ESM .

In diesem Schritt erfassen Sie Beispiele für Korrelationsereignisse und ordnen Werte den SIR-Security Incident-Feldern zu.

Vorbereitungen
Erforderliche Rolle: admin, sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Als Benutzer mit der Rolle sn_si.admin können Sie bis zu fünf Beispiele für Korrelationsereignisse aus der Spalte „Beispielerfassung für Korrelationsereignis“ auf der linken Seite des Formulars überprüfen, um die Zuordnung und Übersetzung von Ereignisfeldwerten zu den Feldern für Security Incidents im SIR-Incident zu unterstützen Spalte „Feldzuordnung“ auf der rechten Seite.

Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie im Zuordnungsraster auf der rechten Seite des Formulars Felder hinzufügen oder entfernen. Standardmäßig angezeigte Felder sind normalerweise wichtige Felder, die im Formular für die Reaktion auf Security Incidents ausgefüllt werden müssen. Diese Felder können jedoch entfernt und zusätzliche Felder mit den Schaltflächen „+“ und „-“ angezeigt werden. Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie im Zuordnungsraster auf der rechten Seite des Formulars Felder hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie ArcSight ESM -Felder zuordnen, die nicht im Standardzuordnungsraster für den Security Incident angezeigt werden.

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
2. Sie können entweder die neuesten Beispielkorrelationsereignisse für die ausgewählte Korrelationsregel abrufen oder die eindeutigen Korrelationsereignis-IDs für die spezifischen Korrelationsereignisse angeben, die Sie für Ihre Korrelationsereignis-Zuordnungs-Experience verwenden möchten.
3. Wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus:
   - Ruft die neuesten Korrelationsereignisse ab
   - Wählen Sie Korrelationsereignisse basierend auf der Ereignis-ID aus

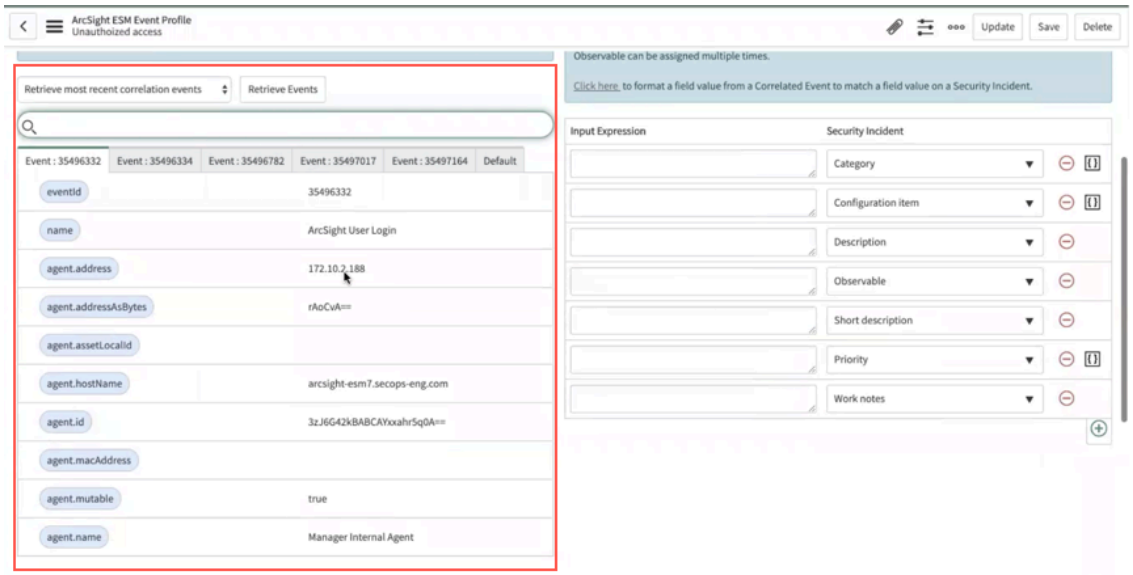
   Klicken Sie **auf Ereignisse abrufen**, um die neuesten Beispielkorrelationsereignisse für die ausgewählte Korrelationssuchregel aus der Konsole ArcSight ESM abzurufen.

   Die Felder für das Korrelationsereignis und die Werteergebnisse werden als einzelne Registerkarten angezeigt.

   Das Abrufen von Beispielkorrelationsereignissen kann einige Minuten dauern. Oben auf dem Bildschirm wird eine Meldung angezeigt, dass die Transaktion funktioniert.

   In der folgenden Abbildung werden auf der linken Seite dieses Formulars die Feld-Name-Wert-Paare für das erfasste Korrelationsereignis oder die importierten Beispielereignisse angezeigt, nachdem der Erfassungsabruf abgeschlossen wurde. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

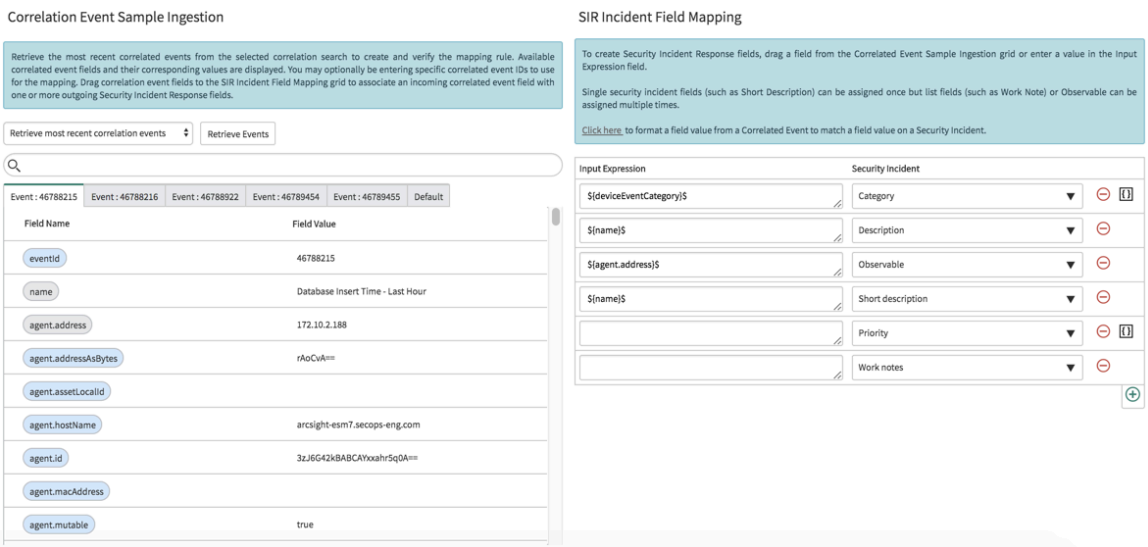
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf einen blauen Feldnamen auf der linken Seite des Formulars.
5. Ziehen Sie den Feldnamen, z. B. agent.hostname, und legen Sie ihn auf ein Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“.

   Um sicherzustellen, dass im Zuordnungsprozess keine Ereignisfelder übersehen oder dupliziert werden, sind Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass das Feld für Korrelationsereignisse noch nicht ausgewählt und dem Security Incident zugeordnet wurde. Unter Umständen möchten Sie ein eingehendes Korrelationsfeld mehreren Feldern in einem Security Incident zuordnen.

   Ein graus Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Anhand dieser Farbcodierung können Sie nachverfolgen, welche Ereignisfelder bereits für zukünftige Zuordnungen von Feldern für Security Incidents verwendet wurden.



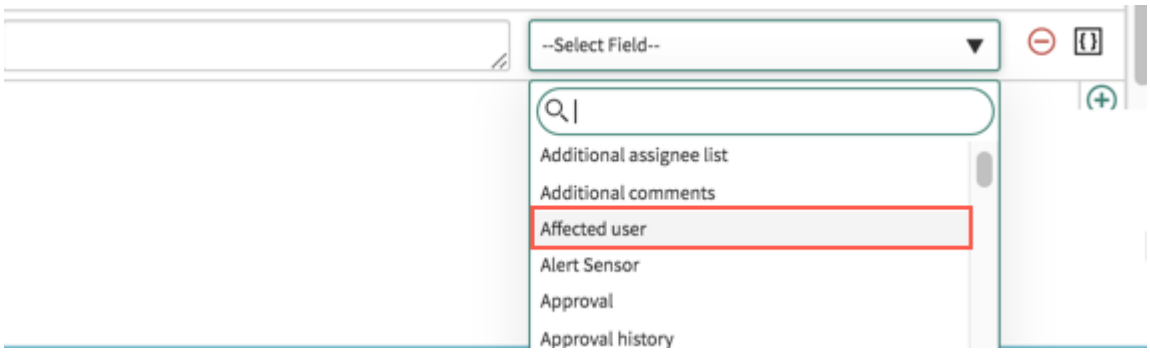
6. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol.
Ein neues Feld wird angezeigt.

b. Erweitern Sie in der Spalte „Security Incident“ die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung ist der betroffene Benutzer grau hinterlegt, da er im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Felder für Korrelationsereignisse auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Felder für Security Incidents auf der rechten Seite, die bereits zugeordneten SIR-Incident-Felder nachzuverfolgen.



Hinweis:
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element “ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der mehrere Optionen ausgewählt werden können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident ebenfalls nicht ausgefüllt.

c. Geben Sie alternativ einen Wert in das Feld Suchen für die neue Zeile ein.

d. Klicken Sie auf der linken Seite des Formulars, um die **Ereignis-ID** auszuwählen, die Sie im Feld **Eingabeausdruck** verwenden möchten.
Ordnen Sie es per Drag-and-Drop neben Ihrem neuen Feld zu.

7. Wahlweise: Öffnen Sie den Skript-Editor und setzen Sie die Bearbeitung fort.

(Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor zum Formatieren von Korrelationsereigniswerten für ArcSight ESM die -Integration.**Filterbedingungen für die Incident-Generierung**

8. Wahlweise: Nachdem Sie die vorhergehenden Feldzuordnungsschritte abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Korrelationsereignis erfüllen muss, um einen SIR -Security Incident zu erstellen.
Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Scrollen Sie im Formular zum Abschnitt „Bedingungen für Incident-Generierung“, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen filtern,** um die Option zu aktivieren.

(Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

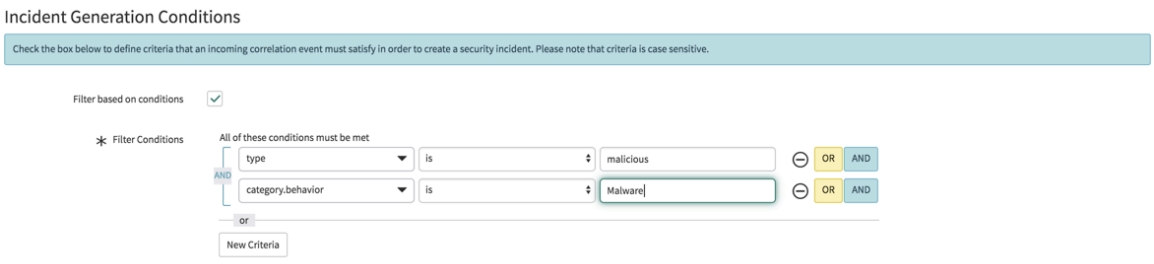
Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt „Beispielerfassung für Korrelationsereignis“ für die von Ihnen erfassten Ereignisse angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach den von Ihnen erfassten Korrelationsereignissen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des Korrelationsereignisses ArcSight ESM übereinstimmen.

Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

b. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **AND** oder **OR**. Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.

c. **Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.



(Optional) Sie haben die Bedingungen für die Incident-Generierung so festgelegt, dass Security Incidents nur erstellt werden, wenn die beiden von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Bedingungsfilterung für die Incident-Generierung hilft Ihnen, die Sicherheitsereignisse einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Korrelationssuche zu ändern oder Ereignisse in ArcSight ESMherauszufiltern. Wenn zusätzliche Filterkriterien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

festgelegt sind, werden nur Korrelationsereignisse, die allen Kriterien entsprechen, Incidents zugeordnet.

Hinweis:
Wenn einer der Ereignisfeldnamen Sonderzeichen wie Anführungszeichen (“), Bindestriche ('), Unterstriche (-) oder Und-Zeichen (@) enthält, müssen diese Zeichen möglicherweise zu Zuordnungsübersetzungszwecken ersetzt werden und führen möglicherweise zu einem duplizierten Ereignis Name. Die Zuordnung kann entsprechend erfolgen, es wird jedoch ein numerisches Suffix angehängt, um Felder mit doppelten Ereignisnamen zu unterscheiden. Wenn beispielsweise das erste Ereignisfeld „events.event“ und das zweite Ereignisfeld „events.event“ist, können diese Felder nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Event-Feld ein Suffix hinzugefügt, und das Feld wird in Events@event(1)umbenannt.

Kriterien für die Zusammenfassung von Ereignissen zur Verarbeitung ähnlicher Korrelationsereignisse und zur Verhinderung doppelter Incidents

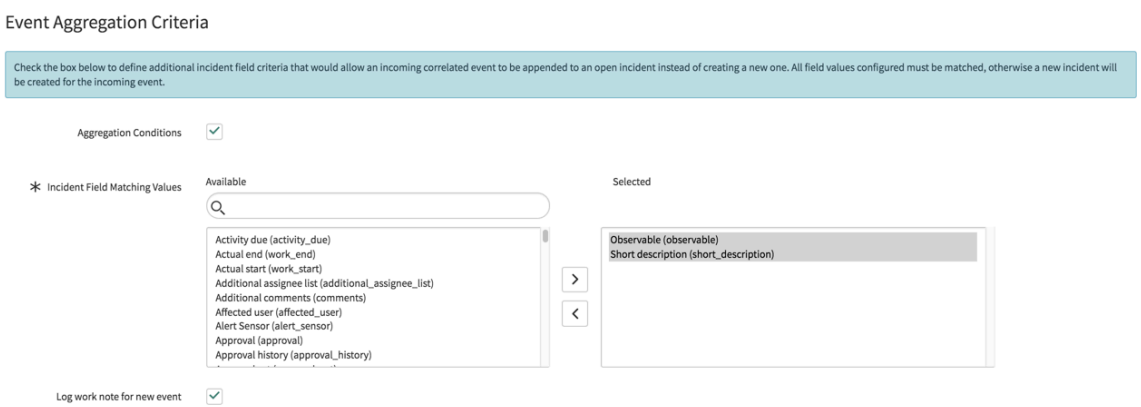
9. **Wahlweise:** Um zu vermeiden, dass doppelte Security Incidents erstellt werden, definieren Sie zusätzliche Kriterien für die Zusammenfassung von Ereignissen, damit eingehende Korrelationsereignisse zu einem offenen Security Incident zusammengefasst werden.
Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:

   a. Scrollen Sie im Formular zum Abschnitt **„Kriterien für Ereigniszusammenfassung“,** und aktivieren Sie das Kontrollkästchen Zusammenfassungsbedingungen, um diese Option zu aktivieren.

      (Optional) Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die im Security Incident SIR konfiguriert sind.

   b. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die mit vorhandenen Security Incidents in Now Platform abgeglichen werden sollen, und verschieben Sie sie in die Liste Ausgewählt.

      (Optional) Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, um dieses eingehende Korrelationsereignis an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Korrelationsereignis-Feldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Ereignis-Zusammenfassung nicht erfüllt, und es wird ein neuer Security Incident erstellt. Screenshot unten für Feldzuordnung mit mehreren Werten.



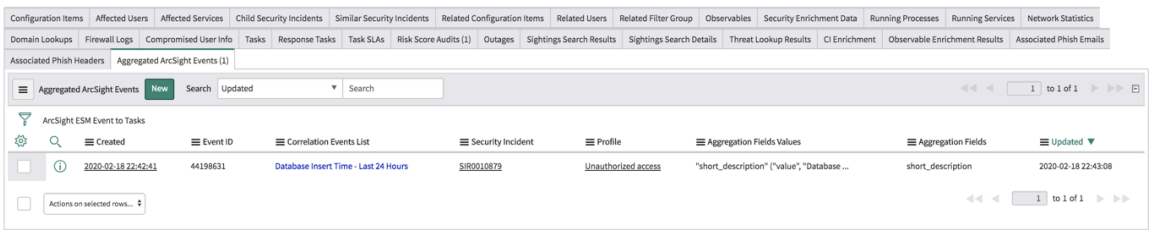
Wenn ein neues Korrelationsereignis mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird das neue Korrelationsereignis automatisch dem zuletzt geöffneten Security Incident

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit denselben Feldwerten hinzugefügt. Als SOC-Analyst, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Korrelationsereignisse in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle aggregierten Korrelationsereignisse für einen Security Incident werden in der zugehörigen Liste **Aggregierte ArcSight-Ereignisse** angezeigt. Diese Liste enthält Details zu zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese Korrelationsereignisse zu vorhandenen Security Incidents aggregiert werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter **„Zugehörige Links“** zur linken Seite des Datensatzes, und klicken Sie auf den Link **Alle zugehörigen Listen anzeigen**.

Hinweis:
Wenn diese zugehörige Liste nicht angezeigt wird, gehen Sie wie folgt vor:

- Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Security Incident“, und klicken Sie auf **Konfigurieren** > **Zugehörige Listen**.
- Wählen Sie **Aggregierte ArcSight-Ereignisse** in der Liste Verfügbar aus, verschieben Sie sie in die Liste Ausgewählt, und klicken Sie auf **Speichern**.
- Klicken Sie **auf Zugehörige Listen anzeigen**. Im Abschnitt „Zugehörige Liste“ wird jetzt die Registerkarte **„Aggregierte ArcSight-Ereignisse“** angezeigt.



c. **Wahlweise:** Aktivieren Sie zum Protokollieren einer Arbeitsnotiz für jedes Mal, wenn ein Ereignis für den Security Incident zusammengefasst wird, das Kontrollkästchen, um diese Option zu aktivieren. Die Arbeitsnotiz protokolliert, dass ein neues korreliertes Ereignis hinzugefügt wurde, zusammen mit einem Link zu den Details des zugehörigen Ereignisses.

Sie haben erfolgreich Werte aus einem Korrelationsereignis Feldern in einem Security Incident SIR zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben Korrelationsereignisse auch zu vorhandenen SIR Security Incidents aggregiert, wenn Ereignisfeldwerte den konfigurierten Zusammenfassungskriterien entsprechen.

10. Wählen Sie eine aus, um mit der Profilkonfiguration fortzufahren.

Zeigen Sie eine Vorschau des Security Incident für die Ereigniserfassungsintegration ArcSight ESM an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Security Incident Now Platform Security Incident Response (SIR) zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Korrelationsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin.

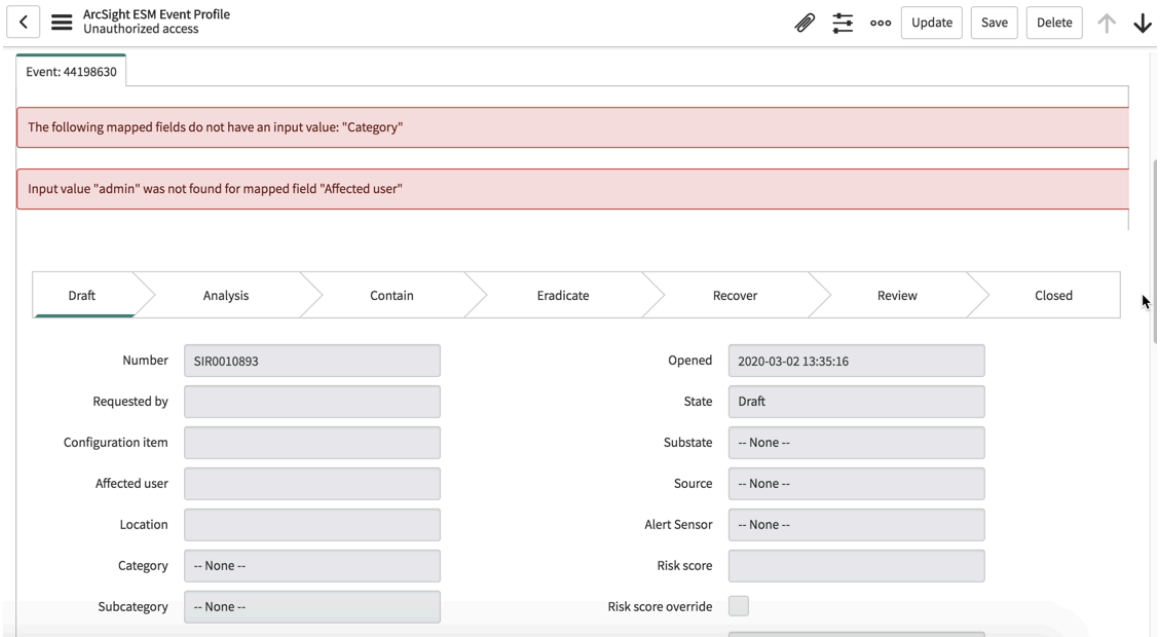
Warum und wann dieser Vorgang ausgeführt wird
Als Benutzer mit der Rolle sn_si.admin können Sie die Vorschau eines Security Incident anzeigen und die Zuordnung nach Bedarf erneut bearbeiten, um Felder mit Fehlern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wird, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen auf Security Incidents werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

Prozedur

1. Wenn die Vorschau des Security Incidents nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Vorschau**.
2. Wählen Sie in der Auswahlliste Beispielereignis-IDs ein Element aus.
   Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Korrelationsereigniswerte für den Security Incident.



   Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel hat ein Feldwert aus dem Korrelationsereignis keinen akzeptablen Wert für das Referenzfeld im SIR-Incident-Formular. Es wird eine Fehlermeldung angezeigt, die darauf hinweist, dass für das Feld Kategorie, bei der es sich um ein Referenzfeld mit einem bestimmten Satz von Werten handelt, kein Eingabewert gefunden wurde. Daher wird dieser zugeordnete Feldwert nicht ohne weitere Änderung im Formular „Security Incident SIR “ angezeigt.

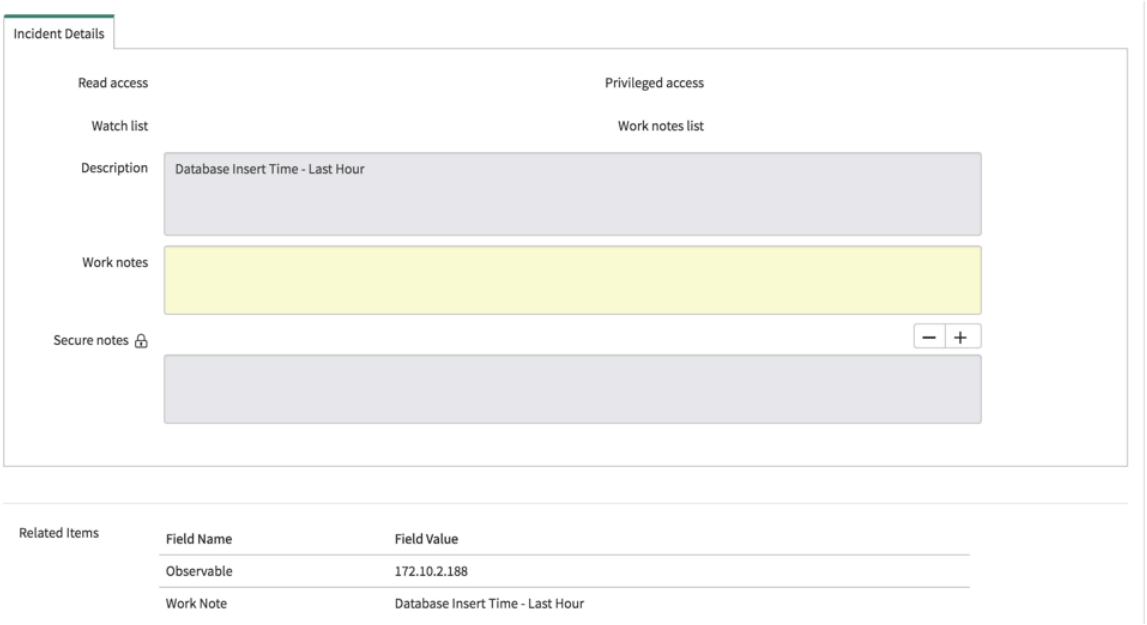
4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in den -Fehlermeldungen beschrieben werden.

   Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Incident-Details in der unteren Hälfte eines Security Incident, nachdem alle Fehlermeldungen gelöst wurden. Für dieses Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und diese

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder werden mit den Werten aus den Wertepaaren gefüllt, die aus den Beispielen für Korrelationsereignisse ArcSight ESM abgerufen wurden.



Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung im Security Incident zufrieden sind, besteht der nächste Schritt in der Definition des Zeitplans.

Erstellen Sie einen Zeitplan für die Erfassung des Ereignisses ArcSight ESM in der Ereigniserfassung

Sie können den Abfrage- oder Abrufzeitplan für neue zugehörige Ereignisse definieren. Während dieses Schritts können Sie die vorhandenen Einstellungen für den Abruf von Korrelationsereignissen überprüfen oder die Zeitplanung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische Korrelationsereignisse mithilfe eines Datumsbereichs abrufen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin.

Warum und wann dieser Vorgang ausgeführt wird

Sie können auswählen, ob Sie während des Schritts „Zeitplanung“ historische Korrelationsereignisse erfassen möchten. Sie können auch auswählen, wie häufig Sie nach zukünftigen neuen Korrelationsereignissen suchen, die der Profilkonfiguration entsprechen.

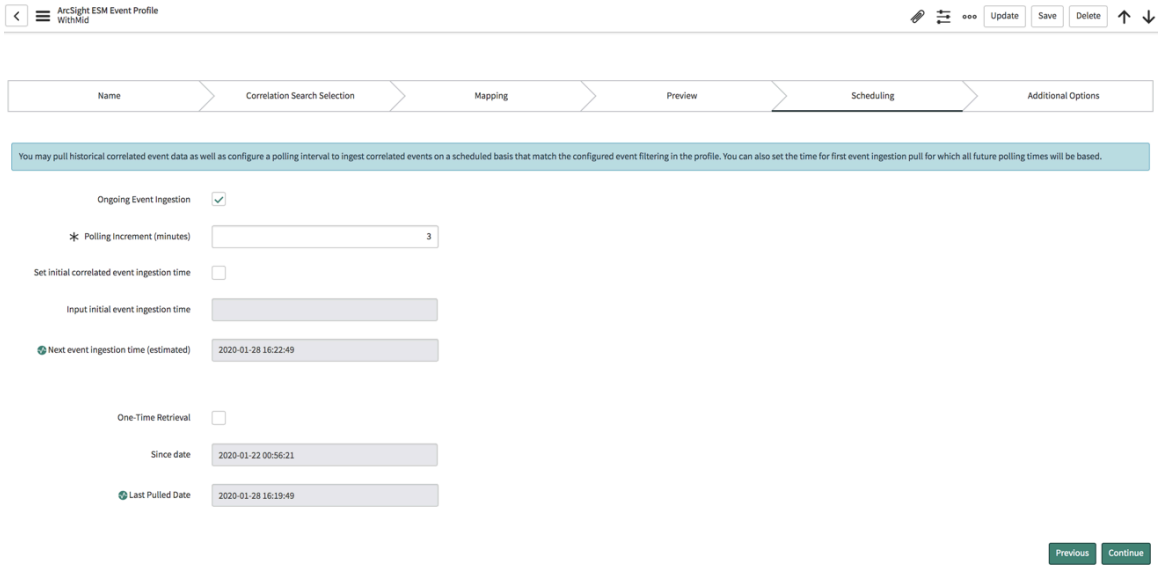
Als Benutzer mit der Rolle sn_si.admin konfigurieren Sie diese Abfrageintervalle für einzelne Profile. Die Leistung der ArcSight ESM Integration zur Korrelationsereigniserfassung kann durch die unterschiedlichen Abfrageintervalle beeinflusst werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrageaufwands auf dem Server ArcSight ESM mit dem Wunsch in Einklang bringen, so bald wie möglich benachrichtigt zu werden, wenn ein Ereignis erstellt oder aktualisiert wird. Für jedes Profil ist ein Standardwert von fünf Minuten festgelegt. Bei Bedarf können Sie diese Einstellung jedoch auch auf einen Wert von nur einer Minute ändern.

Es werden neue und aktualisierte Korrelationsereignisse abgerufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **„Zeitplanung“**aus.
2. Wählen Sie eine aus, um zu planen, wie und wann Korrelationsereignisse aus abgerufen werden<ArcSight> -Konsole.



Als Beispiel für die Planung einer ersten Erfassungszeit des Korrelationsereignisses: Wenn Sie eine tägliche Sicherheitsprüfung ArcSight ESM haben, die einmal pro Tag um 4 Uhr Ortszeit ausgeführt wird, können Sie das entsprechende Korrelationsereignisprofil in Ihrer Instanz Now Platform so einrichten, dass es um 4 Uhr ausgeführt wird :05 Uhr Ortszeit, um das Sicherheitsfehlerereignis sofort zu erfassen und einen Security Incident zu erstellen. Geben Sie 04 05 00 in das Feld Anfängliche Ereigniserfassung ein. Geben Sie im Feld Inkrement (Minuten) den Wert 1440 (24 Stunden) ein, um die nächste Ereigniserfassung für 24 Stunden ab der ersten Ereigniserfassung zu planen. Sowohl die Zeit der ersten Ereigniserfassung als auch die Zeit der nächsten Ereigniserfassung werden in den Feldern angezeigt.

3. Führen Sie die folgenden Schritte aus, um die Einstellungen für dieses Beispiel zu konfigurieren.

   a. Aktivieren Sie auf der Seite „Zeitplanung“ das Kontrollkästchen **Fortlaufende Ereigniserfassung**, um diese Option zu aktivieren.

   b. Geben Sie im Feld Schritt (Minuten) den Wert 1440 (24 Stunden) ein.

   c. Klicken Sie auf das Kontrollkästchen **Erste Zeit der zugehörigen Ereigniserfassung festlegen,** um die Bearbeitung der Felder Erste Ereigniserfassung und Nächste Ereigniserfassung zu aktivieren.

   d. Geben Sie im Feld Zeit der ersten Ereigniserfassung den Wert 04 05 00ein.
   Im Feld Zeit der nächsten Ereigniserfassung (geschätzt) wird die Zeit der nächsten Ereigniserfassung angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **„Fortsetzen** “, um zur Seite „Zusätzliche Optionen“ zu navigieren.

> **Hinweis:**
> Die Anzahl der Security Incidents, die standardmäßig an einem Tag erstellt und zusammengefasst werden können, sowie der Flow-Zeitraum werden in den ArcSight ESM Integrationseinstellungen definiert. Sie können diese Einstellungen bei Bedarf ändern. Details siehe ArcSight ESM Integrationseinstellungen für die Integration der Ereigniserfassung.

Zusätzliche Optionen: Automatisieren Sie die Aktualisierung und den Abschluss korrelierter Ereignisse basierend auf dem Incident-Status SIR .

Die ArcSight ESM -Integration verfügt über eine bidirektionale Schnittstelle, die Korrelationsereignisse zum Erstellen von Security Incidents ermöglicht und die Korrelationsereignisse aktualisiert, sobald der Security Incident mit relevanten Incident-Details wie der Nummer des Security Incidents erstellt und/oder geschlossen wurde , Zuweisungsgruppe, SIR Incident-URL usw.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

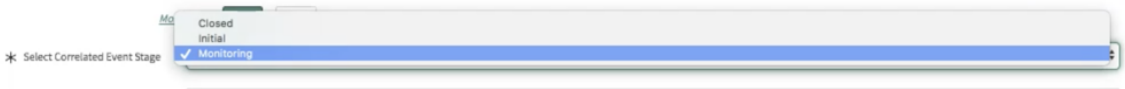
Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration für die Aktualisierung korrelierter Ereignisse abzuschließen, wenn der Security Incident erstellt wird.

   Korrelierte Ereignisphase nicht konfiguriert: Wenn Sie in Ihrer Instanz Now Platform keine zugehörigen Ereignisphasen konfiguriert haben, wird in der Auswahlliste „Aktualisierung der korrelierten Ereignisphase“ nur „ **Phase zuweisen – Ersteinrichtung”** angezeigt. Um die Phase zu konfigurieren, gehen Sie wie folgt vor:

   - Geben Sie im Feld Phasenressourcen-ID eingeben eine Ressourcen-ID ein, und klicken Sie auf **Absenden**. Die Ressourcen-ID wird in der Konsole ArcSight ESM validiert, und der folgende Bildschirm wird angezeigt.

   - Klicken Sie auf **Speichern**, um die neue Phase (**Überwachung**) zu speichern.
   - Klicken Sie auf die Dropdown-Liste Phase für zugehöriges Ereignis auswählen.



   - Sie können die neu erstellte Phase aus der Liste auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelierte Ereignisstufe bereits konfiguriert: Wenn Sie die zugehörige Ereignisphase bereits konfiguriert haben, führen Sie die folgenden Schritte aus:

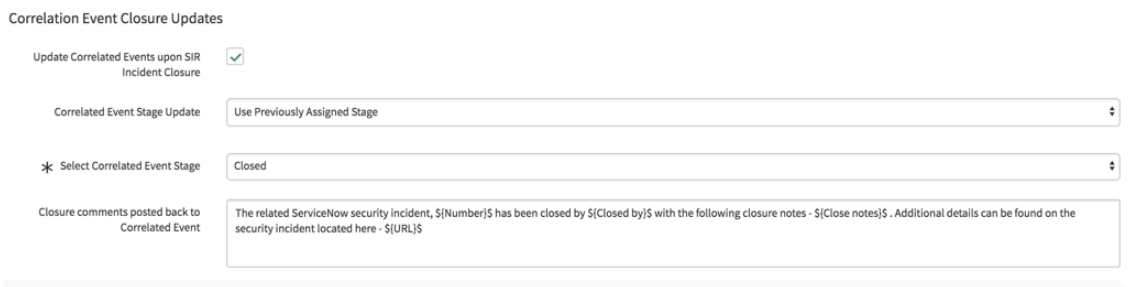
- Wählen Sie **Zuvor zugewiesene Phase verwenden** in der Auswahlliste „Aktualisierung korrelierter Ereignisphasen“ aus.
- Wählen Sie eine vorhandene Phase aus der Auswahlliste Phase für zugehöriges Ereignis auswählen aus (siehe Abbildung unten).

- Anfangskommentare, die an das korrelierte Ereignis zurückgesendet werden: Sie können nicht nur den Wert der Korrelationsereignisstufe aktualisieren, sondern auch Kommentare zu den Anmerkungen zur Korrelationsphase veröffentlichen. Wie in den Anweisungen angegeben, können Sie den im Kommentarbereich angezeigten Standardtext bearbeiten und Ersetzungsvariablen im Format ${Feldname}$ für jedes Feld im Formular „Security Incident Response-Incident“ hinzufügen oder ändern.

Hinweis:
Sie können entweder die in der Konsole ArcSight ESM definierten Standardphasen verwenden oder eigene anwenderdefinierte Phasen erstellen. Führen Sie die folgenden Schritte aus, um eine neue Phase zu erstellen:

- Wählen Sie in der Konsole ArcSight ESM aus **Datei** > **Neu** > **Phase**. Die Registerkarte Überprüfen/Bearbeiten wird angezeigt.
- Definieren Sie die neue Phase, ohne das Kontrollkästchen **Anwender erforderlich** zu aktivieren. Stellen Sie sicher, dass die Phase richtig definiert ist und sich im Ereignislebenszyklus an der richtigen Position befindet.

3. Im Abschnitt „Automatisieren des Schließens relevanter Ereignisse“ können Sie definieren, wie der Security Incident aktualisiert wird, wenn er geschlossen wird.
4. Füllen Sie die Felder des Formulars aus.



5. Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen.
Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um Korrelationsereignisse basierend auf Ihrer Planung aus der -Konsole ArcSight ESM abzurufen.

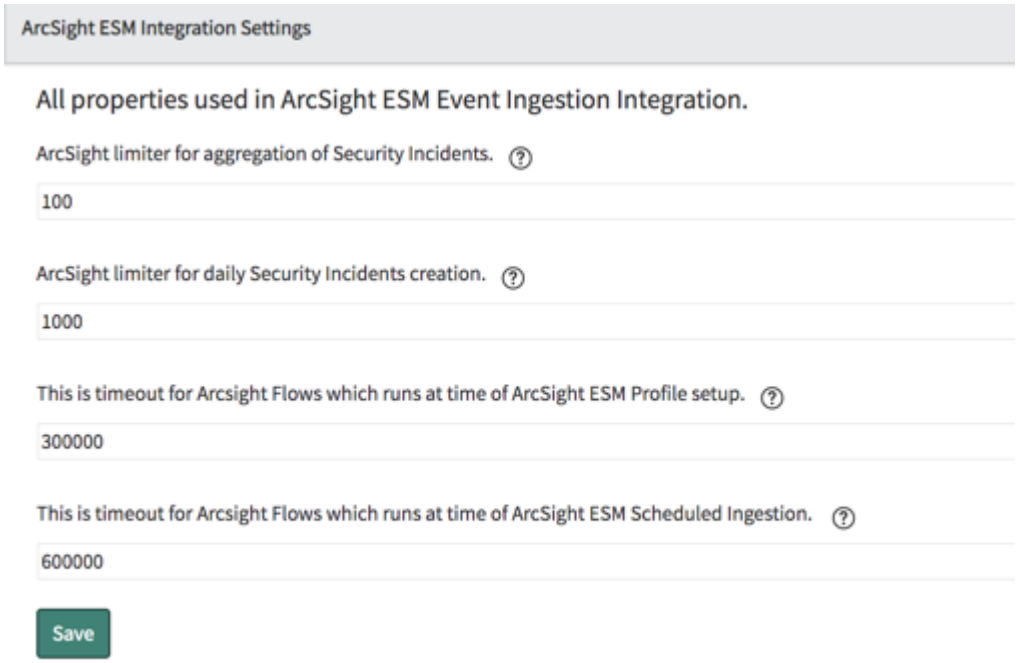
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ArcSight ESM Integrationseinstellungen für die Integration der Ereigniserfassung

Verwenden Sie diese Option, um die ArcSight ESM Einstellungen für die Standarderfassung zu ändern.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **ArcSight ESM Integration** > **ArcSight ESM-Integrationseinstellungen**.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.



Problembehandlung bei der Integration der Ereigniserfassung ArcSight ESM.

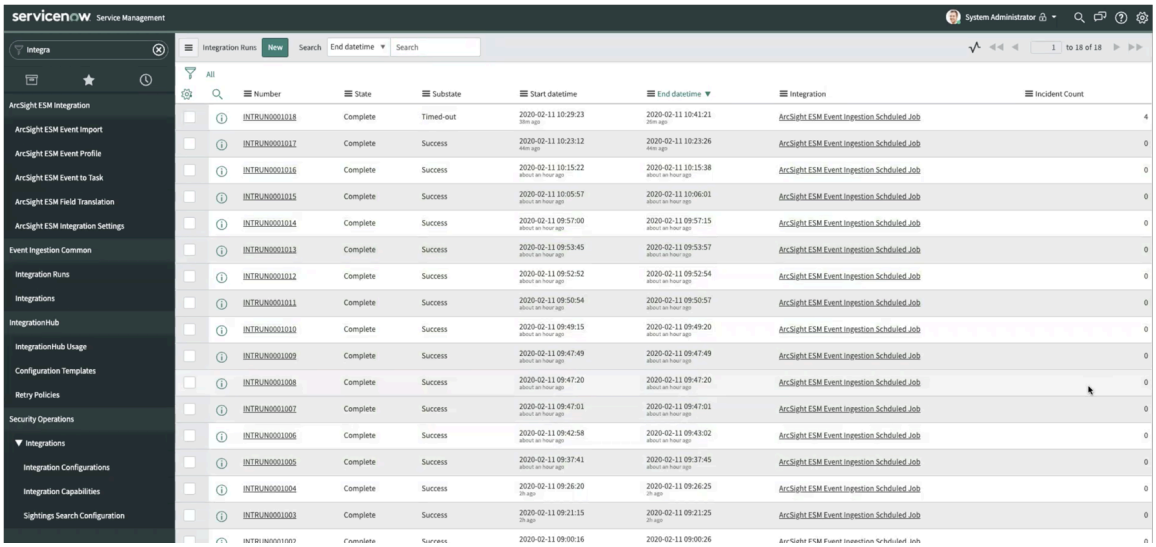
Dieser Abschnitt enthält Informationen zur Behebung von Fehlern, die während der Ereigniserfassung auftreten können.

Integrationsausführungen

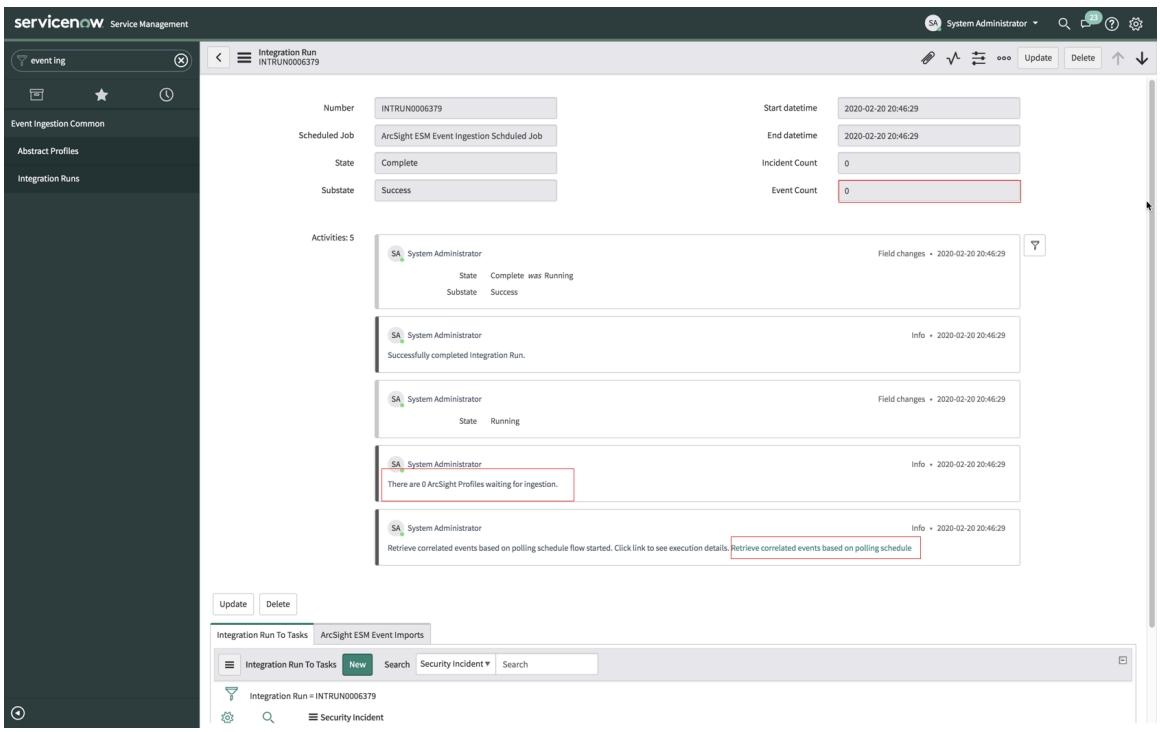
Navigieren zu **Ereigniserfassung allgemein** > **Integrationsausführungen**. Jede Minute findet eine Integrationsausführung statt, bei der Details zu den während der geplanten Aufgabe erfassten Ereignissen erfasst werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Liste der Integrationsausführungen und den Status jeder Ausführung (Erfolg, Zeitüberschreitung, Warten) und die Anzahl der erstellten Security Incidents anzeigen. Klicken Sie auf den Link Nummern, um einen Drilldown zur detaillierten Integrationsausführungsseite durchzuführen.

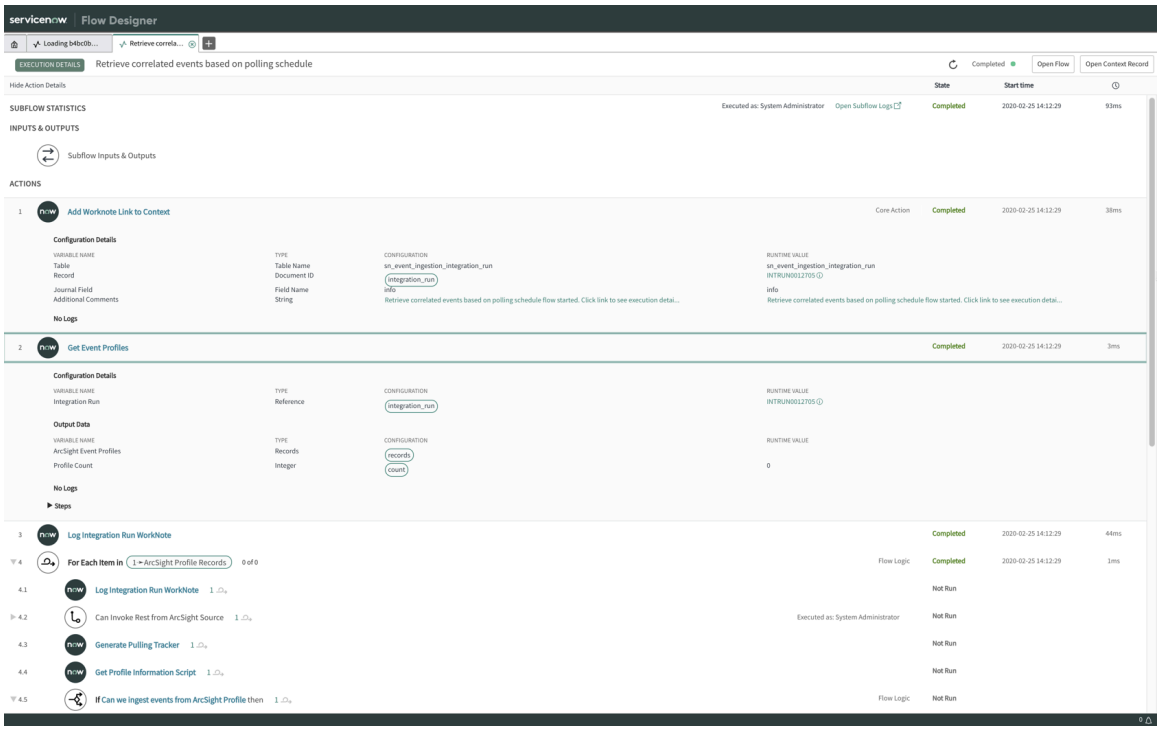


Sie können Details wie die Anzahl der erfassten Ereignisse, den Status, welches Ereignis in einen Security Incident umgewandelt wurde und die verschiedenen Aufgaben anzeigen, die während der Erfassung ausgeführt wurden. Außerdem können Sie auf den Link klicken, um die Details zur Flow-Ausführung anzuzeigen.

Flow-Ausführungsdetails

Klicken Sie auf den Link „Ausführungsdetails“, um den Flow anzuzeigen, der der Ereigniserfassung zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können eine Schritt-für-Schritt-Ausführung des Flows anzeigen, in der die verschiedenen Aktionen und Subflows aufgeführt sind, die als Teil des Flows ausgeführt wurden.

Kopieren Sie das Profil ArcSight ESM für die Integration der Ereigniserfassung

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich möglicherweise, Profile zu kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

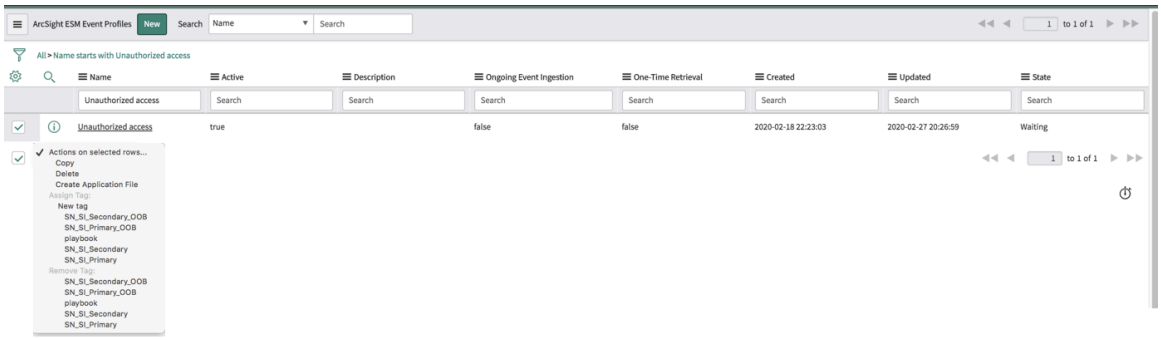
Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname zunächst geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es nicht versehentlich aktiviert wird, bevor die Konfiguration abgeschlossen wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

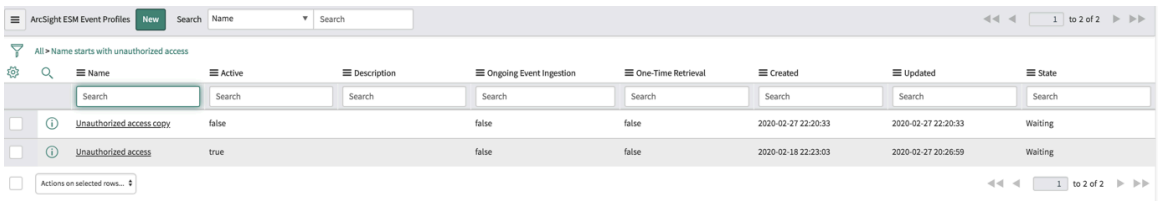
Prozedur

1. Navigieren zu **Alle** > **ArcSight ESM Integration** > **ArcSight ESM Ereignisprofil**.
2. Wählen Sie in der Liste der ArcSight-Profile, die angezeigt wird, ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Zeitplankonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie an dieser Stelle deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **„Aktiv“** auf „falsch“ festgelegt ist, da das Profil aktiviert werden muss.

Verwenden Sie den Skript-Editor zum Formatieren von Korrelationsereigniswerten für ArcSight ESM die -Integration

Verwenden Sie zusätzlich zu den direkt zugeordneten Feldern aus den erfassten Korrelationsereigniswerten den Skript-Editor, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Der Skript-Editor ändert die Werte eines ArcSight ESM -Korrelationsereignisfelds so, dass Werte, die vom Security Incident Now Platform SIR unterstützt werden, den Feldern „Kategorie“, „Configuration Item (CI“), „Erkennbares Element“ und anderen Security Incident-Feldern zugeordnet werden.

In bestimmten Fällen werden die Werte des Korrelationsereignisses ArcSight ESM Referenzfeldern wie „Kategorie“, „Configuration Item (CI)“ und „Erkennbares Element“ im Security Incident zugeordnet. Als Benutzer mit der Rolle sn_si.admin möchten Sie möglicherweise die zugeordneten Ereignisfeldwerte bearbeiten, um Format- oder Datenwerte so zu übersetzen, dass sie den erwarteten Incident-Feldformaten und -Werten entsprechen. Wenn Sie den Wert eines ArcSight ESM -Korrelationsereignisses in einen Wert übersetzen möchten, der von diesen Feldern im Security Incident SIR unterstützt wird, verwenden Sie den Skript-Editor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.
2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt „SIR-Incident-Feldzuordnung“ auf das Klammersymbol [{}] neben einem Feld klicken, um den Skript-Editor für dieses Feld zu öffnen.

   In bestimmten Fällen ist möglicherweise eine Skripteinbindung für das Feld Konfigurationselement geeignet. Bei einem Korrelationsereignis stimmt beispielsweise ein Wert für das Configuration Item möglicherweise nicht mit überein.

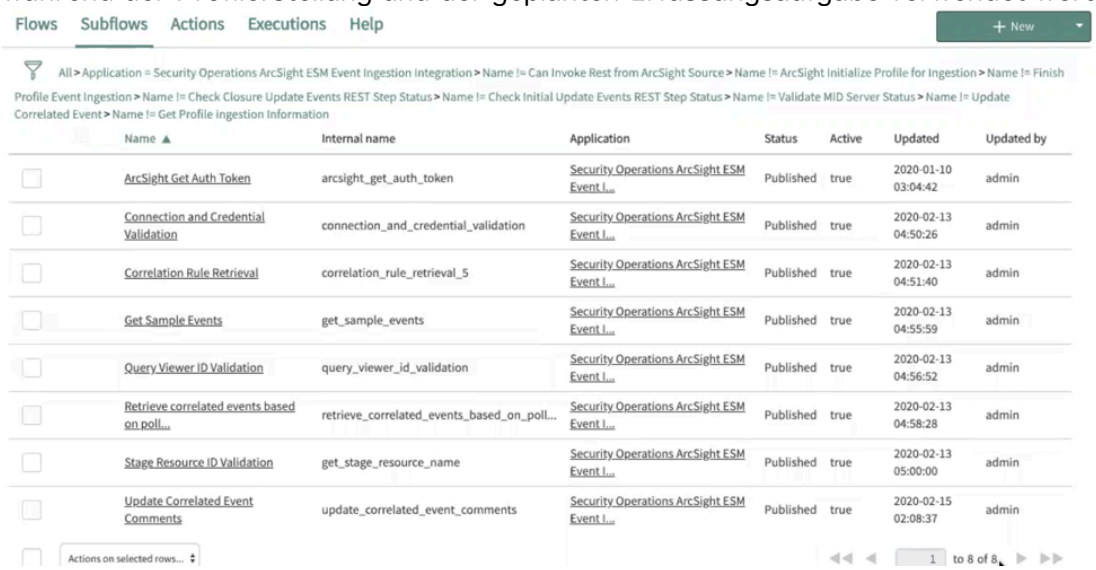
   Wie in der folgenden Abbildung gezeigt, können Sie, wenn in der CMDB Now Platform für das Feld Konfigurationselement keine Übereinstimmung mit einem Hostnamen gefunden wird, die Regel so bearbeiten, dass das Feld Konfigurationselement ausgefüllt wird, sobald eine IP-Adresse gefunden wird.

   Der Editor wird mit dem Feld unter Zielfeld geöffnet.
4. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
   Die Tabelle „Feldübersetzungen ArcSight ESM “ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Verwendung von Flow Designer mit Integration der Ereigniserfassung ArcSight ESM .

Bei Verwendung von Integration Hub und Flow Designer sind mit der ArcSight ESM -Integration mehrere Flows, Subflows und Aktionen verfügbar.

Um diese Subflows anzuzeigen, navigieren Sie zu **Flow Designer** > **Designer** und klicken Sie auf die Registerkarte **SubFlows**. Die folgende Abbildung zeigt die wichtigen Subflows, die während der Profilerstellung und der geplanten Erfassungsaufgabe verwendet werden.



Diese Subflows sind in der Reihenfolge aufgeführt, in der sie unten ausgeführt werden:

- **Validierung von Verbindungs- und Anmeldeinformationen**: Dieser Subflow validiert die Konnektivität ServiceNow von mit dem Server ArcSight ESM und den angegebenen Anmeldeinformationen. Dieser Subflow wird verwendet, wenn Sie in der Kachel **ArcSight ESM – Ereigniserfassung** in auf die Schaltfläche **Konfigurieren**klicken **Security Operations** > **Integrationen** > **Integrationskonfiguration** Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **ArcSight Authentifizierungstoken abrufen**: Dieser Subflow generiert das ArcSight ESM Authentifizierungstoken aus dem Anwendernamen und dem Passwort unter Verwendung des ArcSight ESM Anmeldeservice. Der Anmeldeservice stellt das Authentifizierungstoken bereit, mit dem jeder andere ArcSight ESM -Endpunkt aufgerufen werden kann. Dieser Subflow wird in allen anderen Subflows verwendet.
- **Validierung der Abfrage-Viewer-ID**: Dieser Subflow überprüft, ob die bei der Profilerstellung angegebene Abfrage-Viewer-ID auf dem Server ArcSight ESM vorhanden ist.
- **Abruf der Korrelationsregel**: Dieser Subflow ruft die Korrelationsregeln basierend auf der Abfrage-Viewer-ID ab.
- **Beispielereignis abrufen**: Dieser Subflow ruft die Beispiele für Korrelationsereignisse vom Server ArcSight ESM ab. Diese Beispielereignisse werden dann den Security Incident-Feldern im Abschnitt „Zuordnung“ des Profils zugeordnet.
- **Validierung der Phasenressourcen-ID**: Dieser Subflow validiert die angegebene Phasenressourcen-ID in der Konsole ArcSight ESM und ruft den Ressourcennamen ab.
- **Kommentare zu korrelierten Ereignissen aktualisieren**: Dieser Subflow aktualisiert die Kommentare zu korrelierten Ereignissen in den Abschnitten Initialisieren und Schließen von Incident auf der Seite Zusätzliche Optionen des Profils.
- **Korrelierte Ereignisse basierend auf Abfragezeitplan abrufen**: Dieser Subflow führt die geplante Aufgabe aus, die die korrelierten Ereignisse basierend auf dem Abfrageintervall abruft.

Während der Ausführung lösen die oben genannten Subflows direkt oder indirekt auch mehrere andere Subflows und Aktionen aus, wie unten gezeigt.

Flows | Subflows | Actions | Executions | Help

+ New

Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Amazon Web Services (AWS) Security Hub Integration

AWS Security Hub ist ein CSPM-Service (Cloud Security Posture Management), der automatisierte und kontinuierliche Sicherheitsprüfungen und Best Practice-Prüfungen für Ihre AWS-Ressourcen bereitstellt.

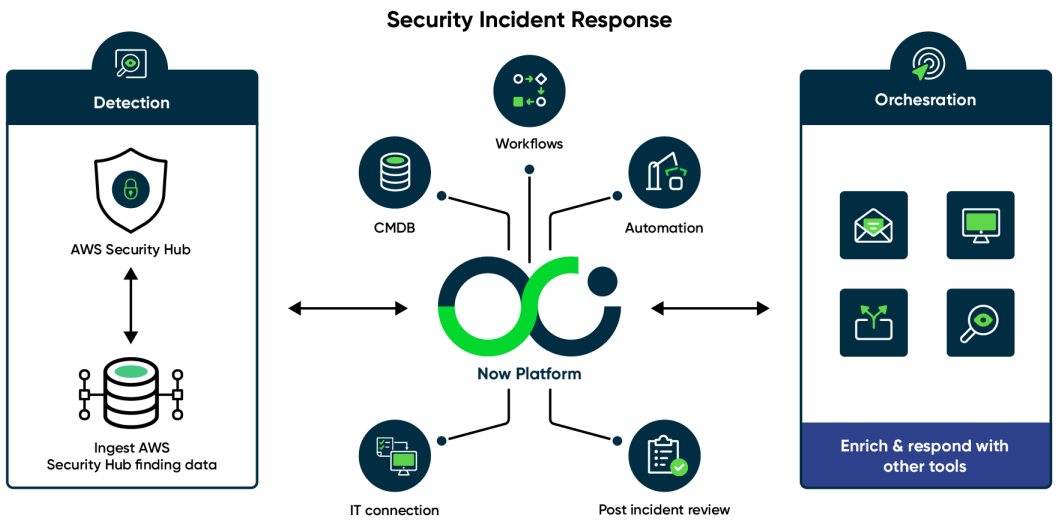
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über die AWS Security Hub -Integration

AWS Security Hub Mit können Sie Probleme in Ihren Konfigurationen identifizieren. Security Hub fasst Ihre Sicherheitswarnungen zusammen, die als Ergebnisse bezeichnet werden. AWS Security Hub generiert diese Ergebnisse in einem standardisierten Format und priorisiert sie, damit Sie sie leichter ergänzen, untersuchen und korrigieren können. Sie können die AWS Security Hub -Integration verwenden, um Security Hub-Ergebnisse zu erfassen und automatisch Security Incidents in Security Incident Responsezu erstellen.

AWS Security Hub Die -Integration in SIR folgt einer bidirektionalen Architektur. SIR erfasst Security Hub Ergebnisdaten, um einen Security Incident zu erstellen, und aktualisiert gleichzeitig ein Security Hub -Ergebnis mit allen Aktualisierungen im entsprechenden Security Incident.

Im folgenden Diagramm können Sie erfahren, wie AWS Security Hub in die -Anwendungen Now Platform Security Operations integriert wird.



Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erkennen Sie AWS Security Hub-Ergebnisse, die Kandidaten für Security Incidents sind, und automatisieren Sie die Erstellung dieser Security Incidents.
- Ordnen Sie die AWS Security Hub-Ergebnisse und -Entitätsfelder den Feldern „Security Incident SIR “ zu.
- Filtern Sie AWS Security Hub-Ergebnisse.
- Fassen Sie Ergebnisse zu vorhandenen offenen Security Incidents zusammen, damit Sie keine doppelten Security Incidents erstellen müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Automatisieren Sie die Statusaktualisierungen von AWS Security Hub-Ergebnissen für Security Incident Response, damit Sie Security Incidents erstellen und schließen können.

  Hinweis:
  ServiceNow aktualisiert auch den Status der AWS Security Hub-Ergebnisse basierend auf der Erstellung, dem Fortschritt oder der Schließung des Security Incident. Dieses Update enthält auch Kommentare von aggregierten und neuen Ergebnissen.

- Planen Sie die Erfassung von Ergebnissen, um regelmäßig Security Incidents zu erstellen.
- AWS Security Hub-Ergebniskommentare mit SIR -Arbeitsnotizen synchronisieren.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
Website mit Produktdokumentation zu AWS Security Hub	Dokumentationswebsite für AWS Security Hub
ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

Erste Schritte mit AWS Security Hub der -Integration

Aktivieren Sie die AWS Security Hub -Ergebnisintegration für das Plugin „Security Operations“ als Schnittstelle mit Ihrer ServiceNow® -Instanz und Security Incident Response Ihrem -Produkt.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Bevor Sie die AWS Security Hub -Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

Warum und wann dieser Vorgang ausgeführt wird
Sehen Sie sich die folgende Setupprüfliste an, und vergewissern Sie sich, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben.

Prüfliste

Weisen Sie die erforderlichen Rollen für die Plattform ServiceNow® und Security Incident Response zu, und überprüfen Sie sie.	Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:
	• Die Rolle admin installiert die Integration aus ServiceNow Store und weist die Rolle sn_si.admin zu.
	• Die Rolle sn_si.admin führt die folgenden Aufgaben aus:
	  ○ Konfiguriert die Integration.
	  ○ Erstellt Incident-Profile.
	  ○ Ordnet die Ergebnisdatenfelder AWS Security Hub den Feldern für Security Incidents zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

	○ Plant die laufende Incident-Erfassung. ○ Aktiviert Incident-Updates, wenn der Incident Security Incident Response erstellt oder geschlossen wird.
Weisen Sie die AWS Security Hub erforderlichen Rollen zu.	Die folgenden Rollen sind in AWS Security Hub erforderlich, um Ihre Anwendung zu registrieren und zu konfigurieren: • SecurityHubReadOnlyAccess • SecurityHubFullAccess
Überprüfen Sie die Integrationseinstellungen für AWS Security Hub .	Navigieren zu **Alle** > **AWS Security Hub-Ergebnisintegration** > **Integrationseinstellungen für AWS-Security-Hub-Ergebnisse**. Überprüfen oder ändern Sie die Eigenschafteneinstellungen entsprechend Ihren Anforderungen.
Konfigurieren Sie Ihre -Anwendung im -Portal AWS.	Registrieren Sie Ihre Anwendung im -Portal AWS, und gewähren Sie Ihren Benutzern Lese- und Schreibzugriff auf die Anwendung. Weitere Informationen finden Sie in den folgenden Themen: • AWS Config mit der -Konsole einrichten • Security Hub-Integrationen.

Registrieren und konfigurieren Sie das -Portal AWS Security Hub .

Registrieren Sie Ihre Anwendung im -Portal AWS Security Hub, und gewähren Sie Ihren Benutzern Lese- und Schreibzugriff auf die Anwendung.

Registrieren eines ServiceNow® -Anwenderprofils im AWS -Portal

Vorbereitungen

Erforderliche Rolle: AWSSecurityHubFullAccess

Prozedur

1. Melden Sie sich beim AWS-Portal an.
2. Navigieren zu **Identity and Access Management (IAM)** > **Anwender** > **Neuen Anwender erstellen**.
3. In der folgenden Tabelle werden die Felder beschrieben, die Sie konfigurieren müssen, um ein Anwenderprofil zu erstellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Anwenderprofil

Feld	Beschreibung
Geben Sie Benutzerdetails an > **Anwendername**	Name für das Anwenderprofil.
Berechtigungen festlegen > **Fügen Sie der Gruppe den Anwender hinzu**	Fügen Sie das Anwenderprofil einer Gruppe mit vordefinierten Berechtigungsrichtlinien hinzu. Sie können eine Gruppe nach Ihren Wünschen erstellen und der Gruppe Berechtigungsrichtlinien zuweisen. Später können Sie der Gruppe Anwenderprofile hinzufügen, und die der Gruppe zugewiesenen Berechtigungsrichtlinien werden den Anwenderprofilen automatisch zugewiesen.
Berechtigungen kopieren	Kopieren Sie Berechtigungen aus einem Anwenderprofil, und weisen Sie sie dem neuen Anwenderprofil zu.
Richtlinien direkt anhängen	Fügen Sie AWSSecurityHubFullAccess als Berechtigungsrichtlinie für Ihr Anwenderprofil hinzu. Weisen Sie dem Anwenderprofil entsprechend Ihren Einstellungen eine neue Berechtigungsrichtlinie zu.
Überprüfen und erstellen Sie	Überprüfen Sie alle Details, die Sie dem Anwenderprofil hinzugefügt haben.

4. Wählen Sie **Anwender erstellen aus**.
5. Wählen Sie im angezeigten Popup-Fenster **Anwender anzeigen** aus.
6. Erstellen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel für das Anwenderprofil.
   Sie benötigen diese Schlüssel, um von Ihrer Instanz ServiceNow® aus auf die Integration AWS Security Hub zuzugreifen.
7. Navigieren zu **AWS-Services** > **Suchen** > **AWS Security Hub** > **.**
8. Wählen Sie **Gehe zu aus** *`Security Hub`*.
9. Wählen Sie auf der Seite „Aktivieren AWS Security Hub “ **die Option Herunterladen** aus, um die Konfiguration AWS zu aktivieren.
   Laden Sie die Dateien herunter, und führen Sie sie in Ihrem Account aus. Dadurch erhalten Sie die Berechtigung, alle Informationen aus verschiedenen AWS-Berichterstellungsservices zu sammeln und in AWS Security Hubzusammenzufassen.
10. Wählen Sie unten auf der Seite **Aktivieren** *`AWS Security Hub`*aus.
    Es dauert einen Moment, bis im Dashboard *`AWS Security Hub`* alle Details angezeigt werden.
11. Ändern Sie die Region von **Global** in **USA Ost (Ohio)**.
    Der Code für **USA Ost (Ohio)** lautet **us-east-2**. Alle ServiceNow® -Ressourcen sind diesem Regionscode zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie die -Integration AWS Security Hub .

Installieren und konfigurieren Sie die AWS Security Hub -Integration über ServiceNow Store in Ihrer Now Platform -Instanz, um mit der Erfassung AWS Security Hub von -Ergebnissen zu beginnen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie die AWS Security Hub -Integration von ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel AWS Security Hub, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

AWS Security Hub Konfigurationsformular

Feld	Beschreibung
Name	Name für die Konfiguration der Instanz AWS Security Hub
Regionsname	Region, die Sie im Anwenderprofil ServiceNow® im Portal AWS Security Hub zugewiesen haben.
Geheimer Schlüssel	Geheimer Schlüssel, den Sie für das Anwenderprofil ServiceNow® im Portal AWS Security Hub erstellt haben.
Zugriffsschlüssel	Zugriffsschlüssel, den Sie für das Anwenderprofil ServiceNow® im Portal AWS Security Hub erstellt haben.

5. Klicken Sie auf **Absenden**.

Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird jede Security Hub -Ergebniserfassungsserverkonfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für AWS Security Hub, um die Integration zu finden

Erstellen Sie ein AWS Security Hub Profil in Ihrer Instanz Now Platform, das Sie verwenden werden, um Daten aus AWS Security Hub zu erfassen und einen entsprechenden Security Incident in Arbeitsbereich für Security Incident Responsezu erstellen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Mit der -Integration können Sie Security Incidents für verschiedene Arten von Ergebnissen auf der Plattform AWS Security Hub erstellen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Incidents werden basierend auf den Profilen erstellt, die Sie in der Instanz Now Platform konfigurieren. Alle Incidents werden zunächst für einen konfigurierten Ergebnistyp in einem Profil erstellt. Sie können die von Ihnen erstellten Ergebnisse weiter filtern, um anzugeben, welche Ergebnisse Security Incidents verursachen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Ergebnisse, die die Auswahlkriterien in Ihrem Mandanten AWS Security Hub erfüllen und über die AWS Security Hub API verfügbar sind, werden zunächst in Ihrer Instanz Now Platform aufgenommen.

Prozedur

1. Navigieren zu **Alle** > **Integration von AWS-Security-Hub-Ergebnissen** > **AWS Security Hub-Ergebnisprofil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

AWS Security Hub Formular „Konfiguration der Ergebniserfassung“.

Feld	Beschreibung
Name	Name für das Profil Dieser Name hilft Ihnen, den Profiltyp zu identifizieren, und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist.
Aktiv	Wählen Sie diese Option, um das Profil zu aktivieren. Wenn das Profil aktiv ist, impliziert dies, dass Now Platform aktiv die Ergebnisdaten AWS Security Hub von erfasst und entsprechende Security Incidents in SIR erstellt werden, wenn die Filterbedingungen erfüllt sind.
Quelle	Der AWS Security Hub Integrationsmandant, den Sie für die Erfassung von Ergebnissen konfiguriert haben. Wenn Sie mehrere Mandanten konfiguriert haben, wählen Sie den entsprechenden Mandanten für die Ergebnistypen aus, die Sie für das Profil erfassen möchten.
Bestellung	Geben Sie einen Wert für dieses Feld ein, der die Reihenfolge angibt, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Flow mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Beispiel: 100, 200, 300, 400. Der Standardwert ist 100.
Beschreibung	Zusätzlicher Text, mit dem Sie dieses Profil von anderen Profilen unterscheiden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie die Ergebnisfelder AWS Security Hub zu

Ordnen Sie die einzelnen AWS Security Hub -Ergebnisfelder den Feldern im Security Incident SIR zu, um mit den zugeordneten Daten Incidents zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wählen Sie auf der Zuordnungsseite im Abschnitt AWS Security Hub Zuordnung eine der Beispielerfassungsmethoden aus.

Beispiel für Erfassungsmethoden

Feld	Beschreibung
Alle Standardergebnisfelder	Verwenden Sie diese Erfassungsmethode, um die statische Liste aller Ergebnisfelder anzuzeigen. Diese Methode enthält nur Standardfeldnamen ohne Werte. Sie können diese Informationen verwenden, um die Zuordnung zu den Feldern SIR vorzunehmen.
Rufen Sie die neuesten AWS Security Hub Ergebnisse ab	Verwenden Sie diese Erfassungsmethode, um die neuesten Ergebnisdaten zu importieren. Sie können standardmäßig 5 Beispielergebnisse und maximal 20 Beispielergebnisse erfassen. Die Feldwerte für das Beispielergebnis werden gefüllt, wenn das Profil die Beispielergebnisse erfasst. Sie können diese Ergebnisse den **SIR-Incident-Zielfeldern**zuordnen. Die Ergebnisfelder und -werte werden als einzelne Registerkarten angezeigt.
Importieren Sie Beispieldaten	Wählen Sie **Beispieldaten importieren**, um Beispielergebnisse aus AWS Security Hubzu importieren. Diese Schaltfläche wird angezeigt, wenn Sie die Erfassungsmethode „Neueste AWS Security Hub Ergebnisse abrufen“ auswählen. Das Abrufen der Beispielergebnisse vom Server AWS Security Hub dauert einige Minuten. Ordnen Sie diese Ergebnisse den **SIR-Incident-Zielfeldern**zu. Die Ergebnisfelder und -werte werden als einzelne Registerkarten angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Führen Sie die folgenden Aktionen aus, um den Standardfeldern, die im Security Incident angezeigt werden, Felder hinzuzufügen:

   Wählen Sie im Abschnitt „SIR-Incident-Zielfelder“ die

Schaltfläche. Es zeigt eine Liste von Feldern SIR, aus denen Sie ein neues Feld auswählen können.

   a. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie dann ein Feld aus.

   Hinweis:
   Für denselben Security Incident können mehrere erkennbare Elemente angezeigt werden. Beispielsweise kann das Feld „ **Erkennbares Element** “ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder **Konfigurationselement** und **Arbeitsnotizen** mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird eine Fehlermeldung angezeigt, dass dieses Feld nicht mehrere Werte unterstützt. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

   b. Ziehen Sie Ihr Feld aus dem Abschnitt AWS Security Hub Quellfelder, um es dem neuen Feld zuzuordnen.

   c. Wenn Sie das Kontrollkästchen aktivieren, das einem Feld entspricht, werden alle neuen oder aktualisierten Changes, die in AWS Security Hub vorgenommen werden, im jeweiligen SIR automatisch mit neuen Incident-Daten aktualisiert.

   Hinweis:
   Im Basissystem ist die Systemeigenschaft sn_sec_security.finding_updates standardmäßig auf „True“ festgelegt, um die AWS Security Hub -Updates im Zusammenhang mit neuen Warnungen zu erhalten, die mit SIR verknüpft sind.

   - Standardmäßig sind die Felder Betroffene Anwender, Konfigurationselemente und Erkennbare Elemente aktiviert. Dies bedeutet, dass jedes Mal, wenn neue erkennbare Elemente oder zugehörige Konfigurationselemente oder betroffene Benutzer dem Incident hinzugefügt werden, diese Informationen während dieses Abfrageintervalls automatisch extrahiert und in die entsprechenden zugehörigen Listen in Security Incident Response (SIR) eingetragen werden.
   - Für alle anderen Felder müssen Sie das Kontrollkästchen aktivieren, das einem Feld für alle neuen oder aktualisierten Änderungen entspricht, die im Ergebnis in AWS Security Hubvorgenommen werden. Dadurch werden die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

   Wichtig:
   Vor der Auswahl dieser Funktionalität muss die Sorgfaltspflicht erfüllt werden, da das Überschreiben der vorhandenen Daten zu instabilen Daten führen kann, mit denen der Analyst arbeiten kann, und jede andere Automatisierung, die auch durch die Feldwerte des Security Incident festgelegt wird, betroffen sein kann. Daher ist es wichtig, die Sorgfaltspflicht zu erfüllen, bevor Sie eine Überschreibungsfunktion auswählen.

3. Um ein Feld zu entfernen, klicken Sie auf die , die Schaltfläche (**Element entfernen**) neben dem Eingabeausdrucksfeld im Abschnitt „SIR-Incident-Zielfelder“.

4. Um einen Feldwert aus dem Abschnitt AWS Security Hub „ Quellfelder einem Feld im Abschnitt „SIR-Incident-Zielfelder“ zuzuordnen, verwenden Sie eine der folgenden Aktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Ziehen Sie den Feldnamen (z. B. ID), und legen Sie ihn neben einem Feldnamen in der Spalte „SIR-Incident-Zielfelder“ ab.

Sie können einen beliebigen Wert aus dem Abschnitt „Quellfelder AWS Security Hub “ mit einem Feld im Abschnitt „SIR-Incident-Zielfelder“ abgleichen. Felder sind farbcodiert, damit Sie im Zuordnungsprozess keine Ergebnisfelder übersehen oder duplizieren. Hellblaue Felder zeigen an, dass im Security Incident noch kein Ergebnisfeld ausgewählt und zugeordnet wurde. Unter Umständen möchten Sie ein eingehendes Ergebnisfeld mit mehr als einem Feld in einem Security Incident verknüpfen. Ein graus Feld zeigt an, dass ein Ergebnisfeld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Auf diese Weise können Sie visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Ergebnisinformationen nicht zugeordnet bleiben. Allerdings gibt es einige Felder im Abschnitt AWS Security Hub „ Quellfelder, die nicht mit Feldern im Abschnitt „SIR-Incident-Zielfelder“ kompatibel sind. Wenn Sie solche Werte zuordnen, werden sie nicht angezeigt, wenn der SIR erstellt wird.

b. Sie können eine Kombination aus Text und Feld hinzufügen.
Beispiel: `Ergebnisname ist ${name}$`. Hier kann `der Ergebnisname` manuell eingegeben werden, während `${name}$` im Abschnitt AWS Security Hub Quellfelder zugeordnet wird.

c. Sie können ein Quellergebnisfeld manuell eingeben und einem Zielfeld zuordnen.
Verwenden Sie das Format ${Feldname}$, um ein Quellergebnisfeld manuell zuzuordnen. Um beispielsweise ein Ergebnisfeld „Schweregrad“ zuzuordnen, lautet das Format`${properties(severity)}$`.

Diese Integration klassifiziert bestimmte Untertypen von erkennbaren Elementen. Wenn Sie ein Ergebnisfeld AWS Security Hub dem erkennbaren SIR-Feld zuordnen, klassifiziert Now Platform das erkennbare Element automatisch. Wenn Sie das eingehende erkennbare Element AWS Security Hub generisch dem erkennbaren Elementtyp in SIRzuordnen möchten, ziehen Sie das Feld AWS Security Hub per Drag-and-Drop in das Feld Erkennbares Element. Wenn Sie jedoch den erkennbaren Elementtyp für das eingehende erkennbare Element AWS Security Hub in SIRkennen, ordnen Sie ihn speziell dem Feld „Erkennbarer Typ SIR “ zu. Einige Beispiele für bestimmte erkennbare Elemente in SIR sind „Erkennbares Element“ (Domänenname), „Erkennbares Element“ (E-Mail-Adresse), „Erkennbares Element“ (IP-Adresse (V4)) und „Erkennbares Element“ (Hostname).

Manchmal werden gefundene Feldwerte in AWS Security Hub möglicherweise nicht direkt in die Felder im SIR-Security Incident übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten.

5. Um eine Feldübersetzung für ein neues Feld aus dem Ergebnis AWS Security Hub so zu formatieren, dass sie einem Feldwert in einem Security Incident entspricht, klicken Sie auf den Link **Hier klicken** im Header **„SIR-Incident-Zielfelder“**.

6. Um die Felder zu ändern, die die Feldübersetzung unterstützen, klicken Sie auf das Symbol für .
Die Felder, die die Feldübersetzung unterstützen, sind **Kategorie**, **Konfigurationselement**und **Priorität**.

Klicken Sie beispielsweise auf das Symbol neben der Kategorie. Der Skript-Editor für die AWS Security Hub -Ergebnisfeldübersetzung wird geöffnet.

7. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.
Definieren Sie beispielsweise für Kategorie Folgendes im Skript-Editor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"<Incoming Security Hub finding Field Value>" : "<Category to assign to the Security Incident>".
```

Diese Zuordnung stellt sicher, dass ein Profil nur konfigurierte Kategorien verwendet.

8. Setzen Sie Ihre Zuordnung fort, indem Sie Feldwerte hinzufügen oder entfernen.
   Dieselben Feldwerte können Sie im Builder für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ergebnis erfüllen muss, um einen Security Incident zu erstellen.
9. Um zum Abschnitt „Filtern und Aggregieren“ zu wechseln, klicken Sie auf **Fortsetzen**.

Nächste Maßnahme

Definieren Sie Filterbedingungen, und legen Sie sie fest, um festzulegen, welche Ergebnisse Security Incidents erstellen. Sie können dieselben Feldwerte (definiert im Abschnitt „Zuordnung“) im Generator für Bedingungen für Incident-Generierung (im Abschnitt „Filtern und Zusammenfassung“) verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ergebnis erfüllen muss, um einen Security Incident zu erstellen.

Definieren Sie Filter- und Zusammenfassungskriterien für die Erfassung der Ergebnisse AWS Security Hub von [].

Sie können Filterbedingungen definieren und festlegen, um festzulegen, welche eingehenden Ergebnisse Security Incidents erstellen sollen. Sie können auch zusätzliche Incident-Feldkriterien definieren, die es ermöglichen, ein eingehendes Ergebnis an einen offenen Security Incident anzuhängen, anstatt einen anderen Security Incident für dasselbe Ergebnis zu erstellen.

Legen Sie die Filterbedingungen für die Ergebnisse AWS Security Hub fest, um Security Incidents zu erstellen

Legen Sie die Filterbedingungen so fest, dass Security Incidents nur erstellt werden, wenn die Filterbedingungen erfüllt sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Art der Filterung hilft Ihnen, Security Incidents zu isolieren, und begrenzt die Anzahl der von Ihnen erstellten Security Incidents. Wenn Sie zusätzliche Filterkriterien festlegen, werden nur die erforderlichen Ergebnisse erfasst, ohne dass die Abfrage oder die Konfiguration des ausgelösten Incidents geändert werden muss.

Führen Sie die folgenden Schritte aus, um die Kriterien zu definieren, die ein eingehendes AWS Security Hub -Ergebnis erfüllen muss, damit ein Security Incident erstellt wird:

Prozedur

1. Wählen Sie **Vorfilter anwenden** im Abschnitt Vorfilterung.

   Sie können diese Option verwenden, um bestimmte Ergebnisse zu filtern und die Last der Ergebniserfassung zu reduzieren.

   Geben Sie im Feld **API-Filter** eine JSON-Bedingung gemäß Ihrer Anforderung ein, die bestimmte Ergebnisse basierend auf der Bedingung herausfiltert. Geben Sie beispielsweise den folgenden Wert ein, um Ergebnisse herauszufiltern, deren Workflow-Status in Security Hub gelöst ist:

```
{"Filters"{
 "WorkflowStatus":[{
 "Comparison":"NOT_EQUALS",
 "Value": "RESOLVED"}]
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
}
}
```

Basierend auf der angegebenen Bedingung werden die Ergebnisse AWS Security Hub erfasst und in der Rohtabelle der Ergebnisse AWS Security Hub angezeigt.

Navigieren zu **Alle** > **Integration von AWS-Security-Hub-Ergebnissen** > **AWS Security Hub-Ergebnisse – Rohdaten** um die Rohergebnisdaten anzuzeigen.

2. Wählen Sie im Abschnitt Ergebnisfelder für Filterbedingungen auswählen **Verfügbare Ergebnisfelder anzeigen aus**, um eine Liste aller verfügbaren Felder in einem AWS Security Hub -Ergebnis anzuzeigen. Wählen Sie in der Liste **Alle Ergebnisfelder** die Ergebnisfelder aus, die im Abschnitt „Bedingungen für die Generierung von Security Incidents“ angezeigt werden sollen.

   Hinweis:
   Ein AWS Security Hub-Ergebnis enthält mehrere Felder und Werte. In der Liste **Alle Ergebnisfelder** können Sie nach einem Ergebnisfeld suchen, das Ihren Anforderungen entspricht, und es auswählen.

3. Wählen Sie im Abschnitt Bedingungen für die Generierung von Security Incidents **die Option Filter basierend auf Bedingungen** aus, um die Kriterien zu definieren, die ein eingehendes Ergebnis AWS Security Hub erfüllen muss, damit ein Security Incident erstellt wird.

   Das erste Feld in den Filterbedingungen enthält eine Standardliste von zweihundert Feldern, die für ein AWS Security Hub -Ergebnis verfügbar sind, sowie die Ergebnisfelder, die Sie im Abschnitt „Ergebnisfelder für Filterbedingungen auswählen“ ausgewählt haben.

   Das zweite Feld in den Filterbedingungen enthält bedingte Operatoren. Die von Ihnen gewählte Option bestimmt die Bedingung, die zum Erfassen eines Ergebnisses erfüllt sein muss.

   Das dritte Feld in den Filterbedingungen enthält Werte, die von den verfügbaren Ergebnisfeldern unterstützt werden. Stellen Sie sicher, dass das von Ihnen eingegebene Ergebnisfeld den Werten der Ergebnisse entspricht.

   Verwenden Sie beispielsweise die Filterbedingung *enthält* für die folgenden Felder mit mehreren Werten:

   - Workflow(Status)
   - WorkflowState

4. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter für die erste Zeile fest.
5. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.
   - Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.
6. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.

Ergebnisse

Basierend auf den Filterbedingungen werden AWS Security Hub Ergebnisse in SIRimportiert. Navigieren zu **Alle** > **Integration von AWS-Security-Hub-Ergebnissen** > **AWS Security Hub-Ergebnisse – Import** um die importierten Ergebnisse anzuzeigen.

Definieren Sie Bedingungen, um die Ergebnisse AWS Security Hub zu einem Security Incident zusammenzufassen

Definieren Sie zusätzliche Kriterien für die Incident-Zusammenfassung, die einen eingehenden AWS Security Hub -Ergebnis zu einem vorhandenen SIR-Security Incident

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Wenn Sie für jedes Profil Kriterien für Feldabgleichwerte verwenden, kann diese zusätzliche Zusammenfassung die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Incident-Daten in einem einzigen Security Incident platziert werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein neuer Incident allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird der Incident automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der mit Security Incidents arbeiten, können Sie alle hinzugefügten aggregierten Incidents in einer zugehörigen Liste zu einem Security Incident anzeigen.

Alle zusammengefassten AWS Security Hub Ergebnisse zu einem Security Incident werden in der zugehörigen Liste AWS Security Hub angezeigt. Diese Liste enthält die zugehörigen Zeitstempel und aggregierten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum die Ergebnisse AWS Security Hub den vorhandenen Security Incidents hinzugefügt werden.

Prozedur

1. Um zusätzliche Incident-Feldkriterien zu definieren, die es ermöglichen, einen eingehenden AWS Security Hub -Ergebnis an einen offenen Security Incident anzuhängen, anstatt einen neuen Incident zu erstellen, wählen Sie die Option **Zusammenfassungsbedingungen**.
2. Geben Sie im Feld **Incident-Felder mit übereinstimmenden Werten** die Feldwerte ein, die mit vorhandenen Security Incidents in Ihrer Instanz Now Platform abgeglichen werden sollen.
   Alle Feldwerte, die Sie im Eingabefeld für die Mehrfachauswahl ausgewählt haben, müssen übereinstimmen, damit die Zusammenfassungskriterien erfüllt sind und dieser eingehende Incident an einen vorhandenen Security Incident angehängt werden kann. Diese Auswahl impliziert, dass es sich um eine *UND* -Bedingung handelt, bei der Felder wie erkennbare Elemente und Konfigurationselemente, die mehrere Feldwerte aufweisen können, zugeordnet werden. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Zusammenfassungsbedingungen der AWS Security Hub -Ergebnisse nicht erfüllt, und es wird ein neuer Security Incident erstellt.
3. Um mehrere Feldabgleichbedingungen hinzuzufügen, klicken Sie auf **Neues Kriterium hinzufügen**.
   Die Zusammenfassung erfolgt, wenn eine der von Ihnen definierten Feldbedingungen für die Mehrfachauswahl erfüllt ist. Diese Auswahl impliziert die *ODER* -Bedingung.
4. Um die Arbeitsnotiz für ein neues Ergebnis zu aktualisieren, wenn es einem Security Incident hinzugefügt wird, wählen Sie **Arbeitsnotiz für neues Ergebnis protokollieren**aus.

   Die Arbeitsnotiz protokolliert, dass ein neues Ergebnis hinzugefügt wird, und enthält einen Link zu den Ergebnisdetails. Die Protokoll-Arbeitsnotiz aktualisiert auch weitere Details, die Sie dem Feld „Arbeitsnotiz“ in Ihrem Zuordnungsabschnitt hinzufügen.
5. Klicken Sie zum Konfigurieren des Zeitplans **auf Fortfahren**.

Ergebnisse

Basierend auf den Zusammenfassungsbedingungen werden die Ergebnisse AWS Security Hub zusammengefasst, um einen Incident SIR zu erstellen. Navigieren zu **Alle** > **Integration von AWS-Security-Hub-Ergebnissen** > **AWS Security Hub-Ergebnisse zu Aufgabe** um die Liste der erstellten Security Incidents anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Legen Sie einen Zeitplan fest, um die Ergebnisdaten und Incidents abzurufen, die den Kriterien im Profil entsprechen.

Planen Sie den Abruf des Ergebnisses AWS Security Hub .

Legen Sie einen Zeitplan fest, um die Ergebnisdaten abzurufen und die AWS Security Hub Ergebnisse zu erfassen, die den Kriterien im Profil entsprechen.

Vorbereitungen
Erforderliche Rolle: sn_sni.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie zukünftige AWS Security Hub -Ergebnisse abfragen möchten, die der Konfiguration des AWS Security Hub -Ergebnisprofils entsprechen.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die unterschiedlichen Abfrageintervalle können sich auf die Leistung der AWS Security Hub -Ergebnisintegration auswirken. Planen Sie bei der Zeitplanung, die Systemlast gegen die Dringlichkeit eines incident abzuwägen. Für alle Profile ist ein Standardwert von einer Minute festgelegt. Sie können diese Einstellung je nach Dringlichkeit des incident und der erwarteten Auslastung Ihres Systems ändern.

Alle Warnungen, die dem Incident in einem bestimmten Abfrageintervall hinzugefügt werden, werden verarbeitet und dann an die zugehörigen Listen und Kommentare der Warnungen AWS Security Hub angehängt.

Prozedur
1. Füllen Sie die Felder im Formular „Zeitplanung“ aus.

Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Ergebnisse aus dem -Mandanten AWS Security Hub abrufen.

Formular „Zeitplanung“.

Feld	Beschreibung
Fortlaufende Ergebniserfassung	Fortlaufende Ergebniserfassung, bei der die Instanz Now Platform vom Mandanten AWS Security Hub für neue Incidents abgerufen wird. Security Incidents werden erstellt, wenn ausgelöste Ergebnisse gefunden werden und die Filterkriterien für die Security Incident-Generierung erfüllt sind.
Geschlossene Ergebnisse abfragen	Abrufergebnisse, die gelöst wurden. Diese Ergebnisse werden während der laufenden Incident-Erfassung erfasst.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist.
Legen Sie die Zeit der ersten Ergebniserfassung fest	Erfassung von Ergebnissen, die auf dem konfigurierten Datum und der konfigurierten Uhrzeit basiert. Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung zu definieren. Nachfolgende

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Erfassungen basieren auf dem Zeitraum des Abfrageintervalls.
Zeit der ersten Ergebniserfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Einmaliger Abruf	Aktivieren Sie dieses Kontrollkästchen, um den einmaligen Abruf historischer AWS Security Hub -Ergebnisse zuzulassen und dann den Abgleich der Daten durchzuführen. Wenn Sie dieses Kontrollkästchen aktivieren, ruft die Anwendung alle offenen und geschlossenen AWS Security Hub Ergebnisse für den Zeitraum bis zu ungefähr 90 Tagen ab. Bei der Verarbeitung der Daten werden sowohl laufende Ergebnisse als auch Verlaufsdaten abgerufen, aber die Verarbeitung der laufenden Ergebnisse hat Vorrang vor dem historischen Abruf. Andernfalls kann der Verlaufsabruf je nach Dauer und Anzahl der erfassten Ergebnisse einige Zeit in Anspruch nehmen. **Hinweis:** Die abgerufenen historischen AWS Security Hub -Ergebnisse werden Deduplizierungsprüfungen unterzogen, um Duplikate in der Anwendung Security Incident Response zu verhindern.
Seit Datum	Das Datum, seit dem die historischen Ergebnisse aus AWS Security Huberfasst wurden. **Hinweis:** Die Ergebnisdaten werden ungefähr aus den letzten 90 Tagen abgerufen.

Auf der Seite „Zeitplanung“ können Sie definieren, wie und wann Ergebnisse aus dem Mandanten AWS Security Hub abgerufen werden.

2. Um zur Seite „Weitere Optionen“ zu navigieren, klicken Sie auf **Fortfahren**.

Automatisieren Sie die Aktualisierungen und Abschlüsse AWS Security Hub von Ergebnissen anhand des Incident-Status SIR .

Automatisieren Sie die Aktualisierungen und Abschlüsse von Ergebnissen für AWS Security Hub entsprechend dem Incident-Status SIR. Die AWS Security Hub -Integration verfügt über eine bidirektionale Schnittstelle, die die Erfassung von Ergebnissen ermöglicht, um Security Incidents zu erstellen und den Status der Ergebnisse entsprechend den Änderungen im Incident SIR zu aktualisieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Tragen Sie die Details in das Formular ein.
   Befolgen Sie die Anweisungen, um die Konfiguration für die Aktualisierung AWS Security Hub von -Ergebnissen abzuschließen, wenn Sie in SIReinen Security Incident erstellen oder schließen.

Formular „Automatisieren von Incident-Updates“.

Kategorie	Feld	Beschreibung
Status aktualisieren	SIR Incident-Status	Zeigt eine Liste von Incident-Status SIR an. Wählen Sie eine Option aus dieser Liste aus, um sie einem Security Hub Ergebnisstatus zuzuordnen.
	Security Hub Ergebnisstatus	Zeigt eine Liste von Security Hub Workflow-Status an. Der Workflow-Status eines Ergebnisses wird am AWS Security Hub aktualisiert, wenn sich der entsprechende Incident-Status im SIR-Status ändert.
Priorität aktualisieren	SIR Incident-Priorität	Zeigt eine Liste von SIR Incident-Prioritätsstufen an. Wählen Sie eine Option aus dieser Liste aus, um sie einer Security Hub -Ergebnisprioritätsstufe zuzuordnen.
	Security Hub Ergebnispriorität	Wählen Sie eine Option aus der Liste der Security Hub Schweregrade aus. Der Schweregrad eines Ergebnisses wird am AWS Security Hub aktualisiert, wenn sich die entsprechende Priorität des Security Incident ändert.
Arbeitsnotizen aktualisieren	Wählen Sie diese Option aus, um den Abschnitt „Notizen“ einesSecurity Hub zu aktualisieren, wenn eine Arbeitsnotiz für den entsprechenden IncidentSIR aktualisiert wird. Der Abschnitt „Arbeitsnotizen“ in SIR hat eine Beschränkung von 512 Zeichen, da der Abschnitt „Notizen“ eines Ergebnisses Security Hub dies unterstützt.	
Zusätzliche Kommentare aktualisieren	Wählen Sie diese Option aus, um den Abschnitt „Kommentare zu den Ergebnissen AWS Security Hub “ mit den zusätzlichen Kommentaren zu aktualisieren, die Sie im Incident SIR angegeben haben.	
Lösungsnotizen aktualisieren	Wählen Sie diese Option aus, um den Abschnitt AWS Security Hub mit den Abschlusskommentaren mit den von Ihnen bereitgestellten Lösungshinweisen zu aktualisieren, wenn der Incident SIR gelöst ist.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Jede Aktualisierung aus den Arbeitsnotizen überschreibt die letzte Aktualisierung im Notizenabschnitt eines Security Hub -Ergebnisses. Wir empfehlen Ihnen, relevante Arbeitsnotizen in einem Incident SIR hinzuzufügen.

2. Wählen Sie **Fertigstellen** aus.

Nächste Maßnahme
Das Profil wechselt in den Status Warten. Wenn in der Bestätigungsmeldung angezeigt wird, dass das Setup und die Konfiguration abgeschlossen sind, können Sie das Profil aktivieren.

FormularSIR nach einer AWS Security Hub -Ergebniserfassung

Nachdem Now Platform das Ergebnis AWS Security Hub erfasst hat, wird ein Security Incident erstellt, und die Aktualisierungen werden an diesem Security Incident-Datensatz vorgenommen.

Arbeitsnotizen

Eine Arbeitsnotiz wird veröffentlicht, wenn ein Incident aggregiert wird und Sie die Option **Arbeitsnotiz für neues Ergebnis protokollieren** in Definieren Sie Filter- und Zusammenfassungskriterien für die Erfassung der Ergebnisse AWS Security Hub von [].konfiguriert haben.

Sie können auch den internen Datensatz des Ergebnisimports anzeigen, der die Rohdaten zum Incident enthält.

Wenn Sie auf den Link **Hier klicken** klicken, können Sie den Datensatz in der Umgebung AWS Security Hub anzeigen. Das folgende Beispiel zeigt den Datensatz in der Umgebung AWS Security Hub.

Aggregierte AWS Security Hub Ergebnisse

Aggregierte AWS Security Hub Ergebnisse anzeigen: Zeigen Sie die Incidents an, die zum Security Incident aggregiert werden. Navigieren zu **Alle zugehörigen Listen anzeigen** > **Aggregierte AWS Security Hub-Ergebnisse**.

Security Incident erstellen: Wählen Sie einen Incident aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie dann auf **Security Incident erstellen**. Durch diese Option wird ein neuer Security Incident für den Incident erstellt. Dieser Incident wird aus dem übergeordneten Security Incident deaggregatiert.

Integration mit Carbon Black - Incident Enrichment

Verwenden Sie die Carbon Black-Integration, um Security Incidents mithilfe von APIs zu untersuchen und darauf zu reagieren, um Endpunkte im Zusammenhang mit Security Incidents abzufragen und mit ihnen zu interagieren.

Suchen Sie nach Ressourcen für die Integration mit Carbon Black Incident Enrichment

- Erste Schritte mit der Integration Carbon Black - Incident Enrichment
- Security Operations Carbon Black-Integration – Flow zum Abrufen laufender Prozesse
- Security Operations Carbon Black Integration – Flow zum Isolieren von Hosts
- Security Operations Carbon Black Integration: Flow zum Entfernen der Hostisolierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationskonzepte verstehen

- Arten von ServiceNow Integrationen bereitgestellt
- Security Operations Workflow-Auslöser

Holen Sie sich Hilfe von ServiceNow-Ressourcen

- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- Führen Sie ein Upgrade auf Madrid durch

Erste Schritte mit der Integration Carbon Black - Incident Enrichment

Die Ergänzung von Carbon Black Incidents erleichtert die Untersuchung von Security Incidents, indem Protokolle nach potenziell schädlichen Indikatoren abgefragt werden. Bevor Sie die Integration Carbon Black - Incident Enrichment verwenden können, müssen Sie sie von ServiceNow Store herunterladen und die entsprechende Endpunkt-Basis-URL und den MID-Server hinzufügen.

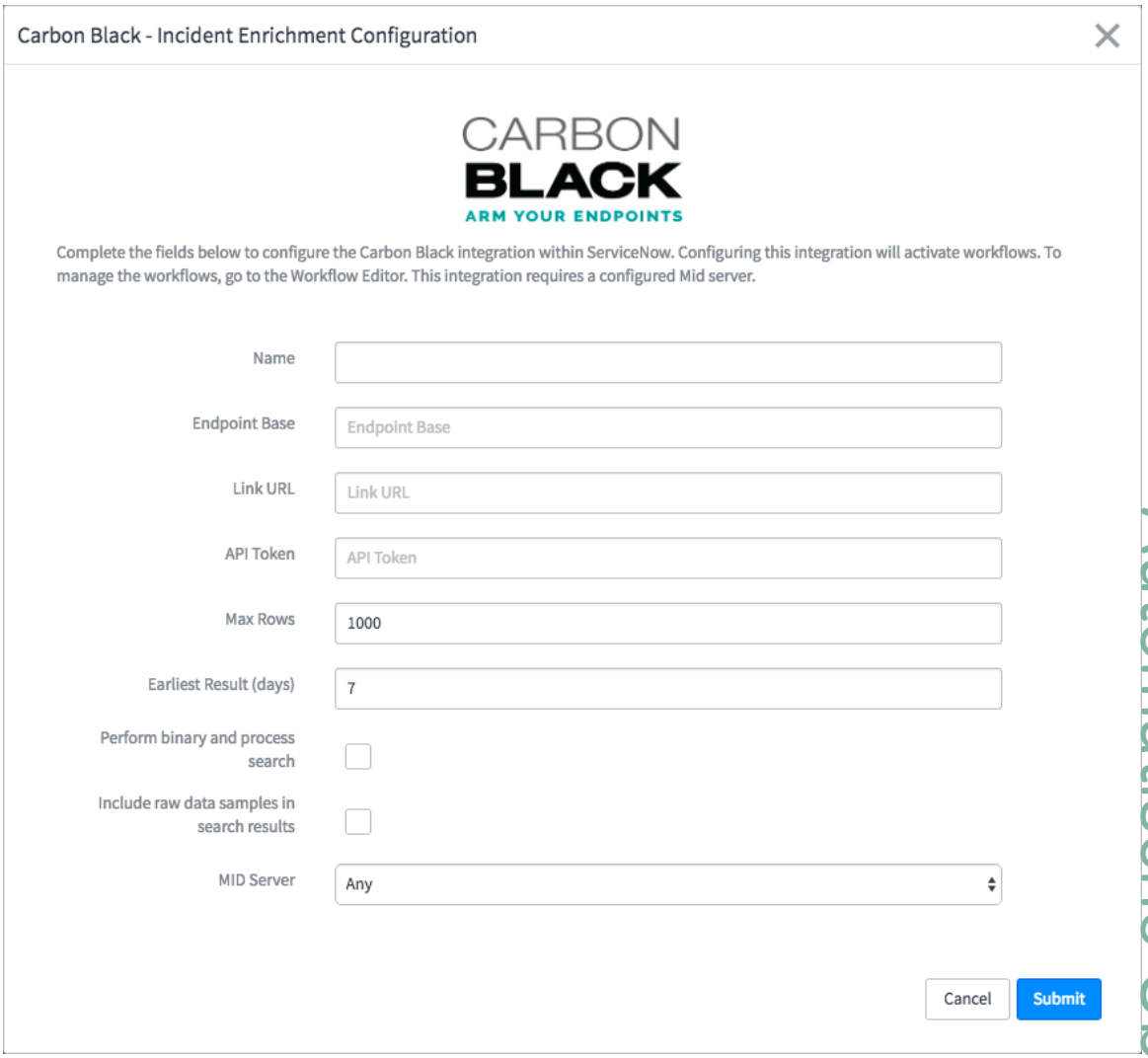
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn der Download abgeschlossen ist, rufen Sie die Website Carbon Black auf, und rufen Sie in Ihrem Profil die Endpunkt-Basis-URL und das API-Token ab.
3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
4. Klicken Sie auf der Karte Carbon Black – Incident Enrichment auf **Konfigurieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Endpunktbasis	Die Endpunkt-URL, die Sie von der Carbon Black-Website erhalten haben.
Link-URL	Die Link-URL, die eine Verknüpfung zu einer Carbon Black-Instanz herstellt, falls verfügbar.
API-Token	Das API-Token, das Sie auf der Carbon Black-Website erworben haben.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. Der Standardwert ist 1000 Zeilen.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.
Binär- und Prozesssuche durchführen	Wählen Sie diese Option aus, um binäre Suchen nach Binärdateien wie Datei-Hashes und Prozesssuchen nach .exe-Prozessen durchzuführen, die möglicherweise ausgeführt wurden.
Rohdatenmuster in	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchergebnissen berücksichtigen	Einstellung in der **Anzahl der Zeilen der Rohdateneigenschaft** in den Security Incident Response-Eigenschaftenab.
MID-Server	Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

Integration mit Carbon Black

Die Carbon Black-Integration ermöglicht es Ihnen, Security Incidents mithilfe von APIs zu untersuchen und darauf zu reagieren, um Endpunkte im Zusammenhang mit Security Incidents abzufragen und mit ihnen zu interagieren.

Erkunden

- Security Incident Response-Integrationen
- Integration mit Carbon Black - Incident Enrichment

Einrichten

Erste Schritte mit der Carbon Black-Integration

Verwenden

- Security Operations Workflow-Auslöser
- Zeigen Sie betroffene Elemente für einen Security Incident an
- Security Operations – Flow für laufende Prozesse abrufen
- Security Operations Carbon Black-Integration – Flow zum Abrufen laufender Prozesse
- Zeigen Sie betroffene Elemente für einen Security Incident an
- Blockierungsanforderung ausführen
- Security Operations Integration – Anforderungs-Flow blockieren
- Führen Sie „Host isolieren“ aus

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Security Operations Carbon Black Integration – Flow zum Isolieren von Hosts
- Security Operations Carbon Black Integration: Flow zum Entfernen der Hostisolierung

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der Carbon Black-Integration

Carbon Black ist ein erweitertes Sicherheitssystem, das sich problemlos in Security Operationsintegrieren lässt. Bevor Sie die Carbon Black-Integration verwenden können, müssen Sie die Integration von ServiceNow Store herunterladen und die entsprechende Endpunktbasis und das entsprechende API-Token hinzufügen.

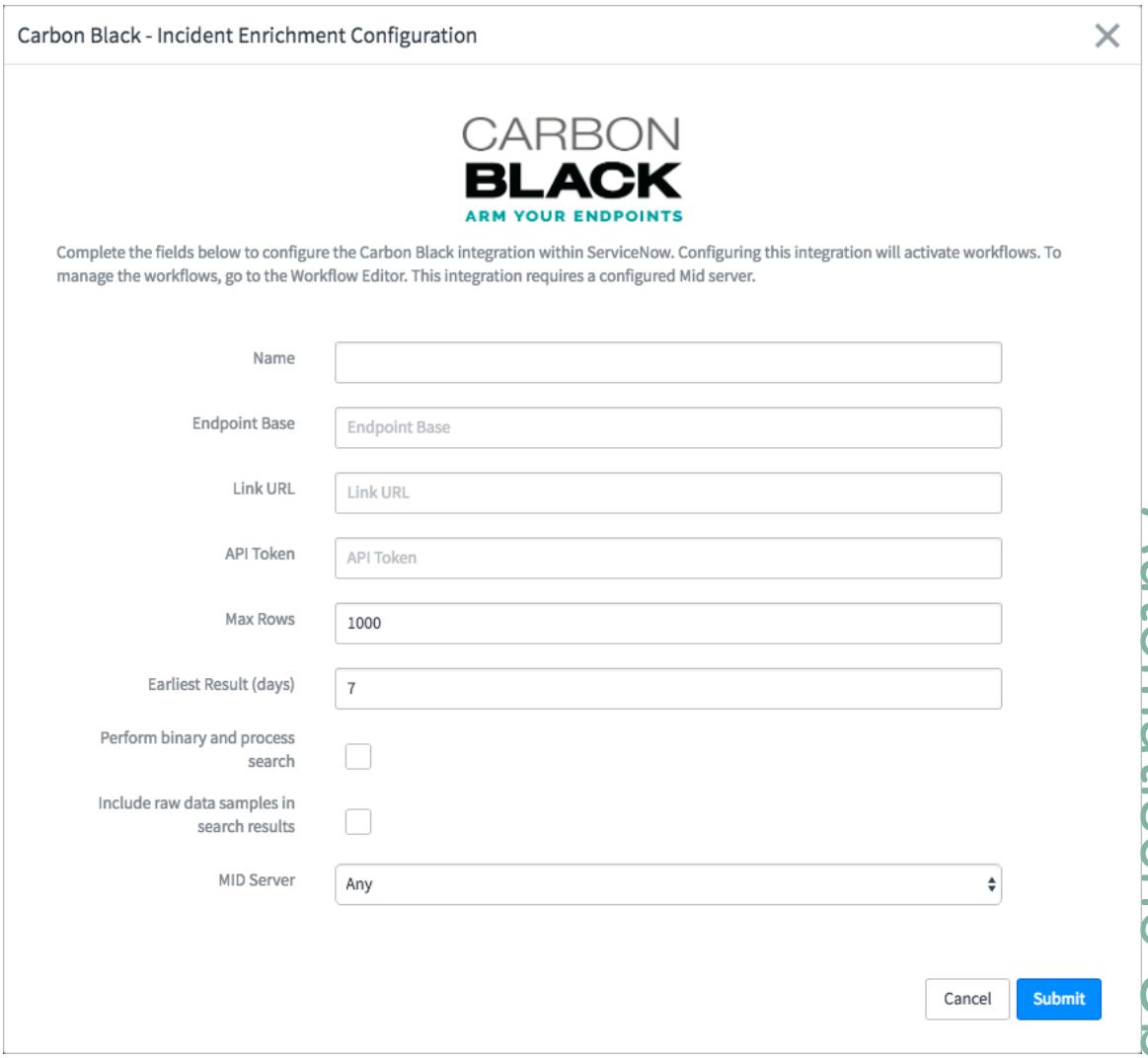
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, rufen Sie die Website Carbon Black auf, und rufen Sie in Ihrem Profil die Endpunkt-Basis-URL und das API-Token ab.
3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte Carbon Black auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Endpunktbasis	Die Endpunktbasis, die Sie von der Carbon Black-Website bezogen haben.
API-Token	Das API-Token, das Sie auf der Carbon Black-Website erworben haben.
MID-Server verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn es noch nicht aktiviert ist.
MID-Server	Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.
Hostisolierung aktivieren	Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, dass ausgewählte Konfigurationselemente von der Registerkarte der zugehörigen Liste **„Konfigurationselemente“** in einem Security Incident isoliert werden.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

Integration mit Check Point Anti-Bot - Email Parser

Die Integration von Prüfpunkt-Anti-Bot – E-Mail-Parser wird durch einen E-Mail-Parser unterstützt, der E-Mail-Benachrichtigungen von Prüfpunkt-Anti-Bot verarbeitet, um Security Incidents zu erstellen und Ergänzungs- und Antwort-Workflows zu steuern.

Konfigurieren Sie die Check Point Anti-Bot – E-Mail Parser Integration

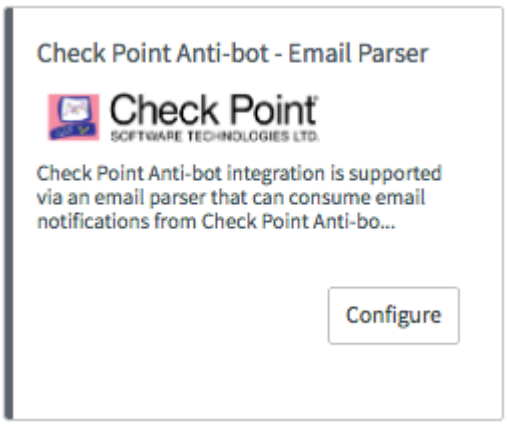
Die Integration des Prüfpunkt-Anti-Bots mit E-Mail-Parser verwendet E-Mail-Benachrichtigungen, um Ergänzungs- und Antwort-Workflows zu unterstützen.

Vorbereitungen
Erforderliche Rolle: sn_si_admin

Warum und wann dieser Vorgang ausgeführt wird
Zur Verwendung für die Integration wird eine Prüfpunkt-Anti-Bot-E-Mail-Parser-Vorlage bereitgestellt. Es muss konfiguriert und aktiviert werden, bevor die Integration stattfindet. Durch das Aktualisieren des Parsers wird er aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.



2. Klicken Sie auf der Karte Prüfpunkt-Anti-Bot – E-Mail-Parser auf **Konfigurieren**.
3. Klicken Sie im Dialogfeld **Prüfpunkt-Anti-Bot – E-Mail-Parser-Konfiguration** auf den Link **E-Mail-Parser konfigurieren**.
4. Klicken Sie auf den Link **Prüfpunkt-Anti-Bot,** um die Einstellungen im bereitgestellten E-Mail-Parser für Vorlagen zu bearbeiten.
   Füllen Sie mindestens das Feld E-Mail ist von aus. Informationen zum Erstellen eines E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**.
6. Klicken Sie im Formular **„E-Mail-Parser“auf Aktualisieren**.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu **Integrationskonfigurationen**zurückkehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Check Point Next Generation Threat Prevention Integration

Dieses Dokument beschreibt die Schritte, die erforderlich sind, um Check Point Next Generation Threat Prevention-Funktionen (NGTP) in ServiceNow® Security Incident Response (SIR) zu integrieren, damit Anwendungen ordnungsgemäß funktionieren.

Nach der Installation und Konfiguration verwendet der Security Incident-Analyst diese Integration, um schädliche IP-Adressen, URLs und Domänen mithilfe von Sperranforderungslistenfunktionen mit den -Produkten ServiceNow Security Incident Response (SIR) zu blockieren. Diese Sperranforderungsliste ist auf Prüfpunkt-Gateways als anwenderdefinierter Intelligenzfeed konfiguriert. Die Funktion „Anwenderdefinierte Intelligenzfeeds“ bietet die Möglichkeit, der Next Generation Threat Prevention-Engine anwenderdefinierte Cyber Intelligence-Feeds hinzuzufügen. Sie ermöglicht das Abrufen von Feeds von einem Drittanbieterserver, in diesem Fall der Anwendung ServiceNow Security Incident Response, direkt an das Check Point Next Generation Gateway, was von Anti-Virus- und Anti-Bot-Blades erzwungen wird. Der Security Incident Response-Analyst erstellt Einträge für die Check Point-Sperrliste aus erkennbaren Elementen, die in ServiceNow SIR-Security Incidents als schädlich eingestuft wurden.

Bei den meisten Implementierungen handelt es sich bei einer Sperranforderungsliste um eine CSV-Datei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihre Now Platform-Instanz, die es der Check Point Next Generation Threat Prevention Engine ermöglicht, die Liste der zu blockierenden IP-Adressen, URLs und Domänen abzurufen.

Um das Blockieren erkennbarer Elemente auf dem Prüfpunkt-Gateway zu erzwingen, stellen Sie sicher, dass die Bedrohungsverhinderungsrichtlinie mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert ist. Wenn die Sperrlisteneinträge geändert werden, importiert die Threat Prevention Engine die Liste dynamisch zum konfigurierten Intervall und erzwingt die Richtlinie ohne Konfigurationsänderung oder Commit auf der Firewall. Für diese Integration hat Now Platform eine Tabelle mit Sperrlisteneinträgen erstellt, die vom autorisierten Check Point Next Generation Gateway in den konfigurierten Abrufintervallen abgerufen werden.

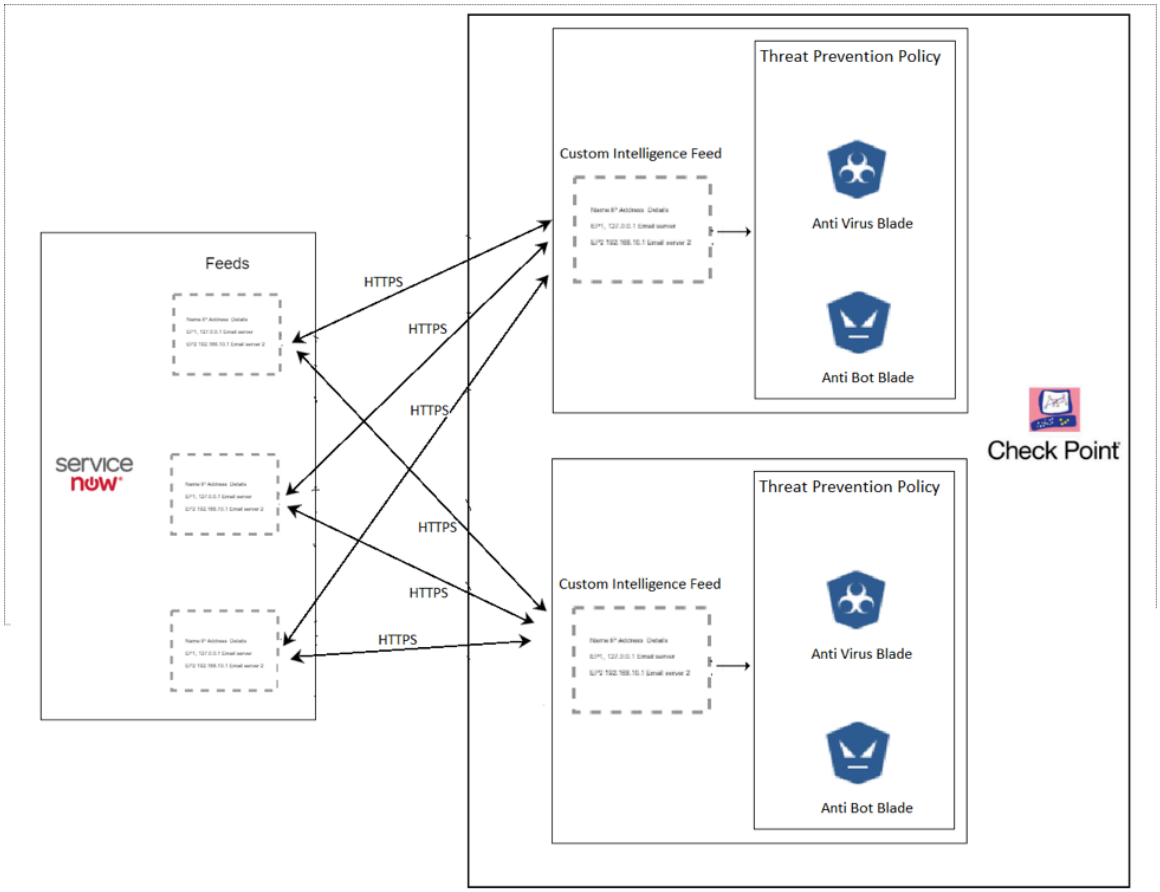
Die Integration umfasst die folgenden Funktionen:

- Flexibilität zum Erstellen mehrerer Sperrlisten, die für mehrere Prüfpunkt-Gateways gelten.
- Detaillierte Berichte zu den Arten von blockierten Websites (Phishing, Malware und auf der Zulassungsliste aufgeführte Websites).
- Tagging von Now Platform-Security Incidents mit Sperrlisteneinträgen nach erkennbarem Elementtyp (URL, Domäne, IP-Adresse).
- Konfigurieren von Ablaufzeiträumen für Sperrlisten, um die Größe der Sperrliste durch automatisches Ablaufen oder Entfernen älterer Einträge aufrechtzuerhalten.
- Sperrlisteneinträge werden in verschiedenen Sperrlisten durchsucht.
- Verknüpfen von Sperrlisteneinträgen mit Datensätzen erkennbarer Elemente und Security Incidents, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert wird.

Diagramm der Integrationsarchitektur

Nachfolgend finden Sie das allgemeine Architekturdiagramm, das die beteiligten Komponenten und Integrationspunkte zwischen NOW Platform und Check Point Systems darstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Das Check Point Systems-Logo, das Anti-Virus-Blade-Bild und das Anti-Bot-Blade-Bild stammen von Check Point Systems ©. Sie sind Eigentum von Prüfpunktsystemen.

Plugins

Zur Integration muss das Plugin Security Incident Response (com.snc.security_incident) aktiviert werden.

So installieren Sie Plugins Security Incident Response :

1. Melden Sie sich mit Ihren HI-Anmeldeinformationen bei Ihrer -Instanz an.
2. Vergewissern Sie sich, dass Sie über die Administratorrolle (admin) verfügen.
3. Navigieren Sie in Ihrer Instanz zu Systemdefinition > Plugins.
4. Wählen Sie Security Incident Response aus, und klicken Sie darauf.

Sobald diese Plugins installiert wurden, können Sie das neue Check Point-Integrations-Plugin aus dem ServiceNow Store hochladen und die folgenden Konfigurationsanweisungen befolgen.

Unterstützte Prüfpunkt-Betriebssystemversionen

Diese Integration erfordert den anwenderdefinierten Intelligenzfeed der Prüfpunkt- und Anti-Bot- und Anti-Virus-Blades. Diese werden ab R80.20 und höher unterstützt. Installieren Sie den Hotfix für die Funktion „Custom Intelligence“ mit der Bezeichnung Check Point R80.10 Jumbo SF (Version 121 und höher). Weitere Informationen zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produktkompatibilitätsmatrix finden Sie im Installationsabschnitt der Check Point-Dokumentation für anwenderdefinierten Intelligenzfeed.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Stellen Sie nach der Installation des Hotfixes sicher, dass die folgenden Befehle auf dem Prüfpunkt-Gateway verfügbar sind. Stellen Sie eine SSH-Verbindung zum Gateway her, und melden Sie sich im Expertenmodus an.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Unterstützte Versionen von ServiceNow

Release-Version San Diego oder höher wird unterstützt.

Referenzen

Nachfolgend finden Sie einige Prüfpunktreferenzen, die beim Einrichten der Voraussetzungen nützlich sind.

1. Funktion für anwenderdefinierte Intelligenzfeeds – https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Informationen zum Einrichten von Anti-Bot- und Anti-Virus-Blades finden Sie im Prüfpunkt-Benutzerhandbuch. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Um die HTTPS-Inspektion für Check Point einzurichten, folgen Sie dem Link unten. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Berechtigungen und Rollen

Die folgenden ServiceNow-Rollen sind erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Administrator (admin) für die Installation des Integrationsanwendungs-Plugins
- Security Incident-Administrator (sn_si.admin) für die Erstellung von Sperrlisten in ServiceNow und die Genehmigung von Anforderungen zum Hinzufügen und Deaktivieren von Sperrlisteneinträgen.
- Sicherheitsanalyst (hier auch als SOC-Analyst bezeichnet, sn_si.analyst) für die Erstellung und Verwaltung von Sperrlisteneintrags-Datensätzen.

Weitere Informationen zum Zuweisen der Rolle „Sicherheitsanalyst“ finden Sie auf der ServiceNow-Dokumentationswebsite unter Security Operations>Security Incident Response> Sicherheitsanalysten zuweisen.

Setup von Check Point NGTP

Bevor Sie die Check Point NGTP -Integration verwenden können, müssen Sie ein API-Konto erstellen, Richtlinien einrichten und die Integration aktivieren.

Erstellen Sie ein API-Konto für die Integration Check Point NGTP .

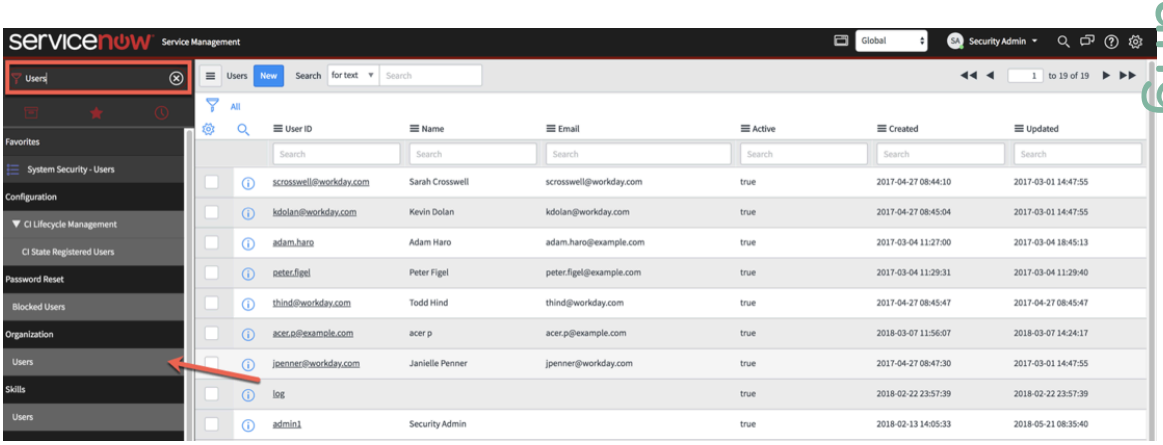
Für diese Integration ist eine API-Kontorolle in Ihrer Now Platform-Instanz erforderlich. Der diesem Account zugeordnete Anwendername und das Passwort werden auf der Now Platform erstellt und in Check Point eingegeben, damit sich der Check Point beim Abrufen von Sperrlisteneinträgen bei Now Platform authentifiziert.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der Now Platform-Administrator erstellt eine API-Kontorolle (sn_sec_checkpoint.api_account_access). Dieser Account wird ausschließlich für die Eingabe von Anmeldeinformationen verwendet, die für die Authentifizierung bei Check Point erforderlich sind, damit das Gateway Sperrlisten von der Now Platform abrufen kann. Dieser Account ist ein separater, eindeutiger API-Anwenderaccount in der Now Platform-Instanz und wird dem Check Point-Administrator zugewiesen.

Prozedur

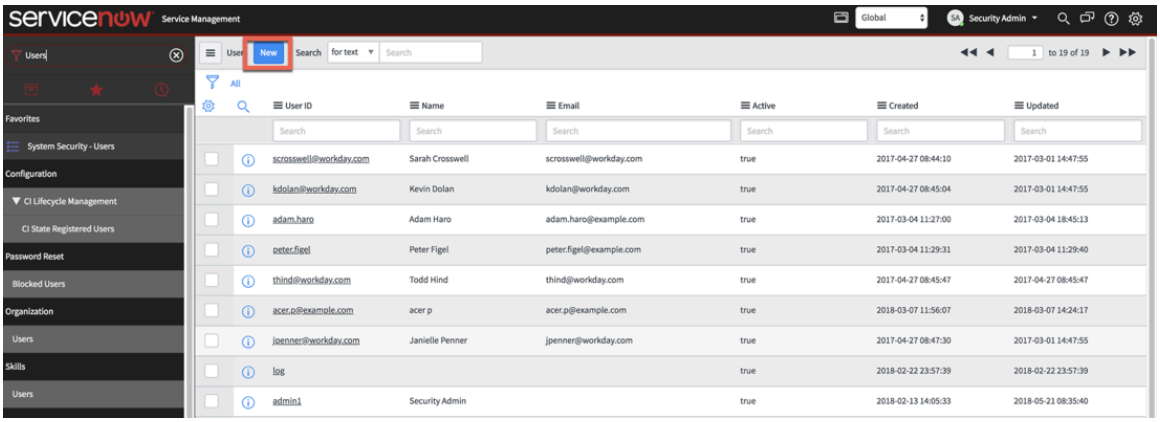
1. Navigieren zu **Alle** > **Organisation** > **Anwender**.
2. Klicken Sie auf das Modul **Benutzer**.



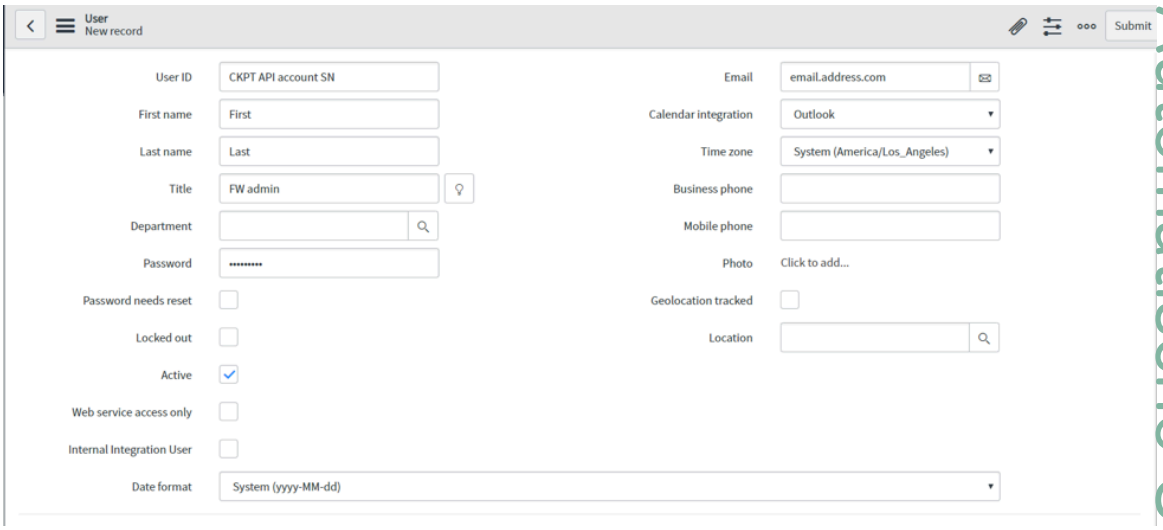
3. Klicken Sie in der angezeigten Benutzerliste auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ein neues Formular wird angezeigt.



4. Füllen Sie das Formular nach Bedarf aus.

Hinweis:

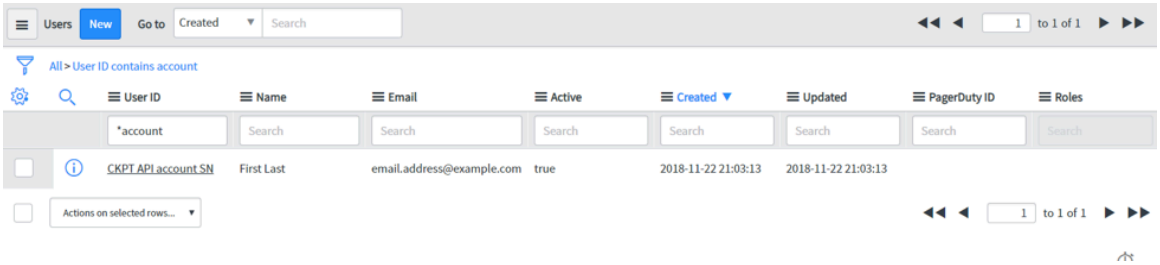
Die in der folgenden Tabelle und Abbildung gezeigten Werte für Anwender-ID-Titel und E-Mail-Adresse sind Beispielwerte.

Feld	Beschreibung
Anwender-ID	Eindeutige Anwender-ID für die Rolle in Ihrer Now Platform-Instanz. Diese Anwender-ID wird im Feld **Anwendername** im Abschnitt **„Client-Authentifizierung“** des Prüfpunkt-Gateways für die Sperrlistenkonfiguration eingegeben. Ein Beispiel ist der CKPT-API-Account SN.
Vorname	Person, die Sie zuweisen
Nachname	Person, die Sie zuweisen
Titel	Stellenbezeichnung, z. B. FW-Administrator.
Passwort	Eindeutiges Passwort, das für diese Rolle erstellt wurde. Dieses Passwort wird im Feld **Passwort** im Abschnitt **„Client-Authentifizierung“** der Sperrlistenkonfiguration auf dem Prüfpunkt-Gateway eingegeben.
E-Mail	Eindeutige E-Mail-Adresse

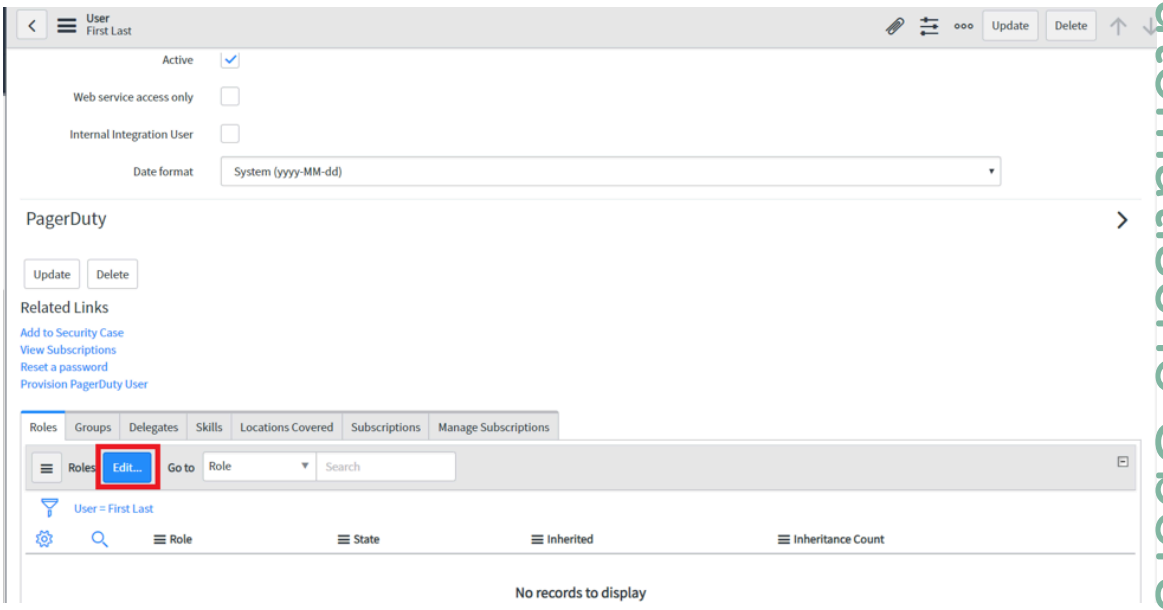
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung können Sie die Rolle zuweisen.
6. Klicken Sie in der Liste Benutzer in der Spalte Benutzer-ID auf den Namen der von Ihnen eingegebenen Benutzer-ID, z. B. CKPTAPI-Konto-SN.



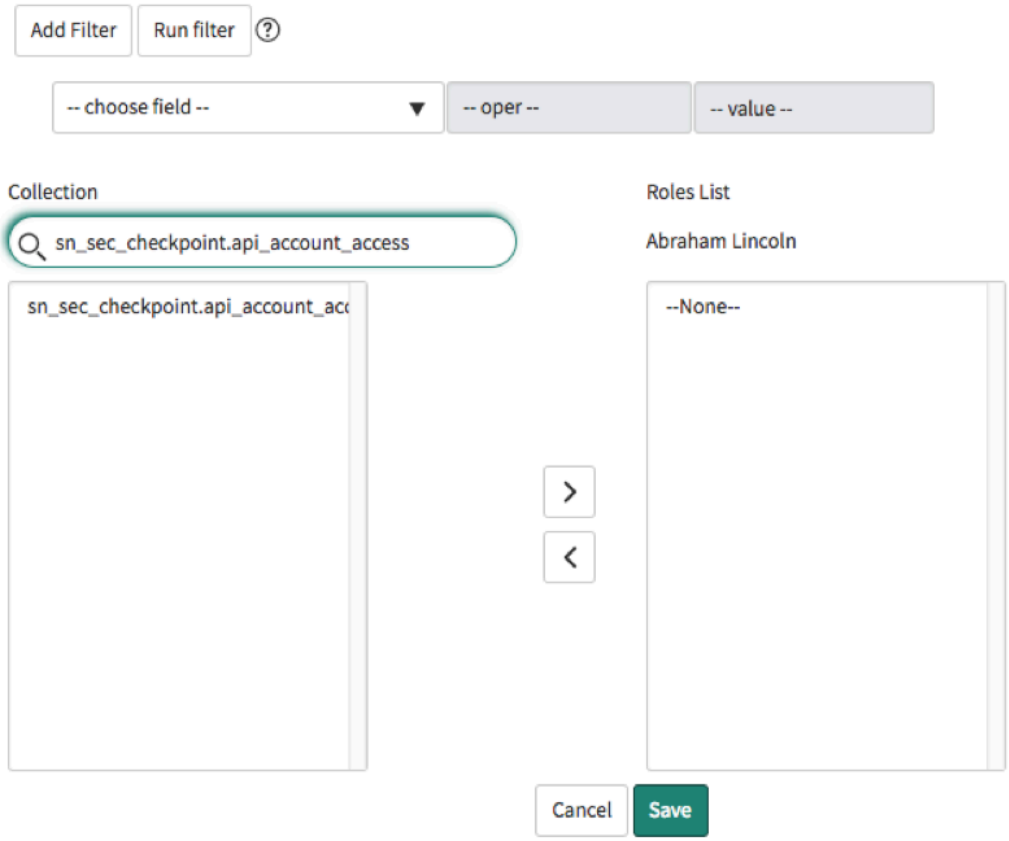
7. Klicken Sie im geöffneten Datensatz im Abschnitt „Rollen“ auf **Bearbeiten**.



8. Geben Sie im angezeigten Formular **„Mitglieder bearbeiten“** im Feld **Sammlung** den Wert sn_sec_checkpoint.api_account_access ein.

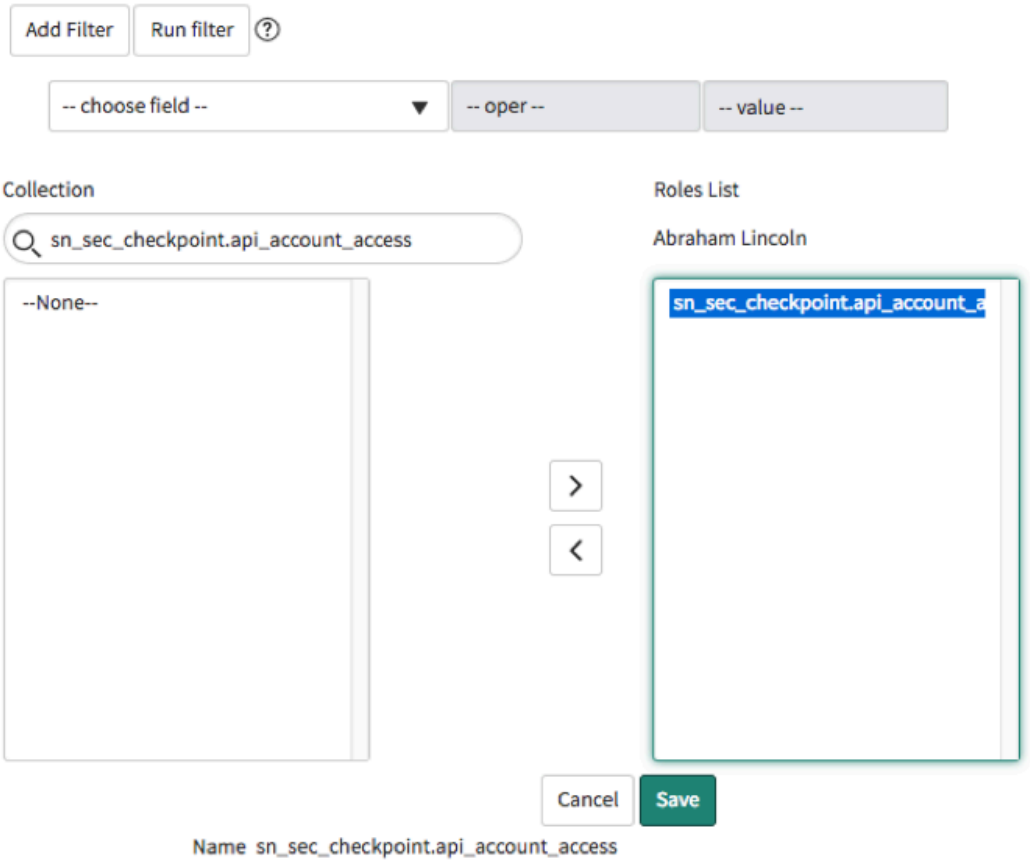
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Wählen Sie in der Spalte **Sammlung** die Option aus, und verschieben Sie sn_sec_checkpoint.api_account_access in die **Rollenliste**.
10. Klicken Sie auf **Speichern**.
11. Navigieren Sie zu **Anwender**, und klicken Sie in der Spalte **Anwender** der Liste auf den ID-Namen, den Sie für die Rolle erstellt haben (CKPT-API-Konto-SN).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



12. Der Benutzerdatensatz wird angezeigt. Dieser Datensatz verifiziert, ob der Anwenderaccount zugewiesen wurde.

Integration mit Check Point NGTP einrichten

Führen Sie die folgenden Schritte aus, um die Integration Check Point Next Generation Threat Prevention einzurichten. Dadurch wird sichergestellt, dass die Voraussetzungen dafür vorhanden sind, dass die Integration funktioniert.

Vorbereitungen
Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

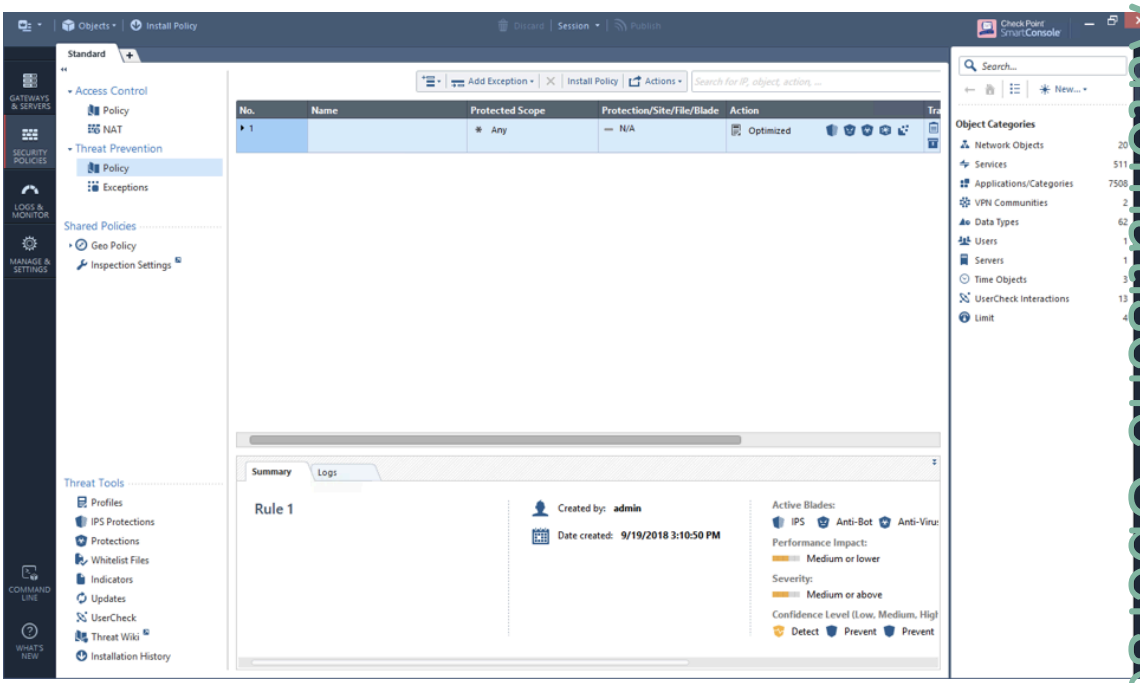
Prozedur

1. Stellen Sie sicher, dass die Bedrohungsabwehrrichtlinie mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert ist.
   Ausführliche Informationen zum Einrichten von Anti-Bot- und Anti-Virus-Blades finden Sie im Prüfpunkt-Benutzerhandbuch im Referenzabschnitt.

   Hinweis:
   Die Bilder in diesem Thema sind privilegiert und proprietär und werden mit Genehmigung von Check Point Software Technologies, Ltd. verwendet.

   a. Melden Sie sich bei **der Smart Console**an.

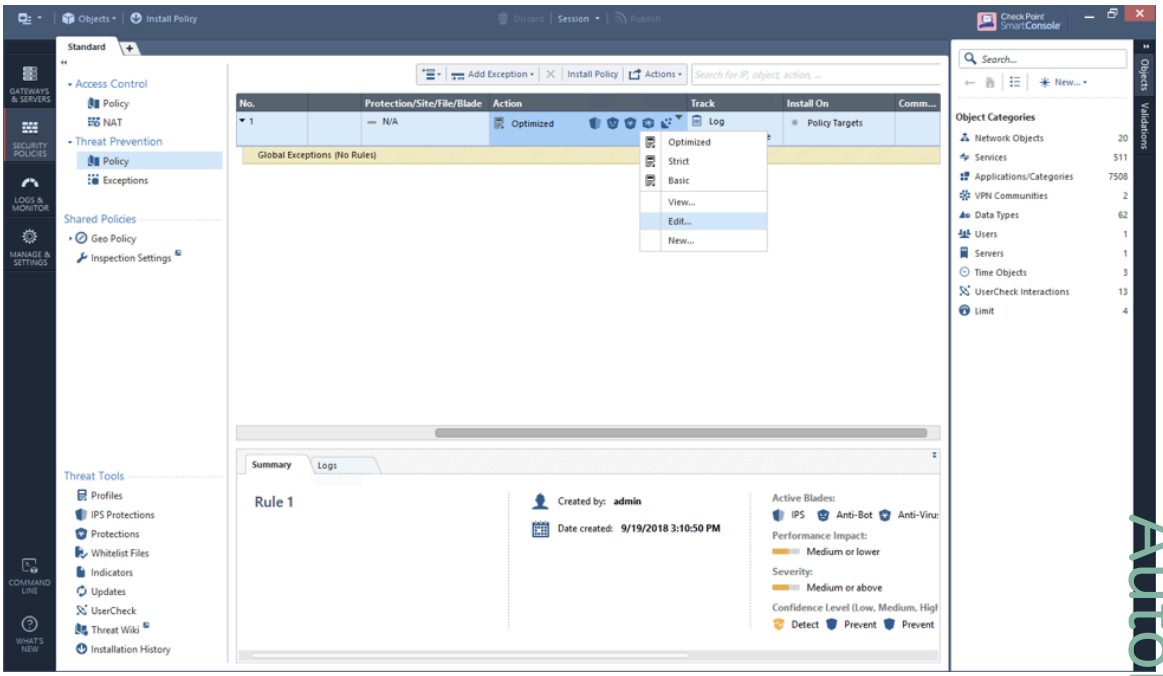
   b. Navigieren zu **Sicherheitsrichtlinien** > **Bedrohungsabwehr** > **Richtlinie**.



   c. Öffnen Sie die Bedrohungsabwehrrichtlinie im Bearbeitungsmodus.

Automatische Übersetzung

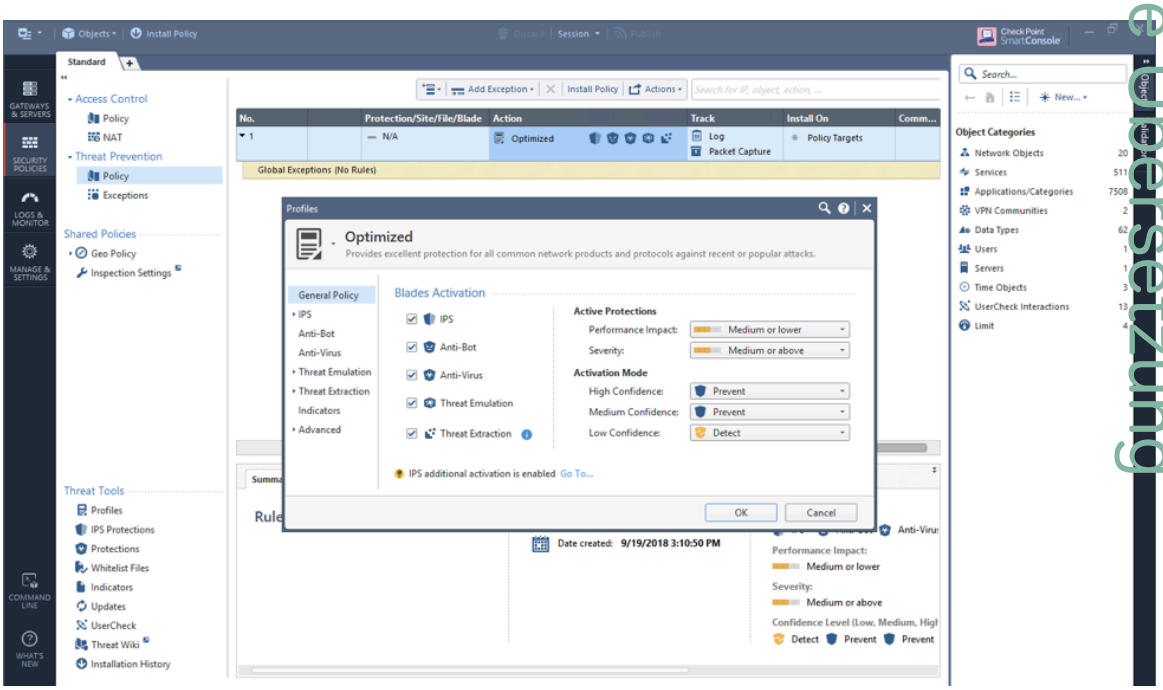
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Aktive Schutzmaßnahmen # Schweregrad muss „Mittel oder höher“ sein

e. Aktivierungsmodus # Hohe Konfidenz muss „Verhindern“ sein.

f. Aktivierung der Klingen # Anti-Virus und Anti-Bot sollten ausgewählt werden.



g. Veröffentlichen Sie die Änderungen (falls vorhanden), und installieren Sie die Richtlinie.

2. Wenn dies noch nicht konfiguriert ist, sollten anwenderdefinierte Intelligenzfeeds nach der Aktivierung von Anti-Bot- und Anti-Virus-Blades hinzugefügt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

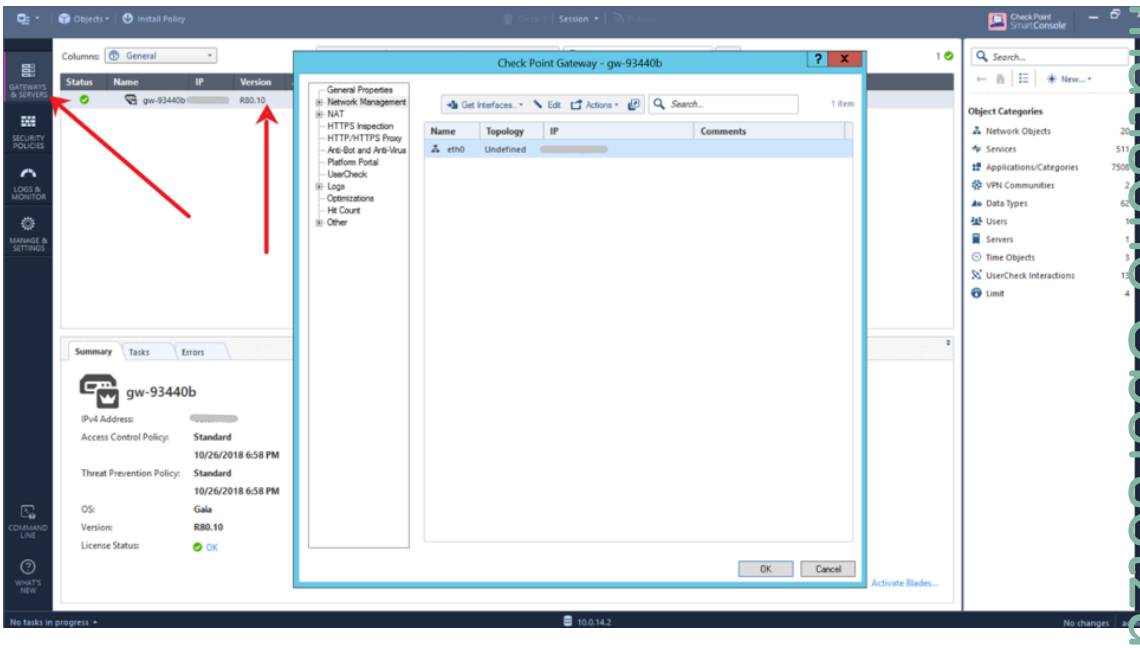
Weitere Informationen finden Sie im Abschnitt zur Installation in der Dokumentation zur anwenderdefinierten Intelligenzfeed-Funktion von Check Point.https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Wenn dies noch nicht konfiguriert ist, richten Sie das Prüfpunkt-Gateway so ein, dass der gesamte Internetverkehr über HTTP-Proxy weitergeleitet wird (bei Konfiguration von HTTPS-Inspektion).

Hinweis:
Für die URL-Blockierung auf Prüfpunkt-NGTP müssen bestimmte Einstellungen sichergestellt werden. HTTPS-Internetdatenverkehr verwendet das SSL-Protokoll (Secure Sockets Layer) und ist aus Datenschutzgründen verschlüsselt. HTTPS kann jedoch schädlichen Datenverkehr verbergen, der hätte blockieren müssen. Damit Prüfpunkt-Gateway Einblick in den HTTPS-Datenverkehr erhält, leiten Sie den Datenverkehr entweder über einen HTTP-Proxy, oder richten Sie eine HTTPS-Inspektion ein (empfohlen). In diesem Abschnitt werden die Schritte beschrieben, die Sie ausführen müssen, um einen HTTP-Proxy auf dem Prüfpunkt-Gateway einzurichten.

a. Melden Sie sich bei **der Smart Console**an.

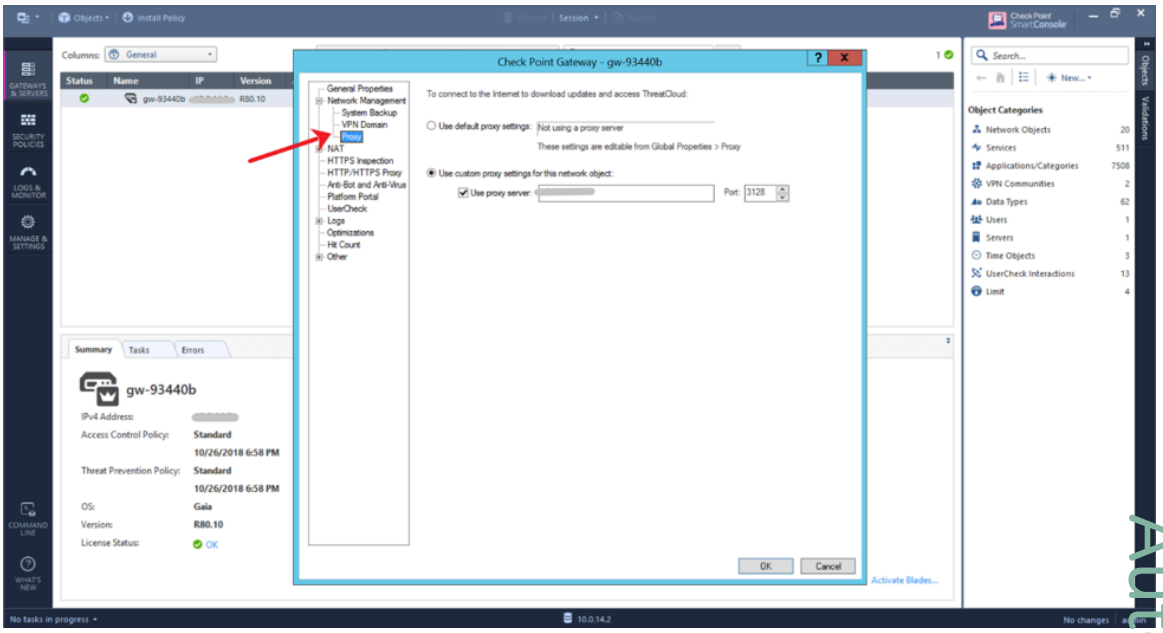
b. Navigieren Sie zu **Server und Gateways**, und doppelklicken Sie auf den entsprechenden Server.



c. Navigieren zu **Netzwerkverwaltung** > **Proxy**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Geben Sie die Proxy-Details an, die für die Weiterleitung des HTTP-Datenverkehrs verwendet werden sollen.

e. Stellen Sie sicher, dass HTTP-Anforderungen vom Client-Endpunkt über den HTTP-Proxy erfolgen.

4. Wenn dies noch nicht konfiguriert ist, aktivieren Sie die HTTPS-Inspektion (wenn ein HTTP-Proxy konfiguriert ist).
Wenn der Großteil des Datenverkehrs über SSL erfolgt, wird die Verwendung des HTTPS-Inspektionsblatts empfohlen. Dadurch wird der Datenverkehr für GW transparent. Aktivieren Sie die HTTPS-Inspektion auf dem Prüfpunkt-Gateway wie folgt.

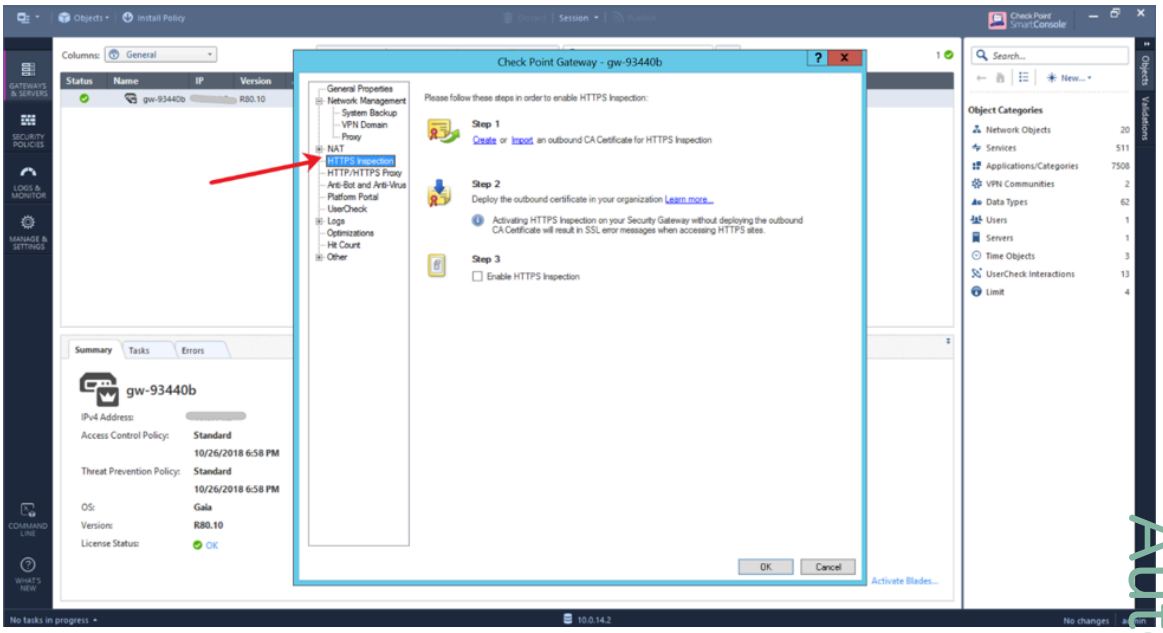
a. Melden Sie sich bei **der Smart Console**an.

b. Navigieren Sie zu **Server und Gateways**, und doppelklicken Sie auf den entsprechenden Server.

c. Navigieren Sie zu **HTTPS Inspektion**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Befolgen Sie die Schritte zum Konfigurieren der HTTPS-Inspektion im Prüfpunkt-Benutzerhandbuch.

Aktivieren Sie die Check Point NGTP -Integration

Wenn Sie die Anwendung nicht installiert haben, befolgen Sie die Anweisungen zur Installation.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie die Anwendung installieren möchten.
2. Navigieren zu **Systemanwendungen** > **Anwendungen**.
3. Klicken Sie auf die Registerkarte **Downloads**.
   Eine Liste der für die Installation verfügbaren Anwendungen wird angezeigt.
4. Suchen Sie die Anwendung Check Point Next Generation Threat Prevention, wählen Sie sie aus, und klicken Sie auf **Installieren**.
   Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Arbeiten mit Sperrlisten

Die ServiceNow Check Point Next Generation Threat Prevention Integration unterstützt Sperrlisten, die erkennbare IP-, URL- und Domänenelemente akzeptieren.

ServiceNow Die konfigurierte Sperrliste von ist eine CSV-Datei, die auf einem externen Webserver gehostet wird, der für diese Integration die Now Platform-Instanz ist. Der anwenderdefinierte Intelligenzfeed wird auf dem Prüfpunkt-Gateway konfiguriert, das die IP-Adressen, URLs und Domänen in vorkonfigurierten Intervallen von Now Platform abruft.

Diese Integration unterstützt drei Arten von Sperrlisten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- IP-Adresse (Dies umfasst eine einzelne IP-Adresse (nur IPv4) für die Sperrliste und CIDR-Blöcke (Bereiche) von Adressen für die Allow-Liste).
- URL
- Domäne

Von der Check Point NGTP -Integration unterstützte erkennbare Elemente

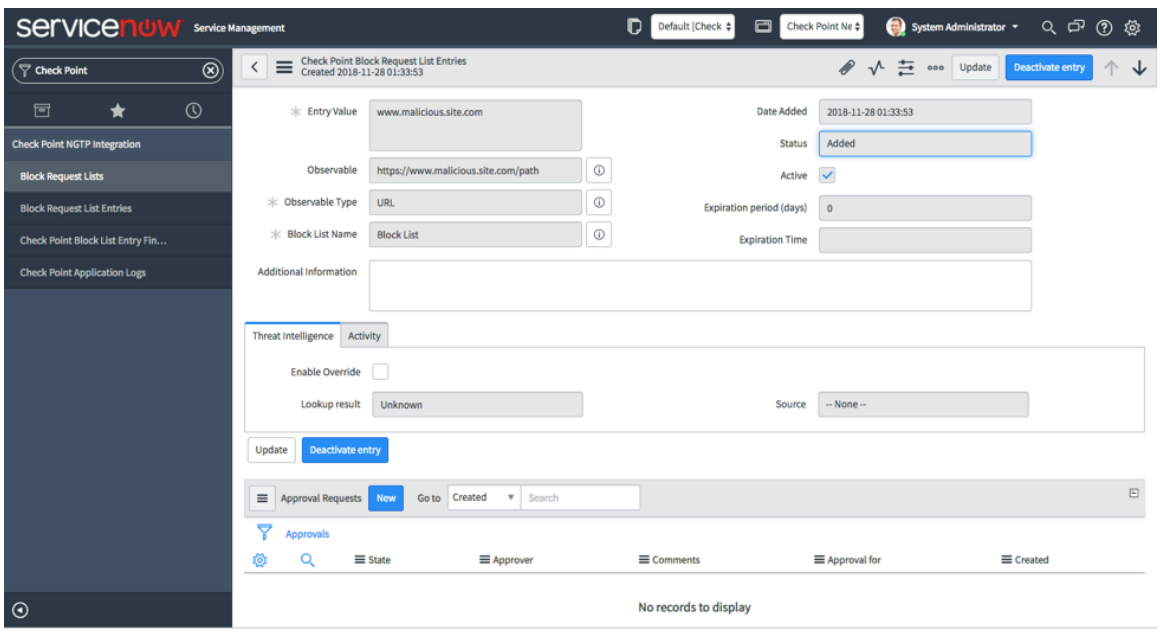
Der Abschnitt enthält Beschreibungen der von dieser Integration unterstützten erkennbaren Elemente und Beispielformate für jeden Typ.

Erkennbarer Typ	Beispiele	Beschreibung
Domäne	• example.com • mail.example.com	Platzhalter werden nicht unterstützt.
IP-Adresse	95.153.103.54 (IPv4)	Stellt eine einzelne, eindeutige Schnittstellenadresse dar. Die Integration unterstützt nur IPv4- und CIDR-Formate (CIDR-Format wird nur für Zulassungslisten unterstützt). Zum Zweck der Zulassungsliste bietet die Integration Unterstützung für erkennbare IP-Adressen einschließlich CIDR-Bereichen (Classless Inter-Domain Routing), z. B. 95.153.100.0/22. **Hinweis:** Wenn Sie versuchen, eine einzelne IP-Adresse an eine Sperrliste anzuhängen, die Sie bereits als Teil eines CIDR-Bereichs zugelassen haben, wird eine Fehlermeldung angezeigt. Zum Beispiel ist die einzelne Adresse 95.153.103.54 Teil des CIDR-Bereichs 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• https://www.example.com • http://www.example.com	Beschreibung: Die HTTPS-URL wird von der Anwendung formatiert, um den Pfad aus der URL zu kürzen und nur den Domänennamen beizubehalten. Check Point NGTP verwendet die HTTP CONNECT-Anforderung,

Automatische Übersetzung

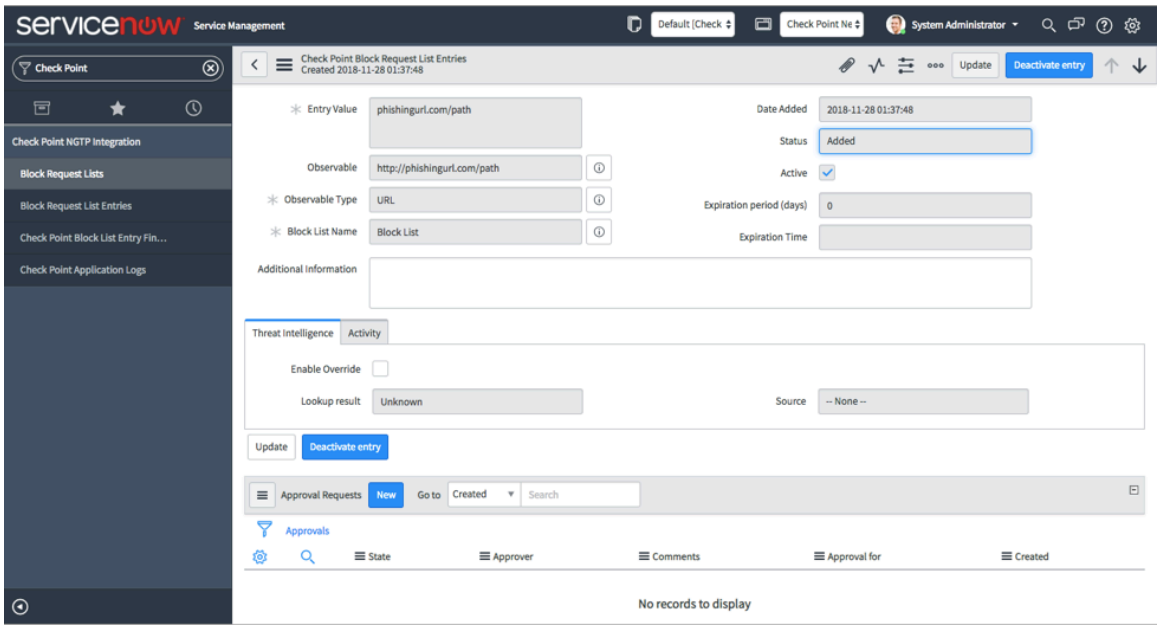
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennbarer Typ	Beispiele	Beschreibung
		um den Webdatenverkehr auszuwerten und die Blockierung zu erzwingen. Bei der HTTPS CONNECT-Anforderung ist nicht die gesamte URL in der Anforderung sichtbar, sondern nur der Domänenname. Wenn ein Anwender eine HTTPS-URL mit einem bestimmten Pfad blockiert (Beispiel: https://www.beispiel.com/path), kürzt die Anwendung den Pfad automatisch (www.beispiel.com). Die Anwendung verwaltet die Beziehung zwischen dem ursprünglichen erkennbaren Element und der formatierten URL. Unten sehen Sie den Screenshot des Sperrlisteneintrags, der die formatierte URL und das ursprüngliche erkennbare Element zeigt.



Bei HTTP-URLs mit einem bestimmten Pfad (z. B. http://www.example.com/path) blockiert Check Point die angegebene URL, da die gesamte URL in der CONNECT-Anforderung sichtbar ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erstellen Sie eine Sperrliste für die Check Point NGTP -Integration

Erstellen Sie eine Sperrliste in Ihrer Now Platform-Instanz. Nach der Genehmigung und Aktivierung können Sie Einträge für diese Sperrlisten aus erkennbaren Elementen erstellen, die bei Now Platform Security Incident Response-Incidents (SIR) als schädlich eingestuft wurden, und die Genehmigung zum Blockieren von Incidents anfordern.

Vorbereitungen

Erforderliche Rolle: Security Incident-Administrator (sn_si.admin)

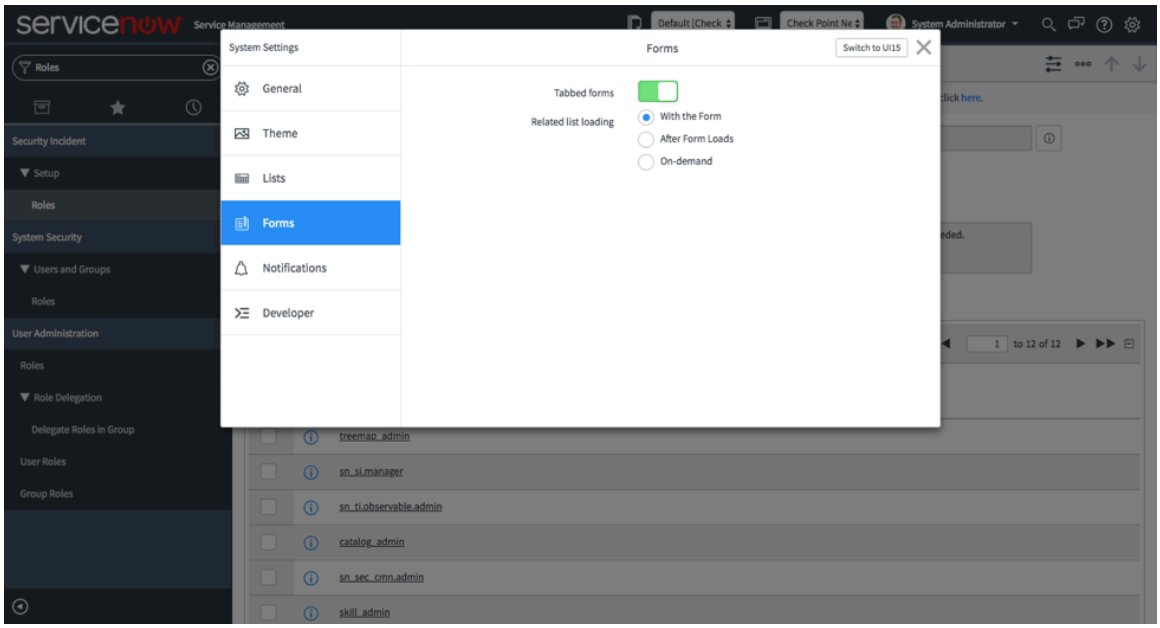
Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie die Sperrliste in Ihrer Now Platform-Instanz, damit der Prüfpunkt die in der Liste enthaltenen Objekte (IP-Adressen, URLs, Domänen) importieren kann. Der anwenderdefinierte Intelligenzfeed wird auf dem Prüfpunkt-Gateway konfiguriert, das die IP-Adressen, URLs und Domänen in vorkonfigurierten Intervallen von der Now Platform abruft. Um sicherzustellen, dass die erkennbaren Elemente blockiert werden, muss die Bedrohungsabwehrrichtlinie mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert werden.

Hinweis:

Die Zahlen in diesem Thema werden mit in den Systemeinstellungen gelöschten **Formularen mit Registerkarten** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozedur

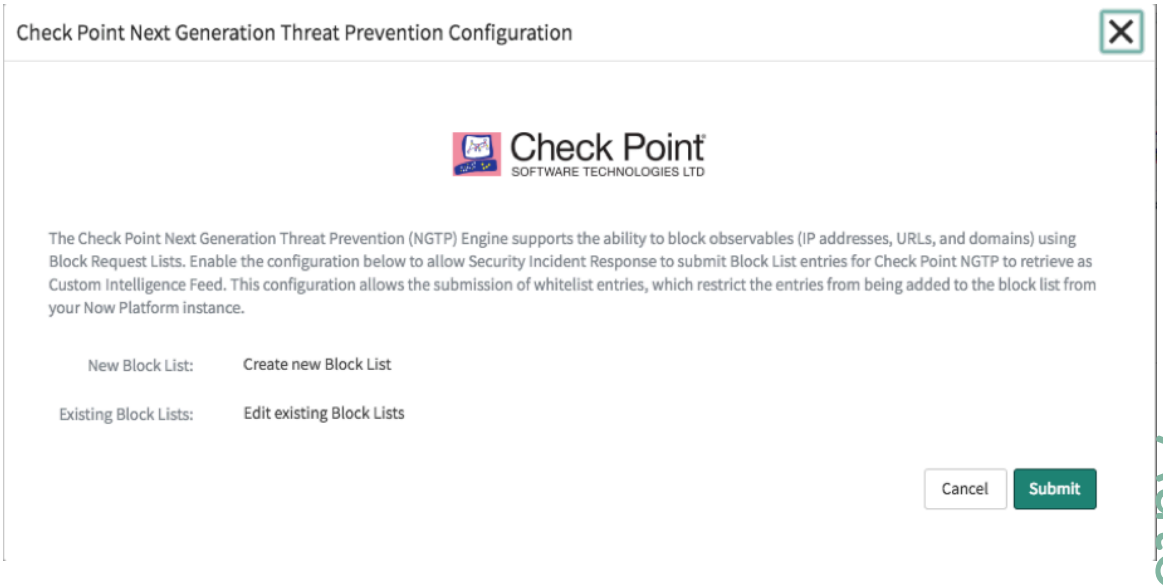
1. Navigieren Sie nach Abschluss der Anwendungsinstallation zu **Integrationen** > **Integrationskonfigurationen**.
2. Suchen Sie die Karte **Prüfpunkt Next Generation Threat Prevention (Prüfpunkt Next Generation Threat Prevention)**, und klicken Sie auf **Konfigurieren**.

Hinweis:
Verwendung privilegierter und proprietärer Inhalte mit Genehmigung von Check Point Software Technologies, Ltd.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Neue Sperrliste erstellen**.



4. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Name der Sperranforderungsliste für Check Point. Fügen Sie den Typ des erkennbaren Elements (URL, IP, Domäne) in dieses Feld ein, damit der Sicherheitsanalyst die Absicht der Sperrliste anhand des Namens leicht erkennen kann. Der Name sollte auch eindeutig angeben, welcher Firewallrichtlinie diese Sperrlistenobjekte zugeordnet sind. Einige Beispiele für Sperrlistennamen sind „Ausgehende Malware-IP“ oder „Ausgehende Phishing-URL“.
Aktiv	Diese Checkbox ist standardmäßig deaktiviert, um anzugeben, dass die Sperrliste inaktiv ist. Wenn die Sperrliste inaktiv ist, können keine zusätzlichen Einträge empfangen werden. Wenn das Kontrollkästchen aktiviert ist (wenn die Change-Anforderung geschlossen oder die Change-Anforderung nicht generiert wird), wird die Sperrliste aktiviert und ist für Sperrlisteneinträge verfügbar.
Tag anzeigen	Das Kontrollkästchen ist standardmäßig aktiviert, um das erkennbare Element und den zugehörigen Security Incident-Datensatz automatisch zu kennzeichnen, wenn das erkennbare Element in der Sperrliste blockiert ist. Wenn diese Option ausgewählt ist, ist das Feld „Tag für erkennbare Elemente“ im Formular verfügbar. **Hinweis:** Ein Tag-Name wird standardmäßig aus dem Wert erstellt, den Sie im Feld Name mit einem Prüfpunkt-Präfix eingeben, z. B. Prüfpunkt – Malware – Ausgehende IP. Sie können den Tag-Namen und die Farbe ändern. Der Tag-Name wird im Feld „Tag für erkennbare Elemente“ angezeigt, sobald die Sperrliste gespeichert wird. Wenn das Kontrollkästchen deaktiviert ist, wird kein Tag erstellt, und das Feld „Tag für erkennbare Elemente“ ist im Formular nicht verfügbar.

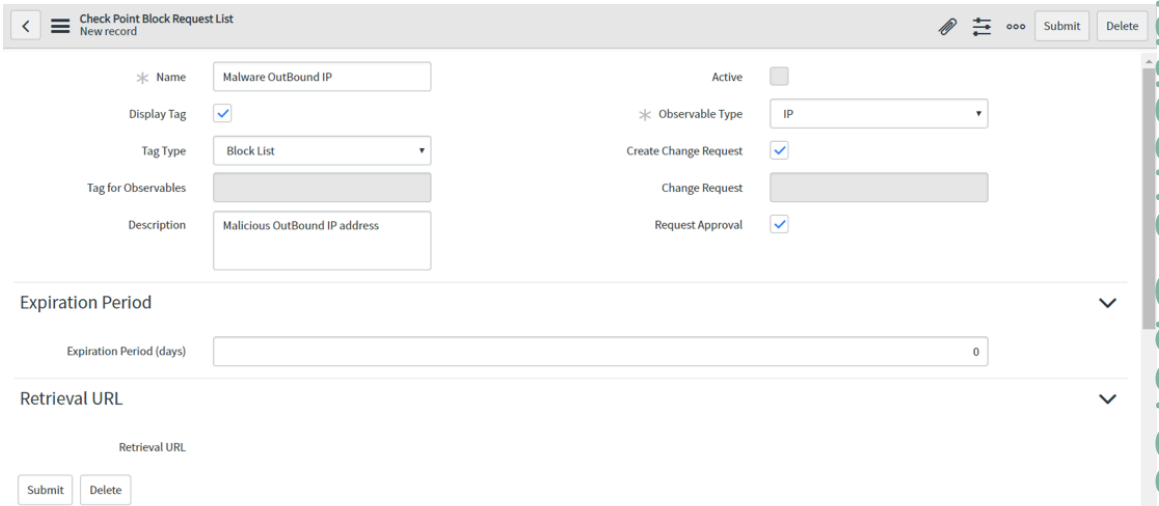
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

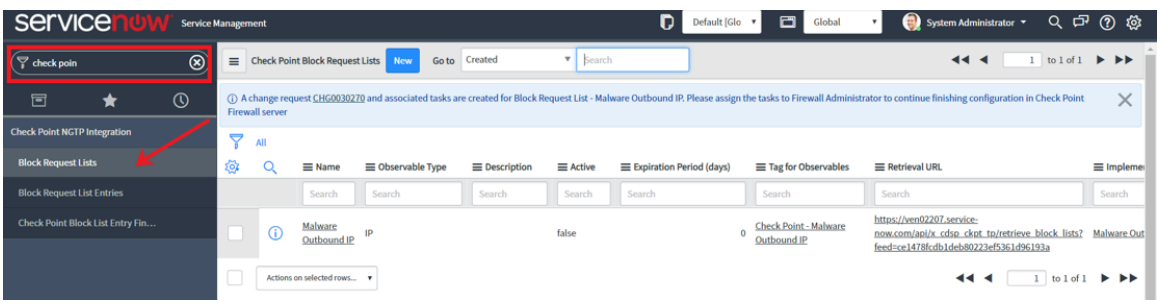
Feld	Beschreibung
Erkennbarer Typ	Wählen Sie einen erkennbaren Elementtyp, den diese Sperrliste akzeptiert, aus der Liste aus: IP-Adresse (einschließlich CIDR für Allow-Liste), URL oder Domäne.
Tag-Typ	Tags, die in der Liste verfügbar sind. Eine Sperrliste ist eine Liste erkennbarer Elemente, die von Check Point Next Generation Threat Prevention blockiert werden sollen. Eine Allow-Liste ist eine Liste von erkennbaren Elementen, die Sie in Prüfpunkt Next Generation Threat Prevention auf keinen Fall blockieren möchten. Standardmäßig ist die Tag-Farbe der Sperrliste schwarz und die Tag-Farbe der Allow-Liste grau. Sie können die Farbe ändern.
Change-Anforderung erstellen	Dieses Kontrollkästchen ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in Ihrer Now Platform-Instanz zu erstellen, die an den Sperrlisten-Datensatz angehängt sind. Die Change-Anforderung wird verwendet, um die Abruf-URL für die Sperrliste im Firewall-Gateway von Check Point Next Generation zu konfigurieren. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch die Now Platform für Firewall-Richtlinien- oder Regeländerungen verwendet. Wenn Sie eine Anforderung erstellen, wird die Sperrliste nach dem Schließen automatisch aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Sperrliste manuell zu aktivieren, nachdem Sie per E-Mail vom Firewall-Administrator benachrichtigt wurden, dass der anwenderdefinierte Intelligenzfeed auf allen Prüfpunkt-Gateways konfiguriert wurde. Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, ist das Feld Change-Anforderung nicht verfügbar.
Genehmigung anfordern	Dieses Kontrollkästchen ist standardmäßig aktiviert, um Genehmigungen für das Aktivieren/Entfernen von Sperrlisteneinträgen aus Sperrlisten anzufordern. Die Genehmigung wird von den Anwendern mit der Rolle „Security Incident-Administrator“ (sn_si.admin) angefordert. Genehmigungsanforderung wird per E-Mail an die Genehmiger gesendet. Sobald die Genehmigung akzeptiert wurde, wird der Eintrag in dieser Sperrliste aktiviert. Wenn das Kontrollkästchen deaktiviert ist, folgen die Einträge für diese Sperrliste nicht dem Genehmigungs-Workflow, sondern werden direkt in der Sperrliste aktiviert.
Tag für erkennbares Element	Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen Tags anzeigen aktiviert ist. Das Feld wird automatisch gefüllt, nachdem die Sperrliste mit einem Standardwert aus dem Feld Name gespeichert wurde. Wenn die Sperrliste mit dem Namen „Malware-URL“ erstellt wird, lautet der abgeleitete Tag-Name „Sperrliste – Malware-URL“.
Change-Anforderung	Wenn das Kontrollkästchen Change-Anforderung erstellen aktiviert ist, wird die Nummer der Change-Anforderung in der Now Platform-Instanz angezeigt, sobald die Sperrliste gespeichert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, wird dieses Feld nicht angezeigt.
Beschreibung	Beschreibung der Check Point-Sperrliste. Der Name enthält im Allgemeinen die Typen von Sites und erkennbaren Elementen, die sich voraussichtlich in dieser Sperrliste befinden. Sie können dieses Feld für weitere Details verwenden.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der Sperrliste. 0 (Standardeinstellung) gibt an, dass der Sperrlisteneintrag nie abläuft. Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben, was 24 Stunden entspricht, und es gibt keinen Höchstwert.
Abruf-URL	Die Abruf-URL wird automatisch generiert, sobald die Sperrliste gespeichert wird. Um diese Sperrliste auf Prüfpunkt-Gateways zu konfigurieren, müssen Sie diese URL verwenden. Sobald diese URL konfiguriert ist, ruft Check Point zu blockierende erkennbare Elemente im CSV-Format ab.



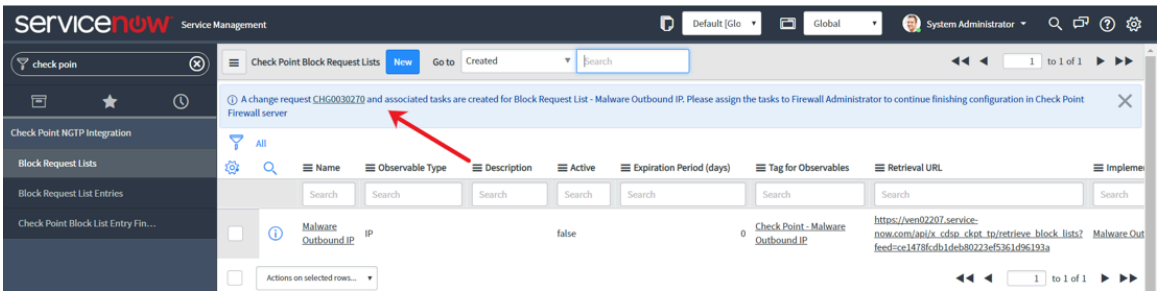
5. Klicken Sie auf **Absenden**.
6. Wenn die Sperranforderungsliste für Check Point nicht angezeigt wird, navigieren Sie zu **Check Point – NGTP-Integration** > **Sperranforderungslisten**.



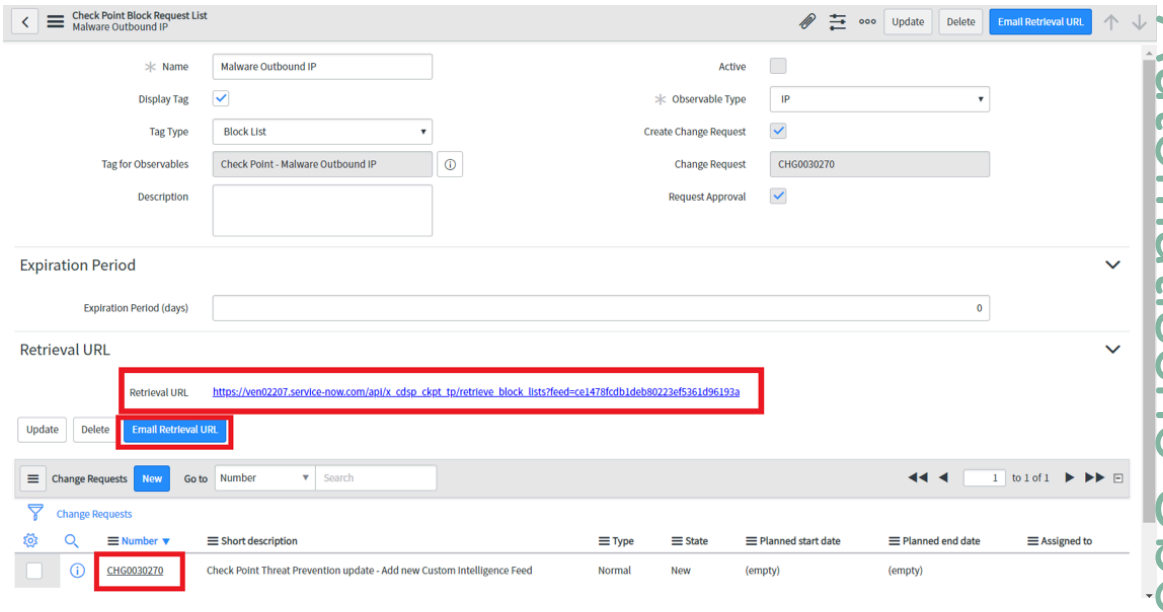
Die neue Sperrliste wird angezeigt. Der Status der Sperrliste ist weiterhin inaktiv (falsch), was bedeutet, dass die Sperrliste nicht für die Annahme von Einträgen verfügbar ist. Wenn Change-Anforderung erstellen konfiguriert wurde, wird eine Nachricht angezeigt, die angibt, dass eine Change-Anforderung und Aufgaben in Ihrer Now Platform-Instanz erstellt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie in der Spalte **Name** auf ein Element, um den Datensatz zu öffnen.
   Der Sperrlistendatensatz wird angezeigt. Dieses Beispiel zeigt eine Sperrliste für ausgehende IP-Adressen für Malware. Die folgenden Felder, Optionen und Links werden nach der Übermittlung im neuen Datensatz angezeigt und in der folgenden Tabelle beschrieben.



Feld	Beschreibung
E-Mail-Abruf-URL	Sendet eine Benachrichtigung per E-Mail, dass der Blocklink zur Konfiguration an den Check Point-Firewall-Administrator verfügbar ist.
Abruf-URL	Diese URL wird zum Konfigurieren des anwenderdefinierten Intelligenzfeeds auf Prüfpunkt-Gateways verwendet. **Hinweis:** Wenn in Ihren Systemeinstellungen Formulare mit Registerkarten festgelegt sind, wird dieser Link auf der Registerkarte Abrufinformationen für Sperrliste unten im Datensatz angezeigt.
Change-Anforderung für die Now Platform	Ein Link zum Datensatz der Change-Anforderung wird im Abschnitt „Change-Anforderungen“ angezeigt, sofern konfiguriert, und die Nummer der Anforderung wird im Feld Change-Anforderung angezeigt.
Aktualisieren	Ändern Sie Daten, und aktualisieren Sie die bearbeitbaren Felder.
Löschen	Löschen Sie den Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Erstellen und fügen Sie nach Bedarf weitere Sperrlisten hinzu.
   Die Sperrlisten werden auf der Seite mit Sperranforderungslisten für Check Point angezeigt.

Nächste Maßnahme
Aktivieren Sie die Sperranforderungsliste manuell oder mit einer Change-Anforderung der Now Platform.

Aktivieren Sie eine Sperrliste für die Check Point NGTP -Integration

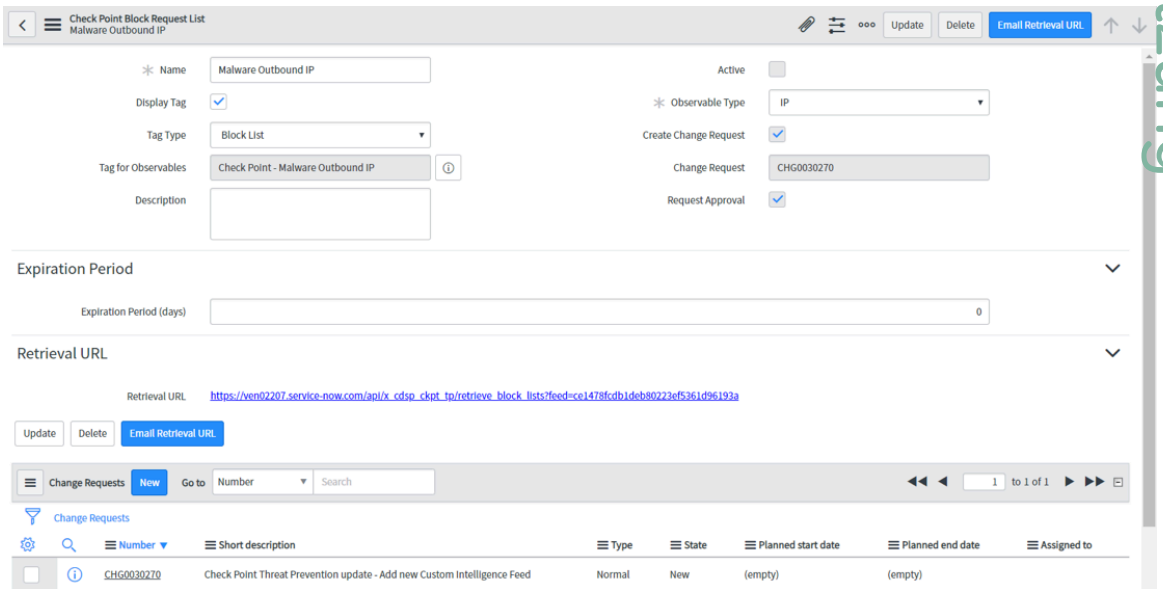
Nachdem die Sperrliste in Ihrer Now Platform erstellt wurde und die URL verfügbar ist, konfiguriert der Prüfpunkt-Administrator die Sperrliste als anwenderdefinierten Intelligenzfeed auf allen Prüfpunkt-Gateways der nächsten Generation. Bevor Sperrlisteneinträge akzeptiert werden können, muss die Sperrliste in Check Point konfiguriert und in der Now Platform aktiviert werden.

Vorbereitungen
Erforderliche Rolle: Security Incident-Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird
Nachdem die Sperrliste konfiguriert wurde, können Sie als Security Incident-Administrator die Sperrliste manuell aktivieren. Oder die Sperrliste wird nach Abschluss einer Now Platform Change-Anforderung automatisch aktiviert. Die Change-Anforderung muss genehmigt und vom Status „Inaktiv“ in den Status „Aktiv“ versetzt werden, bevor Sperrlisteneinträge akzeptiert werden können.

Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Sperranforderungslisten**, und wählen Sie das Modul **Sperranforderungslisten** aus.
2. Wählen Sie in der Liste **„Sperranforderungslisten für Prüfpunkt“,** die angezeigt wird, in der Spalte **Name** die neue Sperrliste aus.
3. Beachten Sie im angezeigten Datensatz die Schaltfläche **URL zum Abrufen von E-Mails**, den aktiven Link zum Abrufen der Sperrliste und, falls konfiguriert, die Change-Anforderung der Now Platform im Abschnitt Change-Anforderungen.
   Beachten Sie auch, dass das Kontrollkästchen Aktiv deaktiviert ist.

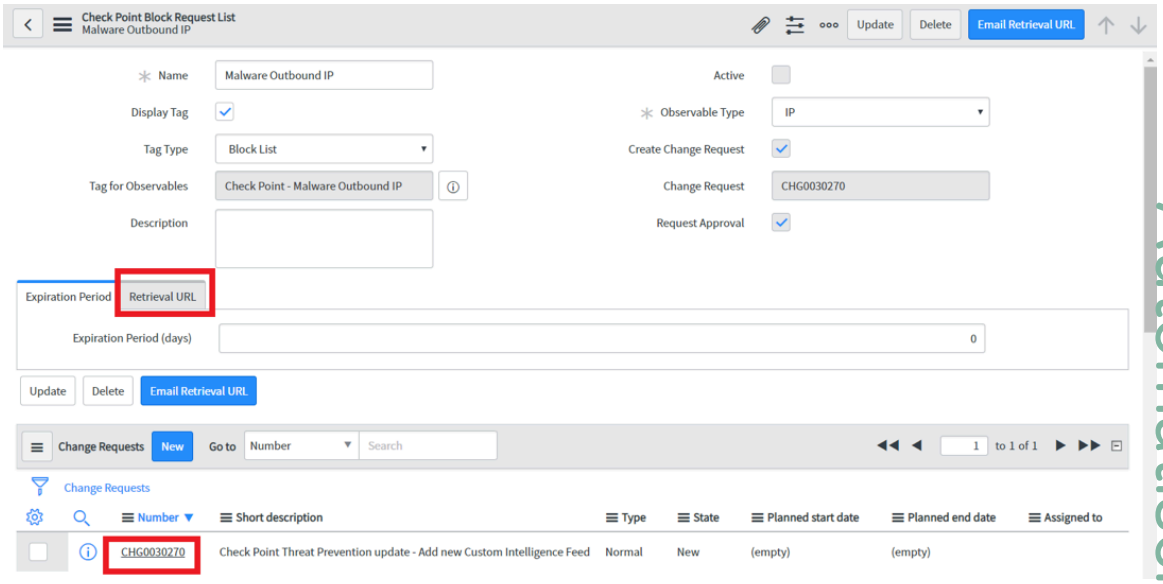


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn in Ihren Systemeinstellungen Formulare mit Registerkarten deaktiviert sind, wird die Sperrlisten-Abruf-URL im Abschnitt „Abruf-URL“ angezeigt.

4. Klicken Sie auf die Registerkarte **Abruf-URL der Sperrliste,** um die Abruf-URL anzuzeigen.
Die folgende Abbildung zeigt die Sperrlisten-Abruf-URL, die als Registerkarte mit in Ihren Systemeinstellungen ausgewählten Formularen mit Registerkarten angezeigt wird. Der Link zum Change Request (CH0030270) wird ebenfalls angezeigt.



5. Um die Konfiguration abzuschließen und die Sperrliste von inaktiv auf aktiv zu verschieben, müssen Sie eine der folgenden Optionen auswählen, um den Firewall-Administrator zu benachrichtigen, dass die Abruf-URL verfügbar ist.

Option	Beschreibung
Klicken Sie auf E-Mail-Abruf-URL.	Abruf-URL für E-Mail-Sperrliste direkt an den Firewall-Administrator. Mit dieser Option kann der Firewall-Administrator die Konfiguration auf der Check Point-Plattform abschließen. Wählen Sie diese Option, wenn der Firewall-Administrator die Now Platform nicht verwendet.
Schließen Sie die Change-Anforderung für die Now Platform ab, und weisen Sie dem Firewall-Administrator die Konfigurationsaufgaben zu.	Diese Option ist nur verfügbar, wenn der Firewall-Administrator für Check Point auch die Now Platform verwendet und die Change-Management- und Genehmigungsprozesse der Now Platform konfiguriert sind. **Hinweis:** Benutzer mit der Rolle „Security Incident-Administrator“ (sn_si.admin) können die Now Platform Change-Anforderung genehmigen. Sobald die Konfigurationsaufgaben abgeschlossen sind und die Change-Anforderung geschlossen wurde, wird die Sperrliste automatisch aktiviert.

Nächste Maßnahme

Nachdem Sie den Firewall-Administrator benachrichtigt haben, dass die Abruf-URL verfügbar ist, und Sie als Security Incident-Administrator bestätigt haben, dass die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sperrliste in Check Point konfiguriert wurde, besteht Ihr nächster Schritt in der Aktivierung der Sperrliste. Sie aktivieren die Sperrliste entweder manuell oder verwenden, falls konfiguriert, das Formular für Change-Anforderungen der Now Platform, um die Sperrliste zu aktivieren. Die Sperrliste wird automatisch aktiviert, wenn die Change-Anforderung geschlossen wird.

Konfigurieren Sie eine Sperrliste als anwenderdefinierten Intelligenzfeed in der Check Point NGTP -Integration

Der Firewall-Administrator muss den anwenderdefinierten Intelligenzfeed entsprechend der auf der Now Platform erstellten Sperrliste konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe muss für jedes Prüfpunkt-NGTP-Gateway ausgeführt werden. Der Firewall-Administrator benötigt den SSH-Zugriff der Gateway-Server. Wenn Ihre Organisation über Change-Management- und Genehmigungsprozesse der Now Platform verfügt, vergewissern Sie sich, dass die Funktion zum Senden/Empfangen von E-Mails aktiviert ist.
Der Firewall-Administrator benötigt die Abruf-URL der Sperrliste und die Anmeldeinformationen des ServiceNow-Anwenders mit der Rolle Check Point API Account Access Role (sn_sec_checkpoint.api_account_access).

Wenn der Firewall-Administrator die NOW Platform nicht verwendet, kann der NOW Security Incident-Administrator die erforderlichen Informationen per E-Mail bereitstellen. Wenn der Firewall-Administrator die Now Platform verwendet, kann die der Sperrliste zugeordnete Change-Anforderung alternativ dem Firewall-Administrator zugewiesen werden. Diese Change-Anforderung enthält die erforderlichen Informationen zum Konfigurieren eines anwenderdefinierten Intelligenzfeeds.

Weitere Informationen zum Einrichten von anwenderdefiniertem Intelligenzfeed für Prüfpunkt-Gateways finden Sie unter: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Prozedur

1. Stellen Sie sicher, dass die Funktion zum Senden/Empfangen von E-Mails in Ihrer Now Platform-Instanz aktiviert ist, indem Sie zu navigieren **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**.
2. Überprüfen Sie unter Konfiguration ausgehender E-Mails, ob **Senden von E-Mails** und **Empfangen von E-Mails** ausgewählt sind.
3. Ändern Sie im Expertenmodus SSH in Prüfpunkt-Gateway.
4. Führen Sie den Befehl aus, um einen anwenderdefinierten Intelligenzfeed hinzuzufügen.
   Die Befehlsausführung ist interaktiv und fragt nach Feed-Format und Passwort.
   - Wenn Sie zur Eingabe des Feed-Formats aufgefordert werden, geben Sie „cp_csv“ ein.
   - Bei Abfrage des NOW Platform-Anwenderpassworts mit API-Zugriff.

   Bei der Befehlsausführung wird davor gewarnt, dass das Serverzertifikat (NOW-Plattform) vom Computer nicht als vertrauenswürdig eingestuft wird, und Sie werden aufgefordert, das Sicherheitszertifikat des Servers dem vertrauenswürdigen Speicher des Computers hinzuzufügen. Geben Sie **Y**ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Meldung „Status:Erfolgreich“ bestätigt, dass der Feed erfolgreich hinzugefügt wurde.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Senden Sie Sperrlisteneinträge aus einem Security Incident für die Check Point NGTP -Integration

Erkennbare Elemente, die an einen Security Incident-Datensatz angehängt sind, werden als Sperrlisteneinträge für verschiedene Sperrlisten zur Genehmigung übermittelt. Ein optionaler Genehmigungsprozess für Sperrlisteneinträge ist Teil des vorkonfigurierten Workflows. Das Gateway importiert Sperrlisteneinträge – IP-Adressen, URLs, Domänen –, die in Sperrlisten enthalten sind.

Vorbereitungen

Erforderliche Rolle:

- Security Incident-Analyst (sn_si.analyst) zum Senden von Sperrlisteneinträgen.
- Security Incident-Administrator (sn_si.admin), um Sperrlisteneinträge zu genehmigen. Diese Berechtigung kann nach Bedarf von Ihrer Organisation zugewiesen werden.

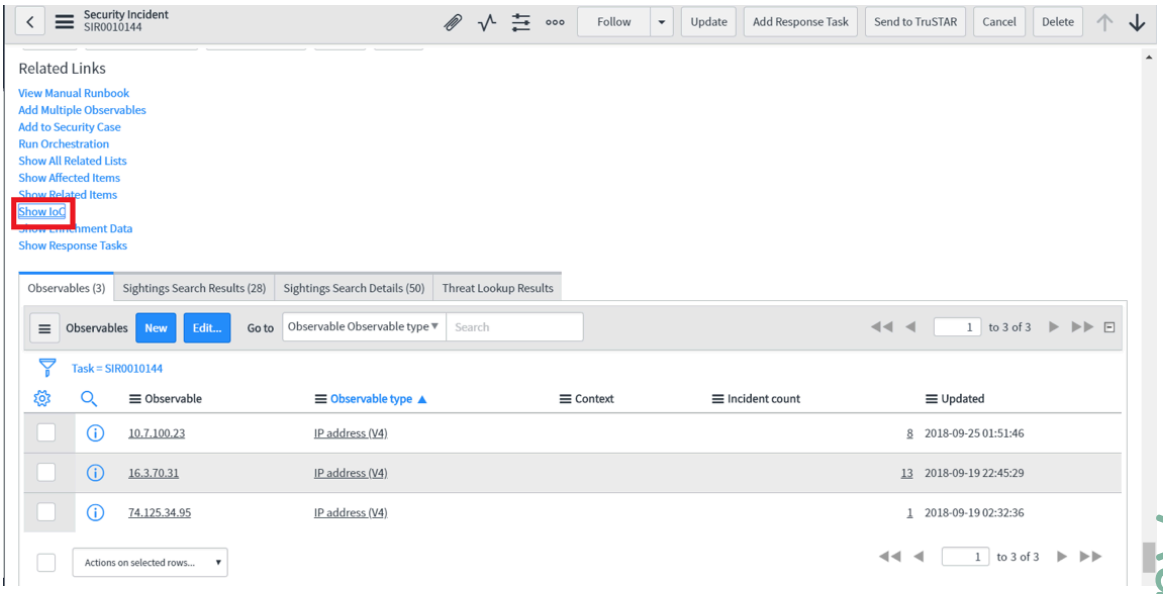
Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der Rolle „sn_si.analyst“ übermitteln Einträge zum Blockieren von Einträgen, indem sie einen Block für erkennbare Elemente anfordern, die an einen Security Incident-Datensatz angehängt sind. Nach der Übermittlung wird ein Sperrlisteneintrag mit dem Status Ausstehend generiert und zur Genehmigung gesendet. Das folgende Beispiel zeigt eine Blockierungsanforderung für ein erkennbares URL-Element.

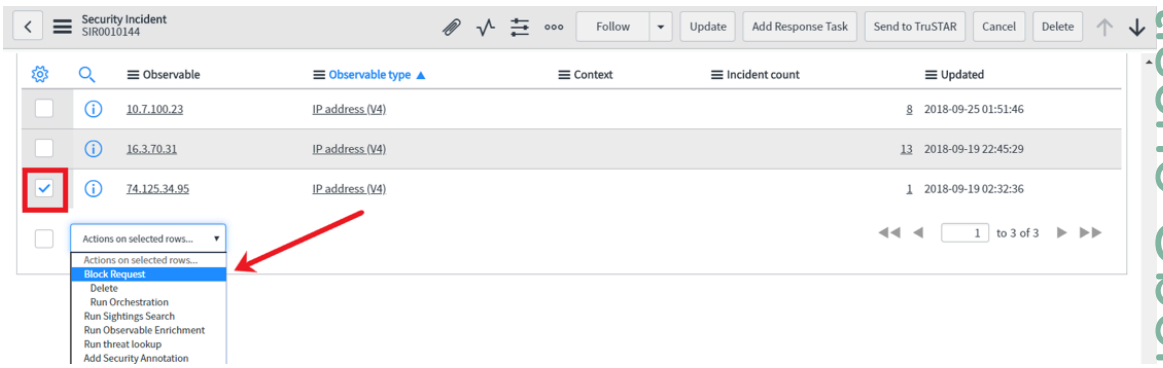
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**, und klicken Sie auf einen Security Incident-Datensatz, um ihn zu öffnen.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.

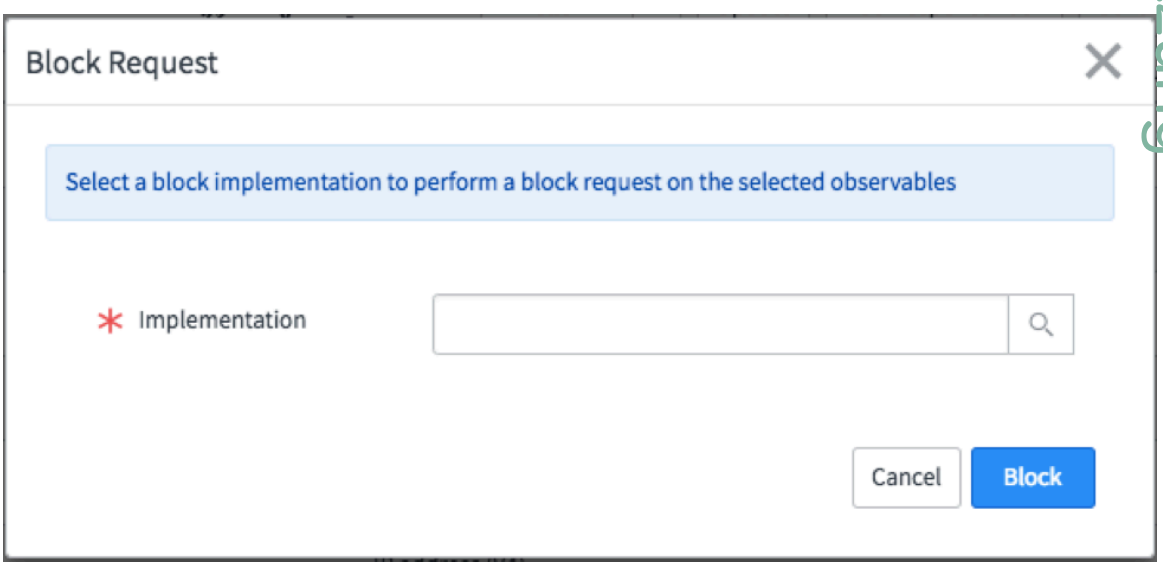
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie in der zugehörigen Liste „Erkennbare Elemente“ die erkennbaren Elemente aus, die Sie blockieren möchten, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die **Option Blockierungsanforderung**aus.



4. Klicken Sie im angezeigten Dialogfeld auf das Suchsymbol ( ).

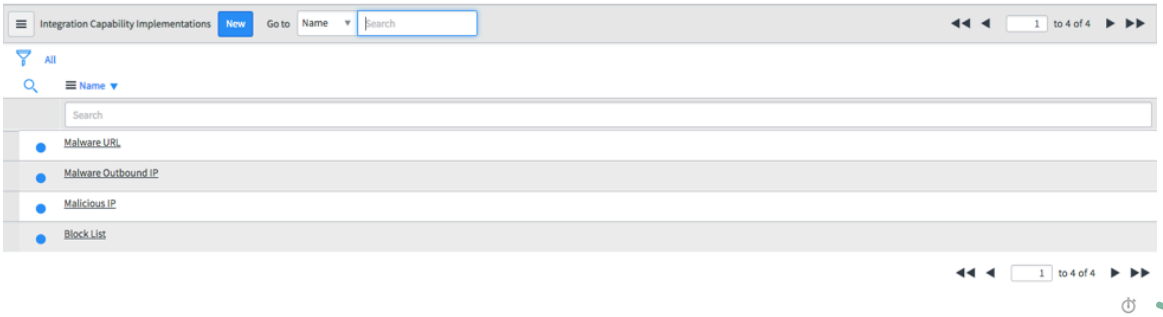


Automatische Übersetzung

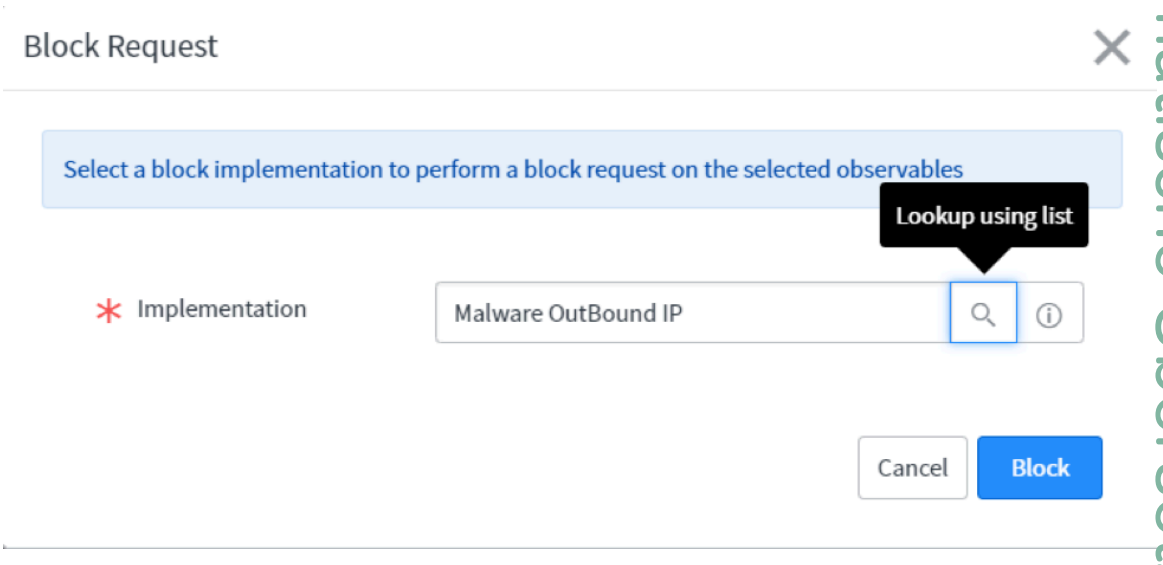
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie in der Liste die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten.

Hinweis:
In diesem Beispiel muss der erkennbare Elementtyp des Eintrags (IP) mit dem erkennbaren Elementtyp der Sperrliste übereinstimmen.

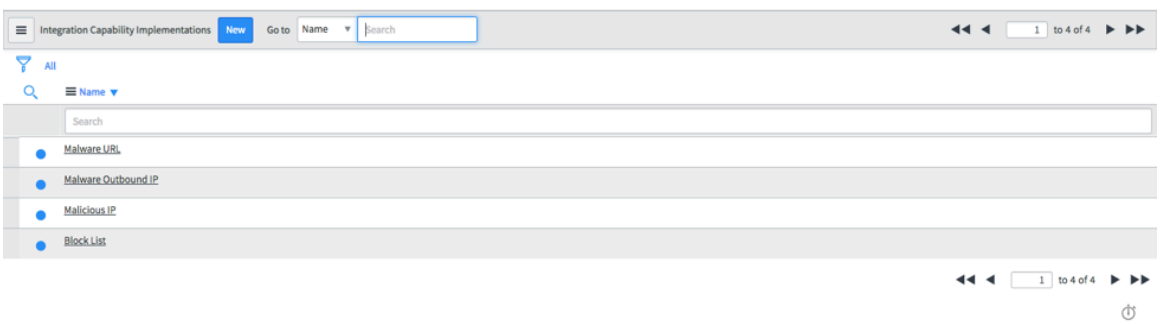


6. Klicken Sie im Dialogfeld Sperranforderung mit dem Sperrlistennamen, der im Feld Implementierung angezeigt wird, auf **Sperren**.



7. Wählen Sie in der angezeigten Liste die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten.

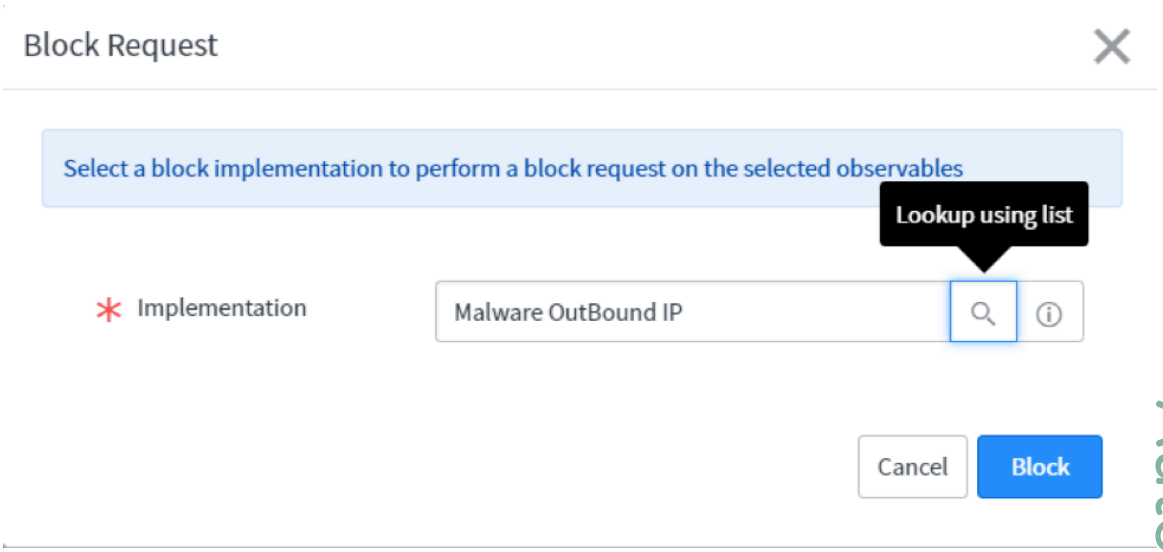
Hinweis:
In diesem Beispiel muss der erkennbare Elementtyp des Eintrags (IP) mit dem erkennbaren Elementtyp der Sperrliste übereinstimmen.



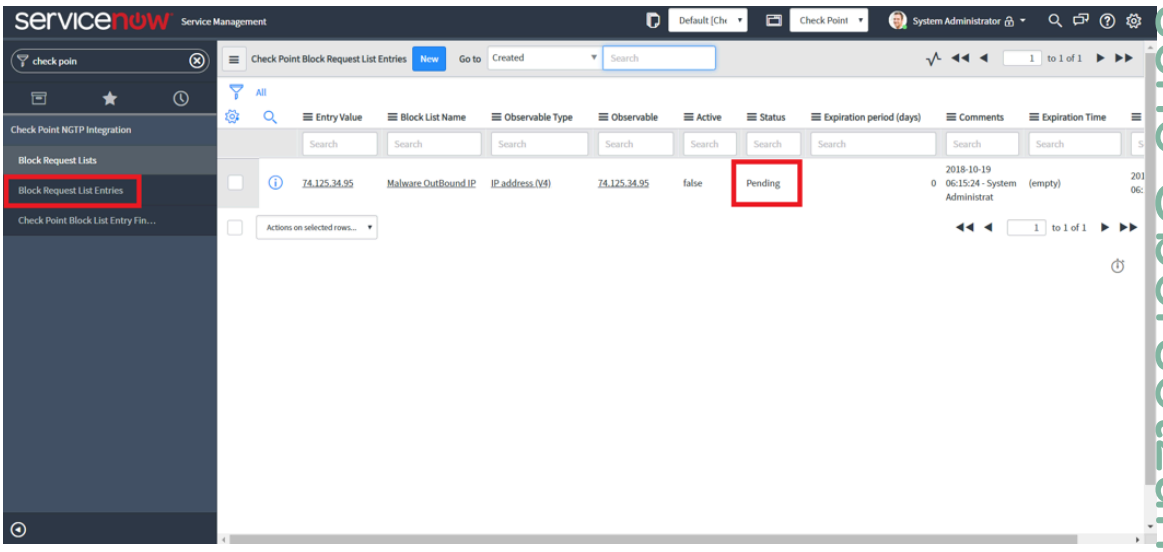
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie im Dialogfeld Sperranforderung mit dem Sperrlistennamen, der im Feld **Implementierung** angezeigt wird, auf **Sperren**.



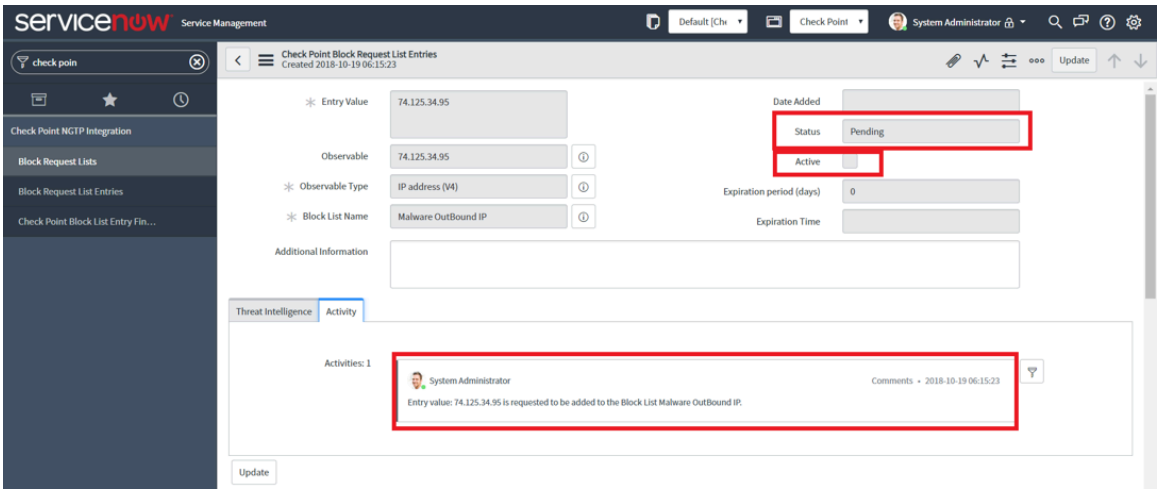
9. Navigieren zu **Check Point – NGTP-Integration** > **Einträge der Sperranforderungsliste**und klicken Sie auf **Einträge der Anforderungsliste sperren**.



10. Klicken Sie in der Liste Einträge der Sperranforderungsliste für Check Point in der **Spalte Eintragswert** auf das erkennbare Element, um den Datensatz zu öffnen.
In diesem Beispiel wird der Datensatz für **74.125.34.95** angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Status lautet Ausstehend, das Kontrollkästchen Aktiv ist deaktiviert, und in den Arbeitsnotizen wird angezeigt, dass eine Anforderung zum Hinzufügen des erkennbaren Elements vorhanden ist. Diese Anforderung für den Sperrlisteneintrag ist zur Genehmigung bereit.

Das Symbol neben dem Feld „Erkennbares Element“ ist ein Link zur Tabelle „Erkennbares Element“ der Now Platform.

Der Wert im Feld „Erkennbares Element“ (74.125.34.95) ist mit der Tabelle „Erkennbares Element“ verknüpft und entspricht dem Format, das aus dem Security Incident Response-Incident-auslösenden Ereignis übernommen wurde.

Senden Sie Sperrlisteneinträge direkt aus der Sperrlisteneintragstabelle

Für erkennbare Elemente, die als schädlich eingestuft wurden und keinem bestimmten Now Platform -Security Incident zugeordnet sind, übermitteln Sie Sperrlisteneinträge aus der Sperrliste.

Vorbereitungen

Erforderliche Rolle: Security Incident-Administrator (sn_si.analyst)

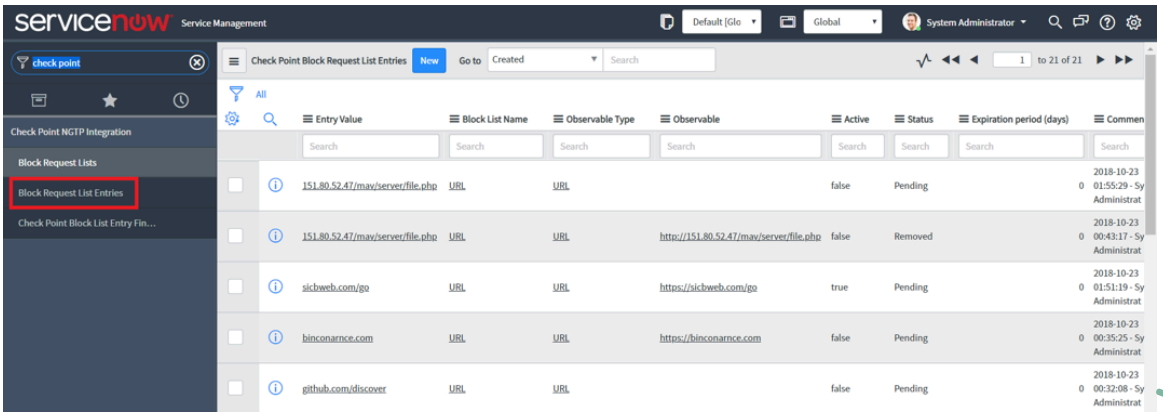
Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein erkennbares Element blockieren möchten, das Sie als schädlich eingestuft haben, oder ein erkennbares Element zulassen möchten, das Sie als nicht schädlich eingestuft haben und das erkennbare Element keinem bestimmten Security Incident-Datensatz der Now Platform zugeordnet ist, übermitteln Sie Sperrlisteneinträge direkt aus der Sperrliste. Beispiele für diese Arten von Sperrlisteneinträgen können URLs oder Domänen für bestimmte Websites sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

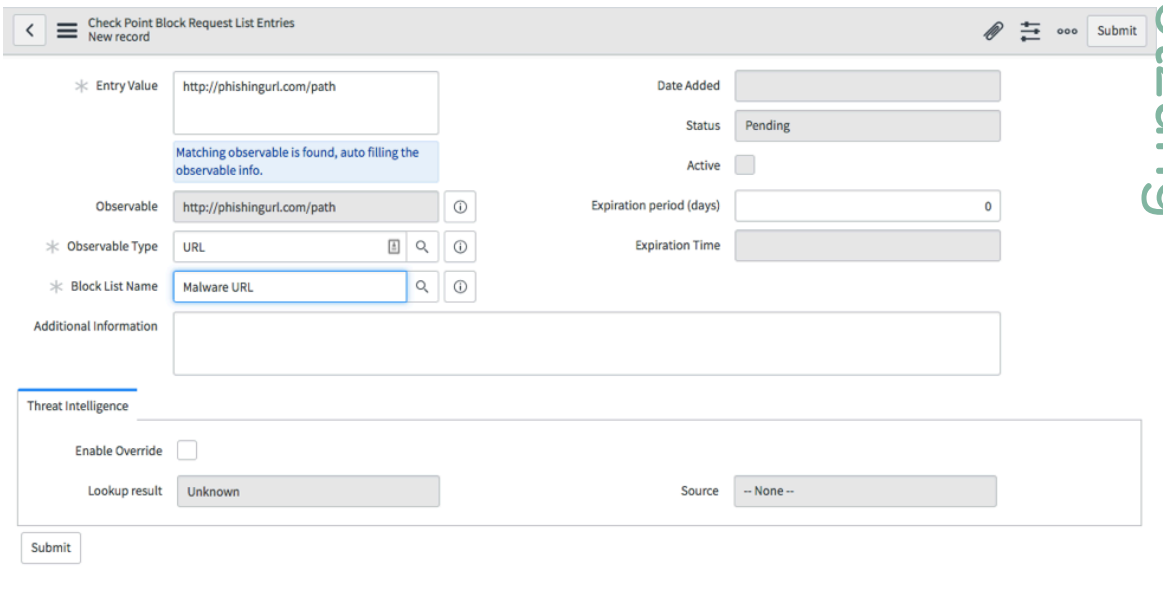
Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Anforderungseinträge blockieren**.



2. Klicken Sie auf das Modul **„Sperranforderungslisten“**.
3. Klicken Sie in der Liste Einträge der Sperranforderungsliste für Check Point auf **Neu**.
4. Geben Sie im Feld **Eingabewert** einen Wert für Ihr erkennbares Element ein.
   Die zwei möglichen Ergebnisse dieses Eintrags:
   - Die übrigen Felder des Formulars werden automatisch ausgefüllt.
   - Es wird ein übereinstimmendes erkennbares Element gefunden, und es wird eine Meldung angezeigt, dass ein übereinstimmendes erkennbares Element vorhanden ist. Wählen Sie die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten, und klicken Sie auf Absenden. Wählen Sie die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.

   Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, das Formular auszufüllen. Es wurde kein passendes erkennbares Element gefunden, und Sie müssen das Formular ausfüllen. Wählen Sie anschließend die Sperrliste aus, an die Sie das erkennbare Element anhängen möchten, und klicken Sie auf Absenden.
   Ein Datensatz eines erkennbaren Elements wird erstellt. Die folgende Abbildung zeigt ein Beispiel für ein vorhandenes erkennbares Domänenelement und wie die Felder automatisch ausgefüllt werden.

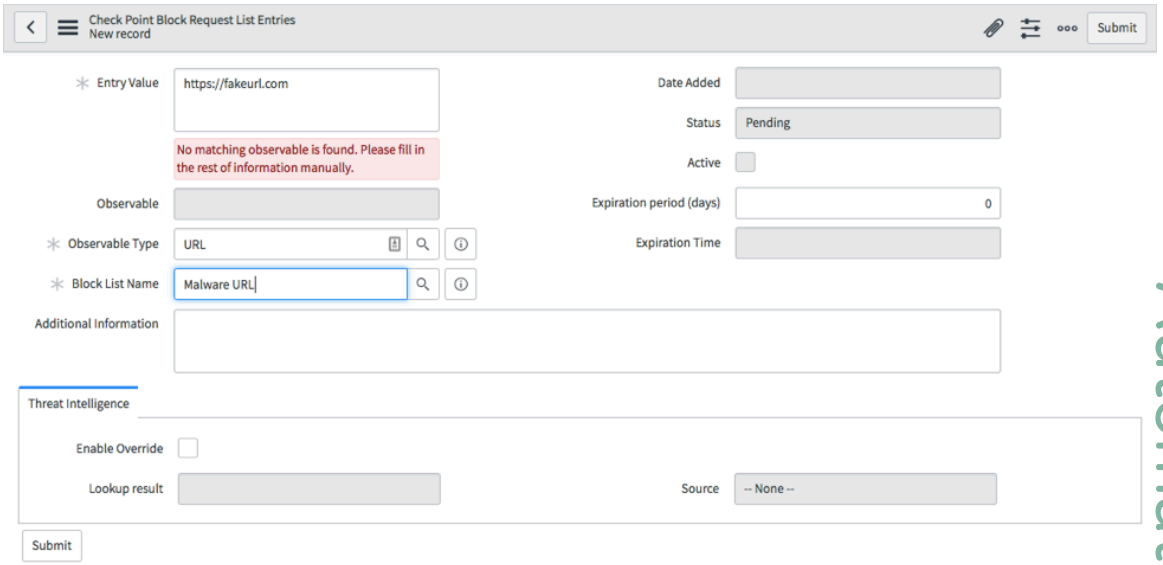


5. Klicken Sie auf das Suchsymbol, um die Sperrliste auszuwählen, an die Sie den Eintrag anhängen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
7. Wenn Sie die E-Mail-Genehmigung in Ihrem Workflow konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
   Wenn eine Meldung angezeigt wird, in der Sie aufgefordert werden, die restlichen Informationen manuell einzugeben, füllen Sie die Felder aus.



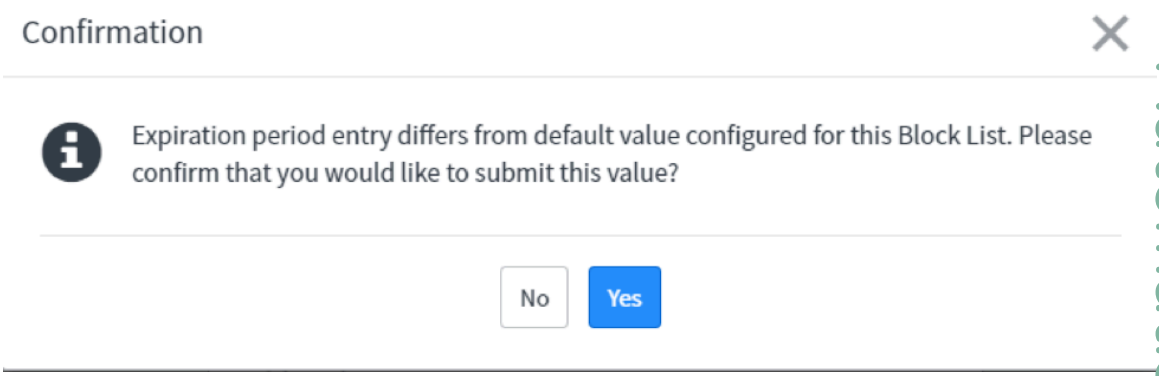
Feld	Beschreibung
Erkennbarer Typ	Erkennbarer Typ, der vom Dialogfeld unterstützt wird.
Sperrlistenname	Sperrliste, der Sie den Eintrag hinzufügen möchten. **Hinweis:** Wählen Sie die Sperrliste aus, an die Sie den Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.
Überschreibung aktivieren (Standardeinstellung ist ausgewählt)	Suchergebnis oder -quelle. Wenn konfiguriert, können Sie ein Suchergebnis und die Quelle eingeben, in der die Ergebnisse gefunden wurden. Diese Felder werden normalerweise gefüllt, wenn ein Security Incident-Datensatz erstellt wird. In diesem Fall gibt es kein Suchergebnis oder keine Suchquelle, und Sie füllen diese Felder in manuell aus.
Suchergebnis	Wählen Sie **Unbekannt** oder **Böswillig**aus.
Quelle	Quelle, die eine Bedrohungssuche für den Sperrlisteneintrag durchführt, z. B. ThreatCrowd usw
Ablaufzeitraum	Der standardmäßig von der Sperrliste geerbte Ablaufzeitraum. Sie können diesen Wert überschreiben, jedoch nur während der Erstellung des Eintrags. 0 gibt an, dass der Sperrlisteneintrag nie abläuft. Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Es gibt keinen Höchstwert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

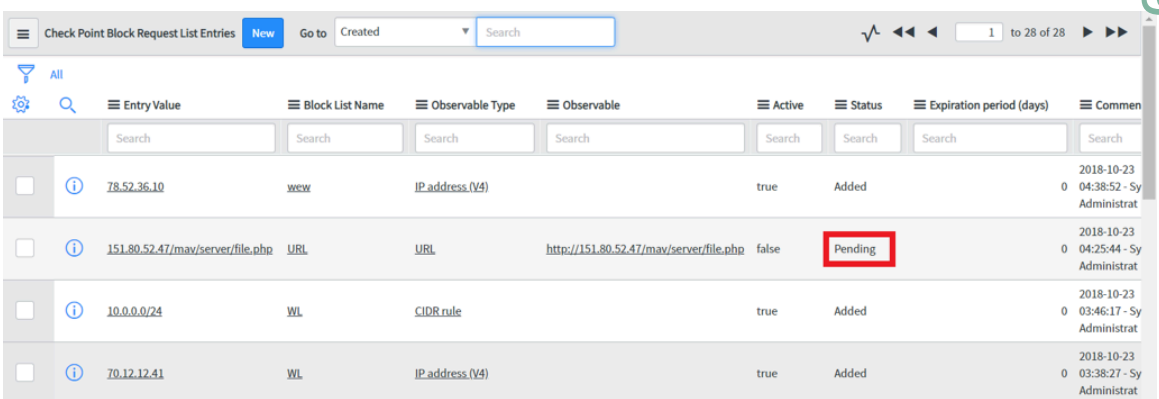
Feld	Beschreibung
	Wenn Sie beispielsweise am 1. Mai um 14:01 Uhr 30 Tage eingeben, läuft der Sperrlisteneintrag am 31. Mai um 14:01 Uhr ab. Der Zeitplaner sucht jedoch jeden Tag um 00:00 Uhr nach abgelaufenen Einträgen und ändert den Status des Eintrags am 1. Juni um 00:00 Uhr in „Abgelaufen“.

8. Klicken Sie auf **Absenden**.
   Wenn Sie den standardmäßigen Ablaufzeitraum des Sperrlisteneintrags geändert haben, wird ein Bestätigungsdialogfeld mit einer Warnung angezeigt, das Sie darauf hinweist, dass der Zeitraum von der ausgewählten Sperrliste abweicht.



Option	Beschreibung
Ja	Bestätigt Ihre Ablaufüberschreibung, speichert den Datensatz und leitet Sie zu den Check Point-Sperrlisteneinträgen zurück. Wenn Sie die E-Mail-Genehmigung in Ihrem Workflow konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
Nein	Bricht die Überschreibung ab. An dieser Stelle können Sie den Wert für den **Ablaufzeitraum**ändern. Nachdem Sie den Wert geändert haben, klicken Sie auf Absenden, um zur Liste der Prüfpunkt-Blockeinträge zurückzukehren.

9. Wird er nicht angezeigt, navigieren Sie zu **Check Point Sperranforderungslisteneinträge**, und beachten Sie, dass der Status für den Eintrag **Ausstehend**ist.



Der Eintrag ist jetzt zur Genehmigung bereit.

Automatische Übersetzung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigen Sie Sperrlisteneinträge für die Check Point NGTP -Integration

Ein Genehmigungsprozess für Sperrlisteneinträge ist Teil des vorkonfigurierten Workflows. Sie genehmigen Sperrlisteneinträge, bevor die Einträge in Sperrlisten aktiviert werden. Nachdem Sie den Sperrlisteneintrag genehmigt haben, ruft das Gateway den Eintrag ab, und Ihr erkennbares Element wird ab diesem Zeitpunkt blockiert.

Vorbereitungen

- Die Genehmigung von Sperrlisteneinträgen wird standardmäßig dem Security Incident-Administrator (sn_si.admin) zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation zugewiesen werden. Im folgenden Beispiel verfügt der Now Platform-Administrator über die Genehmigungsberechtigung.

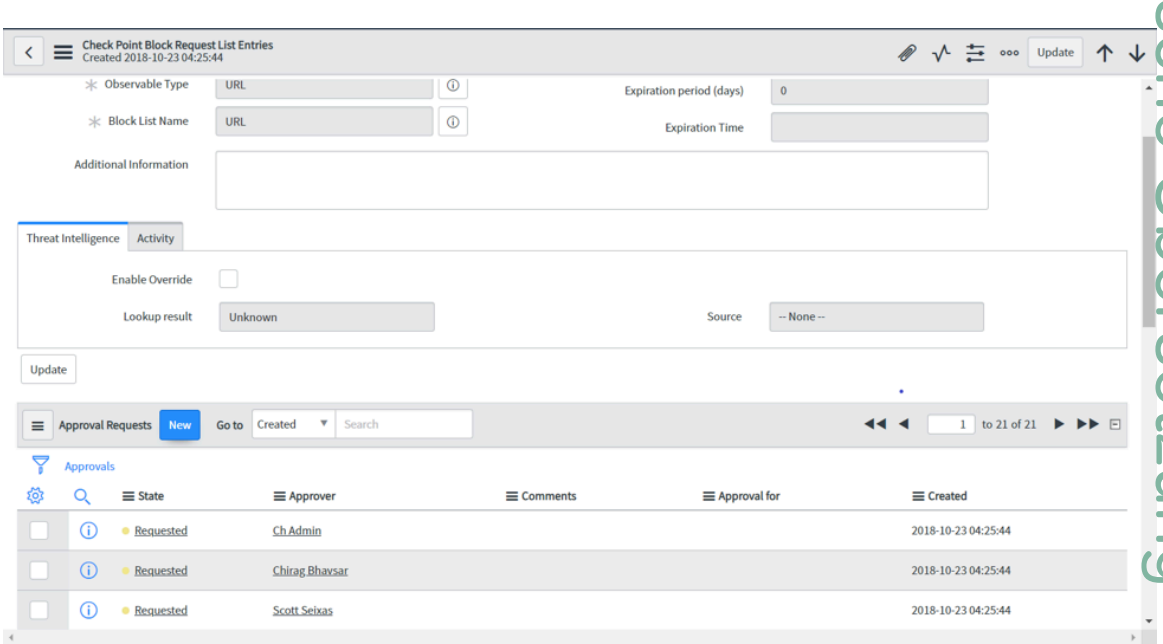
Erforderliche Rolle: sn.si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn der Genehmigungsprozess aktiviert ist, wird ein Sperrlisteneintrag erst dann in der Sperrliste aktiviert oder deaktiviert, wenn er genehmigt wurde.

Prozedur

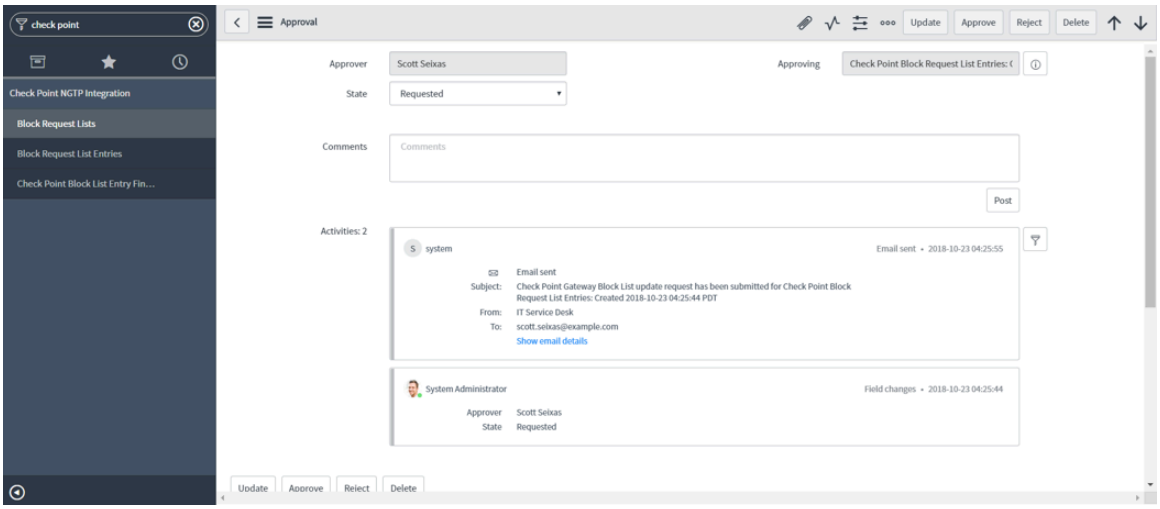
1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Einträge der Sperranforderungsliste**, und öffnen Sie den Datensatz Sperrlisteneintrag.
2. Scrollen Sie im Datensatz „Sperrlisteneintrag“ zum Abschnitt **„Genehmigungsanforderungen“**.



3. Klicken Sie unter Genehmigungsanforderungen auf ein Element in der Spalte **Status**, um es zu öffnen. Der Genehmigungsdatensatz wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



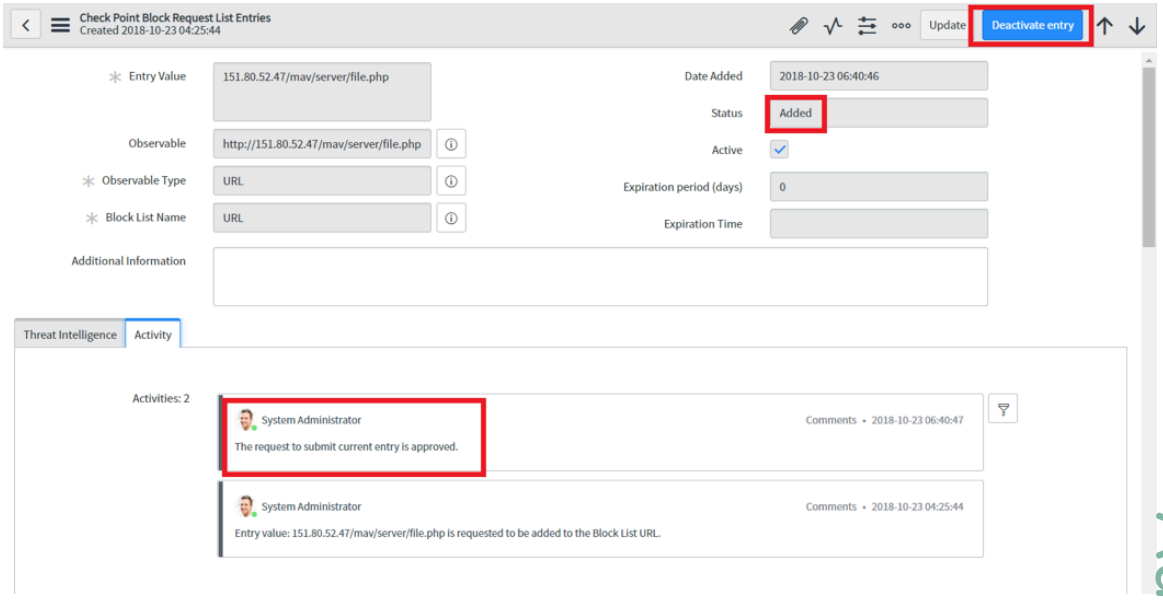
4. Wählen Sie eine Option zum Genehmigen des Sperrlisteneintrags aus.

Option	Beschreibung
Genehmigen	Im Eintragsdatensatz ändert sich das Feld Status in Hinzugefügt, und das Kontrollkästchen Aktiv wird aktiviert. Die Schaltfläche „Deaktivieren“ wird angezeigt und ist aktiv. Aus Arbeitsnotizen geht hervor, dass die Anforderung für den Sperrlisteneintrag genehmigt wurde.
Ablehnen	Im Eintragsdatensatz ändert sich das Feld Status in Abgelehnt, und das Kontrollkästchen Aktiv wird deaktiviert. Dies zeigt an, dass der Eintrag nicht auf dem Gateway blockiert ist. Aus Arbeitsnotizen geht hervor, dass die Anforderung für den Sperrlisteneintrag abgelehnt wurde.

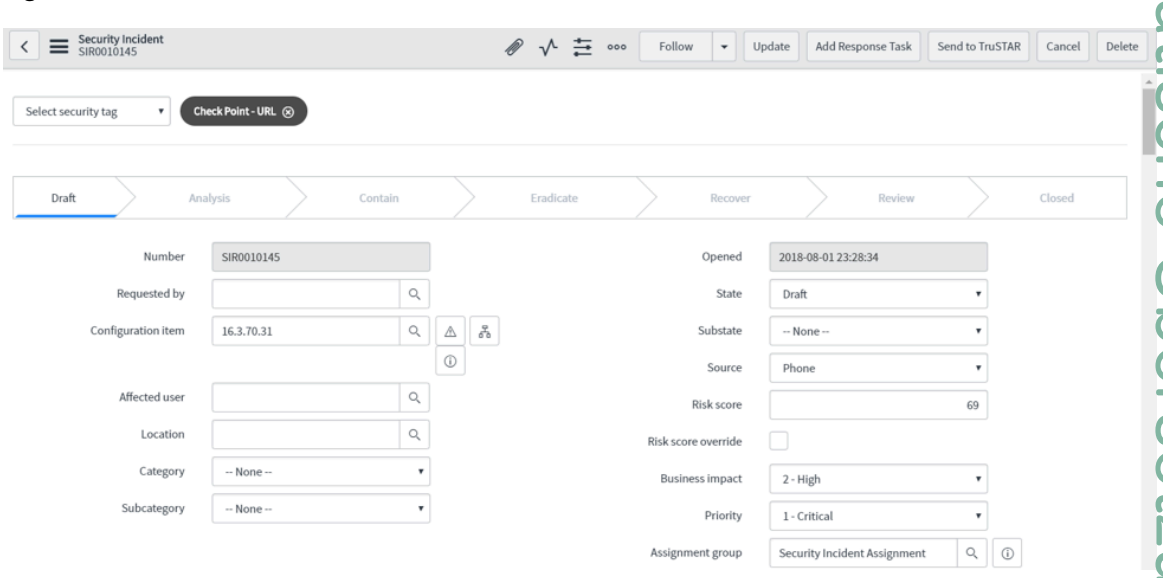
Nachdem Sie den Sperrlisteneintrag genehmigt haben und er aktiviert ist, ruft die Check Point Next Generation Firewall den Sperrlisteneintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, ist das erkennbare Element ab diesem Punkt blockiert. Beachten Sie, dass in der folgenden Abbildung das Kontrollkästchen Aktiv aktiviert ist, der Status Hinzugefügt lautet und in den Arbeitsnotizen angegeben ist, dass die Anforderung genehmigt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

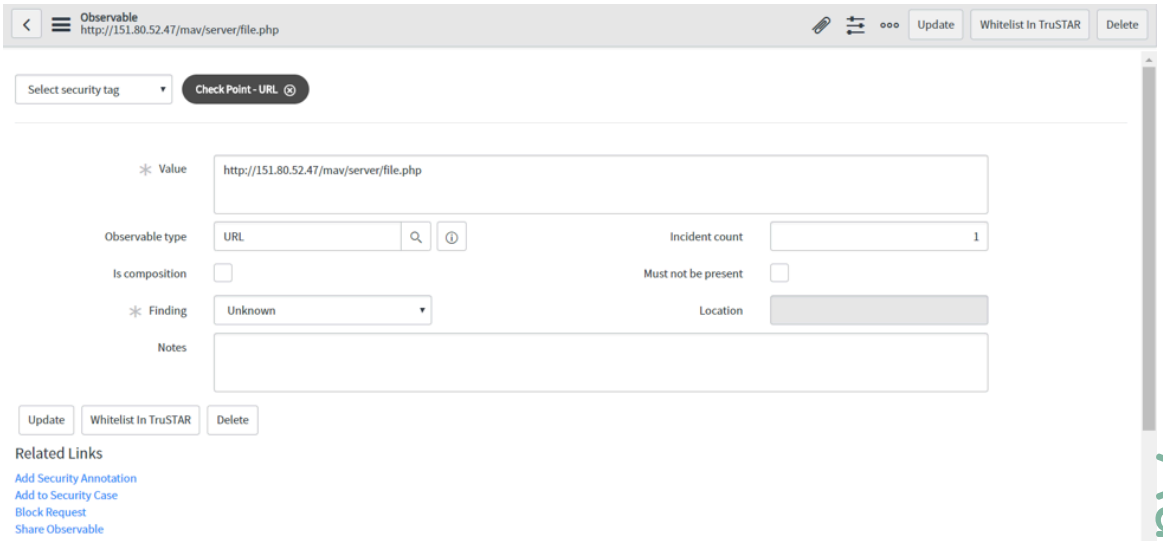


Nachdem der Sperrlisteneintrag genehmigt und aktiviert wurde, wird der Security Incident-Datensatz mit einem Sicherheits-Tag markiert. Das Tag wird oben im Datensatz angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Sicherheits-Tag wird auch im Datensatz des erkennbaren Elements angezeigt.



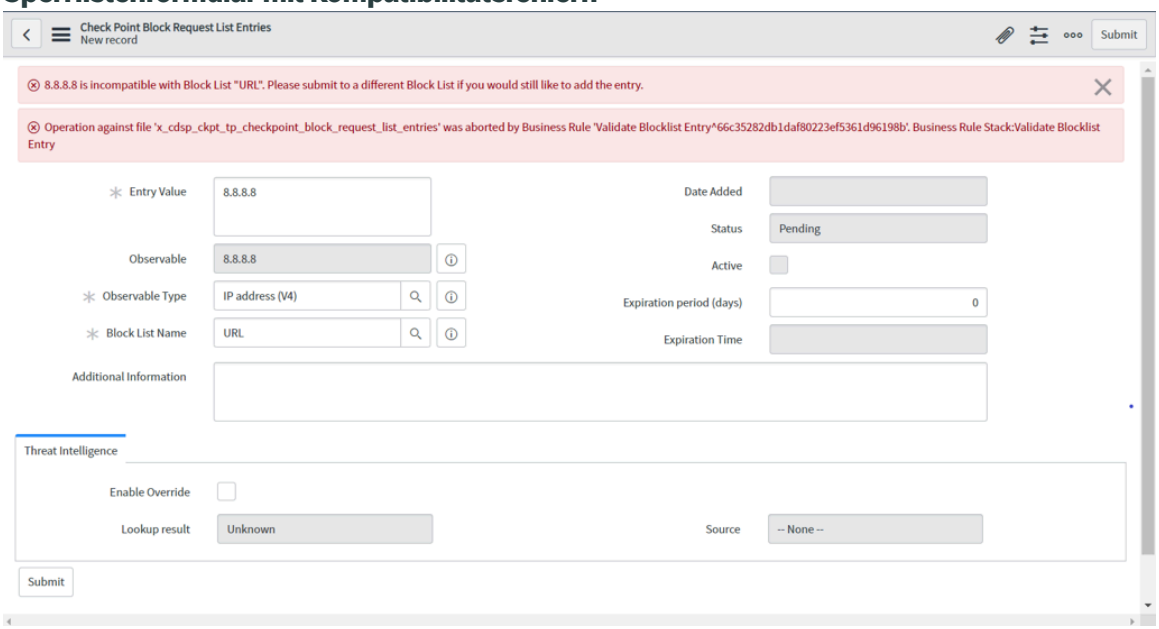
Ausnahmen für Sperrlisteneinträge für die Check Point NGTP Integration

Es gibt Einschränkungen für das Hinzufügen von Sperrlisteneinträgen zu Sperrlisten. Wenn beim Versuch, Sperrlisteneinträge zu Sperrlisten hinzuzufügen, Konflikte aufgrund von Duplikaten, Kompatibilität oder CIDR (Classless Inter-Domain Routing) bestehen, werden Fehlermeldungen angezeigt, die Ihnen helfen, diese Fehler zu beheben.

Kompatibilitätsausnahme

Jede Sperrliste akzeptiert nur Einträge, die mit dem entsprechenden erkennbaren Elementtyp kompatibel sind. Wenn Sie eine Domänen-Sperrliste erstellen und versuchen, ihr ein erkennbares IP-Adressen-Element anzuhängen, wird eine inkompatible Fehlermeldung angezeigt. Beispielsweise kann eine Domänensperrliste nur erkennbare Domänenelemente akzeptieren, wie in der folgenden Abbildung dargestellt.

Sperrlistenformular mit Kompatibilitätsfehlern

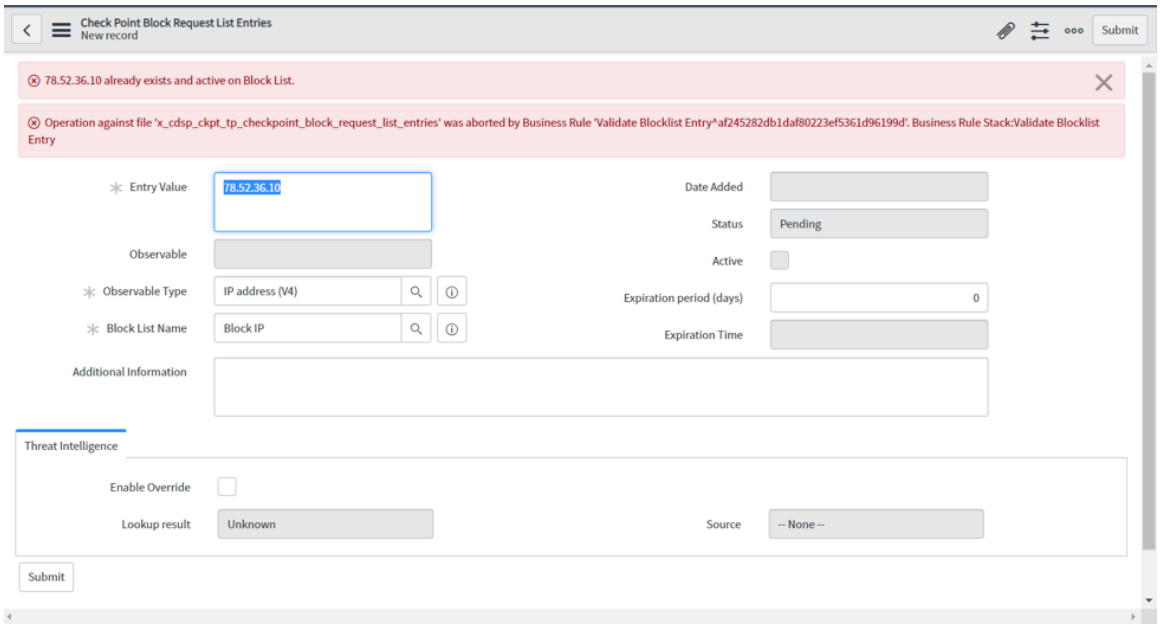


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

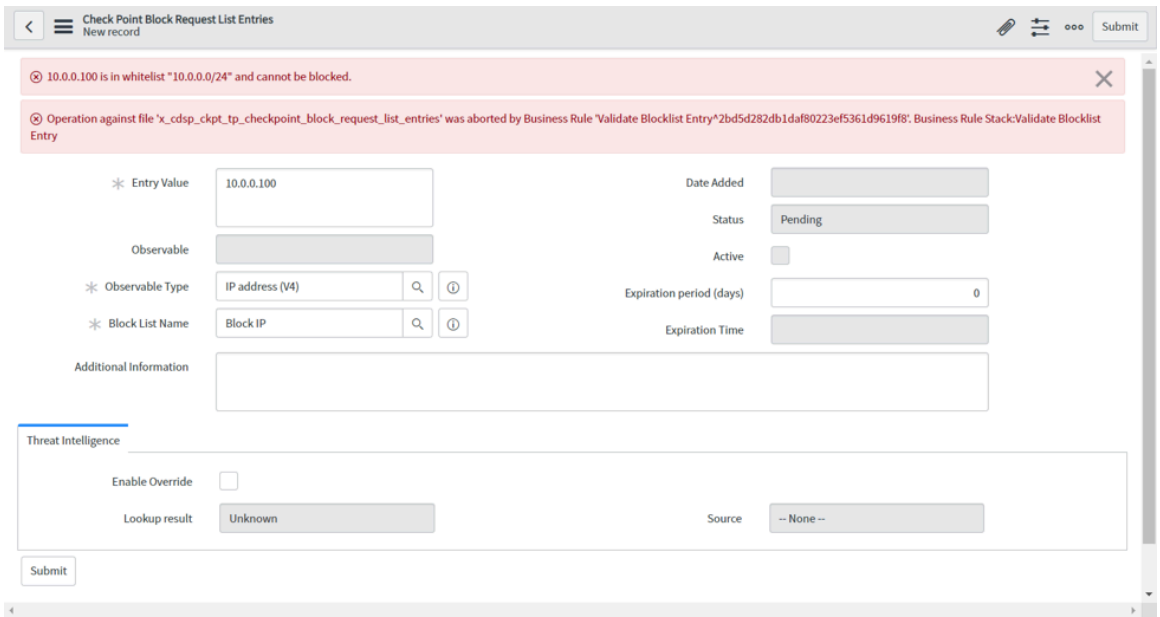
Duplizierungsausnahme

Ein erkennbares Element kann nicht auf mehreren Sperrlisten desselben erkennbaren Elementtyps aktiviert werden. Wenn ein erkennbares URL-Element bereits in einer URL-Sperrliste aktiviert ist und Sie versuchen, dasselbe erkennbare Element in einer Phishing-URL-Sperrliste zu aktivieren, wird eine Duplizierungsfehlermeldung angezeigt.



CIDR-Ausnahme (Classless Inter-Domain Routing).

Wenn Sie versuchen, eine einzelne IP-Adresse an eine Allow-Liste anzuhängen, und diese IP-Adresse Teil eines erkennbaren CIDR-Elements ist, das sich bereits in einer Sperrliste/Allow-Liste befindet, wird ein CIDR-Konfliktfehler angezeigt. Dieser Fehler weist darauf hin, dass eine einzelne IP-Adresse bereits in der Sperrliste oder Allow-Liste als Teil des erkennbaren CIDR-Elements enthalten ist. Beispiel: 192.168.24.25 ist Teil des CIDR-Blocks 192.168.0.0/22.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bearbeiten Sie den Sicherheits-Tag-Namen für die Integration Check Point NGTP

Wenn beim Erstellen des Sperrlistendatensatzes das Kontrollkästchen Tag anzeigen aktiviert ist, können Sie die Tag-Namen und Farben der Sicherheits-Tags bearbeiten. Mit Sicherheits-Tags können Sie bereits blockierte erkennbare Elemente nachverfolgen.

Vorbereitungen

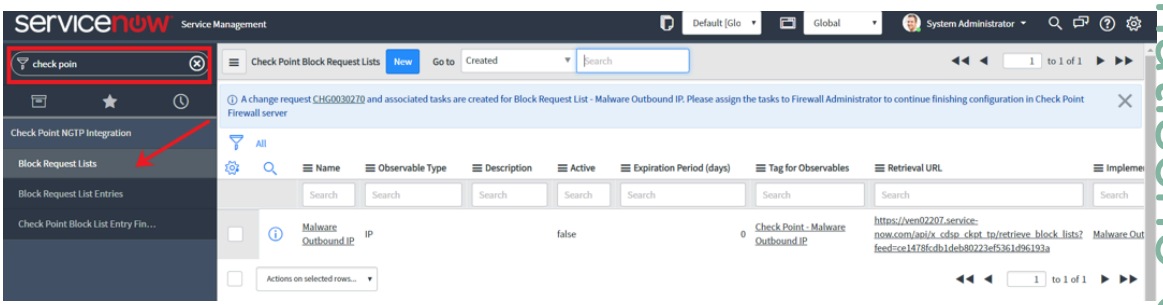
Erforderliche Rolle: sn.si.admin

Warum und wann dieser Vorgang ausgeführt wird

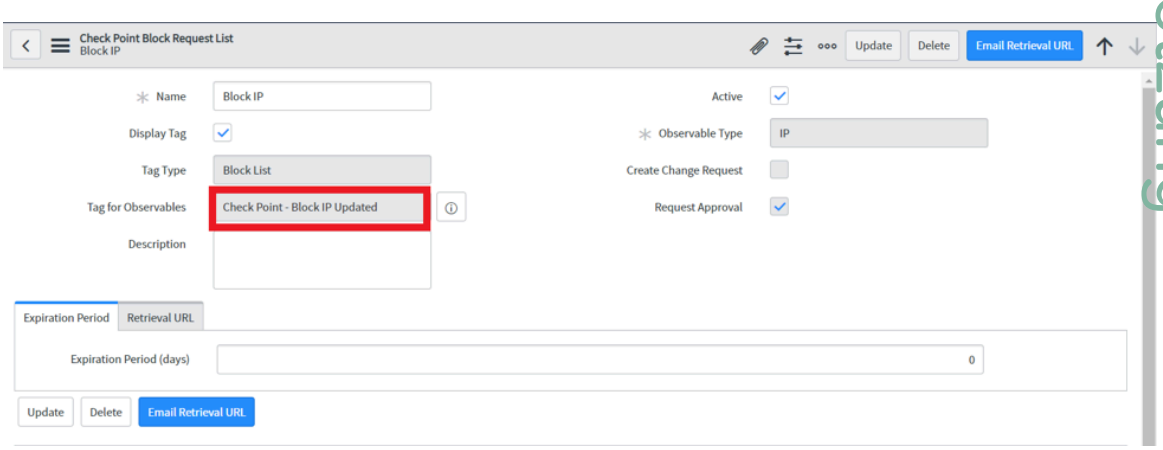
Mit Sicherheits-Tags können Sie schnell identifizieren, welche Security Incidents erkennbare Elemente auf einer Sperrliste haben. Mithilfe von Tags können Sie auch identifizieren, ob ein erkennbares Element bereits blockiert ist oder aus einer Sperrliste entfernt wurde. Standardmäßig ist die Farbe des Sicherheits-Tags für Sperrlisteneinträge schwarz und für Allow-Listeneinträge grau. Sie können die Namen und Farben der Tags ändern, um bestimmte Tags leichter zu erkennen.

Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Konfiguration der Sperranforderungsliste**.



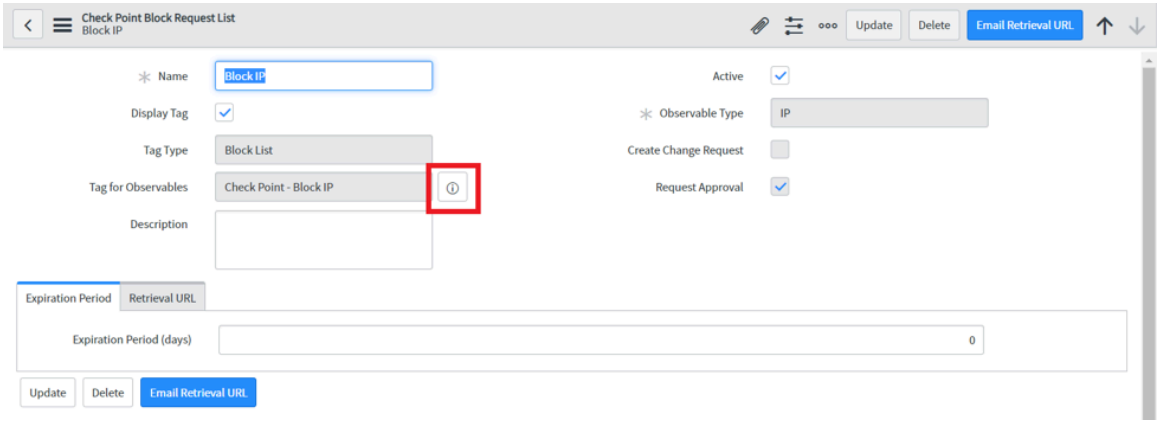
2. Klicken Sie auf ein Element in der Spalte **Name**, um es zu öffnen.
   Der Sperrlistendatensatz wird angezeigt. Standardmäßig ist der Sicherheits-Tag-Name derselbe Wert, den Sie im Feld Name der Sperrliste eingegeben haben, als Sie sie erstellt haben. Standardmäßig enthält der Name auch ein Sperrlistenpräfix, z. B. Sperrliste – Malware – schädliche URLs.



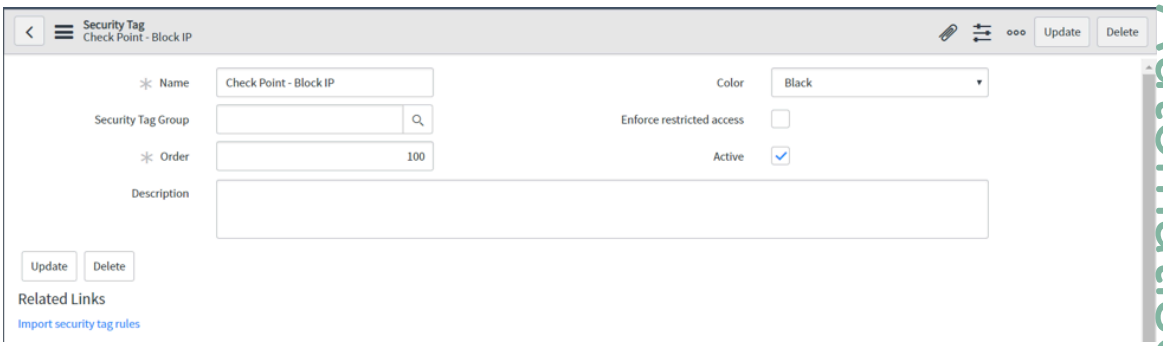
3. Klicken Sie auf das Informationssymbol neben dem Tag für erkennbare Elemente und dann auf Datensatz öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

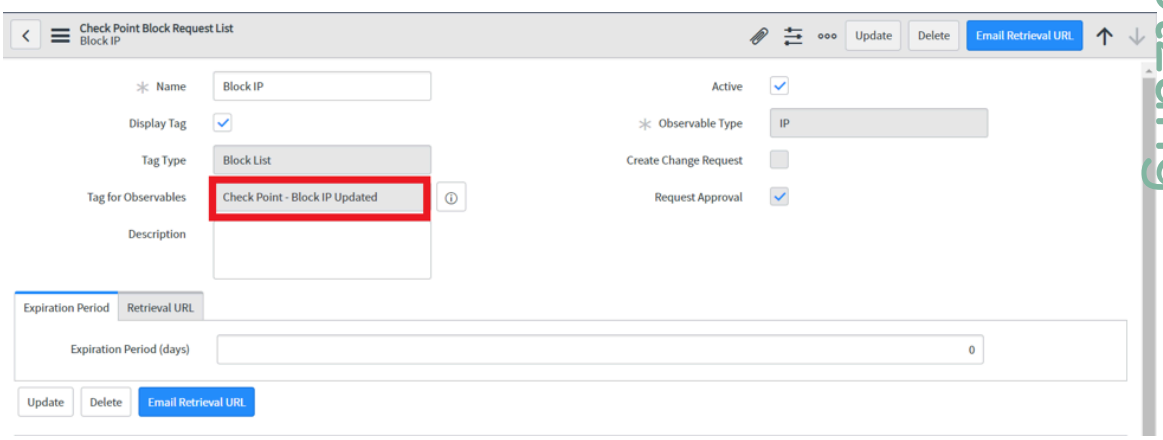


Das Sicherheits-Tag-Formular wird angezeigt.



4. Ändern Sie im Feld **Name** den Sicherheits-Tag-Namen.
5. Klicken Sie auf **Aktualisieren**.
   Der aktualisierte Sperrlistendatensatz wird mit dem geänderten Tag-Namen angezeigt.

Hinweis:
Im folgenden Beispiel wurde dem Tag-Namen „Ausgehend“ hinzugefügt. Behalten Sie das Prüfpunkt-Präfix in Ihrem neuen Tag-Namen bei, damit Sie leichter erkennen können, ob das Tag mit der Prüfpunkt-Firewallintegration der nächsten Generation verknüpft ist.

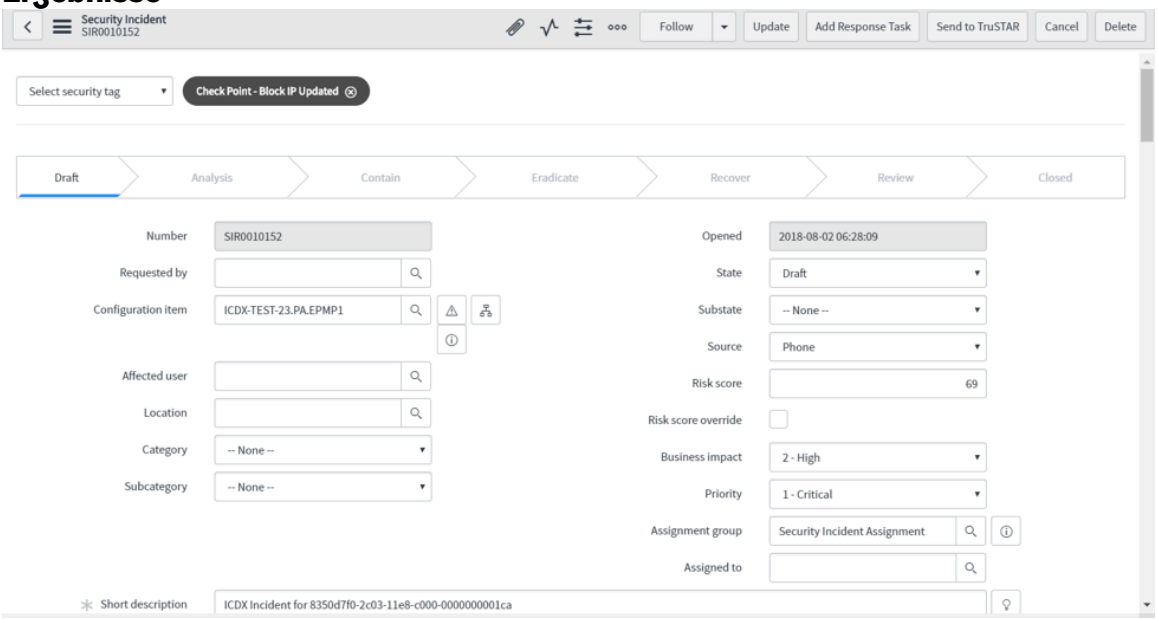


Die Sicherheits-Tags werden für jeden erkennbaren Elementtyp (IP, URL, Domäne) im Security Incident-Datensatz und im erkennbaren Elementdatensatz jedes Mal angezeigt, wenn dieses erkennbare Element zur Sperrliste hinzugefügt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse



Wenn ein erkennbares Element bereits einer Sperrliste hinzugefügt wurde und ein Sicherheits-Tag für einen Security Incident für dieses erkennbare Element angezeigt wird, wird das Sicherheits-Tag für die Sperrliste auch automatisch für alle nachfolgenden Security Incident-Datensätze angezeigt, die erstellt werden. Diese Duplizierung weist darauf hin, dass sich das erkennbare Element bereits in einer Sperrliste befindet. Sie müssen dieses erkennbare Element nicht hinzufügen und erneut blockieren.

Wenn ein erkennbares Element nicht mehr blockiert ist, wird im Security Incident-Datensatz oder im Datensatz des erkennbaren Elements kein Sicherheits-Tag angezeigt. In dieser Instanz gibt kein Sicherheits-Tag an, dass das Ablaufdatum des erkennbaren Elements möglicherweise verstrichen ist oder das erkennbare Element aus einer Sperrliste deaktiviert wurde.

Deinstallieren Sie die -Integration Check Point NGTP .

Wenn Sie die Check Point NGTP Integration von Ihrer Now Platform-Instanz deinstallieren und alle Reste aus der Integration entfernen möchten, finden Sie auf der ServiceNow-Dokumentationswebsite Anweisungen zum Deinstallieren von Anwendungen.

Erforderliche Rolle: admin

Integration mit CrowdStrike Falcon Host

Die CrowdStrike Falcon Host -Integration ermöglicht es Ihnen, erkennbare Elemente in einem Security Incident in eine Beobachtungsliste zu verschieben, um zusätzliche Warnungen zu generieren. Diese Integration ist eine Implementierung des Workflows „CrowdStrike Falcon Host – In Beobachtungsliste veröffentlichen“.

Erkunden	Einrichten
Security Incident Response-Integrationen	Erste Schritte mit der CrowdStrike Falcon Host -Integration

---

Verwenden	Entwickeln

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Führen Sie Suchen für erkennbare Elemente durch	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Automatische Übersetzung

Erste Schritte mit der CrowdStrike Falcon Host -Integration

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der CrowdStrike Falcon Host -Integration, schnell aktivieren und einrichten. Bevor Sie die CrowdStrike Falcon Host -Integration verwenden können, müssen Sie sie von ServiceNow Store herunterladen und dann einen Anwendernamen und ein Passwort hinzufügen.

Vorbereitungen

- Wenn Sie CrowdStrike Falcon Host die -Integration von einer früheren Version aktualisieren, müssen Sie die vorhandene Konfiguration löschen und eine neue Konfiguration einrichten. Die neue Integration unterstützt die OAuth2-Authentifizierung. Dieses Update erfordert die Eingabe der **API-Client-ID** und des **API-Clientgeheimnisses,** um sich zu authentifizieren und die Konfiguration abzuschließen.
- Aktivieren Sie in den **API-Bereichen**des Portals CrowdStrike Falcon Host die Einstellung **Lesen** und **Schreiben** für **IoCs (Indicators of Compromise)**.

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte CrowdStrike Falcon Host auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus, um die Konfiguration abzuschließen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CrowdStrike Falcon-Hostkonfiguration

Feld	Beschreibung
Name	Name der Integration, z. B. demo-1.
API-Client-ID	Client-ID, die Sie im Abschnitt mit den Einstellungen Ihres Kontoprofils im Portal CrowdStrike Falcon Host abrufen.
API-Client-Geheimnis	Der geheime Clientschlüssel, den Sie im Abschnitt mit den Einstellungen Ihres Kontoprofils im Portal CrowdStrike Falcon Host erhalten.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nach der Konfiguration kann die Integration CrowdStrike Falcon Host für die Veröffentlichung von erkennbaren Elementen in Beobachtungslisten in Security Incident Responseausgewählt werden.

CrowdStrike Falcon Host von Security Operations – Flow „In Beobachtungsliste veröffentlichen“.

Der Flow Designer **„CrowdStrike Falcon Host von Security Operations – In Beobachtungsliste veröffentlichen“** wird verwendet, um die Beobachtungsliste für das Generieren von Warnungen oder Ereignissen anzugeben. Die Warnungen und Ereignisse werden im CrowdStrike Falcon Host-System je nach Konfiguration angezeigt.

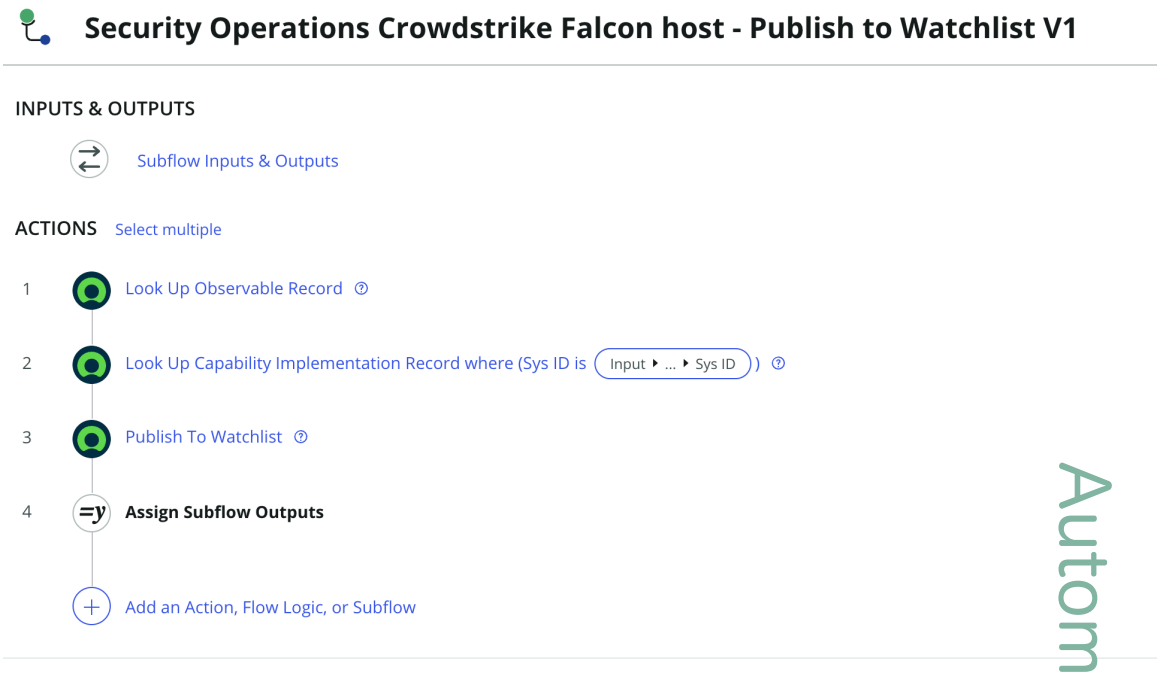
Flow zur Veröffentlichung in Beobachtungsliste

Dieser Flow Designer wird von Security Operations-Integration: Fähigkeit „In Beobachtungsliste veröffentlichen“. ausgelöst, wenn Sie ein oder mehrere erkennbare Elemente auswählen, die einem Security Incident zugeordnet sind, und die UI-Aktion In Beobachtungsliste veröffentlichen verwenden, um die erkennbaren Elemente auf eine Beobachtungsliste zu verschieben. Die erkennbaren Elemente können dann verwendet werden, um zusätzliche Warnungen zu generieren. Weitere

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen finden Sie unter Veröffentlichen Sie erkennbare Elemente in einer Drittanbieter-



Beobachtungsliste.

CrowdStrike Falcon Insight für die Security Operations -Integration

Mit der CrowdStrike Falcon InsightSecurity Operations]-Integration für können Sie Korrekturaktionen für die Endpunkte in Echtzeit durchführen, Profile verwenden, um Details zum Host zu sammeln, und mit dem Produkt Now Platform Security Incident Response spezifische Abfragen oder Aktionen am Endpunkt durchführen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Die CrowdStrike Falcon Insight -Integration für Security Operations funktioniert mit Now Platform, sodass Sie zusätzliche Einblicke in den Umfang eines incident erhalten. CrowdStrike Falcon Insight erfasst alle relevanten Endpunktereignisaktivitäten. Mit Now Platform können Sie sich auf Untersuchungen und Korrekturaktionen konzentrieren.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow
CrowdStrike Falcon Insight für Security Operations	Erste Schritte mit der CrowdStrike Falcon Insight -Integration

Erste Schritte mit der CrowdStrike Falcon Insight -Integration

Sie können CrowdStrike Falcon Insight als Schnittstelle mit Ihrer Instanz Now Platform und Ihrem Produkt Security Incident Response aktivieren und einrichten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Bevor Sie CrowdStrike Falcon Insight für die Security Operations -Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

Warum und wann dieser Vorgang ausgeführt wird

Prüfliste

Setupaufgabe	Beschreibung
Weisen Sie die erforderlichen Rollen Now Platform und Security Incident Response zu, und überprüfen Sie sie.	Diese Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Die Rolle admin installiert die Integration aus ServiceNow Store und weist die Rolle sn_si.admin zu. • Die Rolle sn_si.admin konfiguriert die Integration, erstellt und aktiviert Profile und weist dann die Rolle sn_si.analyst zu. • Die Rolle sn_si.analyst reagiert auf Security Incidents, startet Profile manuell und kann Anforderungen für Aktionen wie das Isolieren des Hosts oder das Entfernen der Hostisolierung für eine genehmigte Gruppe übermitteln.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren.	Das Plugin ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] ist erforderlich. Dieses Plugin ermöglicht die Ausführung von IntegrationHub-Aktionen und -Flows: Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren, die für die Integration erforderlich sind. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie sie einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation zu gewährleisten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	1. Security Incident Response Abhängigkeit (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration **5.** Threat Intelligence Support Common **6.** Trusted Security Circles **7.** Security Operations Setup-Assistent **8.** Security Incident Response
Richten Sie eine Genehmigungsgruppe ein.	Eine optionale Genehmigungsfunktion ist verfügbar, um Hostcomputer zu isolieren, sie im Netzwerk wiederherzustellen und Sichtungssuchen zu initiieren. Zum Aktivieren dieser Option benötigen Sie die vorherige Genehmigung der Rolle „sn_si.admin“, bevor Hostcomputer isoliert und in Ihrem Netzwerk wiederhergestellt werden oder wenn Sichtungssuchen durchgeführt werden. Wenn Sie eine zusätzliche Kontrollebene für diese Aktionen benötigen, aktivieren Sie bei der Konfiguration des Profils die Option **Genehmigung erforderlich**. Die Genehmigungsberechtigung wird dem Benutzer mit der Rolle sn_si.admin zugewiesen. Sie können diese Genehmigungsberechtigung auch einer Genehmigungsgruppe neu zuweisen.
Die CrowdStrike Falcon Platform-Rollen zuweisen und überprüfen	Die folgenden Rollen sind auf der CrowdStrike Falcon-Plattform für die Integrationskonfiguration erforderlich: • Zum Anzeigen, Erstellen oder Ändern von API-Clients oder Schlüsseln ist die Rolle „Falcon-Administrator“ erforderlich. • Zum Erstellen und Ausführen von anwenderdefinierten Skripts ist die Rolle „Real Time Responder – Administrator“ erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	• Die Rolle „Echtzeit-Responder – Aktiver Responder“ ist zum Erstellen und Ausführen von anwenderdefinierten Skripts erforderlich.
Stellen Sie sicher, dass die anwenderdefinierten Skriptrollen und Berechtigungen in der CrowdStrike Falcon-Plattform aktiviert sind.	Diese Integration verwendet die anwenderdefinierten Skripts von CrowdStrike für einige der Ergänzungsfunktionen. • Vergewissern Sie sich, dass die Rollen „Echtzeit-Responder – Administrator“ und „Echtzeit-Responder – Aktiver Responder“ verfügbar sind. • Stellen Sie sicher, dass die **Richtlinienoption Standard (Windows)** unter Konfiguration > Antwortrichtlinien in der CrowdStrike Falcon-UI aktiviert ist. • Vergewissern Sie sich, dass in der CrowdStrike Falcon-UI unter „Echtzeitfunktionalität“ **Echtzeitantwort** und **anwenderdefinierte Skripts** aktiviert sind.
Generieren Sie API-Clients und -Schlüssel in der CrowdStrike Falcon-Plattform.	Erstellen Sie die CrowdStrike-API-Clients oder -Schlüssel in der CrowdStrike Falcon-Plattform, die in der Integrationskonfiguration Now Platform verwendet werden sollen.

Erstellen Sie den CrowdStrike API-Client und generieren Sie Schlüssel

Erstellen Sie den CrowdStrike-API-Client, und generieren Sie die Client-ID und den Schlüssel, die Sie zum Konfigurieren der CrowdStrike Falcon Insight -Integration verwenden.

Vorbereitungen

Erforderliche Rolle: CrowdStrike Falcon-Administrator

Prozedur

1. Navigieren Sie auf der CrowdStrike Falcon-Plattform zu **API-Clients und Schlüssel**.
2. Klicken Sie in der Tabelle „OAuth2-API-Clients **“ auf Neuen API-Client hinzufügen**.
3. Geben Sie die folgenden Details ein, um Ihren API-Client zu definieren:

Feld	Beschreibung
Clientname	Geben Sie den Client-Namen ein. Dies ist ein Pflichtfeld.
Beschreibung	Geben Sie die Beschreibung für den Client-Namen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
API-Bereiche	Das Definieren der Umfänge ist erforderlich. **Wichtig:** Stellen Sie sicher, dass Sie das API-Konto aktivieren, und stellen Sie sicher, dass die folgenden Bereiche für das API-Konto aktiviert sind: ○ Aktivieren Sie Lese- und Schreibbereiche für die Hosts-API ○ Aktivieren Sie den Lesebereich für die Indikatoren-API

4. Klicken Sie auf **Hinzufügen**, um den API-Client zu speichern und die Client-ID und den geheimen Schlüssel zu generieren.

CrowdStrike Falcon Insight installieren und konfigurieren

Installieren und konfigurieren Sie die Anwendung CrowdStrike Falcon Insight für Security Operations aus der Instanz ServiceNow Store in Ihrer Instanz Now Platform.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis:
Eine Fähigkeit kann nur einem Profil zugeordnet werden. Sie können eine Fähigkeit nicht mit mehreren Profilen verknüpfen. Wenn Sie CrowdStrike-Server konfigurieren, können Sie eine CrowdStrike-Fähigkeit nicht für mehrere Profile wiederverwenden, die den CrowdStrike-Server gemeinsam nutzen. Ihre Profile können die gleiche CrowdStrike-Fähigkeit haben. Jedes Profil muss einen eigenen CrowdStrike-Server verwenden.

Prozedur

1. Laden Sie die Integration von CrowdStrike Falcon Insight für Security Operations aus dem ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Integrationskachel CrowdStrike Falcon Insight für Security Operations, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus, um die Konfiguration abzuschließen:

CrowdStrike Falcon Insight-Konfiguration

Feld	Beschreibung
Name	Name der Integration, z. `B. demo-1`.
CrowdStrike Falcon Insight-API-URL	Basis-URL, die die CrowdStrike-API hostet. Geben Sie die URL mit dem HTTPS-Protokoll ein. Beispiel: https://api.rowdstrike.com.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Client-ID	Client-ID, die Sie im Abschnitt mit den Einstellungen Ihres Kontoprofils im -Portal CrowdStrike Falcon Insight abrufen.
Geheimer Clientschlüssel	Der geheime Clientschlüssel, den Sie im Abschnitt mit den Einstellungen Ihres Kontoprofils im Portal CrowdStrike Falcon Insight erhalten.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem die Integration erfolgreich validiert und übermittelt wurde, wird sie auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Sie können das Modul CrowdStrike Falcon Insight im Anwendungsnavigator anzeigen.

Erstellen Sie eine Genehmigungsgruppe

Erstellen Sie eine Genehmigungsgruppe für die Integration CrowdStrike Falcon Insight für Security Operations, die Anforderungen zum Isolieren von Hostcomputern, deren Wiederherstellung im Netzwerk und das Initiieren von Sichtungssuchen genehmigen kann.

Vorbereitungen

Sie können die Genehmigungsberechtigung nicht erneut einer Gruppe zuweisen, es sei denn, in Ihrer Instanz ist eine Genehmigungsgruppe verfügbar.

Hinweis:
Die Option „Genehmigungen“ in der Profilkonfiguration wird nur für die Funktionen „Host isolieren“ und „Hostisolierung entfernen“ angezeigt.

Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**.
2. Klicken Sie in der Gruppenliste auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungsgruppe“

Feld	Beschreibung
Name	Name der Gruppe, die beim Senden einer Genehmigungsanforderung angezeigt wird.
Gruppen-E-Mail	Gruppen-E-Mail-Verteilerliste oder E-Mail-Adresse des Ansprechpartners, z. B. des Gruppenmanagers
Manager	Name des Gruppenmanagers Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen.
Übergeordnet	Name der übergeordneten Gruppe, wenn sie einem übergeordneten Element zugeordnet ist.
Typ	Kategorien von Gruppen
Lieferanten	Rolle vendor_manager, die Sie Benutzern im Vendorenverwaltungsprozess Ihrer Organisation zuweisen.
Beschreibung	Zusätzliche Informationen zur Gruppe.

4. Klicken Sie auf **Absenden**.
   Die neue Gruppe wird in der Gruppenliste angezeigt.

Diese Gruppe ist für die Verarbeitung von Anforderungen verfügbar, wenn Sie während der Konfiguration dieses Profils die Option **„Genehmigung erforderlich“** aktivieren.

Um von Benutzern mit der Rolle sn_si.analyst übermittelte Anforderungen zu überwachen und zu verarbeiten, navigieren alle Mitglieder der Genehmigungsgruppe zur Registerkarte **Meine Genehmigungen** in Now Platform.

Nächste Maßnahme

Der nächste Schritt besteht in der Installation und Konfiguration der Anwendung CrowdStrike Falcon Insight aus dem ServiceNow Store.

Erstellen Sie ein Fähigkeitsprofil für die Integration CrowdStrike Falcon Insight .

Erstellen Sie ein Profil, und wählen Sie die CrowdStrike Falcon Insight -Fähigkeiten aus, die das Profil ausführen soll.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Überlegen Sie, warum Sie ein Profil erstellen möchten, bevor Sie ihm CrowdStrike Falcon Insight -Fähigkeiten hinzufügen. In der folgenden Tabelle sind die Fähigkeiten aufgeführt, die Sie einem Profil hinzufügen müssen, wenn das Profil bestimmte Abfragen oder Aktionen ausführen soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können ein einzelnes Profil erstellen, das Abfragen von Systemdetails ausführt, angemeldete Benutzer auflistet, laufende Services abruft, laufende Prozesse abruft, Netzwerkstatistiken abruft, den Host isoliert und den isolierten Host entfernt. Alternativ können Sie mehrere Profile mit jeweils einer eigenen Fähigkeit erstellen.

Hinweis:
Die Funktionen „Host isolieren“, „Isolierung entfernen“ und „Datei abrufen“ können beim Erstellen eines Profils nicht mit anderen Fähigkeiten zusammengeführt werden.

Profiltypen und erforderliche CrowdStrike Falcon Insight-Fähigkeiten

Profilzweck	CrowdStrike-Fähigkeiten
Erfassen Sie Hostdetails und angemeldete Benutzer	• **Hostdetails abrufen** • **Angemeldete Anwender abrufen**
Ruft die Netzwerkstatistiken, Prozesse und Services ab, die für einen Host ausgeführt werden	• **Netzwerkstatistiken abrufen** • **Laufende Prozesse abrufen** • **Laufende Services abrufen**
Isolieren Sie einen Host	**Host isolieren**
Entfernt die Isolation für einen Host	**Isolation entfernen**
Ruft eine Datei von einem Hostendpunkt ab	**Datei abrufen**

Prozedur

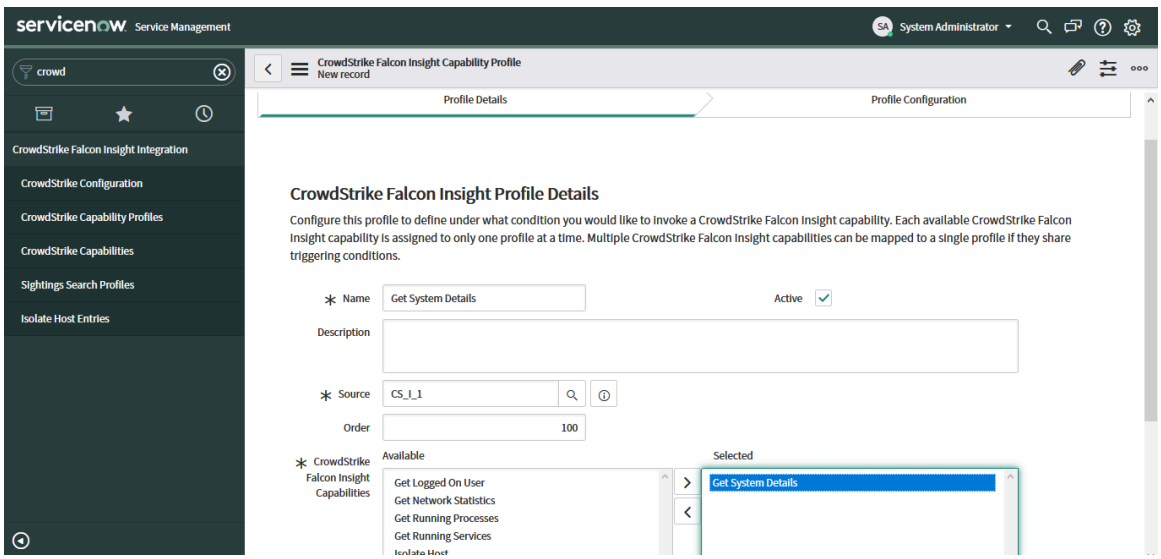
1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **CrowdStrike-Fähigkeitenprofile**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Name für das neue Fähigkeitsprofil. Dieser Name hilft Ihnen, den Profiltyp zu identifizieren, und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist.
Aktiv	Gibt an, ob das Profil aktiv ist oder nicht. Wenn das Profil aktiv ist, wird es automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den von Ihnen in der Konfiguration angegebenen Filterbedingungen entspricht.
Beschreibung	Eindeutige Beschreibung für das Fähigkeitsprofil.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle	Name des Servers. Sie können nur zuvor konfigurierte Server aus der Liste anzeigen.
Bestellung	Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Flow mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Beispiel: 100, 200, 300, 400. Standard: 100
CrowdStrike Falcon Insight-Fähigkeiten	Fähigkeiten des CrowdStrike Falcon Insight-Profils. Wählen Sie in der Spalte **Verfügbar** bis **Ausgewählt**die gewünschten Fähigkeiten für dieses Profil aus.

Das folgende Beispiel zeigt ein vollständiges Formular für ein Profil mit der Fähigkeit „Systemdetails abrufen“.



4. Klicken Sie auf **Next (Weiter)**.

Nächste Maßnahme

Jetzt können SieIhr Profil konfigurieren. Stellen Sie sicher, dass Sie die Konzepte zum Konfigurieren von Profilen und Auslöserbedingungen überprüft haben, bevor Sie das Profil konfigurieren.

Konfigurieren Sie Profile und Security Incidents für die -Integration CrowdStrike Falcon Insight .

Konfigurieren Sie Ihre Profileinstellungen so, dass das Profil nur unter den von Ihnen festgelegten Bedingungen ausgelöst wird.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie die Bedingungen, die die Fähigkeiten CrowdStrike Falcon Insight, die Sie für das Profil ausgewählt haben, automatisch auslösen. Sie können auch ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen. In diesem alternativen Feld können Sie Filterbedingungen festlegen, sodass nur die Security Incidents, die mit dem auslösenden Ereignis zusammenhängen, das Profil automatisch auslösen.

Hinweis:
Navigieren Sie erst zur Seite Profilkonfiguration, nachdem Sie die Profildetails eingegeben haben. Weitere Informationen finden Sie unter Fähigkeitsprofil für die CrowdStrike Falcon Insight-Integration erstellen.

Prozedur

1. Überprüfen und konfigurieren Sie auf der Seite „Profilkonfiguration“ die folgenden Abschnitte:

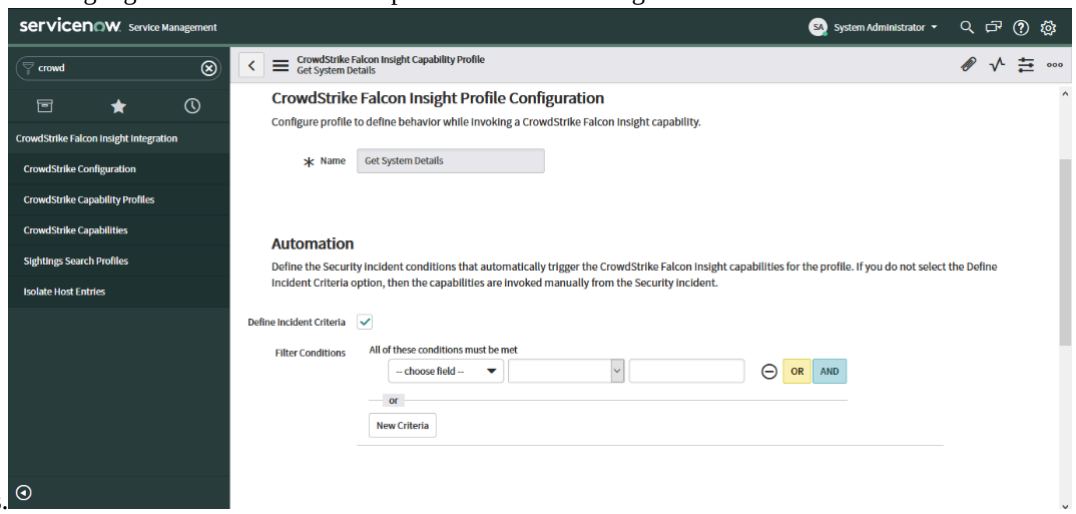
Incident-Kriterien definieren (Automatisierung)

Definieren Sie die Bedingungen für Security Incidents, die automatisch die Fähigkeiten CrowdStrike Falcon Insight für das Profil auslösen. Wenn Sie die Option **Kriterien für Incident definieren** nicht auswählen, werden die Fähigkeiten manuell über den Security Incident aufgerufen.

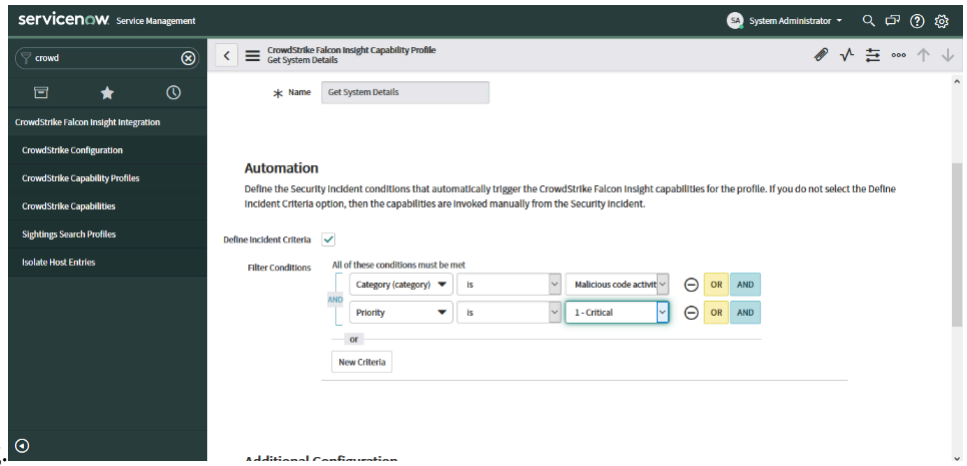
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie die Option **Kriterien für Incident definieren** aus.

b. Um die Bedingungen zu definieren, wählen Sie im Abschnitt Filterbedingungen ein Feld und die entsprechende Anforderung aus.



c. Geben Sie im Feld **Neue Kriterien** die neuen Kriterien ein, und definieren Sie dann die **ODER-** oder die **UND-**Bedingung.

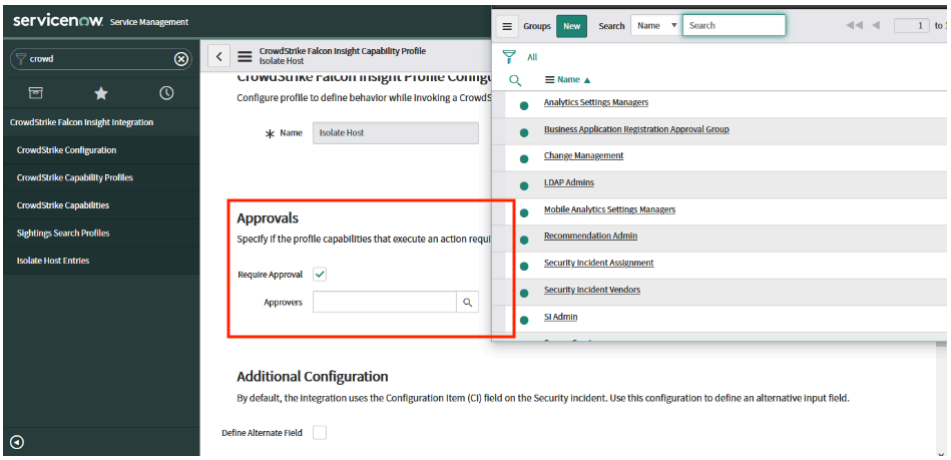


Genehmigungen

Um eine zusätzliche Kontrollebene bereitzustellen, wenn Sie die CrowdStrike Falcon Insight-Fähigkeiten verwenden, wählen Sie die Option **Genehmigung erforderlich** aus. Die Option „Genehmigungen“ in der Profilkonfiguration wird nur für die Funktionen Host isolieren und Hostisolierung entfernen angezeigt.

Hinweis:
Die Genehmigungsberechtigung wird dem Benutzer mit der Rolle sn_si.admin zugewiesen. Sie können diese Genehmigungsberechtigung auch einer Genehmigungsgruppe neu zuweisen. Weitere Informationen finden Sie unter Genehmigungsgruppe einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zusätzliche Konfiguration

Wählen Sie ein alternatives Feld im Security Incident aus, um alle übereinstimmenden CI-Daten anzuzeigen, die Sie beim Scannen Ihrer Assets gefunden haben. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) für den Security Incident.

a. Wählen Sie die Option **Alternatives Feld definieren** aus.

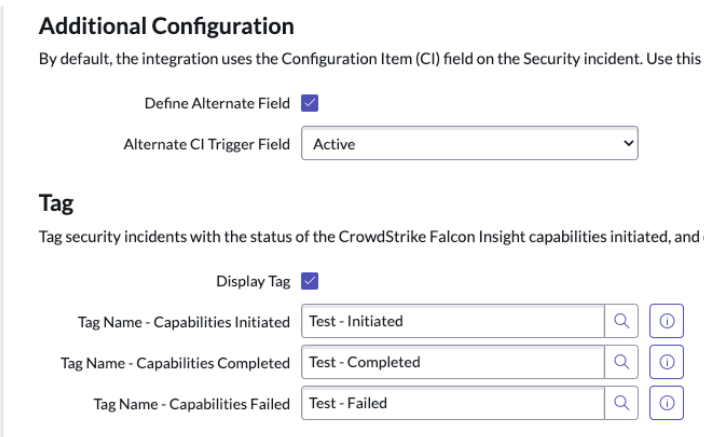
b. Wählen Sie im **Feld Alternative CI-Auslöser**ein Eingabefeld aus.

> **Hinweis:**
> Weitere Informationen hierzu finden Sie unter Funktionsweise von Auslöserbedingungen mit Konfigurationselementen für Profile verstehen.

Tags

Um Security Incidents mit den Tags CrowdStrike Falcon Insight Fähigkeiten – Initiiert, Fähigkeiten – Abgeschlossen und Fähigkeiten – Fehlgeschlagen zu kennzeichnen, wählen Sie die Option **Tags anzeigen** aus. Standardmäßig ist diese Option für alle Profile deaktiviert.

> **Hinweis:**
> Diese Tags werden mit dem Basissystem bereitgestellt. Bei Bedarf können Sie eigene Tags erstellen.



2. Klicken Sie auf **Erledigt**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsweise von Auslösebedingungen mit einem Konfigurationselement für ein Profil

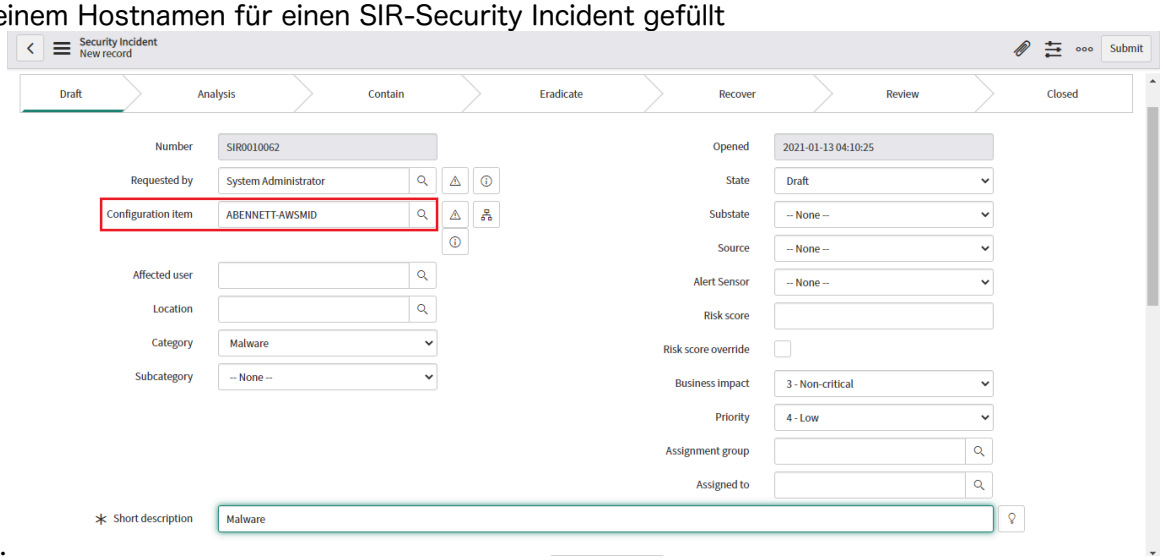
Sie können die Profileinstellungen so konfigurieren, dass ein Profil nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt ist, oder Sie können ein Profil einrichten, um nach bestimmten Feldwerten in einem Security Incident zu suchen.

Nachdem Sie ein Profil erstellt und die Fähigkeiten CrowdStrike Falcon Insight ausgewählt haben, mit denen das Profil ausgeführt werden soll, können Sie Auslöserbedingungen festlegen, sodass Ihr Profil automatisch ausgeführt wird, wenn die Standardfeldwerte mit dem Security Incident Now Platform übereinstimmen.

Standardmäßig verwendet die Integration das Feld **Configuration Item** (CI) für einen Security Incident. Dieses Feld wird verwendet, um Ihre Asset-IDs mit den Informationen abzugleichen, die in der -Datenbank Now Platform gespeichert sind. Wenn ein SIR-Security Incident von einem Sicherheitsereignis erstellt wird und ein Profil aktiviert ist, werden Ihre Assets nach einem übereinstimmenden Wert für den Hostnamen oder eine IP-Adresse gescannt.

Wenn in der Datenbank ein übereinstimmender Wert gefunden wird, werden diese Daten in der Konsole CrowdStrike Falcon Insight gesammelt und in Ihre Instanz Now Platform abgerufen, wo sie in den zugehörigen Listen eines Security Incident angezeigt werden.

Das folgende Beispiel zeigt ein Configuration Item-Feld, das mit einem Hostnamen für einen SIR-Security Incident gefüllt wird.

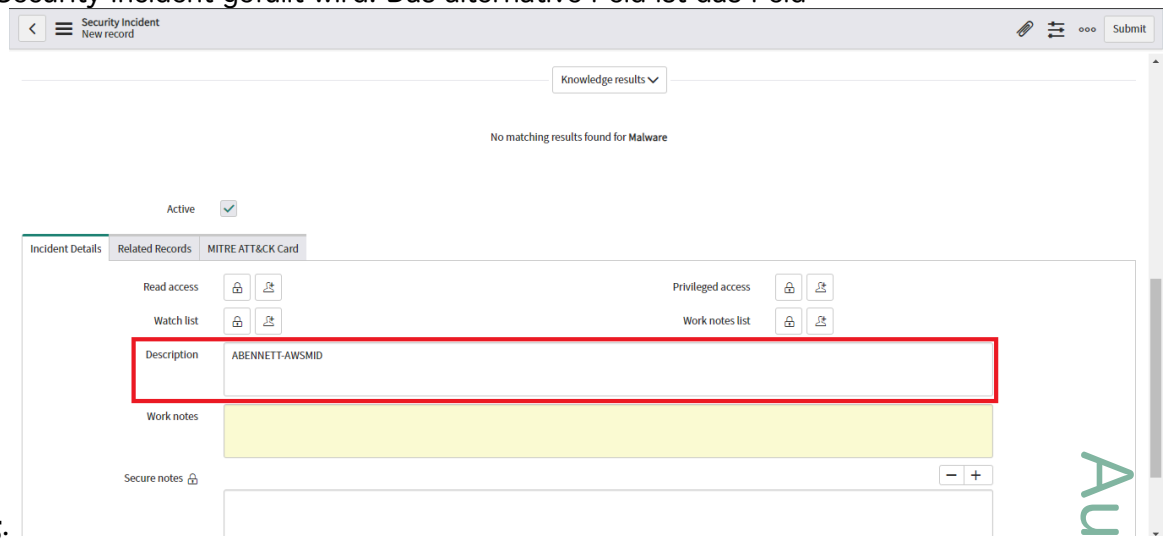


Wenn das Feld **Configuration item** (CI) nicht mit einem Hostnamen oder einer IP-Adresse gefüllt ist, die der -Datenbank entspricht, können Sie ein anderes Feld im Security Incident auswählen, um übereinstimmende CI-Daten anzuzeigen, die Sie beim Scannen Ihrer Assets finden.

Wenn Sie das Profil-Setup konfigurieren, können Sie ein alternatives **CI-** Auslöserfeld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass die CI-Daten aus der Suche CrowdStrike Falcon Insight für den zugehörigen Security Incident ausgefüllt werden. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Wenn das CI-Feld im zugehörigen Security Incident beim Erstellen des incident nicht ausgefüllt ist, wählen Sie das alternative CI-Feld aus, um sicherzustellen, dass Ihre Profile ausgelöst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt ein alternatives Feld, das mit einem Hostnamen in einem SIR-Security Incident gefüllt wird. Das alternative Feld ist das Feld **Beschreibung**.



Überprüfen Sie die Auslösebedingungen des Profils CrowdStrike Falcon Insight .

Testen Sie das Profil, und vergewissern Sie sich, dass die von Ihnen konfigurierten Auslösebedingungsfilter wie erwartet funktionieren.

Vorbereitungen

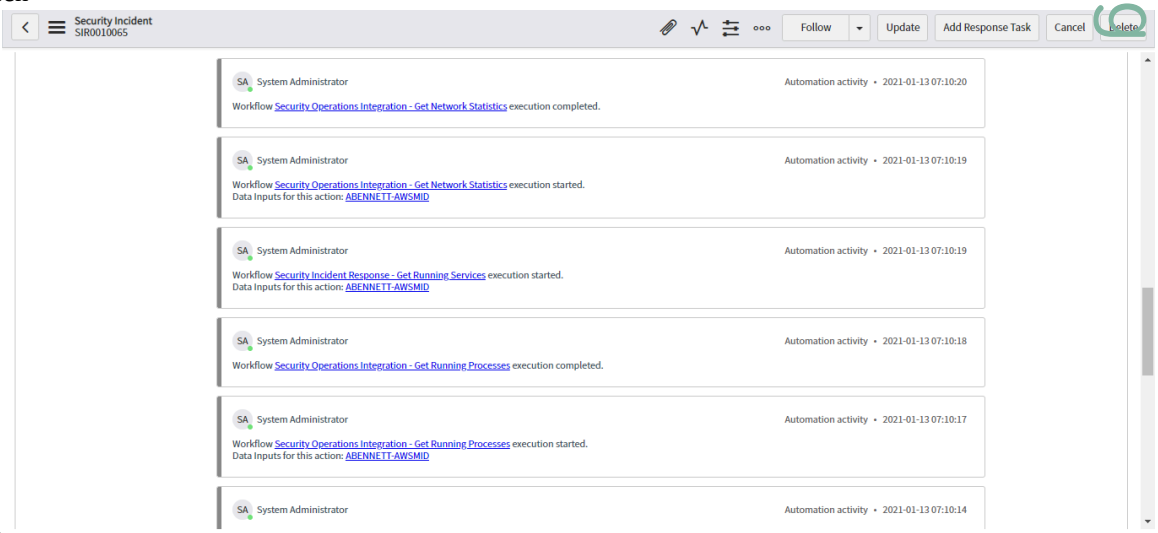
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Aktivieren Sie das Profil basierend auf den von Ihnen angegebenen konfigurierten Auslöserbedingungen, damit Sie die Abfrageergebnisse in den Security Incidents Now Platform anzeigen können.

Prozedur

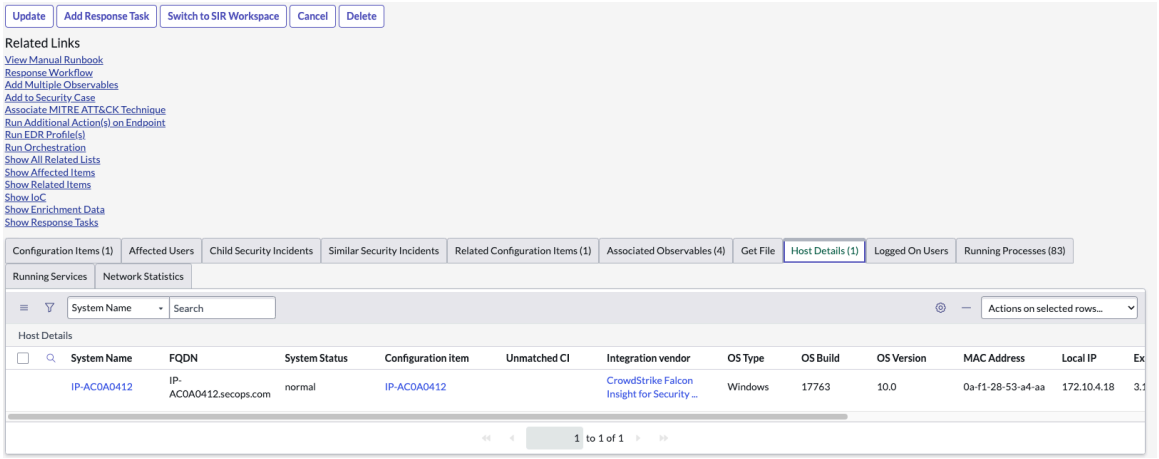
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie **Neu** aus, um einen Security Incident zu erstellen.
3. Um einen Security Incident zu erstellen, geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Speichern**.
4. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“, um die Tags „Profil initiiert“ und „Profil abgeschlossen“ anzuzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Überprüfen Sie die Details in den zugehörigen Listen CrowdStrike Falcon Insight Details, z. B. Datei abrufen, Hostdetails, Angemeldete Benutzer, Laufende Prozesse, Laufende Services, Netzwerkstatistiken usw.



Löst ein CrowdStrike Falcon Insight -Profil manuell über einen Security Incident aus

Lösen Sie ein Profil manuell aus, nachdem Sie einen Security Incident überprüft haben.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sobald Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in den Security Incidents Now Platform anzeigen. Mit CrowdStrike Falcon Insight können Sie auch einzelne Fähigkeiten für Configuration Items (CIs) ausführen, ohne ein Profil zu verwenden.

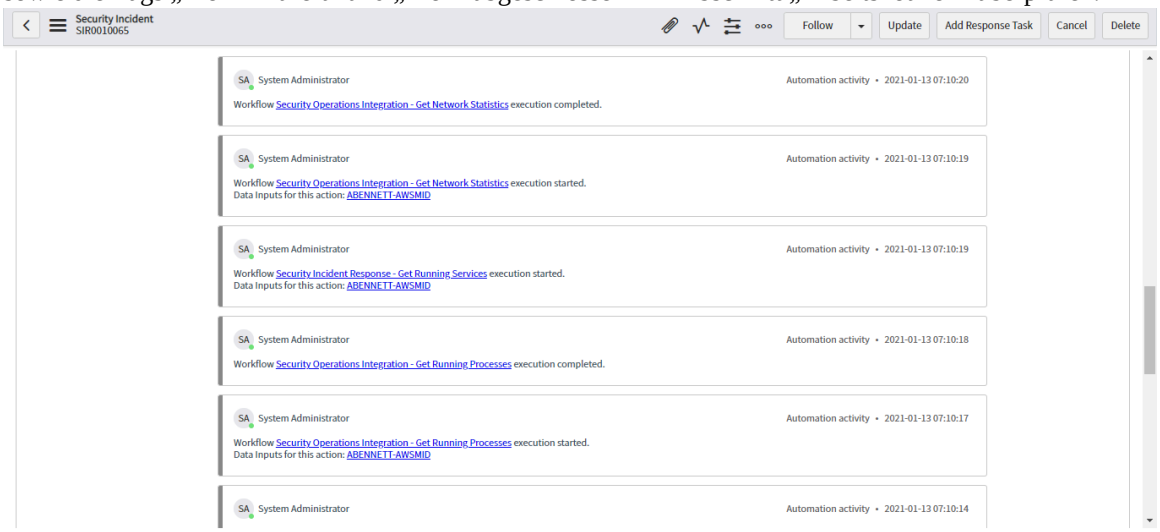
Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen CrowdStrike Falcon Insight aus.
3. Wählen Sie im Abschnitt „Zugehörige Listen“ **EDR-Profil(e) ausführen aus**.
4. Durchsuchen und ein Profil aus der Liste der verfügbaren Profile auswählen
5. Wählen Sie **„Zugehöriges CI einschließen“** aus, um dieses Profil für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.
6. Klicken Sie auf **Absenden**.

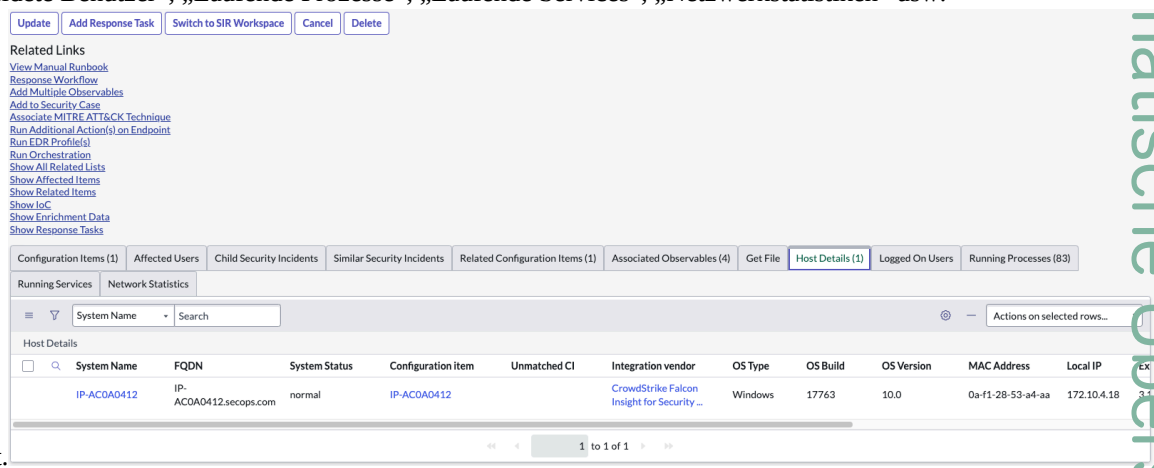
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das ausgewählte Profil wird manuell ausgelöst. Sie können den Abschnitt „Arbeitsnotizen und Aktivitäten“ sowie die Tags „Profil initiiert“ und „Profil abgeschlossen“ im Abschnitt „Arbeitsnotizen“ überprüfen.



7. Die Ergebnisse werden in Form von zugehörigen Listen wie „Datei abrufen“, „Hostdetails“, „Angemeldete Benutzer“, „Laufende Prozesse“, „Laufende Services“, „Netzwerkstatistiken“ usw. angezeigt.



8. Um einzelne Fähigkeiten für ein CI auszuführen, gehen Sie wie folgt vor:

   a. Wählen Sie in der zugehörigen Liste Configuration Items das gewünschte CI aus.

   b. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen Sie die Fähigkeit aus, die Sie für das ausgewählte CI ausführen möchten.
   Beispiel: Host isolieren.

   c. Suchen Sie mithilfe der Suchoption nach der erforderlichen Fähigkeitsimplementierung für das CI, und wählen Sie **CrowdStrike Falcon Insight – Host isolieren**aus.

   d. Klicken Sie auf **Host isolieren,** um die Anwendung für das ausgewählte CI auszuführen.

Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche

Verwenden Sie Sichtungssuchen für CrowdStrike Falcon Insight, um infizierte Computer im Netzwerk Ihrer Organisation zu finden und Security Incident Response-Fälle zu bearbeiten.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in CrowdStrike Falcon Insight durch, um die Verbreitung einer Bedrohung im Zeitverlauf zu bestimmen.

Prozedur

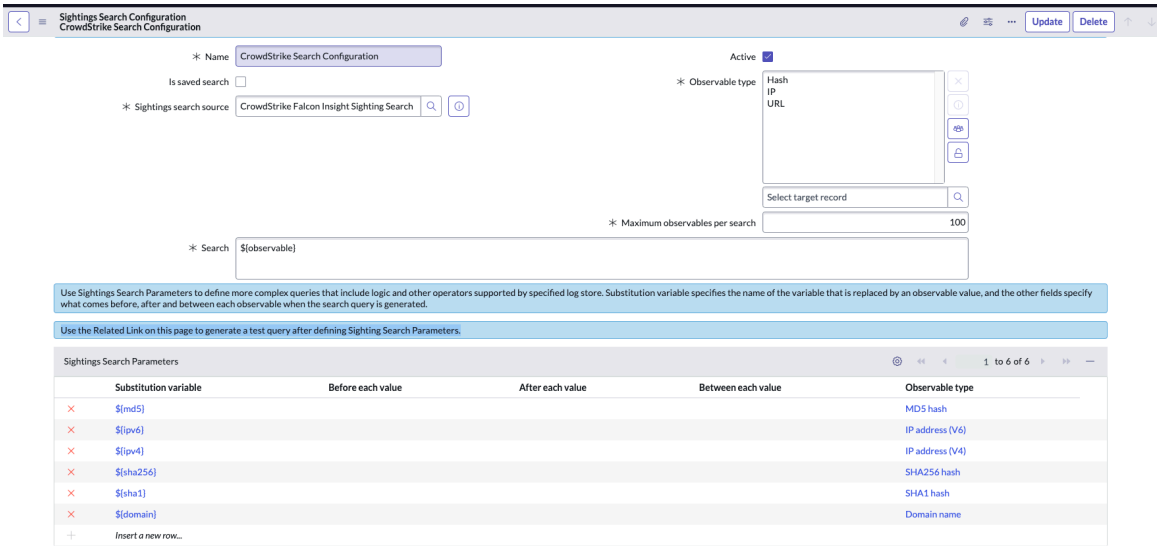
1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **Sichtungssuchprofile**.
2. Klicken Sie auf **Neu**.
3. Konfigurieren Sie dieses Profil, um zu bestimmen, welche Server nach einer bestimmten Suchfunktion von CrowdStrike Falcon Insight gesucht werden sollen.
4. Füllen Sie im Formular die folgenden Felder aus:

Feld	Beschreibung
Name	Name für das Sichtungssuchprofil.
Ist gespeicherte Suche	Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt.
Sichtungssuchquelle	Die Quelle für die Sichtungssuche. Wählen Sie **CrowdStrike Falcon Insight-Sichtungssuche** als Quelle aus.
Aktiv	Option, um anzugeben, ob der Zusatz aktiv ist oder nicht.
Erkennbarer Typ	Die CrowdStrike Falcon Insight-Integration unterstützt die folgenden erkennbaren Elemente: ○ Hash ○ IP ○ URL Die Sichtungssuche wird für die folgenden Typen erkennbarer Elemente unterstützt: ○ Domänenname ○ IP-Adresse (V4) ○ IP-Adresse (V6) ○ MD5-Hash ○ SHA1-Hash ○ SHA256-Hash
Maximale erkennbare Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die Sie in einer Suchabfrage anzeigen können.
Suchen	Die Standardsuchzeichenfolge ist `$(observable)`, Sie können jedoch Ihre eigene Suchabfrage definieren, indem Sie Parameter angeben, die von der CrowdStrike Falcon Insight -Integration unterstützt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sichtungssuchparameter	Parameter zum Definieren komplexerer Abfragen, die Logik und andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden Sie können die zugehörigen Links unten auf der Seite verwenden, um nach der Definition von Sichtungssuchparametern eine Testabfrage zu generieren.



5. Klicken Sie auf **Absenden**.
   Die Konfiguration ist abgeschlossen, und Sie können die Sichtungssuche über den Security Incident Now Platform aufrufen.
6. Um die Konfiguration zu verifizieren und eine Sichtungssuche auszuführen, gehen Sie wie folgt vor:

   a. Öffnen Sie einen Security Incident, scrollen Sie zum Ende des Security Incidents, und klicken Sie **auf Alle zugehörigen Listen anzeigen**.

   b. Wenn Sie ein oder mehrere Configuration Items (CI) aus den zugehörigen Listen **„Laufende Prozesse“** auswählen.

   Hinweis:
   Wenn Sie eine Sichtungssuche für ein CI aus der zugehörigen Liste „Laufende Prozesse“ ausführen, handelt es sich nur um eine Prozess-Hash-Sichtungssuche.

   c. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen Sie **Run CrowdStrike Sightings Search (CrowdStrike-Sichtungssuche**ausführen) aus.

   d. Suchen Sie mithilfe der Suchoption nach dem erforderlichen Sichtungssuchprofil.

   e. Wählen Sie das gewünschte Sichtungssuchprofil aus, und klicken Sie auf **Absenden**.

   f. Wenn Sie ein oder mehrere erkennbare Elemente aus den **zugehörigen Listen für zugeordnete erkennbare Elemente** auswählen.

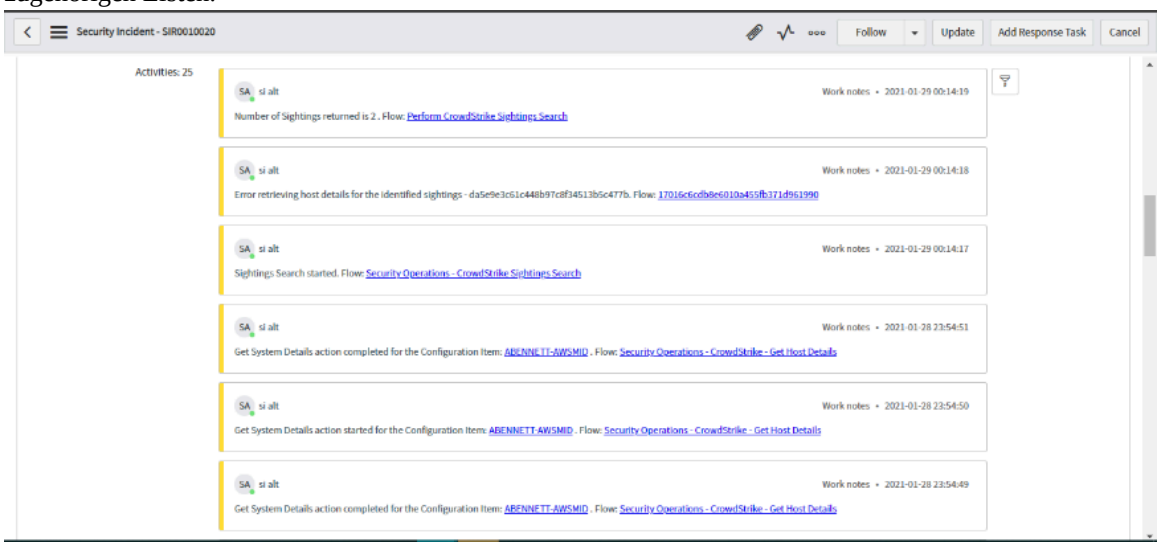
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen Sie **die Option Sichtungssuche ausführen**aus.

h. Wählen Sie im Popup-Fenster für den Zeitrahmen einen beliebigen Wert aus, und klicken Sie auf **Suchen**.

i. Validieren Sie nach Abschluss der Suche die Ergebnisse und Details in den Arbeitsnotizen und zugehörigen Listen.



j. Wählen Sie die Registerkarte **Sichtungen** aus, um die Sichtungsdetails anzuzeigen.

k. Klicken Sie auf das **Vorschausymbol** neben dem CI, um weitere Informationen zu CrowdStrike-Sichtungsdetails anzuzeigen.

l. Klicken Sie auf die **Details der Sichtungssuche,** um die Details der Sichtungssuche anzuzeigen, und klicken Sie auf die Registerkarte **Sichtungssuchergebnisse,**um die Suchergebnisse anzuzeigen.

Konfigurieren und lösen Sie zusätzliche Aktionen in aus CrowdStrike Falcon Insight

Die CrowdStrike Falcon Insight -Integration unterstützt die Ausführung zusätzlicher Aktionen wie reguläre Ausdrücke (reguläre Ausdrücke). Die CrowdStrike Falcon Insight -Integration bietet 40 zusätzliche Aktionen mit dem Basissystem.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **CrowdStrike: zusätzliche Aktionen**.
2. Klicken Sie auf **Neu**, um eine eigene zusätzliche Aktion zu erstellen, oder wählen Sie eine vorhandene Aktion aus, die im Basissystem enthalten ist.
   Erstellen wir beispielsweise eine neue zusätzliche Aktion.
3. Füllen Sie die Felder im Formular aus.

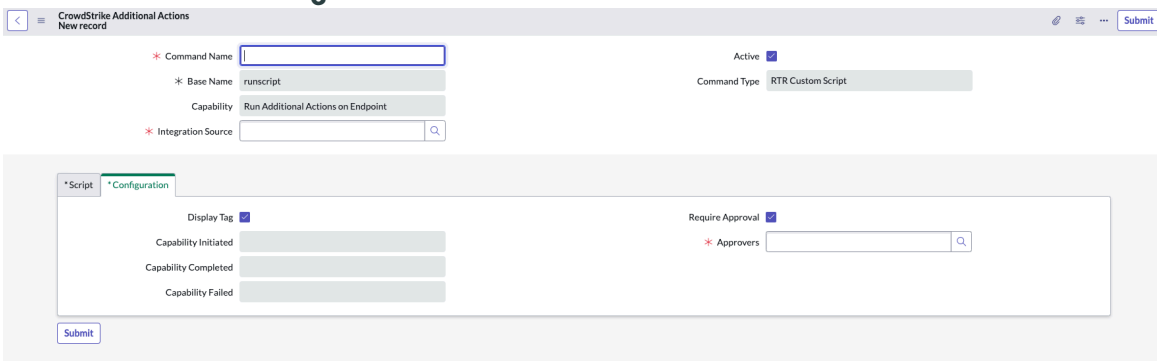
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Befehlsname	Befehlsname für die zusätzliche Aktion. Beispiel: reg.
Basisname	Basisname für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: reg.
Fähigkeit	Fähigkeitsname für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: Zusätzliche Aktionen für Endpunkt ausführen.
Integrationsquelle	Die Quelle für die zusätzliche Aktion. Beispiel: CrowdStrike Falcon Insight-Integration.
Aktiv	Option, um anzugeben, ob der Zusatz aktiv ist oder nicht.
Befehlstyp	Befehlstyp für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: Anwenderdefiniertes RTR-Skript.
Skript	○ **BS-Typ**: Option zum Auswählen des Betriebssystemtyps für Ihr Skript. Wählen Sie eine der folgenden Optionen aus: ▪ **Windows** ▪ **Mac OS X** ▪ **Linux** ▪ **Keine** ○ **Skript**: Option zum Eingeben Ihres Skripts, wenn Sie eines der folgenden Betriebssysteme ausgewählt haben, mit Ausnahme der Option Keine.
Konfiguration	○ **Tag anzeigen**: Option zum Anzeigen des Tags für die Konfiguration. Sie können das Tag für die folgenden Felder auswählen: ▪ Fähigkeit: Initiiert. Beispiel: Registrierungssatz – Initiiert. ▪ Fähigkeit: Abgeschlossen. Beispiel: Registrierungssatz – Abgeschlossen. ▪ Fähigkeit: Fehlgeschlagen Beispiel: Registrierungssatz – Fehlgeschlagen. ○ **Genehmigung erforderlich**: Option zum Auswählen eines Genehmigers oder einer Gruppe, der bzw. die die Konfiguration genehmigen muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CrowdStrike Falcon Insight – Zusätzliche Aktionen



4. Klicken Sie auf **Absenden**.

5. Sie können auch aus den folgenden vorhandenen zusätzlichen Aktionen auswählen.
   Das Basissystem enthält 40 zusätzliche Aktionen, mit denen Sie zusätzliche Konfigurationen durchführen können.

   Hinweis:
   Stellen Sie sicher, dass Sie die Liste „Zusätzliche CrowdStrike-Aktionen“ öffnen und die erforderliche zusätzliche Aktion auf **wahr**festlegen, andernfalls ist die zusätzliche Aktion im Arbeitsbereich nicht verfügbar.

Liste der zusätzlichen Aktionen, die im Basissystem enthalten sind

CrowdStrike Additional Actions — Command Name — Search — Actions on selected rows... — New

All

Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

6. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.

7. Wählen Sie den Security Incident aus, den Sie überprüfen möchten, indem Sie zusätzliche Aktionen für den Endpunkt ausführen.

   a. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.

   b. Durchsuchen und die gewünschte Fähigkeit auswählen
   Beispiel: Klicken Sie auf **reguläre** Satzfähigkeit.

   c. Wählen Sie **Zugehöriges CI einschließen aus**, um die zusätzlichen Aktionen für alle zugehörigen CIs des Endpunkts auszuführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Sie können den **Unterschlüssel** für die Ausführung der zusätzlichen Aktionen auf dem Endpunkt definieren.
Dieser Unterschlüssel kann ein KBLM-/Software-/neuer Schlüssel sein.

8. Um die Ausführung zusätzlicher Aktionen für den Endpunkt zu initiieren, klicken Sie auf **Zusätzliche Aktion ausführen**.
9. Zeigen Sie die Automatisierungsaktivitäten der -Ausführung an, und validieren Sie sie.
10. Validiert den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

Verwenden der -Integration CrowdStrike Falcon Insight von in Analyst Workspace

Verwenden Sie die CrowdStrike Falcon Insight -Integration, um die CrowdStrike Falcon Insight -Fähigkeiten im SIR-Analystenarbeitsbereich zu nutzen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Bevor Sie CrowdStrike Falcon Insight die -Integration im Security Incident Response-Arbeitsbereich verwenden, müssen Sie sie aus dem ServiceNow Store herunterladen und konfigurieren. Weitere Informationen finden Sie unter Erste Schritte mit der CrowdStrike Falcon Insight -Integration.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Integration CrowdStrike Falcon Insight verwenden, um Korrekturaktionen für die Endpunkte in Echtzeit durchzuführen, Profile zum Sammeln von Details zum Host zu verwenden und über den Arbeitsbereich Security Incident Response spezifische Abfragen oder Aktionen für den Endpunkt durchzuführen.

Die CrowdStrike Falcon Insight -Integration ermöglicht Analysten die Verwendung der folgenden CrowdStrike Falcon Insight -Funktionen im Security Incident Response -Arbeitsbereich für Analysten:

- **Hostdetails abrufen**
- **Angemeldete Anwender abrufen**
- **Netzwerkstatistiken abrufen**
- **Laufende Prozesse abrufen**
- **Laufende Services abrufen**
- **Host isolieren**
- **Isolation entfernen**
- **Datei abrufen**

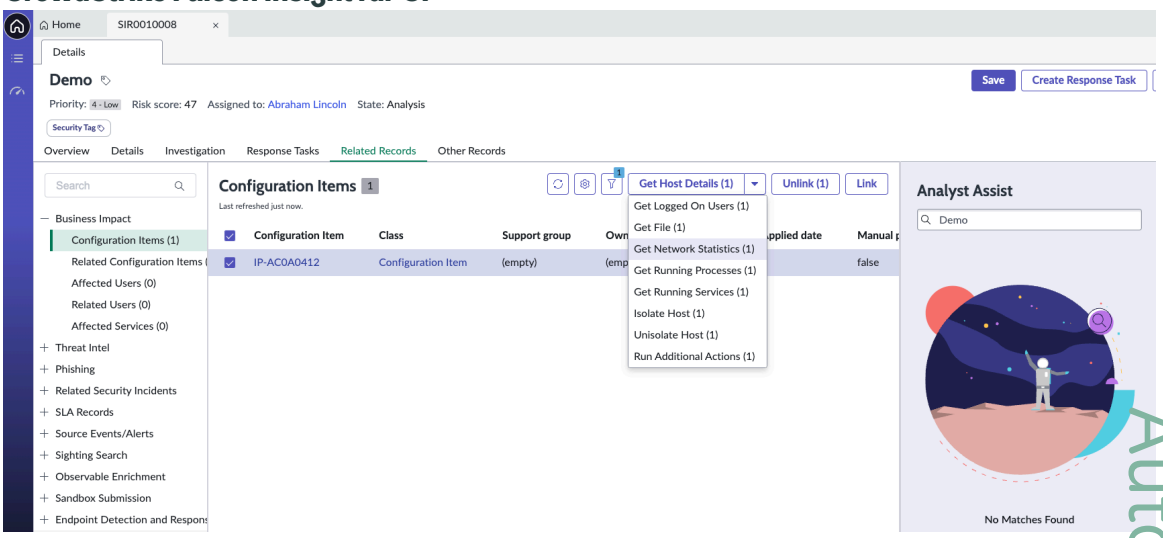
Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich den gewünschten Security Incident, und wählen Sie die Registerkarte **Zugehörige Datensätze**.
2. Sie können die CrowdStrike Falcon Insight-Fähigkeiten in der zugehörigen Liste „Geschäftsauswirkung“ zur Analyse verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie ein **Configuration Item**und anschließend eine Fähigkeit aus der Dropdown-Liste aus.

CrowdStrike Falcon Insight für CI



b. Wählen Sie die Implementierung **CrowdStrike Falcon Insight** aus, und klicken Sie auf **Absenden**. Die Fähigkeit „Netzwerkstatistiken abrufen“ wird für das CI aufgerufen. Sie können die Arbeitsnotizen für die -Ergebnisse und -Ergebnisse anzeigen.

3. Sie können die CrowdStrike Falcon Insight-Fähigkeiten in der zugehörigen Liste **„Endpoint Detection and Response (EDR)“** für Analysen verwenden.

a. Wählen Sie in der zugehörigen Liste Endpoint Detection and Response (EDR) einen EDR aus der Liste aus.

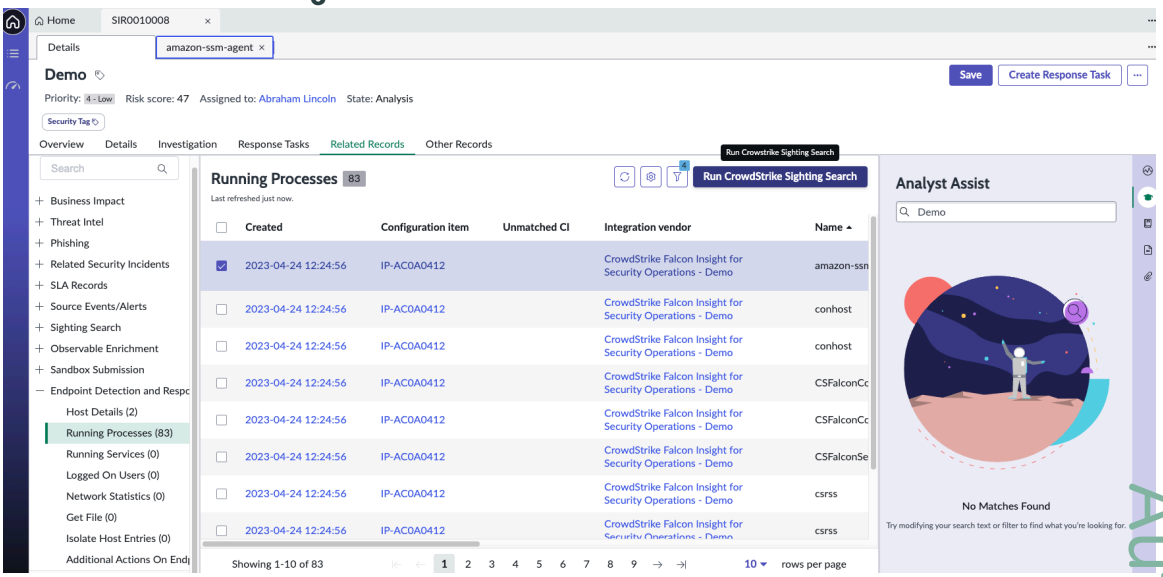
b. Klicken Sie auf einen bestimmten laufenden Prozess, um die Details des laufenden CrowdStrike Falcon Insight-Prozesses anzuzeigen.

c. Um eine CrowdStrike Falcon Sighting-Suche für einen bestimmten laufenden Prozess auszuführen, wählen Sie den laufenden Prozess aus, und klicken Sie auf **CrowdStrike Sighting ausführen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CrowdStrike Falcon Insight für EDR



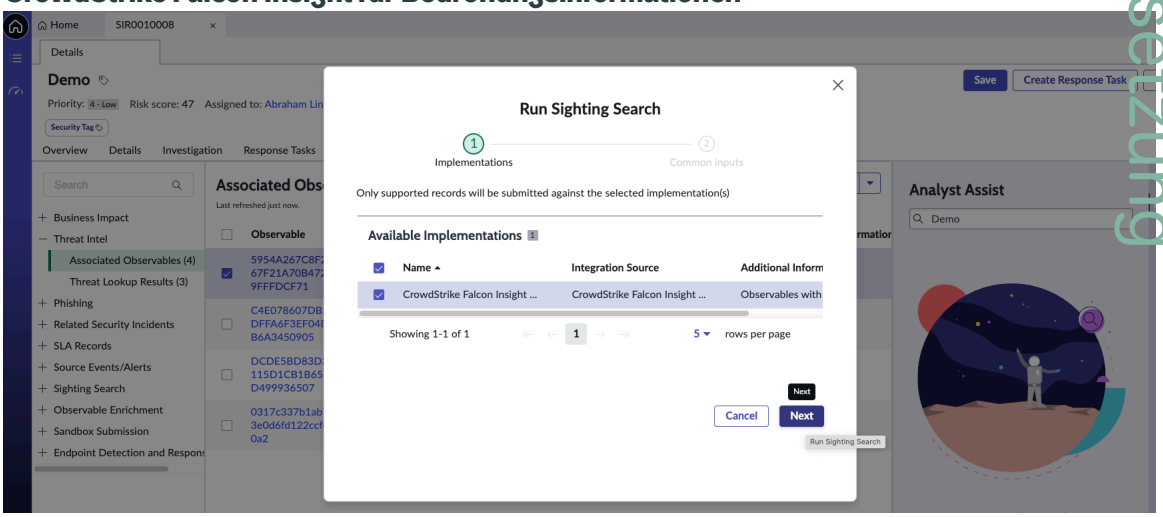
d. Wählen Sie die Implementierung **CrowdStrike Falcon Insight** aus, und klicken Sie auf **Run Search (Suche ausführen)**.
Dann wird eine Hash-Sichtungssuche für den ausgewählten laufenden Prozess ausgeführt. Sie können die Arbeitsnotizen für die -Ergebnisse und -Ergebnisse anzeigen.

4. Sie können die CrowdStrike Falcon Insight-Fähigkeiten für die **Bedrohungsinformationen** zur Analyse verwenden.

a. Wählen Sie in der Gruppe „Bedrohungsinformationen“ ein **erkennbares Element**aus, und wählen Sie in der Dropdown-Liste eine Fähigkeit CrowdStrike Falcon Insight aus.

b. Wählen Sie die Implementierung **CrowdStrike Falcon Insight** aus, und klicken Sie auf **Weiter**.

CrowdStrike Falcon Insight für Bedrohungsinformationen



c. Wählen Sie im Popup-Fenster „Datum/Uhrzeit auswählen“ einen zufälligen Wert aus, und klicken Sie auf **Absenden**.
Dann wird eine Sichtungssuche für das ausgewählte erkennbare Element ausgeführt. Sie können die Arbeitsnotizen für die -Ergebnisse und -Ergebnisse anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration mit CrowdStrike Falcon X Sandbox für Security Operations

Mit der CrowdStrike Falcon X SandboxSecurity Operations]-Integration für können Sie Dateien und URLs als Teil des Security Incident Response-Prozesses an CrowdStrike Falcon X Sandbox übermitteln, um eine detaillierte Malware- und Bedrohungsanalyse durchzuführen.

Die CrowdStrike Falcon X Sandbox -Integration bietet Ihnen eine isolierte virtuelle Umgebung, in der Sie bei Bedarf die Malware-Analyse durchführen und über die -Integration Ergebnisse für den Security Incident ServiceNow bereitstellen können.

Wenn Sie Ihre Malware-Incidents senden, werden sie als Teil des Security Incident-Datensatzes beibehalten. Sie können diese Datensätze füroder zur weiteren Lösung von Incidents verwenden und die Übermittlung von Dateien und URLs automatisieren.

Die Integration unterstützt die Automatisierung von Phishing- und Malware-Response-Playbooks , wodurch die Mitarbeiter des Centers Security Operations produktiver und effizienter auf Security Incidents reagieren können.

Hauptvorteile

Mit tseiner Integration, können Siewie folgt vorgehen:

- Automatisieren Sie die Übermittlung von Dateien und URLs von vom Anwender–gemeldetem Phishing (URP), E-Mail-Nachrichten, Anhängen und anderen Security Incidents.
- Übermitteln Sie zuvor analysierte Dateien und URLs manuell, oder übermitteln Sie sie erneut, um eine aktualisierte Analyse zu erhalten.
- Erstellen Sie mehrere Übermittlungskonfigurationen, die automatisch CrowdStrike Falcon X Sandbox Übermittlungsparameter wie Betriebssystem, Scan-Typ und Laufzeitoptionen anwenden.
- Analysieren Sie Malware und Bedrohungsergebnisse in einem HTML-formatierten Bericht innerhalb des Incidents SIR. Sie können die Ergebnisse der HR-Suche bisund den Indikatorverlauf für Dateien und URLs anzeigen, die mehrmals analysiert wurden.
- Taggen Sie Incidents ServiceNow mit dem Status der Übermittlungsverarbeitung sowie den Ergebnissen der Bedrohungssuche.

Siehe auch

Dokumentbezeichner	Dokumententitel
CrowdStrike Falcon X Sandbox	Häufig gestellte Fragen zu CrowdStrike Falcon Sandbox
ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

Erste Schritte mit der CrowdStrike Falcon X Sandbox -Integration

Aktivieren Sie CrowdStrike Falcon X Sandbox, und richten Sie es als Schnittstelle mit Ihrer Instanz ServiceNow und Ihrem Produkt Security Incident Response ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Bevor Sie CrowdStrike Falcon X Sandbox für die Security Operations-Integration verwenden können, müssen Sie es aus dem ServiceNow Storeherunterladen.
- Sehen Sie sich die folgende Setup-Prüfliste an, und vergewissern Sie sich, dass Sie alle Aufgaben für eine reibungslose CrowdStrike Falcon X Sandbox -Integration abgeschlossen haben.

Erforderliche Rolle: admin, sn_si.admin

Prüfliste

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen haben.	Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der -Administrator (admin) installiert die andbox-Integration saus dem ServiceNow App Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • sn_si.admin erstellt und bearbeitet die Konfiguration und globale Einstellungen. Dann weist die Rolle „Analyst für Sicherheits-Incidents“ (sn_si.analyst) zu. • Der Security Incident-Analyst (sn_si.analyst) reagiert auf Security Incidents, , z. B., übermittelt Dateien und URLs an die s-andbox und analysiert die Übermittlungsergebnisse.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren.	Diese Integration wird für die Releases Paris und Orlando unterstützt. Stellen Sie sicher, dass diese abhängigen Plugins installiert sind. Diese Plugins ermöglichen die Ausführung von IntegrationHub Aktionen und Flows: • ServiceNow IntegrationHub-Aktionsschritt – REST (com.glide.hub.action_step.rest) • ServiceNow IntegrationHub-Laufzeit (com.glide.hub.integration.runtime) **Hinweis:** Wenn Sie't ein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter ServiceNow von anfordern. Um ein Plugin anzufordern, befolgen Sie die in Plugin anfordern erläuterten Schritte. Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren, die für die Integration erforderlich sind. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response Abhängigkeit (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration **5.** Threat Intelligence Support Common (erforderlich fürse die Sandbox-Integrationsfunktionen) **6.** Trusted Security Circles **7.** Security Operations Setup-Assistent **8.** Security Incident Response Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Berechtigungen für ein Produkt oder eine Anwendung von Security Operations erwerben und eine Anwendung aus dem ServiceNow Store aktivieren.
Stellen Sie sicher, dass Sie für den privaten API-Schlüssel von Falcon Sandbox lizenziert sind, und oderbehalten Sie den vollständigen API-Schlüssel CrowdStrike Falcon X Sandbox.	Diese Integration unterstützt nur die Falcon Sandbox Private Cloud. **Hinweis:** Diese Version unterstützt keine Falcon X-Integration. CrowdStrike Falcon X Sandbox bietet einen selbstsignierten eingeschränkten API-Schlüssel und einen aktualisierten vollständigen API-Schlüssel. Verwenden Sie den vollständigen API-Schlüssel für

Automatische Übersetzung

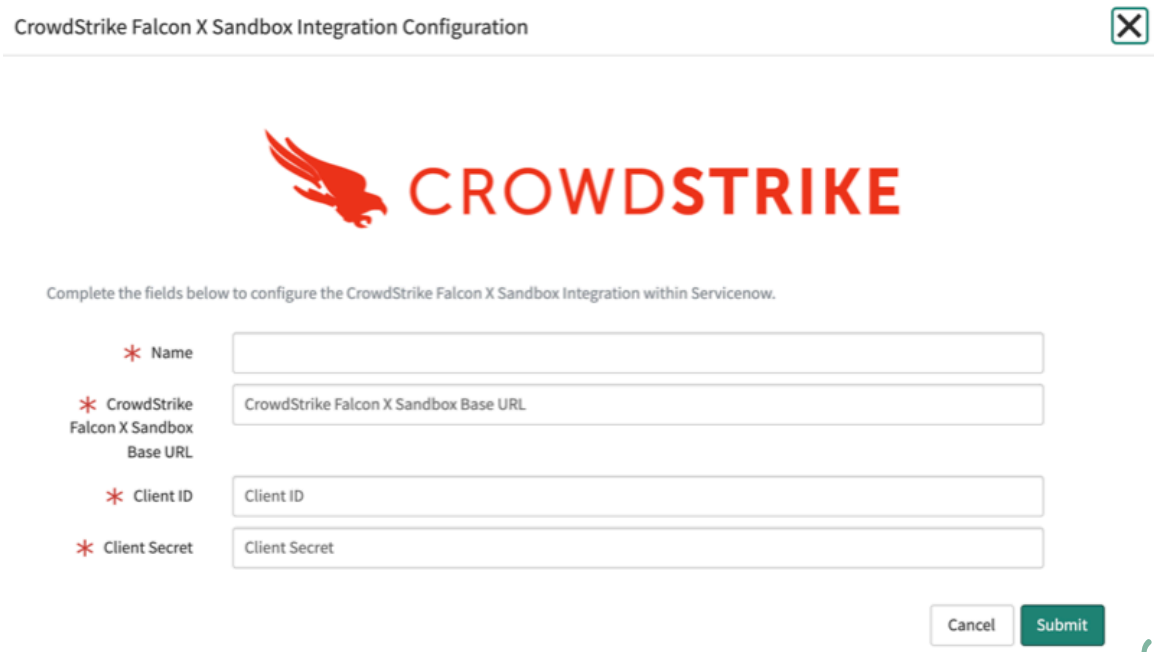
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	diese Integration , da sie uneingeschränkten Zugriff für automatisierte Übermittlungen ermöglicht. Weitere Informationen finden Sie in der CrowdStrike Falcon Sandbox-Knowledge Base .

Prozedur

1. Laden Sie die Integration mit CrowdStrike Falcon Sandbox für Security Operations aus dem ServiceNow Store herunter.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Integrationskachel CrowdStrike Falcon X Sandbox, und klicken Sie auf **Konfigurieren**.



4. Geben Sie die folgenden Details ein, um die Konfiguration abzuschließen:

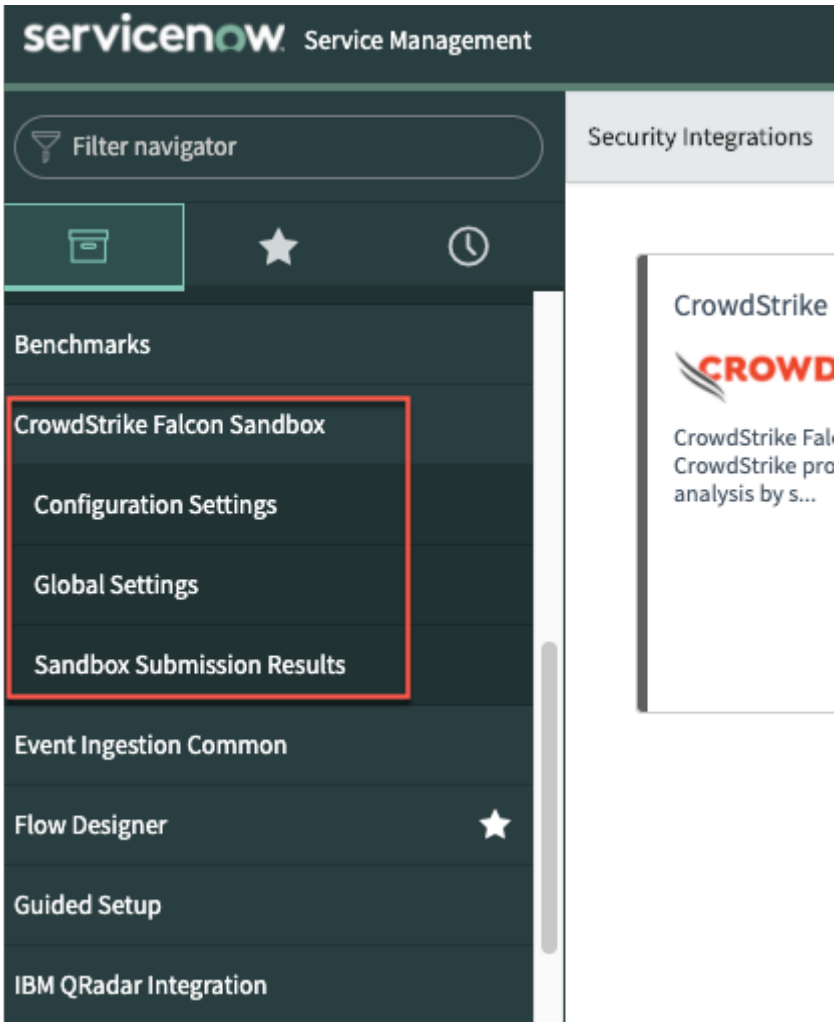
Feld	Beschreibung
Name	Name dieser Integration, z. `B. demo-1`. Dies ist zwar ein eindeutiger Name zur Identifizierung der andbox-Konfiguration von s, Sie können jedoch nur eine Integration pro ServiceNow-Instanz konfigurieren.
CrowdStrike Falcon Sandbox-Basis-URL	S-andbox-Basis-URL. Diese URL ist verfügbar , nachdem Sie die andbox skonfiguriert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	haben.Beispiel: `https://servicenow.falcon-sandbox.com` ist eine Basis-URL.
Client-ID	ID des OAuth2-API-Clients. Weitere Informationen finden Sie unter API-Clients und -Schlüssel .
Geheimer Clientschlüssel	Geheimer OAuth2-API-Clientschlüssel. Weitere Informationen finden Sie unter API-Clients und -Schlüssel .

5. Klicken Sie auf **Absenden**.
   Nachdem die Sandbox erfolgreich validiert und übermittelt wurde, wird sie auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Sie können das Sandbox-Modul jetzt im -Anwendungsnavigator anzeigen.



Nächste Maßnahme

Nachdem Sie die Integration erfolgreich abgeschlossen haben, besteht der nächste Schritt in der Einrichtung von Sandbox-Übermittlungskonfigurationen.

Richten Sie Sandbox-Übermittlungskonfigurationen ein

Richten Sie die Sandbox-Konfiguration ein, um die Analyseumgebung und Laufzeitoptionen für die Übermittlungen von Security Incident-Datensätzen für die Malware-Analyse zu definieren.

Automatische Übersetzung

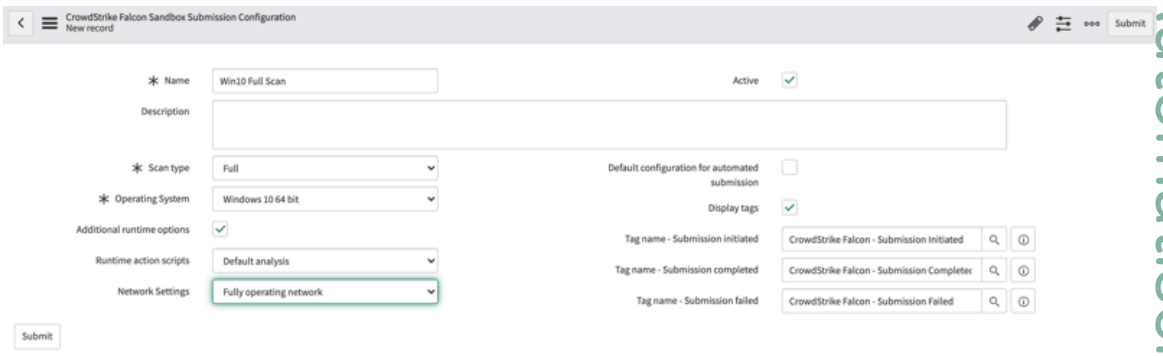
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Bevor Sie Dateien oder URLs mithilfe der Integration an CrowdStrike Falcon X Sandbox übermitteln können, müssen Sie mindestens eine Übermittlungskonfiguration konfigurieren. Die Übermittlungskonfiguration definiert das Sandbox-Betriebssystem, den Überprüfungstyp, die Laufzeitoptionen und andere Eigenschaften der Incident-Behandlung. Sie möchten möglicherweise mehrere Konfigurationen erstellen, um die verschiedenen Optionen zu verwenden , [], die in der Umgebung CrowdStrike Falcon X Sandbox verfügbar sind.

Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon X Sandbox** > **Konfigurationseinstellungen**.
2. Klicken Sie auf **Neu**.



3. Füllen Sie die folgenden Felder aus, um eine Konfiguration für den Typ Vollständiger **Scan**zu erstellen.

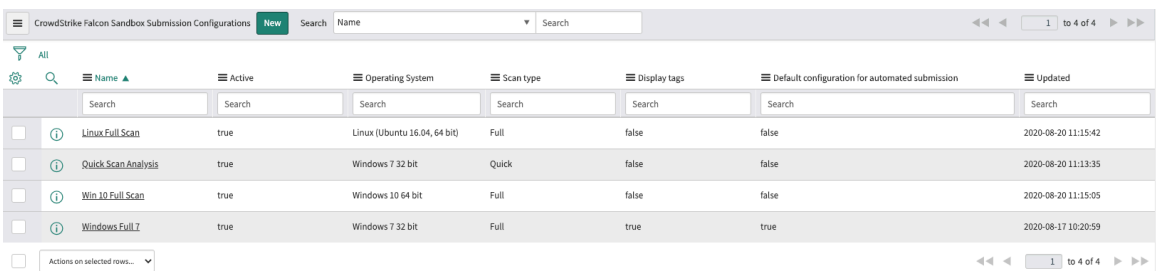
Feld	Beschreibung
Name	Eindeutiger Name für die Übermittlungskonfiguration. Dieser Name wird Analysten angezeigt, wenn sie eine Datei übermitteln. Es ist wichtig sicherzustellen, dass der Name beschreibend ist und sich leicht von den anderen Konfigurationen unterscheiden lässt (Beispiel: vollständiger Win 10-Scan). Wenn der Name nicht eindeutig ist, wird ein Fehler angezeigt, und doppelte Namen von Konfigurationsdatensätzen werden nicht gespeichert.
Überprüfungstyp	Skann als **„Vollständig"**eingegeben werden. Ein **Schnell-** Scan-Typ bietet eine eingeschränkte Bedrohungsanalyse.
Betriebssystem	EineAnalyse-VM-Umgebung, bei der die -Andboxdie Datei oder URL in scannt.
Aktiv	OOption , die Sie auswählen, wenn Sie Dateien oder URLs manuell übermitteln.
Standardkonfiguration für automatisierte Übermittlung	OOption , dass standardmäßig deaktiviert ist. Durch Auswahl dieser Option ist diese Konfiguration für

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die Automatisierung der Übermittlung von Malware-Analysen verfügbar. **Hinweis:** Sie können nur eine aktive Übermittlungskonfiguration als Standardkonfiguration für automatisierte Übermittlungen haben.
Tags anzeigen	OOption , dass standardmäßig deaktiviert ist. Wenn Sie diese Option auswählen, werden Tags angezeigt, um den Status einer Datei- oder URL-Übermittlung anzugeben. Die Verarbeitung der Analyse kann einige Minuten dauern. Die Anzeige-Tags sind Übermittlung initiiert, Übermittlung abgeschlossen, oder Übermittlung fehlgeschlagen.
Weitere Laufzeitoptionen	OOption , dass standardmäßig deaktiviert ist. Wenn Sie diese Option auswählen, sind zusätzliche Laufzeitparameter verfügbar, die die Sandbox unterstützt.
Laufzeit-Aktionsskripts	Mit dieser Option können Sie Aktionsskripts vom Typ und verwenden, die menschliches Verhalten vonund simulieren und während der Analyse mit der Datei oder URL interagieren. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ Weitere Informationen finden Sie in der Dokumentation CrowdStrike Falcon X Sandbox.
Netzwerkeinstellungen	Mit dieser Option können Sie den Typ der Netzwerkeinstellungen auswählen, die beim Senden einer URL oder Datei an Sandbox verwendet werden.

4. Klicken Sie auf **Absenden**.
   Nachdem Sie die Konfiguration gesendet haben, wird sie auf der Seite Konfigurationseinstellungen als Datensatz gespeichert. Die Konfiguration muss „ **Aktiv“** sein, damit sie in sandbox-Übermittlungen verwendet werden kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Nachdem Sie sundbox-Übermittlungen konfiguriert haben, besteht der nächste Schritt in der manuellen Übermittlung von Dateien oder ULRs an Sandbox

.

Übermitteln Sie Dateien oder URLs manuell an die Sandbox

Sie können eine Datei oder URL manuell an eine Sandbox senden, wenn bestimmte Incident-Kriterien erfüllt sind, z. B. Kategorie ist Phishing.

Vorbereitungen

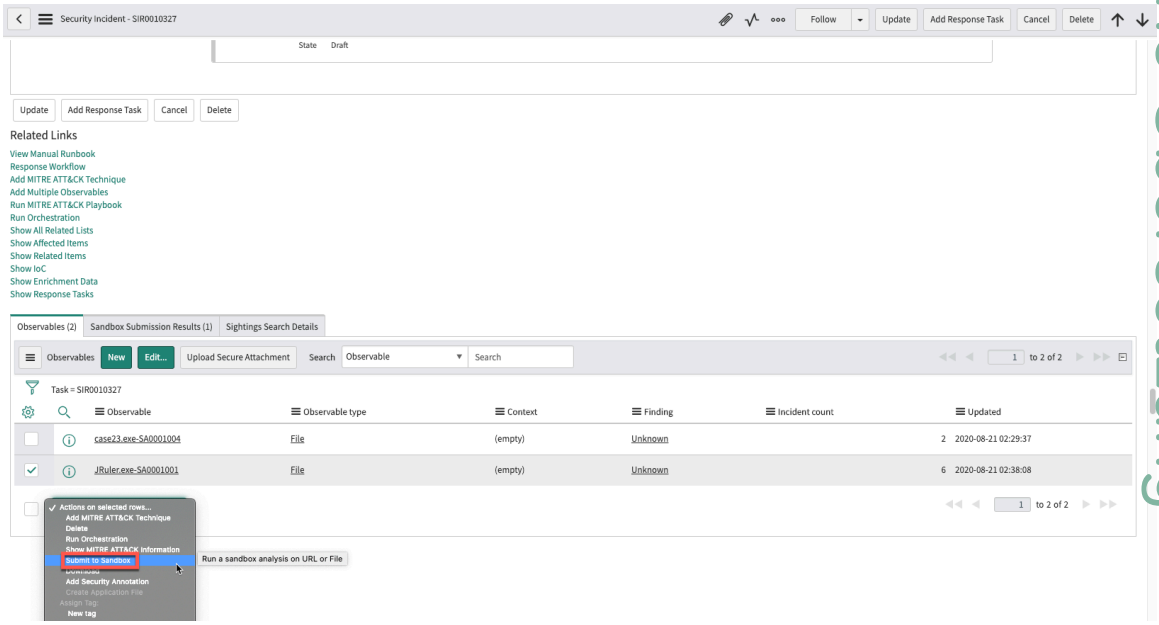
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Nach Überprüfung des Security Incident und der Datei oder URL können Sie die Option **An die Sandbox übermitteln** auswählen, um eine Malware-Analyse durchzuführen.

Prozedur

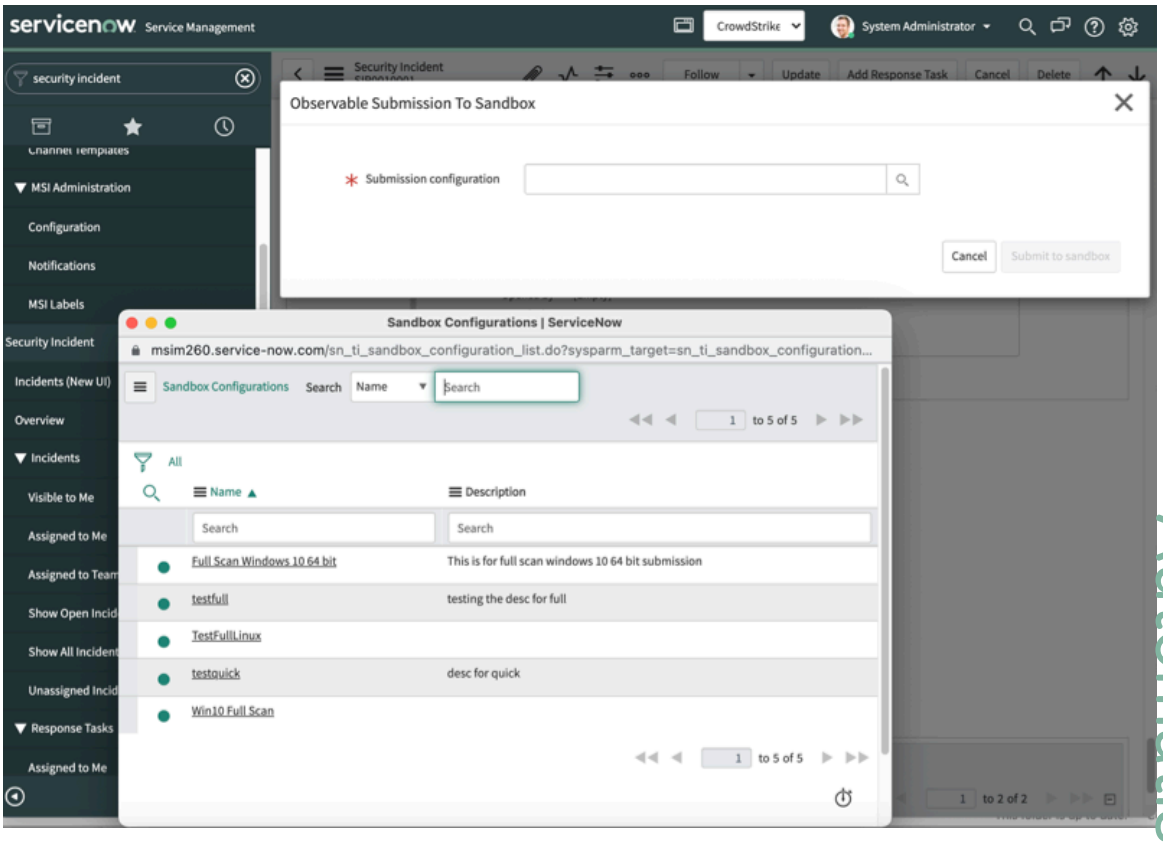
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie einen Security Incident, an den Sie eine Datei oder einen URL-Datensatz vom Typ „Erkennbares Element“ senden möchten.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.
3. Wählen Sie auf der Registerkarte **Erkennbare** Elemente einen oder mehrere Datensätze aus, für die Sie eine Malware- oder Bedrohungsanalyse durchführen möchten, und klicken Sie auf **An die Sandbox senden**.



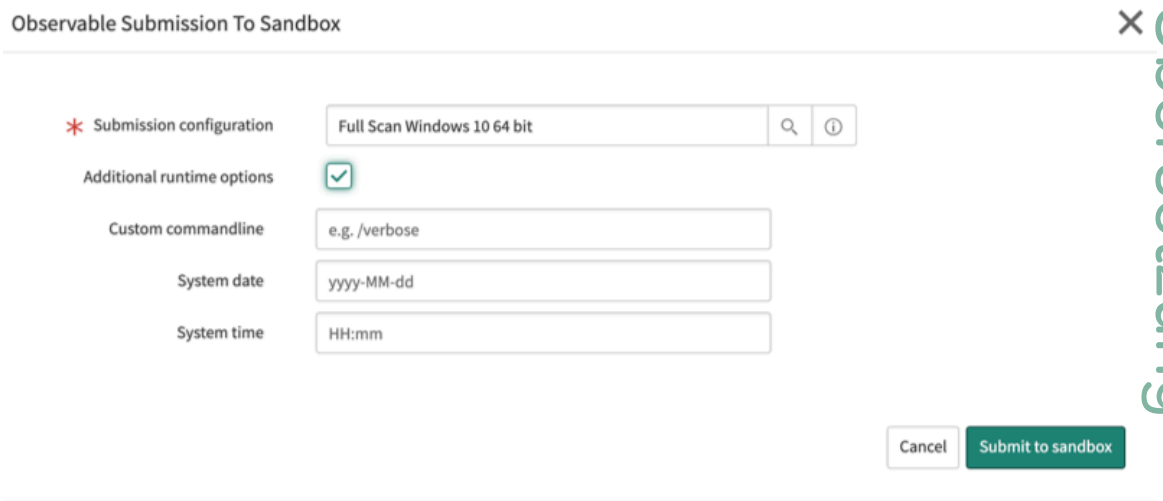
4. Wenn der Filter „Dateiübermittlung“ angezeigt wird, wählen Sie unter **Übermittlungskonfiguration**Ihre bevorzugte Sandbox-Konfiguration aus, und klicken Sie auf **An die Sandbox übermitteln**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. **Wahlweise:** Wählen Sie **Zusätzliche Laufzeitoptionen** aus, wenn Sie weitere anwenderdefinierte Optionen angeben möchten.



Feld	Beschreibung
Anwenderdefinierte Befehlszeile	Reguläre Anwendungsbefehlszeile oder spezieller Vorgang.
Systemdatum	Systemdatum im Format JJJJ-MM-TT.
Systemzeit	Systemzeit im Format HH:mm.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die Übermittlung initiiert haben, können Sie in den Arbeitsnotizen den Status Ihrer Übermittlung einsehen. Um weitere Informationen zum Status der Übermittlung zu erhalten oder die Ergebnisse zu analysieren, rufen Sie die **Sandbox-Übermittlungsergebnisse**auf.

Hinweis:
In CrowdStrike Falcon X Sandbox wird kein Schnell-Scan für URLs unterstützt. Wenn die Arbeitsnotizen zu viele Informationen enthalten, können Sie die Filteroption verwenden, um einen Drilldown zu den erforderlichen Arbeitsnotizen durchzuführen, die für Sie relevant sind.

Nächste Maßnahme

Wenn Sie die erkennbaren Elemente zur Malware-Analyse an die Sandbox übermitteln, zeigen Sie die Ergebnisse der Sandbox-Übermittlung an, um die nächsten Schritte bei potenziellen Bedrohungen auszuführen.

Automatisieren Sie CrowdStrike Falcon Sandbox-Übermittlungen mit Flow Designer

Die CrowdStrike Falcon X Sandbox -Integration enthält Flow-Vorlagen, die mit Workflow-Studio erstellt wurden und mit Security Incident-Datensätzen arbeiten.

Vorbereitungen

- Stellen Sie sicher, dass Sie eine Sandbox-Übermittlungskonfiguration erstellt und eine Konfiguration als **Standardkonfiguration für die automatisierte Übermittlung**aktiviert haben. Wenn der Flow ausgelöst wird, erfolgt die Sandbox-Übermittlung in Ihrer Standardkonfiguration.

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Flows sollen Ihnen in erster Linie den Einstieg erleichtern, wenn Sie die Datei- oder URL-Übermittlungen als Teil Ihres Workflows zur Reaktion auf Incidents automatisieren möchten.
Wenn Sie einen Beispiel-Flow aktivieren, werden Ihre Phishing-Dateianhänge automatisch übermittelt, wenn Sie die Security Incidents in Ihrem Beispiel-Flow als Phishing definieren. Alternativ können Sie alle .exe-Dateien übermitteln, wenn dieser Dateityp an einen Datensatz eines erkennbaren Elements angehängt ist.

Sie können diese Beispiel-Flows so ändern, dass eine automatisierte Übermittlung unter verschiedenen Bedingungen, Kategorien, zusammengesetzten Bedingungen usw. ausgelöst wird.

Die Sandbox-Integration besteht aus zwei Basissystem-Flows, die standardmäßig deaktiviert sind.

- **Datei senden, wenn Kategorie Phishing ist**: Dieser Flow übermittelt eine Datei zur Malware-Analyse an die Sandbox, wenn die Kategorie des Security Incident als Phishing definiert wird. Sie müssen eine Datei an den Datensatz des erkennbaren Elements im Security Incident anhängen. Wenn Sie die Funktion User Reported Phishing (URP) verwenden, werden E-Mail-Anhänge automatisch analysiert und dem SIR-Incident-Datensatz als erkennbares Element hinzugefügt. Um die Übermittlung zu automatisieren, ist keine weitere Aktion erforderlich.
- **Absenden, wenn der Dateityp für das erkennbare Element „exe“ ist**: Dieser Flow übermittelt eine Datei zur Malware-Analyse an die Sandbox, wenn das erkennbare Element des Security Incidents eine „exe“ ist. Ähnlich wie beim Phishing-Kategorie-Flow müssen Sie im Security Incident eine Datei an einen erkennbaren Datensatz anhängen. Sie können dies manuell tun, indem Sie die Datei hochladen, oder automatisch, wenn den erkennbaren Datensätzen ein Phishing-E-Mail-Anhang oder ein anderer Mechanismus zugeordnet ist, der den Incident erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Flows konfiguriert sind und die Incident-Bedingungen die Parameter erfüllen, werden die Sandbox-Übermittlungen automatisch ausgelöst, wenn Sie den Security Incident überprüfen. Überprüfen Sie die Arbeitsnotiz, die anzeigt, dass eine Übermittlung initiiert wurde, ein Tag angezeigt wird (sofern in der Konfiguration aktiviert) und ein Ergebnisdatensatz für die ausstehende Übermittlung angezeigt wird.

Die Sandbox-Integration enthält auch mehrere Subflows. Die Subflows sind interne Komponenten der allgemeinen Integrationsübermittlungsfunktionen. Sie können die Subflows an Ihre Sicherheitskriterien anpassen und bearbeiten.

Sie können auf die Subflows verweisen, um Probleme mit Sandbox-Übermittlungen zu beheben. Jedes Mal, wenn Sie einen Subflow aufrufen, wird ein Ausführungsdatensatz erstellt. Dieser Datensatz gibt an, wo im Flow ein bestimmter Fehler aufgetreten ist, und ermöglicht Ihnen, das Problem zu beheben.

Sandbox-Integration: Mehrere Workflows

Flows | Subflows | Executions | Help

+ New

All > Application Name contains Sandbox

Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

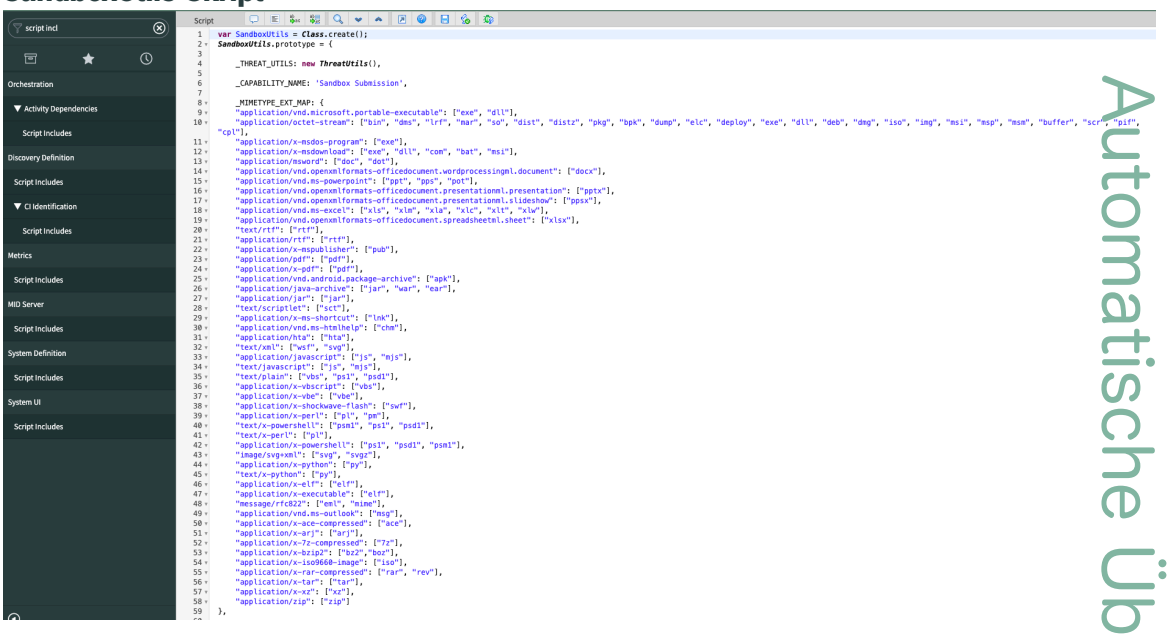
Actions on selected rows... 1 to 11 of 11

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

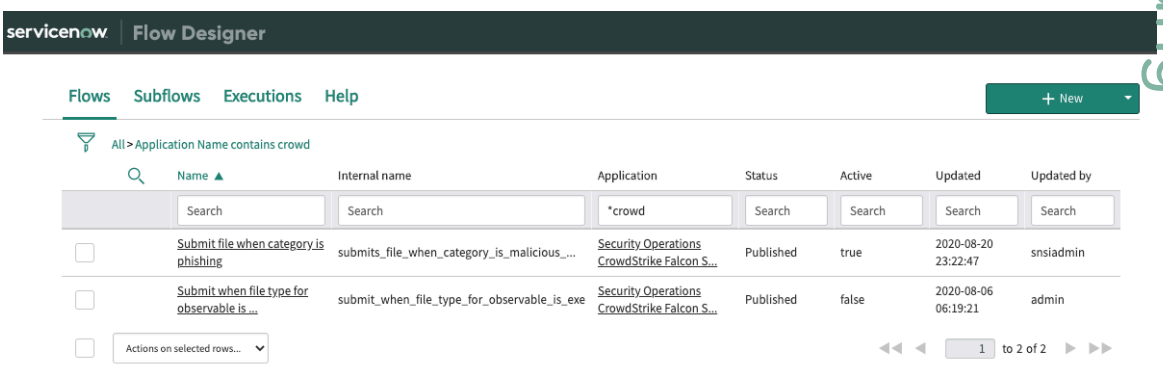
- Wenn Sie die Standard-Flows anpassen möchten, sollten Sie sich vergewissern, dass der Subflow „Erkennbares Element für die automatisierte Übermittlung übermitteln“ in Ihrem Flow enthalten ist, um automatische Übermittlungen auszulösen.
- Sie können Ihre Dateierweiterungen für eine exe anpassen und definieren. Erstellen Sie eine Kopie des Flows **Absenden, wenn der Dateityp für das erkennbare Element exe ist**, und nehmen Sie Änderungen an der Kopie vor. Der Inhaltstyp und die Dateierweiterungen werden im SandboxUtils -Skript zugeordnet. Um auf Skripteinbindungen zuzugreifen, navigieren Sie zu **Systemdefinitionen > Skripteinbindungen**, und suchen Sie nach SandboxUtils.

SandboxUtils-Skript



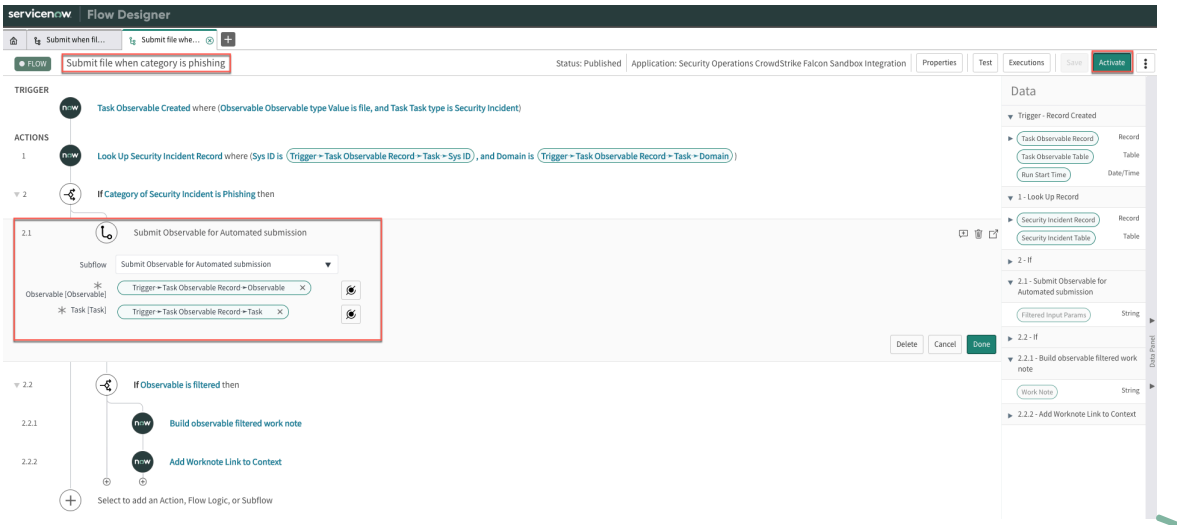
Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer** > **Flows**.
2. Filtern Sie die Flows nach **Anwendungstyp**.
   Zum Beispiel filtert *Crowd die beiden CrowdStrike Falcon X Sandbox -Flows.



3. Wählen Sie einen Flow aus, um die Details anzuzeigen.
   Das folgende Beispiel zeigt den Flow Datei senden, wenn die Kategorie Phishing ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Aktivieren** und dann auf **OK**, wenn die Bestätigungsmeldung angezeigt wird.

Nächste Maßnahme

Nachdem Sie automatisierte Übermittlungs-Flows konfiguriert haben, können Sie die Ergebnisse der Sandbox-Übermittlung anzeigen, um Bedrohungen zu analysieren.

Überwachen Sie die Übermittlungsergebnisse in der Sandbox

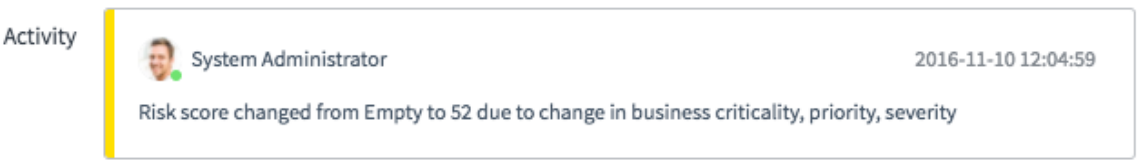
Die Ergebnisse für alle Sandbox-Übermittlungen werden auf der Registerkarte **„Sandbox-Übermittlungsergebnisse“** für jeden Security Incident angezeigt.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

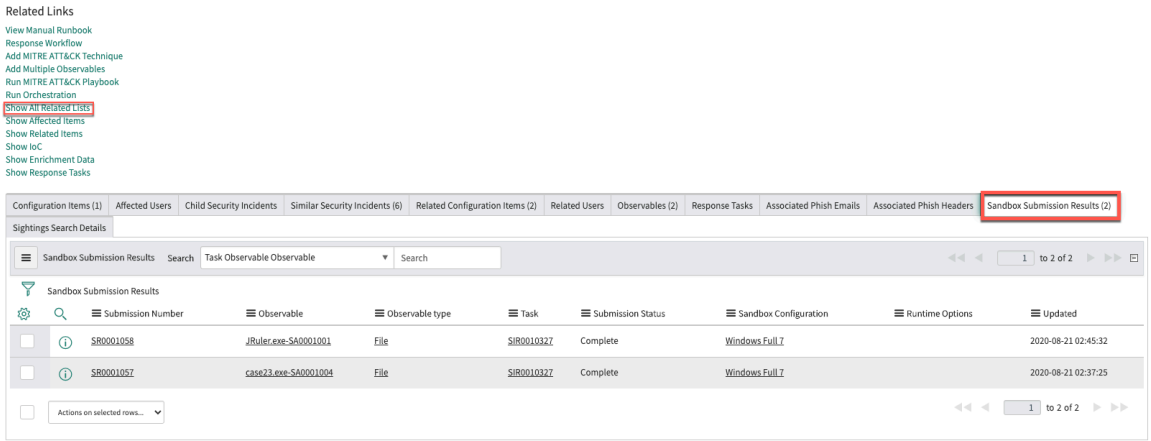
Prozedur

1. Öffnen Sie den Security Incident , mit dem Sie arbeiten, und vergewissern Sie sich, dass die andbox-Übermittlung der serfolgreich war.

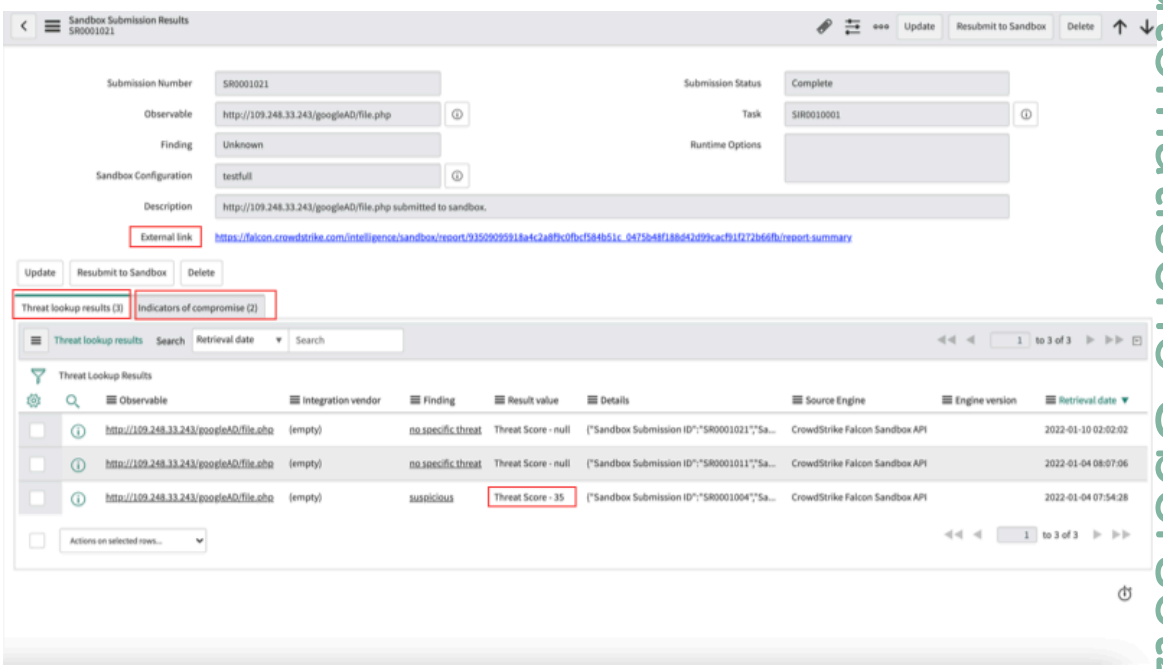


2. Lesen Sie die Arbeitsnotizen , um weitere Informationen zu erhalten, und erfahren Sie, wie Sie vorgehen, wenn Sienicht überprüfen können, ob der Scan erfolgreich war.
3. Klicken Sie entweder auf den Link zu vollständigen Ergebnissen in der Arbeitsnotizs oder am am Ende des Security Incidentsund navigieren Sie zu **Alle zugehörigen Listen anzeigen**> **Sandbox-Übermittlungsergebnisse**.
   Die Ergebnisse werden auf der Registerkarte Sandbox-Übermittlungsergebnisse angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf, um einen beliebigen -Datensatz zu öffnen, um die vollständigen s-andbox-Analyse anzuzeigen.



5. **Wahlweise:** Klicken Sie auf **Erneut an die Sandbox übermitteln,** um das erkennbare Element erneut zu verarbeiten.

Ergebnisse

- Die Registerkarte **Ergebnisse der Bedrohungssuche** enthält die Bedrohungsbewertung, einschließlich schädlicher Ergebnisse, Bedrohungsbewertungen und zusätzlicher Details. DieDetailinformationen werden in der Standardformatstruktur der Bedrohungssuche für alle ServiceNow Integrationen der Bedrohungssuche bereitgestellt.
- Die **Registerkarte Kompromittierungsindikatoren** zeigt die böswilligen oder verdächtigen sandbox-Ergebnisse mit Konfidenzpunktzahlen an. Die Vertrauensbewertungen ähneln anderen Indikatorinformationen, die auf der Plattform ServiceNow gespeichert werden. Indikatoren, die als informative klassifiziert sind, sind nicht auf dieser Registerkarteenthalten.

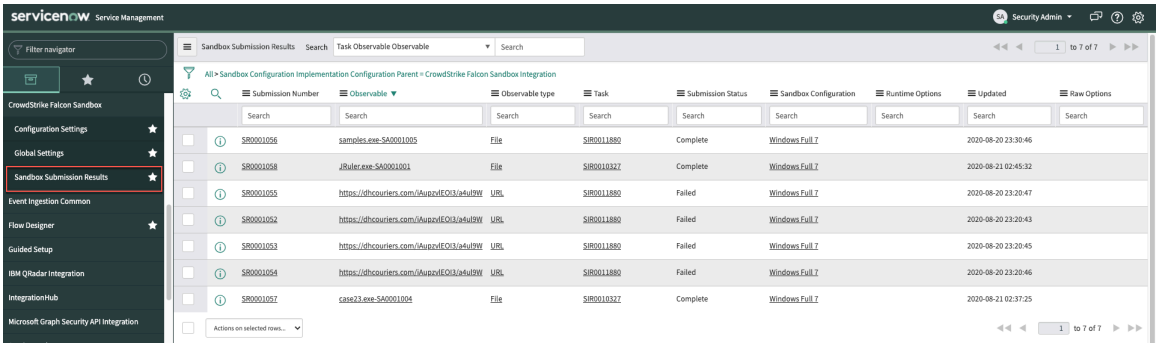
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf **den Link „Extern“**, um die Sandbox-Ergebnisse im Portal CrowdStrike Falcon X Sandbox anzuzeigen.

> **Hinweis:**
> Diese Option setzt voraus, dass , dass Sie über die CrowdStrike Falcon X Sandbox Rolle verfügen, um die Ergebnisse anzuzeigen.

Sie können auch die Andbox-Übermittlungsergebnisse von für alle Security Incidents überwachen, indem Sie zu navigieren **CrowdStrike Falcon Sandbox** > **Sandbox-Übermittlungsergebnisse**.



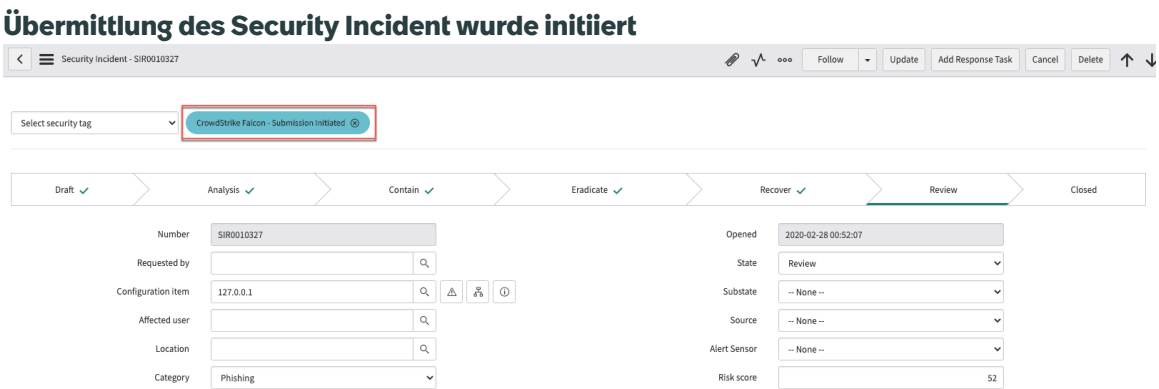
Markieren Sie Security Incidents mit dem Sandbox-Übermittlungsstatus

Sie können Security Incidents optional mit den Tags Übermittlung initiiert und Übermittlung abgeschlossen versehen.

Wenn Sie in der Sandbox-Übermittlungskonfiguration die Option **Tags anzeigen**auswählen, werden Tags angezeigt, um den Status einer Datei- oder URL-Übermittlung anzugeben. Diese Überprüfung des Status ist nützlich, , da die Verarbeitung der s-Andbox-Analyse mehrere Minuten dauern kann.

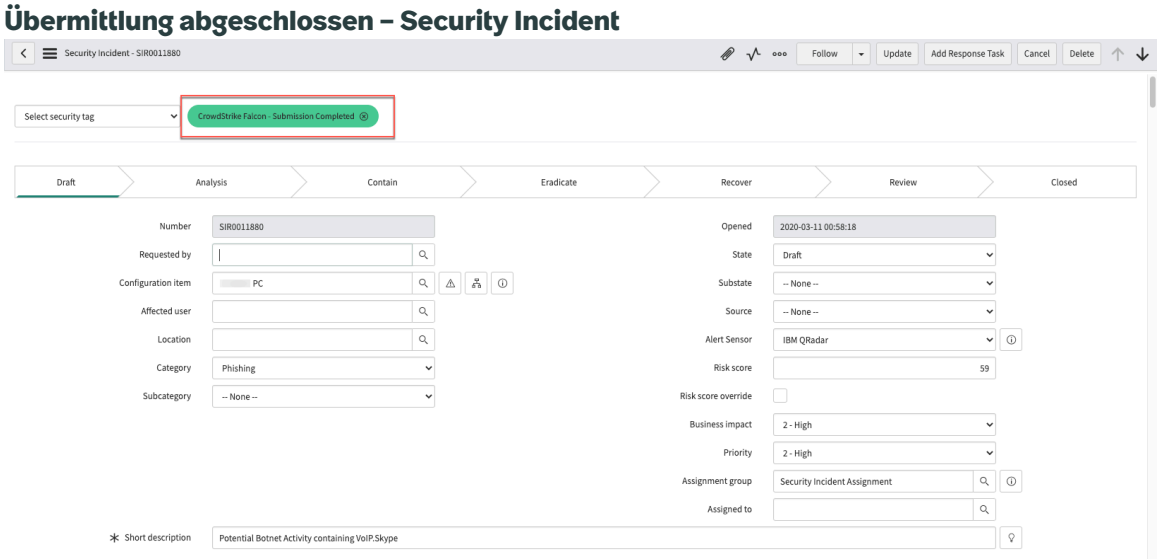
Die Anzeige-Tags sind und werden als „Übermittlung “ „initiiert“, „Übermittlung abgeschlossen“ und „Übermittlung fehlgeschlagen“ bezeichnet.

Das folgende Beispiel zeigt einen Security Incident, bei dem die Übermittlung initiiert wurde.



Das folgende Beispiel zeigt einen Security Incident, bei dem die Übermittlung abgeschlossen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Überprüfen Sie die globalen Einstellungen von sandbox

Wenn Probleme mit den Ergebnissen der Datei- oder URL-Übermittlung auftreten, überprüfen und ändern Sie die globalen s-andbox-Einstellungen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon Sandbox** > **Globale Einstellungen**.
2. Überprüfen und ändern Sie die Einstellungen nach Bedarf.

Feld	Beschreibung
Dateigrößenbeschränkung (MB)	Sandbox-Upload-Dateigrößenbeschränkung in Megabyte. **Hinweis:** Die Dateigrößenbeschränkung von 256 MB ist standardmäßig konfiguriert. Erhöhen Sie den Wert nicht über 256 MB. Möglicherweise möchten Sie jedoch die maximale Dateigröße reduzieren, um zu vermeiden, dass große Dateien übermittelt werden.
Maximale Zeitüberschreitung für die Übermittlung von Ergebnissen (Minuten)	Maximale Zeitüberschreitung für die Übermittlung von Ergebnissen von an sandbox. **Hinweis:** Die Standardzeitüberschreitung beträgt 30 Minuten. Wenn Ihre Ergebnisse länger als 30 Minuten dauern, , können Sie die Zeit verlängern. Außerdem können Sie die Ergebnisse im andbox-Portal sanzeigen.

3. Klicken Sie auf **Speichern** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration mit Elasticsearch Incident Enrichment

Die Integration Elasticsearch – Incident Enrichment durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden	Einrichten
Security Incident Response-Integrationen	• Erste Schritte mit der Integration Elasticsearch - Incident Enrichment • Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

Verwenden	Entwickeln
• Führen Sie eine Sichtungssuche aus • Security Operations Integration - Sichtungssuche-Flow • Security Operations – Elasticsearch Sightings-Such-Flow	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der Integration Elasticsearch - Incident Enrichment

Elasticsearch ist eine verteilte RESTful-Such- und Analyse-Engine, die sich problemlos in Security Operationsintegrieren lässt. Bevor Sie die Integration Elasticsearch - Incident Enrichment verwenden können, müssen Sie sie von ServiceNow Store herunterladen und die entsprechende API-Basis-URL sowie Anmeldeinformationen hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

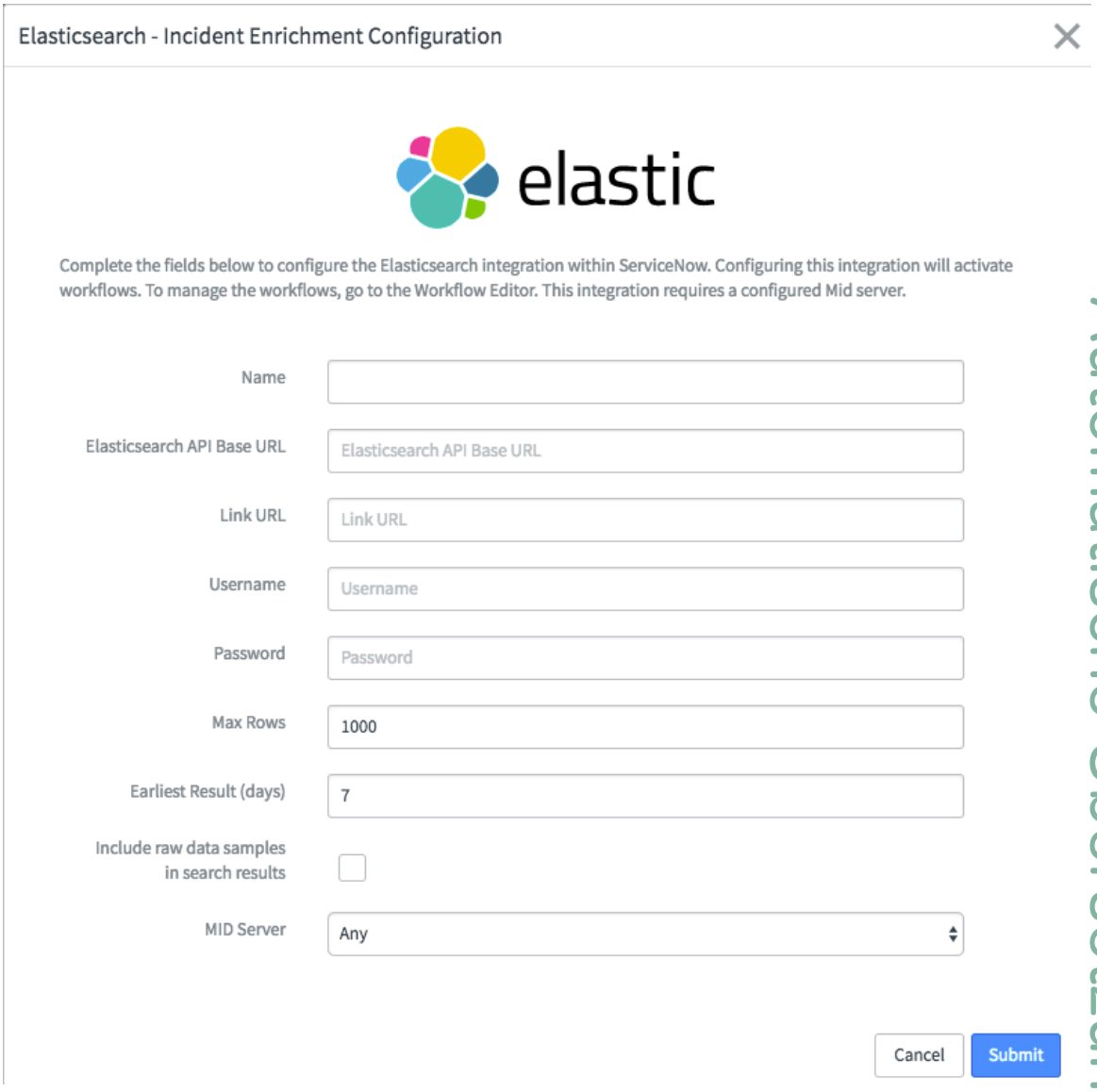
Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf Elasticsearch zu, und rufen Sie die API-Basis-URL in Ihrem Elasticsearch-Profil ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte Elasticsearch – Incident-Ergänzung **auf Neu**.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der Elasticsearch-API	Die Basis-URL, die Sie von der Website Elasticsearch erhalten haben.
Link-URL	[Optional] Links zu einer Kibana-Instanz, falls verfügbar
Anwendername	Ihr Intel-Anwendername Elasticsearch.
Passwort	Ihr Intel-Passwort Elasticsearch.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der **Anzahl der Zeilen der Rohdateneigenschaft** in den Security Incident Response-Eigenschaftenab.
MID-Server	Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern bzw. zu löschen.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

Ergebnisse
Nach der Konfiguration kann die Integration Elasticsearch - Incident Enrichment für die Veröffentlichung von erkennbaren Elementen in Beobachtungslisten in Security Incident Response ausgewählt werden.

FireEye Endpoint Security-Integration

FireEye Endpoint Security (HX-Serie) hilft Unternehmen zu überprüfen und zu analysieren, welche bekannte und unbekannte Bedrohungen auf jedem Endpunkt enthält.

Heutige geschickte Angreifer umgehen traditionelle Abwehrmaßnahmen, auf die sich die meisten Sicherheitsteams seit Jahren zum Schutz ihrer Endpunkte verlassen. Selbst wenn eine herkömmliche Verteidigung eine bekannte Bedrohung stoppt, kann sie nicht feststellen, was diese Bedrohung versucht hat. FireEye HX Endpunktsicherheit hilft Ihrem Sicherheitsteam, bekannte und unbekannte erweiterte Bedrohungen für Ihre Endpunkte aufzuspüren und zu stoppen.

Die Integration von Gold Standard Security Incident Response mit FireEye HXmacht es Sicherheitsanalysten einfacher und effizienter, Security Incidents im Handumdrehen zu untersuchen und zu beheben, ohne zwischen Tools navigieren zu müssen. Mithilfe der Netzwerkeindämmung können Sie Korrekturaktionen an den Endpunkten durchführen, Profile implementieren, um bestimmte Details zum Host zu sammeln, und am Endpunkt bestimmte Abfragen oder Aktionen ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

- Fähigkeit, Host-Ergänzungsaktionen auszuführen, um weitere Details zum Endpunkt zu sammeln, z. B. Hostdetails, Netzwerkstatistiken, Benutzerdetails, Dateidetails, Prozessdetails und Servicedetails.
- Fähigkeit, Enterprise Security Search durchzuführen, um potenziell schädliche erkennbare Elemente über Endpunkte hinweg zu erkennen und Korrekturmaßnahmen zu ergreifen.
- Fähigkeit zur Erfassung von Selektierung und Datenerfassung für eingehende Endpunktprüfungen und -analysen.

Einschränkungen

Im Folgenden sind die bekannten Einschränkungen dieser Integration aufgeführt:

1. Der Wert im Feld „MID-Anwendung“ muss manuell eingegeben werden.
2. „Host isolieren“ und „Laufende Services abrufen“ können auf dem Linux-Agent nicht ausgeführt werden.
3. „Isolation entfernen“ bietet keine Unterstützung für Linux-Agent.
4. Selektierungsakquisition bietet keine Unterstützung für Linux-Agent.
5. Benutzer müssen zugehörige Links zum Anzeigen der Ergänzungsdaten konfigurieren. Es ist nicht standardmäßig verfügbar.
6. Für die Sichtungssuche können nur fünf aktive Suchen gleichzeitig vorhanden sein. Die verbleibenden werden in die Warteschlange gestellt und beginnen nach Abschluss einer der laufenden Sichtungen.
7. Sichtungen sind sofort einsatzbereit und werden standardmäßig als aktiv „falsch“ festgelegt.
8. Hash wird für „Laufende Prozesse abrufen“ nicht unterstützt.

Richten Sie Ihre Now Platform-Instanz für die FireEye-Integration ein

Überprüfen Sie das folgende Konfigurationsverfahren, um die Now Platform-Instanz für die FireEye-Integration einzurichten.

Vorbereitungen
Erforderliche Rolle: Now Platform Administrator (sn_si.admin)

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in Ihrer Now Platform-Instanz ausführen müssen, bevor Sie die Anwendung für die FireEye-Integration installieren.

Stellen Sie sicher, dass Sie die folgenden Aufgaben abgeschlossen haben, bevor Sie die Anwendung aus dem ServiceNow Store installieren.

Aufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen für Now Platform und Security Incident Response (SIR) zugewiesen haben.	Die folgenden Rollen sind erforderlich: 1. Zur Installation der Anwendung für die Integration ist ein Benutzer mit der Rolle „Systemadministrator“ (admin) erforderlich. 2. Ein Anwender mit der Rolle „Security Incident-Administrator“ (sn_si.admin)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	ist erforderlich, um die Integration zu konfigurieren sowie Profile zu erstellen, zu aktivieren und zu entfernen. 3. Benutzer mit der Rolle „Security Incident-Analyst“ (sn_si.analyst) sind für die Arbeit mit Security Incidents erforderlich. Ein Benutzer mit dieser Rolle kann alle in der Integration verfügbaren Fähigkeiten initiieren.
Stellen Sie sicher, dass Sie einen MID-Server installiert und konfiguriert haben.	MID-Server konfigurieren: Ein MID-Server in Ihrer Now Platform-Instanz ist erforderlich, um Dateien zu verwalten und eine Verbindung zum FireEye-Service herzustellen, der in Ihrem Organisationsnetzwerk bereitgestellt wird. Weitere Informationen zu MID-Servern finden Sie unter https://servicenow.com/docs
Stellen Sie sicher, dass die ServiceNow Core-Anwendungen, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung installieren.	Die folgenden Anwendungen müssen im ServiceNow Store installiert und aktiviert werden, bevor Sie diese Anwendung installieren. Installieren Sie eine Anwendung nach der anderen in der unten aufgeführten Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten: 1. Security Incident Response-Support 2. Security Support Core 3. Security Support Common 4. Security Incident Response 5. Threat Intelligence Support Common 6. Installationsprogramm für das ServiceNow Integration Hub Enterprise-Paket
Bevor Sie die Genehmigungsoption für Profile aktivieren, vergewissern Sie sich, dass Sie eine Genehmigungsgruppe erstellt haben.	Ein optionaler Genehmigungsworkflow ist verfügbar, um Hostcomputer zu isolieren, sie wieder im Netzwerk herzustellen, Dateien abzurufen und zusätzliche Aktionen für den Endpunkt auszuführen. Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünscht, aktivieren Sie bei der Konfiguration der Profile die Option Genehmigung erforderlich. Wenn kein Profil vorhanden ist und eine Fähigkeit direkt aus der zugehörigen Liste aufgerufen wird, können Genehmigungen über das FireEye-Standardeinstellungsmodul bearbeitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

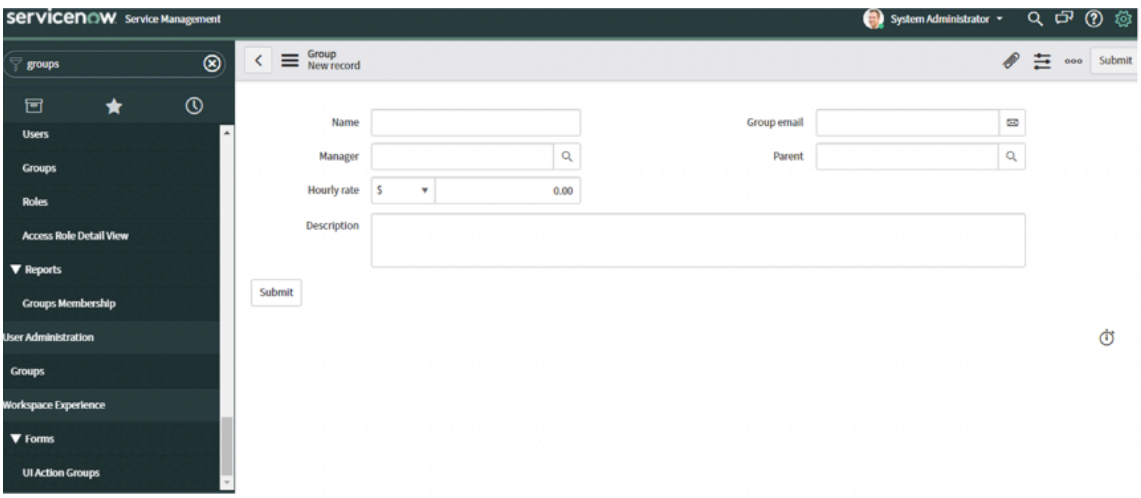
Aufgabe	Beschreibung
	Als Sicherheitsadministrator können Sie Genehmigungen einrichten, während Sie die Profile und Standardeinstellungen konfigurieren. Eine Genehmigungsgruppe muss in der Gruppenliste in Ihrer Instanz verfügbar sein.

Prozedur

1. Navigieren zu **Anwenderadministration** > **Gruppen**.
2. Klicken **Neu** in der Liste Gruppen.
3. Füllen Sie das Formular mit den folgenden Details aus:

Feld	Beschreibung
Name	Name der Gruppe, der angezeigt wird, wenn eine Genehmigungsanforderung übermittelt wird.
Gruppen-E-Mail	(Optional) Gruppen-E-Mail-Verteilerliste oder die E-Mail-Adresse des Kontaktpunkts, z. B. des Gruppenmanagers.
Manager	(Optional) Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen.
Übergeordnet	(Optional) Name der übergeordneten Gruppe, falls einem übergeordneten Element zugeordnet.
Stundensatz	(Optional) Der bezahlte Betrag für jede geleistete Stunde.
Beschreibung	(Optional) Zusätzliche Informationen zur Gruppe.

4. Klicken **Absenden**.



Die neue Gruppe wird in der Gruppenliste angezeigt. Sie haben erfolgreich eine Genehmigungsgruppe erstellt. Fügen Sie Ihrer neuen Gruppe nach Bedarf Benutzer hinzu, die die vom Sicherheitsanalysten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

übermittelten Anforderungen genehmigen können. Ein Benutzer erbt Rollen von allen Gruppen, denen er angehört. Sie können Rollen auch direkt einem Benutzer zuweisen.

Zur Überwachung und Verarbeitung von Anforderungen, die von Anwendern mit der Rolle „sn_si.analyst“ übermittelt werden, müssen alle Mitglieder der Genehmigungsgruppe in der Now Platform zu „Meine Genehmigungen“ navigieren. Alternativ finden Genehmiger die Anforderungen, die speziell für die FireEye-Integration übermittelt wurden, unter FireEye Approvals (FireEye-Genehmigungen).

Nächste Maßnahme

Der nächste Schritt besteht in der Installation und Konfiguration der Anwendung über den ServiceNow Store.

Zeitstempeleinstellungen für Selektierungsakquisition werden konfiguriert

Konfigurieren und überprüfen Sie die Zeitstempeleinstellungen vor dem Installationsverfahren.

Vorbereitungen

Erforderliche Rolle: Now Platform Security Incident Administrator (sn_si. admin)

Vor der Installation der Anwendung FireEye müssen in FireEye einige Voraussetzungen erfüllt sein.

Die Selektierungserfassung kann durch Eingabe des Felds „Um Zeitstempel“ oder „Standard“ angefordert werden. Um Zeitstempel-Anforderungsinformationen, die während eines angegebenen Zeitraums vor dem Zeitstempel bis zu einem angegebenen Zeitraum nach dem Zeitstempel gesammelt wurden. Der Zeitstempel gibt die Uhrzeit an, zu der das Ereignis aufgetreten ist, von dem die Warnung generiert wurde. Wenn Sie Standard auswählen, fordert die Endpoint Security-Appliance vom Host Informationen zu allen Daten rund um ein Ereignis an.

Wenn ein Endpoint Security-Benutzer eine Selektierungssammlung basierend auf einem bestimmten Datum und einer bestimmten Uhrzeit anfordert, gibt der Agent Informationen für ein bestimmtes Zeitfenster vor und nach der Warnung zurück. Die Zeitstempeleinstellungen steuern die Länge des Fensters für die Selektierungssammlung. Zeitstempeleinstellungen gelten nur für Agent-URL-Ereignisse (URL-Überwachungsereignisse) und Registrierungsschlüssel-Ereignisse (Registrierungsschlüssel-Ereignisse).

Auf der Registerkarte Zeitstempeleinstellungen können Sie festlegen, wie lange vor und nach dem Zeitstempel Informationen gesammelt werden. Zeitstempeleinstellungen können im Bereich von 0 bis 86.400 Sekunden liegen. Der Standardwert für beide Einstellungen beträgt 600 Sekunden.

Auf der Seite Einstellungen für automatische Selektierung können Sie die Registerkarte Zeitstempeleinstellungen verwenden, um die Zeitspanne vor und nach dem Zeitstempel festzulegen, während der Informationen gesammelt werden. Der Zeitstempel gibt die Zeit an, zu der das Ereignis aufgetreten ist, das die Warnung ausgelöst hat.

Prozedur

1. Navigieren zu **Web-UI für Endpunktsicherheit**.
2. Auswahlvorgang **Administrator** > **Selektierungseinstellungen**.
3. Klicken **Zeitstempeleinstellungen** Registerkarte auf **Einstellungen für automatische Selektierung** Seite.
4. Geben Sie an, wie lange vor und nach dem Zeitstempel die Informationen benötigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie die Anzahl der Sekunden vor dem angegebenen Zeitstempel ein, für die die Informationen benötigt werden.
6. Geben Sie die Anzahl der Sekunden nach dem Zeitstempel ein, für die die Informationen benötigt werden.
7. Klicken **Speichern**.

Hinweis:
Sie können alle Werte auf der Seite auf die Standardeinstellungen zurücksetzen, indem Sie auf klicken **Auf Standardwerte zurücksetzen**, und klicken Sie auf Speichern.

- **Beschaffungs-Space-Bereich**: Auf der Seite „Akquisitionen“ wird angezeigt, wie viel Speicherplatz noch für Akquisitionen verfügbar ist.
- **Festlegen von Grenzwerten für die Festplattenauslastung für Akquisitionen:**
  - Selektierungen, Datei- und Datenerfassungen können sich mit der Zeit ansammeln und immer mehr Speicherplatz beanspruchen. Um dies zu steuern, können Sie ihnen eine bestimmte Menge an Speicherplatz zuweisen. 10 % des von Ihnen angegebenen Speicherplatzes sind für automatische Selektierungsakquisitionen reserviert. Wenn der insgesamt zugeteilte Speicherplatz überschritten wird, werden die ältesten automatischen Selektierungen gelöscht.
  - Wenn die Gesamtdatenträgergröße der abgeschlossenen Erfassungen einen bestimmten Grenzwert überschreitet, löscht das Endpoint Security-Gerät die ältesten abgeschlossenen Erfassungen, bis genügend Speicherplatz frei ist, um die Gesamtgröße unter den angegebenen Grenzwert zu bringen. Akquisitionen, die noch nicht abgeschlossen wurden, sind nicht betroffen.
  - Die Endpoint Security-Appliance löscht automatisch Erfassungen, wenn ein Administrator, Analyst oder Ermittler die Endpoint Security-Web-UI verwendet, um den zugehörigen Agent manuell zu löschen.

  So legen Sie Grenzwerte für die Datenträgerauslastung für vollständige Beschaffungen über die Web-UI fest:
- Navigieren Sie zu **Endpunktsicherheit Web-UI**.
- Auswahlvorgang **Grenzwerte für die Festplattenauslastung** aus dem **Administrator** Menü.
- Im **Platzlimit für Beschaffung** Bereich; geben Sie die maximale Menge an Festplattenspeicher (in GB) an, der zum Speichern von Selektierungen, Datei- und Datenerfassungen verwendet werden kann. Gültige Werte und Standardwerte variieren je nach Ihrem Endpunktsicherheits-Appliance-Modell. Die für Ihr Modell geeigneten Werte werden auf der Seite „Limits für die Festplattenauslastung“ angezeigt.
- Klicken **Speichern**.

Hinweis:
Alle genannten Einstellungen werden berücksichtigt, und bei Fehlern gibt Now Platform nur diese Fehler zurück.

Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration

Installieren und konfigurieren Sie die Anwendung aus dem ServiceNow Store in Ihrer Now Platform-Instanz.

Vorbereitungen
Erforderliche Rolle: Now Platform-Administrator (admin)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

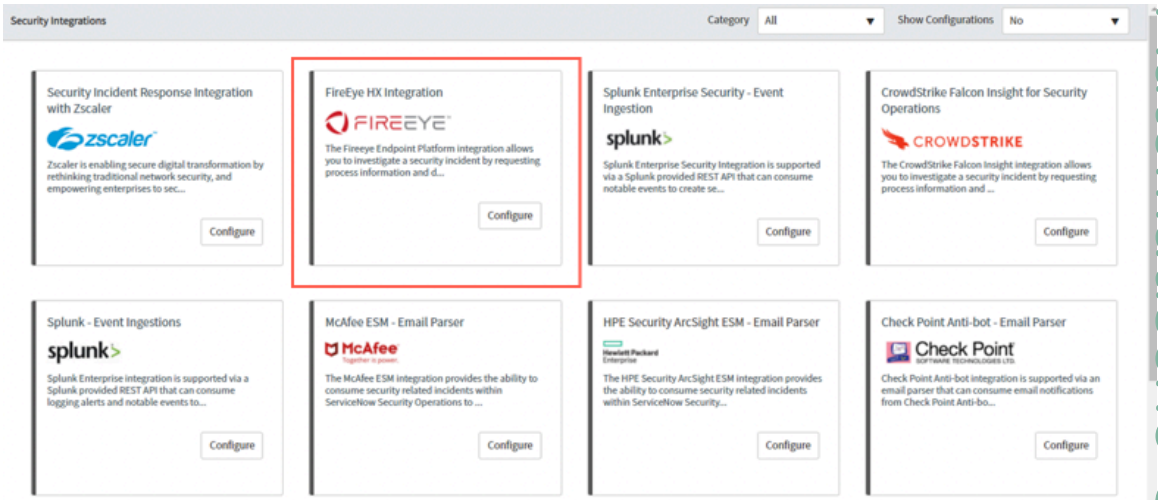
Hinweis:
Zum Konfigurieren einer Quelle ist ein aktiver MID-Server erforderlich.

Laden Sie die Anwendung „Security Incident Response integration with FireEye HX “ aus dem ServiceNow Store herunter, und installieren Sie sie.

Nachdem Sie die Anwendung erfolgreich installiert haben, konfigurieren Sie sie mit den folgenden Schritten:

Prozedur

1. Navigieren zu **Integrationen** > **Integrationskonfigurationen**.
2. Rufen Sie die Eigenschaft **Integrationskonfigurationen** Modul, um die verfügbaren Integrationen anzuzeigen, und suchen Sie das **FireEye** Kachel.



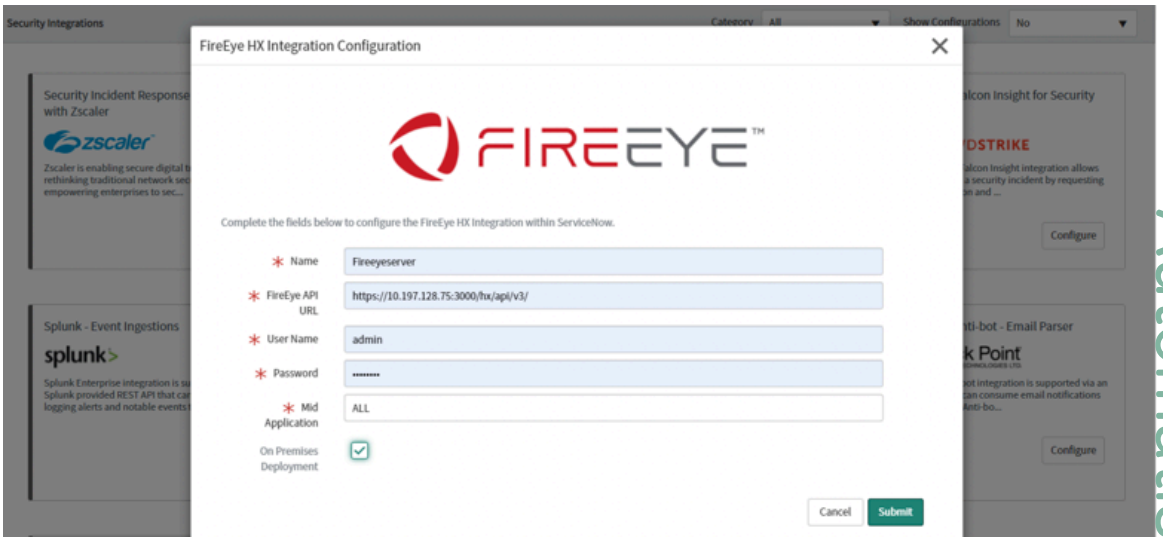
3. Klicken **Konfigurieren** auf der FireEye-Kachel.
4. Geben Sie die folgenden Details an, um die FireEye-Integration einzurichten:

Feld	Beschreibung
Name	Name der FireEye-Konfiguration. Dieser Name wird verwendet, um die Quelle und die zugehörigen Anmeldeinformationen und die Konfiguration zu identifizieren. Dieser Name hilft Ihnen, die Anmeldeinformationen und Konten zu unterscheiden und jede Quelle zu identifizieren, um Konflikte mit Profilen zu vermeiden.
API-URL	Basis-URL, die die FireEye-API hostet.
Anwendername	Geben Sie den Anwendernamen des FireEye-Kontos ein.
Passwort	Geben Sie das Passwort des FireEye-Kontos ein.
MID-Anwendung	MID-Anwendung, die in Ihrer Umgebung eingerichtet ist. Für einige der Ergänzungsfunktionen ist ein MID-Server erforderlich, um ZIP-Dateien zu verarbeiten.

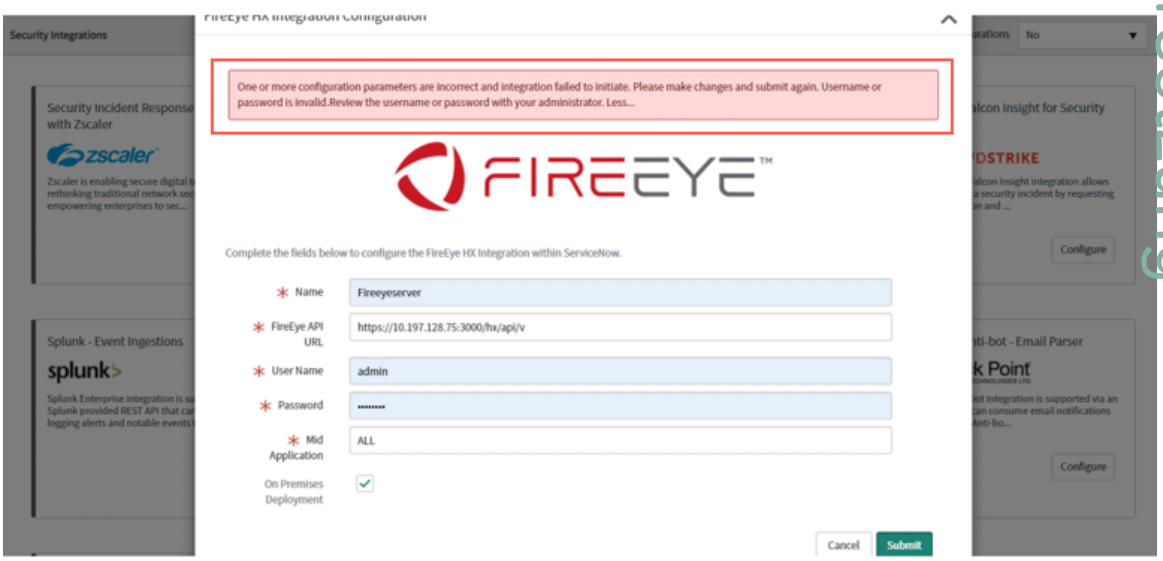
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standardmäßig ist dies ALLE. Anwender müssen einen gültigen Anwendungsnamen manuell angeben.
Lokale Bereitstellung	Standardmäßig ist deaktiviert. Wenn Sie die cloudbasierte Version von FireEye verwenden, stellen Sie sicher, dass das Kontrollkästchen deaktiviert ist.



5. Klicken **Absenden**.
   Die FireEye-Konfigurationsliste wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für einen FireEye-Server abgeschlossen. Wenn Sie keine Verbindung mit FireEye herstellen können oder Ihre Anmeldeinformationen falsch sind, wird eine Validierungsfehlermeldung angezeigt (siehe folgende Abbildung). Stellen Sie sicher, dass Ihre Anmeldeinformationen korrekt sind, und versuchen Sie es erneut.



FireEye: Standardeinstellungen

Im Folgenden finden Sie die zusätzlichen Konfigurationseinstellungen nach Abschluss der Installation.

Automatische Übersetzung

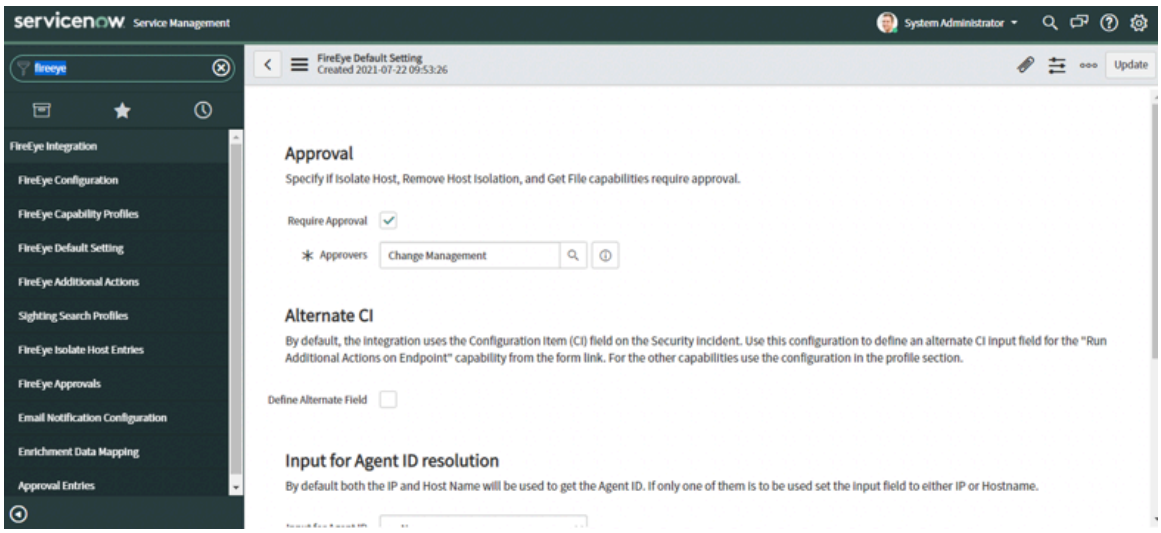
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald Sie die Installation abgeschlossen haben, finden Sie das Modul FireEye-Standardeinstellungen in der linken Navigationsleiste. Sie enthält Standardeinstellungen für verschiedene FireEye-Funktionen.

Zusätzliche Konfigurationen

Im Folgenden finden Sie die zusätzlichen Konfigurationseinstellungen:

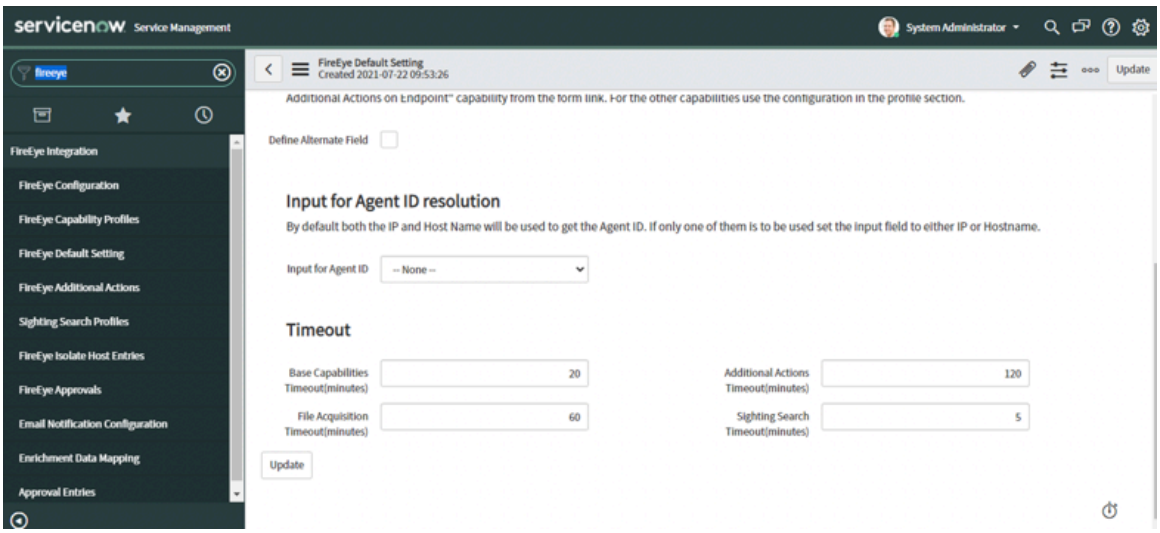
1. **Genehmigung**: Diese Genehmigung gilt speziell für die Funktionen „Host isolieren“, „Hostisolierung entfernen“ und „Datei abrufen“, wenn sie direkt über die zugehörige Liste ausgelöst werden und keine Profile für sie vorhanden sind. Wenn für diese Fähigkeiten Profile vorhanden sind, wird die Genehmigungskonfiguration im Profil berücksichtigt.
   - **Genehmigung erforderlich:** Wenn Sie „Genehmigung erforderlich“ aktivieren, ist das Feld „Genehmiger“ im Formular verfügbar.
   - **Verantwortliche Vertragsgenehmigung**: Liste der Genehmigergruppen. Nachdem Sie eine Anforderung übermittelt haben, ist zum Abschließen der Anforderung eine Genehmigung durch die Gruppe erforderlich.
2. **Alternatives CI**: Durch Aktivieren dieses Kontrollkästchens wird eine Liste der Felder angezeigt, mit denen ein alternatives CI an die Fähigkeit übergeben werden kann. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Diese Konfiguration gilt nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“. Verwenden Sie diese Konfiguration also, um ein alternatives CI-Eingabefeld nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“ zu definieren. Verwenden Sie für die anderen Fähigkeiten die Konfiguration im Profilabschnitt. Wenn die Profile kein alternatives CI definieren, wählen die Fähigkeiten das CI-Feld aus dem Formular „Security Incident“ aus.
3. **Eingabe für die Auflösung der Agent-ID**: Standardmäßig werden IP und Hostname zum Abrufen der Agent-ID verwendet. Wenn nur einer von ihnen verwendet werden soll, setzen Sie das Eingabefeld auf „IP“ oder „Hostname“.



4. **Zeitüberschreitung**:
   - **Basisfähigkeiten – Zeitüberschreitung (Minuten):** Die Funktionen „Anreicherung“, „Host isolieren“ und „Hostisolierung entfernen“ schlagen fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.
   - **Zeitüberschreitung für zusätzliche Aktion (Minuten):** Die Funktion „Zusätzliche Aktionen für Endpunkt ausführen“ schlägt fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Zeitüberschreitung bei Dateierfassung (Minuten):** Die Funktion „Datei abrufen“ schlägt fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.
- **Sichtungssuche – Zeitüberschreitung (Minuten):** Die Suche wird nach der festgelegten Zeit beendet.



Erstellen Sie ein neues Fähigkeitsprofil für die FireEye-Endpunktintegration

Erstellen Sie ein Profil, und wählen Sie die FireEye HX -Fähigkeiten aus, die das Profil ausführen soll.

Vorbereitungen
Erforderliche Rolle: Now Platform Security Incident Administrator (sn_si. admin)

Warum und wann dieser Vorgang ausgeführt wird
Profile werden erstellt, um Fähigkeiten zu bündeln und es Analysten zu ermöglichen, die Untersuchung/Nachbesserung einfach durchzuführen.

Im Folgenden finden Sie die Liste der Fähigkeiten, die Sie Profilen hinzufügen können:

1. Hostdetails abrufen
2. Angemeldete Anwender abrufen
3. Netzwerkstatistiken abrufen
4. Laufende Prozesse abrufen
5. Laufende Services abrufen
6. Datei abrufen
7. Host isolieren
8. Isolation entfernen

Sie können die Funktionen „Datei abrufen“, „Host isolieren“ und „Hostisolierung entfernen“ nicht mit anderen Funktionen kombinieren, während Sie ein Profil erstellen. Profile dafür müssen einzeln erstellt werden. Die Aktionen „Systemdetails abrufen“, „Angemeldete Anwender abrufen“, „Netzwerkstatistiken abrufen“, „Laufende Prozesse abrufen“ und „Laufende Services abrufen“ können hingegen zusammengefasst werden. Sie können Profile einzeln erstellen oder sie je nach Bedarf ganz oder teilweise zusammenstellen. Sobald eine Fähigkeit in einem Profil enthalten ist, kann sie nicht in ein anderes Profil aufgenommen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um ein neues Fähigkeitsprofil zu erstellen, gehen Sie wie folgt vor:

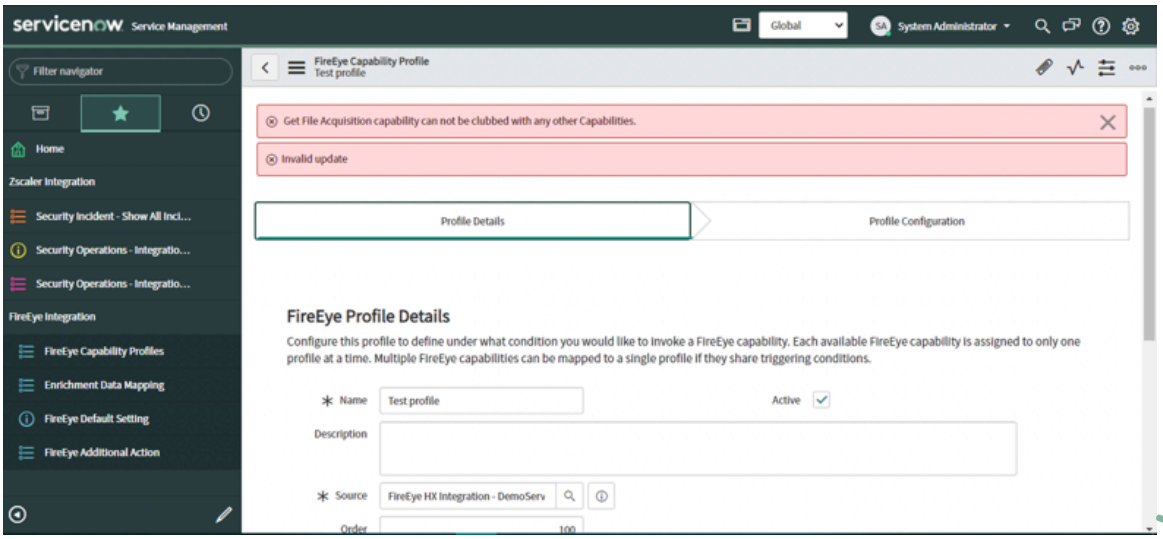
Prozedur

1. Navigieren zu **FireEye-Integration** > **FireEye-Funktionalitätsprofile**.
   Die Liste der Fähigkeitsprofile wird angezeigt.
2. Klicken **Neu**.
3. Füllen Sie die Felder im Formular aus.

Name	Name für das Fähigkeitsprofil FireEye HX. Mit diesem Namen können Sie den Profiltyp identifizieren und beschreiben.
Beschreibung	Zusätzliche Informationen zum Profil, die das Profil weiter beschreiben.
Quelle	Name der FireEye HX -Quelle. In der Auswahlliste sind nur konfigurierte Quellen verfügbar.
FireEye HX-Fähigkeiten	Fähigkeiten des Profils FireEye HX. Wählen Sie die gewünschten Fähigkeiten für dieses Profil aus der Spalte Verfügbar aus, und verschieben Sie sie in die Spalte Ausgewählt.
Bestellung	Flow-Priorität. Der Standardwert ist 100. Der Wert dieses Felds gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Flow mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Beispiel: 100, 200, 300, 400.
Aktiv	Dies zeigt an, dass das Profil aktiv ist. Wenn das Profil aktiv ist, wird es automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den von Ihnen in der Konfiguration angegebenen Filterbedingungen entspricht.

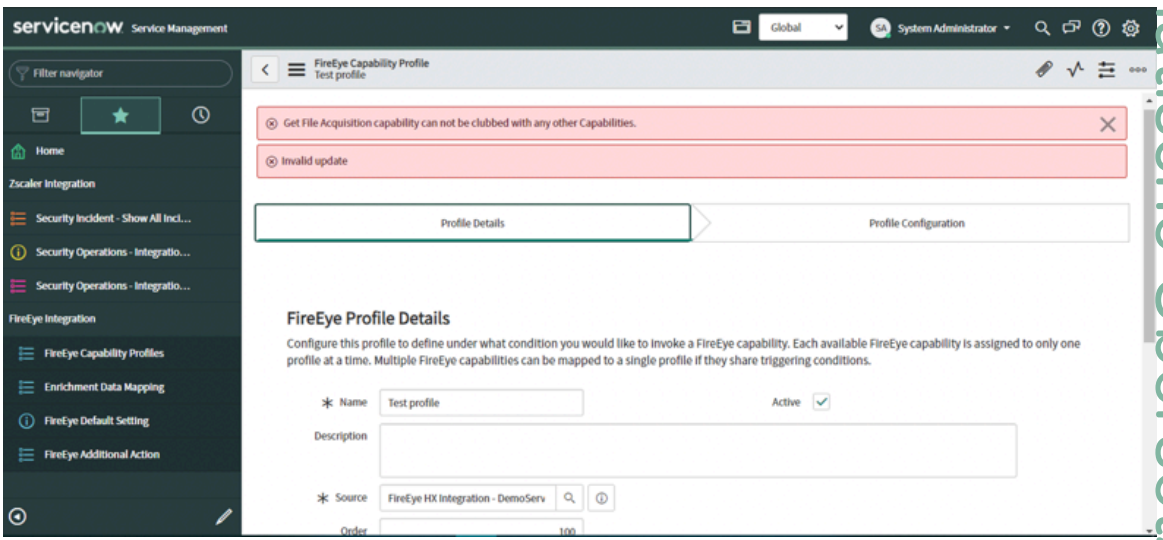
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für Profildetails mit der Fähigkeit „Hostdetails abrufen“.

4. Klicken **Weiter** um mit der Profilkonfiguration fortzufahren.



Hinweis:
Die Funktionen „Host isolieren“, „Hostisolierung entfernen“ und „Datei abrufen“ können nicht mit anderen Funktionen verknüpft werden.

Nächste Maßnahme

Im nächsten Schritt konfigurieren Sie Ihr Profil. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie sich die Konzepte zum Konfigurieren von Profilen und Auslösebedingungen ansehen. Weitere Informationen finden Sie unter Funktionsweise von Auslösebedingungen mit Konfigurationselementen für Profile verstehen.

Verstehen, wie Auslöserbedingungen mit einem Configuration Item funktionieren

Nachdem Sie ein Profil erstellt und die FireEye-Funktionen ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Profileinstellungen so, dass es nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt ist.

Sie können Auslöserbedingungen festlegen, sodass das Profil automatisch ausgeführt wird, wenn ein Security Incident erstellt wird, der der Auslöserbedingung entspricht. Wenn die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

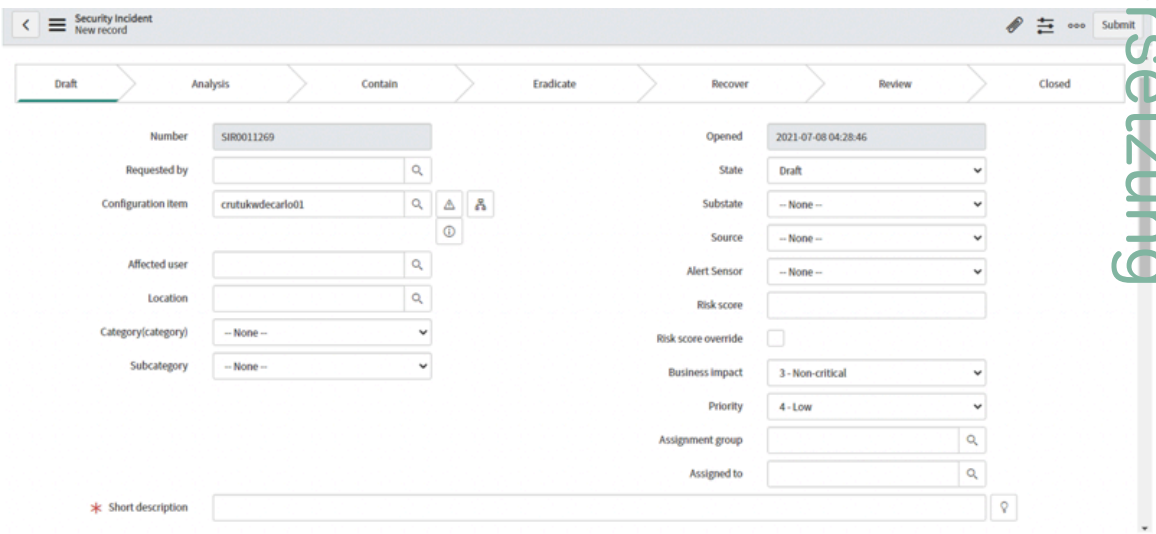
Auslöserbedingung nicht festgelegt ist, können diese Profile manuell ausgeführt werden, indem Sie im Security Incident auf das Formular „EDR-Profil(e) ausführen“ klicken und das Profil auswählen.

Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in der Now Platform-CMDB gespeicherten Informationen abzugleichen. Wenn ein Security Incident erstellt wird und ein Profil entweder automatisch oder manuell ausgeführt wird, wird die CMDB durchsucht, um den Hostnamen und/oder die IP-Adresse basierend auf dem Wert des CI-Felds abzurufen. Der Hostname und/oder die IP werden verwendet, um die Agent-ID auf FireEye HX aufzulösen und den Endpunkt zu identifizieren.

Im Idealfall wird ein übereinstimmender Wert in der -Datenbank gefunden, und Daten werden von der Konsole FireEye HX für das übereinstimmende Asset gesammelt. Die Daten für verschiedene Fähigkeiten werden in Ihre Now Platform-Instanz abgerufen und in den zugehörigen Listen von Security Incidents angezeigt. Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der -Datenbank entspricht, können Sie im Security Incident ein alternatives Feld auswählen, das entweder den Hostnamen oder die auszuführende IP-Adresse enthält die Agent-ID-Auflösung.

Während des Konfigurationsschritts des Profil-Setups können Sie ein alternatives CI-Feld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass Sie den Endpunkt unter FireEye HXidentifizieren können. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Durch Auswahl dieses alternativen CI-Felds als Sicherung stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung im zugehörigen Security Incident nicht ausgefüllt wird.

Hinweis:
Die alternativen CI-Felder werden nur für Fähigkeiten berücksichtigt, die einem Profil hinzugefügt werden können. Für alle zusätzlichen Aktionen wird das alternative CI von der Seite mit den Standardeinstellungen ausgewählt.



Konfigurieren Sie Profile und Security Incidents für die -Integration FireEye HX .

Nachdem Sie ein Profil erstellt und die FireEye HX -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Einstellungen so, dass das Profil nur unter den definierten Bedingungen aufgerufen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Konfigurieren Sie das Profil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Wählen Sie bei Bedarf ein alternatives Eingabefeld für das Feld Configuration Item (CI) aus, und legen Sie Filterbedingungen fest, damit das Profil automatisch ausgelöst werden kann, wenn ein Security Incident erstellt wird, der die Auslöserbedingungen erfüllt.

Hinweis:
Sie können zu folgendem Ort navigieren: **Profilkonfiguration** Seite nur nach Eingabe von **Profildetails**.

Prozedur

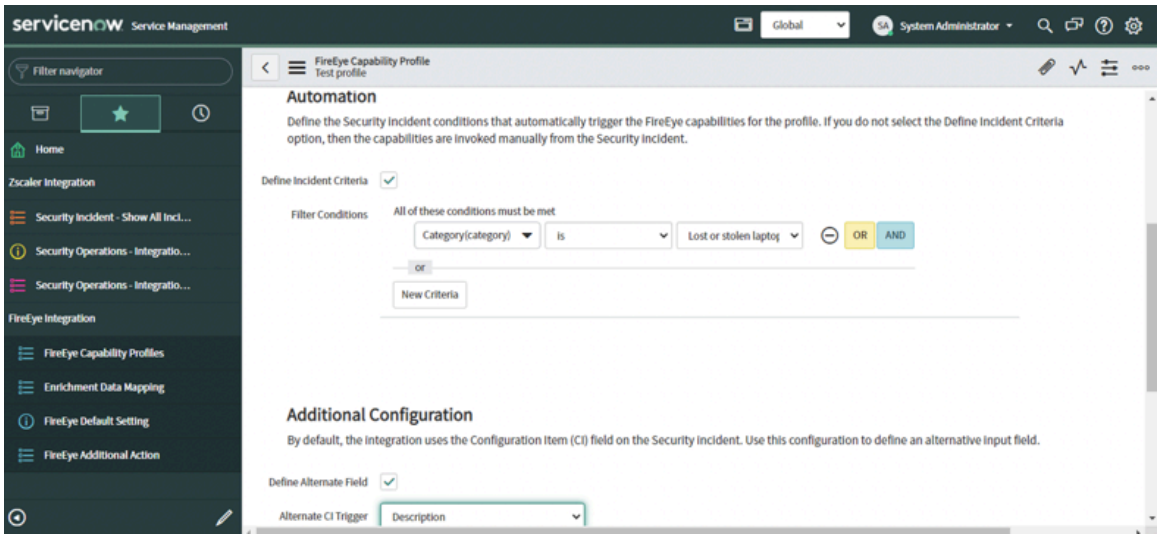
1. Navigieren zu **FireEye-Integration** > **FireEye-Funktionalitätsprofile**.
2. Klicken **Weiter** auf der **Profildetails** Seite nach Abschluss des Abschnitts Profildetails.
3. Überprüfen und konfigurieren Sie die folgenden Abschnitte:
   - **Incident-Kriterien definieren (Automatisierung)**: Definieren Sie die Bedingungen für Security Incidents, die automatisch die Fähigkeiten FireEye HX für das Profil auslösen. Wenn Sie nicht auswählen, wählen Sie **Definiert Incident-Kriterien** können das Profil und die zugrunde liegenden Fähigkeiten manuell über den Security Incident aufgerufen werden.
     - Auswahlvorgang **Definiert Incident-Kriterien** Option zum automatischen Auslösen von FireEye HX -Fähigkeiten im Profil.
     - Im **Filterbedingungen**, wählen Sie das Pflichtfeld aus.
     - Sie können hinzufügen **Neues Kriterium** und definieren auch die ODER- oder die UND-Bedingung.

       Hinweis:
       „Host isolieren“, „Hostisolierung entfernen“ und „Datei abrufen“ können nicht automatisch ausgelöst werden.

   - **Zusätzliche Konfiguration**: Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, um die FireEye HX APIs abzufragen.
     - Rufen Sie die Eigenschaft **Definieren Sie ein alternatives Feld** Option zum Definieren eines alternativen Eingabefelds.
     - Wählen Sie das Eingabefeld aus **Alternatives CI-Auslöserfeld**.

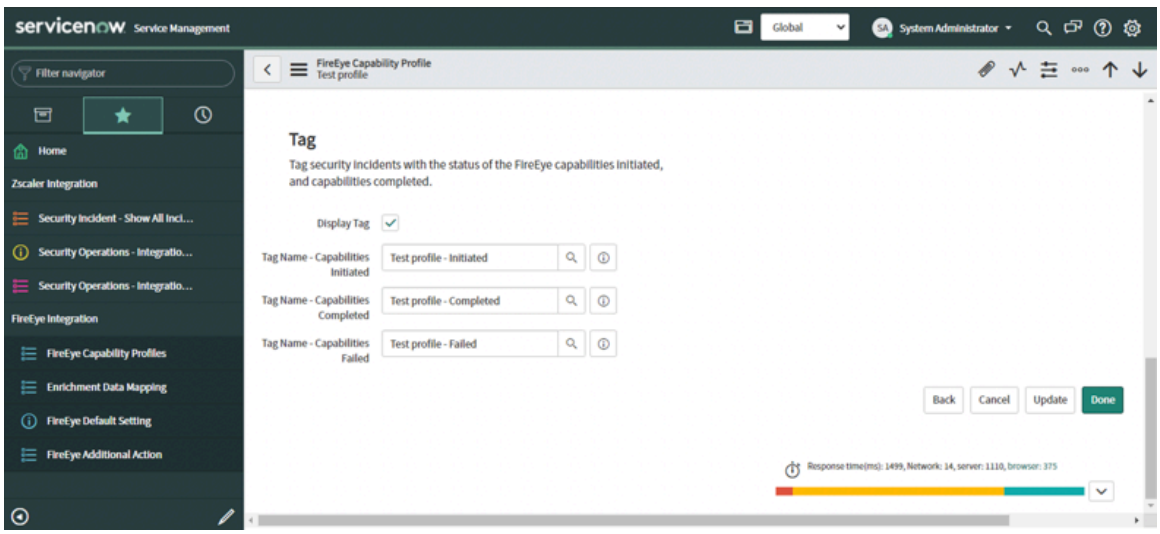
       Hinweis:
       Weitere Informationen finden Sie unter Verstehen, wie Auslöserbedingungen mit einem Configuration Item funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- **Tags**: Sie können Security Incidents optional mit den Tags FireEye HX Profil initiiert, Profil abgeschlossen und Profil fehlgeschlagen versehen.

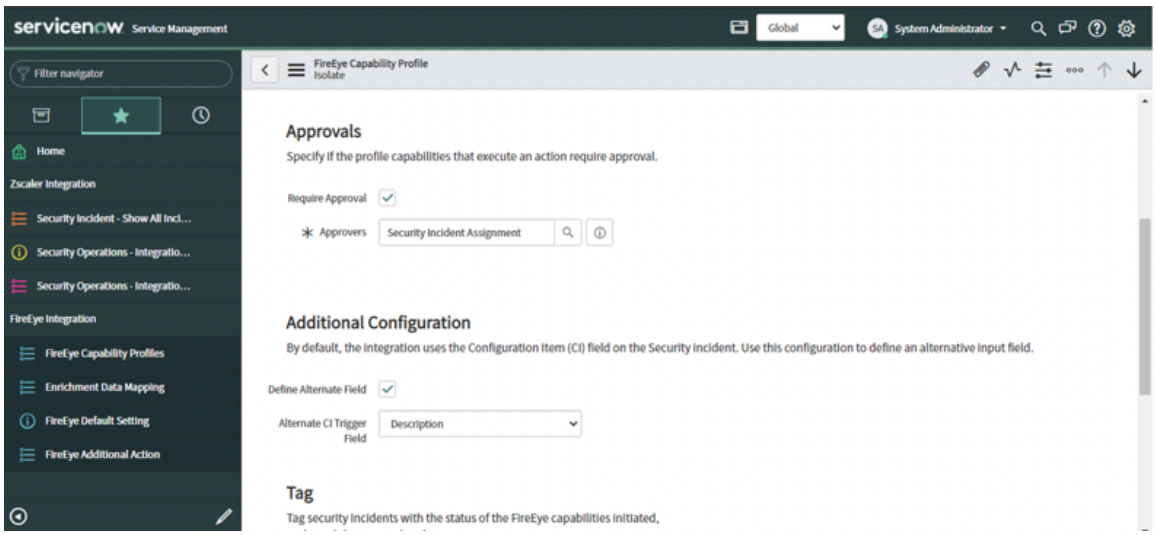
  Rufen Sie die Eigenschaft **Tag anzeigen** Aktivieren Sie das Kontrollkästchen, um das Tagging von Security Incidents zu aktivieren. Bei Aktivierung des Tags wird der Profilname vorangestellt. Standardmäßig ist diese Option für alle Profile deaktiviert.



- **Genehmigungen**: Wählen Sie aus **Genehmigung erforderlich** Kontrollkästchen, um eine zusätzliche Kontrollebene bereitzustellen, wenn die Fähigkeiten FireEye HX zum Isolieren von Hostcomputern, Wiederherstellen im Netzwerk und Abrufen der Dateien verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Option „Genehmigungen“ in der Profilkonfiguration wird nur für die Funktionen „Host isolieren“, „Hostisolierung entfernen“ und „Datei abrufen“ angezeigt.



4. Klicken Sie auf **Erledigt**.
5. Überprüfen Sie die Auslöserbedingungen FireEye HX.

Verifiziert die Auslöserbedingungsfilter

Testen Sie das Profil, und vergewissern Sie sich, dass die von Ihnen konfigurierten Auslöserbedingungsfilter wie erwartet funktionieren.

Vorbereitungen

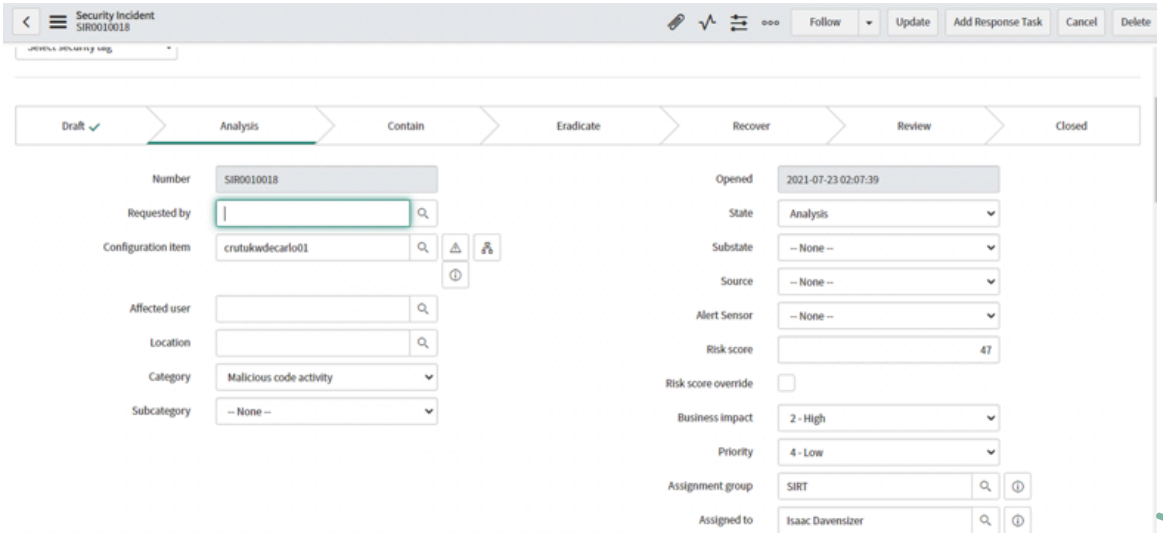
Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Sobald Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in den Now Platform -Security Incidents anzeigen.

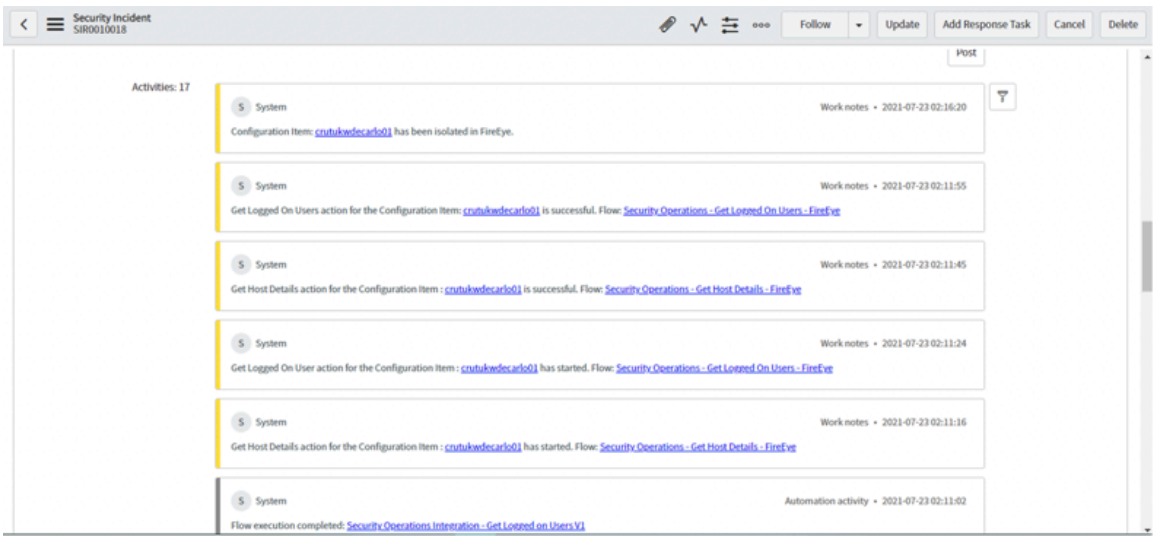
Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Auswahlvorgang **Neu** um einen neuen Security Incident zu erstellen.
3. Geben Sie die im Fähigkeitsprofil angegebenen Filterbedingungen an, um das jeweilige Profil auszulösen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken **Speichern**.

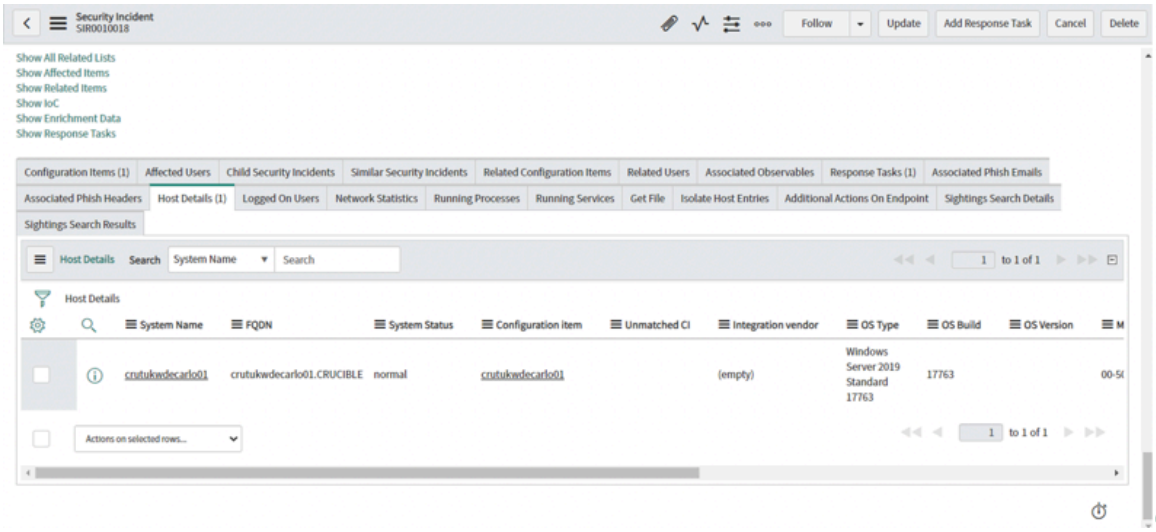


5. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
6. Zeigen Sie die Tags „Profil initiiert“, „Profil abgeschlossen“ oder „Profil fehlgeschlagen“ an.
7. Klicken **Alle zugehörigen Listen anzeigen**.
8. Klicken Sie auf eine beliebige zugehörige Liste (Registerkarte).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Hostdetails.



Löst ein FireEye-Fähigkeitsprofil über „Zugehörige Links“ aus

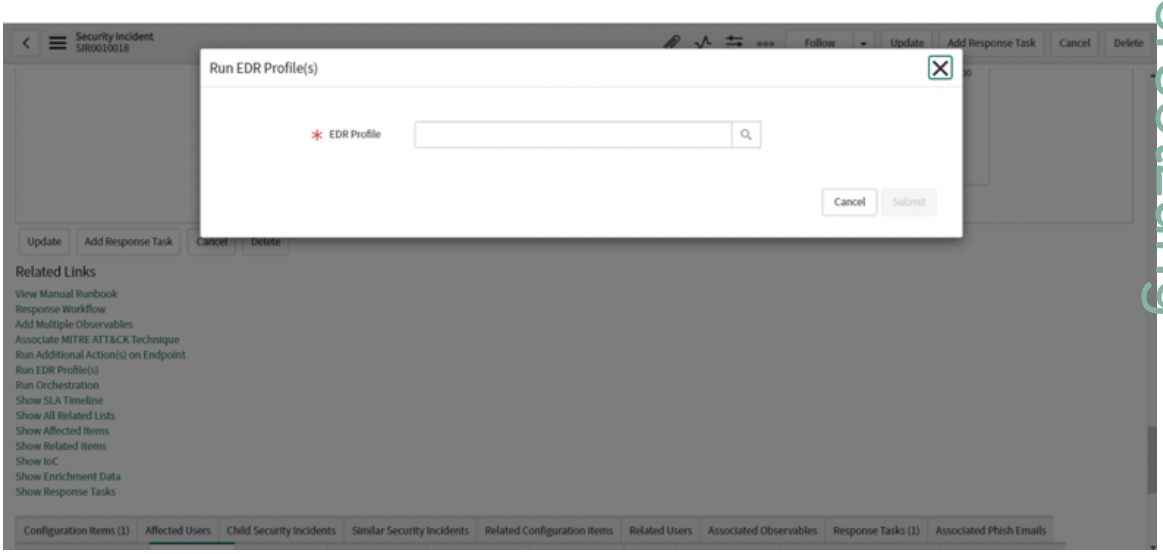
Lösen Sie ein Fähigkeitsprofil manuell aus, nachdem Sie einen Security Incident über zugehörige Links überprüft haben.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Prozedur

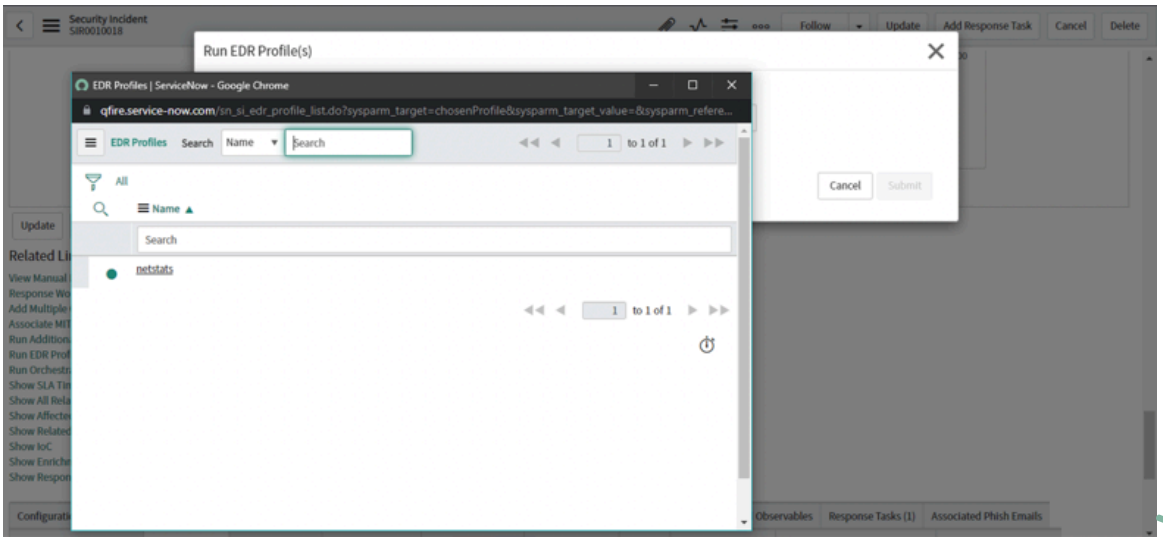
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie überprüfen möchten.
3. Klicken **EDR-Profil(e) ausführen**im Abschnitt „Zugehörige Links“.

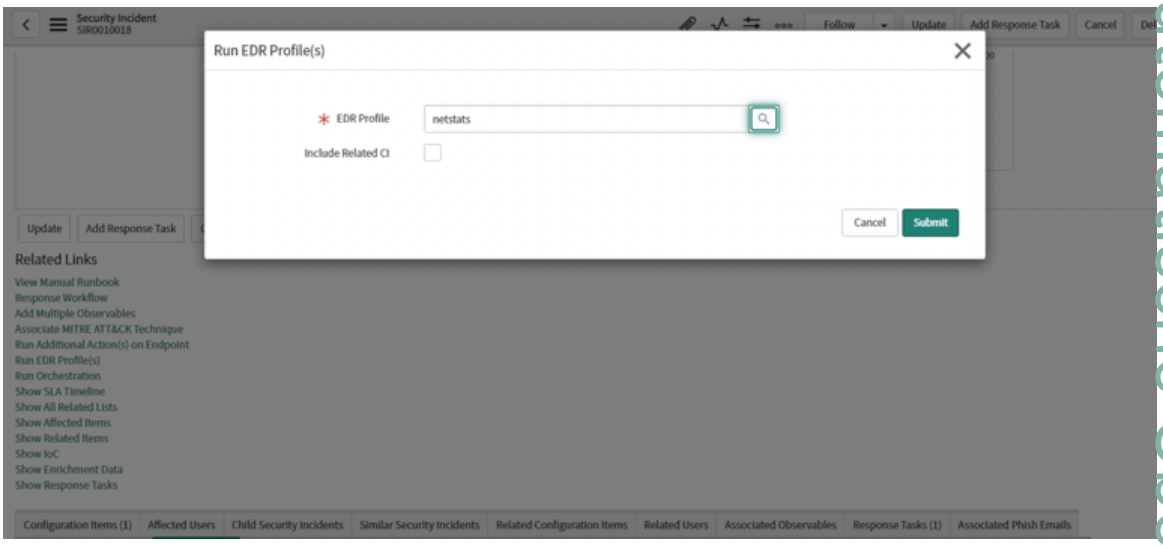


4. Suchen Sie, wählen Sie ein Profil aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





5. Das ausgewählte Profil wird manuell ausgelöst.
6. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
7. Zeigen Sie die Tags an, und überprüfen Sie die zugehörigen Listen auf die Daten.

Hinweis:
Zusätzlich zur Ausführung des Profils für das CI oder das alternative CI des Security Incident können Sie das Profil auch für CI-Werte ausführen, die in der zugehörigen Liste des Konfigurationselements vorhanden sind, indem Sie im Dialogfeld „Zugehöriges CI einbeziehen“ aktivieren. Dadurch werden auch Daten für die CI-Werte abgerufen, die in der zugehörigen Liste vorhanden sind. Alternativ können Sie das Profil nur für die CI-Werte ausführen, die in der zugehörigen Liste vorhanden sind.

Löst ein FireEye-Fähigkeitenprofil über die zugehörige Liste „Konfigurationselement“ aus

Lösen Sie ein Fähigkeitsprofil manuell über die zugehörige Liste des Konfigurationselements aus.

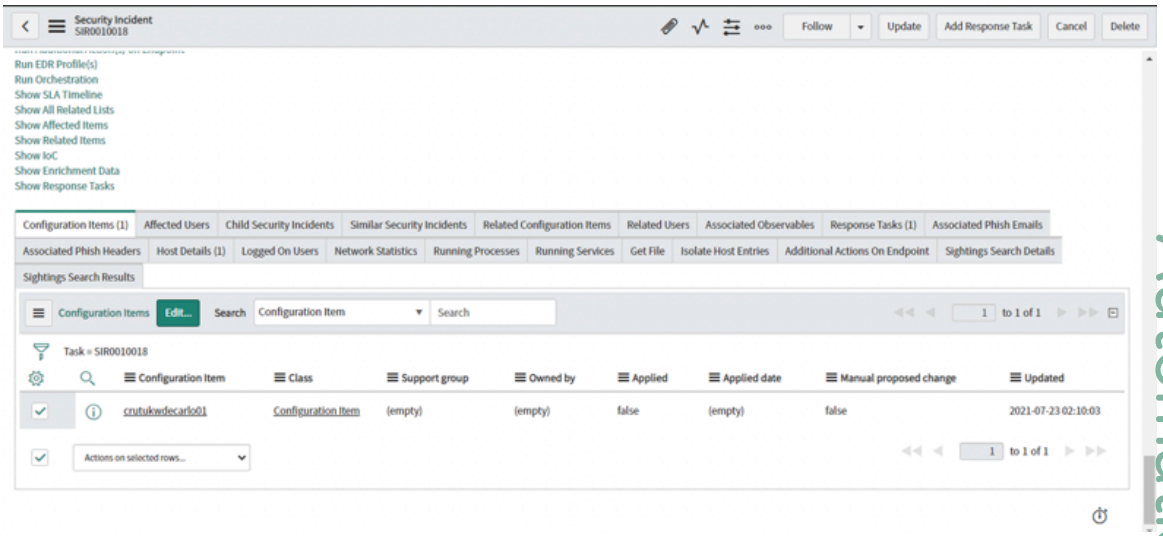
Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.analyst

Automatische Übersetzung

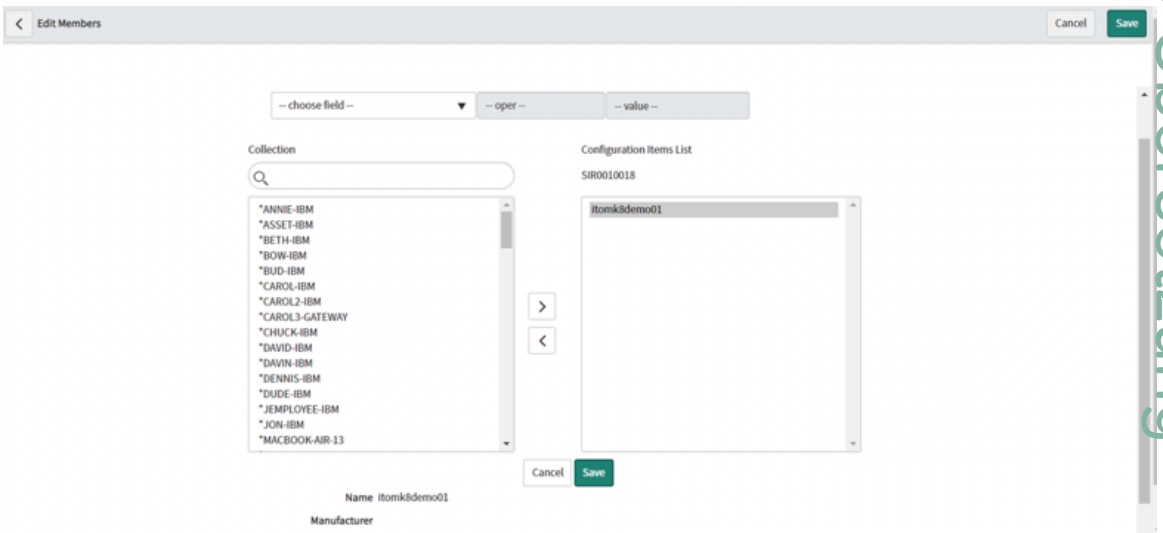
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen FireEye HX aus.
3. Klicken **Alle zugehörigen Listen anzeigen** im Abschnitt „Zugehörige Listen“ .
4. Klicken Sie auf die Schaltfläche **Konfigurationselement** Zugehörige Liste.



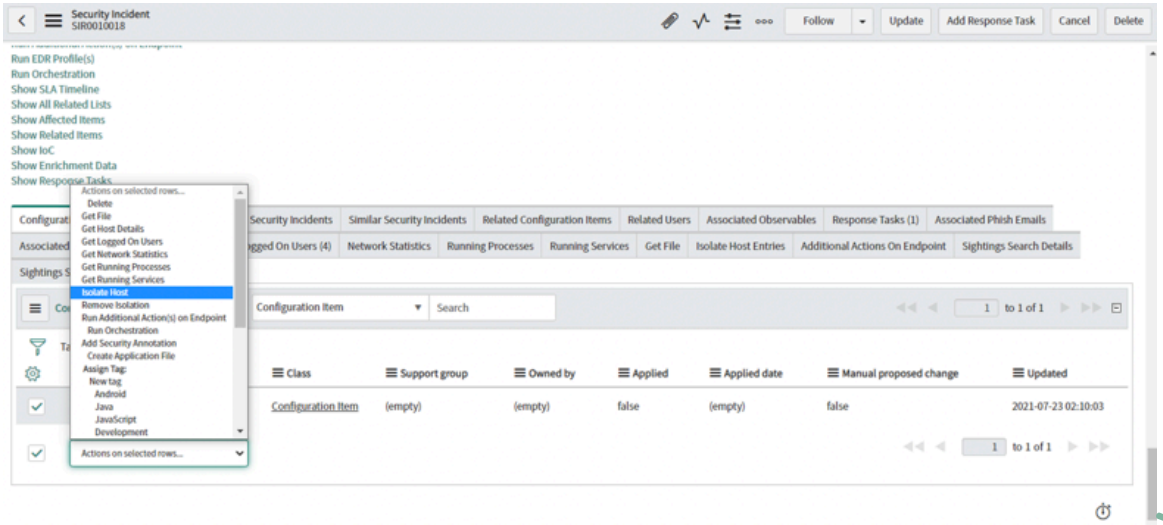
5. Klicken **Bearbeiten** um die verfügbaren Konfigurationselemente hinzuzufügen, wenn noch keine Werte vorhanden sind, und klicken Sie auf **Speichern**.



6. Wählen Sie die hinzugefügten Konfigurationselemente aus, und wählen Sie unter Aktionen für ausgewählte Zeilen eine Fähigkeit aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Die ausgewählte Fähigkeit wird manuell ausgelöst.
8. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
9. Zeigen Sie die Tags an, und überprüfen Sie die Daten in den zugehörigen Listen.

FireEye-Funktion zum Abrufen von Dateien

Dateierfassungsanforderungen weisen einen Endpoint Security Agent an, eine Datei von ihrem Hostendpunkt abzurufen. Dateierfassungen werden für die statische oder dynamische Analyse potenzieller oder verifizierter Kompromittierungen sowie für die Aufbewahrung von Nachweisen bei Untersuchungen interner Bedrohungen verwendet. Die Fähigkeit „Datei abrufen“ muss als separates Profil erstellt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Get File Profile auslösen und mit ein FireEye HX -Fähigkeitsprofil erstellen **Datei abrufen** Fähigkeit.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie überprüfen möchten.
3. Klicken **EDR-Profil(e) ausführen**im Abschnitt „Zugehörige Links“.
4. Durchsuchen und Dateiprofil abrufen aus der Liste der verfügbaren Profile auswählen.
5. Geben Sie an **Dateiname** und **Dateipfad**.

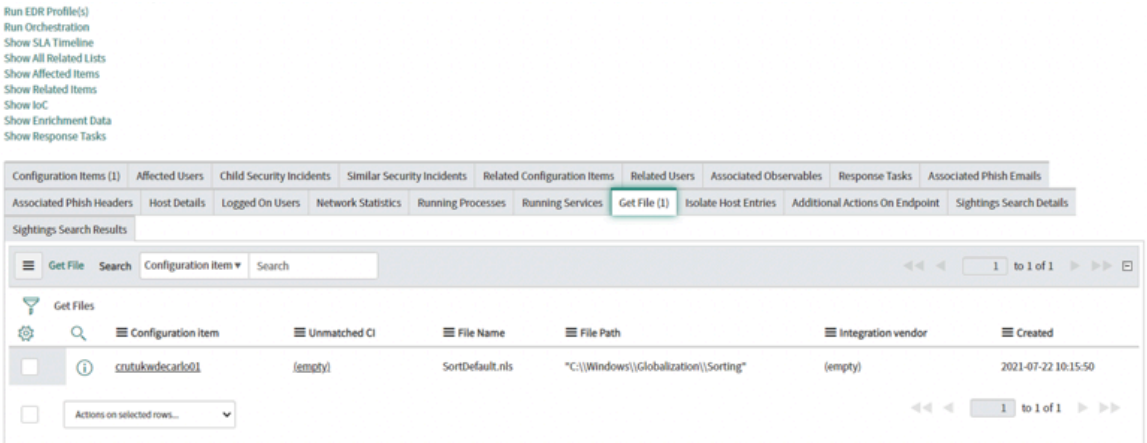
> **Hinweis:**
> Geben Sie den Namen der Datei ein, für die Sie abrufen möchten. Geben Sie einen genauen Pfadnamen oder eine andere geeignete pfadbasierte Windows-Umgebungsvariable an. Sie müssen den Laufwerksbuchstaben oder Pfadnamen angeben. Verschiedene Endpunkte können unterschiedliche Laufwerkszuordnungen haben. Wenn Sie explizit einen Ordnernamen angeben, können Sie den Pfad mit einem umgekehrten Schrägstrich beenden. Der abschließende umgekehrte Schrägstrich ist jedoch nicht obligatorisch.

6. Klicken **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
8. Zeigen Sie die Tags an, und überprüfen Sie die Ergebnisse im **Datei abrufen** Zugehörige Liste.

Hinweis:
Das Profil „Datei abrufen“ wird jetzt manuell ausgelöst.



So überprüfen Sie die Beschaffung einer heruntergeladenen Datei:

- Öffnen Sie die ZIP-Datei für die Dateierfassung.
- Geben Sie das zum Öffnen der Datei erforderliche Passwort ein. Das Passwort kann angezeigt werden, indem Sie den Mauszeiger über den Download-Link in FireEye HX der -Konsole bewegen. Führen Sie die folgenden Schritte aus, um das Passwort anzuzeigen:
  - Melden Sie sich bei der FireEye HX-Konsole an.
  - Navigieren zu **Akquisitionen** und filtern nach Beschaffungstyp – Datei.
  - Wählen Sie den gewünschten Datensatz aus.

    Hinweis:
    Auf der rechten Registerkarte werden die Details der erfassten Datei angezeigt.

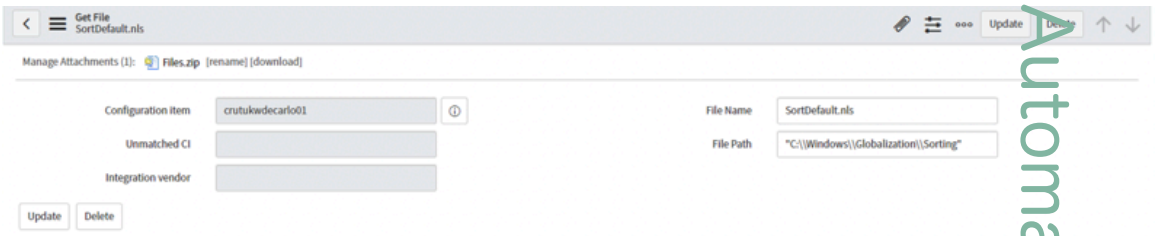
  - Bewegen Sie den Mauszeiger über **Herunterladen** Link oben zum Abrufen des Passworts verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

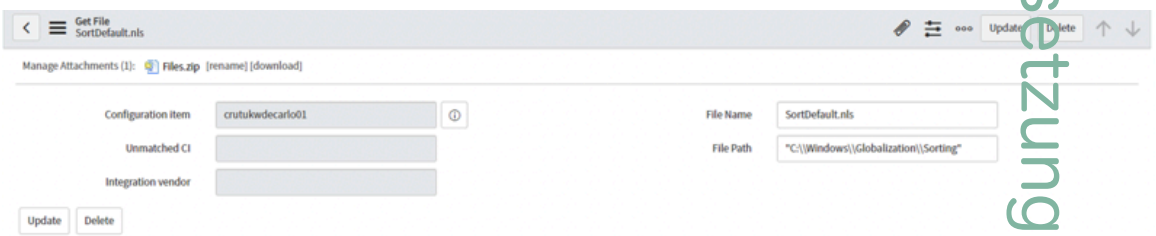
- Öffnen und überprüfen Sie die Dateien in der ZIP-Datei mit einem beliebigen Text- oder XML-Editor.

Hinweis:

- Es wird empfohlen, die abgerufene Datei manuell als erkennbares Element hinzuzufügen, damit sie als Beweis für den Security Incident nachverfolgt werden kann. Dies hilft auch, die Dateien in Zukunft anzuzeigen, wenn das Passwort vergessen oder geändert wird.
- Die maximale Dateigröße, die für die Aktion Datei abrufen unterstützt wird, beträgt 1024 MB, und dieser Wert kann durch Ändern von konfiguriert werden **com.glide.attachment.max_size**, und die standardmäßige Zeitüberschreitung beträgt 60 Minuten und kann auf der Seite FireEye HX Standardeinstellungen konfiguriert werden.



- Das Abrufen der Datei kann auch über die zugehörige Liste des Konfigurationselements ausgelöst werden.



Automatische Übersetzung

Zusätzliche FireEye-Aktionen für Endpunkt

Die FireEye-Integration unterstützt die Ausführung zusätzlicher Aktionen, die über die Goldstandardaktionen hinausgehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Aktionen umfassen Selektierungserfassung und Datenerfassung. Standardmäßig werden zwei Datenerfassungen unterstützt:

- Skript für umfassende Untersuchungsdetails
- Standardskript für Untersuchungsdetails

Darüber hinaus wird auch die Selektierungsakquise standardmäßig unterstützt. Alle diese drei werden standardmäßig zusammen mit der Quelle erstellt. Kunden können auch eigene Aktionen erstellen, z. B. Datenerfassungen aus dem FireEye-Modul „Zusätzliche Aktionen“.[1] Die maximale Dateigröße, die für zusätzliche FireEye-Aktionen unterstützt wird, beträgt 1024. Dieser Wert kann durch Ändern von konfiguriert werden **com.glide.attachment.max_size**, und die standardmäßige Zeitüberschreitung beträgt 120 Minuten und kann auf der Seite „FireEye-Standardeinstellungen“ konfiguriert werden.

Skript für umfassende Untersuchungsdetails

Ermöglicht das Sammeln aller forensischen und untersuchenden Artefakte vom Endpunkt, ist jedoch die teuerste Option. Diese Konfiguration ist ideal für Situationen, in denen nur ein Fenster zum Sammeln von Daten vom betreffenden Endpunkt vorhanden ist und die Möglichkeit zum Erfassen weiterer Daten später nicht garantiert werden kann. Verwenden Sie diese Aktion daher mit Vorsicht.

Standardskript für Untersuchungsdetails

Aktiviert die gängigsten Optionen zum Sammeln von forensischen und untersuchenden Artefakten von einem Endpunkt. Dient als primäres Reaktionstool, wenn Sie den Verdacht haben, dass ein Endpunkt gefährdet ist, und eine eingehende Analyse dieses Endpunkts durchführen müssen. Ziel ist es, ein Gleichgewicht zwischen der Erfassung der relevantesten und wertvollsten Daten und der Vermeidung kostspieliger Optionen zu finden, die später erfasst werden können, wenn weitere Untersuchungen sie als erforderlich erweisen.

Selektierung – Akquisition

Selektierungssammlungen enthalten Informationen aus dem Rückblick-Cache sowie zusätzliche forensische Audit-Informationen, z. B. URL-Downloadverlauf, Dateidownloadverlauf, Prozess- und Portlisten sowie Standardsysteminformationen. Möglicherweise möchten Sie diese Informationen überprüfen, wenn anomaler Netzwerkverkehr erkannt wird und Sie mehr Transparenz in Endpunktaktionen wünschen.

Datenerfassungsskripts in FireEye verwalten

Mit Datenanforderungen für die Erfassung (manchmal auch als Live-Antwortanforderungen bezeichnet) können Sie alle benötigten Daten von einem einzelnen laufenden Endpunkt abrufen. Auf der Seite „Datenerfassungsskripts“ in FireEye können Sie die für Datenerfassungsanforderungen verwendeten Datenerfassungsskripts erstellen, bearbeiten, kopieren und löschen.

Zugriff auf die Seite „Datenerfassungsskripts“ in FireEye

So greifen Sie auf die Seite „Datenerfassungsskripts“ zu:

1. Navigieren Sie zu Endpunktsicherheit Webbenutzeroberfläche.
2. Wählen Sie im Menü Administrator die Option Datenerfassungsskripts aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen eines Skripts in FireEye

So erstellen Sie ein Datenerfassungsskript:

1. Auswahlvorgang **Datenerfassungsskripts** > **Administrator** Menü der Endpoint Security-Webbenutzeroberfläche.
2. Klicken **Skript erstellen**.
3. Geben Sie einen Namen für das neue Skript in ein **Skriptname** an.
4. Geben Sie optional eine Beschreibung des Skripts ein.
5. Wählen Sie das Betriebssystem aus, für das das Skript gilt. Sie können im Dialogfeld „Skript erstellen“ nur ein einzelnes Betriebssystem auswählen.
6. Klicken **Erstellen** um die Skriptdefinition zu starten.
7. Wählen Sie in einen Beschaffungsdatentyp aus **Fügen Sie einen Beschaffungstyp hinzu**Dropdown-Feld und klicken Sie auf **Hinzufügen**. Optionen für den angeforderten Beschaffungstyp werden rechts neben der Skriptliste angezeigt.
8. Geben Sie Werte für die Beschaffungstypoptionen an, oder verwenden Sie die bereits ausgewählten Standardwerte. Die Web-UI warnt Sie nicht und entfernt auch keine Tabulatoren, Leerzeichen oder unerwünschte Zeichen (z. B. \n) in Ihren Spezifikationen.
9. Wiederholen Sie die vorherigen beiden Schritte, um zusätzliche Daten für das Datenerfassungsskript anzufordern. Einige Beschaffungsdatentypen sind nur einmal für ein Skript verfügbar, während andere mehrmals angegeben werden können. Nach dem Hinzufügen eines Beschaffungstyps zu einem Skript wird die Liste der im verfügbaren Beschaffungstypen angezeigt **Fügen Sie einen Beschaffungstyp hinzu**Dropdown-Feld wird entsprechend angepasst.
10. Um einen Beschaffungsdatentyp aus dem Skript zu entfernen, klicken Sie auf das x-Symbol ( ) auf der Registerkarte „Beschaffung“ auf der linken Seite der Seite.

Hinweis:
Diese Integration unterstützt nicht **Bearbeitungen vor Erwerb zulassen** Option beim Erstellen von Skripts. Stellen Sie daher sicher, dass das Kontrollkästchen deaktiviert ist.

Es wird ein Skript aus FireEye exportiert

Sie können ein Datenerfassungsskript in eine JSON-Datei exportieren. So exportieren Sie ein Datenerfassungsskript:

1. Auswahlvorgang **Datenerfassungsskripts** > **Administrator** der Endpoint Security-Webbenutzeroberfläche.
2. Wählen Sie im Menü Administrator die Option Datenerfassungsskripts aus.
3. Wählen Sie links auf der Seite das Skript aus, das Sie exportieren möchten.
4. auswählen **Aktionen** > **Skript exportieren**.
5. Eine JSON-Datei wird auf Ihren Computer heruntergeladen. Der JSON-Dateiname enthält das Betriebssystem, sodass Sie leicht bestimmen können, welche Skripts für welches Betriebssystem geeignet sind.

Es wird eine neue Datenerfassungsaktion auf der Now Platform erstellt

Um eine neue Aktion zu erstellen, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **FireEye-Integration** > **FireEye: zusätzliche Aktionen**. Die Liste Zusätzliche FireEye-Aktionen wird angezeigt.
2. Klicken **Neu**. Das Formular für die neue Aktion wird angezeigt.
3. Füllen Sie das Formular aus.

Aktionsname	Name der ausgeführten FireEye-Aktion Dieser Name hilft Ihnen, den Aktionstyp zu identifizieren und zu beschreiben.
Akquisition	Eine Akquisition ruft die zu analysierenden Daten ab. Dies ist ein schreibgeschütztes Feld und standardmäßig auf „Datenerfassung“ eingestellt.
Quelle	Name der FireEye-Quelle. In der Auswahlliste sind nur konfigurierte Quellen verfügbar.
Fähigkeit	Dies ist ein schreibgeschütztes Feld und wird mit der Fähigkeit „Zusätzliche Aktion(en) ausführen“ ausgefüllt
Akquisitionstyp	Typ der Beschaffungsaktion, die abgerufen und analysiert werden muss.
Aktiv	Dies zeigt an, dass die Aktion aktiv ist.
Genehmigung erforderlich	Wenn Sie die Option Genehmigung erforderlich aktivieren, ist das Feld Genehmiger im Formular verfügbar. Nachdem Sie eine Anforderung übermittelt haben, ist zum Abschließen der Anforderung eine Genehmigung durch die Gruppe erforderlich.
Tag anzeigen	Typ des Betriebssystems, z. B. Windows, Mac, Linux zum Hinzufügen von Skripts. **Hinweis:** Derzeit wird nur ein Betriebssystemtyp unterstützt. Sie können eine Aktion pro Betriebssystem erstellen. Erstellen Sie für andere Betriebssysteme nach Bedarf neue Aktionen.
Skripte	Das aus FireEye importierte Skript muss für den ausgewählten Betriebssystemtyp angegeben werden. Jedem Betriebssystemtyp kann nur ein Skript hinzugefügt werden.

4. Klicken **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerfassungen aus Security Incident auslösen

Die erstellten zusätzlichen Aktionen können über den aufgerufenen zugehörigen Link ausgeführt werden **Zusätzliche Aktion(en) für Endpunkt ausführen** über den Security Incident.

Hinweis:
Bearbeitungen vor Erwerb zulassen Die FireEye-Funktion wird für die zusätzlichen Aktionen für den Endpunkt nicht unterstützt.

Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche mit der FireEye-Integration

Konfigurieren Sie das Sichtungssuchprofil mit dem folgenden Verfahren.

Vorbereitungen
Erforderliche Rolle: Now Platform Security Incident Administrator (sn_si. admin)

Wenn eine Quelle erstellt wird, werden individuelle Sichtungssuchkonfigurationen für fünf Typen (Datei, IPs (v4), MD5, SHA1 und SHA256) erstellt und standardmäßig deaktiviert. Sie sollten die Option aktivieren, bevor Sie die Sichtungssuche verwenden. Jeder erkennbare Elementtyp hat eine andere Suchabfrage, um Sichtungen abzurufen. Wir würden für jeden erkennbaren Elementtyp eine andere Suche initiieren. Die Suche nach mehreren erkennbaren Elementen für eine Sichtungssuche ist in FireEye nicht möglich, da dies eine UND-Operation für die erkennbaren Elemente ausführen würde und das Ergebnis möglicherweise ungenau ist.

Hinweis:
Für die Sichtungssuche können nur fünf aktive Suchen gleichzeitig vorhanden sein. Die verbleibenden werden in die Warteschlange gestellt und beginnen nach Abschluss einer der laufenden Sichtungen.

Wenn Sie ein neues Sichtungssuchprofil erstellen möchten, führen Sie die folgenden Schritte aus, um eines zu erstellen:

Prozedur

1. Navigieren zu **Integrationen** > **Sichtungssuche – Konfiguration**.
2. Klicken **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Name des Fähigkeitsprofils.
Ist gespeicherte Suche	Dadurch wird eine gespeicherte Suche ausgeführt, d. h. das Feld „Name“ muss mit dem Namen der gespeicherten Suche übereinstimmen.
Sichtungssuchquelle	Definiert die für die Integration konfigurierte Quelle.
Suchen	Fügen Sie eine native Suchzeichenfolge hinzu, um eine Abfrage zu bilden.
Aktiv	Abfrage wird nur ausgeführt, wenn sie aktiv ist.
Erkennbarer Typ	Definiert den Typ der Kategorie des erkennbaren Elements.
Maximale erkennbare Elemente pro Suche	Die Anzahl der erkennbaren Elemente bevor die Suchabfrage in mehrere Abfragen aufgeteilt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Legen Sie diesen Wert für diese Integration auf 1 fest.
Sichtungssuchparameter	Verwenden Sie Sichtungssuchparameter, um komplexere Abfragen zu definieren, die Logik und andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden.

4. Klicken **Absenden** um die Konfiguration abzuschließen.

Ruft die Sichtungssuche aus einem Security Incident auf

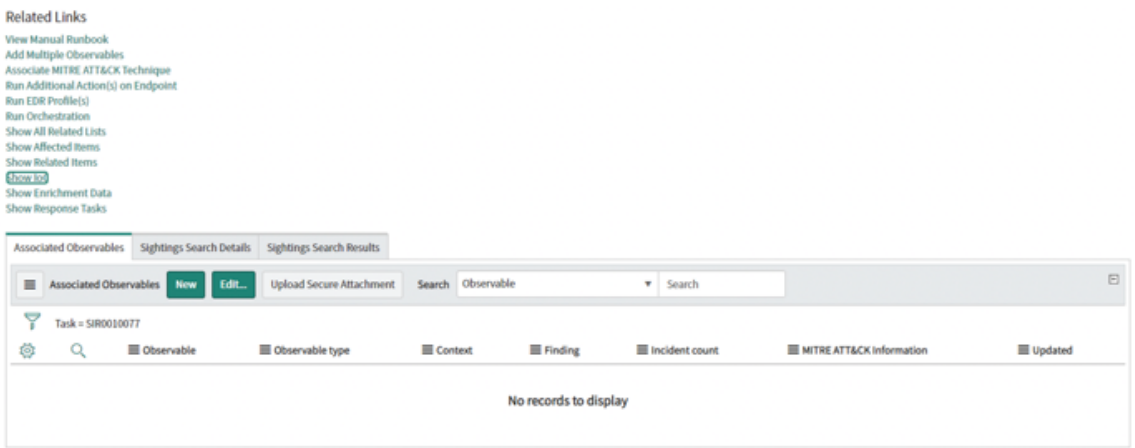
Rufen Sie die Sichtungssuche aus einem SIR-Security Incident auf, indem Sie das folgende Verfahren ausführen.

Vorbereitungen

Erforderliche Rolle: Now Platform Administrator (sn_si.admin)

Prozedur

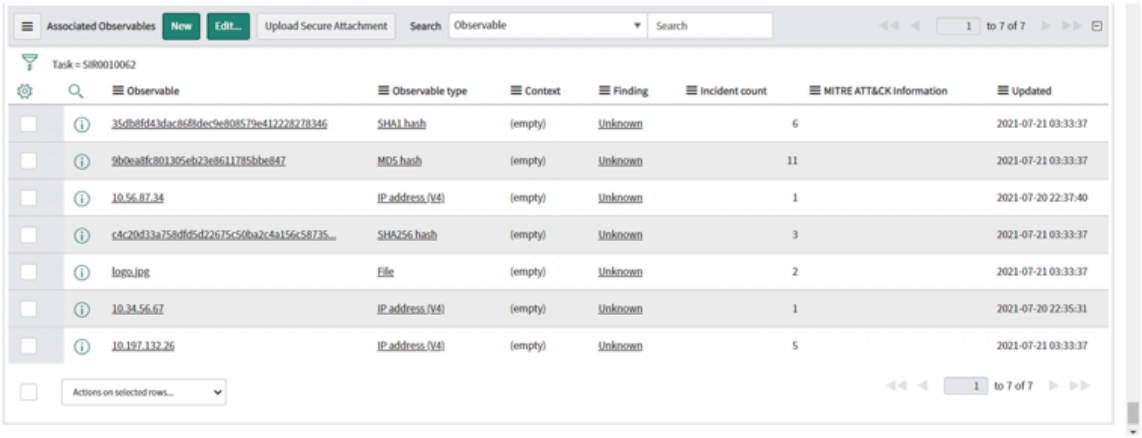
1. Navigieren Sie zu Security Incidents.
2. Öffnen Sie einen vorhandenen SIR, oder erstellen Sie einen neuen SIR.
3. Klicken Sie auf IoC in zugehörigen Links anzeigen.
4. Klicken **Zugehörige erkennbare Elemente** zugehörige Listen.



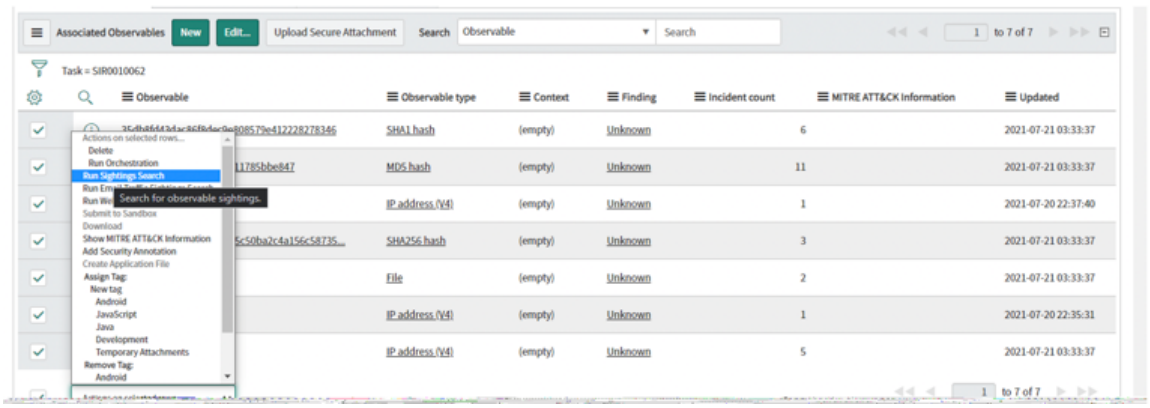
5. Fügen Sie vorhandene erkennbare Elemente hinzu, oder erstellen Sie ein neues erkennbares Element.

Automatische Übersetzung

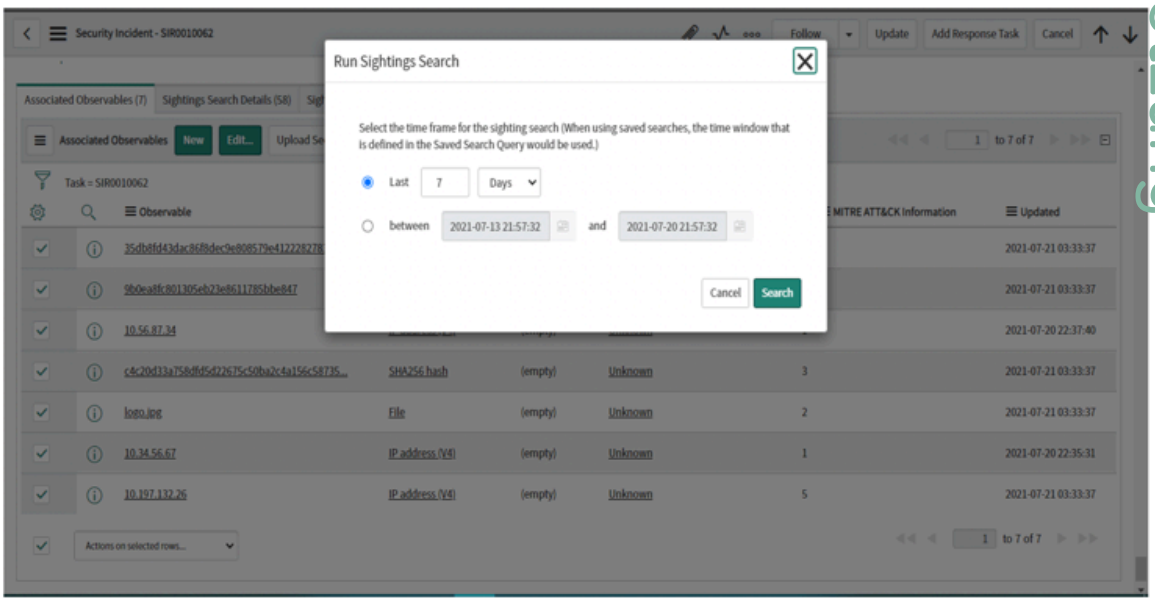
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie die erkennbaren Elemente aus, und klicken Sie unter Aktionen für ausgewählte Zeilen auf **Sichtungssuche ausführen**.



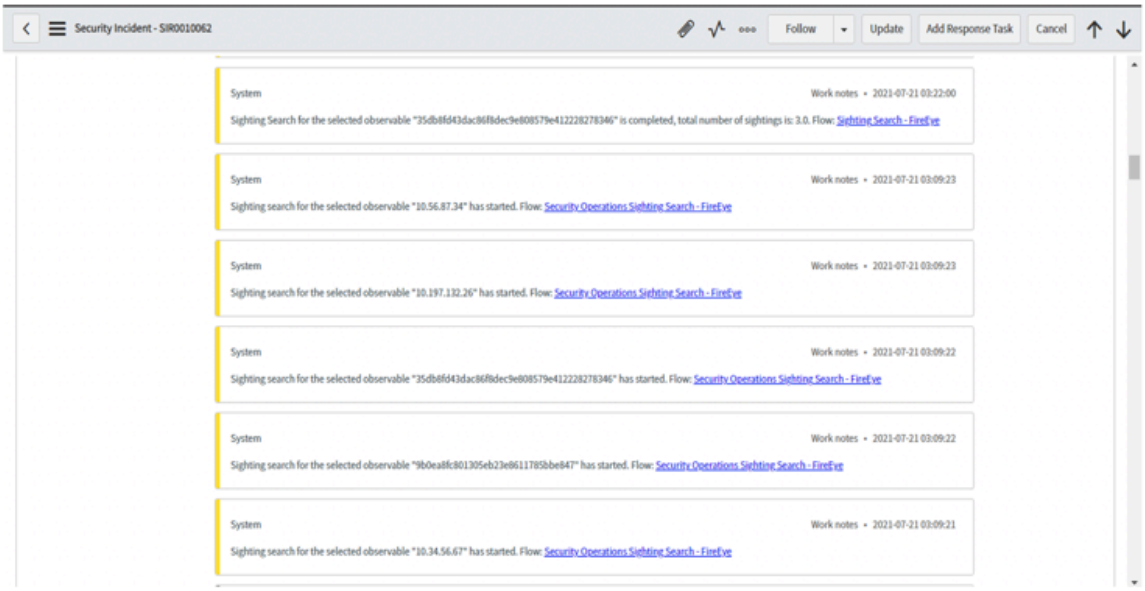
7. Ignorieren Sie die Eingaben im nächsten Dialogfeld, in dem Sie nach Zeitdaten gefragt werden.
Es sind Standardwerte ausgefüllt. Die Suche wird jedoch in Echtzeit durchgeführt, und die Zeitwerte werden für diese Integration ignoriert.



8. Überprüfen Sie den Status in den Arbeitsnotizen.

Automatische Übersetzung

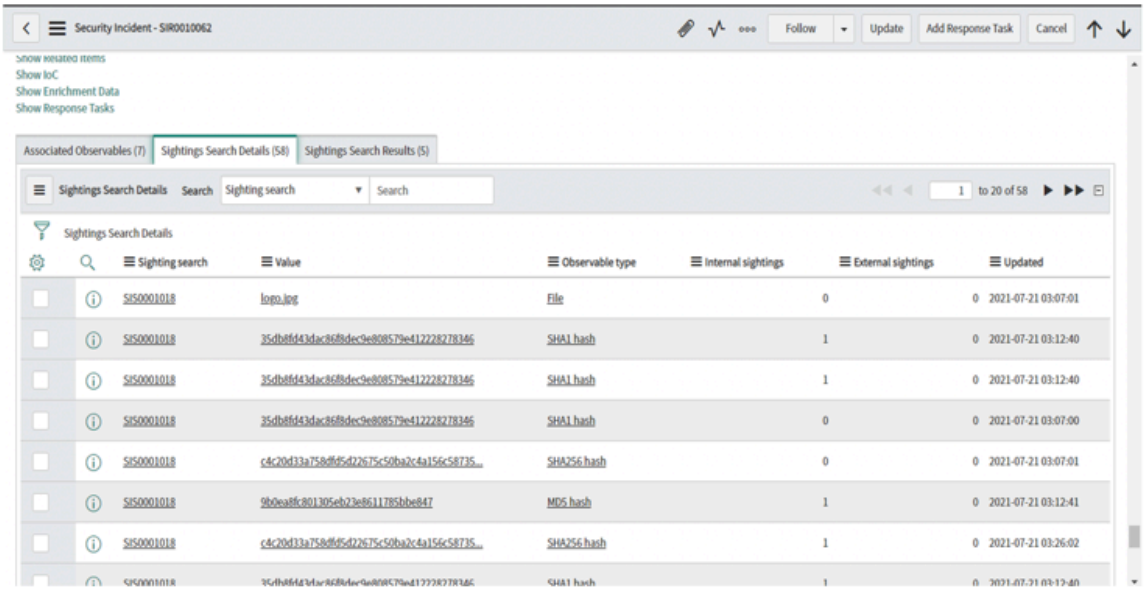
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

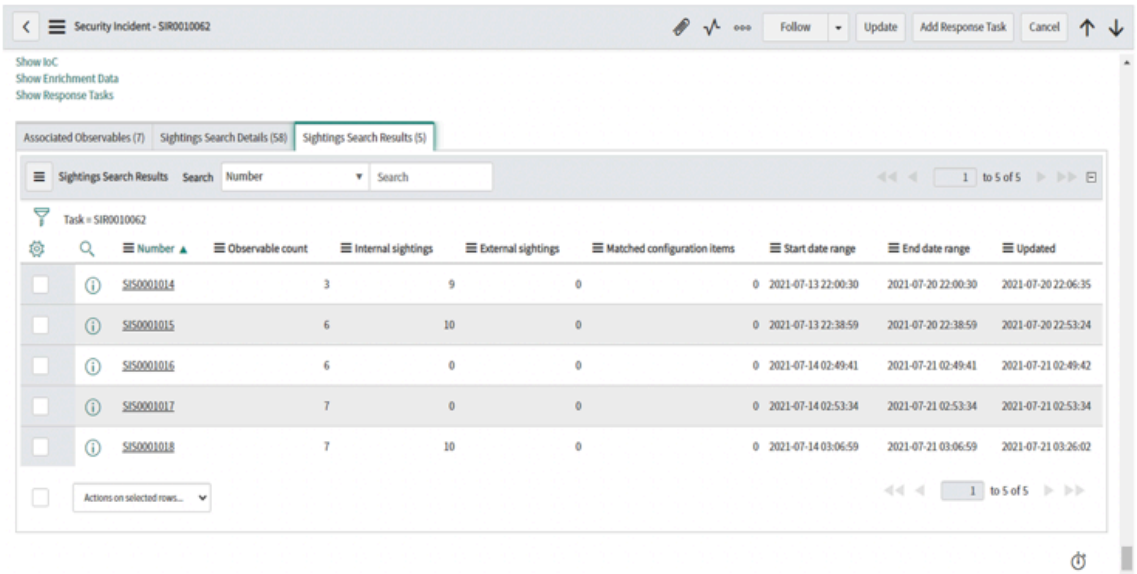


9. Überprüfen Sie nach Abschluss der Suche die Ergebnisse und Details in den zugehörigen Listen.
10. Klicken Sie auf **Details einer Sichtungssuche** Registerkarte für Details und **Ergebnisse der Sichtungssuche** Registerkarte für Suchergebnisse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





Automatische Übersetzung

Have I Been Pwned? Integration

Mit der Security Operations Have I Been Pwned? -Integration können Sie Suchvorgänge für Domänennamen und E-Mail-Adressen übermitteln, um festzustellen, ob die persönlichen Daten des Anwenders durch Datenschutzverletzungen gefährdet wurden.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Integrationssetup für Security Operations Have I Been Pwned? .
- Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? .

Verwenden

Entwickeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Führen Sie Suchen für erkennbare Elemente durch Bedrohungssuche – Flow Have I Been Pwned?.

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Integrationssetup für Security Operations Have I Been Pwned? .

Have I Been Pwned? ist eine kostenlose Ressource, mit der bewertet werden kann, ob jemand gefährdet wurde, weil sein Online-Konto bei einer Datenschutzverletzung gefährdet oder „pwned“ wurde. Es lässt sich problemlos in Security Operationsintegrieren.

Bevor Sie die -Integration Have I Been Pwned? verwenden können, müssen Sie das Plugin aktivieren. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Die Plugins Security Incident Response, Threat Intelligenceund Security Operations Have I Been Pwned? sind erforderlich, um die Integration Security Operations Have I Been Pwned? zu implementieren.

Bedrohungssuche – Flow Have I Been Pwned?.

Der Flow „Bedrohungssuche – Have I Been Pwned? “ führt eine Suche für ausgewählte erkennbare Elemente durch. Wenn es sich bei den erkennbaren Elementen um einen von Have I Been Pwned?erkannten Typ handelt, werden sie auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Erforderliche Rolle: sn_si_admin

Dieser Flow wird von Security Operations-Integration – Funktionalität zur Bedrohungssuche ausgelöst, wenn Sie eine Bedrohungssuche für mindestens ein erkennbares Element durchführen und die Implementierung Have I Been Pwned? ausgewählt ist. Weitere Informationen finden Sie unter Führen Sie Suchen für erkennbare Elemente durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wurde ich pwned Flow

Informationen zu den von diesem Flow verwendeten Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? .

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der Security Operations Have I Been Pwned? -Integration, schnell aktivieren und einrichten. Bevor Sie die Have I Been Pwned? -Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

Vorbereitungen

- Das Plugin Threat Intelligence muss installiert und aktiviert werden, bevor Sie die Security Operations Have I Been Pwned? -Integration verwenden können.

Erforderliche Rolle: sn_si_admin

Prozedur

Laden Sie die -Integration aus dem herunter ServiceNow Store.
Diese Integration unterstützt eine offene API und erfordert keine weitere Konfiguration. Have I Been Pwned? kann jetzt für die Suche nach erkennbaren Elementen in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

Zugehörige Informationen

Führen Sie Suchen für erkennbare Elemente durch

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Fälle, in denen das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erwerben Sie das SSL-Zertifikat von einem Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) wie folgt von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie auf **Weitere Informationen** und anschließend auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen** und anschließend auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Export**, um die PEM-Datei in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu** und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn ein Zertifikat abgelaufen ist, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .

HPE Security ArcSight ESM – Integration mit E-Mail-Parser

Die Integration „HPE Security ArcSight ESM – Email Parser“ wird durch die Verwendung eines E-Mail-Parsers unterstützt, der E-Mail-Benachrichtigungen von ESM verarbeitet, um Security Incidents zu erstellen.

Konfigurieren Sie die Integration von HPE Security ArcSight ESM – E-Mail Parser

Die Integration „HPE Security ArcSight ESM – Email Parser“ verwendet E-Mail-Benachrichtigungen von ESM, um Ergänzungs- und Antwort-Workflows zu unterstützen.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

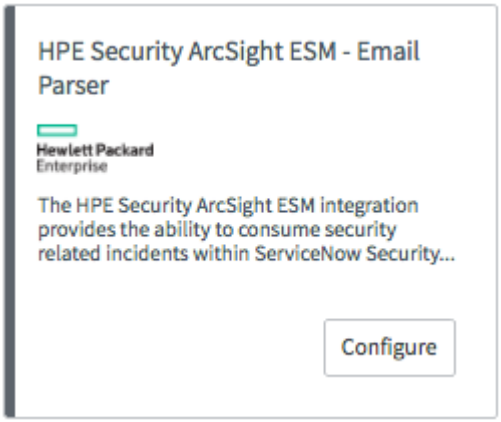
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Zur Verwendung für die Integration wird die Vorlage „HPE Security ArcSight ESM – Email Parser“ bereitgestellt. Es muss konfiguriert und aktiviert werden, bevor die Integration stattfindet. Durch das Aktualisieren des Parsers wird er aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.



2. Klicken Sie auf der Karte HPE Security ArcSight ESM – E-Mail Parser auf **Konfigurieren**.
3. Klicken Sie im Dialogfeld **„HPE Security ArcSight ESM – E-Mail-Parser-Konfiguration“** auf den Link **E-Mail-Parser konfigurieren**.
4. Klicken Sie auf den Link **ArcSight ESM,** um die Einstellungen im bereitgestellten Parser für E-Mail-Vorlagen zu bearbeiten.
   Füllen Sie mindestens das Feld E-Mail ist von aus. Informationen zum Erstellen eines eigenen E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**.
6. Klicken Sie im Formular **„E-Mail-Parser“auf Aktualisieren**.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu **Integrationskonfigurationen**zurückkehren.

HPE ArcSight Logger Integration mit der Ergänzung von Incidents

Die Integration HPE ArcSight Logger – Incident Enrichment durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Erste Schritte mit der Integration HPE ArcSight Logger - Incident Enrichment
- Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

---

Verwenden

Entwickeln

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Führen Sie eine Sichtungssuche aus
- Security Operations Integration - Sichtungssuche-Flow
- Security Operations: Sichtungssuch-Flow für Arcsight Logger
- Zeigen Sie Details der Sichtungssuche an
- Sichtungssuchergebnisse anzeigen
- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der Integration HPE ArcSight Logger - Incident Enrichment

HPE ArcSight Logger streamt Echtzeitdaten, kategorisiert sie in bestimmten Protokollen und lässt sich problemlos in Security Operationsintegrieren. Bevor Sie die Integration HPE ArcSight Logger - Incident Enrichment verwenden können, müssen Sie sie von ServiceNow Store herunterladen und die API-URL sowie Anmeldeinformationen hinzufügen.

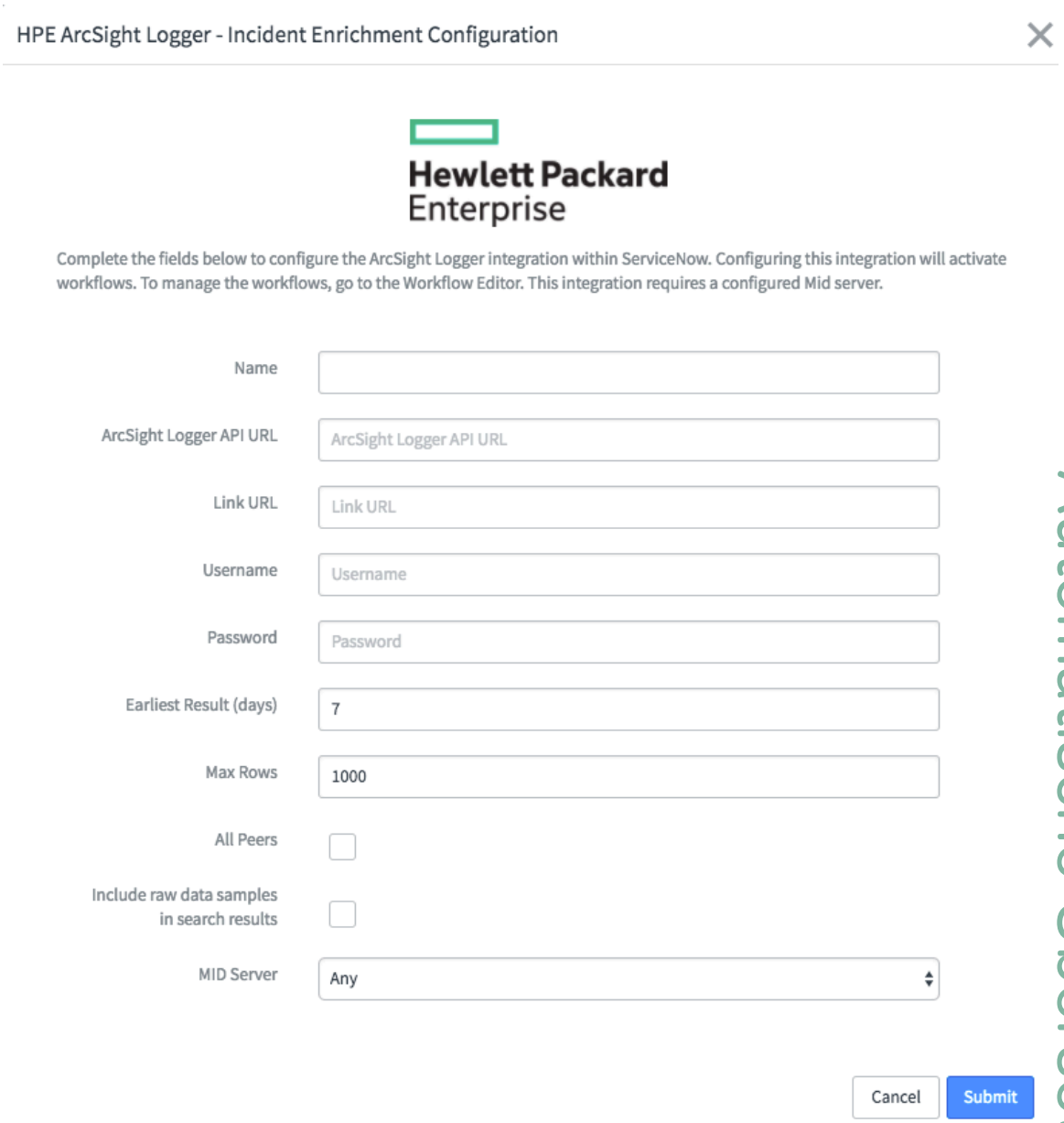
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte HPE ArcSight Logger – Incident-Ergänzung **auf Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

4. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der ArcSight Logger-API	Die Basis-URL, die Sie von der HPE Security ArcSight Logger-Website erhalten haben.
Link-URL	[Optional] Die Link-URL, die eine Verknüpfung zu einer HPE Security ArcSight Logger-Instanz herstellt, falls verfügbar.
Anwendername	Ihr Intel-Anwendername HPE ArcSight Logger.
Passwort	Ihr Intel-Passwort HPE ArcSight Logger.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Alle Peers	Standardmäßig ist diese Option deaktiviert und durchsucht nur die lokale Protokollierung, mit der Sie verbunden sind. Wenn diese Option aktiviert ist, werden alle Protokollierungen durchsucht, die miteinander verbunden sind.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der **Anzahl der Zeilen der Rohdateneigenschaft** in den Security Incident Response-Eigenschaftenab.
MID-Server	Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

5. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern bzw. zu löschen.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

Hybrid-Analyse Integration

Die Anwendung Hybrid-Analyse ist Teil einer offenen Online-Community, in der Anwender Dateien und URLs auf Bedrohungen analysieren. Sie teilen Ergebnisse und nutzen Forschungsergebnisse aus der Community, um effektiver auf Incidents reagieren zu können. Bei Integration mit dem -Produkt Now Platform Security Operations erhalten Sie durch gemeinsam genutzte Bedrohungsinformationen zusätzliche Einblicke in den Schweregrad bestimmter erkennbarer Elemente.

Die Hybrid-Analyse -Integration führt Bedrohungssuchen für die folgenden erkennbaren Elemente durch:

- Datei-Hashes
- IP-Adressen
- URLs

Der Flow sucht nach neuen erkennbaren Elementen, sobald sie in Security Incidents eingehen. Wenn die erkennbaren Elemente von einem Typ sind, der von der API-Integration erkannt wird, werden die erkennbaren Elemente ausgewertet. Als schädlich erkannte erkennbare Elemente werden getaggt.

Hybrid-Analyse installieren und konfigurieren

Bevor Sie die Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit die Anwendung Hybrid-Analyse ordnungsgemäß in Now Platform Security Operationsintegriert werden kann.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen haben.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der -Administrator (admin) installiert die App und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf das Modul Security Operations und weist die Rolle sn_si.analyst zu.
Rufen Sie einen API-Schlüssel ab.	Besuchen Sie die Hybrid-Analyse -Website, um Informationen zu API-Schlüsseln zu erhalten und ein Konto zu erstellen: Hybrid-Analyse-Website . Die Konfiguration erfordert die Eingabe der API-Schlüssel.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Für das Madrid-Release und spätere Familienreleases ist das Plugin com.snc.si_dep erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren. Die folgenden Security Operations -Anwendungen müssen über ServiceNow Storeinstalliert und aktiviert werden. Installieren Sie eine Anwendung nach der anderen in der unten aufgeführten Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten: **1.** Security Integration Framework **2.** Security Support Common **3.** Security Support Orchestration **4.** Security Incident Response Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Administrator

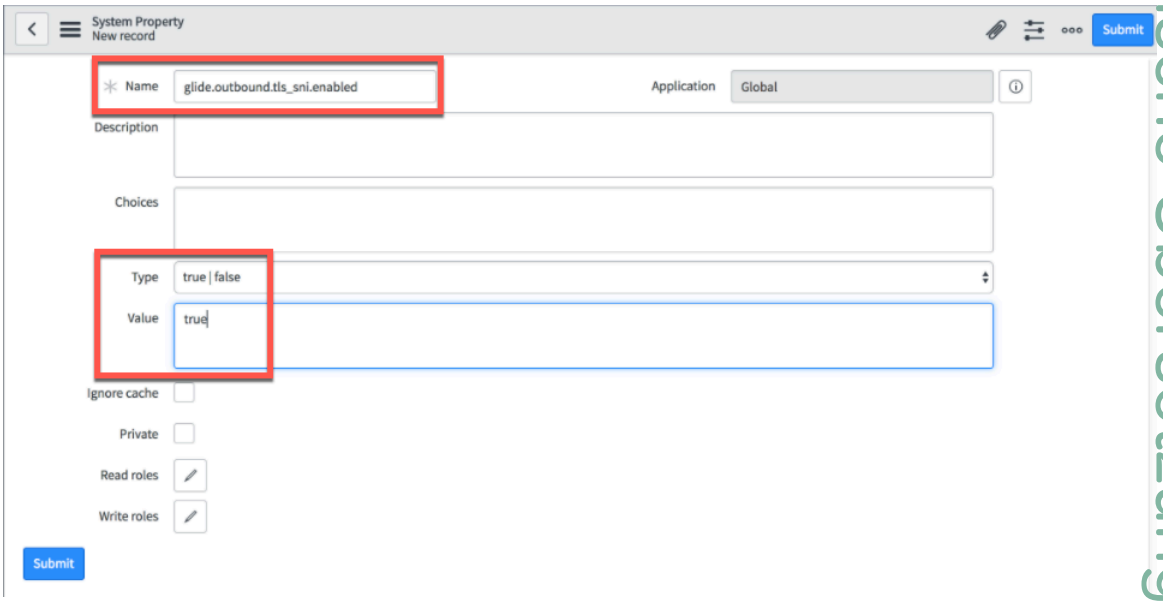
Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Schritte aus, um die Systemeigenschaften zu aktualisieren und die Integration zu installieren und zu konfigurieren.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein, und drücken Sie die **Eingabetaste**.
   Die Liste **der Systemeigenschaften** wird angezeigt.
2. Klicken Sie auf **Neu**.
   Ein neuer Datensatz wird angezeigt.
3. Füllen Sie die Felder aus, oder wählen Sie die Werte in der folgenden Tabelle aus, und klicken Sie auf **Absenden**.

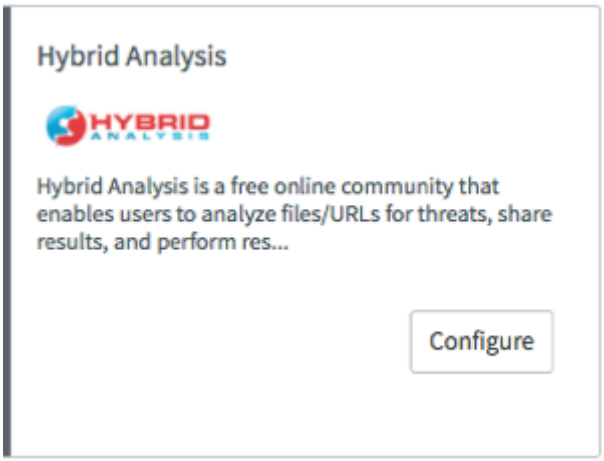
Feldname	Wert
Name	glide.outbound.tls_sni.enabled
Typ	Wählen Sie **true (wahr) und false (falsch)**aus
Wert	true



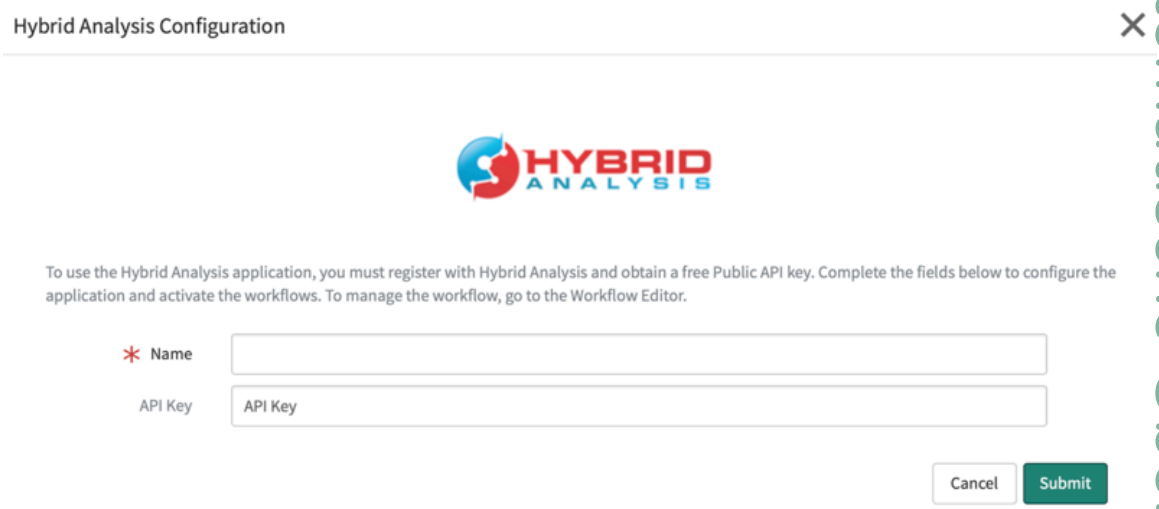
4. Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
5. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Hybrid-Analyse.
6. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Geben Sie im Dialogfeld **„Hybrid-Analysekonfiguration“** den API-Schlüssel ein, den Sie von der Website Hybrid-Analyse erhalten haben, und klicken Sie auf **Absenden**.



8. Überprüfen Sie die erfolgreiche Konfiguration.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, es wird eine Fehlermeldung angezeigt.

   Trouble?

   Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, ist der API-Schlüssel Hybrid-Analyse möglicherweise ungültig.

Überprüfen Sie die erwarteten Ergebnisse für Hybrid-Analyse

Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Suchen Sie die Suchergebnisse im Security Incident, um zu überprüfen, ob die Bedrohungssuche erfolgreich ausgeführt wurde. Zeigen Sie auch Rohdaten an, und führen Sie Bedrohungssuchen für untergeordnete erkennbare Elemente aus.

Vorbereitungen

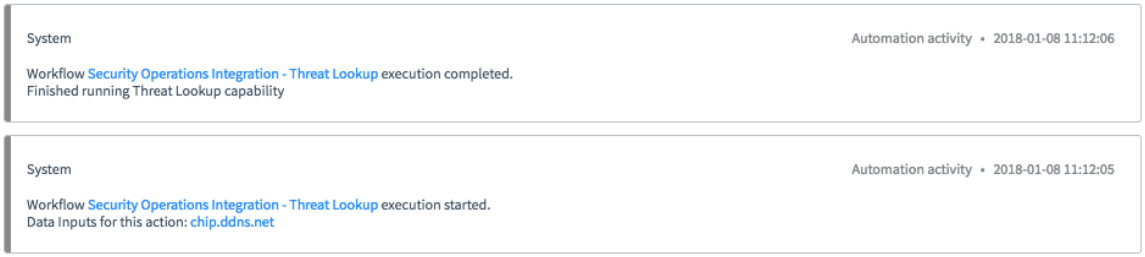
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.

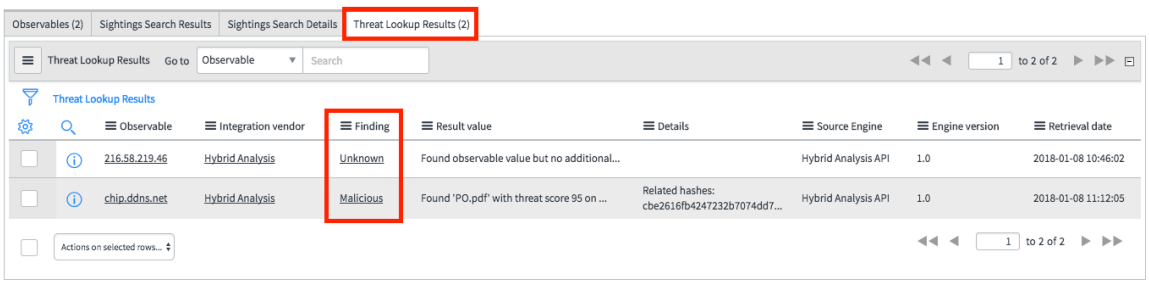


   Nachdem die Anwendung konfiguriert wurde, wird der Flow bei der Erstellung des incident automatisch gestartet. Der Ausführungs- und Abschlussstatus der Suche wird dann in den Arbeitsnotizen im Security Incident angezeigt.

2. Überprüfen Sie die Arbeitsnotizen auf weitere Informationen zum Vorgehen, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**, um die Ergebnisse anzuzeigen.

   Hinweis:
   Die Abbildungen in den folgenden Schritten werden mit aktivierter Einstellung **für Formulare mit Registerkarten** in den Systemeinstellungen angezeigt. Klicken Sie in der oberen rechten Ecke des Bannerframes auf das Zahnradsymbol Einstellungen. Klicken Sie im angezeigten Dialogfeld **„Systemeinstellungen“** auf **Formulare**, und vergewissern Sie sich, dass **Formulare mit Registerkarten** und **Mit Formular** ausgewählt sind.

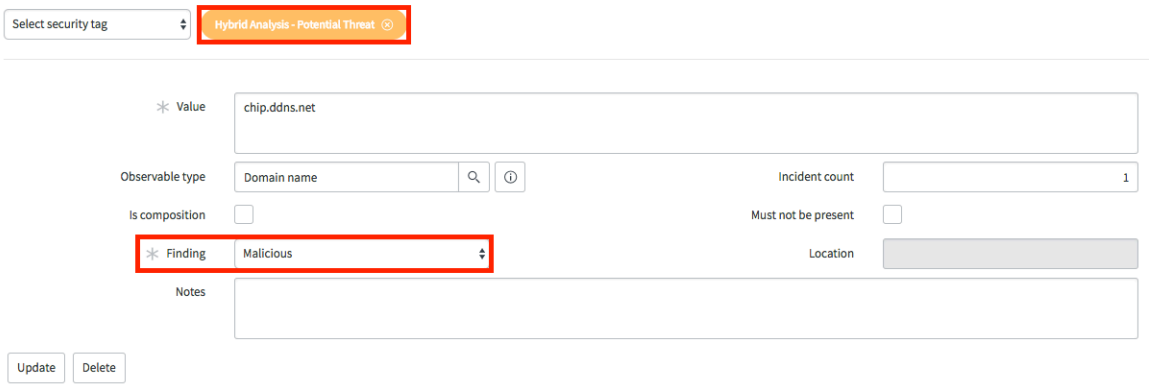


   Auf der Registerkarte **Ergebnisse der Bedrohungssuche** werden die Suchergebnisse am Ende des Security Incident-Datensatzes angezeigt. Beachten Sie, dass in der Spalte „ **Ergebnis** “ für Datensätze, die nicht als schädlich eingestuft wurden, Unbekannt angezeigt wird. Bei Ergebnissen, die mit „böswillig“ übereinstimmen, zeigt die Spalte „ **Ergebnisergebnis** “ Böswilligan.

4. Klicken Sie in der Spalte **Erkennbares** Element auf ein erkennbares Element, um den Datensatz zu öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

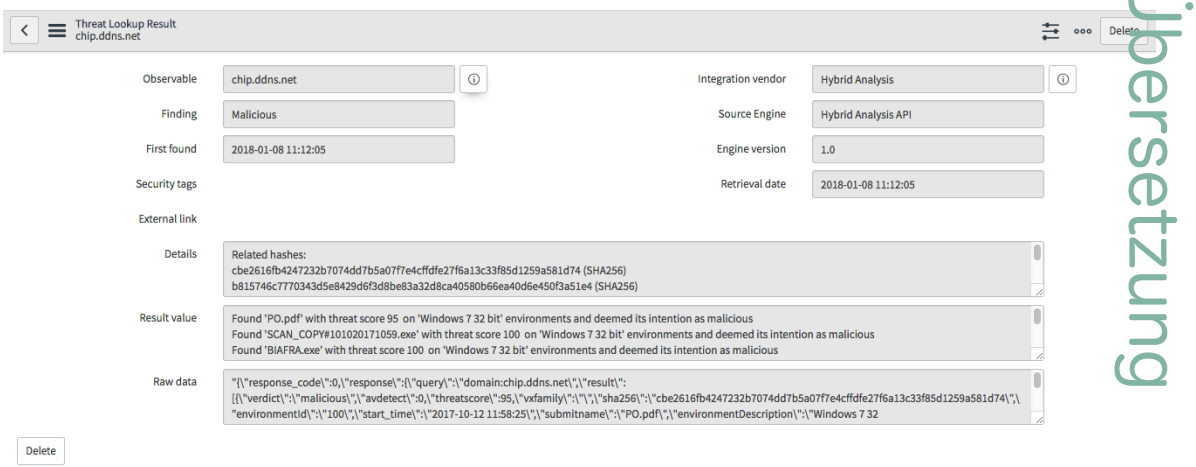


Bei Suchen nach schädlichen Elementen wird im Feld **Ergebnis** der Wert Böswilligangezeigt, und das erkennbare Element wird mit der Quelle Threat Intelligence getaggt, die es für schädlich befunden hat, in diesem Fall die Hybrid-Analyse -Integration.

5. **Wahlweise:** Führen Sie die Schritte aus, um Rohdaten anzuzeigen, eine Liste untergeordneter erkennbarer Elemente anzuzeigen und eine Bedrohungssuche für ausgewählte untergeordnete erkennbare Elemente auszuführen.

   a. Navigieren Sie zurück zum Security Incident, und klicken Sie auf der Registerkarte **Ergebnisse der Bedrohungssuche** auf das blaue Informationssymbol neben einem erkennbaren Element.

   b. Klicken Sie im angezeigten Fenster **auf Datensatz öffnen**, um die Daten anzuzeigen.
   Aus allen erkennbaren Elementen, die in den von der Suche angezeigten Rohdaten sichtbar sind, erstellt die Integration Hybrid-Analyse auch untergeordnete oder zugehörige erkennbare Elemente.



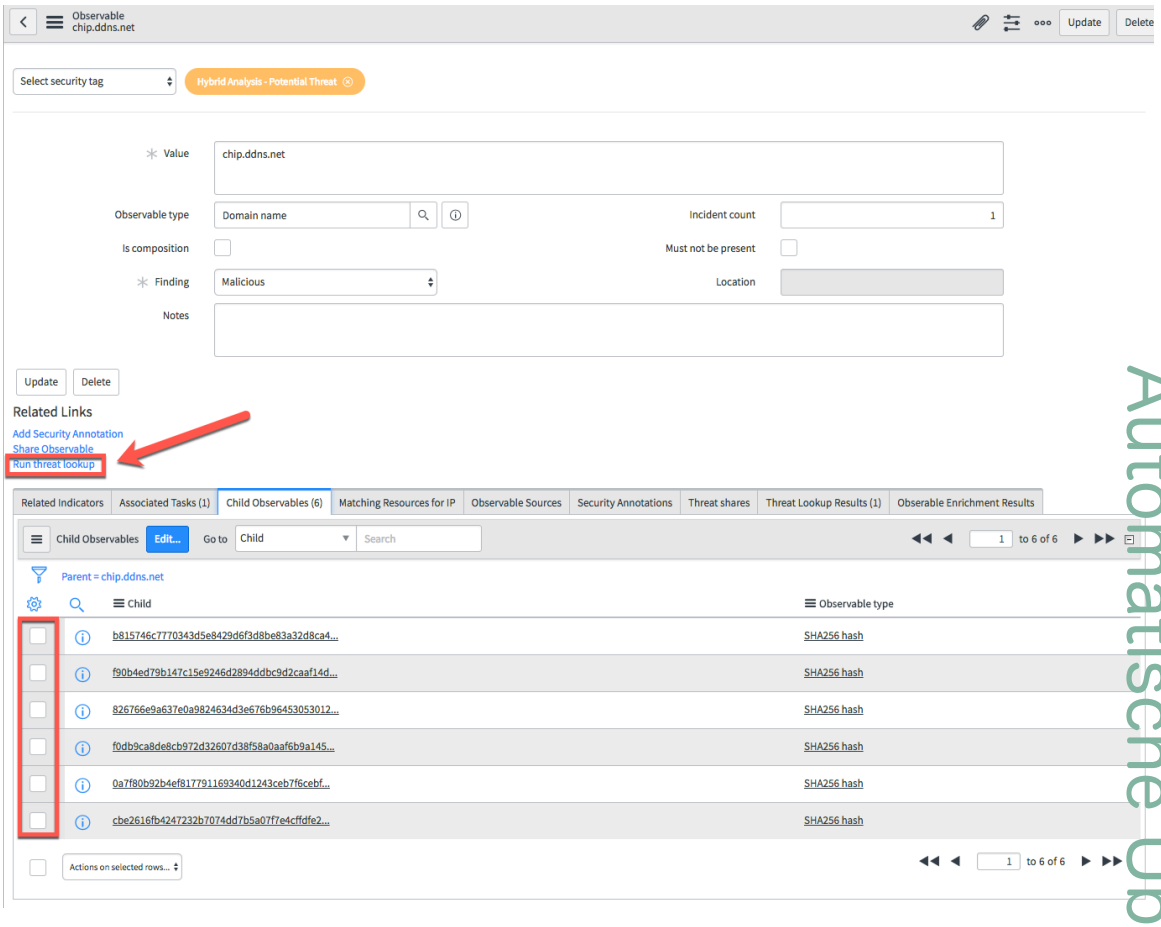
   Der von der API erstellte Link, die Rohdaten und andere Informationen werden angezeigt.

   c. Navigieren Sie zurück zum Security Incident, und klicken Sie auf den zugehörigen Link **IoC anzeigen**.
   Die untergeordneten erkennbaren Elemente werden auf der Registerkarte **„Untergeordnete erkennbare Elemente“** des Security Incident angezeigt, da bei der Suche eine Verbindung zwischen diesen zugehörigen erkennbaren Elementen und dem ursprünglich übermittelten erkennbaren Element gefunden wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Klicken Sie auf das Feld neben einem erkennbaren Element in der **Spalte Untergeordnetes** Element, um es auszuwählen, und anschließend auf den zugehörigen Link **Bedrohungssuche ausführen**, um eine Suche durchzuführen.



e. Stellen Sie im angezeigten Dialogfeld sicher, dass die Integration Hybrid-Analyse ausgewählt ist, und klicken Sie auf **Absenden**.

f. Überprüfen Sie in den Arbeitsnotizen, ob die Suche erfolgreich ausgeführt wurde, und suchen Sie auf der Registerkarte **„Ergebnisse der Bedrohungssuche“** im Security Incident die Suchergebnisse für die untergeordneten erkennbaren Elemente.

Trouble?
Wenn auf der Registerkarte **Ergebnisse der Bedrohungssuche** keine Ergebnisse angezeigt werden, vergewissern Sie sich, dass das erkennbare Element ein Typ ist, der von der Integration für die Suche unterstützt wird.

(Optional) Fügen Sie manuell ein erkennbares Element für hinzu Hybrid-Analyse

Sie können erkennbare Elemente manuell anhängen, wenn Sie Bedrohungssuchen für erkennbare Elemente durchführen möchten, die beim ersten Ereignisauslöser nicht an einen Security Incident angehängt sind. Außerdem können Sie diese Aufgabe ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

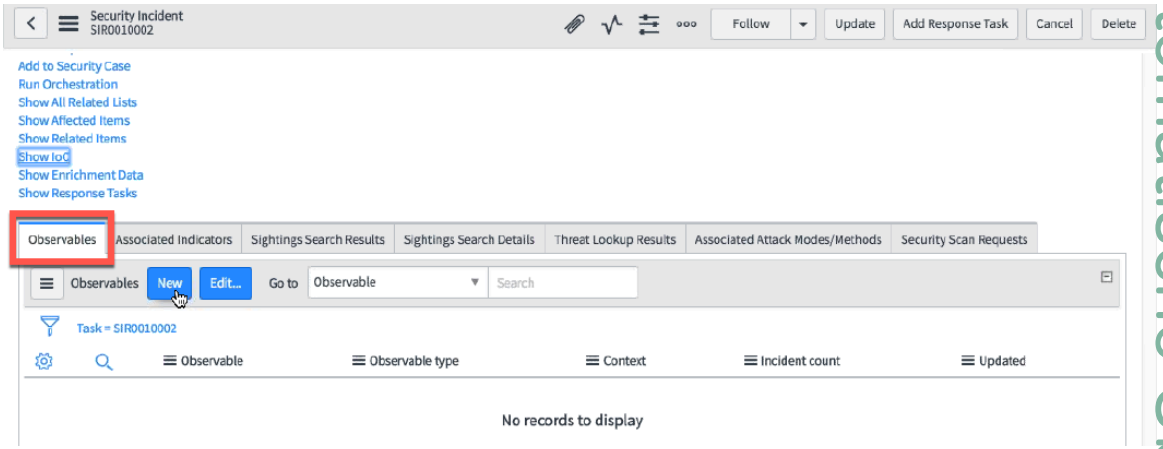
Stellen Sie sicher, dass das erkennbare Element einen von der Integration unterstützten Typ aufweist. Die -Integration führt Suchen für die folgenden Arten von erkennbaren Elementen durch:

- Datei-Hashes
- IP-Adressen
- URLs

Erforderliche Rolle: sn_si.analyst

Prozedur

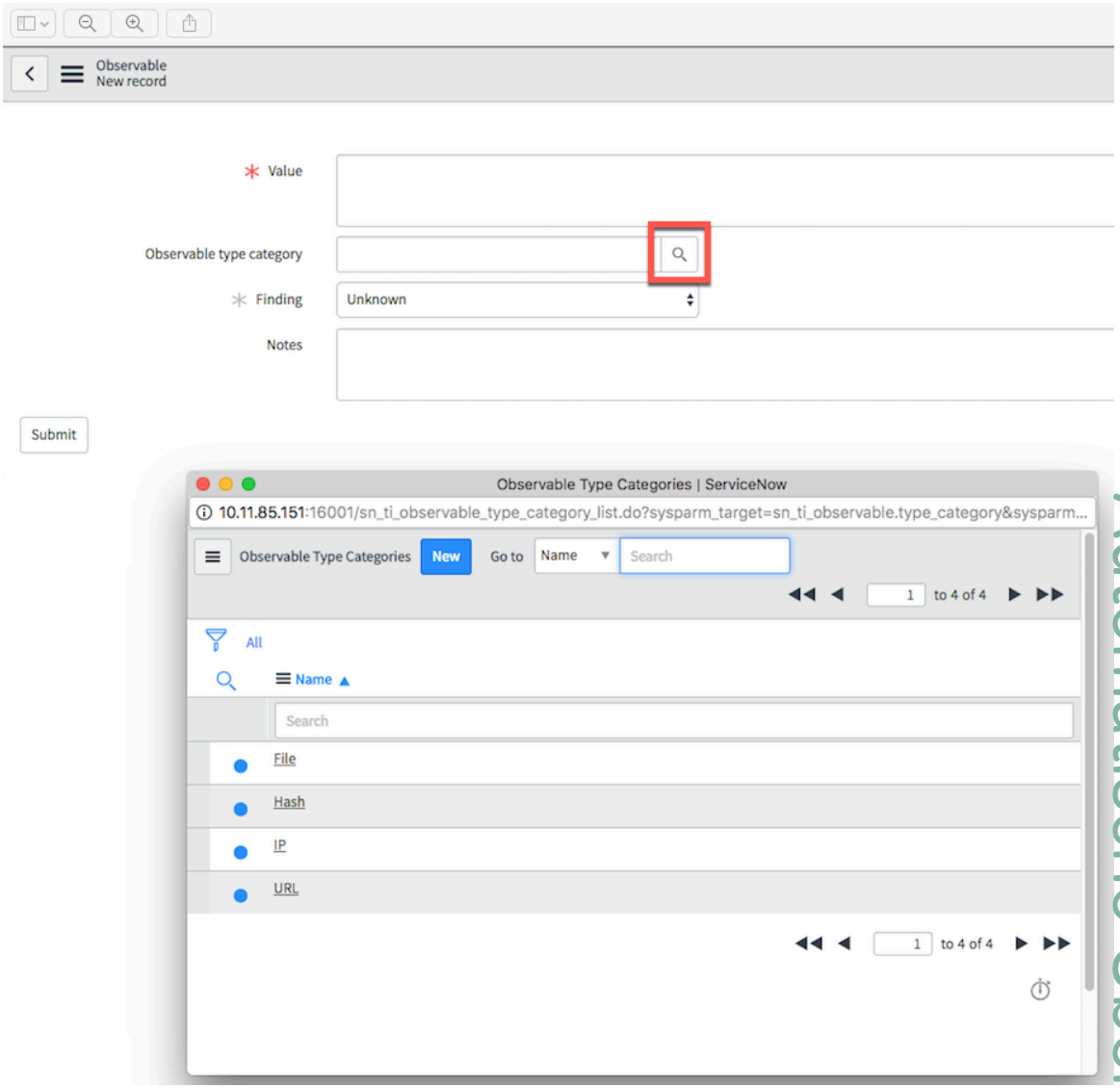
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie einen Security Incident, an den Sie das erkennbare Element anhängen möchten.
2. Klicken Sie im offenen Security Incident auf den Link **IoC anzeigen**unter **Zugehörige Links**.



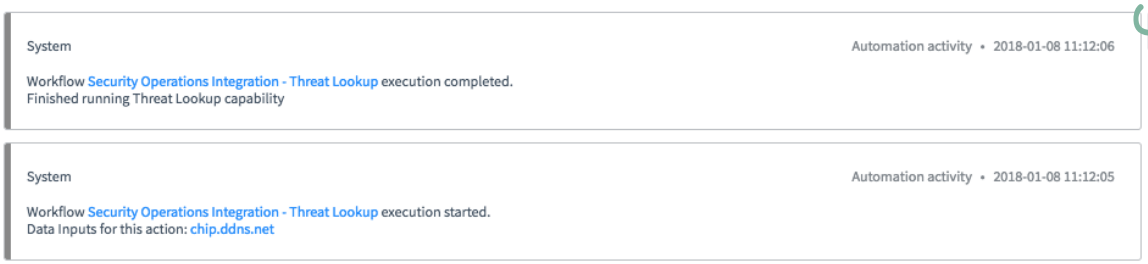
3. Klicken Sie auf der Registerkarte **Erkennbare Elementeauf Neu**.
   Das Formular „Erkennbares Element“ wird angezeigt.
4. Geben Sie im Feld **Wert** ein erkennbares Element ein (Datei-Hash, IP-Adressen oder URL).
5. Klicken Sie auf das Suchsymbol, und klicken Sie im Dialogfeld **„Kategorien erkennbarer Elemente“** in der Liste auf den Typ des gewünschten erkennbaren Elements, um das Feld auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



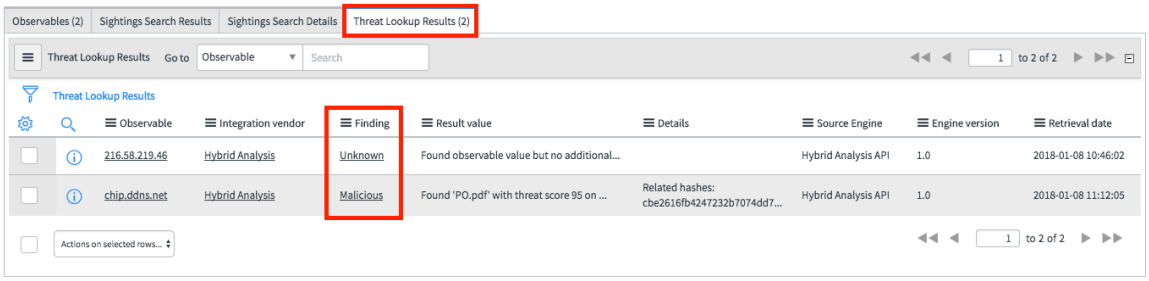
6. Klicken Sie auf **Absenden**.
   Der Flow wird gestartet und sucht nach dem neuen erkennbaren Element. Der Ausführungs- und Abschlussstatus werden im Abschnitt „Arbeitsnotizen“ des Security Incident-Datensatzes angezeigt.
7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.



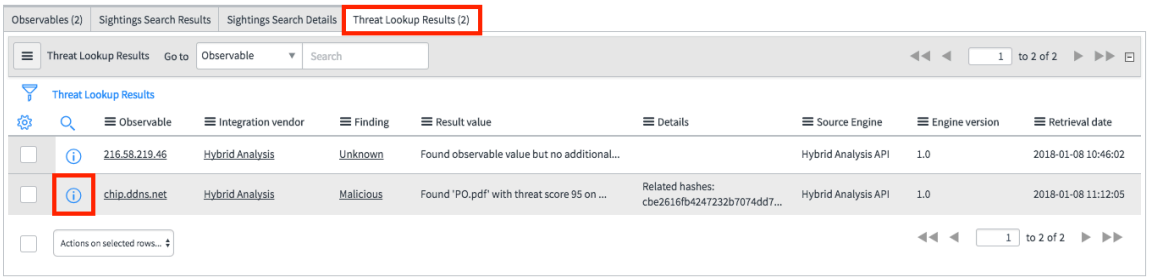
8. Klicken Sie unten im Datensatz auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**.
9. Klicken Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche,** um die Ergebnisse anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Klicken Sie in der Spalte „ **Erkennbares** Element“ auf das blaue Informationssymbol neben einem bestimmten erkennbaren Element, um weitere Informationen und Rohdaten zu erhalten.



11. Klicken Sie im angezeigten Dialogfeld **auf Datensatz öffnen**, um die Rohdaten und weitere Details anzuzeigen.
    Alternativ können Sie auch ein vorhandenes erkennbares Element an den Security Incident-Datensatz anhängen.
12. **Wahlweise:** Klicken Sie bei ausgewählter Registerkarte **Erkennbare Elementeauf Bearbeiten**.
13. **Wahlweise:** Verschieben Sie im angezeigten Formular **„Mitglieder bearbeiten“** ein vorhandenes erkennbares Element aus **Sammlung** in **Liste erkennbarer Elemente**, und klicken Sie auf **Speichern**. Sie kehren zum Security Incident zurück.
14. Wählen Sie in der Spalte ganz links die erkennbaren Elemente aus, für die Sie die Suche ausführen möchten, und wählen Sie in der Auswahlliste **Aktionen für ausgewählte Zeilen...** die Option **Bedrohungssuche ausführen aus**.
    Oben im Datensatz wird eine Meldung angezeigt, dass die Anforderung verarbeitet wird. Vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.

Trouble?
Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweise, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

IBM QRadar Offense Ingestion Integration

Die IBM QRadar Offense Ingestion -Integration ermöglicht es Ihnen, IBM QRadar -Vergehen automatisch abzurufen, in Security Incidents umzuwandeln und automatisierte Antwortaktionen zu aktivieren.

Diese Integration unterstützt:

- Erkennung von IBM QRadar Vergehen, die Kandidaten für Security Incidents sind.
- Die neuesten Ereignisse oder Flows, die einem Vergehen zugeordnet sind, werden abgerufen.
- Verfolgen Sie regelmäßig wichtige Updates für Vergehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zuordnung von Vergehen-, Ereignis- und Flow-Feldern zu Feldern für Security Incidents.
- Vorläufige Ansicht der zugeordneten Felder.
- Richten Sie geplante Erfassungen von Vergehen ein, um regelmäßig Security Incidents zu erstellen.
- Schließen Sie die Vergehen, wenn die Security Incidents geschlossen werden.

Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration der Vergehenserfassung IBM QRadar von [].

Bevor Sie die -Integration in Ihrer Instanz Now Platform® ausführen, führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in die -Produkte Security Incident Response und Security Operations in Ihrer Instanz Now Platform integriert werden kann.

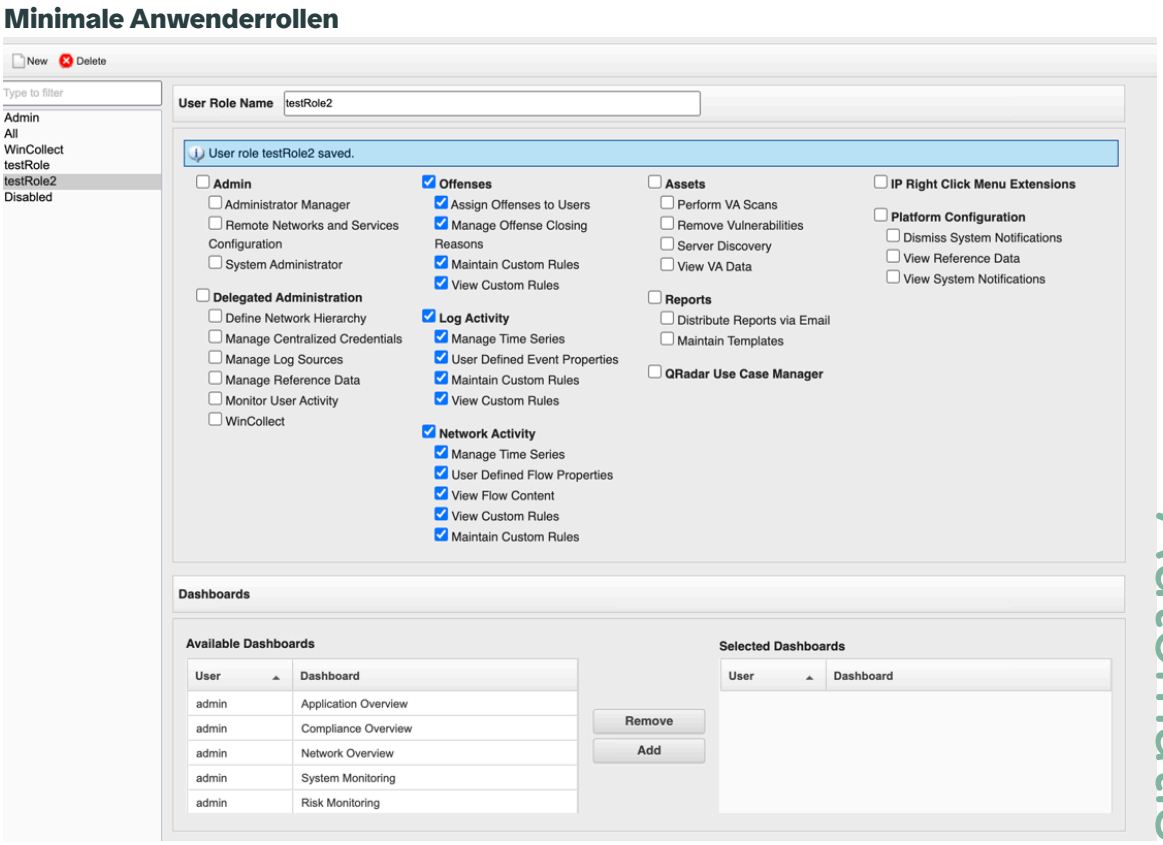
Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

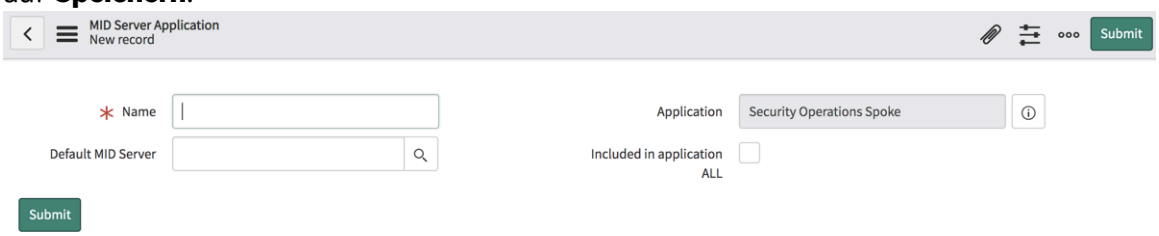
1. Wenn Sie die Anwendung IBM QRadar für die Integration nicht aus ServiceNow Store installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel IBM QRadar.
3. Klicken Sie zum Konfigurieren der Anwendung auf **Neu**.
4. Alternativ: Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, können Sie darauf klicken, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie im angezeigten Dialogfeld **„Konfiguration der Angriffserfassungen“** die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um eine neue MID-Server-Anwendung zu erstellen, gehen Sie wie folgt vor:

- Navigieren zu **MID-Server** > **Anwendungen** und klicken Sie auf **Neu**.
- Geben Sie einen Namen für die MID-Server-Anwendung ein, und wählen Sie einen MID-Server aus, der als Standard verwendet werden soll.
- Deaktivieren Sie das Kontrollkästchen In Anwendung ALLE enthalten, und klicken Sie auf **Speichern**.

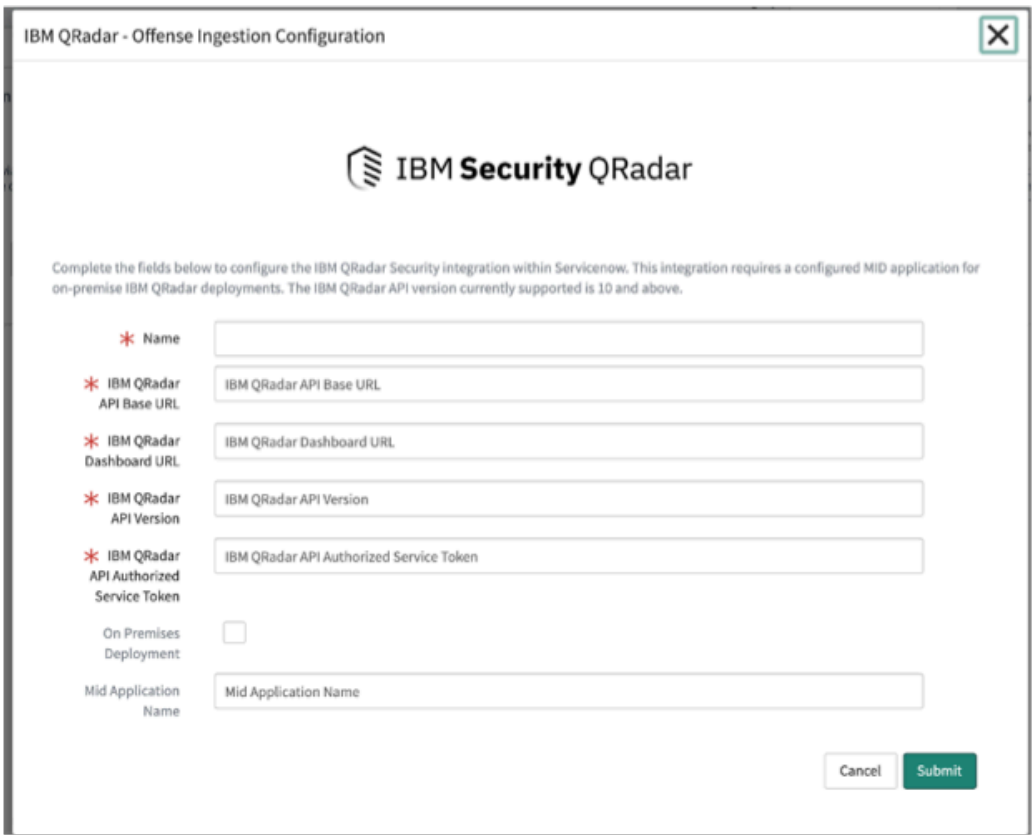


- Klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **„Mitglieder bearbeiten“** alle verfügbaren MID-Server aus, verschieben Sie sie in die Liste der MID-Server, und klicken Sie auf **Speichern**. Je nach Verfügbarkeit wird einer der mit der MID Server-Anwendung konfigurierten MID Server verwendet.

6. Geben Sie die Konfigurationsdetails ein, und geben Sie die von Ihnen erstellte MID-Server-Anwendung an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Quelle, die Sie im Formular **„IBM QRadar Offense Ingestion Configuration“** konfigurieren, kann für mehrere Now Platform Profile wiederverwendet werden, solange jedes Profil Vergehen erfasst.

7. Klicken Sie auf **Absenden**.
   Nach erfolgreicher Validierung und Übermittlung wird jede IBM QRadar -Serverkonfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite mit den Sicherheitsintegrationen angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.

Hinweis:
Wenn Probleme mit der Domänensegmentierungsfunktion IBM QRadar auftreten, wenden Sie sich an den Kundensupport von IBM QRadar.

Nächste Maßnahme
Sie haben die Anwendung erfolgreich installiert und konfiguriert. Im nächsten Schritt wird das Profil erstellt.

Richten Sie Ihre Instanz Now Platform® für die Integration der Vergehenserfassung für IBM QRadar ein

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in der Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung von ServiceNow Storeinstallieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sehen Sie sich die folgende Tabelle an, und vergewissern Sie sich, dass Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben.	Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Instanz Now Platform® von erforderlich. • Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Ein Benutzer mit der Rolle sn_si.admin überwacht die folgenden Aufgaben in Now Platform®: ◦ Benennt, erstellt und bearbeitet Vergehensprofile. ◦ Wählt die Felder mit Daten für Vergehen IBM QRadar aus und ordnet sie den Feldern für Security Incidents zu. ◦ Zeigt eine Vorschau der Details von Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird. ◦ Plant die laufende Erfassung von Vergehen. ◦ Aktiviert die Aktualisierung von Vergehen, wenn ein SIR-Incident erstellt und geschlossen wird. ◦ Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu. ◦ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Rollen auf der Website der ServiceNow-Produktdokumentation .
Stellen Sie sicher, dass Sie die folgenden Versionen verwenden: • IBM QRadar Version 7.3.2 oder höher. • IBM QRadar API-Version 10 oder höher Frühere Versionen werden nicht unterstützt.	Wenn Sie Zugriff auf die -Konsole IBM QRadar haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich.
Stellen Sie sicher, dass Sie eine MID-Serveranwendung installiert und konfiguriert haben.	Konfigurierte MID-Server-Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	Ein MID-Server in Ihrer Instanz Now Platform® ist erforderlich, um eine Verbindung zum Service IBM QRadar herzustellen, wenn der Server IBM QRadar innerhalb Ihres Unternehmensnetzwerks bereitgestellt wird. Informationen zu MID-Servern finden Sie auf der Website der ServiceNow-Produktdokumentation . Wenn Sie den Cloud-Service IBM QRadar verwenden, ist kein MID-Server erforderlich.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Event and Alert Ingestion for Security Operations: Diese Anwendung benötigt: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST **Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Ereignis- und Warnungserfassung“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport. Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Automatische Übersetzung

Nächste Maßnahme

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht in der Installation der Anwendung IBM QRadar aus ServiceNow Store für die Integration.

Erstellen Sie ein Profil für die Integration der Straftaterfassung IBM QRadar .

Als Benutzer mit der Rolle sn_si.admin erstellen Sie in Ihrer Instanz Now Platform ein Vergehenprofil und bestimmen, welche Vergehen Security Incidents erzeugen. Bevor Security Incidents vom Now Platform Security Incident Response Typ (SIR) aus Vergehen erstellt werden, werden die Feldwerte aus Vergehen in einem Layout eines Now Platform -Security Incidents angezeigt, sodass Sie eine Vorschau auf die Erstellung des konkreten Security Incidents anzeigen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Aus der Perspektive der Integration mit verfügbaren APIs werden Vergehen IBM QRadar je nach definiertem Profiltyp automatisch in die Umgebung Security Operations Ihrer Instanz Now Platform aufgenommen. Die Integrations-Workflows erfassen verschiedene Arten von Vergehen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Vergehen werden basierend auf den Profilen erfasst, die Sie in der Umgebung Security Operations Ihrer -Instanz konfigurieren. Alle Vergehen werden zunächst für einen konfigurierten Vergehenstyp in einem Profil erfasst. Erfasste Vergehen können dann weiter gefiltert werden, um anzugeben, welche Vergehen Security Incidents erzeugen. Beispielsweise können Sie Filter bevorzugen, die Security Incidents nur für Vergehen erstellen, die als hoch riskant eingestuft wurden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Vergehen erstellt werden, werden einzelne Feldwerte für die Vergehen den entsprechenden Feldern in einem Layout von Security Incidents zugeordnet, um eine Vorschau anzuzeigen.

Namen für die Vergehensprofile in Ihrer Instanz Now Platform müssen eindeutig sein. Sie können mehrere Konfigurationen für mehrere Quellen erstellen und Sie können auch mehrere Profile für eine einzige Quelle erstellen.

Erstellen Sie Profile für die Erfassung von IBM QRadar -Vergehen

Sie können ein Profil einrichten, um Vergehen zu erfassen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur
1. Um ein Profil für einen Vergehen in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

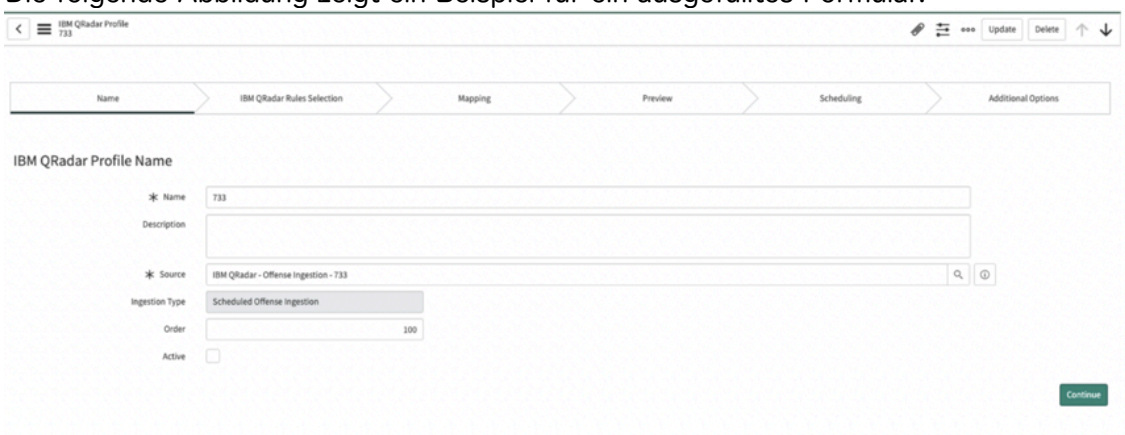
   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn die Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert. Profilnamen in Ihrer Instanz Now Platform müssen eindeutig sein.
Aktiv	Checkbox ist standardmäßig deaktiviert. Wenn diese Option deaktiviert ist, ist das Profil nicht aktiv, und es findet keine Erfassung statt. **Hinweis:** Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.
Quelle	Der IBM QRadar -Server, den Sie für die Erfassung von Vergehen konfiguriert haben. Wenn Sie mehrere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	IBM QRadar -Server konfiguriert haben, wählen Sie den entsprechenden Server für die Vergehenstypen aus, die für das Profil erfasst werden. Sie müssen einen Wert eingeben.
Bestellung	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile dieselben Auslösebedingungen verwenden. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität.
(Optional) Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



Nächste Maßnahme

Der nächste Schritt besteht in der Auswahl der Vergehen für die Erfassung.

Wählen Sie IBM QRadar Regeln aus

Wählen Sie basierend auf der IBM QRadar -Quelle eine oder mehrere IBM QRadar -Regeln für das Profil aus.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren IBM QRadar -Regeln in Ihrer Now Platform-Instanz an, damit Sie wissen, für welche aktiven IBM QRadar -Regeln Sie Security Incidents erfassen und erstellen möchten.

In IBM QRadarkönnen Sie Regeln anhand ihres Ursprungs als System-, Überschreibungs- und Benutzerregeln identifizieren. Standardmäßig ist der Ursprung einer Regel mit einer Systemregel verknüpft. Wenn Sie eine Systemregel in IBM QRadarändern, wird ihr Ursprung als Überschreiben festgelegt.

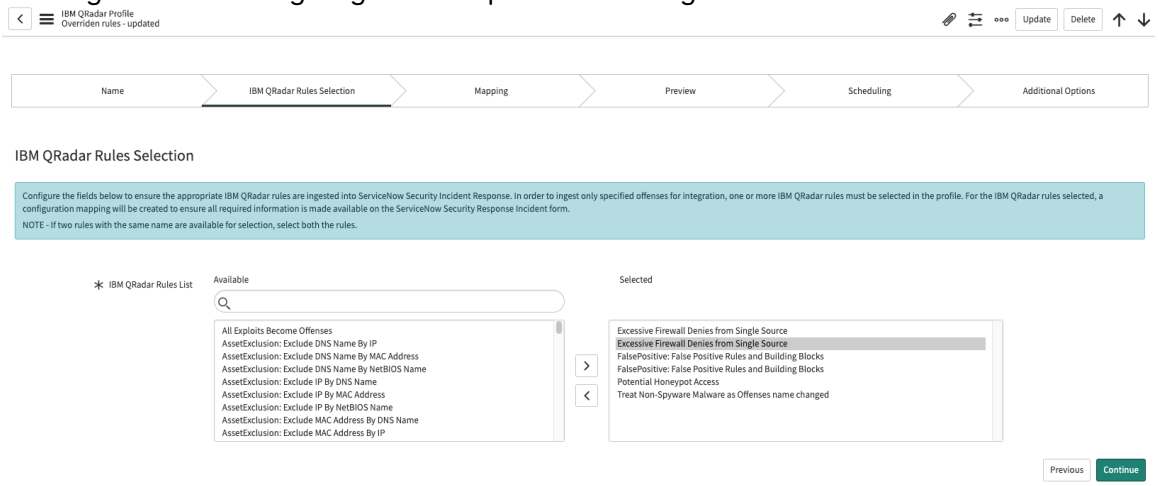
Klicken Sie auf die Liste im Feld IBM QRadar Regelliste. Eine Liste der aktiven IBM QRadar -Regeln, die in der Konsole IBM QRadar vorhanden sind, wird angezeigt. Wählen Sie eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

oder mehrere Regeln aus der Liste aus, und verschieben Sie sie in die Spalte **Ausgewählt**. Vergehen, die durch eine oder mehrere der ausgewählten IBM QRadar -Regeln ausgelöst wurden, werden in diesem Profil erfasst.

Regeln mit demselben Namen: In der Instanz Now Platform wird eine Liste aktiver oder aktivierter Regeln angezeigt. Wenn Sie eine aktive oder aktivierte Systemregel in IBM QRadarändern, wird eine neue Überschreibungsregel erstellt. Dies führt dazu, dass zwei Regeln mit demselben Namen in Now Platformangezeigt werden. Wenn dieses Szenario auftritt, wählen Sie sowohl die Regeln zur Erfassung als auch zur Erstellung von Security Incidents aus.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular:



Klicken Sie auf **„Fortsetzen“**, um mit dem nächsten Schritt im Assistenten fortzufahren.

Zuordnung von Vergehen-Feldern für die IBM QRadar -Integration

Nachdem Sie die Regeln ausgewählt haben, besteht der nächste Schritt darin, die Felder für Vergehen, Ereignisse oder Flow den Feldern im Formular „Security Incident“ zuzuordnen.

Übersicht

Für den Zuordnungsschritt müssen Sie zuerst Beispielvergehen für eine oder mehrere ausgewählte IBM QRadar -Regeln erfassen. Dann müssen Sie sicherstellen, dass alle relevanten Vergehensfelddaten an der entsprechenden Stelle im Incident-Formular SIR zugeordnet sind, und dann den Incident SIR im Vorschaubereich visualisieren.

Die Zuordnung der Felder für ein Beispielvergehen umfasst Folgendes:

- Beispieldaten werden abgerufen und ausgefüllt: Siehe Erfassung des Beispielvergehens IBM QRadar.
- Vergehen-Felder werden dem Security Incident zugeordnet: Siehe IBM QRadar -Vergehensfelder werden Security Incident-Antwortfeldern zugeordnet.

Erfassung des Beispielvergehens IBM QRadar

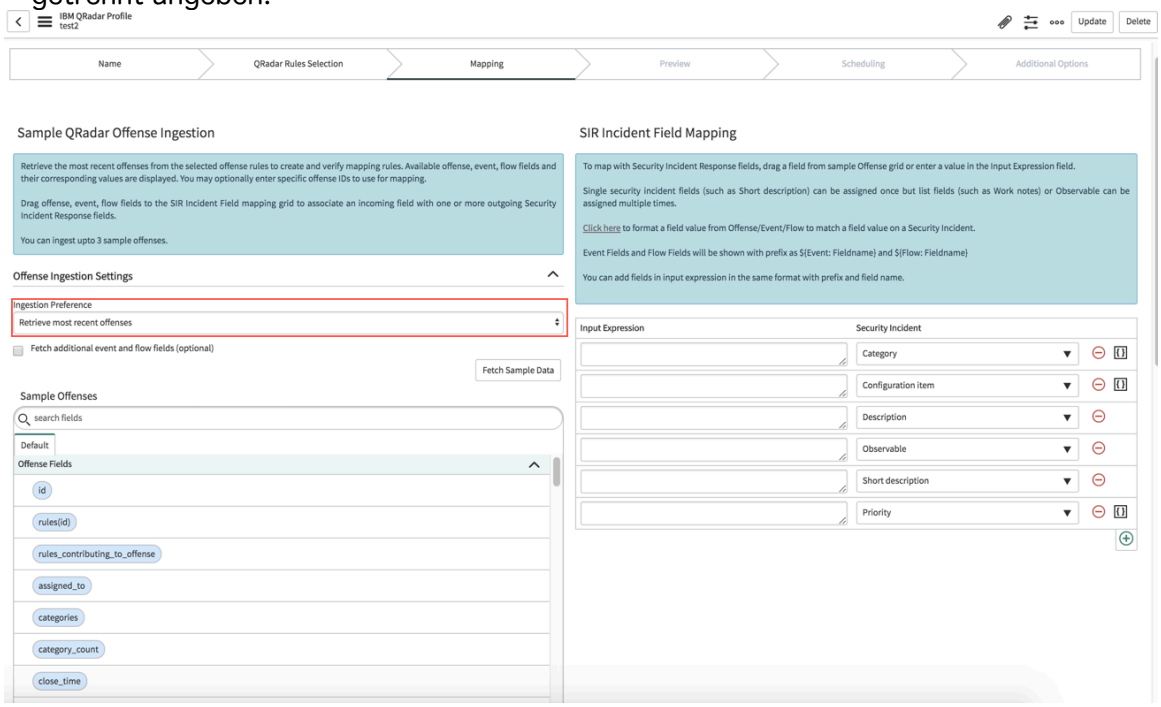
Sie können Beispielvergehen für eine oder mehrere ausgewählte IBM QRadar -Regeln erfassen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
2. Sie können entweder die drei neuesten Beispielvergehen abrufen oder die eindeutigen Vergehen-IDs für die spezifischen Vergehen angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   Wählen Sie in der Auswahlliste **Erfassungseinstellung** eine der folgenden Optionen aus:
   - Neueste Vergehen abrufen: Die drei neuesten Vergehen für die ausgewählten Regeln werden abgerufen.
   - Wählen Sie Vergehen basierend auf der Vergehen-ID aus: Geben Sie die Vergehen-ID für die abzurufenden Vergehen an. Sie können maximal 3 Vergehens-IDs durch Kommas getrennt angeben.



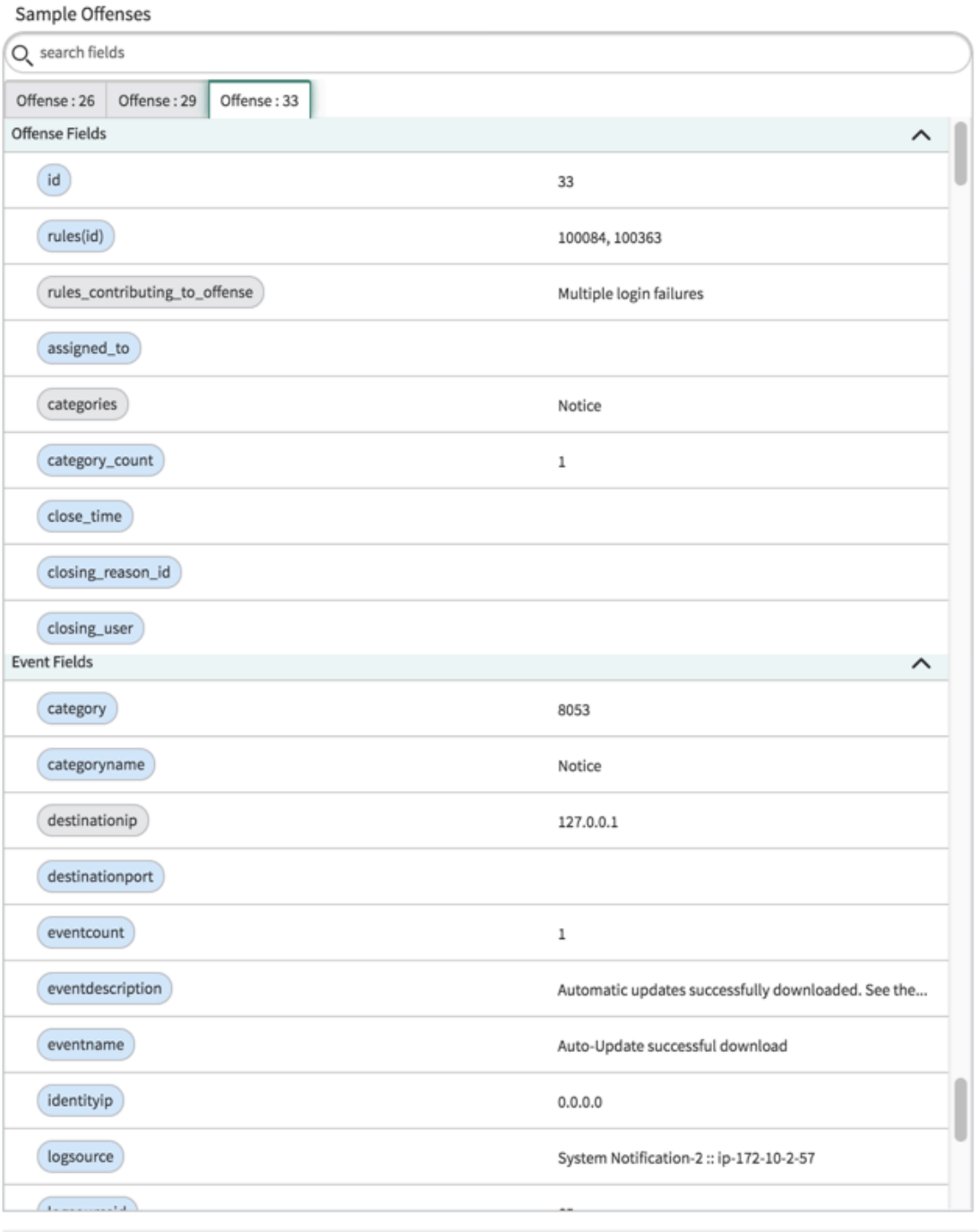
3. Klicken Sie **auf Beispieldaten abrufen**, um die neuesten Beispielvergehensdaten für die ausgewählten Vergehensregeln aus der Konsole IBM QRadar abzurufen.

   Die Vergehen-Felder und -Werteergebnisse werden als einzelne Registerkarten angezeigt. Ein Vergehen kann durch drei Arten von Regeln ausgelöst werden:
   - Ereignis: In dieser Regel werden Ereignisprotokolle überprüft. Wenn die angegebenen Kriterien erfüllt sind, wird ein Vergehen erstellt.
   - Flow: Netzwerkdaten und -verkehr werden überprüft. Wenn bestimmte Bedingungen erfüllt sind, wird ein Vergehen erstellt.
   - Häufig: In diesem Fall können Sie Bedingungen für Ereignisse oder Flows angeben. Wenn eine oder beide Bedingungen erfüllt sind, wird ein Vergehen erstellt.

   Das Abrufen von Beispielvergehen kann einige Minuten dauern. Oben auf dem Bildschirm wird eine Meldung angezeigt, dass die Transaktion funktioniert. Abhängig von der Regel, die den Vergehen ausgelöst hat, werden zusammen mit den Vergehen-Feldern die Ereignis- oder Flow-Felder ausgefüllt, wie in der folgenden Abbildung dargestellt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die angezeigten Ereignis- oder Flow-Felder gehören zum ersten Ereignis- oder Flow-Feld, das den Vergehen basierend auf dem entsprechenden Ereignis oder der entsprechenden Flow-Regel ausgelöst hat.

4. Die folgenden anwenderdefinierten Vergehen-Felder wurden für diese Integration erstellt. Zusätzlich zu diesen anwenderdefinierten Feldern sind Standardvergehen-Felder für die Zuordnung verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- rules_contributing_to_offense: IBM QRadar Regeln, die basierend auf der Regel-ID zu dem Vergehen beigetragen haben.
- users: Anwendernamen für den Vergehen
- remote_destination_ip: Die Remote-Ziel-IPs für den Vergehen.

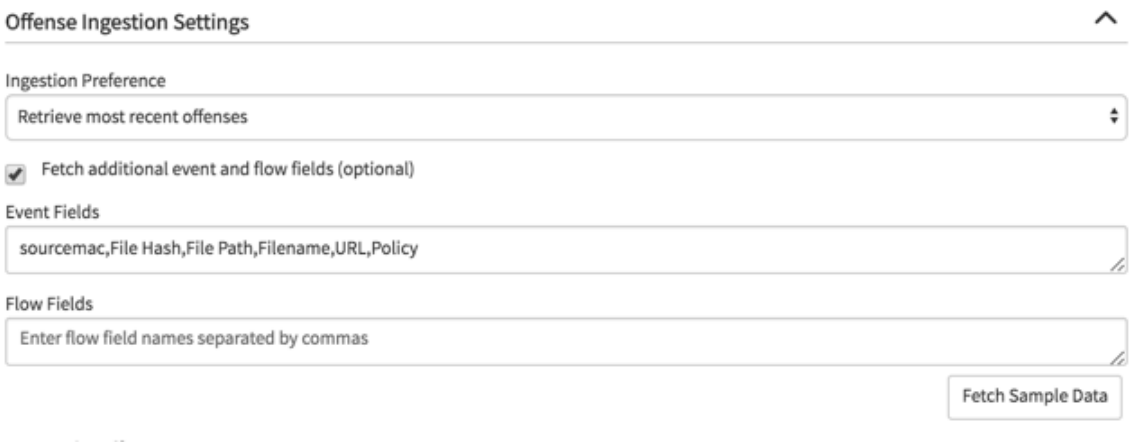
  Basierend auf den lokalen Ziel-IDs für den Vergehen sind die folgenden anwenderdefinierten lokalen Zieladressfelder verfügbar:

  - local_destination_address (domain_id)
  - local_destination_address (event_flow_count)
  - local_destination_address (first_event_flow_seen)
  - local_destination_address (id)
  - local_destination_address (last_event_flow_seen)
  - local_destination_address (local_destination_address_ids)
  - local_destination_address (Größe)
  - local_destination_address (Netzwerk)
  - local_destination_address (offense_ids)
  - local_destination_address (local_destination_ip)

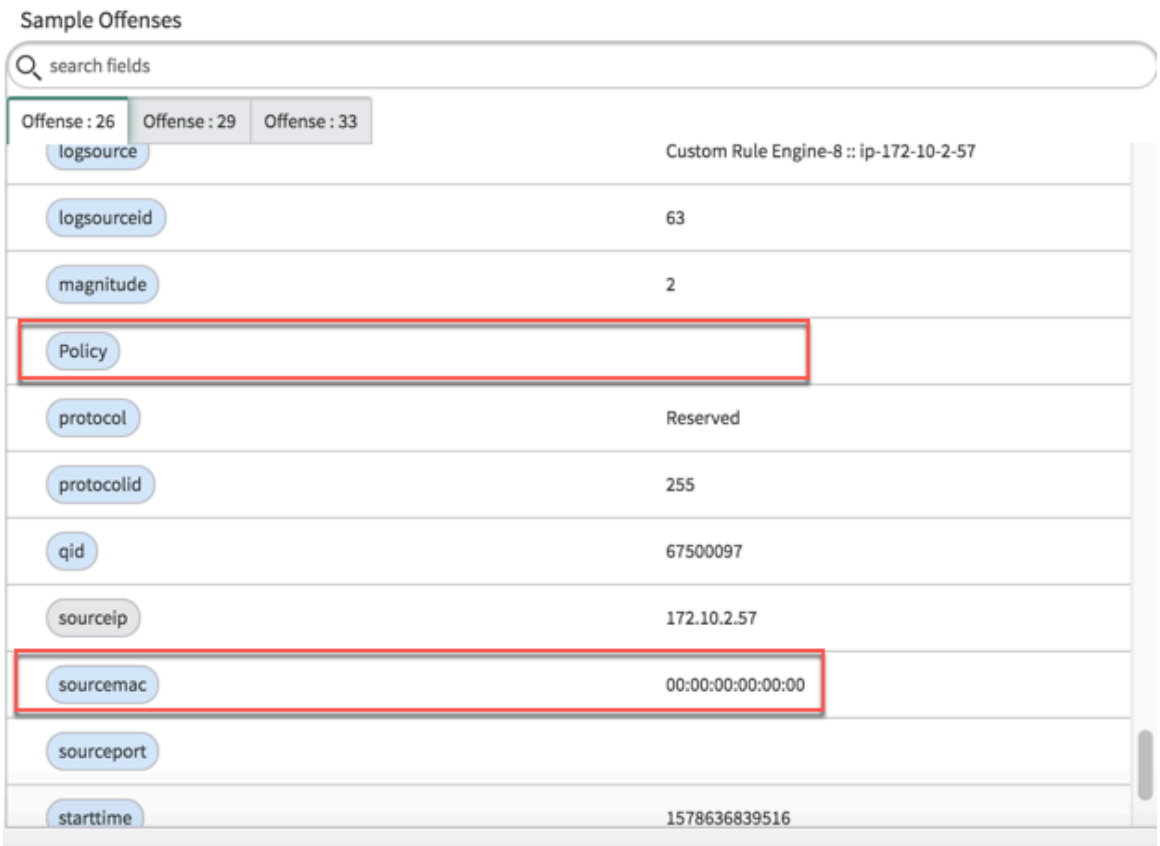
- Die folgenden Quelladressen sind basierend auf den Quell-IDs des Vergehens verfügbar:
  - source_addresses (Domäne_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (ID)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (Größe)
  - source_addresses (Netzwerk)
  - source_addresses (offense_ids)
  - source_addresses (source_ip)

Aktivieren Sie das Kontrollkästchen **Zusätzliche Ereignis- und Flow-Felder abrufen (optional)**. Sie können Beispielereignis- und Flow-Daten aus allen aktiven, gültigen anwenderdefinierten Ereignis- und Flow-Feldern abrufen. Geben Sie die anwenderdefinierten Felder wie folgt durch Kommas getrennt an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

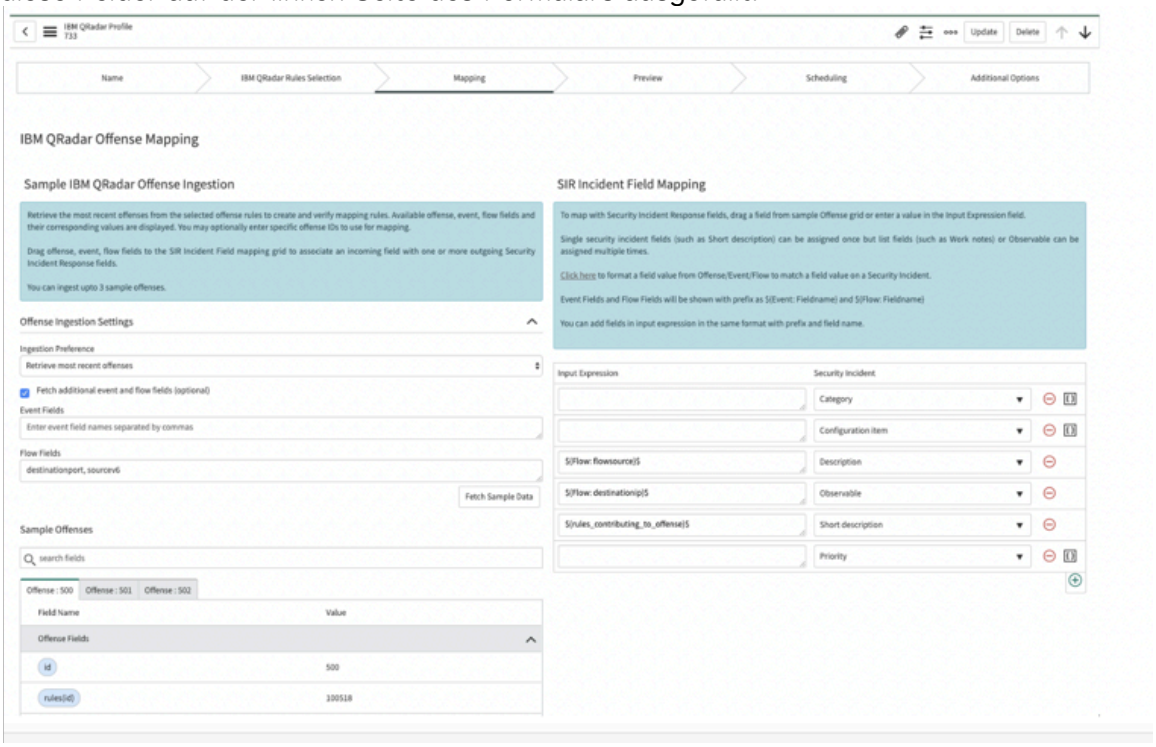


Klicken Sie **auf Beispieldaten abrufen**. Die angegebenen Ereignis- oder Flow-Felder werden zusammen mit ihren Werten (falls verfügbar) wie unten gezeigt an den Abschnitt „Ereignis“ oder „Flow“ angehängt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die Beispieldaten abgerufen haben, werden die entsprechenden Werte für diese Felder auf der linken Seite des Formulars ausgefüllt.



Nächste Maßnahme

Nachdem Sie die Beispieldaten abgerufen haben, besteht der nächste Schritt darin, die Vergehen-Felder dem Security Incident zuzuordnen.

IBM QRadar -Vergehensfelder werden Security Incident-Antwortfeldern zugeordnet

Ordnen Sie einzelne Vergehen-, Ereignis- und Flow-Felder Feldern in einem Security Incident Now Platform SIR zu.

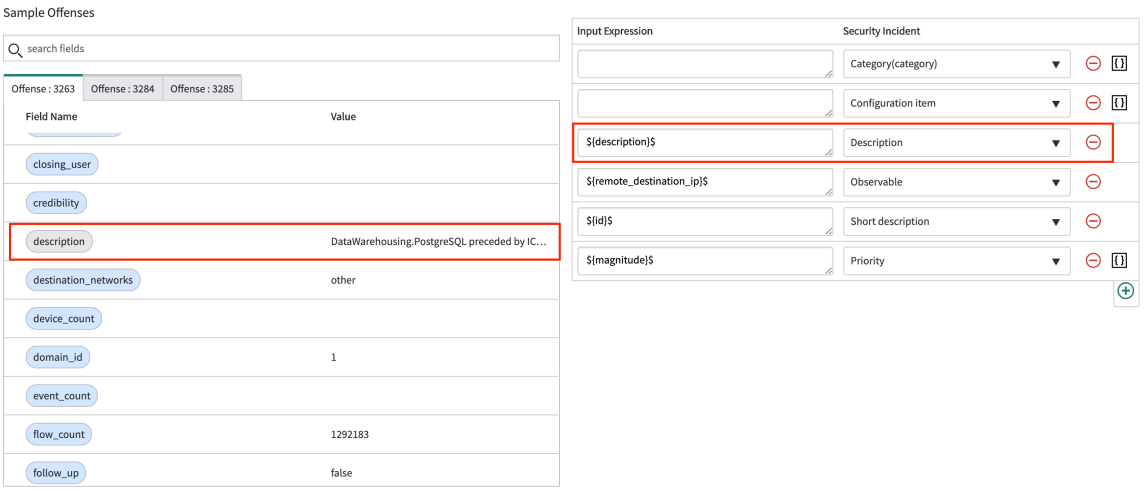
Feldzuordnung für Vergehen

Als Benutzer mit der Rolle sn_si.admin verwenden Sie die Felder aus dem Abschnitt Beispielvergehen auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Vergehen-, Ereignis- oder Flow-Felder aus der linken Seite in den Abschnitt ServiceNow SIR Incident-Zuordnung auf der rechten Seite ziehen. Die Zuordnung auf der rechten Seite ordnet das Feld für eingehende Vergehen einem Feld für ausgehende Security Incidents zu.

1. Nachdem Sie die Beispieldaten abgerufen haben, besteht der nächste Schritt darin, die Felder für Vergehen, Ereignisse oder Flow dem Security Incident zuzuordnen. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf einen blauen Feldnamen auf der linken Seite des Formulars.
2. Ziehen Sie den Feldnamen, z. B. Beschreibung, und legen Sie ihn auf ein Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“.

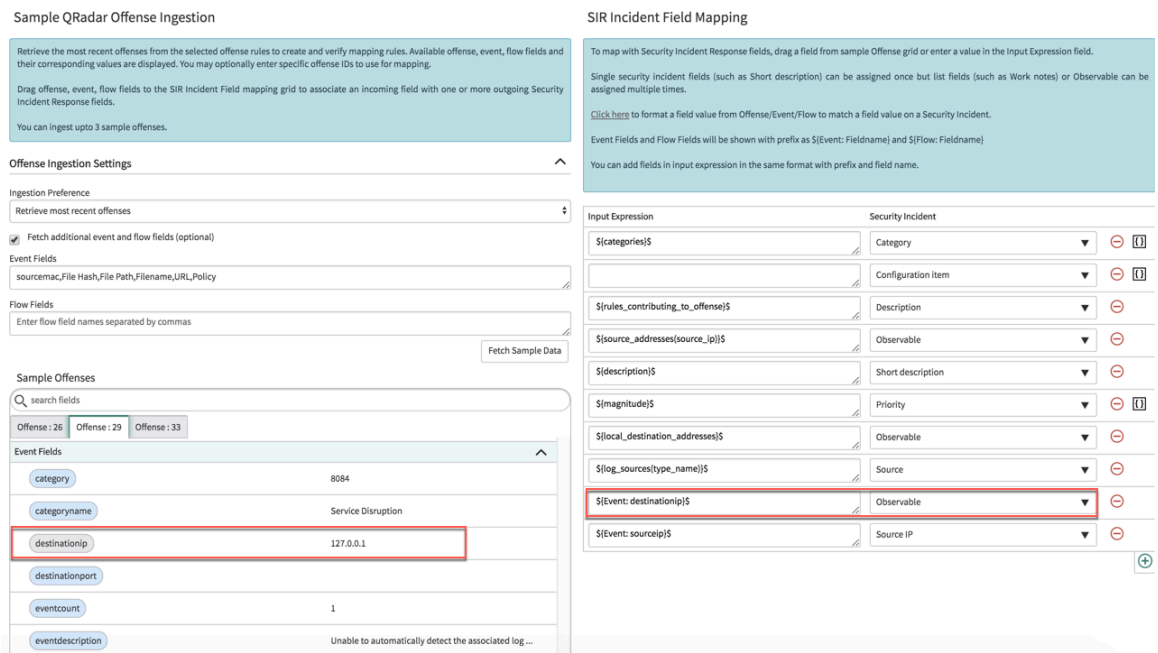
   Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird die Beschreibung dem Feld Beschreibung im Security Incident zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

Wenn Sie den Namen des Ereignis- oder Flow-Felds manuell im Abschnitt „Eingabeausdruck“ eingeben, müssen Sie vor dem Namen des zuzuordnenden Felds ein Präfix als `${Event:eventfield}$` oder `${Flow:flowfield}$` hinzufügen.



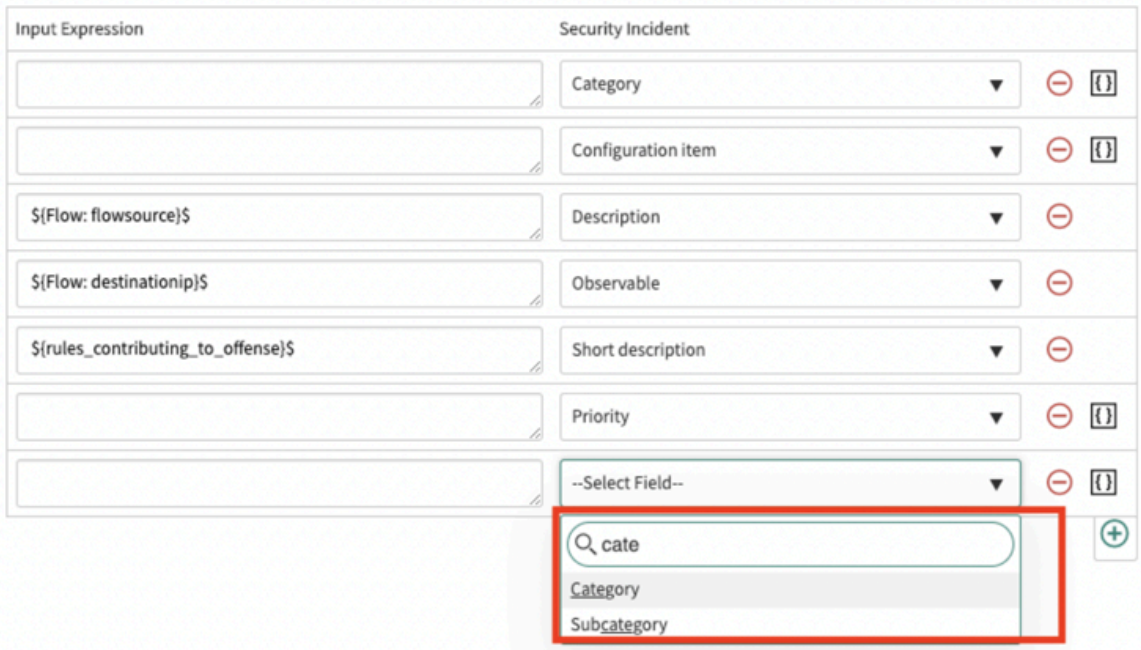
Um sicherzustellen, dass im Zuordnungsprozess keine Vergehen-, Ereignis- oder Flow-Felder übersehen oder dupliziert werden, sind Felder farbcodiert. Die Farbcodierung der Vergehen-Felder hilft Ihnen, die bereits zugeordneten Vergehen-Werte nachzuverfolgen, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob wichtige Vergehensinformationen verbleiben.

Hellblaue Felder auf der linken Seite zeigen an, dass das Feld für Vergehen noch nicht ausgewählt und dem Security Incident zugeordnet wurde. Unter Umständen möchten Sie ein eingehendes Vergehen-, Ereignis- oder Flow-Feld mehreren Feldern in einem Security Incident zuordnen. Ein graus Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen:
   a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Pluszeichen (+). Ein neues Feld wird angezeigt.
   b. Erweitern Sie in der Spalte „Security Incident“ die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

      In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung ist die Kategorie grau hinterlegt, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Vergehensfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Felder für Security Incidents auf der rechten Seite beim Nachverfolgen der bereits zugeordneten SIR-Incident-Felder.



Hinweis:
Da für denselben Security Incident mehrere erkennbare Elemente angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der mehrere Optionen ausgewählt werden können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident ebenfalls nicht ausgefüllt.

   c. Geben Sie alternativ einen Wert in das Feld Suchen für die neue Zeile ein.
   d. Wählen Sie auf der linken Seite des Formulars das Feld für den Vergehen aus, und ziehen Sie es per Drag-and-Drop in ein geeignetes Feld für Security Incidents auf der rechten Seite.
4. Entfernen Sie Felder, indem Sie das Symbol – neben dem Feldnamen im Abschnitt „SIR-Incident-Feldzuordnung“ verwenden.
5. Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.

Vergehensfelder mit mehreren Werten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Incident-Felder wie **Kategorie** und **Anwender** (z. B. Betroffener Anwender, Zugewiesen an), die mit dem Basisprodukt verfügbar sind, unterstützen nicht mehrere Werte.
- Die folgenden IBM QRadar -Felder unterstützen mehrere Werte:
  - *Kategorien*
  - *target_networks*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*
  - *rule_contributing_to_offense*
  - *Benutzer*

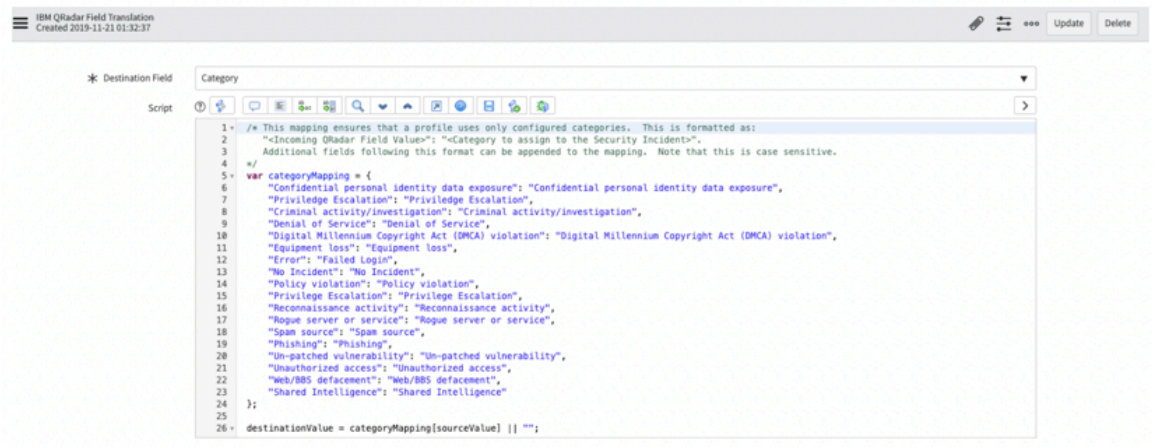
  Wenn Sie die obigen Felder anderen Security Incident Response -Feldern als CI-Feldern und Feldern des Typs „Erkennbares Element“ zuordnen müssen, müssen Sie neue Security Incident Response -Felder vom Typ „ **Liste“** erstellen und für die Zuordnung verwenden.

Hinweis:
Standardmäßig werden nur Nicht-Referenzfelder vom Typ **Liste** unterstützt.

Formatfeldübersetzung

In bestimmten Fällen werden Feldwerte für Vergehen in IBM QRadar möglicherweise nicht direkt in die Felder im SIR-Security Incident übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten. Beispielsweise können mit dem Skript-Editor die Kategoriewerte „Malware-Warnung“ und „Virusinfizierung“ unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mithilfe des Formats in eine gemeinsame böswillige Code-Aktivität im Feld „Kategorie“ des SIR-Security Incident übersetzt werden Feldübersetzungsfunktion.

Um den Skript-Editor zu verwenden, klicken Sie auf das {}:. Der Skript-Editor wird angezeigt.



Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen für Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um festzulegen, welche Vergehen Security Incidents erstellen und welche Vergehen herausgefiltert werden sollen, z. B. Vergehen mit niedriger Priorität. Dieselben Feldwerte können Sie im Builder für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Vergehen erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

1. Scrollen Sie im Formular zum Abschnitt **„Bedingungen für Incident-Generierung“,** und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen filtern,** um die Option zu aktivieren.

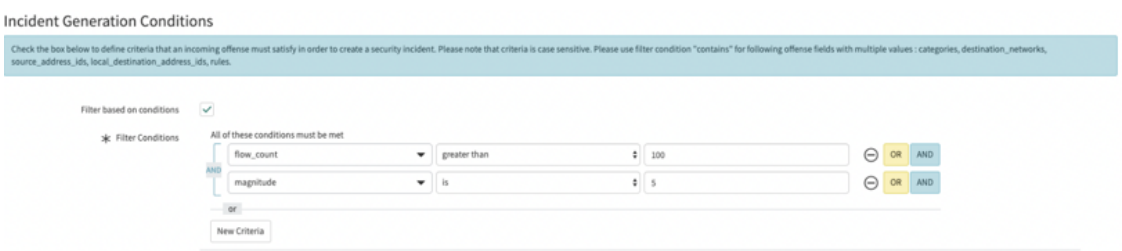
   Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt „Beispiel für QRadar-Vergehen – Erfassung“ für die von Ihnen erfassten Vergehen angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach den von Ihnen erfassten Vergehen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des Vergehens IBM QRadar übereinstimmen. Wenn Sie sich bei den Werten, die Sie in die Filterfelder eingeben sollen, nicht sicher sind, kehren Sie möglicherweise zu Ihrer IBM QRadar -Konsole zurück und überprüfen Ihre Vergehen auf die Schlüsselwörter.

   Hinweis:
   Die Felder *„category“*, *„ destination_networks“*, *„ source_address_ids“*, *„ local_destination_address_ids“*, *„remote_destination_ips“*, *„ rules_contributing_to_offense“*und *„users* Offense“ (Anwendervergehen) können mehrere Werte enthalten (da die Werte in Arrays gespeichert werden). Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie für diese Felder die Filterbedingung *„ Enthält “* verwenden, um sicherzustellen, dass die Daten ordnungsgemäß gefiltert werden.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **AND** oder **OR**.
   - Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.
4. (Optional) Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

   Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Bedingungen für die Incident-Generierung so festgelegt, dass Security Incidents nur erstellt werden, wenn die beiden von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Filterung von Bedingungen für die Incident-Generierung hilft Ihnen, die Vergehen einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Regel oder Filter in IBM QRadarzu ändern. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Vergehen, die allen Kriterien entsprechen, Incidents zugeordnet.

Hinweis:
Wenn einer der Vergehensfeldnamen Sonderzeichen wie Anführungszeichen (“), Bindestriche ('), Unterstriche (-) oder zeichenhafte Und-Zeichen (@) enthält, müssen diese Zeichen möglicherweise zu Filterzwecken ersetzt werden, es wird jedoch ein numerisches Suffix angehängt Differenzieren Sie Felder mit doppelten Vergehensnamen. Beispiel: Wenn das erste Vergehenfeld alerts.alert und das zweite Vergehenfeld alerts@alertsist, können diese Felder nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem Feld für den zweiten Vergehen ein Suffix hinzugefügt, und das Feld wird bei Anzeige in der Liste Filterbedingungen in alerts@alert(1) umbenannt.

Zusammenfassungskriterien für Vergehen, um ähnliche Vergehen zu behandeln und doppelte Incidents zu verhindern

Definieren Sie zusätzliche Kriterien für die Zusammenfassung von Vergehen, die einen eingehenden Vergehen zu einem vorhandenen SIR-Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Durch die Verwendung von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Daten zu Vergehen in einem einzigen Security Incident zusammengefasst werden. Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:

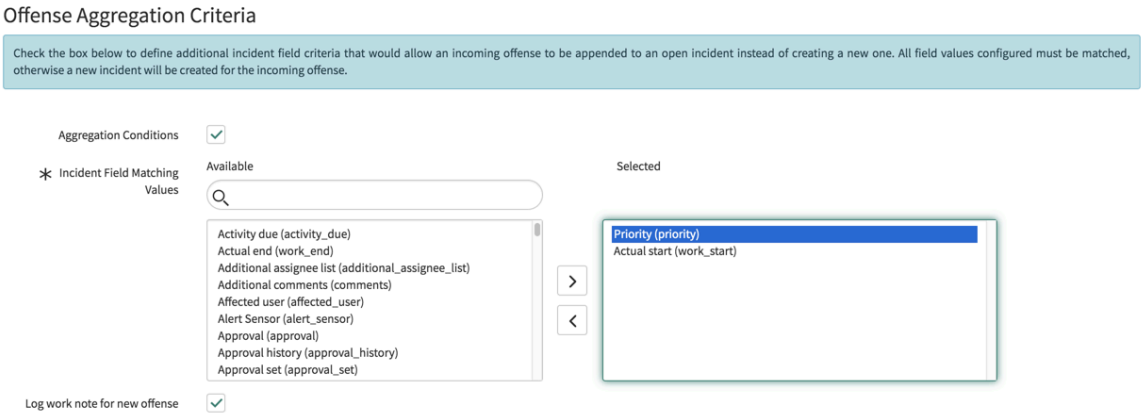
1. Scrollen Sie im Formular zum Abschnitt „Kriterien für die Strafzusammenfassung“, und aktivieren Sie das Kontrollkästchen **„Zusammenfassungsbedingungen“,** um diese Option zu aktivieren.

   Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die im Security Incident SIR konfiguriert sind.

2. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die mit vorhandenen Security Incidents in Now Platform abgeglichen werden sollen, und verschieben Sie sie in die Liste Ausgewählt.

   Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, damit diese eingehende Warnung an einen vorhandenen Security Incident angehängt wird. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Vergehen-Feldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Zusammenfassung von Vergehen nicht erfüllt, und es wird ein neuer Security Incident erstellt. Screenshot unten für Feldzuordnung mit mehreren Werten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn ein neuer Vergehen allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird der neue Vergehen automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der mit Security Incidents arbeiten, können Sie alle hinzugefügten aggregierten Vergehen in einer zugehörigen Liste zu einem Security Incident anzeigen. Diese Liste enthält Details zu zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese Vergehen mit vorhandenen Security Incidents aggregiert werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter „Zugehörige Links“ zur linken Seite des Datensatzes, und klicken Sie auf den Link **Alle zugehörigen Listen anzeigen**.

3. (Optional) Um eine Arbeitsnotiz für einen neuen Vergehen zu protokollieren, der kürzlich dem Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren. Die Arbeitsnotiz protokolliert, dass ein neuer Vergehen hinzugefügt wurde, zusammen mit einem Link zu den Vergehensdetails und allen anderen Details, die möglicherweise dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben erfolgreich Werte aus einem Vergehen IBM QRadar Feldern in einem Security Incident zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben Vergehen auch an vorhandene Security Incidents angehängt, wenn Feldwerte für Vergehen den konfigurierten Zusammenfassungskriterien entsprechen.

4. Klicken Sie auf **„Fortsetzen** “, um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht in der Vorschau der Felder, die Sie im Security Incident SIR zugeordnet haben

Zeigen Sie eine Vorschau des Security Incident für die -Integration IBM QRadar an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Security Incident SIR zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Vergehen-Felder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

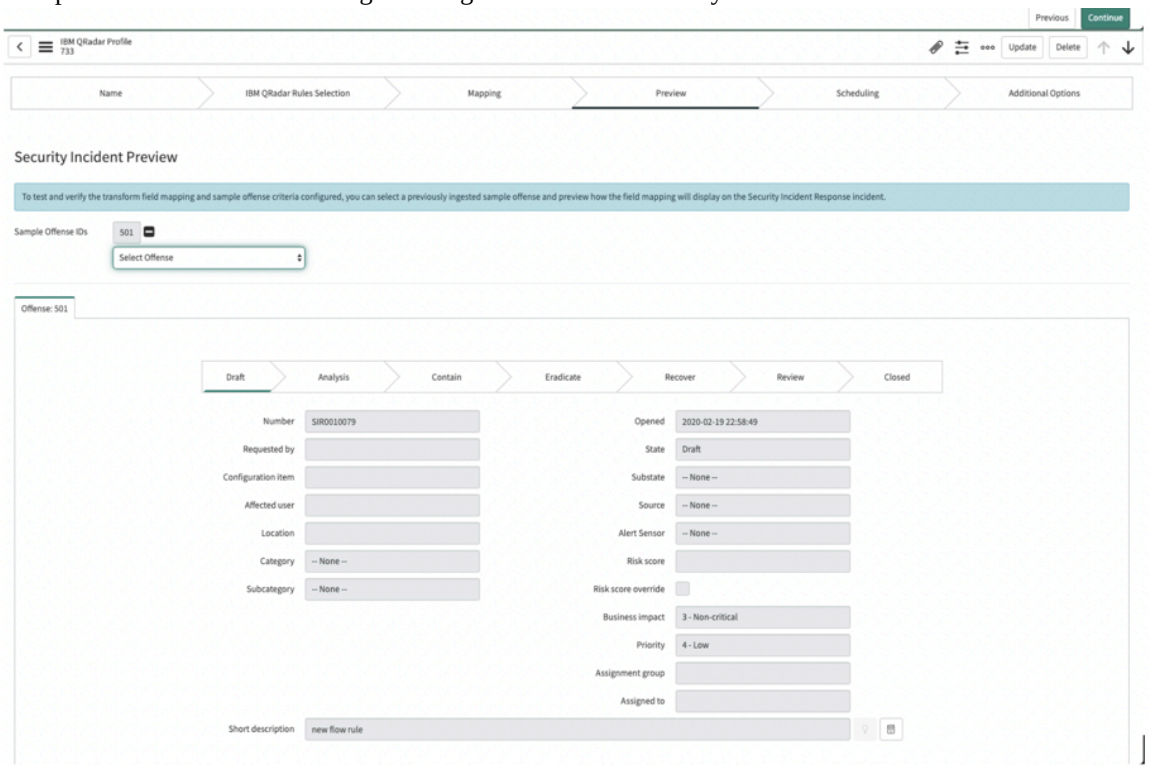
Als Benutzer mit der Rolle sn_si.admin können Sie die Vorschau eines Security Incident anzeigen und die Zuordnung nach Bedarf erneut bearbeiten, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wird, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incidents SIR werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

Prozedur

1. Wenn die Vorschau des Security Incidents nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Vorschau**.
2. Wählen Sie in der Auswahlliste Beispiel-Angriffs-IDs ein Element aus.
   Der Security Incident wird angezeigt. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Vergehenswerte im Security Incident.



   Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in den -Fehlermeldungen beschrieben werden.

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung im Security Incident zufrieden sind, besteht der nächste Schritt in der Definition des Zeitplans.

Definieren Sie einen Zeitplan für die Integration IBM QRadar .

Sie können den Zeitplan für die Erfassung des Vergehens definieren. Während dieses Schritts können Sie die Standardeinstellungen für den Abruf des Vergehens überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische Vergehen anhand eines Datumsbereichs abrufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können auswählen, ob Sie historische Vergehen während des Schritts „Zeitplanung“ erfassen möchten. Sie können auch auswählen, wie häufig Sie Abfragen für zukünftige neue und aktualisierte Vergehen durchführen, die der Profilkonfiguration entsprechen.

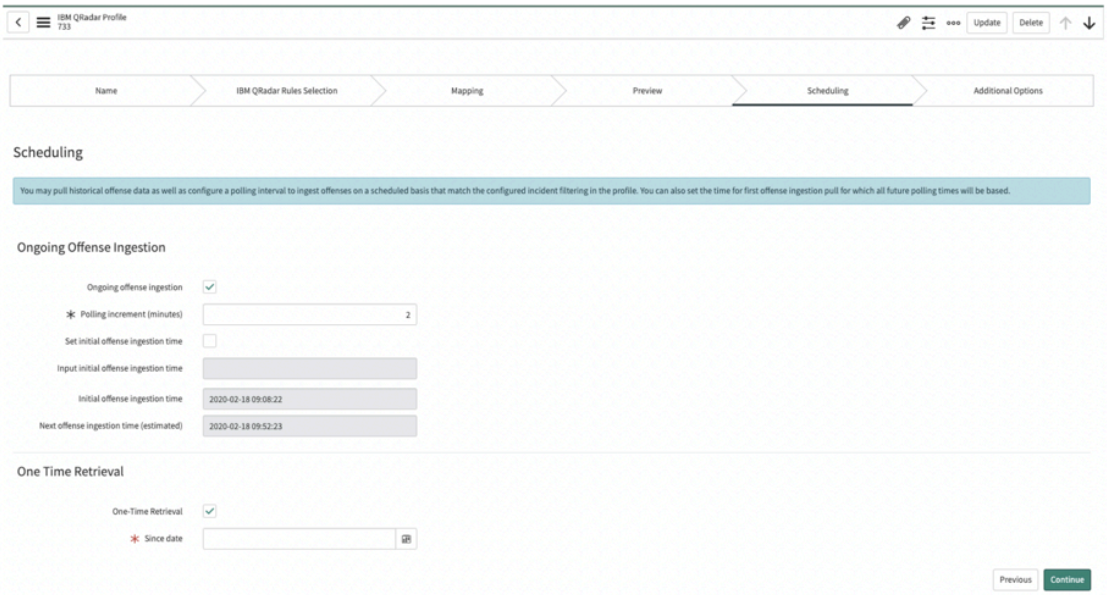
Als Benutzer mit der Rolle sn_si.admin konfigurieren Sie diese Abfrageintervalle für einzelne Profile. Die Leistung der IBM QRadar -Integration zur Erfassung von Straftaten kann durch die unterschiedlichen Abfrageintervalle beeinträchtigt werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrageaufwands auf dem Server IBM QRadar mit dem Wunsch in Einklang bringen, so bald wie möglich benachrichtigt zu werden, wenn ein Vergehen erstellt oder aktualisiert wird. Für jedes Profil ist ein Standardwert von fünf Minuten festgelegt. Bei Bedarf können Sie diese Einstellung jedoch auch auf einen Wert von nur einer Minute ändern.

Abrufen neuer und aktualisierter Vergehen

Wenn der Abfragezeitplan festgelegt ist, ruft die geplante Aufgabe sowohl neue als auch aktualisierte Vergehen ab, die zuvor abgerufen wurden, aber die Filterkriterien für Incidents nicht erfüllt haben. Dies gibt Ihnen die Flexibilität, Incidents basierend auf Kriterien zu erstellen, die bei der ersten Erstellung eines Vergehen möglicherweise nicht vorhanden sind, aber nach einer Aktualisierung verfügbar werden, z. B. während der Untersuchungsphase. Nachdem ein Incident für einen bestimmten Vergehen erstellt wurde, werden nachfolgende Updates ignoriert, da zu erwarten ist, dass der Vergehen jetzt als aktiver ServiceNow Security Incident behandelt wird. Alle anderen Vergehen, die zuvor erfasst wurden, aber die Kriterien für die Incident-Generierung nicht erfüllen, werden weiterhin abgerufen und anhand der Kriterien für die Incident-Generierung überprüft, bis sie Teil eines aktiven Incidents werden.

Prozedur
1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **„Zeitplanung“**aus.
2. Wählen Sie eine aus, um zu planen, wie und wann Vergehen aus der Konsole IBM QRadar abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **„Fortsetzen** “, um zur Seite „Zusätzliche Optionen“ zu navigieren.

Automatisieren Sie die Aktualisierung und den Abschluss von Vergehen basierend auf dem SIR-Incident-Status

Die IBM QRadar -Integration verfügt über eine bidirektionale Schnittstelle, die es ermöglicht, bei Vergehen durch Vergehen Security Incidents zu erstellen und/oder mit relevanten Incident-Details wie Security Incident-Nummer und Zuweisung zu schließen Gruppe, Security Incident-URL usw.

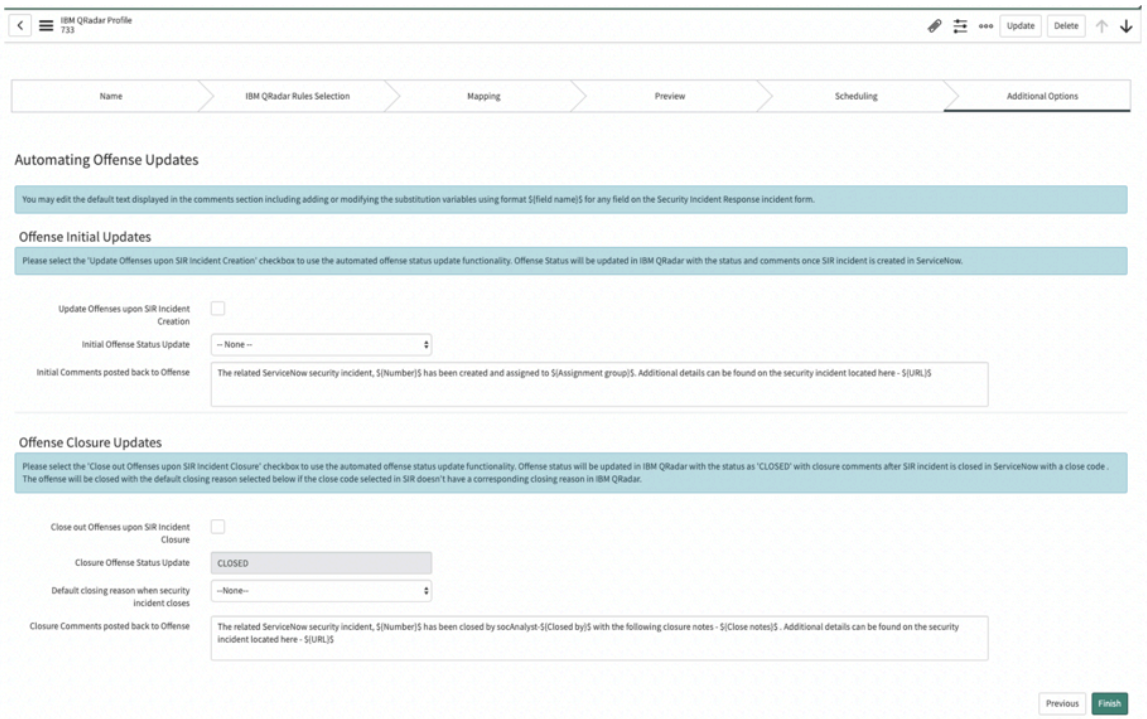
Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration für die Aktualisierung von Vergehen abzuschließen, wenn der Security Incident erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen und das Profil in den Status **Warten** zu versetzen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um -Angriffe basierend auf Ihrer Planung aus der -Konsole IBM QRadar abzurufen.

IBM QRadar Konfigurationseinstellungen für die Integration

Verwenden Sie diese Option, um die Standardsystemeigenschaften der IBM QRadar -Erfassungsintegration zu ändern.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Integrationseinstellungen**.

IBM QRadar-Integrationseinstellungen

Eigenschaftsname	Beschreibung
Grenzwert für die Anzahl von Security Incidents erzwingen, die innerhalb von 24 Stunden erstellt werden können. sn_sec_qradar.max_si_per_day	Gibt die maximale Anzahl von Security Incidents an, die innerhalb von 24 Stunden erstellt werden können. • Typ: Ganzzahl • Standardwert: 1000
Erzwingt einen Grenzwert für die Anzahl von Vergehen, die zu einem einzelnen Incident zusammengefasst werden können. sn_sec_qradar.max_aggregation_per_si	Der Grenzwert der Vergehen-Zusammenfassung für einen Security Incident. Wenn beispielsweise 102 Vergehen vorliegen, werden die ersten 100 Vergehen zu „Security Incident_1“ und die verbleibenden 2 zu „Security Incident_2“aggregiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM QRadar-Integrationseinstellungen (Fortsetzung)

Eigenschaftsname	Beschreibung
	• Typ: Ganzzahl • Standardwert: 100
Diese Eigenschaft legt den Zeitraum von AQL fest, um die neuesten Ereignisse/Flows für einen bestimmten Vergehen abzurufen. sn_sec_qradar.on_demand_recent_days_limit	Gibt die Anzahl der Tage für den Abruf der neuesten Ereignisse oder Flows für einen bestimmten Vergehen an. • Typ: Ganzzahl • Standardwert: 7
Diese Eigenschaft begrenzt die Anzahl der kürzlichen Ereignisse, die für einen bestimmten Vergehen abgerufen wurden. sn_sec_qradar.on_demand_event_limit	Gibt die Anzahl der Ereignisse an, die für einen Vergehen abgerufen werden. Die neuesten Ereignisse werden basierend auf dem Ereigniszeitstempel zuerst abgerufen. • Typ: Ganzzahl • Standardwert: 100
Diese Eigenschaft begrenzt die Anzahl der aktuellen Flows, die für einen bestimmten Vergehen abgerufen wurden. sn_sec_qradar.on_demand_flow_limit	Gibt die Anzahl der Flows an, die für einen Vergehen abgerufen werden. Die neuesten Flows werden basierend auf dem Flow-Zeitstempel zuerst abgerufen. • Typ: Ganzzahl • Standardwert: 100
Diese Eigenschaft legt den Zeitüberschreitungswert (Sekunden) für die AQL fest, die die neuesten Flows/Ereignisse für einen bestimmten Vergehen abruft. sn_sec_qradar.on_demand_timeout	• Typ: Ganzzahl • Standardwert: 300
Zeitüberschreitung der Such-IDs (Sekunden) für Datensätze in der Warteschlange zum Abfragen von AQLs eines Vergehens. sn_sec_qradar.sid_ttl	Die Zeitüberschreitung der AQL für einen Vergehen in der Warteschlange, bevor ein Security Incident erstellt wird. Wenn beispielsweise 90 Vergehen vorliegen, werden die ersten 50 Vergehen für AQL-Daten im ersten Batch verarbeitet und die verbleibenden 40 Vergehen im nachfolgenden Batch im selben Abfrageintervall. • Typ: Ganzzahl • Standardwert: 300
Schwellenwert zur Steuerung der Anzahl der Suchvorgänge, die in IBM QRadar gleichzeitig ausgeführt werden können und	Gibt die Anzahl der Vergehen an, die Sie in einem einzelnen Batch in einem Abfrageintervall abrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM QRadar-Integrationseinstellungen (Fortsetzung)

Eigenschaftsname	Beschreibung
durch die geplante Integration ausgelöst werden job.sn_sec_qradar.records_threshold_in_que_for_aql	• Typ: Ganzzahl • Standardwert: 50
Dies ist die Anzahl der Tage für die Bereinigung von Integrationstabellen. sn_sec_qradar.queue_item_expire	Im Folgenden finden Sie die Integrationstabellen: • sn_sec_qradar_events: IBM QRadar-Ereignisse • sn_sec_qradar_flows: IBM QRadar-Flows • sn_sec_qradar_offense_updates: IBM QRadar – Offense-Updates • sn_sec_qradar_offense_to_task: IBM QRadar-Vergehen bei Aufgabe • Typ: Ganzzahl • Standardwert: 30
Grenzwert für Vergehen pro geplanter Aufgabe, die pro Profil ausgeführt werden, entweder beim einmaligen Abruf oder bei der laufenden Erfassung. sn_sec_qradar.max_offense_limit_per_run	Gibt die Anzahl der Vergehen an, die Sie in einem einzelnen Abruf in die Now Platform abrufen. • Typ: Ganzzahl • Standardwert: 1000
Legen Sie diese Eigenschaft fest, um die Funktion „Angriffsaktualisierungen“ zu aktivieren. sn_sec_qradar.get_offense_updates	**Hinweis:** Das Aktivieren dieser Einstellung kann zu einer Verzögerung beim Erstellen eines Security Incident führen. • Typ: true| Falsch • Standardwert: falsch

Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

Optional: Kopieren Sie ein IBM QRadar -Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich möglicherweise, Profile zu kopieren, um Zeit zu sparen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname zunächst geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil

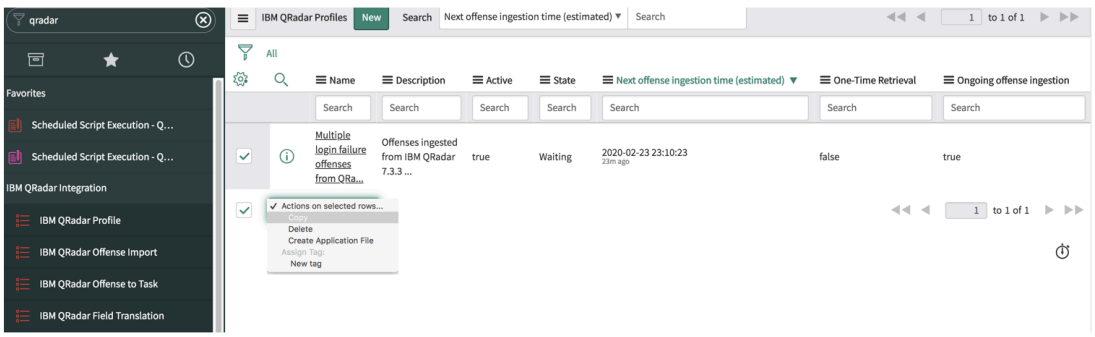
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

deaktiviert (falsch), damit es nicht versehentlich aktiviert wird, bevor die Konfiguration abgeschlossen wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

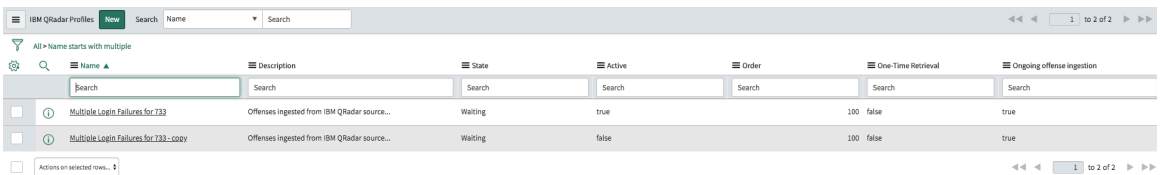
Prozedur

1. Navigieren zu **Alle** > **Integration mit IBM QRadar** > **IBM QRadar-Profil**.
2. Wählen Sie in der angezeigten Liste der IBM QRadar-Profile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Zeitplankonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie an dieser Stelle deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.

Hinweis:
Wenn Sie eine andere Quelle für das Profil auswählen, müssen Sie neue Regeln (Wählen Sie IBM QRadar Regeln aus) für das Profil auswählen. Wenn Sie jedoch dieselbe Quelle verwenden und neue Regeln auswählen, werden die Beispielvergehen gelöscht.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **„Aktiv“** auf „falsch“ festgelegt ist, da das Profil aktiviert werden muss.

Nächste Maßnahme
Sie werden aufgefordert, das neue Profil zu aktivieren, nachdem Sie die Konfigurationsschritte abgeschlossen haben.

Domain Separation und IBM QRadar Offense Ingestion

Domänentrennung wird bei der Vergehenserfassung von IBM QRadar unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

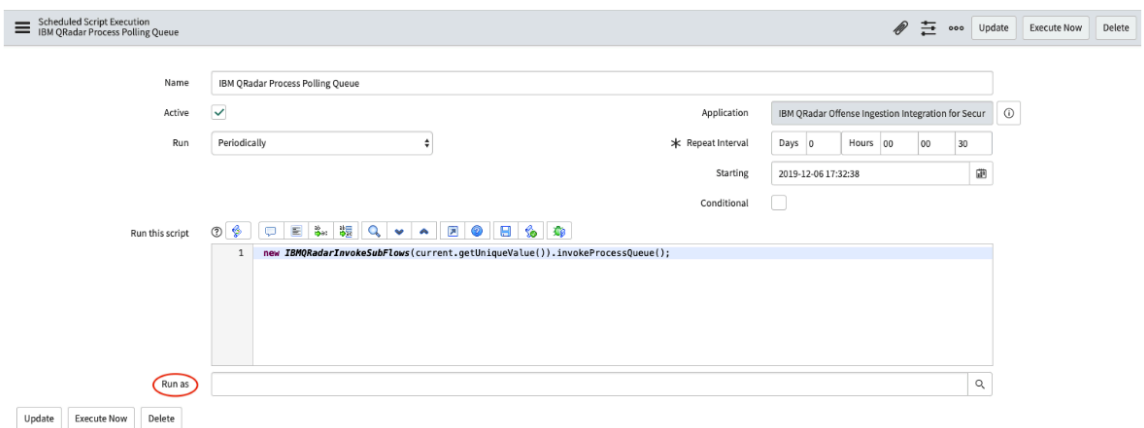
Funktionsweise der Domänentrennung in IBM QRadar Erfassung von Vergehen

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

- Erstellen Sie in der entsprechenden Domäne einen Benutzer mit der Rolle `sn_si.admin`.

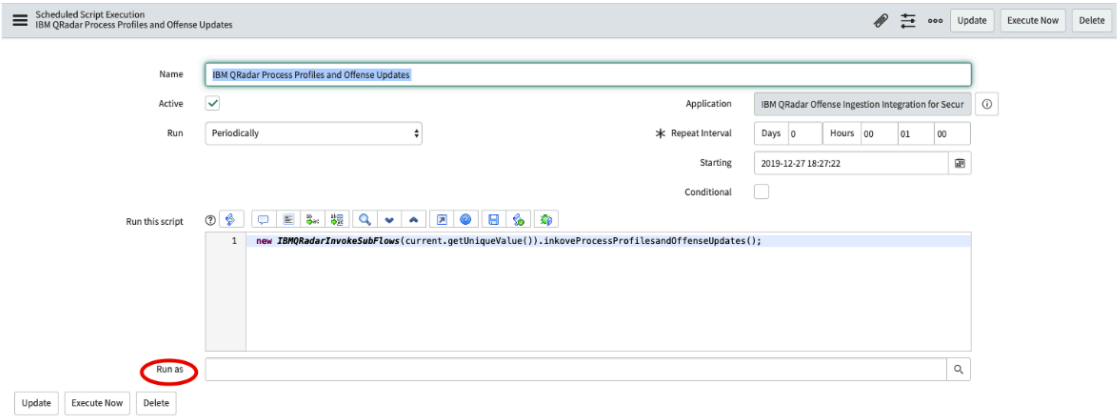
> **Hinweis:**
> Wenn Sie das Profil erstellen, verwenden Sie die Domänenauswahl, um die gewünschte Domäne auszuwählen. Erstellen Sie den Benutzer nicht in der übergeordneten Domäne, und ändern Sie später die Domäne des Profils. Sie müssen für jede Domäne einen bestimmten Benutzer für Ihr Profil mit der Rolle `sn_si.admin` haben. Verwenden Sie diesen Anwender, um Einstellungen im Profil zu erstellen oder zu ändern.

- Deaktivieren Sie vorhandene geplante Aufgaben.
- Replizieren Sie die Prozessabfragewarteschlange IBM QRadar, die Prozessprofile IBM QRadar und die geplanten Aufgaben zur Vergehensaktualisierung für jede Domäne.
- Ändern Sie **Ausführen als** vom Systembenutzer in den Benutzer mit der Rolle `sn_si.admin` in der entsprechenden Domäne, und führen Sie die geplante Aufgabe aus.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zugehörige Informationen

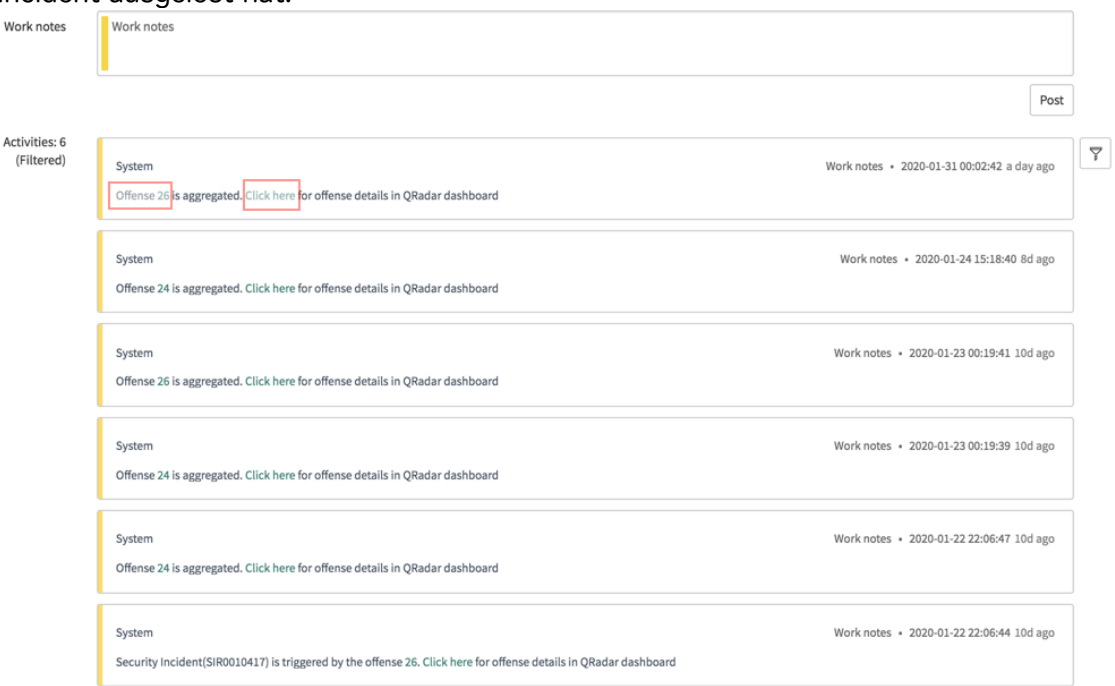
Domänentrennung für Service Provider

Formular „Security Incident Response“ nach Erfassung eines Vergehens

Nachdem ein Verstoß gegen IBM QRadar erfasst wurde, wird ein Security Incident erstellt, und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

Arbeitsnotiz

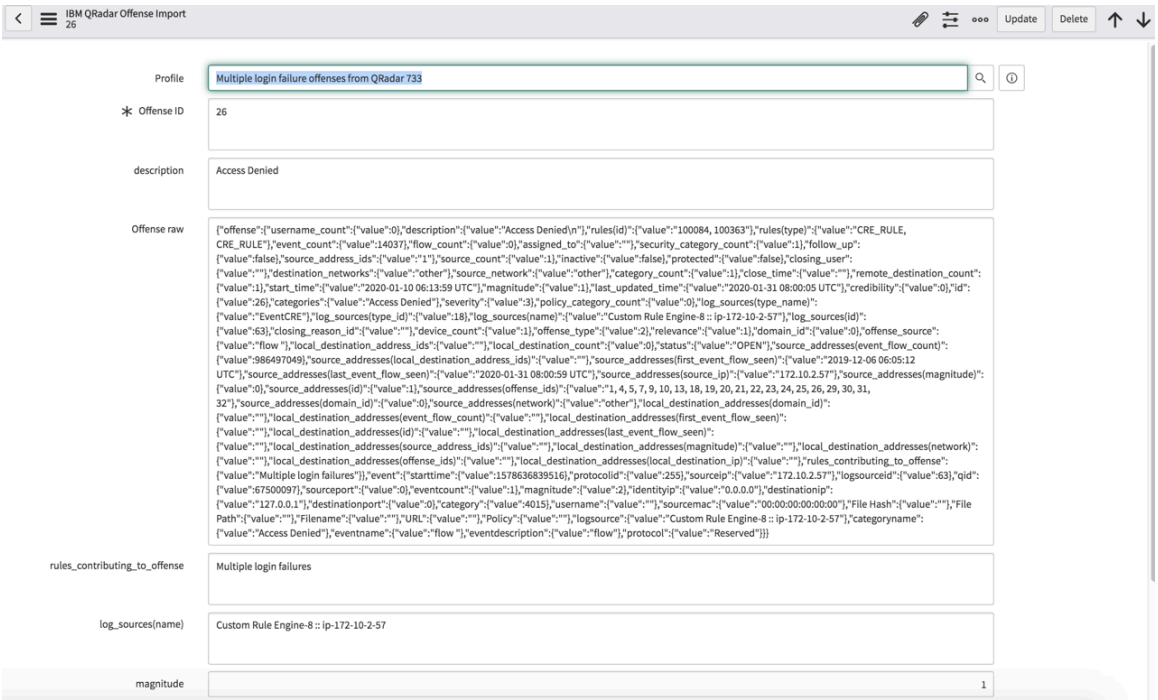
Es wird eine Arbeitsnotiz mit Details zu dem Vergehen veröffentlicht, das den Security Incident ausgelöst hat.



Klicken Sie auf den Link für den Vergehen, um zum Datensatz des internen Security Incident zu navigieren. Über den Hyperlink **Hier klicken** gelangen Sie zum Dashboard IBM QRadar, in dem Sie die Vergehensdetails anzeigen können.

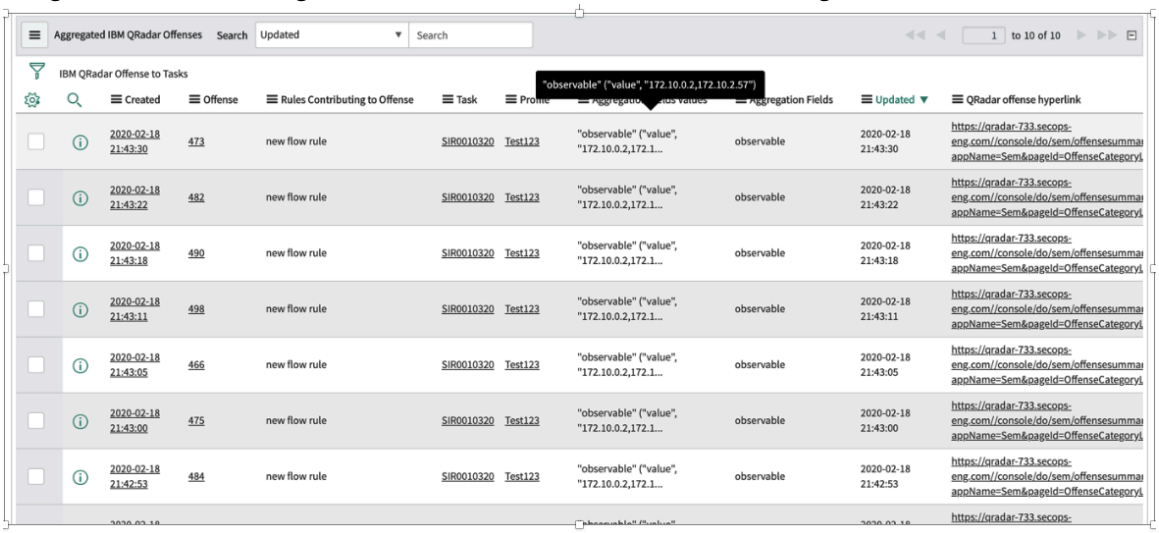
Wenn Sie die Option **Arbeitsnotiz für neuen Vergehen protokollieren** in den Kriterien für die Zusammenfassung von Vergehen ausgewählt hatten, wie in IBM QRadar -Vergehensfelder werden Security Incident-Antwortfeldern zugeordnetbeschrieben, wird bei der Zusammenfassung des Vergehen eine Arbeitsnotiz veröffentlicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aggregierte Vergehen

Klicken **Zugehörige Listen** > **Aggregierte IBM QRadar-Vergehen** um die für den Security Incident aggregierten Vergehen anzuzeigen. Klicken Sie auf den Hyperlink für QRadar-Vergehen, um den Vergehen im Dashboard IBM QRadar anzuzeigen.

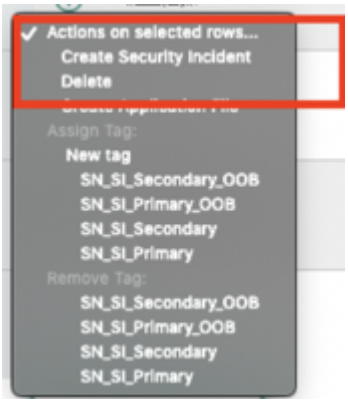


Security Incident erstellen: Wählen Sie einen Vergehen aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie auf **Security Incident erstellen**. Durch diese Option wird ein Security Incident für den Vergehen erstellt, und für diesen Vergehen wird die Zusammenfassung des übergeordneten Security Incident aufgehoben.

Vergehendatensatz löschen: Wählen Sie einen Vergehen aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie auf **Löschen**. Mit dieser Option wird der Vergehensdatensatz gelöscht.

Automatische Übersetzung

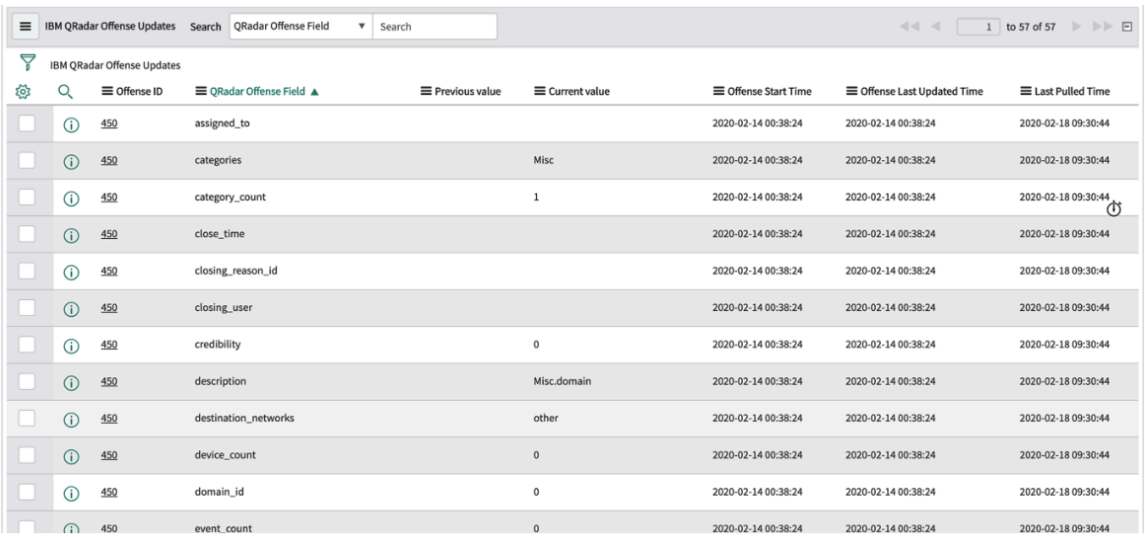
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



IBM QRadar-Vergehensaktualisierungen

Dies zeigt die Standard- und anwenderdefinierten Vergehen-Felder und verfolgt Änderungen am Vergehen während jedes Abfrageintervalls. Dies ist hilfreich, da Sie alle Vergehensaktualisierungen direkt anzeigen können, ohne zum Dashboard IBM QRadar navigieren zu müssen. Alle Änderungen an den Werten werden in den Feldern Vorheriger Wert und Aktueller Wert angezeigt.

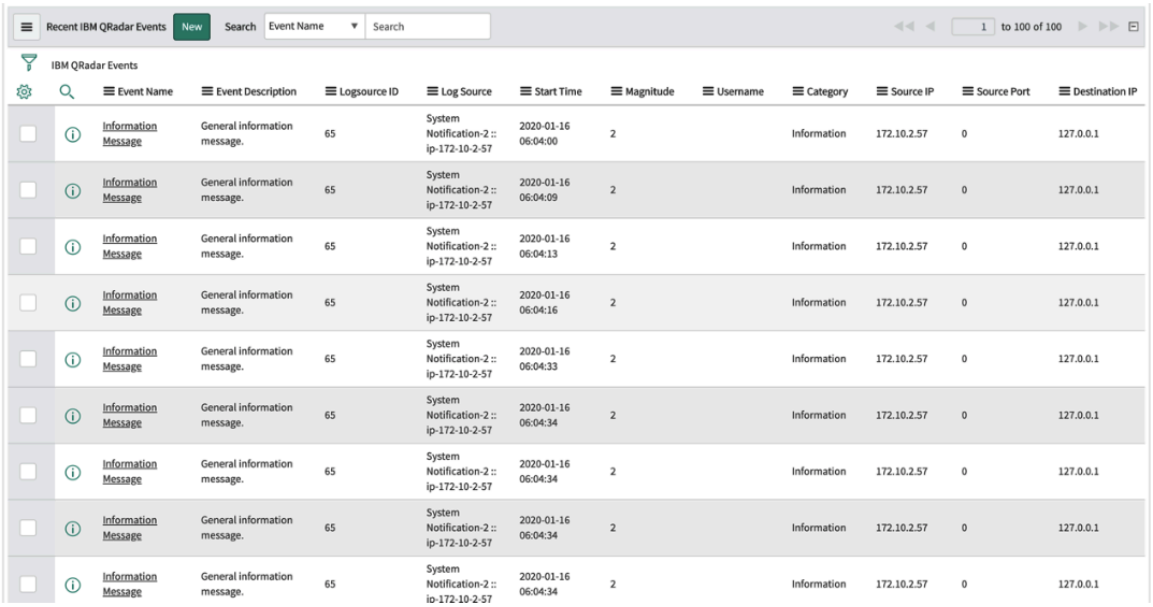
Um die Funktion zur Aktualisierung von Vergehen zu aktivieren, navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Integrationseinstellungen** und aktivieren Sie **Diese Eigenschaft festlegen, um die Funktion zur Aktualisierung von Vergehen zu aktivieren**. Standardmäßig ist diese Einstellung deaktiviert.



Letzte IBM QRadar-Ereignisse

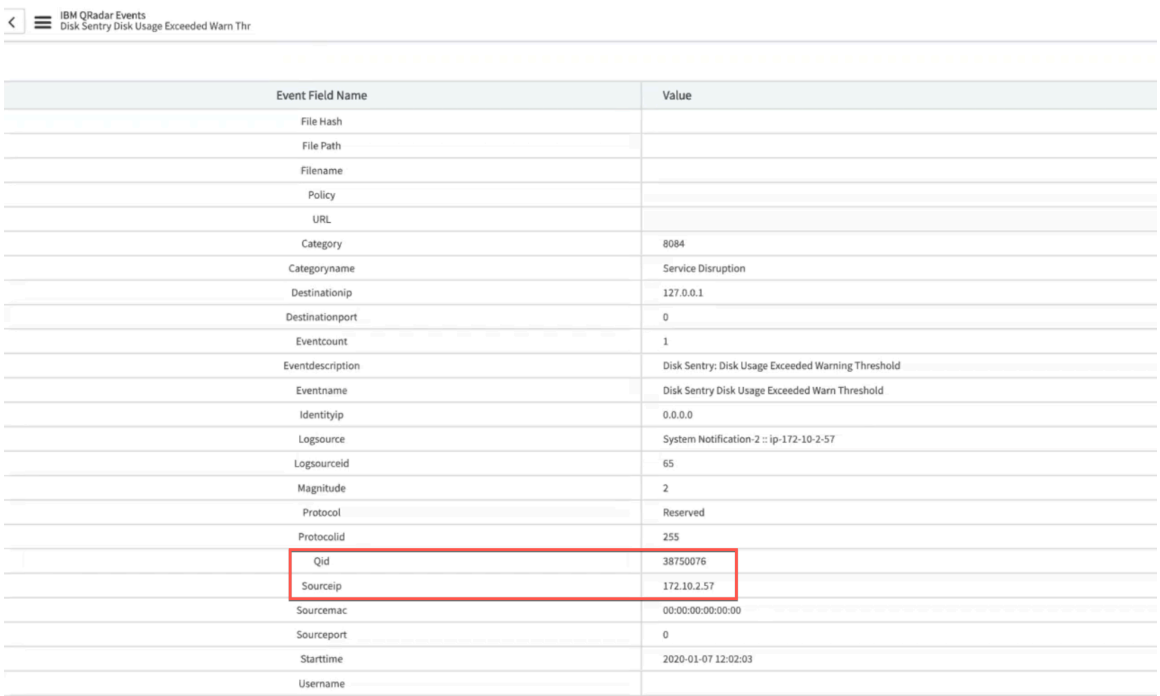
Klicken Sie unter „ **Zugehörige Links“** auf die Option **Aktuelle IBM QRadar-Ereignisse abrufen,** um die neuesten IBM QRadar -Ereignisse anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Standardmäßig werden maximal 100 Ereignisse angezeigt. Sie können diese Standardeinstellung unter IBM QRadar Konfigurationseinstellungen für die Integrationändern.

Hinweis:
Die obige Abbildung zeigt die Standardereignisfelder, die dem Vergehen zugeordnet sind. Wenn Sie anwenderdefinierte Ereignisfelder konfiguriert und zugeordnet haben (siehe IBM QRadar -Vergehensfelder werden Security Incident-Antwortfeldern zugeordnet), können Sie sie in der Listenansicht anzeigen, indem Sie auf den Link Ereignisname klicken.

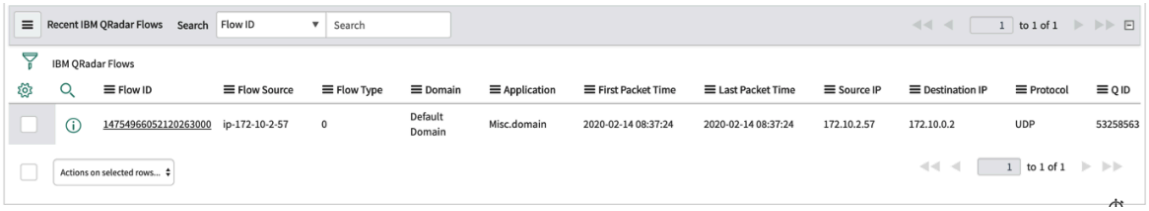


Aktuelle IBM QRadar-Flows

Bei Verwendung von Integration Hub und Flow Designer sind mit der Integration IBM QRadar mehrere Flows, Subflows und Aktionen verfügbar. Wenn Sie unter den zugehörigen Links auf die Option **Aktuelle IBM QRadar-Flows abrufen** klicken, werden die neuesten Flows

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

abgerufen. Um diese Flows anzuzeigen, klicken Sie auf **Recent IBM QRadar Flows (Aktuelle IBM QRadar-Flows)**.



Standardmäßig werden maximal 100 Flows angezeigt. Sie können diese Standardeinstellung unter IBM QRadar Konfigurationseinstellungen für die Integrationändern.

Hinweis:
Die obige Abbildung zeigt die Standard-Flow-Felder, die dem Vergehen zugeordnet sind. Wenn Sie anwenderdefinierte Flow-Felder (siehe IBM QRadar -Vergehensfelder werden Security Incident-Antwortfeldern zugeordnet) konfiguriert und zugeordnet haben, können Sie sie in der Listenansicht anzeigen, indem Sie auf den Link Flow ID klicken.

Verwendung von Flow Designer und Integration Hub mit IBM QRadar-Integration zur Vergehenserfassung

Unter Verwendung der Funktionalität von Flow Designer und Integration Hub wurden mehrere Subflows und Aktionen als Teil der IBM QRadar -Integration zur Vergehenserfassung erstellt.

Die folgenden IBM QRadar -Subflows sind verfügbar:

- Validierung von Verbindungs- und Anmeldeinformationen: Wird in der Konfigurationskachel zum Validieren des Hosts und der Anmeldeinformationen beim ersten Setup verwendet.
- IBM QRadar-Regelabruf: Wird im Abschnitt „Regeln“ des Profil-Setups verwendet, um alle aktiven Regeln in IBM QRadarabzurufen. Dieser Subflow wird asynchron ausgelöst.
- Beispieldaten zu Straftaten aus IBM QRadar abrufen: Wird im Abschnitt „Zuordnung“ des Profil-Setups verwendet, um Beispieldaten abzurufen. Dieser Subflow wird asynchron ausgelöst.
- IBM QRadar – Statusaktualisierungen für Vergehen: Wird jede Minute von einer geplanten Aufgabe ausgelöst und aktualisiert den Vergehen in IBM QRadar, wenn der Security Incident erstellt oder geschlossen wird.
- Profile aus geplanten Aufgaben und Warteschlangenvergehen verarbeiten: Dies wird jede Minute von einer geplanten Aufgabe ausgelöst, um Vergehen pro Profil basierend auf dem Abfrageintervall abzurufen. Dadurch werden Vergehen abgerufen und zur weiteren Verarbeitung in die Abfragetabelle gestellt.
- Abfragewarteschlange und Abfrage in Batches verarbeiten: Dies wird alle 30 Sekunden von einer geplanten Aufgabe ausgelöst, um die Abfragetabellenwarteschlange zu verarbeiten.
- Aktuelle IBM QRadar-Flows abrufen: Wird über den Link des Security Incident-Formulars ausgelöst, um die neuesten Flows des Vergehens abzurufen.
- Aktuelle IBM QRadar-Ereignisse abrufen: Wird über den Link des Security Incident-Formulars ausgelöst, um die neuesten Vergehensereignisse abzurufen.

Um diese Subflows anzuzeigen, melden Sie sich als Benutzer mit der Rolle `sn_si.admin` an, und navigieren Sie zu **Flow Designer** > **Designer**. Klicken Sie auf den Link Name eines der oben aufgeführten Subflows, um den Subflow im Detail anzuzeigen.

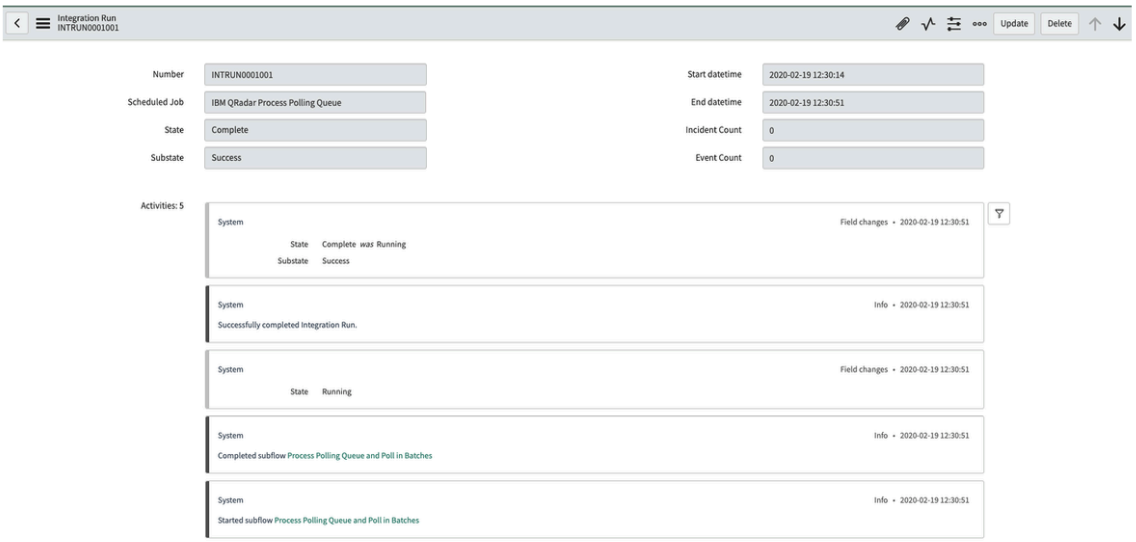
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung bei der Integration der Straftaterfassung IBM QRadar.

Dieser Abschnitt enthält wichtige Tipps zur Problembehandlung und häufig gestellte Fragen im Zusammenhang mit der Erfassung von Vergehen bei IBM QRadar.

- Integrationsausführung: Wenn die Ausführung einer geplanten Aufgabe beginnt, wird ein Integrationsausführungsdatensatz mit Protokollen, Fehlern und Warnungen angezeigt. Die Anzahl der abgerufenen Vergehen und die Anzahl der Incidents, die in einer Ausführung einer geplanten Aufgabe erstellt wurden, werden ebenfalls angezeigt. Benutzer mit der Rolle sn_si.analyst können sehen, ob das Abrufen von Fehlern/Profilen während der Integrationsausführung fehlgeschlagen ist.

  Arbeitsnotizen in der Integrationsausführung enthalten Links zu den ausgeführten Subflows. Benutzer mit der Rolle sn_si.analyst können die Tabelle sn_event_ingestion_integration_run auf aufgetretene Fehler überprüfen. Um Integrationsprobleme zu beheben, müssen Sie zuerst die Integrationsausführung überprüfen. Fehler werden als Arbeitsnotizen in den Datensätzen der Integrationsausführung für jede Ausführung einer geplanten Aufgabe protokolliert.



- SSL-Probleme: Stellen Sie beim Herstellen einer Verbindung mit Cloud-Instanzen IBM QRadar sicher, dass die Instanz über ein gültiges CA-Zertifikat verfügt, das nicht abgelaufen ist. Sie können RSA-Zertifikate oder eigene Zertifikate in die Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Details siehe https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 .
- Unvollständiges Profil: Klicken Sie bei der Konfiguration des Profils im Abschnitt „Zusätzliche Optionen“ (Automatisieren Sie die Aktualisierung und den Abschluss von Vergehen basierend auf dem SIR-Incident-Status) auf die Schaltfläche **Fertig stellen**, um sicherzustellen, dass das Profil in den Status „Warten“ versetzt wird und damit auf die Erfassung wartet.
- Profil validieren: Um zu validieren, ob die Integration ordnungsgemäß funktioniert, überprüfen Sie die Profilstatus, das Datum des letzten Abrufs des Profils, die Vergehensimporttabelle und die Datensätze der Vergehen-zu-Aufgaben-Tabelle.
- MID-Serverkonfiguration: Wenn Sie die Anwendung IBM QRadar lokal installieren, müssen Sie nach der Konfiguration des MID-Servers eine MID-Server-Anwendung erstellen. Der Name der MID-Server-Anwendung sollte auf der Kachel der Integrationskonfiguration anstelle des Namens des MID-Servers verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die standardmäßige Zeitüberschreitung für den MID-Server beträgt 30 Sekunden. Anweisungen zum Deaktivieren der Zeitüberschreitung finden Sie unter <link>. Beachten Sie, dass dies eine systemweite Änderung ist und sich auf andere Integrationen auswirken kann.

- Updates für Vergehen: Wenn Sie die Eigenschaft *sn_sec_qradar.get_offense_updates* aktiviert haben und eine Verzögerung bei der Erstellung von Security Incidents feststellen, deaktivieren Sie die Eigenschaft. Aktivieren Sie diese Eigenschaft nicht, wenn das Abfrageintervall niedrig und die Last der Vergehen in QRadar hoch ist, da dies die Warteschlangenlast erhöht.
- Fehlende Ereignisse, Flow-Daten, Remote-_IP oder Anwenderdaten in einem Security Incident: Wenn Sie feststellen, dass Event-, Flow-Daten, Remote-IP- oder Anwenderdaten in einem Security Incident fehlen, erhöhen Sie die Zeitüberschreitung (Sekunden) für den Parameter *„sn_sec_qradar.sid_ttl“*. Durch Erhöhen der Dauer wird die Erstellung des Security Incident verzögert, bis die AQLs die Analyse der einzelnen Vergehen abschließen.
- Zeitüberschreitungen: Wenn Sie Zeitüberschreitungsfehler in den Anwendungsprotokollen anzeigen, überprüfen und ändern Sie die folgenden Flow Designer-Aktionen:

Flow Designer-Aktionen

Parameter	Aktion
Beispielvergehen abrufen `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000);`	Überprüfen und aktualisieren Sie die Dauer in Millisekunden.
Beispielvergehen abrufen `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs);`	Fügen Sie einen Parameter für *executeAction* hinzu, und geben Sie die Dauer in Millisekunden ein.
Ruft Vergehen für Profil- und Warteschlangendatensätze in der Abfragetabelle ab `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000);`	Überprüfen und aktualisieren Sie die Dauer in Millisekunden.
Wrapper zum Testen der Verbindungs-REST `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs);`	Fügen Sie einen Parameter für *executeAction* hinzu, und geben Sie die Dauer in Millisekunden ein.
Wrapper für das REST zum Validieren der API-Anmeldeinformationen	Fügen Sie einen Parameter für *executeAction* hinzu, und geben Sie die Dauer in Millisekunden ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Aktion
`var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);`	
REST-Schritt für IBM QRadar Offense-Updates `var result = sn_fd.FlowAPI.executeAction('sn_sec_qradar.'+restStep, inputs,60000);`	Überprüfen und aktualisieren Sie die Dauer in Millisekunden.

IBM QRadar – Integration zur Ergänzung von Incidents

Die Integration IBM QRadar – Incident Enrichment durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Erste Schritte mit der Integration IBM QRadar - Incident Enrichment
- Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

Verwenden

- Führen Sie eine Sichtungssuche aus
- Security Operations Integration - Sichtungssuche-Flow
- Security Operations – QRadar-Sichtungssuch-Flow
- Zeigen Sie Details der Sichtungssuche an
- Sichtungssuchergebnisse anzeigen

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit der Integration IBM QRadar - Incident Enrichment

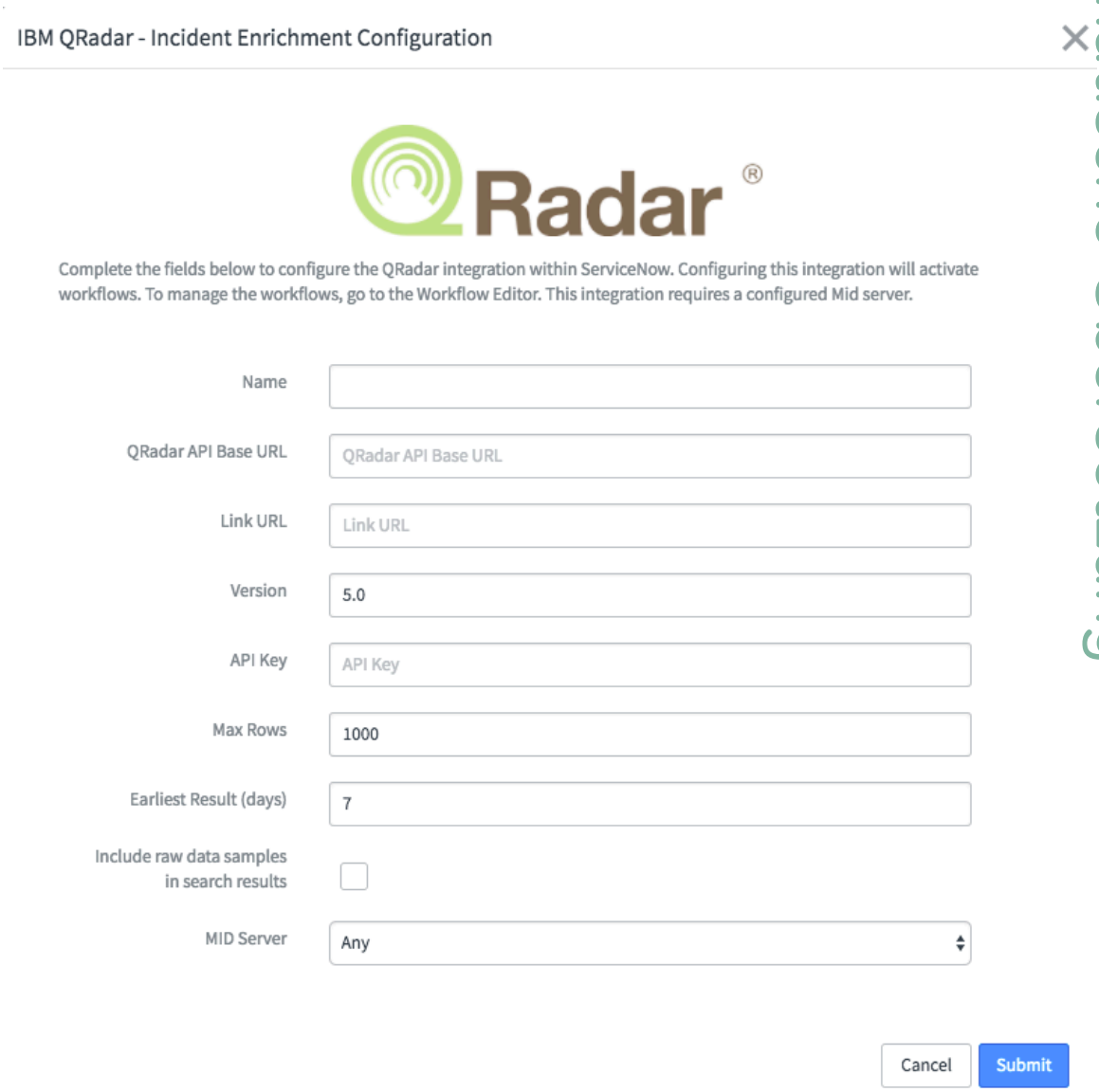
IBM QRadar ist ein SIEM-Produkt (Enterprise Security Information and Event Management), das sich problemlos in Security Operationsintegrieren lässt. Bevor Sie die Integration IBM QRadar - Incident Enrichment verwenden können, müssen Sie sie von ServiceNow Store herunterladen und die entsprechende API-Basis-URL und den API-Schlüssel hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, rufen Sie in Ihrem Profil IBM QRadar auf IBM QRadar auf, und rufen Sie die API-Basis-URL und den API-Schlüssel ab.
3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte IBM QRadar – Incident-Ergänzung **auf Neu**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der QRadar-API	Die Basis-URL, die Sie von der Website IBM QRadar erhalten haben.
Link-URL	[Optional] Die Link-URL, die auf eine Instanz IBM QRadar vom Typ verweist, falls verfügbar.
Version	Die Version IBM QRadar ; 5.0 ist der Standardwert.
API-Schlüssel	Der API-Schlüssel, den Sie von der Website IBM QRadar erhalten haben.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der **Anzahl der Zeilen der Rohdateneigenschaft** in den Security Incident Response-Eigenschaftenab.
MID-Server	Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern bzw. zu löschen.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

LogRhythm Übersicht

Die Flexibilität bei der Zuordnung dieser Integration bietet Analysten Einblick in Ereignisse und zugehörige Alarmdaten, die zur weiteren Untersuchung und Behebung in Security Incidents Now Platform von integriert werden können.

Alarmprofile werden in Ihrer Instanz Now Platform erstellt, um anzupassen, wie verschiedene LogRhythm -Alarmfelder für einen Now Platform -Security Incident angezeigt werden. Es wird eine Standardzuordnung von Alarmfeldern bereitgestellt, die bearbeitet werden kann, um kundenspezifische Anforderungen zu erfüllen.

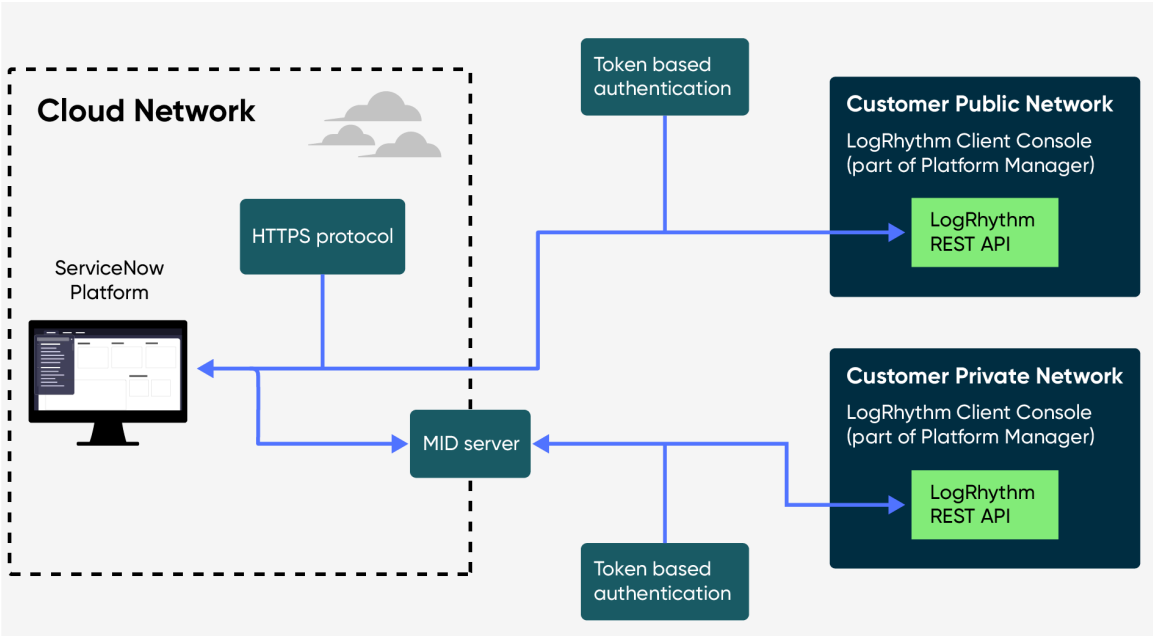
Die folgende Abbildung zeigt ein Beispiel für eine Kundenumgebung. Wenn ein Ereignis die Erstellung eines Security Incident in der Instanz Now Platform® auslöst, wird von Ihrer Instanz Now Platform® eine Anforderung gesendet, um Alarme aus der Clientkonsole LogRhythm entweder über einen MID-Server oder ohne diesen abzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der REST-API-Schlüssel wird von Now Platform® zur Authentifizierung bei der Clientkonsole LogRhythm verwendet. Über diese Verbindung kann Ihre Instanz Now Platform einzelne LogRhythm -Alarme basierend auf konfigurierten Profilen abrufen.

Die REST API wird zum Sammeln von Nachrichtendetails verwendet, auf die die REST API nicht zugreift.

LogRhythm-Integration



Schlüsselfunktionen

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Flexibilität zum Erstellen mehrerer Alarmprofile für verschiedene Alarmtypen wie Phishing und Malware.
- Drag-and-Drop-Zuordnung von LogRhythm -Alarmfeldwerten zu zugehörigen SIR -Security-Incident-Feldern.
- Eine Vorschau des SIR Security Incident-Layouts basierend auf LogRhythm Beispielalarmen.
- Erfassung historischer Alarme und laufender zukünftiger Alarme in konfigurierbaren Intervallen.
- Automatisiertes Schließen von LogRhythm -Alarmen nach Abschluss eines Incidents SIR von . Zur einfachen Referenz werden eine URL zum Incident SIR sowie eine Incident-ID bereitgestellt.

Unterstützte Releases von Now Platform

Diese Integration ist kompatibel mit den Releases Quebec oder höher von Now Platform®.

Unterstützte Versionen von LogRhythm

Diese Integration ist kompatibel mit LogRhythm 7.8 oder höher. Die früheren Versionen werden aufgrund von API-Einschränkungen nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die folgenden Themen sind nummeriert. Für eine reibungslose Installation und zur Überprüfung der erwarteten Ergebnisse führen Sie die Themen in der Reihenfolge aus, in der sie angezeigt werden.

Richten Sie die REST API für ein LogRhythm

Mit dem REST-API-Schlüssel LogRhythm können Sie zusätzliche Ereignisdetails für einzelne Alarmfelder erfassen. Der API-Schlüssel bietet Details, die mit der REST-API LogRhythm nicht verfügbar sind.

Vorbereitungen

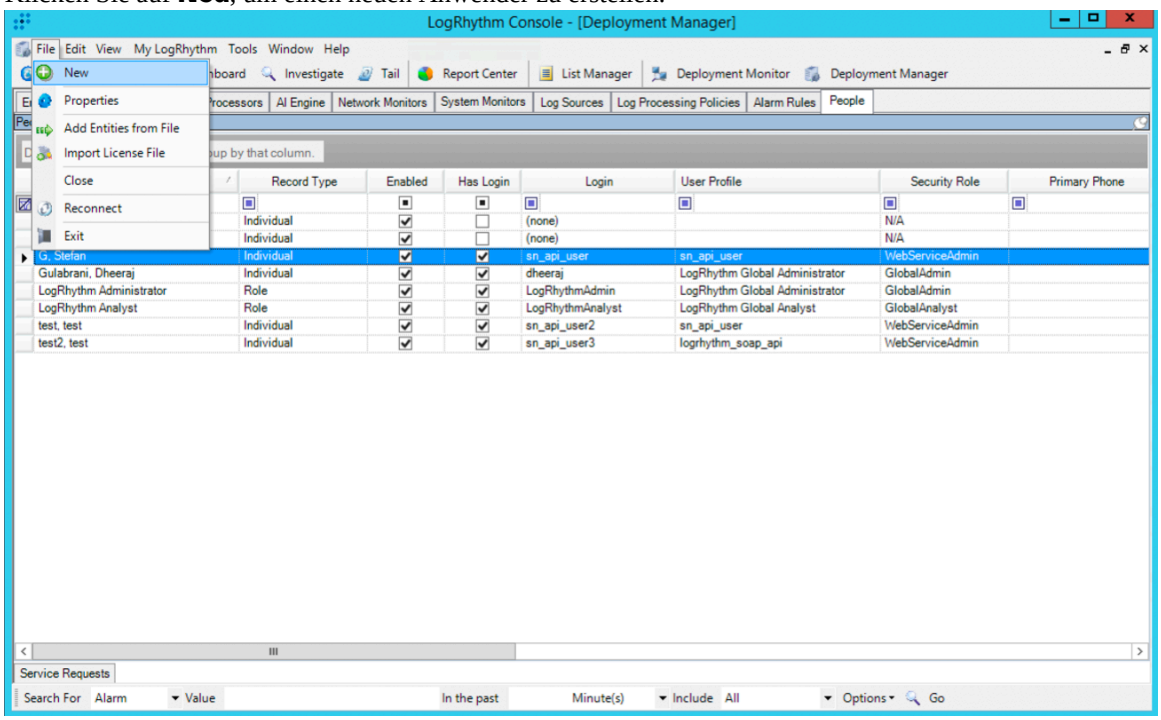
Erforderliche Rolle: LogRhythm Clientkonsolen-/Plattformmanager-Administrator

Warum und wann dieser Vorgang ausgeführt wird

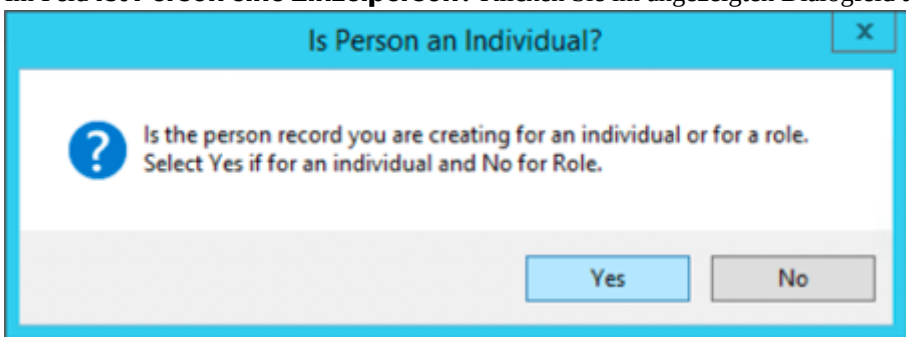
Diese Aufgabe wird in der Clientkonsole LogRhythm ausgeführt. Richten Sie die LogRhythm REST API ein, bevor Sie das Plugin von ServiceNow Storeinstallieren.

Prozedur

1. Navigieren Sie zur Client-Konsole LogRhythm, und wählen Sie das Menü **„Datei“**.
2. Klicken Sie auf **Neu**, um einen neuen Anwender zu erstellen.



3. Im Feld **Ist Person eine Einzelperson?** Klicken Sie im angezeigten Dialogfeld auf **Ja**.

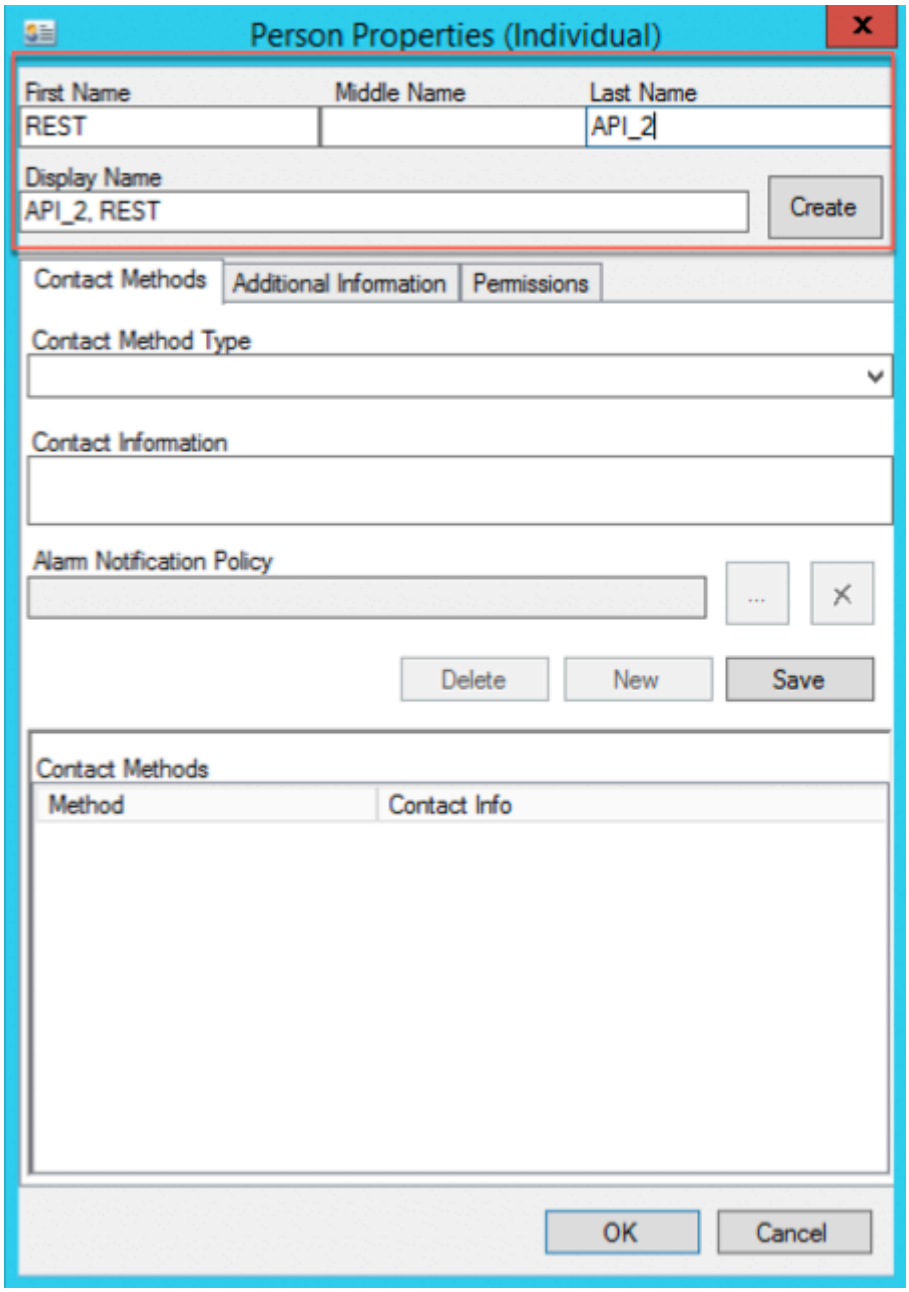


4. Füllen Sie im angezeigten Dialogfeld „Personeneigenschaften“ die Felder Name aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

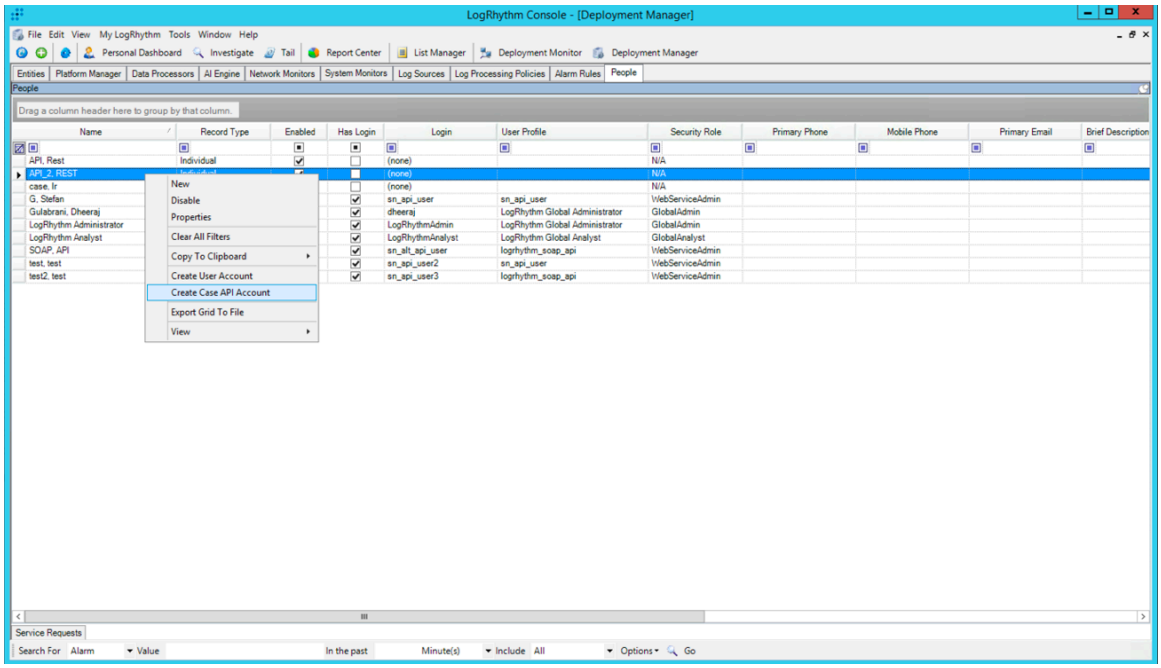
Verwenden Sie einen anderen Namen für die REST-API LogRhythm als den, den Sie zum Erstellen der REST-API verwendet haben, z. B. REST API_2.



5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf den neuen Eintrag in der Spalte Name (**API_2_REST**), und wählen Sie in der Auswahlliste **Create Case API Account (API-Account für Fall erstellen**).

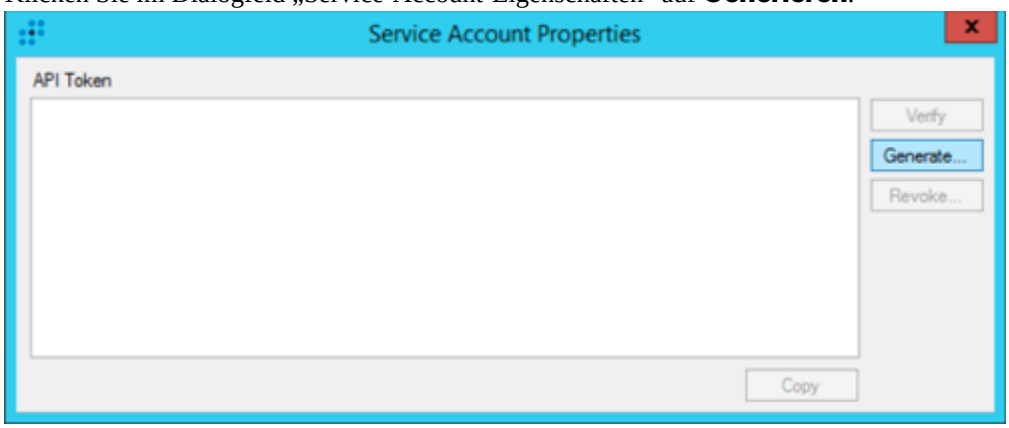
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

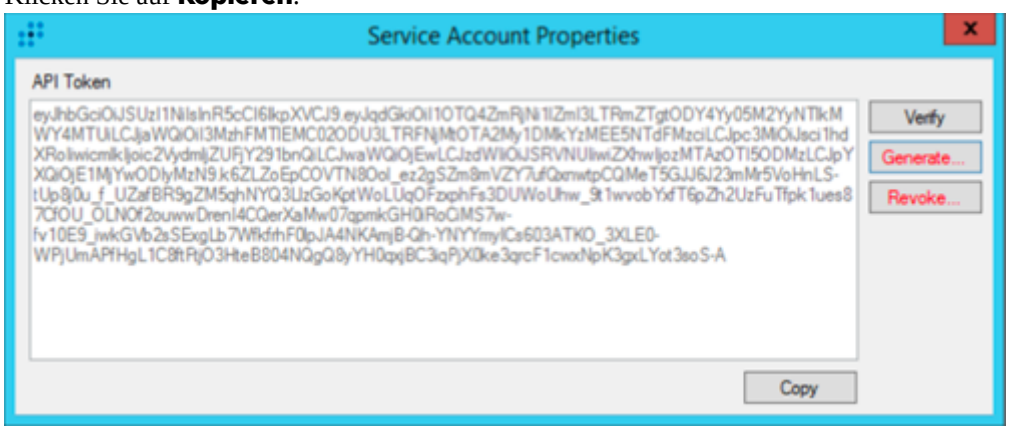


Hinweis:
Die Fall-API wird nicht verwendet, aber die Anmeldeinformationen für das Fall-API-Konto und die LogRhythm REST API sind identisch.

7. Klicken Sie im Dialogfeld „Service-Account-Eigenschaften“ auf **Generieren**.



8. Klicken Sie auf **Kopieren**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben jetzt die REST API LogRhythm eingerichtet. Sie fügen die Zeichenfolge, die Sie im vorherigen Schritt kopiert haben, während der in Installieren Sie das Plugin, und konfigurieren Sie es LogRhythmaufgeführten Konfigurationsschritte in Ihre Instanz [Now Platform im Feld LogRhythm REST-API-Token ein.

Nächste Maßnahme

Sie sind jetzt bereit für Installieren Sie das Plugin, und konfigurieren Sie es LogRhythm.

Installieren Sie das Plugin, und konfigurieren Sie es LogRhythm

Bevor Sie die Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in Security Operations auf der Seite Now Platform®integriert werden kann.

Vorbereitungen

Erforderliche Rolle: Administrator

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich. Die neueste Version LogRhythm ist 7.8 oder höher.

Hinweis:
Ihre vorhandenen Alarmprofile werden in der neuesten Version LogRhythm nicht mehr unterstützt. Sie müssen daher neue Alarmprofile erstellen und die erforderlichen Konfigurationen durchführen.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (admin) installiert das Anwendungs-Plugin und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • (sn_si.admin) überwacht die folgenden Aufgaben: ○ Benennt, erstellt und bearbeitet Alarmprofile. ○ Ordnet Alarme zu und filtert sie – identifiziert bestimmte LogRhythm -Alarme, die Security Incidents erstellen, und konfiguriert, wie diese Alarmfelder einem Now Platform® -Security Incident zugeordnet werden. ○ Zeigt eine Vorschau der Details von Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird. ○ Erfasst historische Alarme und plant abgerufene Alarme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	○ Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu. ○ Diese Rolle hat auch Zugriff auf das Modul Security Operations. • Der Security Incident-Analyst (sn_si.analyst) reagiert auf Security Incidents, die basierend auf den Alarmprofileinstellungen erstellt werden.
Rufen Sie einen LogRhythm API-Anwendernamen und ein Passwort ab, und vergewissern Sie sich, dass Sie Version LogRhythm 7.8 oder höher verwenden.	Informationen zu API-Schlüsseln und zur Erstellung eines Accounts finden Sie auf der Produktwebsite: LogRhythm Enterprise-Website . Anwenderaccounts, Anmeldeinformationen und Zertifikate müssen vor der Installation der Anwendung ordnungsgemäß konfiguriert werden. Die -Integration erfordert LogRhythm Version 7.8 oder höher und die LogRhythm REST APIs. Weitere Informationen finden Sie unter Richten Sie die REST API für ein LogRhythm.
Stellen Sie sicher, dass Sie einen MID-Server installiert und konfiguriert haben.	In Ihrer Umgebung Now Platform ist ein MID-Server erforderlich. Auf der Website der ServiceNow-Produktdokumentation finden Sie Informationen zum Einrichten und Konfigurieren von MID-Servern.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Für das Rome-Release und spätere Familienreleases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.

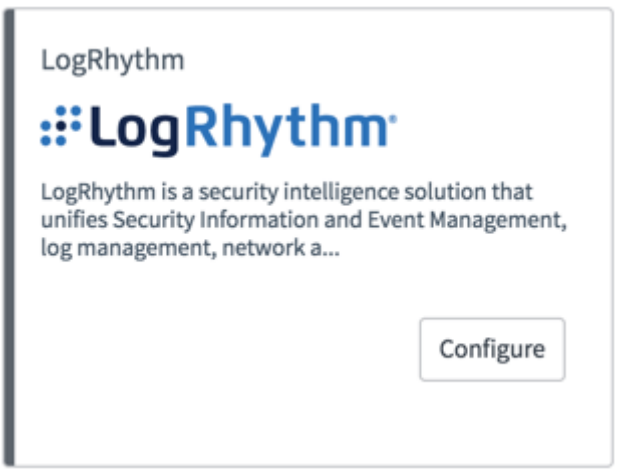
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	1. Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Wichtig:
Wenn Verbindungsprobleme mit der Clientkonsole LogRhythm auftreten, lesen Sie Überprüfen Sie die Konnektivität für LogRhythm.

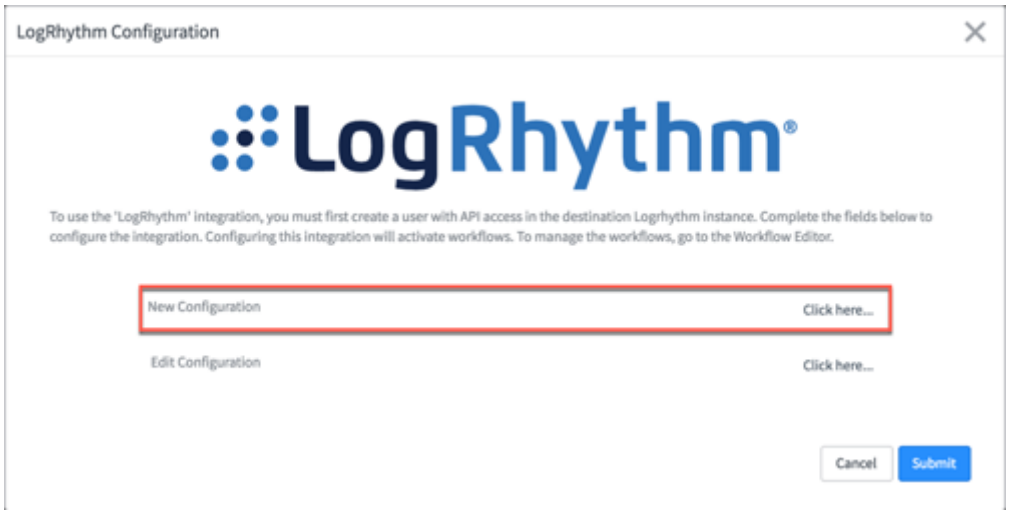
Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel LogRhythm.
3. Klicken Sie auf **Konfigurieren**.



4. Klicken Sie auf den Link **Neue Konfiguration**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder des Formulars aus.

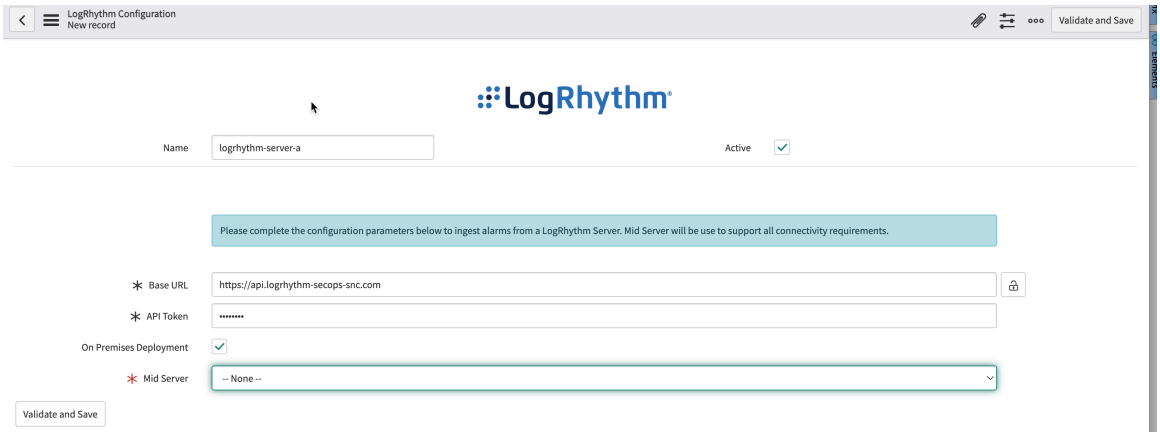
LogRhythm-Konfiguration

Feld	Beschreibung
Name	LogRhythm Servername, z. B. logrhythm-server-a.
Basis-URL	Basis-URL, die die LogRhythm REST API hostet. Der MID-Server ermöglicht den Zugriff auf das Netzwerk, in dem sich die LogRhythm-Clientkonsole befindet. Diese URL gibt an, wo der Server LogRhythm in diesem Netzwerk gehostet wird. Klicken Sie auf das Schlosssymbol rechts, um das Feld zu bearbeiten und Text für eine URL einzugeben, z. B. https://logrhythm.secops-eng.com:8501/.
API-Token	Geben Sie das Token ein, das Ihrer REST API zugeordnet ist, die Sie in der Client-Konsole LogRhythm erstellt haben.
Lokale Bereitstellung	Option zum Auswählen, ob es sich um eine lokale LogRhythm -Bereitstellung handelt.
MID-Server	Spezifischer MID-Server, der in Ihrer Umgebung eingerichtet ist. In dieser Auswahlliste sind nur die MID-Server verfügbar, die aktiv sind und validiert wurden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie auf **Validieren und speichern**.
   Nach erfolgreichem Abschluss der Validierung wird eine Meldung angezeigt, und die Seite „Konfigurationen LogRhythm “ wird neu geladen. Der nächste Schritt besteht im Erstellen eines Alarmprofils.

Nächste Maßnahme

Nachdem Sie die Validierung erfolgreich abgeschlossen haben, gehen Sie als Nächstes zu Erstellen eines Alarmprofils für LogRhythm.

Erstellen eines Alarmprofils für LogRhythm

In einem von Ihnen erstellten und benannten Alarmprofil geben Sie an, welche Alarme Sie aus der Client-Konsole LogRhythm abrufen möchten. Sie definieren auch, wie sie Feldern in einem Security Incident Now Platform zugeordnet werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

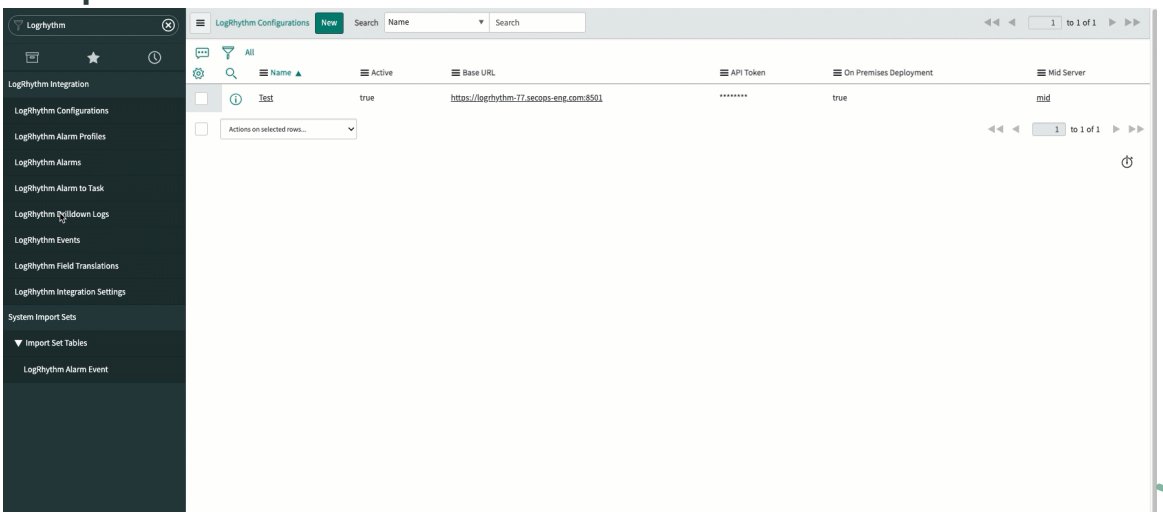
Basierend auf dem konfigurierten Alarmprofil kann ein Alarmprofil alle Arten von Alarmen sofort erfassen. Sie können jedoch Filterkriterien verwenden, um bestimmte Arten von Alarmen zu erfassen. Mit dieser Now Platform Integration werden alle konfigurierten Alarmregeln oder bestimmte basierend auf dem erstellten Profil erfasst. Alarmregeln, z. B. nur für Alarme bei hohen Risikostufen, können dann gefiltert werden, um anzugeben, welche Alarme Security Incidents erstellen sollen. Bevor Security Incidents erstellt werden, werden einzelne Feldwerte der gefilterten Alarme den entsprechenden Feldern im Security Incident Now Platform zugeordnet. Diese Konfiguration erfolgt über ein Alarmprofil innerhalb Ihrer Instanz Now Platform.

Prozedur

1. Navigieren zu **Alle** > **LogRhythm-Integration**.
2. Wählen Sie das Modul **LogRhythm-Alarmprofile** aus, um die Liste **der Alarmprofile** anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alarmprofil



3. Klicken Sie auf **Neu**, um ein neues Alarmprofil zu erstellen.
   Ein neues Alarmprofilformular wird angezeigt. Oben auf der Seite wird in der Fortschrittsleiste **Name** ausgewählt. Diese Leiste verfolgt Ihren Fortschritt während der Konfiguration.
4. Füllen Sie die Felder im Formular aus.

Alarmprofil

Feld	Beschreibung
Name	Name für das Alarmprofil. Anhand dieses Namens können Sie die Alarmtypen wie z. B. *Nicht autorisierter Zugriff* (*VPN*), *Malware*oder *Phishing*identifizieren.
Kurzbeschreibung	Kurztext für zusätzliche Informationen zum Alarmprofil, die den Typ der Alarme oder eine Alarmkategorie enthalten können. Beispielbeschreibung: Alle Alarme, die nicht autorisierten PowerShell- und Sudo-Zugriffsversuchen zugeordnet sind.
Quelle	Quellserver aus der Auswahlliste. Die Liste besteht aus LogRhythm Konfigurationen, die Sie bereits eingerichtet haben, z. B. `logrhythm-server-a`. Weitere Informationen finden Sie unter Installieren Sie das Plugin, und konfigurieren Sie es LogRhythm.
Bestellung	Priorität des Alarmprofils. Dieses Feld gibt die Reihenfolge an, in der die Alarmprofile ausgeführt werden, wenn zwei oder mehr Alarmprofile die Auslösebedingungen gemeinsam nutzen.
Aktiv	Standardmäßig ist diese Option nicht ausgewählt. Nachdem Sie alle Schritte zur Einrichtung des Alarmprofils abgeschlossen und auf **Fertigstellen**geklickt haben, werden Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	aufgefordert, dieses Kontrollkästchen zu aktivieren, um das Alarmprofil zu aktivieren. Wenn das Alarmprofil aktiv ist, werden automatisch Alarme aus der Client-Konsole LogRhythm abgerufen.

5. Klicken Sie auf **„Fortsetzen“**, um Ihre Daten zu speichern und mit dem Zuordnungsformular fortzufahren.

   Wenn die Validierung erfolgreich ist, wird die Seite neu geladen, und das **Zuordnungsformular** wird angezeigt. Sie können mit der Konfiguration erst fortfahren, wenn Sie Ihre Verbindung und Ihre Anmeldeinformationen erfolgreich validiert haben.

Zugehörige Informationen

LogRhythm -Alarme werden dem Security Incident zugeordnet

LogRhythm -Alarme werden dem Security Incident zugeordnet

Nachdem Sie die Quelle LogRhythm ausgewählt haben, die Sie erfassen möchten, müssen Sie einzelne Alarmfelder LogRhythm den Security Incident-Feldern Now Platform zuordnen.

Die Zuordnung von Alarmen umfasst die folgenden Aufgaben:

- LogRhythm Alarme zuordnen. Für diese Aufgabe listen Sie Beispielalarme anhand der Alarm-IDs oder der neuesten Alarme aus der Client-Konsole LogRhythm auf und erfassen (Abruf).
- Die Felder „Beispielalarm“ sind in drei Gruppen unterteilt:
  - Alarmfelder: Die verfügbaren Alarmfelder und ihre entsprechenden Werte werden angezeigt.
  - Ereignisfelder: Die verfügbaren Ereignisfelder und ihre entsprechenden Werte werden angezeigt.
  - DrillDownLog-Felder: Die verfügbaren Drilldown-Protokollfelder und ihre entsprechenden Werte werden angezeigt.
- Jede abgerufene Alarm-ID wird als Registerkarte angezeigt. Überprüfen Sie auf den Registerkarten „Alarm ID“, ob alle kritischen Alarmfelder aus dem Abschnitt „Erfassung des Alarmbeispiels“ auf der linken Seite des Formulars dem Abschnitt „SIR-Incident-Feldzuordnung“ auf der rechten Seite des Formulars zugeordnet sind.
- Nachdem Sie die Alarme dem Feld „SIR-Incident-Feldzuordnung“ zugeordnet haben, wird die Alarmkategorie auch im Feld „Eingabeausdruck“ angezeigt. Beispiel: `${Alarm: Alarmid}$`.
- Sie können die -Konfiguration ändern, indem Sie im Security Incident Felder hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder anhand der angegebenen Farbcodierung.
- Sie können Alarme filtern, um anzugeben, welche Alarme in der SIR-Anwendung erfasst werden. Sie können die Alarme entweder direkt filtern oder die Alarmkategorien verwenden, um Ihre Suche basierend auf Alarmen, Ereignissen oder DrillDownLogs aufzuschlüsseln.
- Verwenden Sie den Skript-Editor, wenn Sie Werte für die Felder Priorität und Kategorie im Security Incident formatieren möchten.

Der nächste Schritt führt Sie zu Ordnen Sie LogRhythm Alarmfelder Security Incident-Feldern zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Ordnen Sie LogRhythm Alarmfelder Security Incident-Feldern zu

Verwenden Sie den Skript-Editor zum Formatieren von LogRhythm -Werten

Filtern Sie Alarme nach LogRhythm

Ordnen Sie LogRhythm Alarmfelder Security Incident-Feldern zu

Sie ordnen einzelne Alarmfelder den Security Incident-Feldern zu. Die vorkonfigurierte Zuordnung kann bearbeitet werden, und die für die Felder bereitgestellte Farbcodierung hilft Ihnen, bereits zugeordnete Alarme zu überwachen. Mit diesem Schritt können Sie visualisieren, wie sich Ihre Änderungen auf die Felder im Security Incident auswirken.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Wenn Sie mit den LogRhythm -Alarmen nicht vertraut sind, navigieren Sie zur Client-Konsole LogRhythm, und sehen Sie sich einige Beispiele für Alarm-IDs an. Im folgenden Beispiel LogRhythm wurden die Alarme 9468 und 9474 verwendet, um die Alarme dem Security Incident zuzuordnen.

Warum und wann dieser Vorgang ausgeführt wird

Mit diesem Formular ordnen Sie die Alarmregeln LogRhythm auf der linken Seite den Feldern für Security Incidents auf der rechten Seite zu.

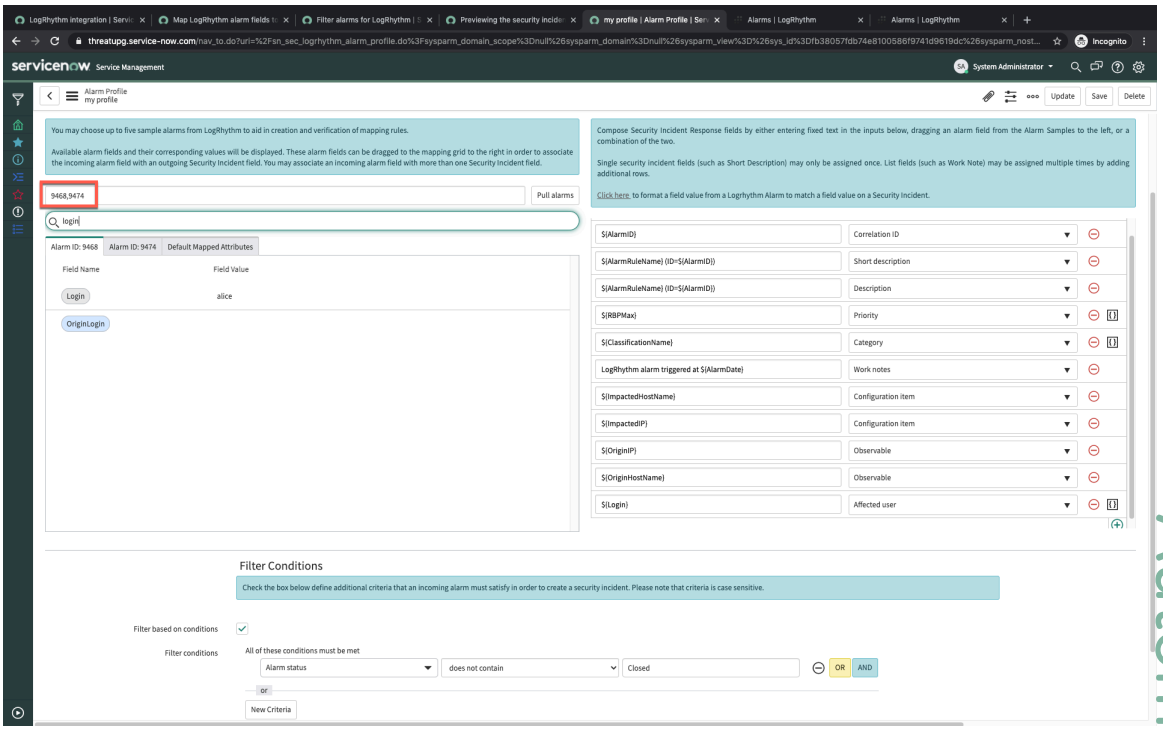
Die folgende Abbildung zeigt die Standardzuordnung von Alarmen, die für jedes Alarmprofil vorkonfiguriert ist. Diese Standardzuordnung kann bearbeitet werden, und mit diesem Formular passen Sie die Felder an, die den Security Incident ausfüllen. Nachdem Sie diese Zuordnung abgeschlossen haben, können Sie sehen, wie sich das Hinzufügen oder Entfernen von Alarmfeldern potenziell auf die Feldwerte im Security Incident auswirkt.

Auf der linken Seite dieses Formulars sind in der folgenden Abbildung die Alarmregeln LogRhythm dargestellt. Die Werte dieser Alarmregeln werden den Security Incident-Feldern auf der rechten Seite des Formulars zugeordnet.

Prozedur

1. Nachdem Sie ein Alarmprofil für LogRhythm erstellt haben, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
2. Geben Sie im Feld **Erfassung des Alarmbeispiels** bis zu fünf Beispielalarm-IDs LogRhythm durch Kommas getrennt (9468,9474) ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie neben dem Alarmfeld **auf Alarme abrufen**.

   Das Abrufen von Beispielalarmen kann einige Minuten dauern. Oben auf dem Bildschirm wird eine Meldung angezeigt, dass die Transaktion funktioniert.

   Nachdem die Beispielalarm-IDs übermittelt und erfolgreich vom Server LogRhythm abgerufen wurden, werden die Alarmfelder und die entsprechenden Werte auf Registerkarten angezeigt.

   Hinweis:
   Nachdem eine Alarm-ID erfolgreich abgerufen wurde, gibt Now Platform möglicherweise die folgende Nachricht zurück: Die folgenden neuen Felder stehen in Kürze für die Filterung zur Verfügung. Laden Sie dieses Profil in einigen Minuten neu, wenn eine Filterung basierend auf diesen Feldern erforderlich ist. Itemspacketsin, Itemspacketsout.

   Diese Nachricht wird angezeigt, wenn der einzelne abgerufene Alarm Feldnamen enthält, die zuvor nicht von Now Platformverarbeitet wurden. Diese Felder sind für die Zuordnung verfügbar. Wenn jedoch diese Nachricht angezeigt wird, laden Sie das Formular neu, damit diese Felder angezeigt und in den Filterauswahllisten des Bedingungsgenerators verfügbar sind, wenn Sie bereit sind, Filterbedingungen festzulegen.

Durch das Erfassen dieser Beispielalarme in der Alarmprofilkonfiguration können Sie verhindern, dass dem Security Incident Alarmfelder zugeordnet werden, die keine Werte enthalten. Außerdem werden Alarmfelder mit Werten an den entsprechenden Feldern im Security Incident ausgerichtet. Dieser Schritt stellt sicher, dass alle kritischen Alarmfelder zugeordnet sind und dass keine Feldwerte im Security Incident fehlen.

Alarmfelder sind farbcodiert, um sicherzustellen, dass im Zuordnungsprozess keine Alarme übersehen oder dupliziert werden. Ein transparentes Alarmfeld (Account, AlarmRuleID, AlarmStatususw.) zeigt an, dass das Feld noch nicht für die Zuordnung zu einem Security Incident ausgewählt wurde.

Ein grau Feld (AlarmDate, AlarmIDund AlarmRuleName) zeigt an, dass bereits ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung

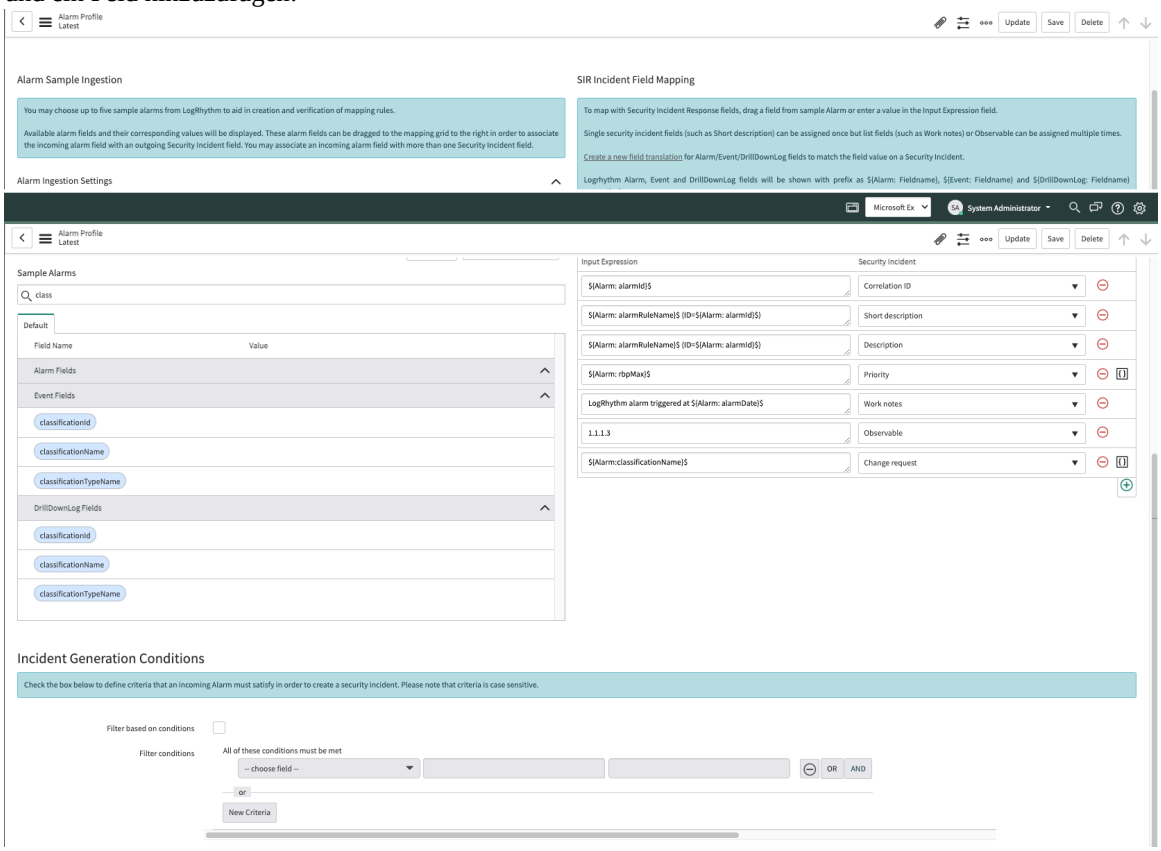
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

hilft Ihnen, die Zuordnung nachzuverfolgen, da in bestimmten Fällen ein Alarmfeld mehreren Feldern in einem Security Incident zugeordnet werden kann. Beispielsweise können die Felder Erkennbare Elemente und Arbeitsnotiz mehr als einen Wert haben.

4. Klicken Sie auf Beispielalarmdaten löschen, um die **Beispielalarmdaten zu löschen**.

5. Führen Sie die folgenden Schritte aus, um die Standardkonfiguration für den Security Incident zu bearbeiten und ein Feld hinzuzufügen:



a. Klicken Sie unten rechts im Formular auf das Plus-Symbol.
Ein neues Feld wird angezeigt.

b. Wählen Sie in der Spalte Security Incident ein verfügbares Feld aus der Auswahlliste aus.

In der erweiterten Auswahlliste sind einige der Felder schattiert. Beispiel: Die Kategorie hat einen grauen Hintergrund, was darauf hinweist, dass sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Alarmfelder LogRhythm stellt diese Farbcodierung für die Security Incident-Felder sicher, dass Werte aus den Alarmfeldern nicht versehentlich demselben Security Incident-Feld zugeordnet werden.

In der Abbildung oben ist die Alarmregel ${Alarm:classificationName}$ bereits dem Feld Kategorie im Security Incident in diesem Profil zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Feld „Erkennbares Element“ kann mehr als dem Feld im selben Security Incident zugeordnet werden, sodass mehrere erkennbare Elemente angezeigt werden können. Ebenso können die Felder Konfigurationselement und Arbeitsnotizen so zugeordnet werden, dass mehrere Werte angezeigt werden.

Auf der Seite „Alarmbeispielerfassung“ des Formulars zeigt Blau an, dass ein Alarmregelfeld nicht zugeordnet wurde. Grau zeigt an, dass zugeordnet wurde. Weiß zeigt in der Auswahlliste auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars an, dass kein Feld zugeordnet wurde. Grau zeigt an, dass ein Feld zugeordnet wurde. Verwenden Sie diese Farbcodierung, um Ihre Feldzuordnung nachzuverfolgen.

In der obigen Abbildung wurde Betroffener Benutzer aus der Auswahlliste als neues Feld im Security Incident ausgewählt.

c. Klicken Sie im Abschnitt Erfassung des Alarmbeispiels auf der linken Seite des Formulars mit der linken Maustaste, um die gewünschte Alarm-ID im Feld Eingabeausdruck auszuwählen.

In der obigen Abbildung wurde Anmeldung ausgewählt.

d. Ziehen Sie es in das gelöschte Feld, und lassen Sie es los.
In der linken Spalte im Abschnitt „SIR-Incident-Feldzuordnung“ wird der neue Wert für das Feld Betroffener Benutzer angezeigt. In diesem Fall wird der Anmeldungswert aus dem Alarm LogRhythm im Feld „Betroffener Benutzer“ im Security Incident angezeigt.

6. Um manuell einen Wert für Felder in der Spalte „Eingabeausdruck“ einzugeben, platzieren Sie alternativ den Cursor im Feld „Eingabeausdruck“, und geben Sie den gewünschten Alarmwert ein.

Beispiel: In der obigen Abbildung wurde dem Security Incident-Formular ein weiteres Feld hinzugefügt (Zuweisungsgruppe), und in diesem Feld wurde manuell die Zuweisung des Security Incident eingegeben.

7. Bearbeiten Sie die vorkonfigurierte Zuordnung nach Bedarf weiter.
Wenn Sie Werte aus Alarmfeldern LogRhythm in Werte übersetzen müssen, die von den -Feldern im Security Incident unterstützt werden, können Sie den Skript-Editor verwenden. Weitere Informationen finden Sie unter Verwenden Sie den Skript-Editor zum Formatieren von LogRhythm -Werten.

Nächste Maßnahme
Nachdem Sie die Feldzuordnung abgeschlossen haben, gehen Sie als Nächstes zu Filtern Sie Alarme nach LogRhythm.

Filtern Sie Alarme nach LogRhythm

Indem Sie Filterkriterien für Alarme festlegen, nachdem Sie Felder zugeordnet haben, können Sie bestimmen, welche Alarme in der Anwendung SIR erfasst werden sollen. Durch das Filtern von Alarmen können Sie die Anzahl der erfassten Alarme erheblich reduzieren, wenn das Alarmprofil aktiviert ist.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie die Filterbedingungen unten im Zuordnungsformular, um bestimmte Alarme herauszufiltern oder die Erfassung auf Alarme zu beschränken, die bestimmte Kriterien auf Feldebene erfüllen. Durch das Filtern wird die Anzahl der erfassten Alarme erheblich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

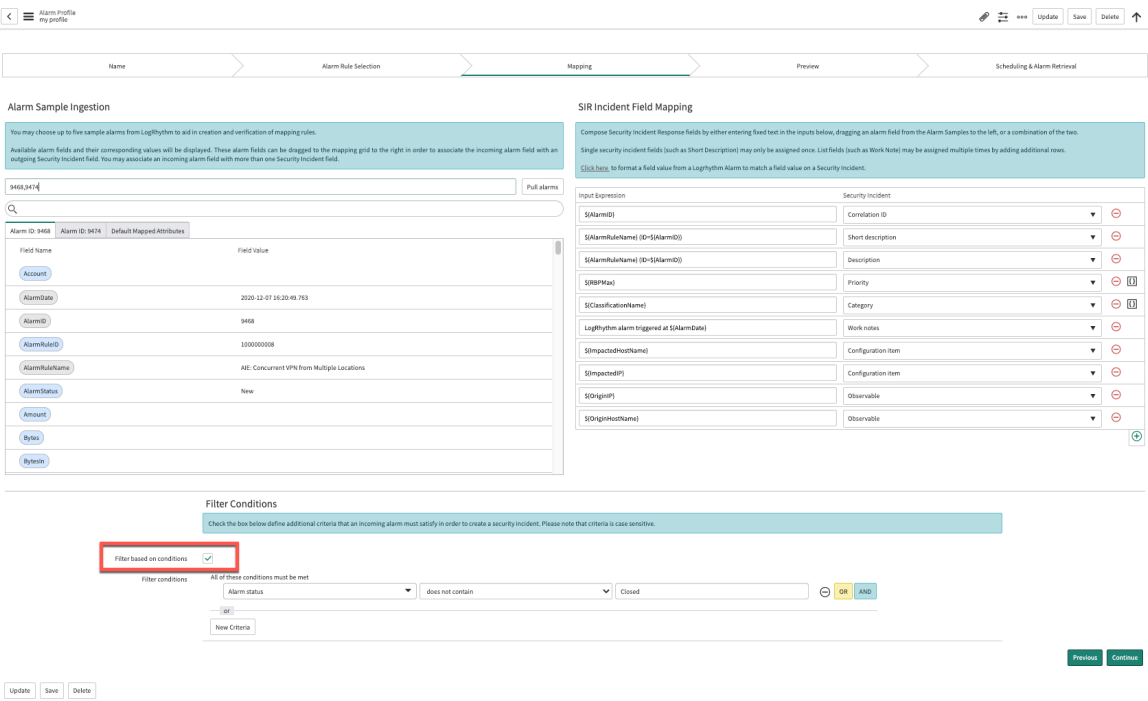
reduziert, sobald das Alarmprofil aktiviert ist. Verwenden Sie Filter, um eine verwaltbare Menge von Alarmen zu erfassen, die Ihre Mitarbeiter des Security Operations Center (SOC) unterstützen können.

Hinweis:

Das folgende Beispiel zeigt eine Standardfiltereinstellung, in der Alarmstatus-does-not-contain-Closed die Standardeinstellung ist. Dieser Filter ruft nur aktive Alarme ab, und diese Einstellung reduziert die Anzahl der abgerufenen Alarme. Die folgenden Schritte veranschaulichen, wie Sie einen weiteren nützlichen Filter hinzufügen, der nur Alarme mit den höchsten Schweregrad- oder Prioritätswerten enthält.

Prozedur

1. Um die Filterkriterien zu bearbeiten, aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen filtern**.

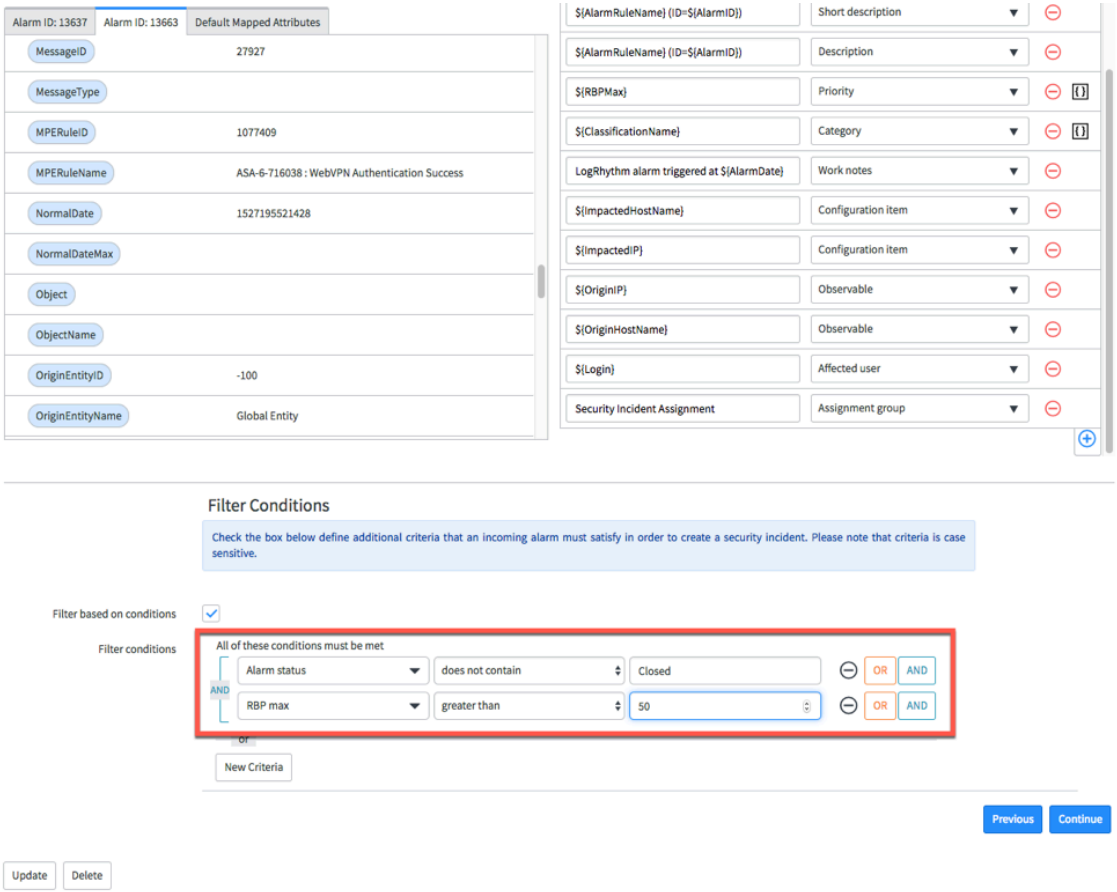


2. Klicken Sie rechts neben dem Feld **Filterbedingungenauf ODER** oder **auf UND**.
3. Wählen Sie in der neuen Zeile, die angezeigt wird, die Filterbedingungen aus den Auswahllisten aus.

Die folgende Abbildung zeigt einen zusätzlichen Filter, der den Kriterien hinzugefügt wird, bei denen die risikobasierte Priorität (RPP max.) größer als 50ist. Mit dieser Filtereinstellung werden nur LogRhythm -Alarme mit einem risikobasierten Prioritätswert größer als 50 abgerufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Nachdem Sie verifiziert haben, dass alle kritischen LogRhythm -Alarmfelder dem Security Incident Now Platform zugeordnet sind, und Sie Filterkriterien zur Begrenzung der Alarmerfassung festgelegt haben, wählen Sie eines aus, um die Konfiguration fortzusetzen.

Nächste Maßnahme

Der nächste Schritt besteht darin, eine Vorschau der zugeordneten Felder im Security Incident anzuzeigen. Weitere Informationen finden Sie unter Vorschau des Security Incident mit zugeordneten LogRhythm Alarmwerten wird angezeigt.

Vorschau des Security Incident mit zugeordneten LogRhythm Alarmwerten wird angezeigt

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie den Feldern im Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle kritischen LogRhythm -Alarmfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Erforderliche Rolle: sn_si.admin.

Security Incident

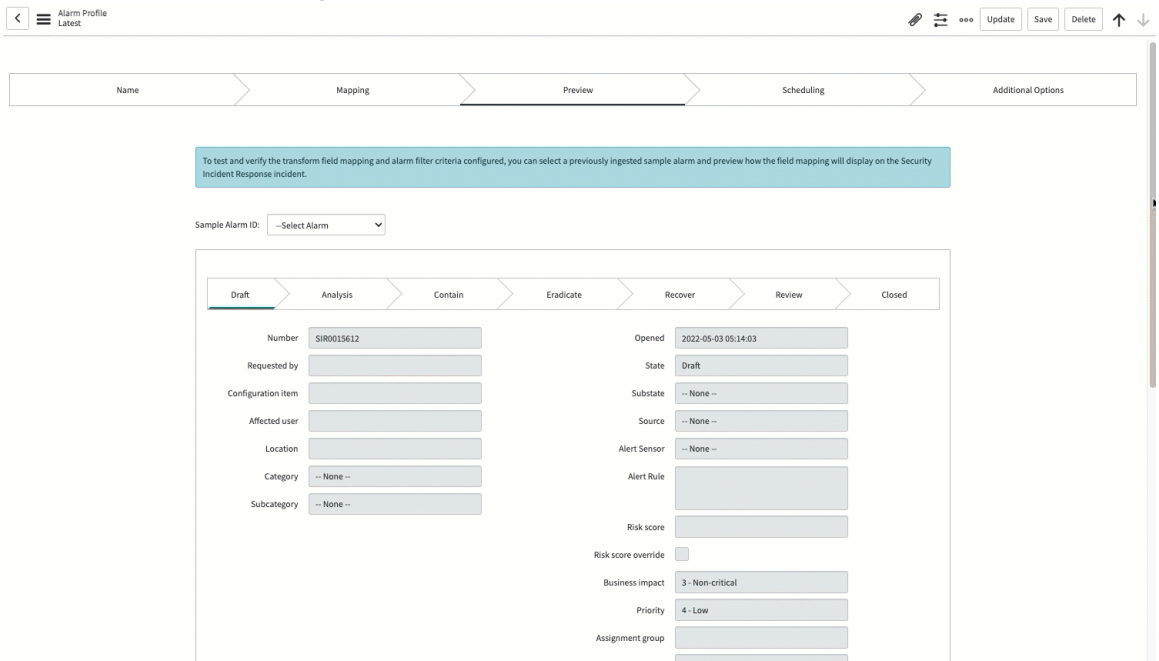
Wenn die Vorschau des Security Incidents nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Vorschau**.

Ein Beispiel für die Vorschau für den gesamten Security Incident Now Platform ist in den beiden folgenden Abbildungen dargestellt. Dieses Beispiel der Vorschau auf einen Security Incident ist mit den Feldern LogRhythm Alarme ausgefüllt, die dem Beispielalarm 13663zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sind die Felder Konfigurationselement, Betroffener Benutzer, Priorität, Zuweisungsgruppeund Kurzbeschreibung des Security Incidents ausgefüllt.

Obere Hälfte des Security Incidents



In der unteren Hälfte des Formulars „Security Incident“ wird das Beschreibungsfeld ausgefüllt. Im Abschnitt „Zugehörige Elemente“ sind die Felder Konfigurationselement, ErkennbaresElement und Arbeitsnotiz mit Werten gefüllt. Wenn mehrere Werte für diese Felder zugeordnet sind, wird jeder Wert im Security Incident angezeigt, da jedes dieser Felder mehr als einen Wert akzeptieren kann.

Fehlerbedingungen in Vorschau

Die folgenden Warnmeldungen werden möglicherweise in der Vorschau auf den Security Incident angezeigt. Wenn ein Beispielalarm die Filterkriterien nicht erfüllt, wird der gesamte Security Incident nicht ausgefüllt.

Eingabewert nicht gefunden

Wenn die Alarm-ID in den Filterbedingungen enthalten ist, wird möglicherweise weiterhin eine Warnmeldung angezeigt, wenn für bestimmte zugeordnete Felder keine bestimmten Eingabewerte gefunden werden. Für das folgende Beispiel wird in der Vorschau des Datensatzes davon ausgegangen, dass das Feld Zugewiesen an keinen Wert enthält, obwohl es zugeordnet wurde.

Überprüfen Sie bei diesem Nachrichtentyp im Zuordnungsdatensatz, ob der Eingabewert korrekt ist. In diesem Fall ist die Person im Feld Zugewiesen an in Security Incident in der Instanz Now Platform falsch. Wenn dieser Alarm erfasst wird und einen Security Incident mit dieser Bedingung erstellt, werden Felder mit diesem Eingabewert (Abel Tuter) im Security Incident leer gelassen.

Die verbleibenden Nachrichten in Blau dienen nur zur Information und zeigen an, dass diese Felder keinen Wert zur Anzeige in der Vorschau haben. Mit dieser Vorschau kann der Security Incident-Administrator, der das Alarmprofil konfiguriert, überprüfen, ob diese Felder bei der ersten Erstellung keinen Wert haben dürfen, da Security Incident-Felder in bestimmten Fällen später automatisch ausgefüllt werden können. Andere Zuordnungsfehler werden ebenfalls angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie mit der Zuordnung und der Vorschau des Security Incidents zufrieden sind, wählen Sie eine Option aus, um die Konfiguration fortzusetzen.

Option	Beschreibung
Klicken Sie in der Fortschrittsleiste **auf Fortfahren** oder **Zeitplanung**.	Fahren Sie mit dem Formular **„Zeitplanung und Alarmabruf“** fort. Auf dem Fortschrittsbalken ist **„Zeitplanung und Alarmabruf“** ausgewählt. Der nächste Schritt besteht darin, den Alarmabruf zu planen.
Klicken Sie auf **Zurück**.	Kehren Sie zum Alarmprofil zurück, und setzen Sie die Zuordnung fort.
Geben Sie in der Auswahlliste **Beispielalarm-ID** oben im Vorschauformular eine andere Alarm-ID ein.	Die Auswahlliste **Beispielalarm-ID** wird für jede von Ihnen eingegebene Alarm-ID angezeigt. Sie können bis zu fünf Alarme auswählen. Mit dieser Option können Sie eine Vorschau einer anderen LogRhythm -Alarm-ID für einen Security Incident anzeigen.

Nachdem Sie eine Vorschau des Security Incident angezeigt haben und mit den Ergebnissen zufrieden sind, gehen Sie als Nächstes auf Planen Sie LogRhythm -Alarme, und rufen Sie sie ab.

Planen Sie LogRhythm -Alarme, und rufen Sie sie ab

Nachdem Sie eine Vorschau des Security Incident mit den von Ihnen ausgewählten und zugeordneten Alarmen LogRhythm angezeigt haben, können Sie den Alarmabruf planen. Nachdem Sie diesen Schritt abgeschlossen haben, kann das Alarmprofil aktiviert werden.

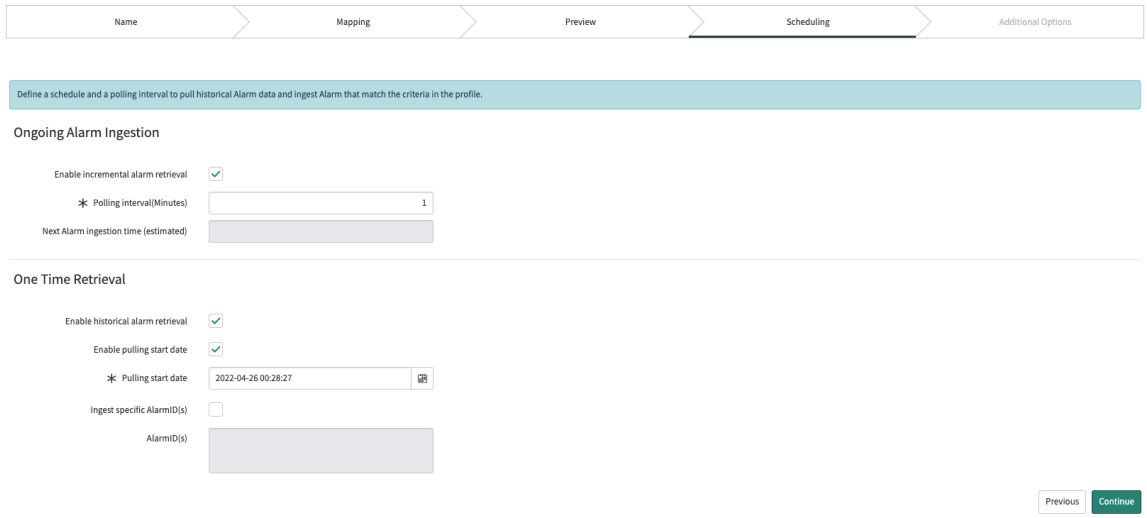
Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Zeitplanung ermöglicht Ihnen, die Zeitplanung und die für den Abruf ausgewählten Alarmtypen zu ändern. Sie filtern die von Ihnen erfassten Alarme basierend auf einem Datumsbereich oder bestimmten Alarm-IDs. Mit diesem Schritt bestimmen Sie, ob Sie historische Alarme erfassen möchten und wie oft Sie zukünftige Alarme abfragen, die der Alarmprofilkonfiguration entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie in der Fortschrittsleiste auf den Schritt **Zeitplan**.

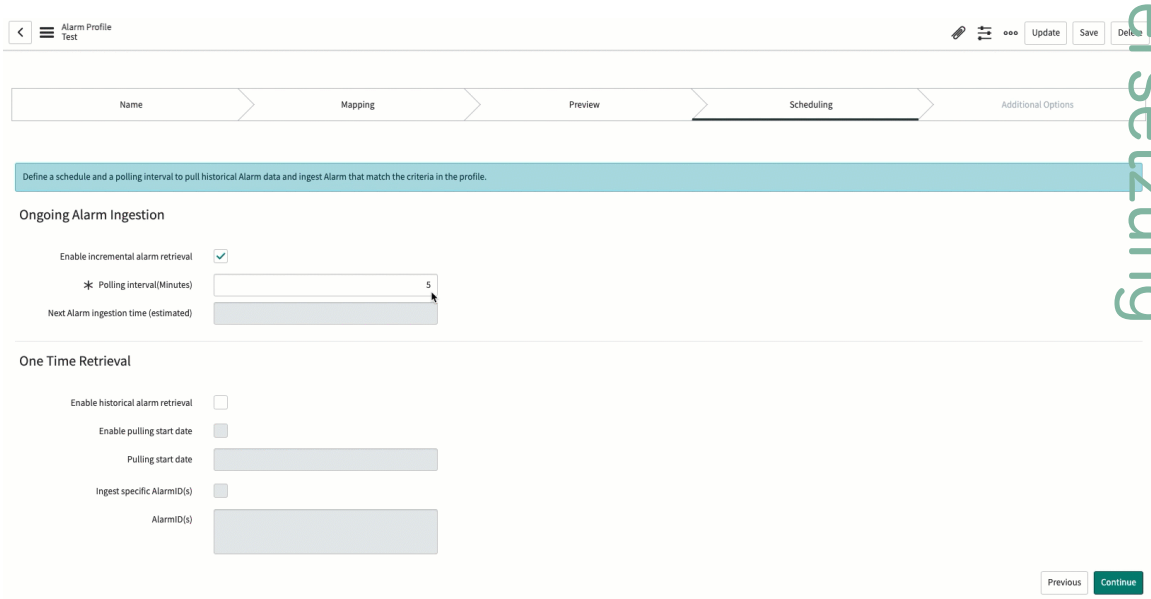


2. Wählen Sie aus den folgenden Optionen aus, um Ihren Alarmabruf zu konfigurieren.

3. Führen Sie zum Bearbeiten des historischen Alarmabrufs die folgenden Schritte aus, um ein Datum für den Alarmabruf oder eine bestimmte Alarm-ID einzugeben.

   a. Wählen Sie **Abrufen des Startdatums aktivieren**und wählen Sie **Startdatum abrufen**.

   b. Klicken Sie im Feld **Startdatum des Abrufs** auf den angezeigten Kalender, wählen Sie das Datum und anschließend das grüne Häkchen aus, um Ihren Eintrag zu speichern.



   Das Datum wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Alternativ können Sie die Option **Bestimmte Alarm-ID(s) erfassen** auswählen und im Feld **AlarmID(s)** die spezifischen Alarm-IDs für die Verlaufsdaten eingeben, um bestimmte Alarm-IDs abzurufen.

   Sie können bis zu fünf durch Kommas getrennte Alarme eingeben.

d. Klicken Sie auf **Aktualisieren**.

4. Wählen Sie eine der folgenden Optionen aus, um die Bearbeitung fortzusetzen oder die Konfiguration abzuschließen.

Nächste Maßnahme

Nachdem Sie die Details für die kontinuierliche Alarmerfassung und den einmaligen Abruf konfiguriert haben, fahren Sie als Nächstes mit Zusätzliche Optionen für LogRhythm -Alarmefort.

Zusätzliche Optionen für LogRhythm -Alarme

Die LogRhythm Enterprise-Integration bietet Ihnen die Möglichkeit, die LogRhythm -Alarme basierend auf Security Incidents automatisch zu aktualisieren oder zu schließen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die Option Erste Alarmaktualisierungen aktivieren, werden die Alarme in den LogRhythm-Kommentaren automatisch mit den ersten Alarmaktualisierungen aktualisiert. Ebenso werden, wenn Sie die Option Alarmschließung aktualisieren aktivieren, die Alarme in LogRhythm zusammen mit dem SIR-Abschlusscode und den Abschlusskommentaren automatisch geschlossen.

Die ID des Alarms LogRhythm wird während des gesamten Lebenszyklus des Incidents mit der ID des Security Incidents Now Platform verknüpft. Diese Korrelation ermöglicht einen gleichzeitigen und automatisierten Abschluss von Security Incidents/Alarmen. Wenn der Security Incident-Datensatz Security Incident Response (SIR) geschlossen wird, wird im Alarm in der Webkonsole LogRhythm ein Kommentar gepostet. Dieser Kommentar gibt an, dass der Alarm basierend auf der Schließung des Security Incident Now Platform geschlossen wurde. Die Incident-Nummer und eine URL, die als Referenz auf den Security Incident verweist, sind auch im Kommentarabschnitt im Alarm LogRhythm enthalten.

Prozedur

1. Klicken Sie auf den Schritt **Zusätzliche Optionen** in der Fortschrittsleiste.
2. Um die automatisierte Alarmaktualisierung für die Erstellung von SIR-Incidents zu verwenden, wählen Sie aus den folgenden Optionen aus, um Ihren Alarmabruf zu konfigurieren.
3. Um das automatisierte Alarm-Update für das Schließen von SIR-Incidents zu verwenden, wählen Sie aus den folgenden Optionen aus, um Ihren Alarmabruf zu konfigurieren.
4. Klicken Sie auf **Fertigstellen**, um das Alarmprofil zu speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?
Wenn Sie keine Hinweise sehen, dass der Alarm im Security Incident erfolgreich geschlossen wurde, lesen Sie in den Arbeitsnotizen nach, wie Sie das Problem beheben können. Überprüfen Sie auch Ihre Serververbindung. Wenn Sie bestätigen, dass der Security Incident Now Platform geschlossen wurde und beim Server kein Timeout aufgetreten ist, müssen Sie den Alarm möglicherweise manuell in der Webkonsole LogRhythm schließen.

Zusätzliche Konfigurationen für die LogRhythm -Integration

Verwenden Sie die LogRhythm Integrationseinstellungen, um die voreingestellten System- und Problembehandlungseigenschaften gemäß Ihren Anforderungen zu ändern.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **LogRhythm-Integration** > **LogRhythm-Integrationseinstellungen**.
2. Konfigurieren Sie die Systemeigenschaften entsprechend Ihren Anforderungen.
3. Füllen Sie die Felder im Formular aus.

LogRhythm Systemeigenschaften für die Integration

Feld	Beschreibung
Dadurch wird der Filter angewendet, bevor die Daten in ServiceNow-Tabellen gespeichert werden.	Mit dieser Option können Sie festlegen, ob der Filter angewendet werden soll, bevor die Daten in den ServiceNow-Tabellen gespeichert werden. Standardmäßig ist der Wert auf Ja festgelegt.
Max. Security Incident kann an einem Tag erstellt werden	Option zum Definieren der maximalen Anzahl von Security Incidents, die an einem Tag erstellt werden können. Standardmäßig ist der Wert auf 2000 festgelegt.
LogRhythm Die regelmäßige Erfassung kann über 1000 Alarme umfassen, daher wird Paginierung verwendet, um die Alarme zu erfassen. Grenzwert pro Seite, der zum Abrufen der Anzahl von Alarmen pro Seite zulässig ist.	Option zum Definieren der maximalen Anzahl von Alarmen, die auf einer einzelnen Seite abgerufen werden sollen. Standardmäßig ist der Wert auf 100 festgelegt.
Löschen Sie die Datensätze der Tabelle „Quelle für Aufgabe“, die älter als die angegebene Anzahl von Tagen sind.	Option zum Löschen von Quellen-zu-Aufgaben-Tabellendatensätzen, wenn die angegebene Anzahl von Tagen verletzt wurde. Standardmäßig ist der Wert auf 30 festgelegt.

4. Konfigurieren Sie die Problembehandlungseigenschaften gemäß Ihren Anforderungen.
5. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlungseigenschaften für LogRhythm-Integration

Feld	Beschreibung
Geplante Erfassung debuggen: Dies aktiviert Systemprotokolle auf Debug-Ebene für die Erfassung durch eine geplante Aufgabe. Dadurch werden alle Nachrichten/Ausnahmen protokolliert, die durch die geplante Erfassung beim Abrufen von Alarmen/Drilldown-Protokollen/Ereignisse aus LogRhythmgeneriert werden.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Erfassung durch die geplante Aufgabe. Standardmäßig ist der Wert auf Nein festgelegt.
Transformationszuordnung debuggen: Dies aktiviert Systemprotokolle auf Debug-Ebene für die Transformationszuordnung. Dadurch werden alle Nachrichten protokolliert, die von Transformationszuordnungen generiert werden, wenn ein Security Incident aus dem Alarmimport erstellt wird. Dadurch konnte auch die UI-Aktion für die Alarmimporttabelle die Transformationszuordnung erneut ausführen.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Transformationszuordnung. Standardmäßig ist der Wert auf Nein festgelegt.
Beispielerfassung in Alarmprofil debuggen: Dies aktiviert Systemprotokolle auf Debug-Ebene für die Beispielerfassung. Dadurch werden alle Nachrichten protokolliert, die während der Erfassung von Beispielen generiert werden.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Beispielerfassung. Standardmäßig ist der Wert auf Nein festgelegt.
Debug-Vorschau in Alarmprofil: Dies aktiviert Systemprotokolle auf Debug-Ebene für die Alarmprofilvorschau. Dadurch werden alle Nachrichten protokolliert, die generiert werden, während die Vorschau für den Beispielalarm gerendert wird.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Alarmprofilvorschau. Standardmäßig ist der Wert auf Nein festgelegt.
Ausgehende REST-Aufrufe debuggen: Durch Aktivieren dieser Eigenschaft wird die Protokollierung auf Debug-Ebene in der Tabelle „Systemprotokolle“ für alle REST-Aufrufe (Anforderung und Antwort) mit oder ohne MID-Server von LogRhythmermöglicht.	Option zum Aktivieren der Protokollierung auf Debug-Ebene in der Tabelle „Systemprotokolle“ für alle REST-Aufrufe mit oder ohne MID-Server ab LogRhythm. Standardmäßig ist der Wert auf Nein festgelegt.

6. Klicken Sie auf **Speichern**.

Verwenden Sie den Skript-Editor zum Formatieren von LogRhythm -Werten

Zusätzlich zu den direkt zugeordneten Feldern aus den abgerufenen Alarmwerten und den manuell eingegebenen Alarmwerten können Sie den Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Dies ist optional.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Der Skript-Editor ändert die Werte eines LogRhythm -Alarms, sodass die Werte unterstützt werden, die den Feldern Priorität und Kategorie im Security Incident zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

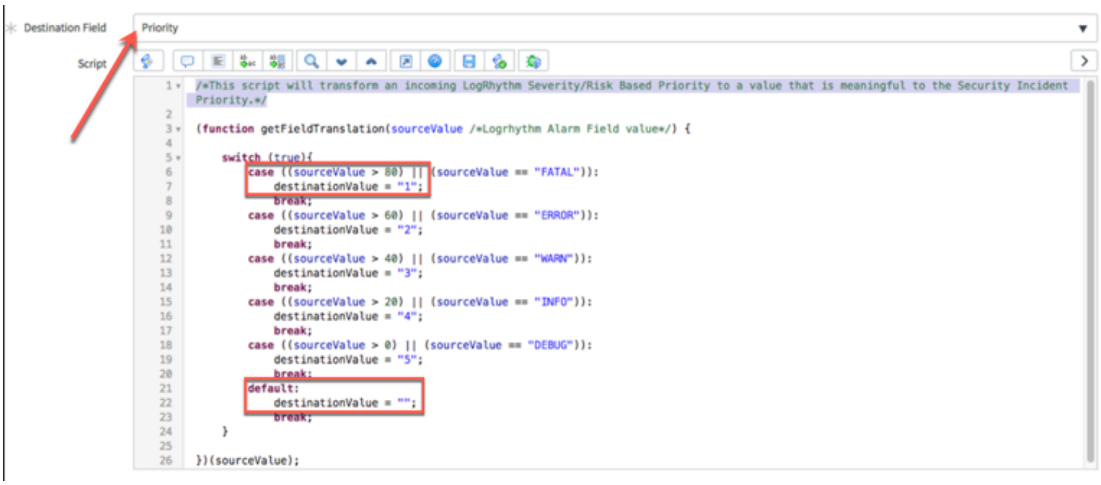
In bestimmten Fällen, wenn die Alarmwerte LogRhythm den Feldern Priorität und Kategorie im Security Incident zugeordnet sind, können Sie die zugeordneten Werte bearbeiten. Wenn Sie den Wert eines LogRhythm -Alarms in einen Wert übersetzen möchten, der von den Feldern Priorität oder Kategorie im Security Incident unterstützt wird, verwenden Sie den Skript-Editor.

Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular im Abschnitt „SIR-Incident-Feldzuordnung“ auf das Klammersymbol [{}], um den Skript-Editor zu öffnen.

   Die Standardwerte sind für die Felder Priorität und Kategorie im Security Incident enthalten. Sie können diese Werte bearbeiten.

   Überprüfen Sie für dieses Beispiel im geöffneten Editor, ob **Priorität** in der Auswahlliste **Zielfeld** angezeigt wird (siehe folgende Abbildung). Beachten Sie, dass es sich bei diesem Feld um die *Priorität*des Security Incident und nicht um die risikobasierte LogRhythm*Priorität*handelt.

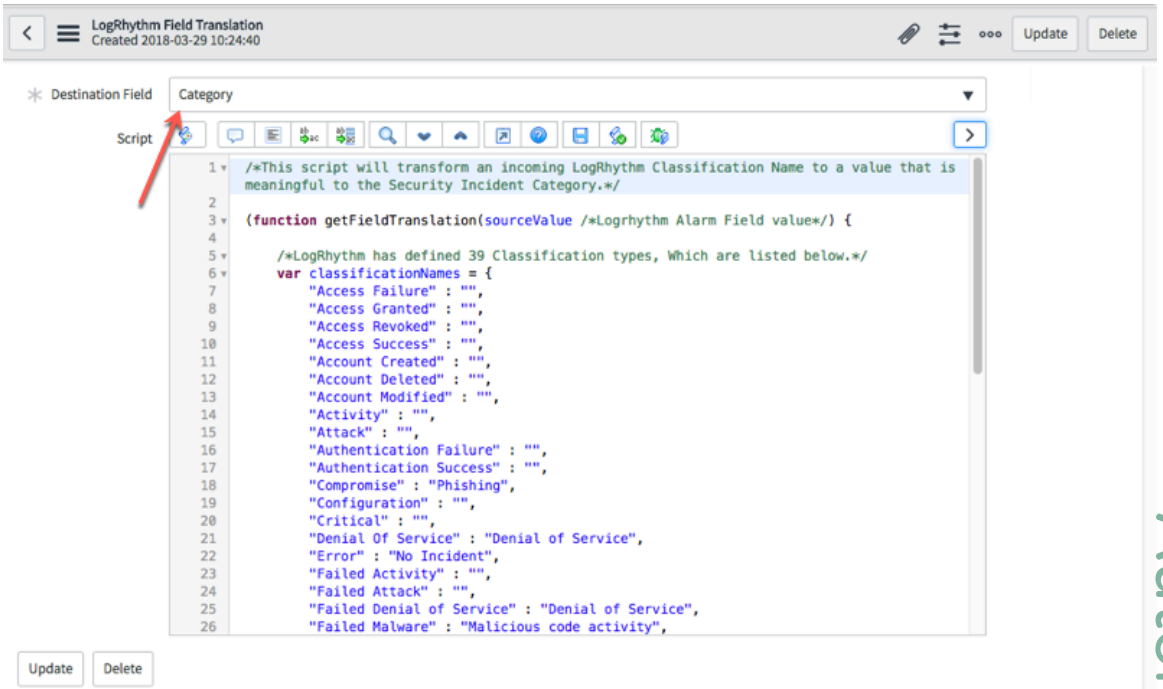
   In bestimmten Fällen ist eine Skripteinbindung für das Feld „Priorität“ geeignet. Für den Alarm LogRhythm wird beispielsweise eine risikobasierte Prioritätspunktzahl ein Wert zwischen 0 und 100 zugewiesen. In Now Platformunterstützt das Feld Priorität für einen Security Incident jedoch Werte zwischen 1 und 5. Wie in der vorherigen Abbildung dargestellt, übersetzt eine Skripteinbindung die Werte des Alarmfelds LogRhythm in die entsprechenden Werte, die vom -Feld im Security Incident in Now Platformunterstützt werden.

   In diesem Beispiel für das Feld Priorität gilt : Wenn der Alarmwert LogRhythm80 oder größer ist, wird im Feld Security Incident (Priorität) 1angezeigt. Dieser Wert entspricht einer kritischen Priorität im Security Incident. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf NULL gesetzt.

2. Geben Sie Änderungen ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern. Die Tabelle „Feldübersetzungen LogRhythm “ wird angezeigt.
3. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

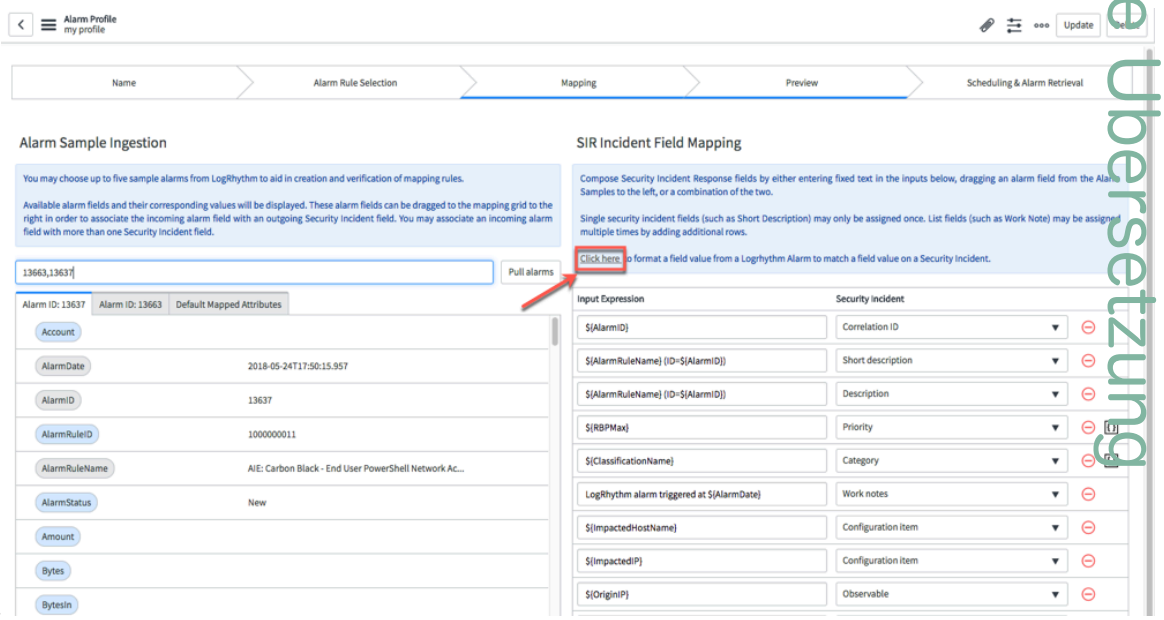
   Die folgende Abbildung zeigt den Skript-Editor mit ausgewählter Kategorie in der Auswahlliste Zielfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wenn Sie der Liste der Feldübersetzungen ein neues Feld hinzufügen möchten, führen Sie die folgenden Schritte aus, um einen neuen Datensatz hinzuzufügen.

   a. Klicken Sie bei angezeigtem Zuordnungsformular im Abschnitt „SIR-Incident-Feldzuordnung“ auf den Link **Hier**



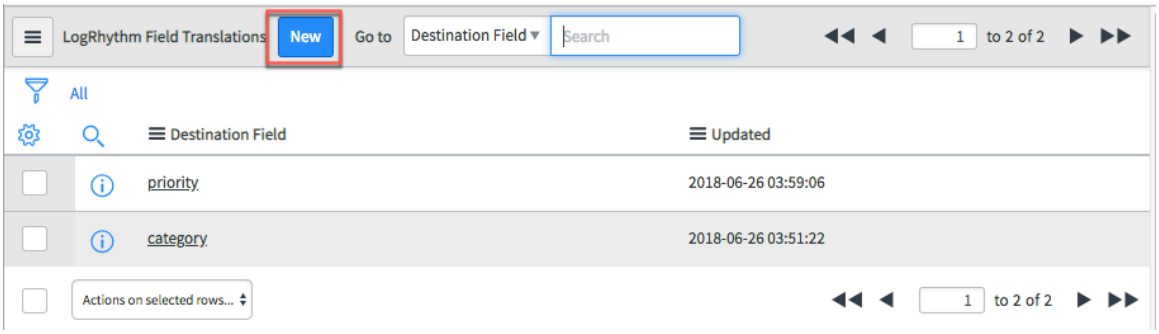
   klicken.

   Die Liste „Feldübersetzung LogRhythm “ mit den Feldern „Priorität“ und „Kategorieziel“ wird angezeigt.

   b. Klicken Sie auf „Neu“.

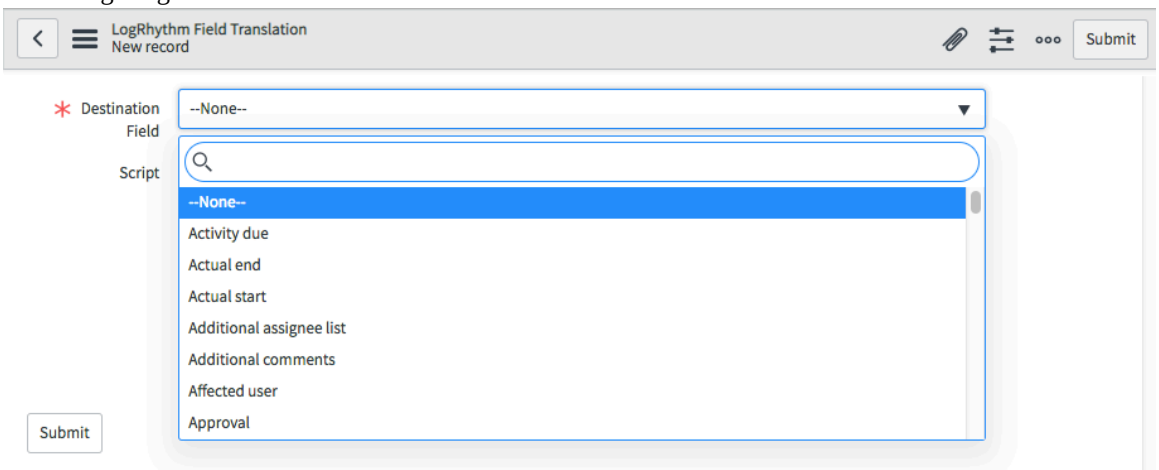
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ein neuer Datensatz wird angezeigt.

c. Wählen Sie in der Auswahlliste Zielfeld ein Zielfeld im Security Incident aus, für den die geskripteten Werte angezeigt werden sollen.



d. Klicken Sie auf **Absenden**.
Der Skript-Editor wird angezeigt.

e. Geben Sie die Änderungen in den Editor ein, und klicken Sie auf **Absenden**, um die Änderungen zu speichern.
Die Tabelle „Feldübersetzungen“ LogRhythm mit dem neuen Datensatz wird angezeigt.

5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Kopieren Sie ein Alarmprofil für LogRhythm

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt ein neues Alarmprofil zu erstellen. Wenn Sie mehrere Alarmprofile für verschiedene Arten von Alarmen erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, können Sie Alarmprofile kopieren, um Zeit zu sparen. Dieser Prozess ist optional.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

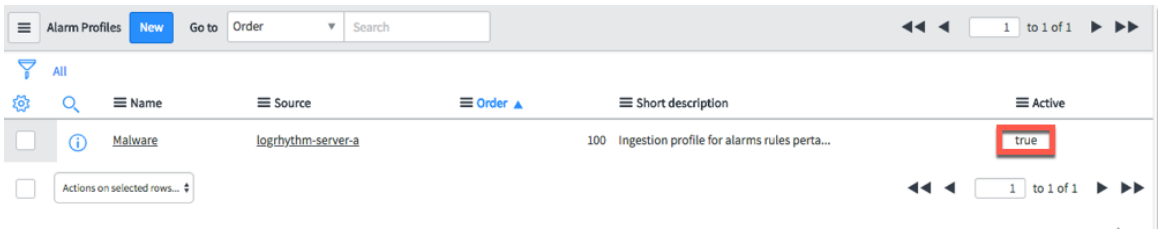
Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie ein Profil kopieren, wird der Profilname zunächst geändert, um doppelte Profile zu vermeiden. Außerdem wird das kopierte Profil auf inaktiv gesetzt, damit es nicht versehentlich aktiviert wird, bevor die Konfiguration abgeschlossen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

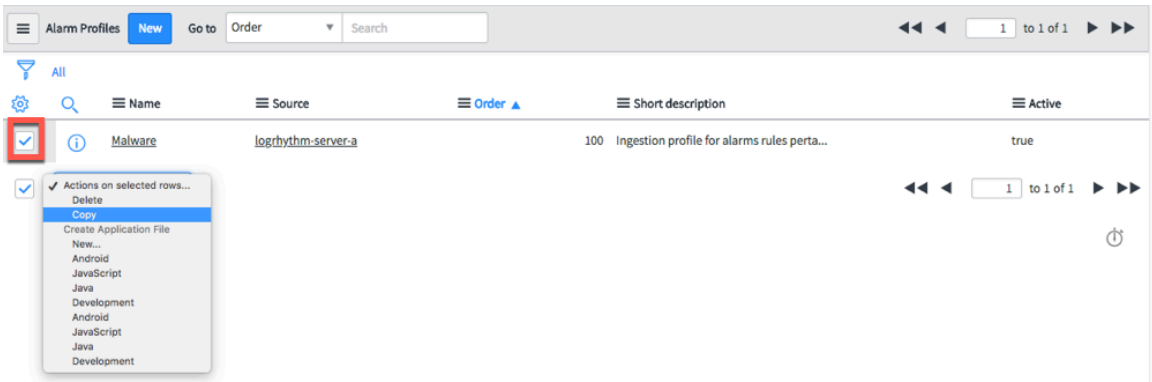
Prozedur

1. Navigieren zu **Alle** > **LogRhythm-Integration** > **LogRhythm-Alarmprofile**.

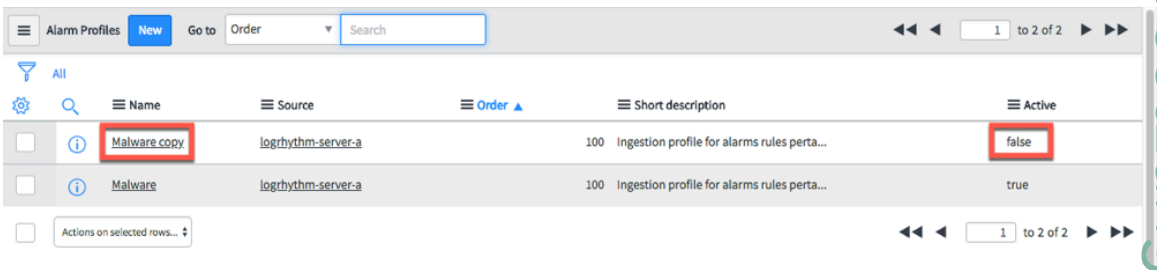
   Beachten Sie, dass in der angezeigten Liste die Spalte Aktiv angibt, ob das Profil aktiv ist (true).



2. Wählen Sie im Feld links neben der Spalte **Name** den Namen des Datensatzes aus.
3. Wählen Sie in der Auswahlliste **Aktionen für ausgewählte Zeilen** die Option **Kopieren aus**.



In der Liste **der Alarmprofile** wird sowohl das Kopie- als auch das Originalprofil angezeigt. Obwohl der ursprüngliche Datensatz aktiv ist, ist die Kopie zu diesem Zeitpunkt inaktiv (falsch). Nachdem Sie es konfiguriert haben, aktivieren Sie dieses kopierte Profil.



Sie können die Werte des kopierten Profils bearbeiten und es umbenennen, sodass abgerufene Alarmregeln für das neue Profil gelten. Sie werden aufgefordert, das neue Profil zu aktivieren, sobald die Konfigurationsschritte abgeschlossen sind.

Deaktivieren Sie das automatisierte Schließen von Alarmen für LogRhythm

Deaktivieren Sie die Funktion zum automatischen Schließen von Alarmen, wenn Sie die Informationen zum Schließen von Security Incidents in der -Webkonsole LogRhythm nicht mehr anzeigen möchten. Nach der Deaktivierung schließt Now Platform keine Alarme mehr in der Webkonsole LogRhythm. Dieser Prozess ist optional.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

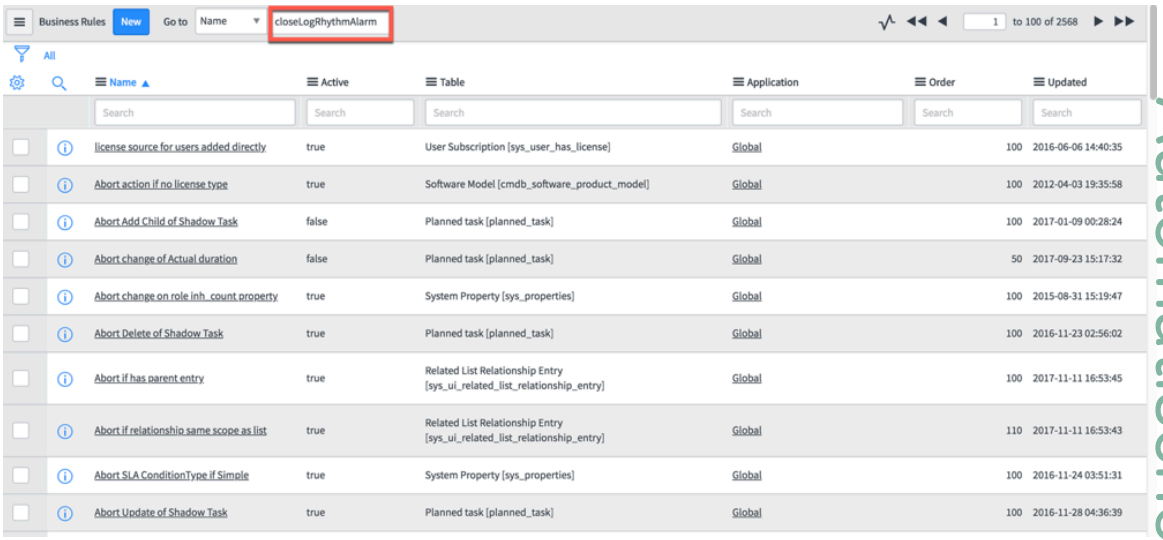
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Nach der Deaktivierung werden die Statusnotizen und andere Abschlussinformationen zum Security Incident nicht mehr in der Webkonsole LogRhythm angezeigt.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln** und wählen Sie das Modul **Geschäftsregeln** aus.
2. Falls er nicht in der Liste **Business-Regeln** angezeigt wird, geben Sie in das Suchfeld **LogRhythm Close Alarm On SI Close (Alarm bei SI-Schließung schließen)** ein, und drücken Sie **die Eingabetaste**.



3. Klicken Sie in der Spalte **„Name“** auf den Link **LogRhythm – Alarm bei SI-Abschluss schließen,** um den Datensatz zu öffnen.
4. Deaktivieren Sie im angezeigten Datensatz das Kontrollkästchen **Aktiv**.
5. Klicken Sie auf **Aktualisieren**.
   Die Funktion zum automatischen Schließen von Alarmen ist jetzt deaktiviert.

Zeigen Sie Drilldown-Ereignisse für LogRhythm an

Zeigen Sie die zugehörigen Roh- oder Basis-Ereignisse für einen LogRhythm -Alarm im Security Incident an.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Als Sicherheitsanalyst können Sie die zugehörigen Roh- oder Basisereignisse für einen LogRhythm -Alarm anzeigen, ohne zur Konsole LogRhythm zurückkehren zu müssen. Rufen Sie dazu eine zugehörige Liste auf, die alle Drilldown-Ereignisse für den Incident SIR enthält.

Prozedur

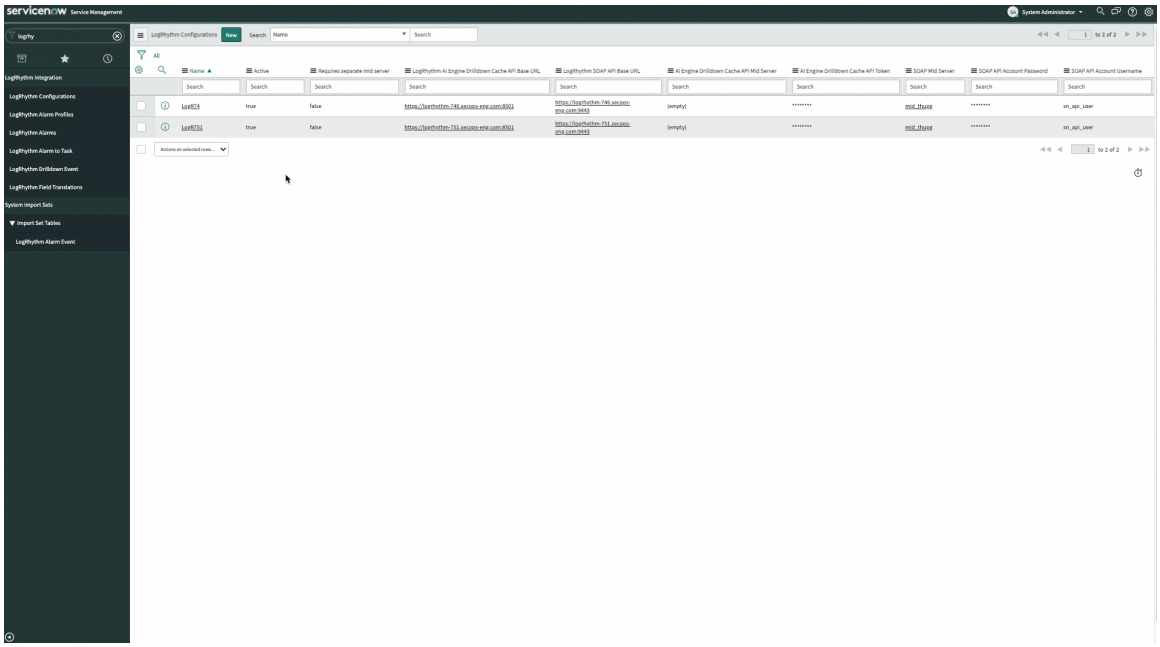
Navigieren zu **Alle** > **LogRhythm-Integration** > **LogRhythm-Drilldown-Ereignisse**.

Die folgende Abbildung zeigt, wie Sie zum Modul **LogRhythm-Drilldown-Ereignisse** navigieren, die Liste der Ereignisse **nach Alarm-ID für Gruppen**sortieren und auf den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugehörigen Security Incident klicken. Im Security Incident finden Sie die Registerkarte **LogRhythm-Drilldown-Ereignisse** unter den zugehörigen Links.



Problembehandlung bei der LogRhythm-Integration

Beheben Sie Konnektivitäts- und Alarmerfassungsprobleme.

Weitere Informationen zur Problembehandlung finden Sie in den folgenden Themen:

- Überprüfen Sie die Konnektivität für LogRhythm
- Skriptausführung und Systemprotokoll für LogRhythm

Überprüfen Sie die Konnektivität für LogRhythm

Überprüfen Sie Ihre Verbindung zur LogRhythm -Client-Konsole, indem Sie Locking-Anforderungen senden, um die LogRhythm -REST-API zu testen. Der Verifizierungsprozess ist optional.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Um zu überprüfen, ob die Verbindung zur LogRhythm -Client-Konsole nach dem Einrichten der LogRhythm -REST APIs ordnungsgemäß funktioniert, senden Sie zwei Locking-Anforderungen von dem Computer, der den in Installieren Sie das Plugin, und konfigurieren Sie es LogRhythmkonfigurierten MID-Server hostet.

Die LogRhythm REST API verwendet WSSE für die Authentifizierung, was einige externe Skripts erfordert, um mit Locken und Postman zu funktionieren.

Die LogRhythm REST API verwendet ein Token für die Authentifizierung, sodass Sie den tatsächlichen Validierungsaufruf durchführen können, den die -Integration verwendet. Die „0“ am Ende der URL ist eine LogRhythm Alarm-ID. Die LogRhythm REST API mit einer Standardkonfiguration benötigt Port 8501. Diese Portnummer sollte in der URL enthalten sein, die Sie für den Test verwenden möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Aktualisieren Sie die URL<LogRhythm REST url> und Token<api token> in der folgenden Rollenanforderung ein, und senden Sie sie, um die LogRhythm REST API zu validieren: **curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/json" -H "Autorisierung: Bearer** „ “https://<cache drilldown url> /lr-drilldown-cache-api/drilldown/0"
Für eine erfolgreiche Verbindung mit der REST API LogRhythm sollten Sie eine HTTP 404-Antwort erhalten, der Antworttext enthält jedoch Alarm ID: 0 not gefunden.

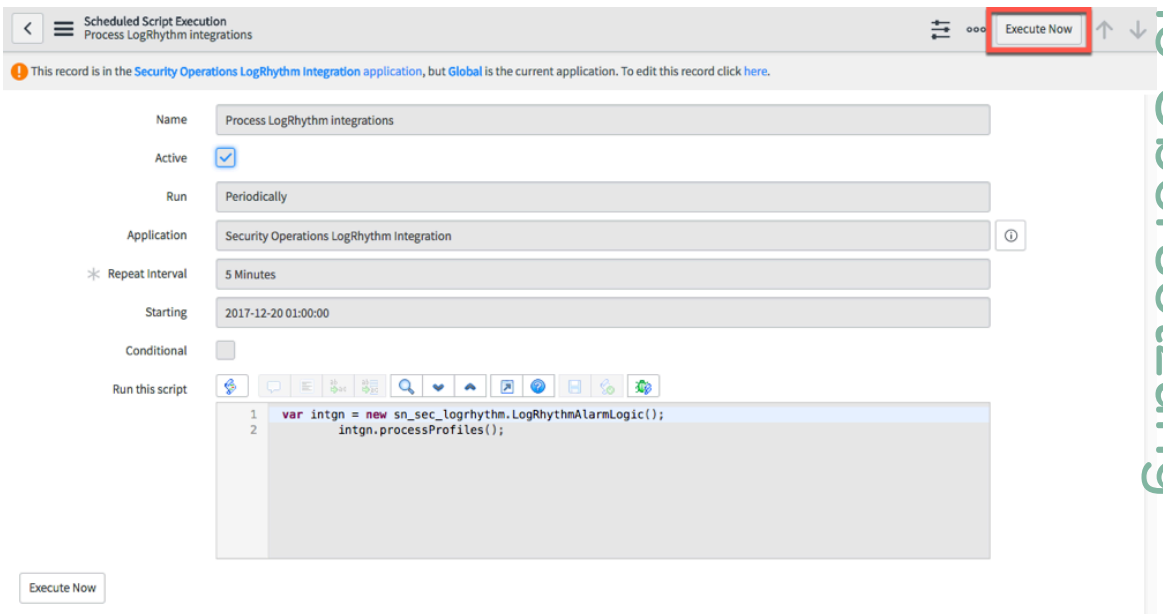
Skriptausführung und Systemprotokoll für LogRhythm

Wenn Sie ein Problem bei der Alarmerfassung beheben, können Sie das standardmäßige Abfrageintervall von fünf Minuten überschreiben, um die Ergebnisse sofort anzuzeigen. Rufen Sie in diesem Szenario die Skriptausführung manuell auf, um eine Abfrage auszuführen. Diese Ausführung ist optional.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Geplante Aufgabe** > **Geplante Aufgaben** und wählen Sie das Modul **Geplante Aufgaben** aus.
2. Klicken Sie auf den Integrationsaufgaben-Datensatz Prozess LogRhythm.
3. Klicken Sie im angezeigten Datensatz Geplante Skriptausführung **auf Jetzt ausführen**.



Wenn Sie weitere Hilfe bei der Problembehandlung benötigen, können Sie auf das Systemprotokoll für die LogRhythm -Abfragen zugreifen.

4. Bei anderen allgemeinen Problembehandlungsproblemen führen Sie die folgenden Schritte aus, um auf die Systemprotokolle zuzugreifen.

   a. Navigieren zu **Systemprotokoll** > **Alle** und wählen Sie **Alle**aus.

   b. Setzen Sie den Filter (Gehe zu) auf **Quelle**, und geben Sie sn_sec_logrhythmein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Drücken Sie die **Eingabetaste**.
Alle von der Integration generierten Nachrichten werden in dieser Tabelle angezeigt. Die aufgelisteten Nachrichten bieten Einblicke in die laufenden Prozesse der Integration und helfen Ihnen möglicherweise bei der weiteren Problembehandlung.

McAfee ePO Integration

Die Funktion „Endpoint Detection and Response (EDR) der McAfee ePO -Integration, die Analysten des Security Operations Center (SOC) hilft, Cyberbedrohungen zu identifizieren und den durch schädliche Dateien verursachten Schaden zu beheben.

Übersicht

In dieser Integration werden zwei Gruppen von McAfee ePO -Fähigkeiten verwendet: zum einen die Fähigkeiten, die Aktionen aufrufen, z. B. das Isolieren eines Hosts und das Initiieren eines Malware-Scans, und zum anderen die Fähigkeiten, die Abfragen ausführen, um Systemdetails und Bedrohungsereignisse zu erfassen. Beide Arten von Fähigkeiten, Aktionen und Abfragen, werden von Ihrer Instanz Now Platform® aus aufgerufen. Sie können diese Fähigkeiten so gruppieren, dass sie automatisch ausgeführt werden, wenn ein bestimmter Typ von Sicherheitsereignis auftritt, oder Sie können sie manuell über einen Security Incident Now Platform® aufrufen.

Die folgenden McAfee ePO -Fähigkeiten sind für diese Integration verfügbar.

Ruft Systemdetails ab

Erfassen Sie Systemdetails, einschließlich Details zum Betriebssystem.

Initiieren Sie die Malware-Prüfung

Initiieren Sie basierend auf der Scan-Konfiguration und -Zeitplanung einen Scan eines betroffenen Endpunkts.

Host isolieren/die Isolierung aufheben

Entfernen Sie ein System zu Untersuchungszwecken aus dem Netzwerkzugriff, und stellen Sie den Zugriff auf das Netzwerk wieder her.

Bedrohungsereignisse auflisten

Compliance-Status und aktuelle Bedrohungsereignisse erfassen

Schlüsselfunktionen

Diese Integration enthält die folgenden Schlüsselfunktionen.

- Unterstützt die automatisierte Auslösung von Abfragen McAfee ePO, die auf Incident-Bedingungen basieren.
- Unterstützt das manuelle Starten von McAfee ePO -Fähigkeiten aus Now Platform® Security Incident Response (SIR) Security Incidents, die bei Bedarf Aktionen ausführen.
- Die Flexibilität, mehrere Profile zum Auslösen verschiedener Arten von McAfee ePO - und Now Platform® Security Operations -Fähigkeiten zu erstellen. Diese Profile sammeln Informationen zu Bedrohungsereignissen oder führen Aktionen basierend auf den Bedingungen bestimmter Incident-Kategorien wie Malware aus.
- Validieren Sie Ihre Profilkonfiguration mit einer Vorschau der McAfee ePO -Ergebnisse für SIR -Security Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Tagging aktiviert ist, geben Sicherheits-Tags an, welche McAfee ePO -Fähigkeiten anfänglich von einem Workflow gestartet werden und wann die Abfragen oder Aktionen erfolgreich abgeschlossen wurden.
- Ein vollständiger Audit-Pfad der McAfee ePO Abfragen und Aktionen wird in den Arbeitsnotizen zu SIR den Security Incidents veröffentlicht, und Befehle von Now Platform® werden in der Konsole McAfee ePO protokolliert.
- Unterstützt mehrere McAfee ePO -Konsolen.

ServiceNow Plugins

Das Plugin com.snc.si_dep ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations -Anwendungen müssen über ServiceNow Storeinstalliert und aktiviert werden. Installieren Sie eine Anwendung nach der anderen in der unten aufgeführten Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response
5. Arbeitsbereich für Security Incident Response

Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration McAfee ePO ein.

Das Erweiterungs-Plugin ServiceNow

Die ServiceNow Security Operations-Erweiterung für das McAfee ePO-# Erweiterungs-Plugin ist für diese Integration erforderlich. Sie installieren dieses ServiceNow Plugin in Ihrer McAfee ePO -Konsole. Weitere Informationen finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration McAfee ePO ein.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrer Instanz Now Platform®, um eine Verbindung zum Server McAfee ePO (Konsole) herzustellen. Weitere Informationen zu MID-Servern finden Sie auf der Website der ServiceNow-Produktdokumentation .

Unterstützte Versionen von McAfee

Die Integration unterstützt Version 5.9.1 und 5.10 von McAfee ePO. Unterstützt McAfee Agent: MA 5.5.1.388 Weitere Informationen zu McAfee-Produkten und ePolicy Orchestrator finden Sie auf der McAfee-Produktwebsite .

Die Integration unterstützt Version 10.5 des Produkts McAfee Endpoint Security Threat Prevention. Wenn Sie Version 10.5 nicht ausführen, wenden Sie sich an Ihren McAfee

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ePO -Administrator, um zu erfahren, ob Ihre Version Scans bei Bedarf über Tag-Aktionen unterstützen kann.

McAfee ePO Sicherheits-Tags werden in dieser Integration verwendet. Sie müssen diese Tags in Ihrer McAfee ePO -Konsole erstellen. Weitere Informationen zu diesen Tags finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..

Referenzen

Referenz	Dokumentbezeichner	Dokumententitel
1	McAfee-Produktwebsite	McAfee-Produktwebsite
2	McAfee Business-Produktdokumentation für ePolicy Orchestrator Cloud	McAfee-Produktdokumentation
3	ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

Eine Prüfliste zum Nachverfolgen Ihres Fortschritts bei der Einrichtung, Installation und Überprüfung der Ergebnisse für die Integration finden Sie unter Prüfliste für die McAfee ePO -Integration.

Damit die Installation der Anwendung reibungslos verläuft und Sie die erwarteten Ergebnisse überprüfen können, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.

Zugehörige Informationen

Integrationsarchitektur für McAfee ePO

Integrationsarchitektur für McAfee ePO

Das folgende Thema bietet einen Überblick über die Systemarchitektur von und listet die wichtigsten Funktionen der Integration auf. Dieser Abschnitt enthält auch Informationen zu den Setupschritten, die Sie in Ihrer -Instanz Now Platform und in der McAfee ePolicy Orchestrator-Konsole (McAfee ePO) ausführen müssen, bevor Sie die Anwendung von ServiceNow Storeinstallieren.

Schlüsselbegriffe für die McAfee ePO Integration

Die folgenden Begriffe werden in der gesamten Installations- und Konfigurationsdokumentation für die Integration verwendet.

Now Platform

Ein Produkt des Unternehmens ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management, (ITSM) und andere -Produkte basieren.

Security Incident Response (SIR)

Eine Anwendung Now Platform, die den Fortschritt von Security Incidents von der Discovery und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur abschließenden Überprüfung und Schließung nach Incident verfolgt.

Plugin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugins sind Softwarekomponenten, die bestimmte Funktionen und Funktionalitäten innerhalb Ihrer Instanz Now Platform bereitstellen. Weitere Informationen zur Installation und Konfiguration der Integrations-Plugins finden Sie unter Installieren Sie die Anwendung, und konfigurieren Sie einen Server für die McAfee ePO -Integration.

ePolicy Orchestrator (McAfee ePO)

Die Anwenderkonsole, mit der Sie die McAfee-Services, -Produkte und -Einstellungen verwalten.

McAfee-Erweiterungs-Plugin

Dieses ServiceNow Erweiterungs-Plugin ist für diese Integration erforderlich. Dieses Plugin befindet sich in Ihrer McAfee ePO -Konsole und verbindet Ihre McAfee ePO -Konsole mit Ihrer Now Platform -Instanz.

Fähigkeit

Eine automatische Aktivität, die von Ihrer Instanz Now Platform initiiert und in der Konsole McAfee ePO ausgeführt wird, um Ergänzungsabfragen und Aktionen für Ihre Assets durchzuführen.

Profil

Einstellungen für Fähigkeiten McAfee ePO, die Sie konfigurieren, um festzulegen, wann und unter welchen Bedingungen Fähigkeiten Ergänzungsabfragen und Aktionen für Ihre Assets durchführen.

MID-Server

Eine Anwendung, die die Kommunikation und die Bewegung von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services erleichtert.

ServiceNow Administrator (admin)

Ein Benutzer mit dieser Rolle lädt die Plugins SIR und McAfee ePO zu Ihrer Instanz Now Platform herunter und installiert sie. Ein Benutzer mit dieser Rolle weist bei Bedarf auch die Rolle „Security Incident-Administrator“ zu.

ServiceNow Security Incident-Administrator (sn_si.admin)

Ein Benutzer mit dieser Rolle führt die Konfiguration der McAfee ePO -Integration mit dem Produkt Security Incident Response (SIR) in Ihrer Instanz Now Platform nach Bedarf durch. Ein Benutzer mit dieser Rolle weist bei Bedarf auch die Rolle „Analyst für Security Incidents“ zu.

ServiceNow Security Incident-Analyst (sn_si.analyst)

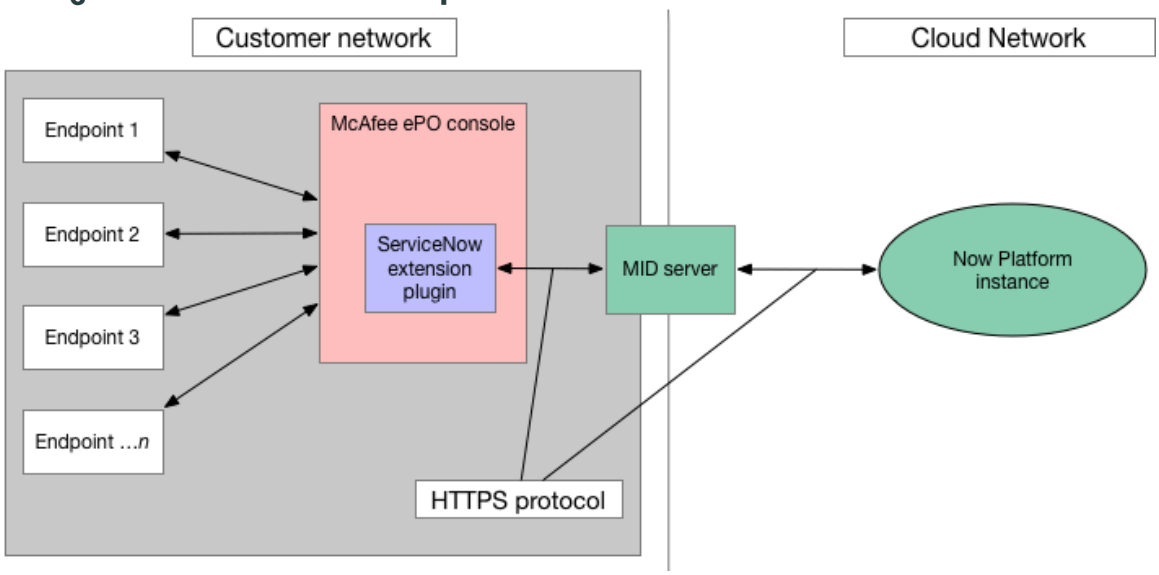
Ein Benutzer mit dieser Rolle interagiert mit Security Incidents im Produkt SIR und analysiert sie.

Systemverbindung und Datenfluss

Die folgende Abbildung zeigt ein Beispiel für eine Kundenumgebung. Ein MID-Server Now Platform ist erforderlich, damit Ihre Instanz Now Platform über ein ServiceNow -Erweiterungs-Plugin eine Verbindung zu einem McAfee ePO -Server (Konsole) herstellen kann. Nachdem die Verbindung hergestellt wurde, rufen Sie Fähigkeiten von Ihrem Now Platform auf, um Malware-Scans zu initiieren, Hostcomputer zu isolieren und in Ihrem Netzwerk wiederherzustellen, die letzten Scan-Ergebnisse abzurufen und Systemdetails zu Ihren Assets zu erfassen. Wenn diese Fähigkeiten Ergebnisse von Ihren Assets zurückgeben, die Ihren Suchkriterien entsprechen, werden Daten über den MID-Server in Ihre Instanz Now Platform abgerufen. Daten werden in den zugehörigen Listen eines Security Incident Now Platform Security Incident Response (SIR) angezeigt. Die folgende Abbildung zeigt den Daten-Flow für eine Gruppe von Endpunkten, die von einer McAfee ePO -Konsole verwaltet werden.

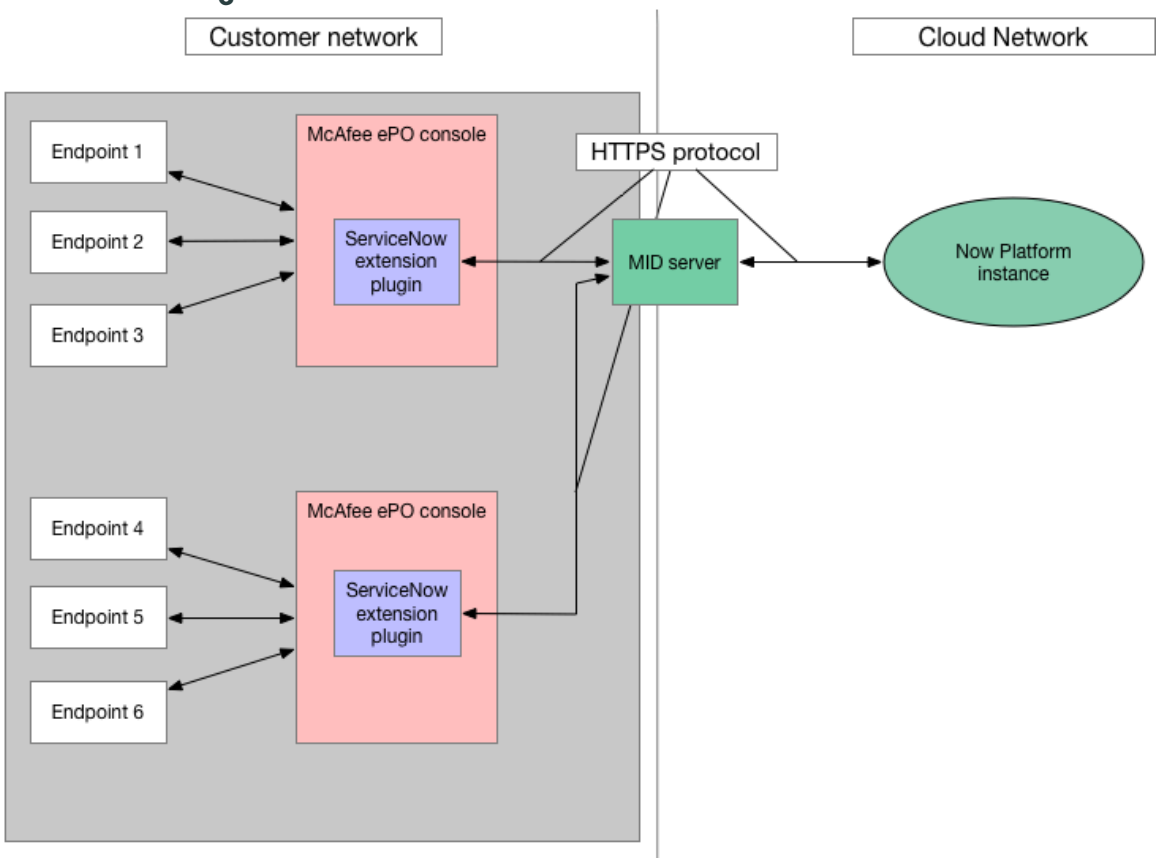
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration eines einzelnen Endpunkts



Wie in der folgenden Abbildung dargestellt, kann diese Integration mehr als eine McAfee ePO -Konsole unterstützen. Sie können eine Gruppe von Endpunkten von einer McAfee ePO -Konsole und eine weitere Gruppe von Endpunkten von einer anderen McAfee ePO -Konsole verwalten. Daten von mehreren McAfee ePO -Konsolen werden über einen einzigen MID-Server abgerufen. Sie können jedoch auch mehrere MID-Server konfigurieren, wenn Ihre Organisation dies erfordert.

MID-Serverkonfiguration



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflows für die -Integration McAfee ePO .

Diese Integration umfasst die folgenden Workflows. Diese Workflows sind vorkonfiguriert und wurden speziell für diese Integration entwickelt. Sie können diese Workflows bei Bedarf so bearbeiten, dass sie den Anforderungen Ihrer Organisation entsprechen. Allgemeine Informationen zu Workflows und zur Verwendung des Workflow-Editors finden Sie unter Erste Schritte mit Workflows .

- McAfee ePO-Integration für Security Operations: Hostdetails abrufen
- Integration von McAfee ePO in Security Operations – Malware-Scan initiieren
- Integration von McAfee ePO in Security Operations – Host isolieren
- Integration von McAfee ePO in Security Operations – Bedrohungsereignisse auflisten
- Integration von McAfee ePO in Security Operations – Isolation entfernen

Verbindung mit externen Systemen

Die Integration erfordert, dass der MID-Server über eine HTTPS-Protokollverbindung mit der McAfee ePO -Konsole kommuniziert.

Prüfliste für die McAfee ePO -Integration

Verwenden Sie diese Prüfliste, um sich durch alle Aufgaben der Integration zu führen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle mit den erwarteten Ergebnissen für die Integration.

Vorbereitungen
Erforderliche Rolle: Für jeden Schritt werden Rollen aufgelistet.

Warum und wann dieser Vorgang ausgeführt wird
Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration anhand der folgenden Tabelle. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jede Zeile der Tabelle listet Aufgaben auf und gibt die Rollen an, die zum Ausführen der Aufgaben erforderlich sind. Außerdem wird auf nummerierte Themen im Installations- und Konfigurationsleitfaden verwiesen.

Prozedur

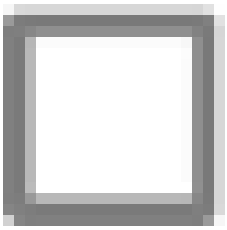
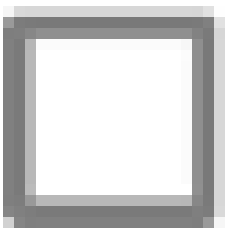
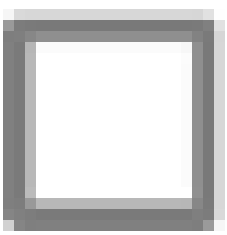
Befolgen Sie die Schritte in der Tabelle in der Reihenfolge, in der sie angezeigt werden.

Prüfliste

Artikel	Beschreibung
☐	Richten Sie als Benutzer mit der Administratorrolle Now Platform® Ihre Instanz Now Platform® ein. **a.** Weisen Sie die Rollen Now Platform® und Security Incident Response zu. **b.** Stellen Sie sicher, dass alle ServiceNow Security Incident Response und andere Plugins, die die Integration unterstützen, für Ihr Release von Now Platforminstalliert und aktiviert sind. **c.** Installieren und konfigurieren Sie einen MID-Server in Ihrer Instanz Now Platform®.

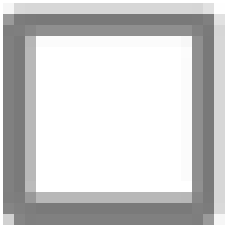
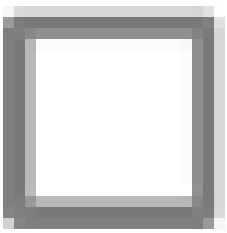
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	d. Erstellen Sie eine Genehmigungsgruppe, wenn Sie Anforderungen verarbeiten möchten, die vom Security Incident-Analysten für den Host zum Isolieren übermittelt wurden, und Malware-Scan-Aktionen initiieren möchten. Weitere Informationen finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration McAfee ePO ein.
	Richten Sie als McAfee ePO -Administrator Ihre McAfee ePO -Konsole ein. **a.** Stellen Sie sicher, dass Sie Version 5.9 von McAfee ePOverwenden. **b.** Installieren Sie das Erweiterungs-Plugin ServiceNow in Ihrer McAfee ePO -Konsole. **c.** Vergewissern Sie sich, dass Sie in Ihrer McAfee ePO -Konsole Sicherheits-Tags für die Aktion „Host isolieren“ und „Initiieren“ von Malware-Scan-Aktionen erstellt haben. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein.. Um weitere Informationen zu erhalten und die Erweiterungs-Plugin-Datei zu erhalten, navigieren Sie in Ihrer Instanz Now Platform zu **Wissen** > **Artikel** > **Alle** und geben Sie im Feld Suchen ServiceNow Security Operations Extension for McAfee ePOein.
	Als Benutzer mit der Administratorrolle Now Platform installieren Sie die Anwendung McAfee ePO von ServiceNow Store, konfigurieren Sie einen -Server, und stellen Sie eine Verbindung zur Konsole McAfee ePO her. Weitere Informationen finden Sie unter Installieren Sie die Anwendung, und konfigurieren Sie einen Server für die McAfee ePO -Integration.
	Bearbeiten Sie als Benutzer mit der Rolle „Security Incident-Administrator“ Now Platform die Sicherheits-Tag-Namen in Ihrer Instanz Now Platform® so, dass sie mit den Tag-Namen übereinstimmen, die Sie in der Konsole McAfee ePO erstellt haben. Weitere Informationen finden Sie unter Bearbeiten Sie Sicherheits-Tags in Now Platform für die McAfee ePO -Integration.
	Erstellen Sie als Benutzer mit der Rolle „Security Incident-Administrator“ ein Profil für die Fähigkeiten McAfee ePO. Informationen zu Profilen finden Sie unter McAfee ePO Integrationsfähigkeitsprofile. Informationen zu den Schritten zum Erstellen eines Profils finden Sie unter Erstellen Sie ein Fähigkeitsprofil für die Integration McAfee ePO ..

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	Als Benutzer mit der Rolle „Security Incident-Administrator“ können Sie ein Profil konfigurieren und Security Incidents testen. **a.** Überprüfen Sie die Informationen zu den Auslösebedingungen und -einstellungen. **b.** Konfigurieren Sie ein Profil. **c.** Testen Sie Security Incidents, und zeigen Sie eine Vorschau an. **d.** Suchen Sie Suchergebnisse und andere Details in den zugehörigen Listen im Security Incident. **e.** Erstellen und konfigurieren Sie verschiedene Arten von Profilen, und testen Sie Security Incidents für jeden Typ. Informationen zu Auslösebedingungen und dem alternativen CI-Feld finden Sie unter Definieren von Auslösebedingungen mit einem Feld Configuration Item (CI) für ein McAfee ePO -Profil. Informationen zu den Schritten zum Konfigurieren eines Profils sowie zum Testen und Anzeigen von Security Incidents und zu Beispielen für Profiltypen finden Sie in den Beispielen nach Profile für die Integration McAfee ePO werden konfiguriert.
	Senden Sie als Benutzer mit der Rolle „Security Incident-Analyst“ Now Platform zusätzliche Anforderungen für Malware-Scans und Listen-Bedrohungsereignisse. Weitere Informationen finden Sie unter Lösen Sie das Profil McAfee ePO manuell über einen Security Incident aus In Now Platformkönnen Sie als Benutzer mit Genehmigungsrolle oder als Mitglied einer Genehmigungsgruppe Anforderungen für die Hostisolierung isolieren und die Isolierung entfernen. Weitere Informationen zur Verarbeitung von Genehmigungsanforderungen finden Sie unter Erstellen Sie eine Genehmigungsgruppe.

Sie haben die Einrichtungsschritte erfolgreich abgeschlossen, die Anwendung installiert und konfiguriert und die erwarteten Ergebnisse für die Integration überprüft.

Richten Sie Ihre Instanz Now Platform® für die Integration McAfee ePO ein

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung für die Integration McAfee ePO installieren.

Richten Sie Anforderungen ein

Erforderliche Rolle: Now Platform Administrator (admin). Überprüfen Sie die folgenden Informationen vor Ihrer Instanz von Now Platform® für die Integration McAfee ePO.

Die folgende Tabelle enthält eine Liste der Setup-Anforderungen für die Anwendung. Vergewissern Sie sich, dass Sie diese Aufgaben abgeschlossen haben, bevor Sie die Anwendung für die -Integration aus ServiceNow Storeinstallieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie die Aufgabe ein	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben.	Die folgenden Rollen sind erforderlich: • Ein Benutzer mit der Rolle „Systemadministrator“ (admin) zum Installieren der Anwendung • Ein Benutzer mit der Rolle „Security Incident-Administrator“ (sn_si.admin) konfiguriert die Anwendung und erstellt, aktiviert und entfernt Profile. • Ein Benutzer mit der Rolle „Security Incident-Analyst“ (sn_si.analyst) arbeitet mit Security Incidents. Zu den Aufgaben gehört das manuelle Starten von Profilen aus Security Incidents. Wenn die Genehmigungsoption während des Konfigurationsschritts in einem Profil ausgewählt wird, senden Benutzer mit dieser Rolle auch Anforderungen, um Hosts zu isolieren und an das Netzwerk zurückzugeben.
Stellen Sie sicher, dass Sie Version 5.9 von McAfee ePOverwenden.	Die Integration unterstützt Version 10.4.3 des McAfee ePolicy Orchestrator.
Stellen Sie sicher, dass das Erweiterungs-Plugin ServiceNow in Ihrer McAfee ePO -Konsole installiert ist.	Installieren Sie das Plugin ServiceNow in Ihrer Konsole McAfee ePO. Um weitere Informationen zu erhalten und die Plugin-Datei zu erhalten, navigieren Sie in Ihrer Instanz Now Platform zu **Wissen** > **Artikel** > **Alle** und geben Sie im Feld Suchen ServiceNow Security Operations Extension for McAfee ePO ein.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Das Plugin „Security Incident Response Dependency“ (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie die Aufgabe ein	Beschreibung
	1. Security Incident Response **2.** Arbeitsbereich für Security Incident Response **3.** Security Integration Framework **4.** Security Support Common **5.** Security Support Orchestration Weitere Informationen zur Installation der Security Operations-Kernanwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.
Stellen Sie sicher, dass Sie einen MID-Server installiert und konfiguriert haben.	In Ihrer Instanz Now Platform® ist ein installierter und konfigurierter MID-Server erforderlich. Weitere Informationen zu MID-Servern finden Sie auf der Website der ServiceNow-Produktdokumentation .
Wenn Sie den Genehmigungsprozess für Profile aktivieren möchten, vergewissern Sie sich, dass Sie eine Genehmigungsgruppe zur Verarbeitung von Anforderungen erstellt haben.	Es ist ein optionaler Genehmigungsprozess verfügbar, um Hostcomputer zu isolieren und im Netzwerk wiederherzustellen. Wenn diese Option aktiviert ist, ist eine vorherige Genehmigung erforderlich, bevor Hostcomputer isoliert und in Ihrem Netzwerk wiederhergestellt werden. Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünscht, aktivieren Sie die Option **Genehmigung erforderlich** während des Konfigurationsschritts für ein Profil. Standardmäßig wird die Genehmigungsberechtigung dem Security Incident-Administrator Now Platform® (sn_si.admin) zugewiesen. Diese Berechtigung kann einer Genehmigungsgruppe neu zugewiesen werden. Innerhalb der Gruppe hat jedes Mitglied die Berechtigung, Anforderungen zu genehmigen oder abzulehnen. Sie wählen während des Konfigurationsschritts Ihrer Profileinrichtung eine aktive Genehmigungsgruppe aus. Weitere Informationen finden Sie unter Erstellen Sie eine Genehmigungsgruppe.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein.

Im folgenden Abschnitt werden die Setup-Schritte aufgeführt, die Sie in der Konsole McAfee ePO ausführen müssen, bevor Sie die Anwendung von ServiceNow Store für die Integration installieren.

Vorbereitungen

Erforderliche Rolle: McAfee ePO Administrator

Stellen Sie als Benutzer mit der Administratorberechtigung McAfee ePO sicher, dass das Erweiterungs-Plugin „Servicenow.zip“ in Ihrer McAfee ePO -Konsole installiert ist. Dieses Erweiterungs-Plugin ist für die Integration erforderlich. Um weitere Informationen zu erhalten und das Plugin zu erhalten, navigieren Sie in Ihrer Instanz Now Platform zu **Wissen** > **Artikel** > **Alle**. Geben Sie im Feld Suche ServiceNow Security Operations Extension for McAfee ePO ein.

Warum und wann dieser Vorgang ausgeführt wird

Das Erweiterungs-Plugin ServiceNow verbindet Ihre Instanz Now Platform mit der -Konsole McAfee ePO. Über diese Verbindung können Sie auf die Sicherheits-Tags verweisen, die Sie in der Konsole McAfee ePO für den Host zum Isolieren erstellen, und Malware-Scan-Aktionen für die Fähigkeitsprofile in Ihrer Instanz Now Platform initiieren.

Die Sicherheits-Tags in Ihrer McAfee ePO -Konsole müssen mit den Sicherheits-Tags in den Fähigkeitsdatensätzen in Ihrer Now Platform -Instanz übereinstimmen.

Die folgenden Schritte zeigen, wie Sie das -Erweiterungs-Plugin installieren, in der Konsole McAfee ePO ein Sicherheits-Tag erstellen und dem Tag eine Aktion zuweisen. Weitere Informationen zu den Sicherheits-Tags in der Konsole McAfee ePO finden Sie auf der Website der McAfee-Produktdokumentation .

Hinweis:
Die Abbildungen im folgenden Abschnitt stammen aus der Konsole McAfee ePO.

Prozedur

1. Wenn Sie das Erweiterungs-Plugin ServiceNow nicht auf Ihrer McAfee ePO -Konsole installiert haben, führen Sie die folgenden Schritte aus, um es zu installieren.

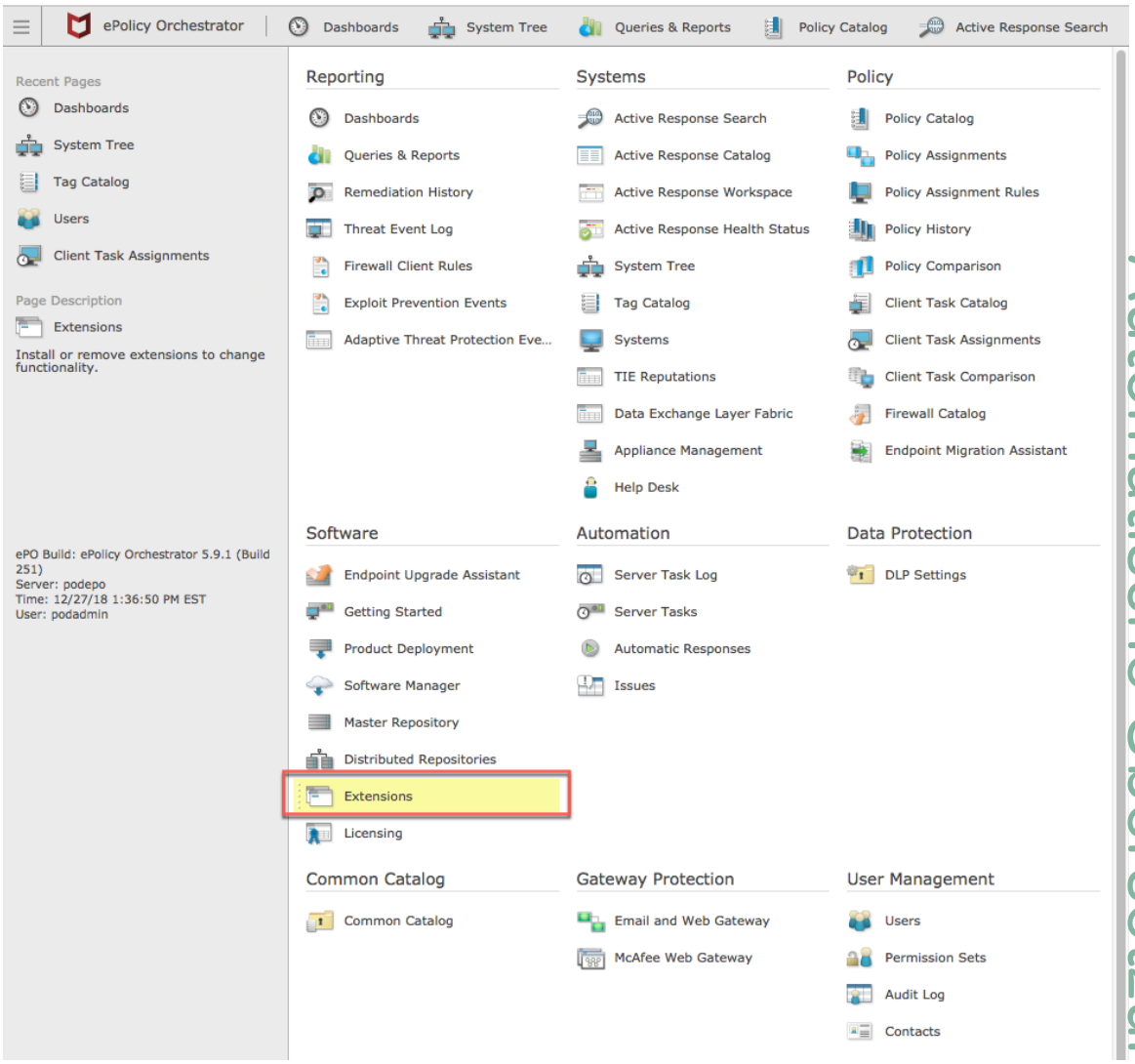
   a. Melden Sie sich mit Ihrem McAfee-Anwendernamen und Passwort bei der McAfee ePO -Konsole an.

Automatische Übersetzung

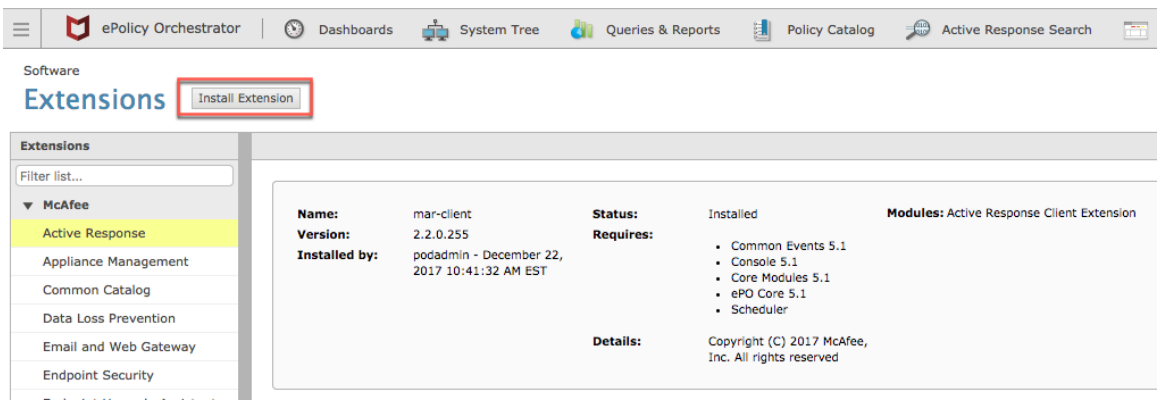
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wenn die in der folgenden Abbildung gezeigte Seite nicht angezeigt wird, klicken Sie oben links im Banner der Homepage auf das Menüsymbol, um sie anzuzeigen.

3. Klicken Sie im Abschnitt „Software“ auf den Link **Erweiterungen**.



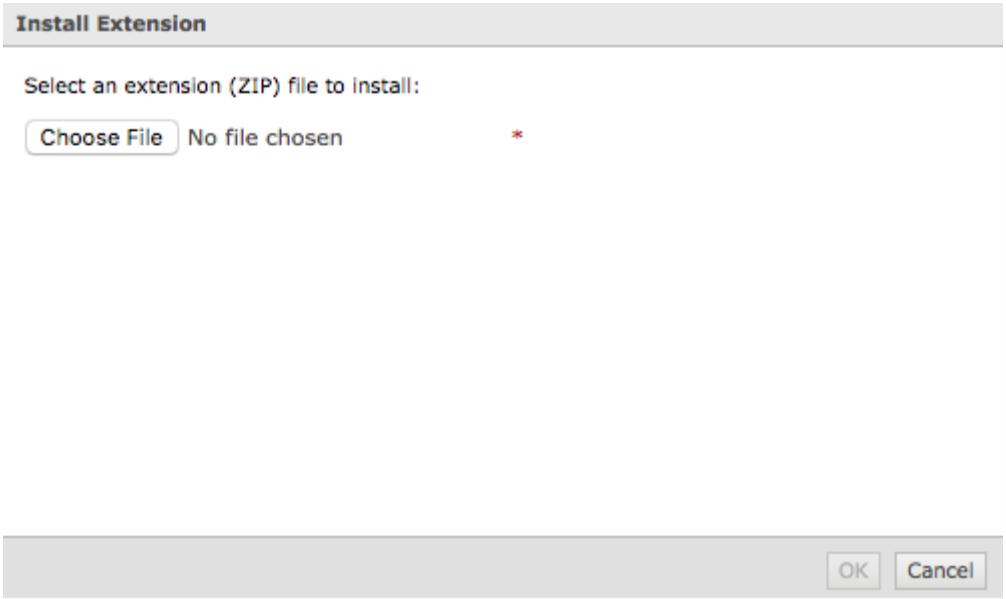
4. Klicken Sie auf der Seite „Erweiterungen“, die angezeigt wird, **auf Erweiterung installieren**.



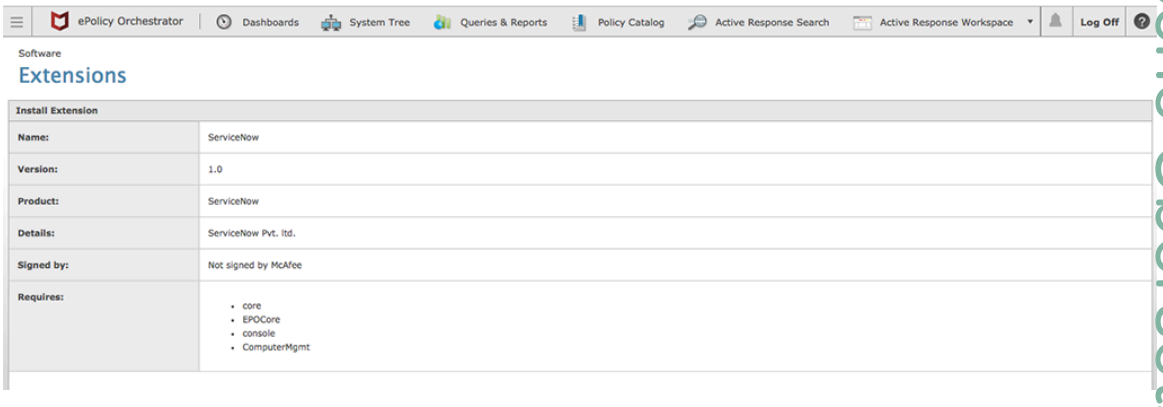
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie im Dialogfeld „Erweiterung installieren“ **auf Datei wählen**, navigieren Sie zur Datei Servicenow.zip auf Ihrem System, und klicken Sie auf **OK**, um sie herunterzuladen.



Nach Abschluss des Downloads wird die Seite „Softwareerweiterungen“ mit dem aufgelisteten Erweiterungs-Plugin ServiceNow angezeigt.



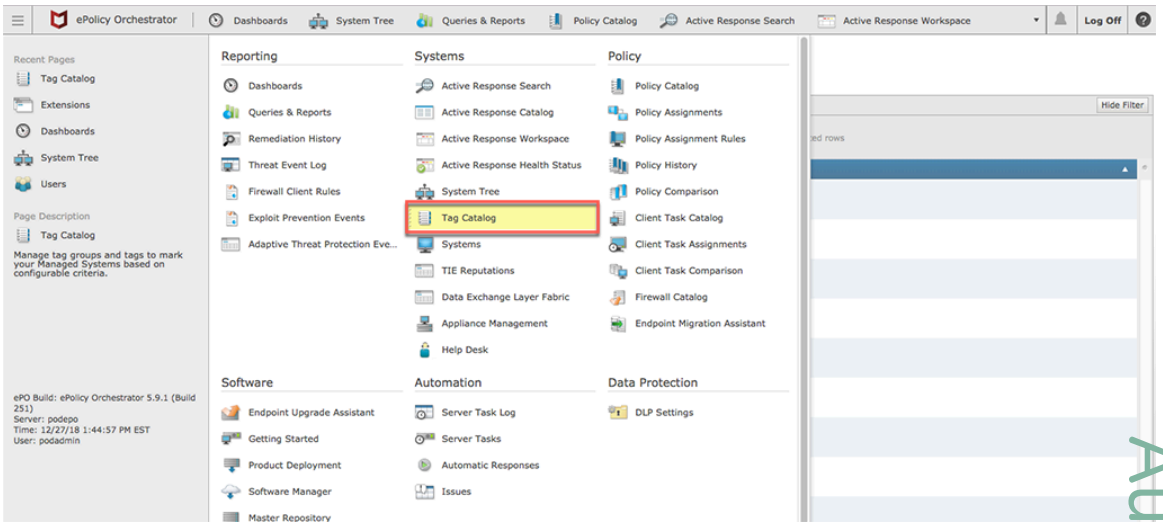
Sie haben die Plugin-Erweiterung ServiceNow erfolgreich in Ihrer McAfee ePO -Konsole installiert.

6. Wenn Sie in der Konsole McAfee ePO keine Sicherheits-Tags für die Aktionen „Malware-Scan initiieren“ und „Host isolieren“ erstellt haben, führen Sie die folgenden Schritte aus.

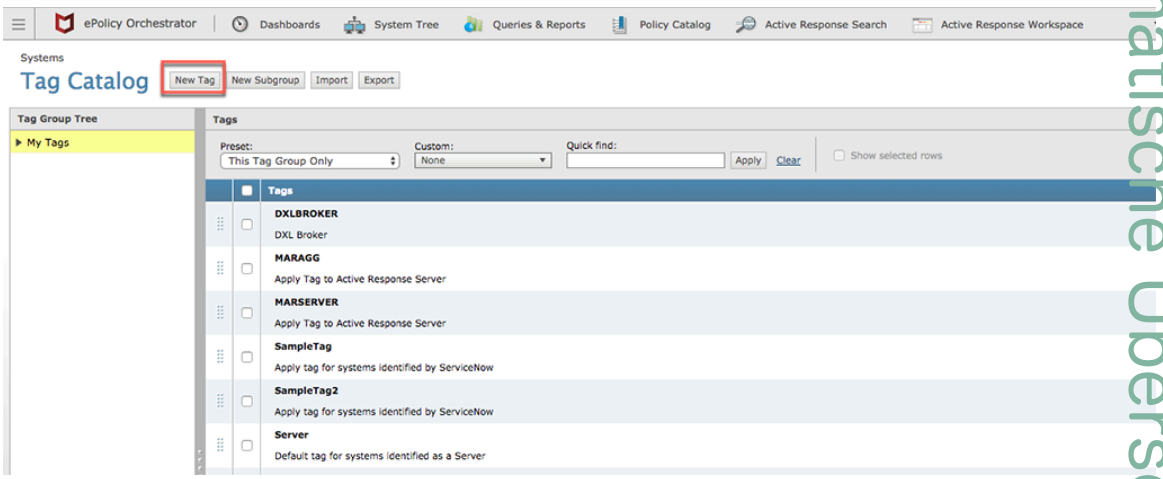
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren Sie zur Homepage von, und klicken Sie auf den Link **Tag-Katalog**.

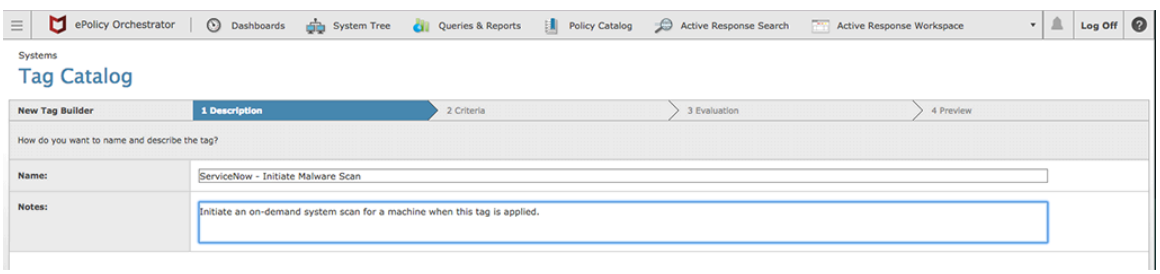


b. Klicken Sie auf der Seite „Tag-Katalog“, die angezeigt wird, auf **New Tag (Neues Tag)**.



c. Wählen Sie im angezeigten Fortschrittsbalken den Schritt Beschreibung aus, und geben Sie einen Namen und eine Beschreibung für das Tag ein.

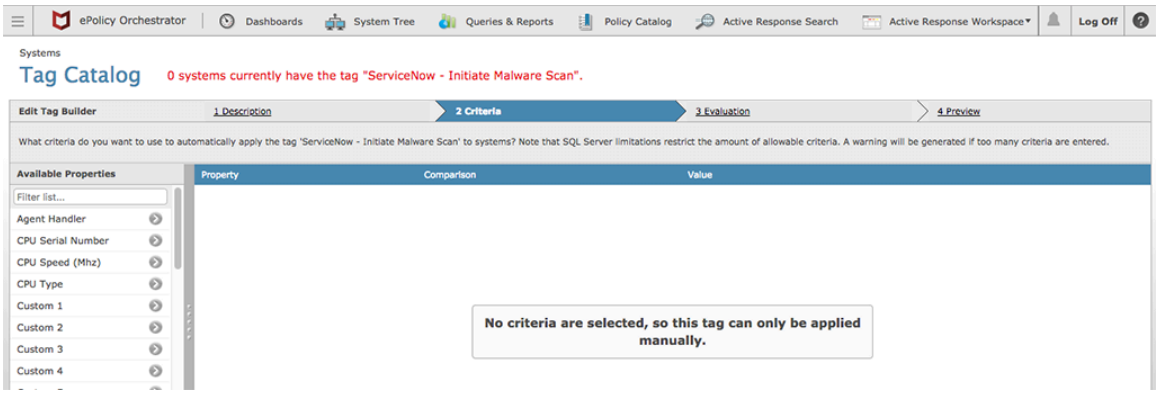
In diesem Beispiel wird ein Tag mit einem Namen und einer Beschreibung für die Funktion „Malware-Scan initiieren“ angezeigt. Dieser Tag-Name wird in Ihrer Instanz Now Platform abgeglichen und referenziert.



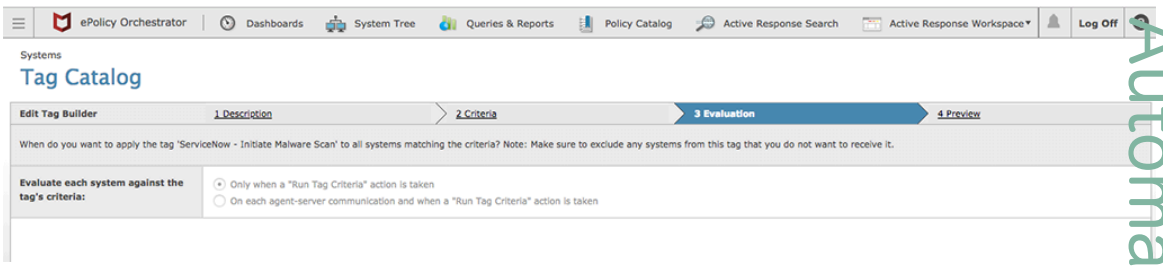
d. Um zum Schritt Kriterien zu gelangen, klicken Sie in der Fortschrittsleiste auf **Kriterien**.
Die angezeigten Nachrichten geben an, dass diesem Tag derzeit keine Aktionen zugewiesen sind und dass das Tag nur manuell angewendet werden kann.

Automatische Übersetzung

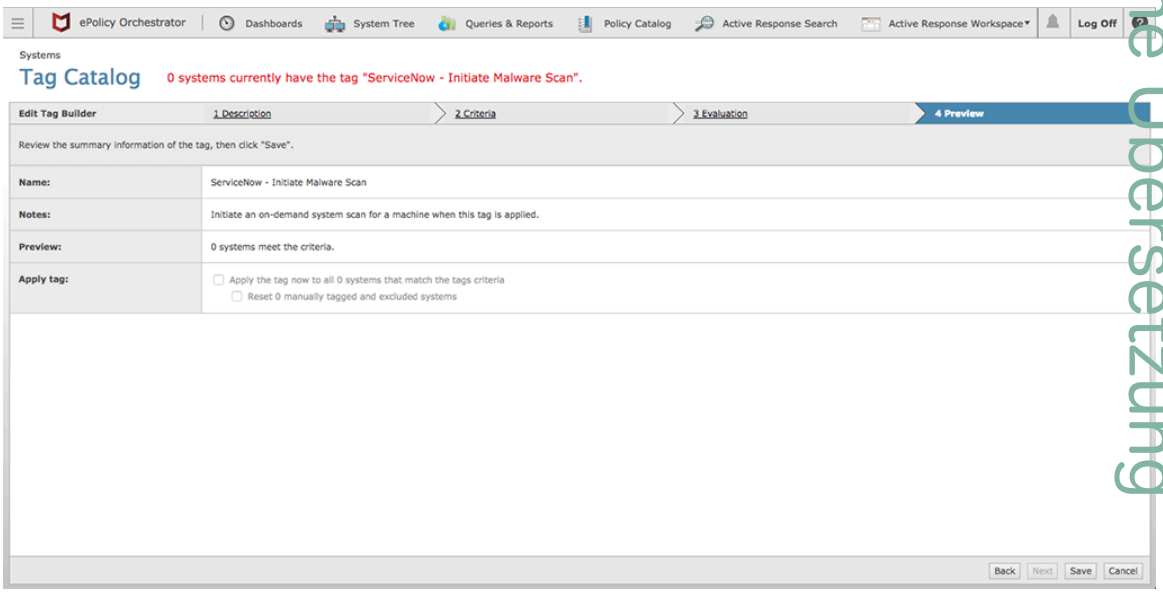
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Klicken Sie in der Fortschrittsleiste auf **Auswertung**, um fortzufahren.



f. Behalten Sie bei angezeigter Seite „Tag-Katalog“ des Auswertungsschritts für die Einstellungen auf dieser Seite ihre Standardwerte bei, und klicken Sie in der Fortschrittsleiste auf **Vorschau**.

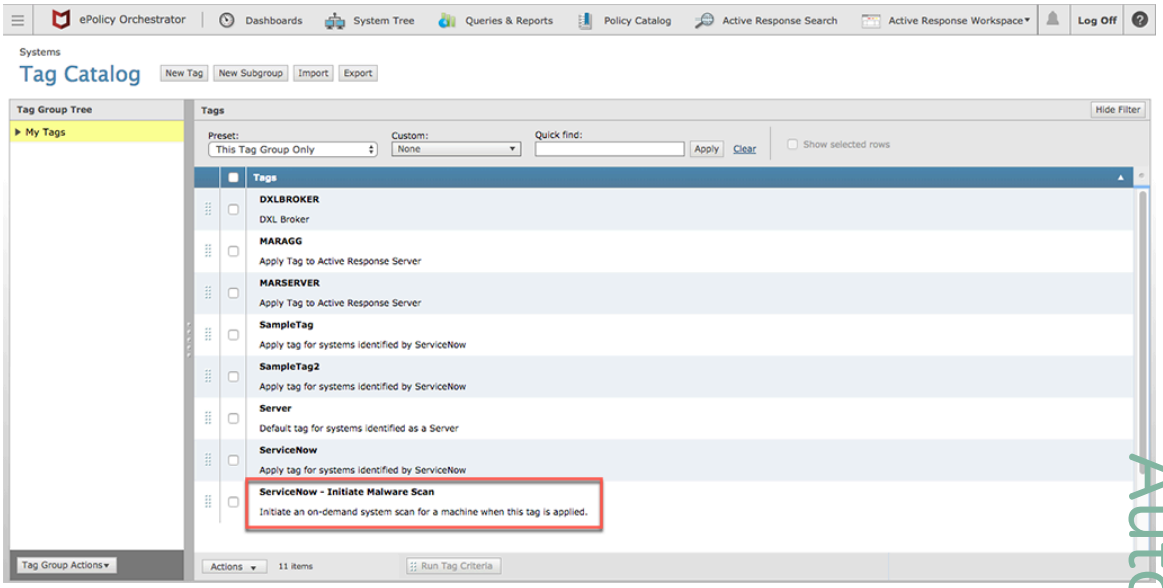


g. Klicken Sie bei angezeigter Vorschauseite unten rechts **auf Speichern**, um den Datensatz zu speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

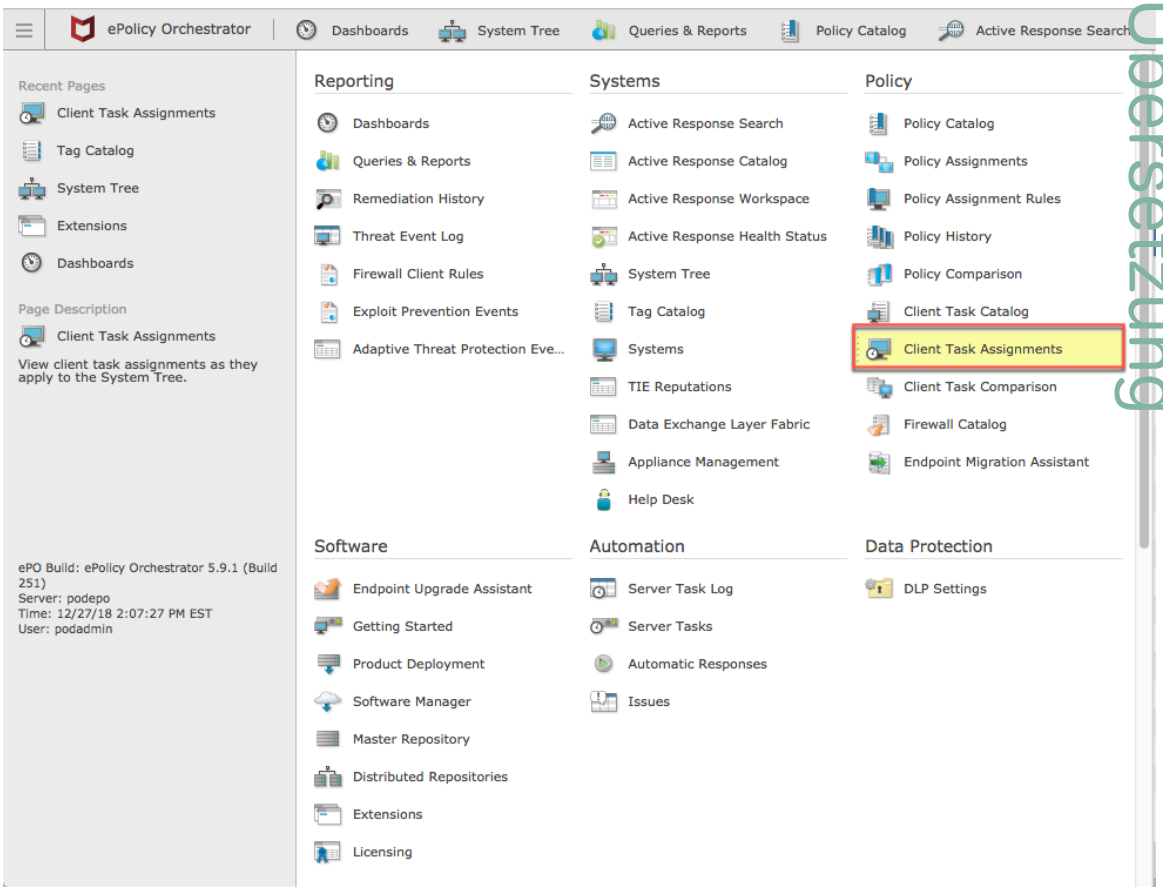
Das neue Tag wird im Tag-Katalog angezeigt (siehe folgende Abbildung).



7. Erstellen Sie ein Sicherheits-Tag für die Host-Isolierungsaktion, indem Sie die vorherigen Schritte wiederholen.
Nachdem Sie beide Tags erstellt haben, können Sie den neuen Tags Aktionen zuweisen.

8. Um Ihrem neuen Tag eine Aktion hinzuzufügen, gehen Sie wie folgt vor.

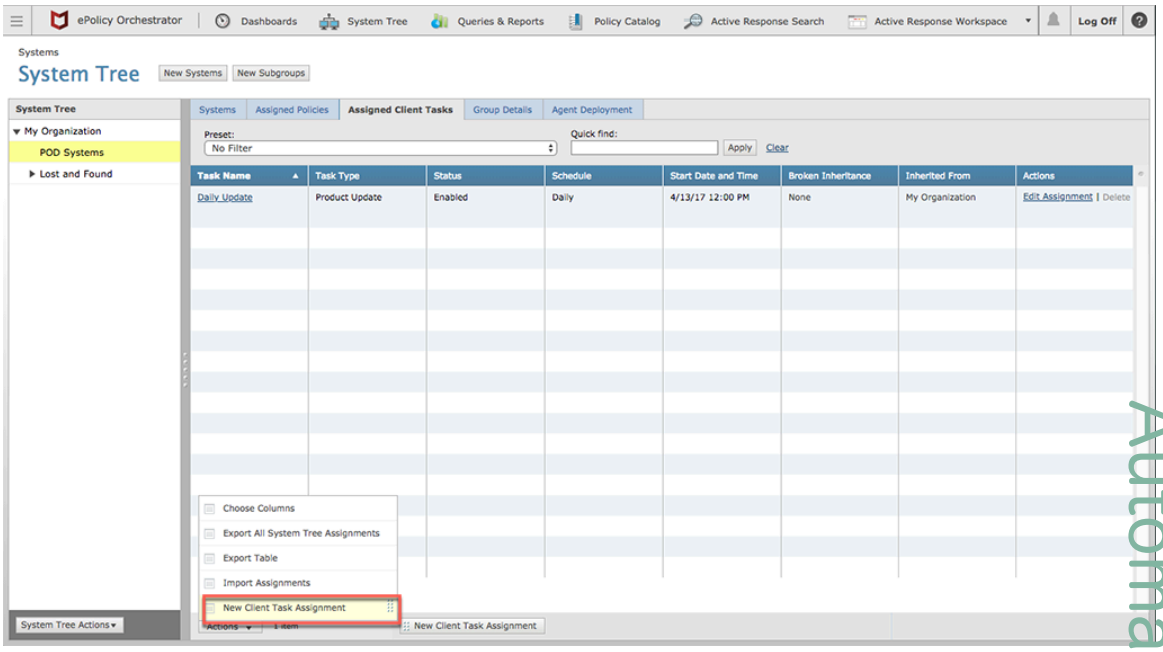
a. Navigieren Sie zur -Homepage, und klicken Sie im Abschnitt „Richtlinie“ auf den Link **Client-Aufgabenzuweisungen**.



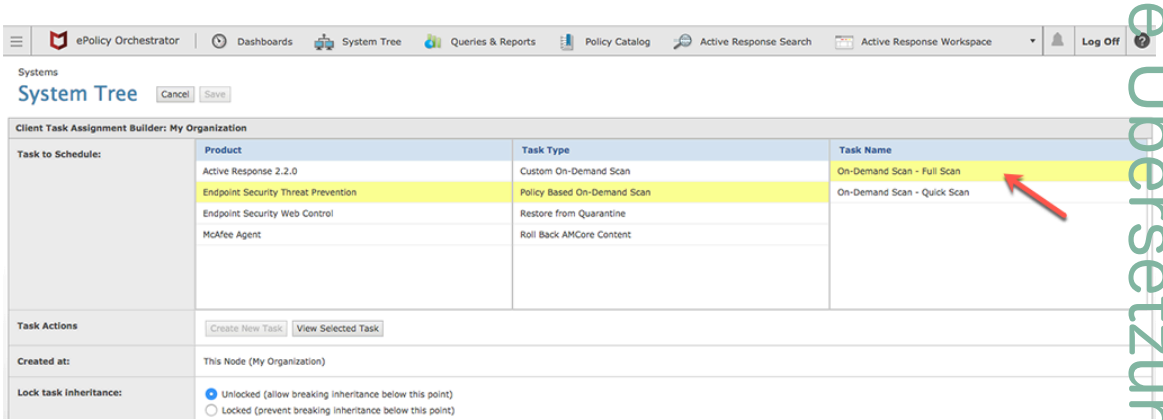
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Erweitern Sie auf der angezeigten Seite „Systemstruktur“ unten auf der Seite das Menü **Aktionen**, und wählen Sie **New Client Task Assignment (Neue Client-Aufgabenzuweisung)**aus.



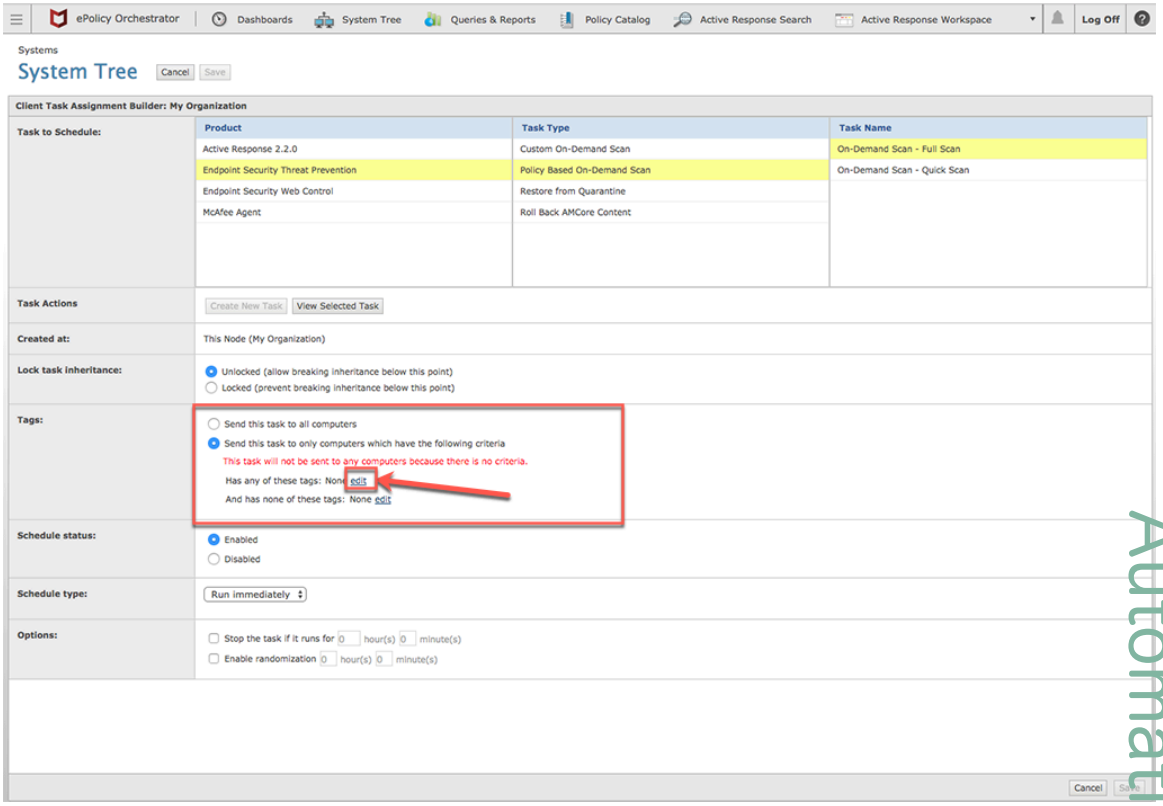
c. Navigieren Sie auf der angezeigten Seite zu **Endpoint Security Threat Prevention** > **Richtlinienbasierter Scan bei Bedarf** > **On-Demand-Scan - Vollständiger Scan** indem Sie den in der folgenden Abbildung gezeigten Pfad auswählen.



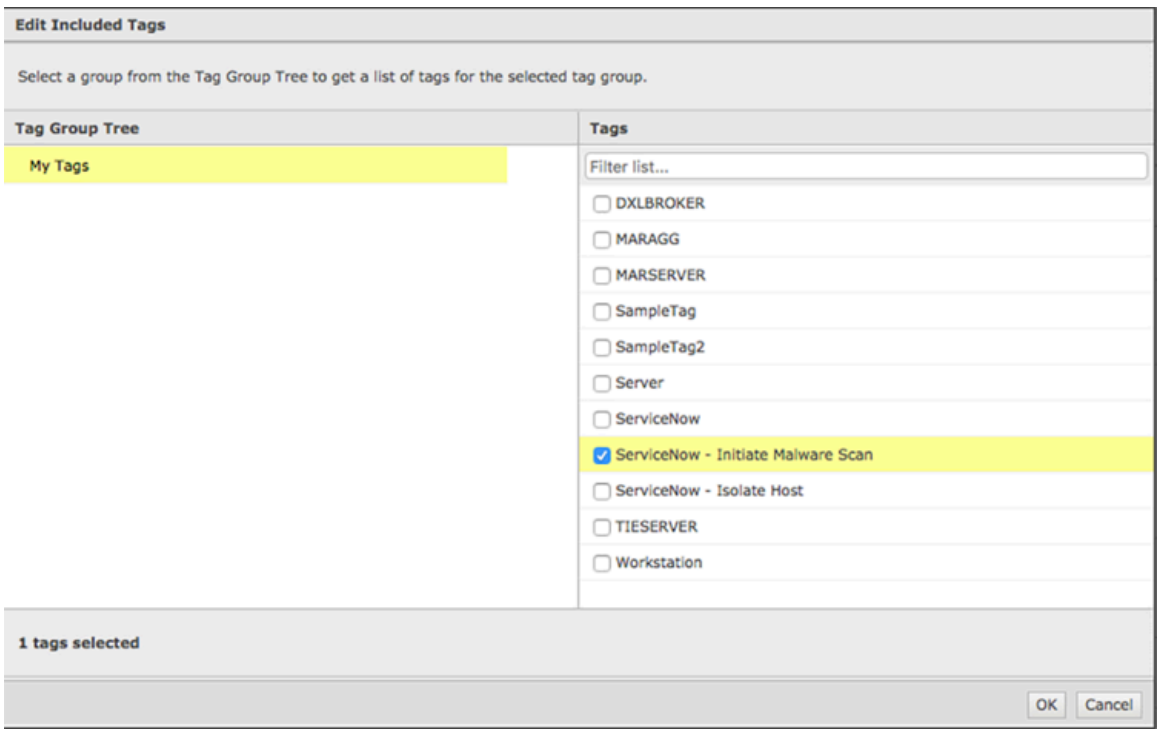
d. Klicken Sie im Abschnitt Tags unter dem Optionsfeld und neben Hat eines dieser Tags:auf den Link **Bearbeiten**, um die Kriterien für das Tag zu bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wählen Sie im angezeigten Dialogfeld das Tag Initiate Malware Scan ServiceNow (Malware-Scan initiieren), das Sie in den vorherigen Schritten erstellt haben, und klicken Sie auf **OK**.



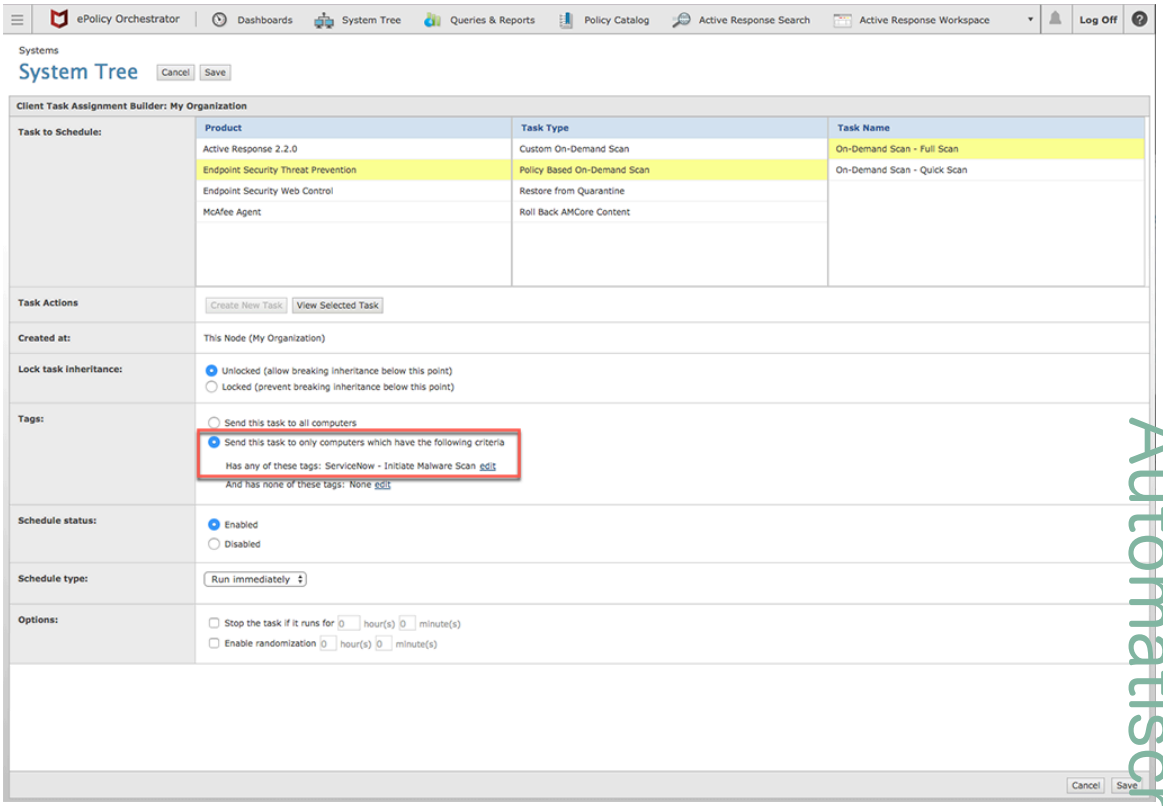
Das von Ihnen erstellte Tag „ServiceNow Malware-Scan initiieren“ ist der Aktion „Scan bei Bedarf“ zugewiesen.

f. Klicken Sie auf **OK**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

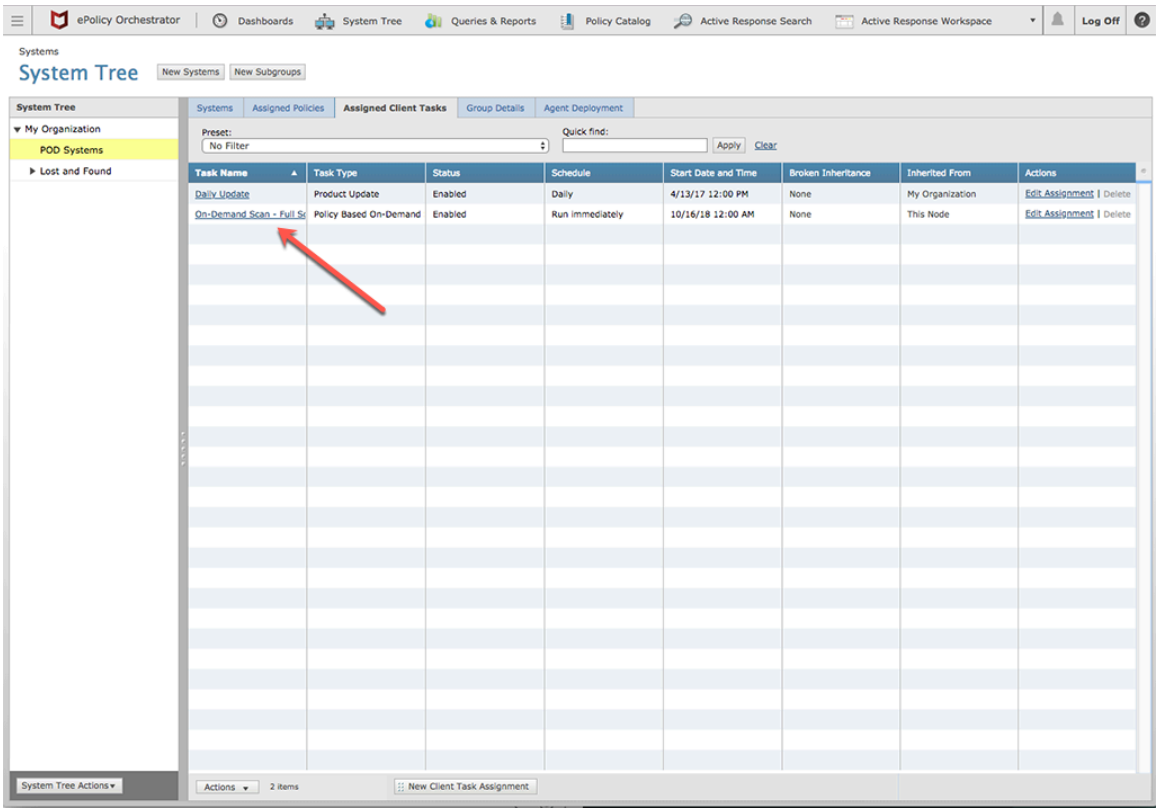
Im Abschnitt Tags wird unter dem Optionsfeld und neben Hat eines dieser Tags:das Tag Malware-Scan initiieren angezeigt.



g. Klicken Sie auf **Speichern**.
Auf der Seite „Systemstruktur“ wird die Aufgabe in der Liste Zugewiesene Client-Aufgaben (Registerkarte) angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



h. Wenn Sie der Aktion „Host isolieren“ keine Aktion zugewiesen haben, wiederholen Sie die vorherigen Schritte, um sie zuzuweisen.

Sie haben das Erweiterungs-Plugin erfolgreich installiert, Sicherheits-Tags erstellt und Ihren Tags Aufgaben zugewiesen. Sie haben das Setup für die Integration in Ihrer McAfee ePO -Konsole abgeschlossen. Der nächste Schritt besteht in der Konfiguration eines Servers in Ihrer Instanz Now Platform.

Installieren Sie die Anwendung, und konfigurieren Sie einen Server für die McAfee ePO -Integration

Bevor Sie die Workflows für die Integration aufrufen, installieren und konfigurieren Sie die Anwendung McAfee ePO aus dem ServiceNow Store in Ihrer Instanz Now Platform. Die Konfiguration ist erforderlich, um eine Verbindung zur Konsole McAfee ePO herzustellen.

Vorbereitungen

Erforderliche Rolle: Now Platform Administrator (admin)

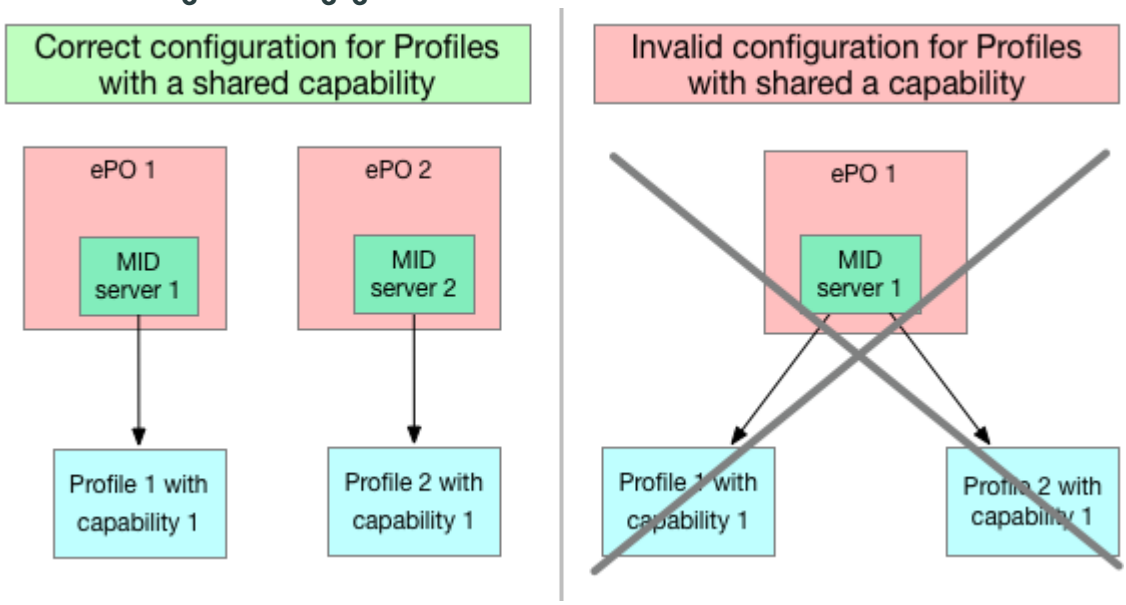
Warum und wann dieser Vorgang ausgeführt wird

Die Integration unterstützt mehrere Server. Um jedoch Konflikte in Profilen zu vermeiden, die dieselben Auslöserbedingungen verwenden, können Sie eine McAfee ePO -Fähigkeit nicht mit mehreren Profilen teilen, die denselben McAfee ePO -Server verwenden. Beispiel: Wie in der folgenden Abbildung dargestellt, können Sie die Fähigkeit 1 in mehr als einem Profil haben, solange jeder McAfee ePO -Server einem eindeutigen Profil mit der Fähigkeit 1 zugeordnet ist.

Automatische Übersetzung

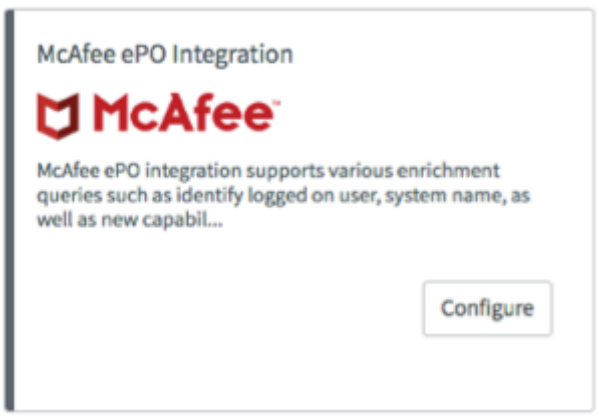
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränkungen für freigegebenes McAfee-Profil



Prozedur

1. Laden Sie McAfee ePO für Security Operations von ServiceNow Store herunter, und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Integrationskachel McAfee ePO für Security Operations, und klicken Sie auf **Konfigurieren**.



4. Füllen Sie die Felder des Formulars aus.

Konfiguration der McAfee ePO-Integration

Feld	Beschreibung
Name	Name der Integration, z. B. demo-1.
ePO-Servername	Name für den McAfee ePO -Server. Wenn Sie einen Server verwenden, ist McAfee Headquart (McAfee Headquarters) ein Beispiel. Anhand dieses Namens werden der Server und die zugehörigen Anmeldeinformationen erkannt.

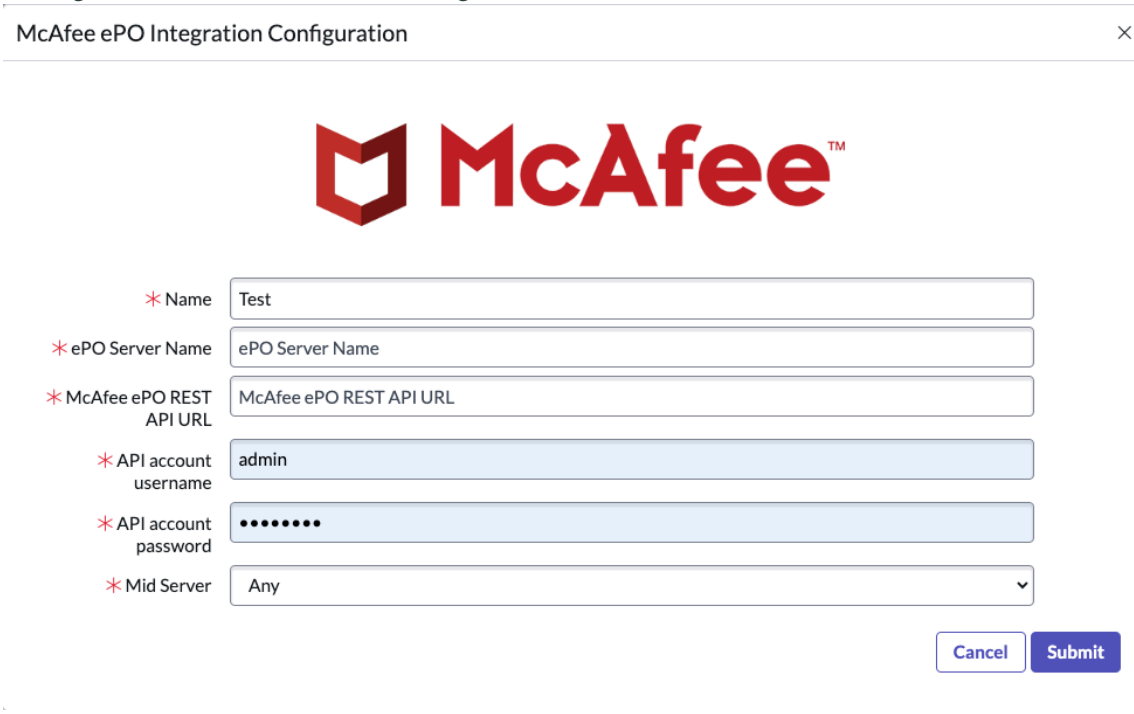
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Ihre Organisation Unterstützung für mehrere Server benötigt, geben Sie den Namen für jeden Server ein, und wiederholen Sie den Vorgang.
McAfee ePO-REST-API-URL	Basis-URL, die die McAfee ePO REST API hostet. Geben Sie die URL mit dem Protokoll https:// ein, z. B. https://corp.epo_server:8443.
API-Kontoanwendername	Eindeutiger Account-Anwendername, z. B. ServiceNow API.
API-Kontopasswort	Eindeutiges Passwort für das API-Konto.
MID-Server	Wählen Sie den Namen des MID-Servers aus, den Sie während des Setups Ihrer Instanz Now Platform konfiguriert haben. Sie können einen bestimmten MID-Server aus der Liste auswählen oder **Beliebig** auswählen, um die automatische Auswahl eines gültigen MID-Servers aus der Liste für diese Integration zu aktivieren. **Hinweis:** ○ Der während dieser Konfigurationszeit ausgewählte MID-Server gilt für die gesamte Integration. ○ In dieser Liste werden nur aktive und validierte MID-Server angezeigt. Standardmäßig ist der Wert auf **Beliebig**festgelegt. Ein Beispielname ist „ secops_local_midserver“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration der McAfee ePO-Integration



5. Klicken Sie auf **Absenden**.
   Die Liste der McAfee ePO-Konfigurationen wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für einen McAfee ePO -Server erfolgreich abgeschlossen.

Hinweis:
Wenn Ihre Organisation Unterstützung für mehrere Server benötigt, wiederholen Sie die Schritte.

Bearbeiten Sie Sicherheits-Tags in Now Platform für die McAfee ePO -Integration

Bearbeiten Sie im Rahmen des Setups für die Integration die Sicherheits-Tag-Namen, die Sie in der McAfee ePO -Konsole erstellt haben, in Ihrer Now Platform -Instanz. Bearbeiten Sie die Tag-Namen in Ihrer Instanz Now Platform so, dass sie mit den Namen der Tags in Ihrer Konsole McAfee ePO übereinstimmen.

Vorbereitungen
Erforderliche Rolle: Now Platform Security Incident Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird
Die Sicherheits-Tag-Namen in Ihrer Konsole McAfee ePO für die Aktionen „Malware-Scan initiieren“ und „Host isolieren“ müssen mit den Sicherheits-Tag-Namen in den Datensätzen für diese Funktionen Ihrer Instanz Now Platform übereinstimmen.

Bevor Sie ein Fähigkeitsprofil zum Ausführen Ihrer Fähigkeiten erstellen, zeigen Sie die Liste der verfügbaren McAfee ePO -Fähigkeiten an, und bearbeiten Sie die Sicherheits-Tags in Ihrer Now Platform -Instanz so, dass sie mit den Sicherheits-Tag-Namen in Ihrer McAfee ePO -Konsole übereinstimmen.

Weitere Informationen zum Erstellen der Sicherheits-Tag-Namen in der -Konsole McAfee ePO finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..

Automatische Übersetzung

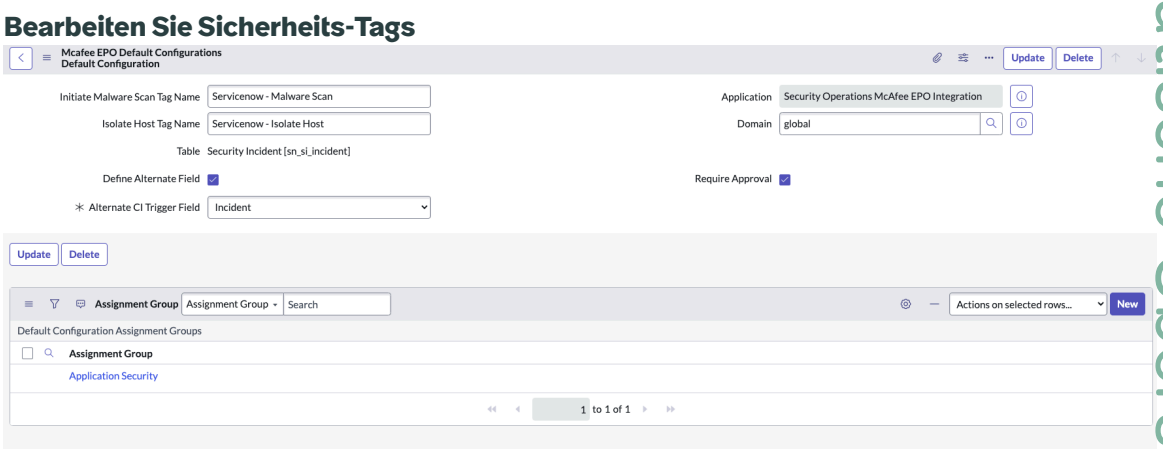
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **McAfee ePO-Integration** > **Standardeinstellungen**.
2. Um den Sicherheits-Tag-Namen der Integration McAfee ePO zu bearbeiten, klicken Sie auf **Standardkonfiguration**.

   Hinweis:
   Stellen Sie sicher, dass Sie diese Konfiguration nach der Installation der McAfee ePO -Integration durchführen.

3. Geben Sie im Feld Name des Malware-Scan-Tags initiieren den Namen des Sicherheits-Tags ein, den Sie in der Konsole McAfee ePO für die Aktion Scan-Initiierung erstellt haben.
   Beispiel: ServiceNow – Malware-Scan
4. Geben Sie im Feld „Host-Tag-Name isolieren“ den Namen des Sicherheits-Tags ein, den Sie in der Konsole McAfee ePO für die Aktion „Host isolieren“ erstellt haben.
   Beispiel: ServiceNow – Host isolieren
5. Wenn Sie das CI-Auslöserfeld bei der Incident-Erstellung nicht verwenden möchten, aktivieren Sie das Kontrollkästchen **Alternatives Feld definieren**.
   Wenn diese Option aktiviert ist, wird die Feldauswahlliste Alternative CI-Auslöser angezeigt.



6. Wählen Sie in der Auswahlliste ein alternatives Feld aus, um nach Ihren CI-Suchkriterien zu suchen.
   In diesem Beispiel gehen Sie als Benutzer mit der Rolle sn_si.admin davon aus, dass das CI-Feld bei der Incident-Erstellung im Security Incident nicht ausgefüllt wird. Alternativ gehen Sie davon aus, dass CI-Informationen für einen FQDN, einen Hostnamen oder eine IP-Adresse im Feld Identifiziertes CI des Security Incident ausgefüllt werden, und wählen Sie alternativ das Feld Identifiziertes CI aus. Für dieses Beispiel ist das identifizierte CI ausgewählt. Sie können jedoch jedes Feld im Security Incident für das alternative CI verwenden.
7. Wählen Sie im Feld Domäne mithilfe der Suchoption eine Domäne oder Gruppe für diese Konfiguration aus.
   Beispiel: global.
8. Aktivieren Sie im Feld Genehmigung erforderlich das Kontrollkästchen **Genehmigung erforderlich**, wenn Sie die Funktionen Host isolieren und Isolierung entfernen verwenden.

   Hinweis:
   Die Funktionen Malware-Scan initiieren, Bedrohungsereignisse auflisten und Systemdetails abrufen müssen nicht genehmigt werden.

9. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der ePO-Tag-Name wird aktualisiert und in der Liste der McAfee ePO-Standardkonfigurationen angezeigt. Der Sicherheits-Tag-Name für die Malware-Scan-Aktion in Ihrer Instanz Now Platform stimmt mit dem Namen für den Scan in Ihrer Konsole McAfee ePO überein.

Sie haben die ePO-Tag-Namen für den Malware-Scan und die Fähigkeiten zum Isolieren von Hosts in Ihrer Instanz Now Platform erfolgreich bearbeitet. Im nächsten Schritt erstellen Sie ein Profil für Ihre Fähigkeiten.

Zugehörige Informationen

McAfee-Produktdokumentation

Erstellen Sie eine Genehmigungsgruppe

Erstellen Sie eine Genehmigungsgruppe für die McAfee ePO für die Security Operations -Integration, die Anforderungen zum Isolieren von Hostcomputern und deren Wiederherstellung im Netzwerk genehmigen kann.

Vorbereitungen

Sie können die Genehmigungsberechtigung nicht erneut einer Gruppe zuweisen, es sei denn, in Ihrer Instanz ist eine Genehmigungsgruppe verfügbar.

Hinweis:
Die Genehmigungsoption in Profile für die Integration McAfee ePO werden konfiguriert wird nur für die Funktionen Host isolieren und Hostisolierung entfernen angezeigt.

Erforderliche Rolle: Now Platform® Security Incident Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird

Vom Security Incident-Analysten übermittelte Genehmigungsanforderungen zum Isolieren von Hostcomputern und Entfernen der Isolierung werden standardmäßig dem Benutzer mit der Rolle sn_si.admin zugewiesen. Als Anwender mit dieser Rolle können Sie diese Genehmigungsberechtigung während des Konfigurationsschritts für ein Profil neu zuweisen. Bevor Sie einer Genehmigungsgruppe eine Berechtigung zuweisen können, muss in der Gruppenliste in Ihrer Instanz Now Platform eine Genehmigungsgruppe verfügbar sein.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**.
2. Klicken Sie in der Gruppenliste auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungsgruppe“

Feld	Beschreibung
Name	Name der Gruppe, die angezeigt wird, wenn eine Genehmigungsanforderung übermittelt wird, z. B. Genehmiger McAfee-Hostisolierung.
Gruppen-E-Mail	Gruppen-E-Mail-Verteilerliste oder die E-Mail-Adresse des Kontaktpunkts, z. B. Gruppenmanager, McAfeeapproval@servicenow.com
Manager	Name des Gruppenmanagers Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übergeordnet	(Optional) Andere Gruppe, in der diese Gruppe Mitglied ist, wenn diese Gruppe ein übergeordnetes Element hat.
Beschreibung	Zusätzliche Informationen zu dieser Gruppe.
Mitglieder einbeziehen	Option zum Einbeziehen von Mitgliedern in diese Gruppe.
Standard-Beauftragter	Option zum Auswählen eines Anwenders als Standardbeauftragter für diese Gruppe. Verwenden Sie die Suchoption, um die Liste der Benutzer zu öffnen.
Rollen	Option zum Auswählen der Rollen für diese Gruppe. Verwenden Sie die Option Hinzufügen und Entfernen, um Rollen hinzuzufügen und zu entfernen.
Typ	Option zum Auswählen einer Kategorie für diese Gruppe. Verwenden Sie die Suchoption, um die Liste der Gruppentypen zu öffnen.
Lieferanten	Option zum Auswählen eines Lieferanten für diese Gruppe. Verwenden Sie die Option Suchen, um die Liste der Lieferanten zu öffnen.

4. Klicken Sie auf **Absenden**.
   Die neue Gruppe wird in der Gruppenliste angezeigt.

   Diese Gruppe ist für die Verarbeitung von Anforderungen verfügbar, wenn Sie während der Konfiguration dieses Profils die Option **„Genehmigung erforderlich“** aktivieren.

   Um von Benutzern mit der Rolle sn_si.analyst übermittelte Anforderungen zu überwachen und zu verarbeiten, navigieren alle Mitglieder der Genehmigungsgruppe zur Registerkarte **Meine Genehmigungen** in Now Platform.

McAfee ePO Integrationsfähigkeitsprofile

Als Benutzer mit der Rolle „Security Incident-Administrator“ (sn_si.admin) erstellen Sie Profile für die Fähigkeiten McAfee ePO in Ihrer Instanz Now Platform®. Sie gruppieren Abfragen oder Aktionen in Profilen und bestimmen, welche McAfee ePO -Fähigkeiten ausgeführt werden sollen, wenn ein neuer Security Incident erstellt wird.

Fähigkeitsprofile

Sie erstellen Profile™, um McAfee ePO -Fähigkeiten zu gruppieren und die Einstellungen für diese Fähigkeiten von Ihrer Instanz Now Platform® aus zu konfigurieren. Sie können mehrere Profile für diese Fähigkeiten erstellen, um zu bestimmen, welche Aktionen oder Abfragen aufgerufen werden, wenn ein Incident vom Security Incident Response Typ (SIR) erstellt wird. Um den Anforderungen Ihrer Organisation gerecht zu werden, können Sie ein einzelnes Profil erstellen, das z. B. Abfragen von Systemdetails ausführt, Malware-Scans initiiert und Hostcomputer isoliert, oder Sie können mehrere Profile mit jeweils einer eigenen McAfee ePO -Fähigkeit erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Profiltypen und erforderliche McAfee ePO -Fähigkeiten

Primärer Zweck Ihres Profils	Richten Sie Anforderungen ein	Für diesen Profiltyp erforderliche McAfee ePO-Fähigkeiten
Erfassen Sie Systemdetails	Keine	**Hostdetails abrufen**
Isolieren Sie einen Host	Vergewissern Sie sich mit Ihrem McAfee ePO -Administrator, dass Sie die Sicherheits-Tags für die Aktion „Host isolieren“ in Ihrer McAfee ePO -Konsole erstellt haben. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..	**Host isolieren**
Scannen Sie Ihren Host, und suchen Sie nach Bedrohungen	Vergewissern Sie sich mit Ihrem McAfee ePO -Administrator, dass Sie in Ihrer McAfee ePO -Konsole die Sicherheits-Tags für die Aktion „Malware-Scan-Aktion initiieren“ erstellt haben. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..	**Initiieren Sie den Malware-Scan** **Hinweis:** Im Rahmen der Malware-Prüfung McAfee ePO wird automatisch die Funktion „Bedrohungsereignisse auflisten“ aktiviert. Sie müssen die Funktion „Bedrohungsereignisse auflisten“ jedoch nicht dem Profil mit der Malware-Scan-Funktionalität hinzufügen. Die Ergebnisse des Malware-Scans werden auf der Registerkarte Details des Bedrohungsereignisses im Security Incident angezeigt.
Entfernt die Isolierung für einen Host	Vergewissern Sie sich mit Ihrem McAfee ePO -Administrator, dass Sie die Sicherheits-Tags für die Aktion „Host isolieren“ in Ihrer McAfee ePO -Konsole erstellt haben. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..	**Isolation entfernen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Profiltypen und erforderliche McAfee ePO -Fähigkeiten (Fortsetzung)

Primärer Zweck Ihres Profils	Richten Sie Anforderungen ein	Für diesen Profiltyp erforderliche McAfee ePO-Fähigkeiten
Sammeln Sie Daten zur Bedrohungsanreicherung.	Keine	**Bedrohungsereignisse auflisten**

Erstellen Sie ein Fähigkeitsprofil für die Integration McAfee ePO .

Erstellen Sie ein Profil, und wählen Sie die McAfee ePO -Fähigkeiten aus, die das Profil ausführen soll.

Vorbereitungen

Erforderliche Rolle: Now Platform® Security Incident Administrator (sn_si.admin)

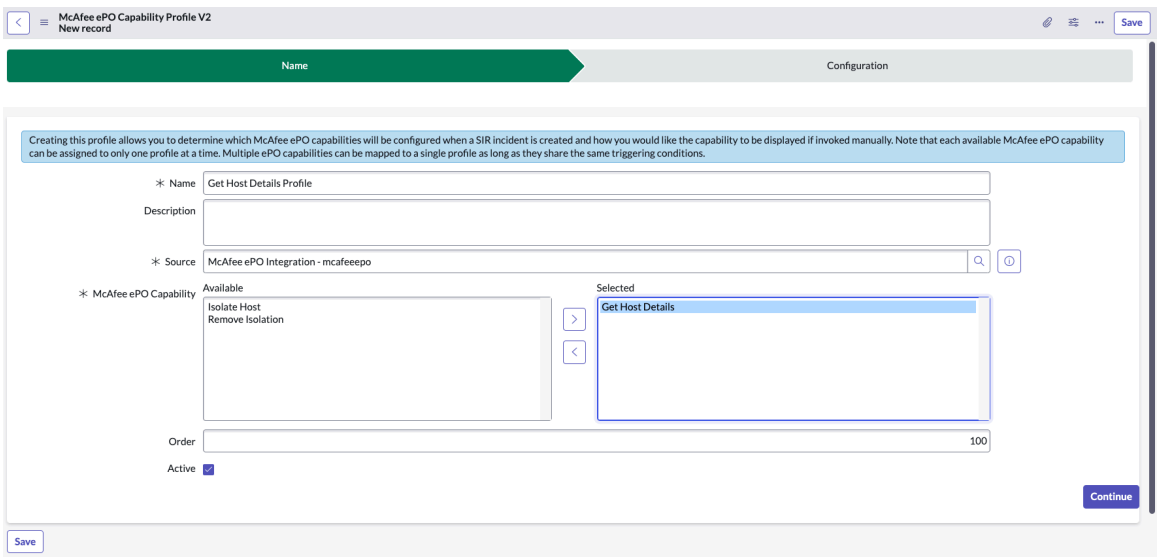
Warum und wann dieser Vorgang ausgeführt wird

Für diesen Konfigurationsschritt erstellen Sie ein Profil für die McAfee ePO -Fähigkeiten. Berücksichtigen Sie beim Erstellen von Profilen die Absicht des Profils, bevor Sie ihm McAfee ePO -Fähigkeiten hinzufügen. Beziehen Sie sich beim Erstellen von Profilen auf die folgende Tabelle.

In der folgenden Tabelle sind die Fähigkeiten aufgeführt, die Sie einem Profil hinzufügen müssen, wenn das Profil bestimmte Abfragen oder Aktionen ausführen soll. Erstellen Sie ein einzelnes Profil, das Abfragen von Hostdetails ausführt, Malware-Scans initiiert, Isolation entfernt und Hostcomputer isoliert, oder erstellen Sie mehrere Profile mit jeweils einer eigenen Fähigkeit.

Prozedur

1. Navigieren zu **McAfee ePO-Integration** > **McAfee ePO-Fähigkeitsprofile**.
   Die Liste der Fähigkeitsprofile McAfee ePO wird angezeigt.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Fortsetzen**, um das Profil zu speichern und zu validieren.
   Wenn die Validierung erfolgreich ist, wird die Seite neu geladen, und das Formular **Konfiguration** wird angezeigt.

Nächste Maßnahme

Im nächsten Schritt konfigurieren Sie Ihr Profil. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie sich die Konzepte zum Konfigurieren von Profilen und Auslösebedingungen ansehen. Siehe Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein. und Definieren von Auslösebedingungen mit einem Feld Configuration Item (CI) für ein McAfee ePO -Profil, um weitere Informationen zu erhalten.

Definieren von Auslösebedingungen mit einem Feld Configuration Item (CI) für ein McAfee ePO -Profil

Nachdem Sie ein Profil erstellt und die McAfee ePO -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Einstellungen des Profils so, dass es nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt ist.

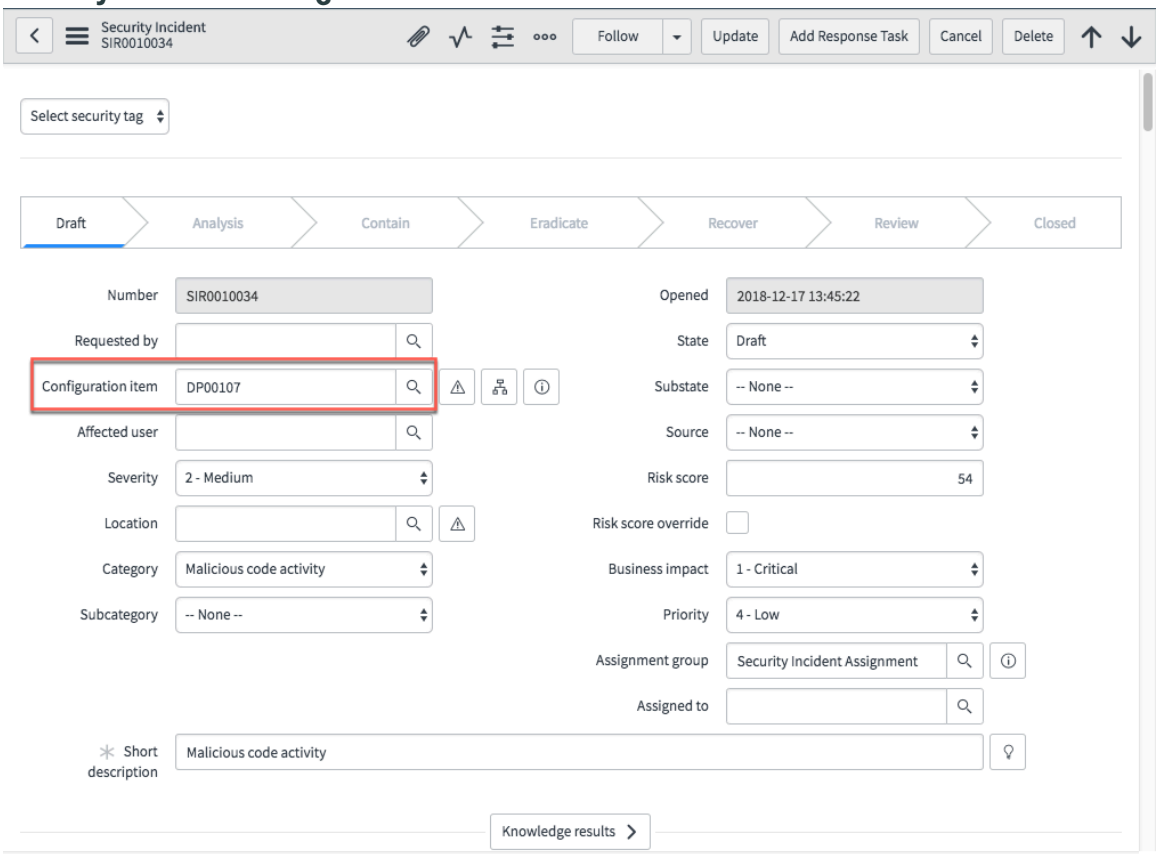
Sie können diese Auslösebedingungen flexibel festlegen, sodass das Profil automatisch basierend auf den Standardfeldwerten ausgeführt wird, die mit einem Security Incident Now Platform® Security Incident Response übereinstimmen. Alternativ können Sie ein Profil einrichten, damit nach Übereinstimmungen in Feldwerten gesucht wird, die Sie speziell im Security Incident identifizieren.

Einer der Schlüssel zur Funktionalität der Integration und zur Funktionsweise eines Profils ist das Feld Configuration Item (CI) im Security Incident Now Platform® Security Incident Response (SIR). Der Wert dieses Felds ist der Prinzipalwert für einen Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in der -Datenbank Now Platform® gespeicherten Informationen abzugleichen. Wenn ein Security Incident SIR von einem Sicherheitsereignis erstellt wird und ein Profil aktiviert ist, werden Ihre Assets nach einem übereinstimmenden Wert für einen vollqualifizierten Domänennamen (FQDN), einen Hostnamen oder eine IP-Adresse basierend auf dem Wert durchsucht Feld Konfigurationselement.

Im Idealfall wird ein übereinstimmender Wert in der Datenbank gefunden, und in der Konsole McAfee ePO können Daten für das passende Asset gesammelt, in Ihre Instanz Now Platform® abgerufen und in den zugehörigen Listen eines Security Incident angezeigt werden. Die folgende Abbildung zeigt ein Beispiel für das Feld Konfigurationselement, das mit einem Hostnamen für einen Security Incident SIR gefüllt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident – Konfigurationselement



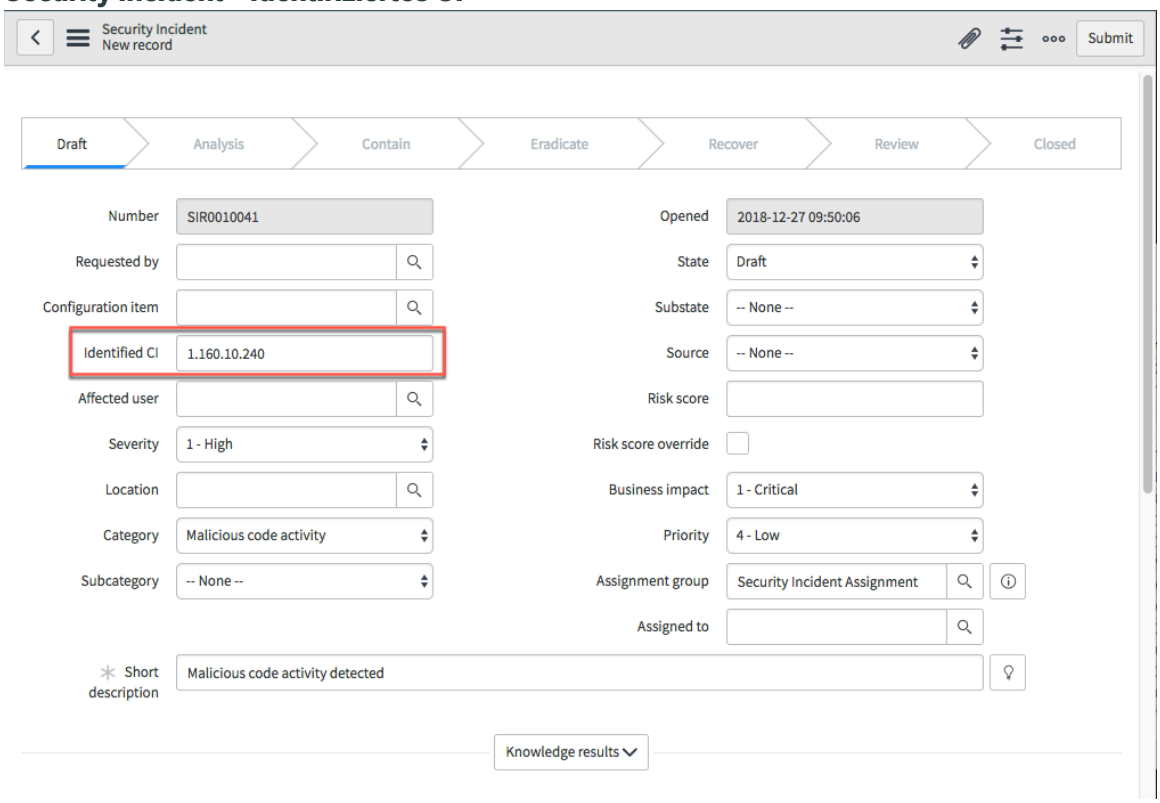
In Fällen, in denen das Feld Configuration Item (CI) im Security Incident nicht ausgefüllt ist oder keine Übereinstimmung für einen FQDN, keinen Hostnamen oder keine IP-Adresse gefunden werden kann, die der Datenbank entspricht, können Sie ein alternatives Feld in der Sicherheit auswählen Incident, um alle übereinstimmenden CI-Ergänzungsdaten anzuzeigen, die bei der Prüfung Ihrer Assets gefunden wurden.

Während des Konfigurationsschritts des Profil-Setups können Sie ein alternatives CI-Auslöserfeld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass die CI-Anreicherungsdaten aus der Suche McAfee ePO für den zugeordneten Security Incident ausgefüllt werden. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Durch Auswahl dieses alternativen CI-Felds als Sicherung stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung im zugehörigen Security Incident nicht ausgefüllt wird.

Beispiel: Als SOC-Analyst (Security Operations Center) erstellen Sie ein anwenderdefiniertes Feld für einen Security Incident mit der Bezeichnung IP-Adresse für meinen Security Incident. Wenn Sie nicht möchten, dass der Wert dieses anwenderdefinierten Felds bei der Incident-Erstellung im Feld „Konfigurationselement“ des Security Incident angezeigt wird, können Sie das Profil so einrichten, dass nach dieser IP-Adresse gesucht wird. Bei Übereinstimmung wird die IP-Adresse für den Security Incident im Feld Ihrer Wahl angezeigt. In der folgenden Abbildung ist für dieses Beispiel das Feld Identifiziertes CI als alternatives Feld für die IP-Adresse ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

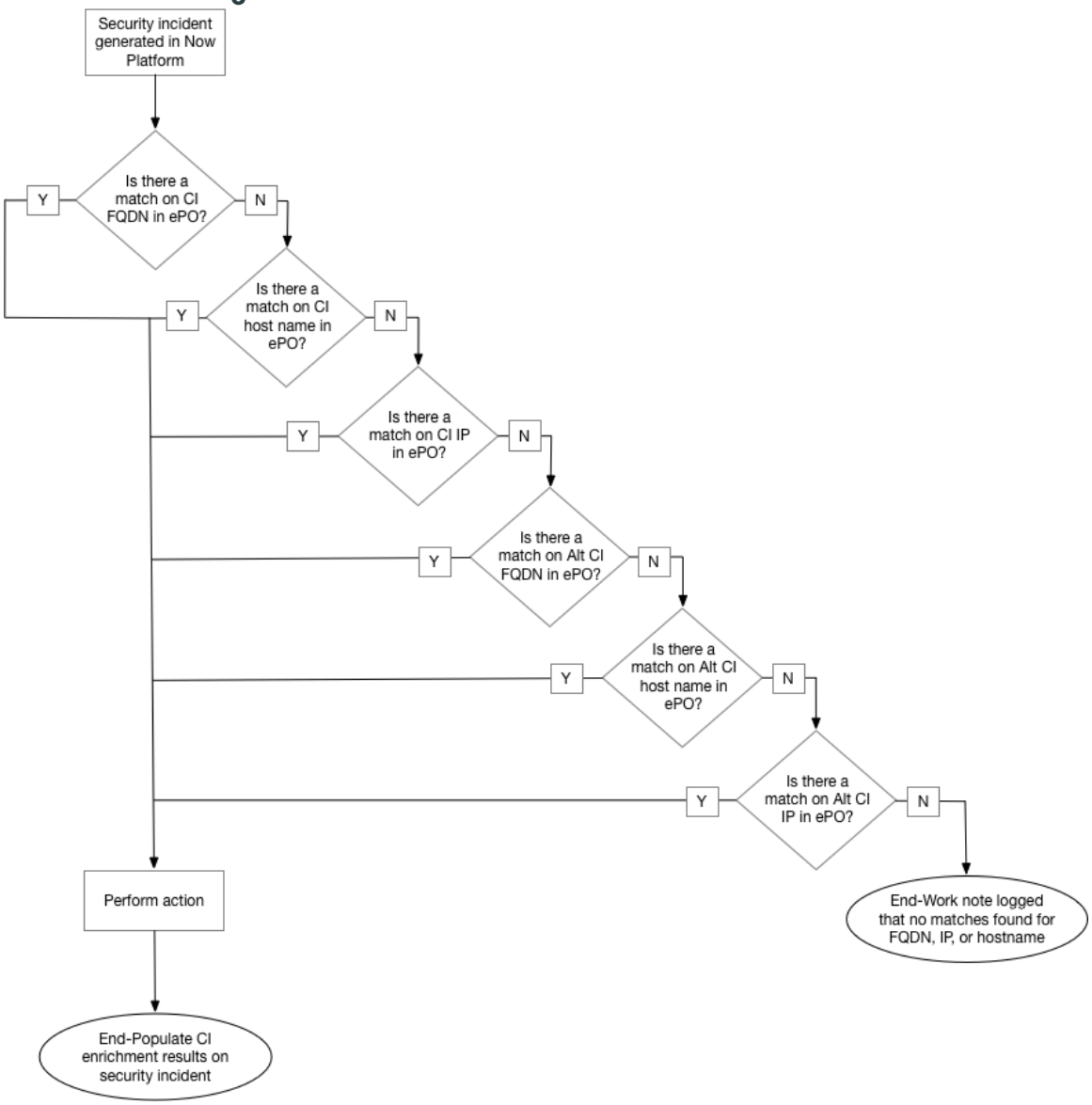
Security Incident – Identifiziertes CI



Die folgende Abbildung zeigt, wie die erste Suche des Workflows nach Übereinstimmungen für Configuration Items sucht. Wenn das Feld Alternativer CI-Auslöser aktiviert ist, sucht die zweite Suche nach Übereinstimmungen für alternative Werte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow für Konfigurationselemente



Wenn für das CI-Feld oder das alternative CI-Feld keine übereinstimmenden IDs gefunden werden, wird eine Arbeitsnotiz protokolliert und eine Nachricht zum Security Incident angezeigt. Wenn keine Übereinstimmungen gefunden werden, werden für die Security Incidents, die sich auf das Ereignis beziehen, keine Ergänzungsdaten eingetragen.

Sie aktivieren das alternative CI-Auslöserfeld und wählen das Feld aus, in dem Sie die entsprechende ID während des Konfigurationsschritts für ein Profil anzeigen möchten. Dieser Schritt zum Aktivieren des alternativen CI-Felds ist zusammen mit den anderen Profilkonfigurationsanforderungen in Profile für die Integration McAfee ePO werden konfiguriertbeschrieben.

Profile für die Integration McAfee ePO werden konfiguriert

Nachdem Sie ein Profil erstellt und die McAfee ePO -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Einstellungen so, dass das Profil nur unter den von Ihnen definierten Bedingungen aufgerufen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Profil wird konfiguriert

In diesem Schritt konfigurieren Sie ein Fähigkeitsprofil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Sie definieren, welche Bedingungen in Security Incidents automatisch die Fähigkeiten McAfee ePO auslösen, die Sie für das Profil ausgewählt haben. Sie haben auch die Möglichkeit, ein alternatives Eingabefeld für das Feld Configuration Item (CI) auszuwählen und Filterbedingungen so festzulegen, dass das Profil nur von den Security Incidents automatisch gestartet wird, die mit dem auslösenden Ereignis in Zusammenhang stehen. Der Konfigurationsschritt enthält die folgenden Einstellungen im Konfigurationsformular für das Profil.

Alternatives Auslöserfeld für Configuration Item (CI).

In Fällen, in denen das Feld Configuration Item (CI) im Security Incident Now Platform® Security Incident Response (SIR) nicht mit einem Wert ausgefüllt ist oder keine Übereinstimmung in der Datenbank gefunden werden kann, können Sie ein alternatives Feld im Security Incident auswählen, um ein beliebiges anzuzeigen übereinstimmende CI-Ergänzungsdaten, die bei der Prüfung Ihrer Assets gefunden wurden. Weitere Informationen zu den Feldern Konfigurationselement und Alternatives Konfigurationselement in einem Security Incident finden Sie unter Definieren von Auslösebedingungen mit einem Feld Configuration Item (CI) für ein McAfee ePO -Profil.

Sicherheits-Tags

Damit Sie den Status isolierter Hostcomputer nachverfolgen können und wenn Malware-Scans initiiert werden, ist eine optionale Tagging-Funktion verfügbar. Standardmäßig ist diese Option im Konfigurationsformular für Profile deaktiviert. Wenn diese Option während des Konfigurationsschritts aktiviert wird, werden Sicherheits-Tag-Namen im Konfigurationsformular angezeigt. Dies sind die Namen der Tags, die für zugehörige Security Incidents angezeigt werden. Diese Tags informieren Sie, wenn eine Hostisolierungsaktion erfolgreich initiiert und genehmigt wurde. Nachdem ein Host erfolgreich an das Netzwerk zurückgegeben wurde, wird das Sicherheits-Tag automatisch aus dem Security Incident entfernt. Bei Malware-Scans wird ein Tag für den zugehörigen Security Incident angezeigt, wenn ein Scan geplant wird. Nach Abschluss des Scanvorgangs wird das geplante Tag automatisch durch ein Tag ersetzt, das angibt, dass der Scanvorgang erfolgreich abgeschlossen wurde.

Automatischer Auslöser basierend auf Incident

Wenn die Option Auf Incident automatisch auslösen aktiviert ist, ist der Generator für Filterbedingungen verfügbar, und Sie müssen Filterbedingungen festlegen, die angeben, wann das Profil automatisch ausgeführt wird. Ein gängiger Filter ist „Kategorie ist schädliche Codeaktivität“™ und „Geschäftsauswirkung“ ist „1 – Kritisch“™. Mit diesen Filtern wird das Profil nur bei Security Incidents gestartet, die mit schädlichem Code zusammenhängen und kritische Geschäftsauswirkungen haben. Mit der Option Automatisch auslösen können Sie die Anzahl der Security Incidents reduzieren, die das Profil automatisch aufrufen.

Genehmigungen

Wenn Ihre Organisation eine zusätzliche Kontrolle über Aktionen wie das Isolieren von Hostcomputern und das Initiieren von Malware-Scans haben möchte, können Sie die Option Genehmigung erforderlich während des Konfigurationsschritts für ein Profil aktivieren.

Wenn beispielsweise sowohl die Genehmigungs- als auch die Tagging-Funktion für ein Profil aktiviert sind und eine Anforderung zur Isolierung oder Rückgabe eines Hostcomputers an das Netzwerk zur Genehmigung übermittelt wurde, wird der zugehörige Security Incident

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

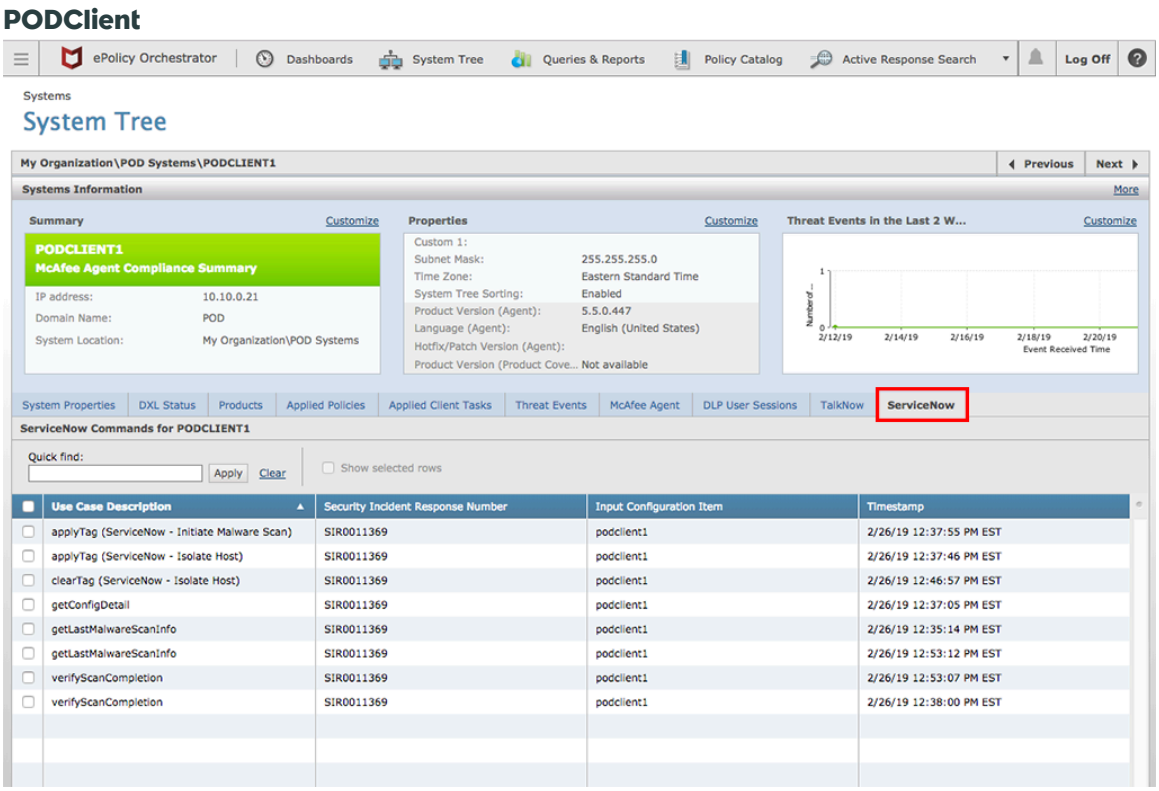
automatisch mit einem Tag versehen und die Aktion initiiert. Anforderungen werden standardmäßig zur Genehmigung an einen Benutzer mit der Rolle sn_si.admin gesendet. Diese Genehmigung kann jedoch entsprechend den Anforderungen Ihres Unternehmens einer anderen Person oder Genehmigungsgruppe zugewiesen werden. Genehmiger verarbeiten Anforderungen in **„Meine Genehmigungen"** in ihren Now Platform® -Instanzen. Sicherheits-Tags werden für zugehörige Security Incidents angezeigt. Alle Workflow-Aktivitäten werden auch in Arbeitsnotizen protokolliert, um einen Audit-Pfad zu erstellen.

ServiceNow Audit-Protokoll in der McAfee ePO -Konsole

In Version 5.10.0 von McAfee ePOwird die Registerkarte ServiceNow mit einem Protokoll der Befehle angezeigt, die von der Instanz Now Platform® aus initiiert werden. Nachdem eine Aktion oder eine Abfrage aus einem Profil in Ihrer Instanz Now Platform® auf einem Hostcomputer (Endpunkt) in der Konsole McAfee ePO aufgerufen wurde, wird in der Konsole McAfee ePO ein Audit-Protokoll mit Befehlen [ServiceNow erstellt. Dieses Protokoll wird in der Systemstruktur der -Konsole McAfee ePO angezeigt und hilft Ihnen, die Uhrzeiten der Befehle zu überwachen, die an bestimmte Endpunkte gesendet werden. Führen Sie die folgenden Schritte aus, um protokollierte ServiceNow -Ereignisse auf bestimmten Computern in einer McAfee ePO -Konsole anzuzeigen.

1. Navigieren Sie in der Konsole McAfee ePO zur Systemstruktur, und suchen Sie die Registerkarte ServiceNow.
2. Klicken Sie auf die Registerkarte, um eine Liste der Hostcomputer zu öffnen.
3. Klicken Sie in der Spalte Name auf einen Hostnamen, um das Audit-Protokoll zu öffnen.

In der folgenden Abbildung wird ein Beispiel für ein Protokoll für einen Host (PODCLIENT1) angezeigt.



Die von den Profilen in Ihrer Instanz Now Platform® initiierten Ereignisse werden aufgezeichnet und im Protokoll angezeigt. Überprüfen Sie den Status des Hostcomputers,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um sicherzustellen, dass die im Protokoll aufgeführten Ereignisse auf dem Host erfolgreich abgeschlossen wurden.

Beispielprofile

Die folgenden Themen enthalten Beispiele zum Konfigurieren von Profilen und zum Testen von Security Incidents. Diese Beispiele enthalten Profile für alle McAfee ePO -Fähigkeiten, die für diese Integration verfügbar sind.

Konfigurieren Sie Profile und Security Incidents für System-Ergänzungsabfragen für die McAfee ePO -Integration

Konfigurieren Sie Ihre Profileinstellungen so, dass das Profil nur unter den von Ihnen festgelegten Bedingungen ausgelöst wird.

Vorbereitungen

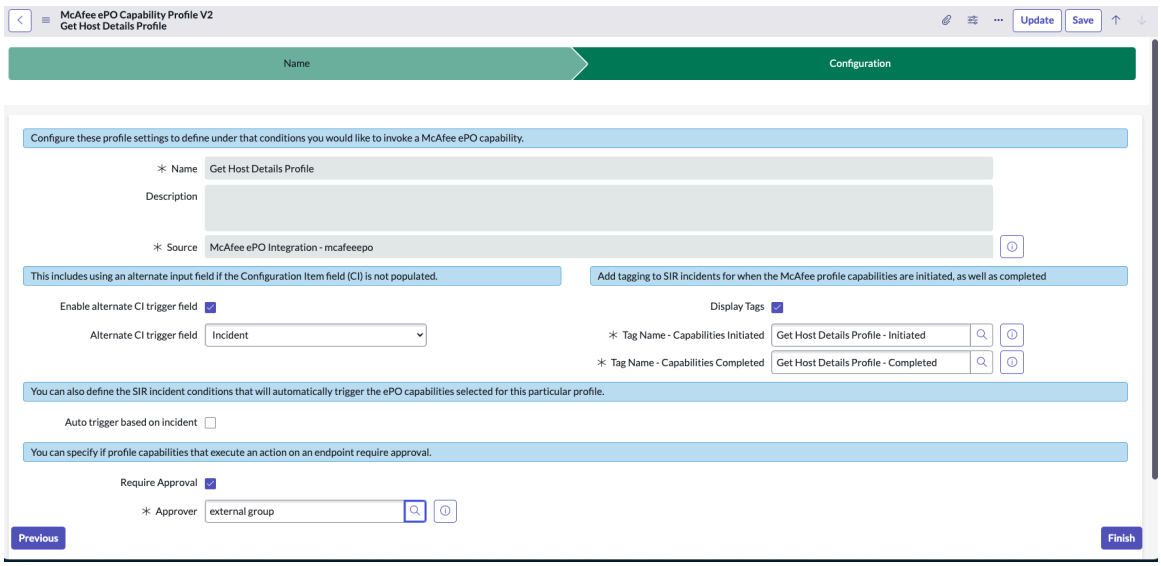
Erforderliche Rolle: Now Platform® Security Incident Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie die Bedingungen, die die Fähigkeiten McAfee ePO, die Sie für das Profil ausgewählt haben, automatisch auslösen. Sie können auch ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen. In diesem alternativen Feld können Sie Filterbedingungen festlegen, sodass nur die Security Incidents, die mit dem auslösenden Ereignis zusammenhängen, das Profil automatisch auslösen.

Prozedur

1. Wenn die Konfigurationsseite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Configuration (Konfiguration)**.
2. Füllen Sie die Felder im Formular aus



3. Führen Sie die folgenden Schritte aus, um die Option für das alternative CI-Feld zu aktivieren und die Filterbedingungen festzulegen, unter denen dieses Profil automatisch aufgerufen wird.

   a. Aktivieren Sie das Kontrollkästchen **Alternatives CI-Auslöserfeld aktivieren**.
   Das Feld Alternative CI-Auslöser wird angezeigt. In diesem Beispiel gehen Sie als Benutzer mit der Rolle sn_si.admin davon aus, dass das CI-Feld bei der Incident-Erstellung im Security Incident nicht ausgefüllt wird. Alternativ gehen Sie davon aus, dass CI-Informationen für einen FQDN, einen Hostnamen oder eine IP-Adresse im Feld Identifiziertes CI des Security Incident ausgefüllt werden, und wählen Sie alternativ

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das Feld Identifiziertes CI aus. Für dieses Beispiel ist das identifizierte CI ausgewählt. Sie können jedoch jedes Feld im Security Incident für das alternative CI verwenden.

b. Wählen Sie in der angezeigten Auswahlliste **Alternatives CI-Auslöserfeld** das Feld **Identifiziertes CI** aus.

Alle verfügbaren Felder für den Security Incident werden in der Liste angezeigt, einschließlich aller anwenderdefinierten Felder. Im Feld Alternativer CI-Auslöser wird Identifiziertes CI angezeigt.

Wenn dieses Profil aufgerufen wird und das CI-Feld im zugeordneten Security Incident beim ersten Event-Auslöser nicht ausgefüllt ist, verwendet das Profil alternativ den Wert aus dem Feld Identifiziertes CI in der Suche.

c. Aktivieren Sie das Kontrollkästchen **Basierend auf Incident automatisch auslösen**.
Der Generator für Filterbedingungen wird angezeigt. Mit dieser Option können Sie Filterbedingungen festlegen und angeben, wann das Profil beim Erstellen eines Security Incident automatisch aufgerufen wird.

d. Definieren Sie die SIR-Incident-Bedingungen, die die für dieses bestimmte Profil ausgewählten ePO-Fähigkeiten automatisch auslösen.

e. Wenn die Profilfähigkeiten, die eine Aktion auf einem Endpunkt ausführen, genehmigt werden müssen, aktivieren Sie das Kontrollkästchen **Genehmigung erforderlich**.

f. Wählen Sie über das Suchsymbol eine Genehmigung aus.

4. Klicken Sie auf **Fertigstellen**.
Sie haben das Profil erfolgreich konfiguriert, sodass es bei der Incident-Erstellung automatisch ausgelöst wird und ein alternatives Feld zum Ausfüllen übereinstimmender CI-Ergebnisse verwendet wird.

Lösen Sie das Profil McAfee ePO manuell über einen Security Incident aus

Lösen Sie ein Fähigkeitsprofil manuell aus einem Now Platform Security Incident Response (SIR) Security Incident aus.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Hinweis:
Die Genehmigungsoption in Profile für die Integration McAfee ePO werden konfiguriert wird nur für die Funktionen Host isolieren und Hostisolierung entfernen angezeigt.

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Anforderung zum automatischen Abrufen von Hostdetails, zum Isolieren des Hostcomputers oder zum automatischen Entfernen der Isolation eines Computers aufrufen, wenn die von Ihnen im Profil angegebenen Auslösebedingungen mit den Bedingungen für Security Incidents übereinstimmen. Wenn Sie eine Anforderung manuell übermitteln möchten, können Sie sie alternativ direkt aus einem Security Incident übermitteln.

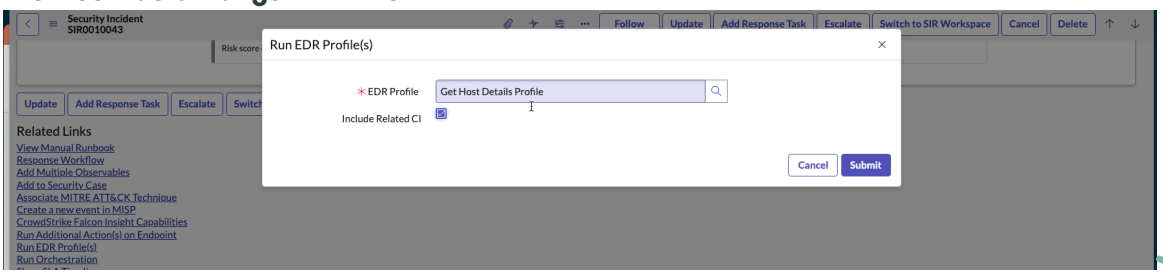
Sobald Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in den Security Incidents Now Platform anzeigen. McAfee ePO Mit Integrationen können Sie auch einzelne Fähigkeiten für Configuration Items (CIs) ausführen, ohne ein Profil zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

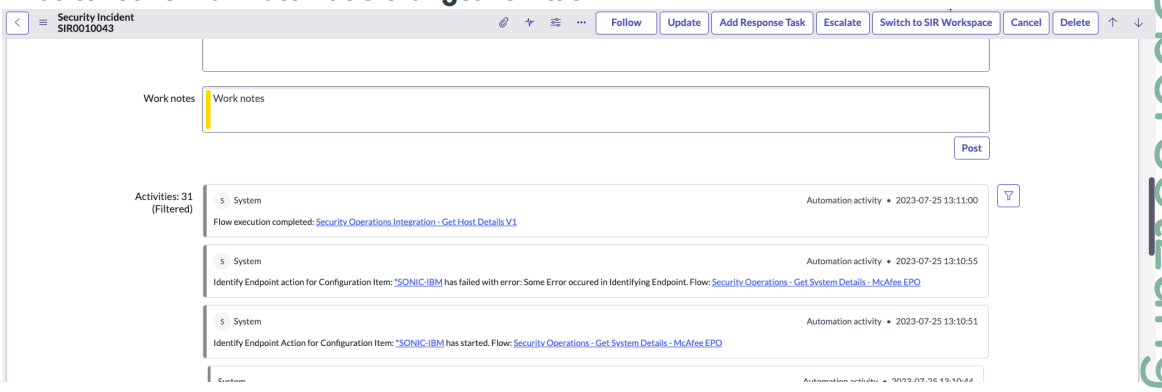
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen McAfee ePO aus.
3. Wählen Sie im Abschnitt „Zugehörige Listen“ **EDR-Profil(e) ausführen aus**.

McAfee-Ausführungs-EDR-Profil



4. Durchsuchen und ein Profil aus der Liste der verfügbaren Profile auswählen
   Die Liste der verfügbaren Profile lautet „Hostdetails abrufen“, „Hostcomputer isolieren“ und „Isolierung entfernen“. Wählen Sie beispielsweise Get Host Details (Hostdetails abrufen).
5. Wählen Sie **„Zugehöriges CI einschließen“** aus, um dieses Profil für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.
6. Klicken Sie auf **Absenden**.
   Das ausgewählte Profil wird manuell ausgelöst. Sie können den Abschnitt „Arbeitsnotizen und Aktivitäten“ sowie die Tags „Profil initiiert“ und „Profil abgeschlossen“ im Abschnitt „Arbeitsnotizen“ überprüfen.

Arbeitsnotizen für Automatisierungsaktivität

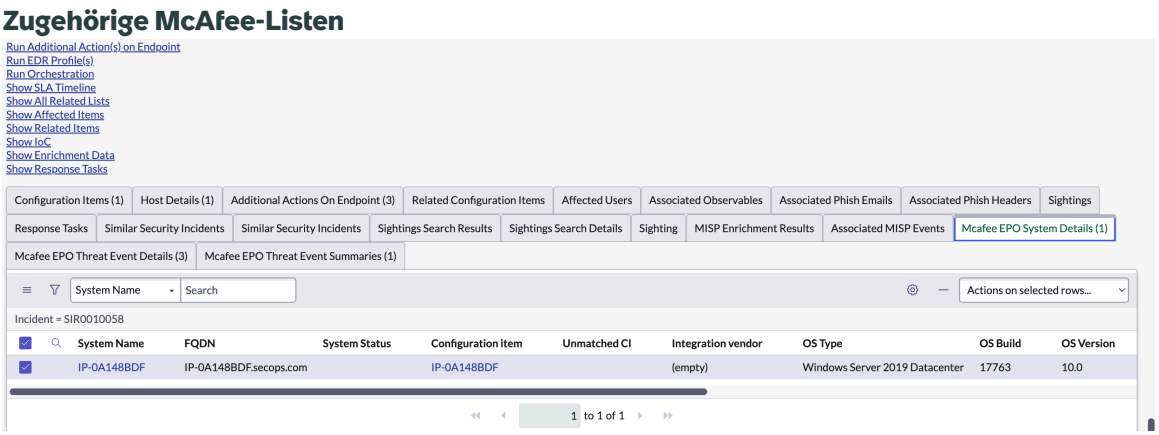


Die Ergebnisse werden in Form von zugehörigen Listen angezeigt, z. B. „Hostdetails abrufen“, „Hostcomputer isolieren“ oder „Isolierung entfernen“.

Hinweis:
Alle zugehörigen Listentabellen erweitern die Basistabellen. In diesem Beispiel sind die McAfee ePO-Systemdetails eine erweiterte Tabelle der Basistabelle „Hostdetails“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Um einzelne Fähigkeiten für ein Configuration Item (CI) auszuführen, gehen Sie wie folgt vor:

   a. Wählen Sie in der zugehörigen Liste Configuration Items das gewünschte CI aus.

   b. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen Sie die Fähigkeit aus, die Sie für das ausgewählte CI ausführen möchten.
   Beispiel: Host isolieren.

   c. Klicken Sie auf **Host isolieren,** um die Anwendung für das ausgewählte CI auszuführen.
   Das ausgewählte CI wird vom Netzwerk isoliert.

Lösen Sie zusätzliche Aktionen in der McAfee ePO -Integration aus

Die Funktionen „Bedrohungsereignisse auflisten“ und „Malware-Scan initiieren“ können über Zusätzliche Aktionen ausführen ausgelöst werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

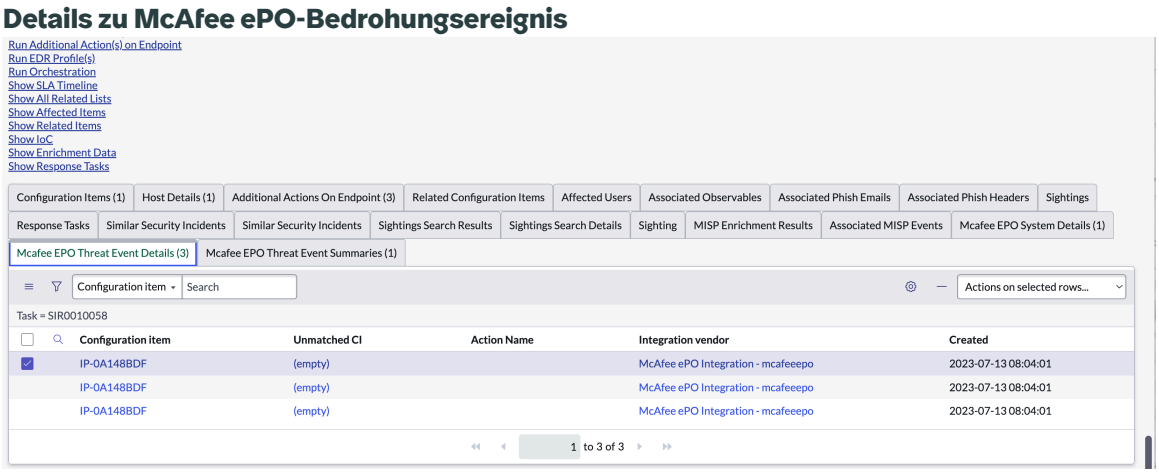
Sie können zusätzliche Aktionen in der Integration McAfee ePO mithilfe von **Zusätzliche Aktionen für Endpunkt ausführen**konfigurieren und auslösen, einschließlich der Funktionen McAfee ePO Bedrohungsereignisse auflisten und McAfee ePO Malware-Scans initiieren.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, für den Sie die zusätzlichen Aktionen ausführen möchten.
3. Klicken Sie im Abschnitt „Zugehörige Links“ **auf Zusätzliche Aktion(en) für Endpunkt ausführen**.
4. Suchen Sie die Fähigkeitsimplementierung, die Sie auslösen möchten, und wählen Sie sie aus der Liste der zusätzlichen Aktionen aus.
   Beispiel: McAfee ePO Liste Bedrohungsereignisse.
5. Wählen Sie **Zugehöriges CI einschließen aus**, um diese zusätzliche Aktion für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.
6. Klicken Sie auf **Zusätzliche Aktionen ausführen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Alle zugehörigen Listentabellen erweitern die Basistabellen. In diesem Beispiel ist die Tabelle „McAfee ePO-Bedrohungsereignisdetails“ eine erweiterte Tabelle der Basistabelle „Zusätzliche Aktionen für Endpunkt“.

7. Zeigen Sie die McAfee ePO-Bedrohungsereignisdetails in den zugehörigen Listen an, und validieren Sie sie.

Verwenden der -Integration McAfee ePO von in Analyst Workspace

Verwenden Sie die McAfee ePO -Integration, um die McAfee ePO -Fähigkeiten im SIR-Analystenarbeitsbereich zu nutzen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Bevor Sie McAfee ePO die -Integration im Security Incident Response-Arbeitsbereich verwenden, müssen Sie sie aus dem ServiceNow Store herunterladen und konfigurieren. Weitere Informationen finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration McAfee ePO ein.

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Integration McAfee ePO verwenden, um Korrekturaktionen für die Endpunkte in Echtzeit durchzuführen, Profile zum Sammeln von Details zum Host zu verwenden und über den Arbeitsbereich Security Incident Response spezifische Abfragen oder Aktionen für den Endpunkt durchzuführen.

Die McAfee ePO -Integration ermöglicht Analysten die Verwendung der folgenden McAfee ePO -Funktionen im Security Incident Response -Arbeitsbereich für Analysten:

- **Hostdetails abrufen**
- **Host isolieren**
- **Isolation entfernen**
- **Zusätzliche Aktion(en) für Endpunkt ausführen**

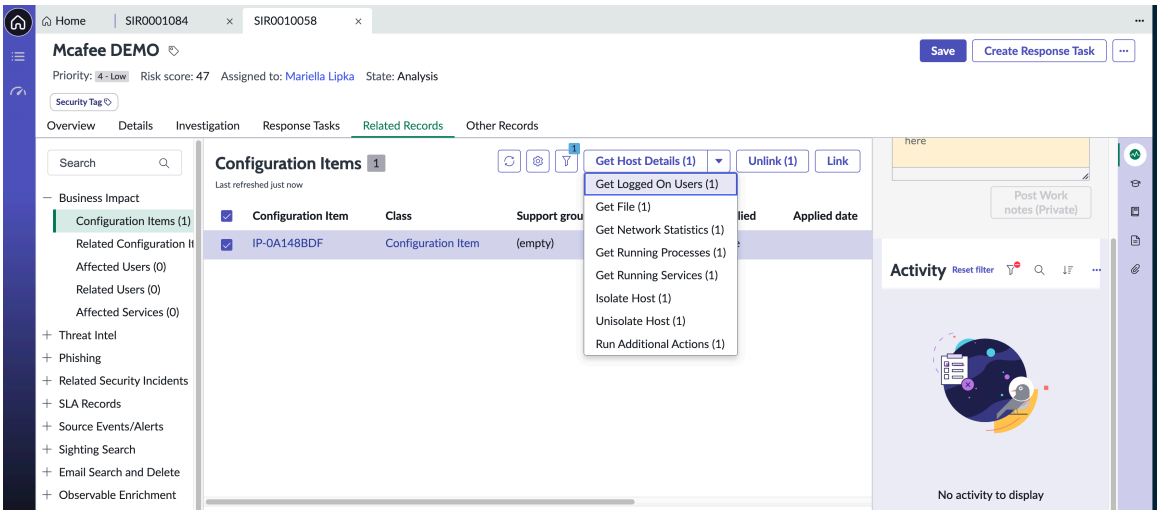
Prozedur

1. Um den Security Incident im SIR-Arbeitsbereich zu öffnen, klicken Sie im Security Incident auf **Zu SIR-Arbeitsbereich wechseln**.
2. Wählen Sie im SIR-Arbeitsbereich die Registerkarte **Zugehörige Datensätze**.

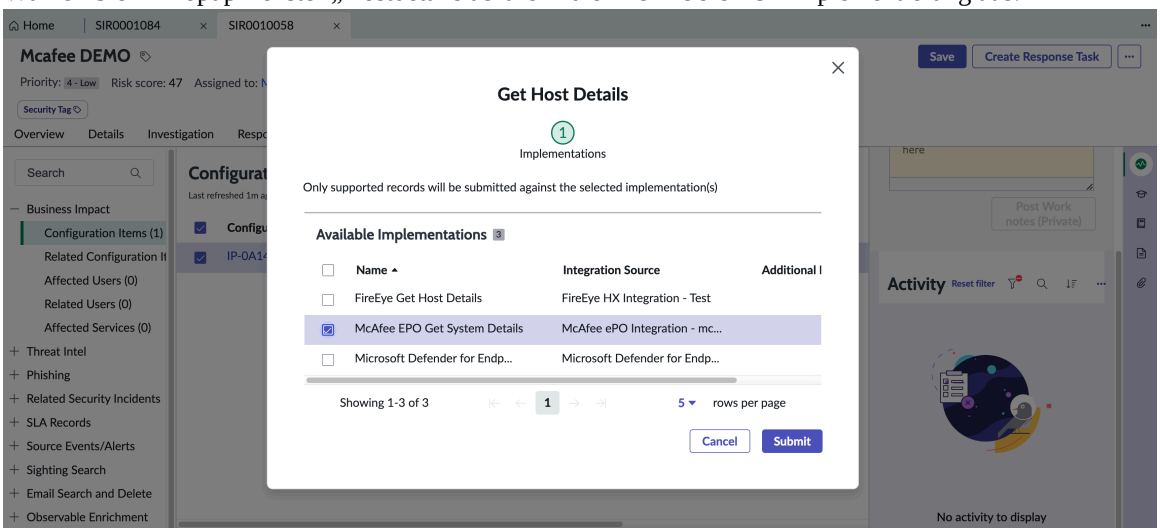
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie ein beliebiges **Konfigurationselement**aus, und wählen Sie eine McAfee ePO-Fähigkeit aus, die in der Dropdown-Aktion der zugehörigen Liste ausgelöst werden soll.
   Beispiel: Hostdetails abrufen.



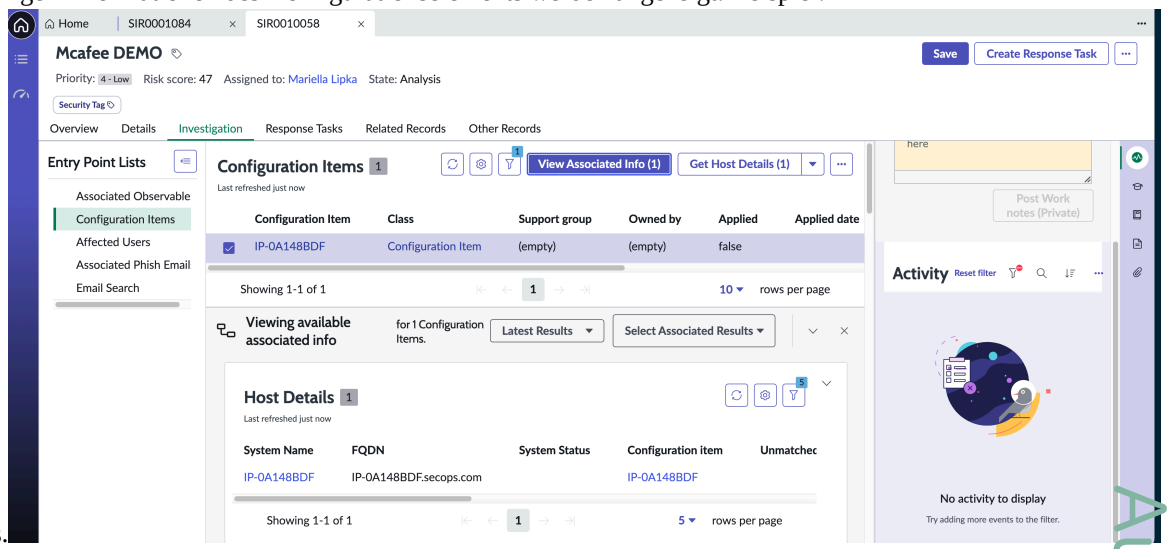
4. Wählen Sie im Popup-Fenster „Hostdetails abrufen“ die **McAfee ePO-** Implementierung aus.



5. Klicken Sie auf **Absenden**.
   Die Fähigkeit „Hostdetails abrufen“ wird für das CI aufgerufen. Sie können die Arbeitsnotizen für die -Ergebnisse und -Ergebnisse anzeigen.
6. Um die Daten für die ausgelöste Fähigkeit anzuzeigen, wählen Sie die Registerkarte **Ermittlung**.
7. Wählen Sie das **Konfigurationselement**aus, und klicken Sie auf die Aktion **Zugehörige Informationen anzeigen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die zugehörigen Informationen des Konfigurationselements werden angezeigt. Beispiel:



Hostdetails.

8. Klicken Sie auf das **Configuration Item (Konfigurationselement)**, um die Hostdetails anzuzeigen. Ebenso können Sie versuchen, die andere McAfee ePO-Funktion für Ihre Security Incidents im SIR-Analystenarbeitsbereich zu verwenden.
9. Sie können die McAfee ePO-Fähigkeiten in der zugehörigen Liste **„Endpoint Detection and Response (EDR)“** für Analysen verwenden.
10. Durchsuchen und ein Profil aus der Liste der verfügbaren Profile auswählen
    Die Liste der verfügbaren Profile lautet „Hostdetails abrufen“, „Hostcomputer isolieren“ und „Isolierung entfernen“. Wählen Sie beispielsweise Get Host Details (Hostdetails abrufen).
11. Wählen Sie die **McAfee ePO-** Implementierung aus, und klicken Sie auf **Absenden**.

McAfee ESM – E-Mail-Parser-Integration

Die Integration „ESM – E-Mail-Parser“ wird von einem E-Mail-Parser unterstützt, der E-Mail-Benachrichtigungen von ESM verarbeitet, um Security Incidents zu erstellen.

Konfigurieren Sie die Integration „McAfee ESM – E-Mail-Parser“.

Die McAfee ESM-E-Mail-Parser-Integration verwendet E-Mail-Benachrichtigungen von ESM, um Ergänzungs- und Antwort-Workflows zu unterstützen.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Warum und wann dieser Vorgang ausgeführt wird

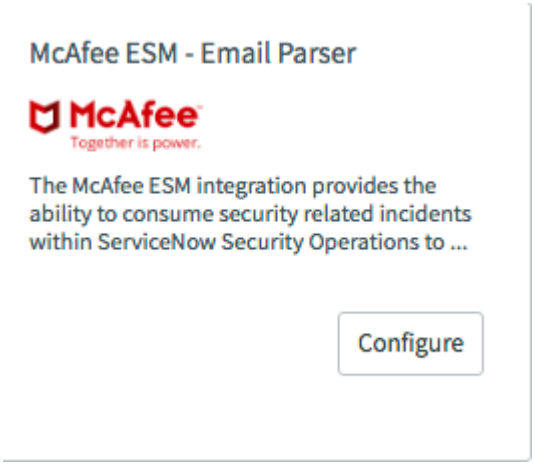
Für die Integration wird eine McAfee ESM-E-Mail-Parser-Vorlage bereitgestellt. Es muss konfiguriert und aktiviert werden, bevor die Integration stattfindet. Durch das Aktualisieren des Parsers wird er aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf der Karte McAfee ESM – E-Mail-Parser auf **Konfigurieren**.
3. Klicken Sie im Dialogfeld **„McAfee ESM – E-Mail-Parser-Konfiguration“** auf den Link **E-Mail-Parser konfigurieren**.
4. Klicken Sie auf den Link **McAfee ESM,** um die Einstellungen im bereitgestellten Parser für E-Mail-Vorlagen zu bearbeiten.
   Füllen Sie mindestens das Feld E-Mail ist von aus. Informationen zum Erstellen eines eigenen E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**.
6. Klicken Sie im Formular **„E-Mail-Parser“auf Aktualisieren**.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu **Integrationskonfigurationen**zurückkehren.

McAfee ESM – Integration zur Ergänzung von Incidents

McAfee ESM Die Integration zur Ergänzung von Incidents durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Erste Schritte mit der Integration McAfee ESM - Incident Enrichment
- Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

---

Verwenden

- Führen Sie eine Sichtungssuche aus
- Security Operations Integration - Sichtungssuche-Flow
- Security Operations – McAfee ESM-Sichtungssuch-Flow

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Zeigen Sie Details der Sichtungssuche an
- Sichtungssuchergebnisse anzeigen

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der Integration McAfee ESM - Incident Enrichment

McAfee ESM schützt Endpunkte vor Viren, Spyware, Trojanern und anderen Malware-Bedrohungen und lässt sich problemlos in Security Operationsintegrieren. Bevor Sie die Integration McAfee ESM - Incident Enrichment verwenden können, müssen Sie sie von ServiceNow Store herunterladen und die entsprechende API-Basis-URL sowie Anmeldeinformationen hinzufügen.

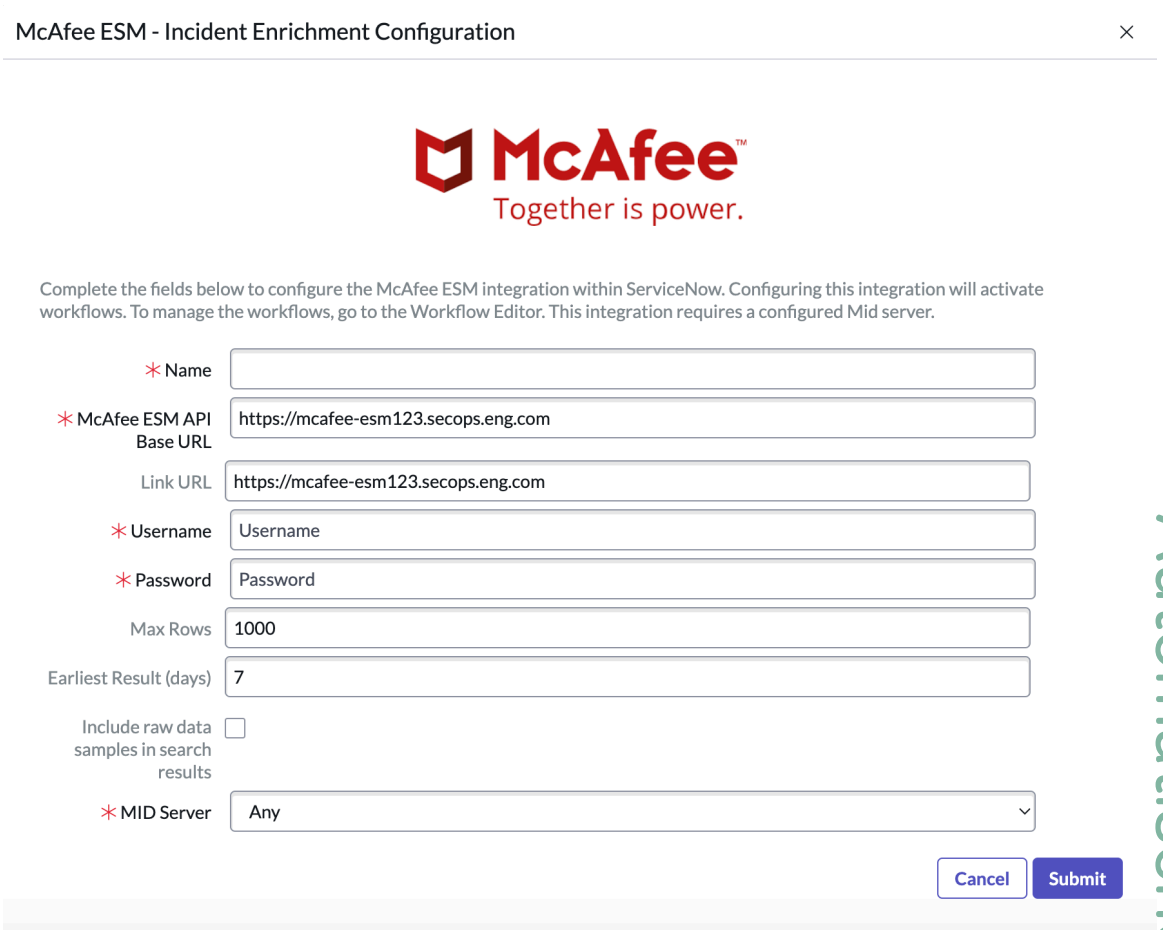
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte McAfee ESM – Incident-Ergänzung **auf Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der McAfee ESM-API	Die Basis-URL, die Sie von der McAfee ESM-Website erhalten haben.
Link-URL	[Optional] Die Link-URL, die auf eine McAfee ESM-Instanz verweist, falls verfügbar. **Hinweis:** Wenn ein Fehler angezeigt wird, verwenden Sie die Basis-URL der McAfee ESM-API.
Anwendername	Ihr McAfee ESM-Anwendername.
Passwort	Ihr McAfee ESM-Passwort.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.
Rohdatenmuster in	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchergebnissen berücksichtigen	Einstellung in der **Anzahl der Zeilen der Rohdateneigenschaft** in den Security Incident Response-Eigenschaftenab.
MID-Server	Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

5. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern bzw. zu löschen.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

Microsoft Azure Sentinel Integration

Microsoft Azure Sentinel ist eine cloudbasierte Lösung für Security Information Event Management (SIEM) und Security Orchestration Automated Response (SOAR). Sie können die Integration Microsoft Azure Sentinel verwenden, um Azure Sentinel-Incidents zu erfassen und automatisch Security Incidents in Security Incident Responsezu erstellen.

Apps im Store anfordern

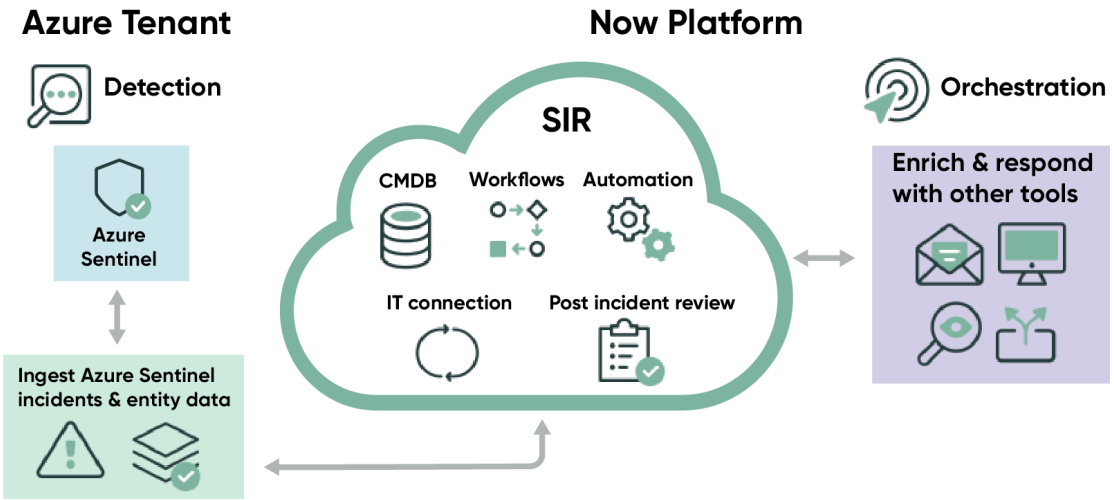
Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht

Im folgenden Diagramm können Sie erfahren, wie Microsoft Azure Sentinel in die Anwendung Now Platform Security Operations integriert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Platform - Azure Sentinel integration overview



Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erkennen Sie Microsoft Azure Sentinel Incidents, die Kandidaten für Security Incidents sind, und automatisieren Sie die Erstellung dieser Security Incidents.
- Ordnen Sie die Incident- und Entitätsfelder Microsoft Azure Sentinel den Security Incident-Feldern SIR zu.
- Filtern Sie Microsoft Azure Sentinel Incidents.
- Fassen Sie Incidents zu vorhandenen offenen Security Incidents zusammen, damit Sie keine doppelten Security Incidents erstellen müssen.
- Automatisieren Sie Microsoft Azure Sentinel die Aktualisierung des Incident-Status für Security Incident Response, damit Sie Security Incidents erstellen und schließen können.

Hinweis:
ServiceNow aktualisiert den Status von Microsoft Azure Sentinel Incidents basierend auf der Erstellung oder dem Abschluss des Security Incidents. Dieses Update enthält auch Kommentare von aggregierten Incidents und neuen Incidents.

- Planen Sie die Incident-Erfassung, um regelmäßig Security Incidents zu erstellen.
- Synchronisieren Sie Microsoft Azure Sentinel Incident-Kommentare mit SIR Arbeitsnotizen.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
MicrosoftMicrosoft Azure Event Hubs Website mit Produktdokumentation	Microsoft-Website mit Produktdokumentation
ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit Microsoft Azure Sentinel der -Integration

Aktivieren Sie das Plugin Microsoft Azure Sentinel – Incident Ingestion for Security Operation, und richten Sie es als Schnittstelle mit Ihrer Instanz Now Platform und Ihrem Produkt Security Incident Response ein.

Vorbereitungen

Erforderliche Rolle: Microsoft Azure Anwendungsentwickler, Microsoft Azure Mandantenadministrator

Bevor Sie die Microsoft Azure Sentinel -Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

Warum und wann dieser Vorgang ausgeführt wird

Sehen Sie sich die folgende Setupprüfliste an, und vergewissern Sie sich, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben.

Prüfliste

Setupaufgabe	Beschreibung
Weisen Sie die erforderlichen Rollen Now Platform und Security Incident Response zu, und überprüfen Sie sie.	Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Die Rolle admin installiert die Integration aus ServiceNow Store und weist die Rolle sn_si.admin zu. • Die Rolle sn_si.admin führt die folgenden Aufgaben aus: ◦ Konfiguriert die Integration. ◦ Erstellt Incident-Profile. ◦ Ordnet die Incident-Datenfelder Microsoft Azure Sentinel den Security Incident-Feldern zu. ◦ Plant die laufende Incident-Erfassung. ◦ Aktiviert Incident-Updates, wenn der Incident Security Incident Response erstellt oder geschlossen wird. ◦ Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu.
Weisen Sie die Microsoft Azure erforderlichen Rollen zu.	Die folgenden Rollen sind in Microsoft Azure erforderlich, um Ihre Anwendung zu registrieren und zu konfigurieren: • Anwendungsentwickler für die Registrierung der Anwendung. • Mandantenadministrator zum Erteilen von Berechtigungen für die Anwendung durch Aufrufen des Endpunkts für die Administratoreinwilligung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren.	Das Plugin ServiceNow IntegrationHub Starter Pack Installer [com.glide.hub.integrations] ist erforderlich. Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren, die für die Integration erforderlich sind. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie sie einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation zu gewährleisten: **1.** Security Incident Response **2.** Security Incident Response-Benutzeroberfläche **3.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **4.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Registrieren Sie sich, und konfigurieren Sie Ihre Anwendung im Microsoft Azure -Portal	Registrieren Sie Ihre Anwendung im -Portal Microsoft Azure, und gewähren Sie Ihren Benutzern Lese- und Schreibzugriff auf die Anwendung.

Registrieren und konfigurieren Sie das -Portal Microsoft Azure .

Registrieren Sie Ihre Anwendung im -Portal Microsoft Azure, und gewähren Sie Ihren Benutzern Lese- und Schreibzugriff auf die Anwendung.

Vorbereitungen

Erforderliche Rolle: Microsoft Azure Anwendungsentwickler, Microsoft Azure Mandantenadministrator

Prozedur

1. Melden Sie sich beim -Portal Microsoft Azure an.

2. Suchen Sie nach **App-Registrierungen**, und wählen Sie sie aus.

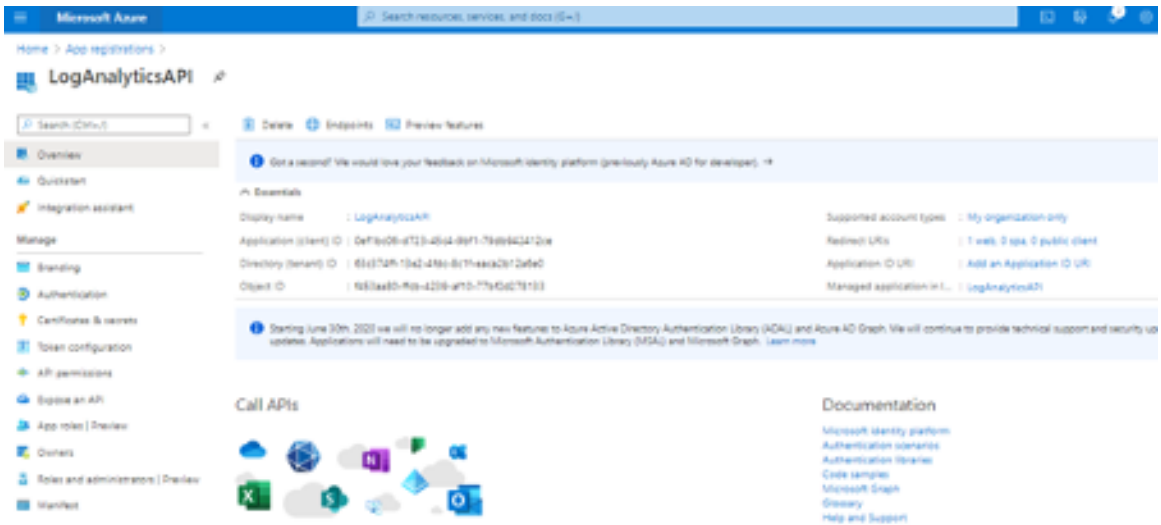
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **New registration (Neue Registrierung)**.
4. Füllen Sie die Felder des Formulars aus.

Registrieren Sie ein Anwendungsformular

Feld	Beschreibung
Name	Dem Anwender angezeigter Anzeigename für die Anwendung. Beispiel: LogAnalyticsAPI.
Unterstützte Account-Typen	Kontotyp, der diese Anwendung verwenden oder auf die API zugreifen kann.
Umleitungs-URI	Umleitungs-URI Die Authentifizierungsantwort wird an diesen URI weitergeleitet, nachdem ein Anwender erfolgreich authentifiziert wurde.

5. Klicken Sie auf **registrieren**.
   Nachdem Sie die Anwendung erfolgreich registriert haben, wird die Seite „Übersicht“ angezeigt.



6. Navigieren zu **Verwalten** > **Zertifikate und Geheimnisse**.
7. Klicken Sie im Abschnitt Geheime Clientschlüssel auf **Neuer Clientschlüssel**.
   Sie können den geheimen Clientschlüssel später nicht anzeigen. Kopieren und speichern Sie ihn daher in diesem Schritt jetzt. Wenn Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen generieren, indem Sie die Anweisungen in den Schritten 4 und 5 befolgen.
8. Navigieren zu **Verwalten** > **API-Berechtigungen**.
9. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
10. Klicken Sie im Fenster API-Berechtigungen anfordern auf die Registerkarte **Von meiner Organisation verwendete APIs**.
11. Suchen und wählen Sie den Namen **der Log Analytics-API-** App aus.
12. Wählen Sie in den Log Analytics API-Berechtigungen **die Option Anwendungsberechtigungen**aus.
    Durch Aktivieren dieser Berechtigung wird sichergestellt, dass die Anwendung als Hintergrundservice oder Daemon ohne angemeldeten Benutzer ausgeführt wird.
13. Wählen Sie im Abschnitt „Daten“ die Option **Data.Read**aus
14. Klicken Sie auf **Berechtigungen hinzufügen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Berechtigungen werden aktualisiert.

15. Aktivieren Sie die Option **Admin-Zustimmung für Standardverzeichnis erteilen** für die Data.Read-API-Berechtigung, die Sie in Schritt 13 aktiviert haben.
16. Suchen Sie nach **Log Analytics-Arbeitsbereichen**, und wählen Sie den entsprechenden Eintrag aus.
17. Wählen Sie Ihren Sentinel Log Analytics-Arbeitsbereich aus.
    Sie sehen jetzt die Übersichtsseite des Sentinel Log Analytics-Arbeitsbereichs.
18. Navigieren zu **Zugriffssteuerung (IAM)** > **Rollenzuweisungen**.
19. Klicken Sie auf **Hinzufügen**, und wählen Sie **Rollenzuweisung hinzufügen**aus.
20. Füllen Sie die Felder des Formulars aus.

Formular für die Zuweisung von Rollen hinzufügen

Feld	Beschreibung
Rolle	Kontotyp, der diese Anwendung verwenden kann. Wählen Sie **Azure Sentinel-Responder**aus.
Assign access zu (Zugriff zuweisen an)	Von Ihnen definierter Berechtigungsbereich. Wählen Sie **Benutzer**, **Gruppe**oder **Serviceprinzipal**aus.
Auswahlvorgang	Anwendung, die Sie zuvor in Schritt 4 erstellt haben. Beispiel: LogAnalyticsAPI.

21. Klicken Sie auf **Speichern**.

Installieren und konfigurieren Sie die -Integration Microsoft Azure Sentinel .

Installieren und konfigurieren Sie die Microsoft Azure Sentinel -Integration aus ServiceNow Store in Ihrer Instanz Now Platform, um mit der Erfassung von Azure Sentinel-Incidents zu beginnen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie die Microsoft Azure Sentinel -Integration von ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel Microsoft Azure Sentinel, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

Microsoft Azure Sentinel Formular „Konfigurationen der Incident-Erfassung“.

Feld	Beschreibung
Name	Name für die Konfiguration der Instanz Microsoft Azure Cloud
Identitäts-URL	Identitäts-URL für den Mandanten Microsoft Azure Cloud Beispiel: login.microsoftonline.com. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Azure Resource Manager	Azure Resource Manager-Endpunkt für Mandanten Microsoft Azure Cloud. Beispiel: Management.azure.com. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation .
Mandanten-ID	Microsoft Azure Sentinel Mandanten-ID Dies ist die Instanz, aus der alle Incidents im Portal Microsoft Azure abgerufen werden.
Client-ID	Client-ID für die Anwendung, die Sie im -Portal Microsoft Azure registriert haben.
Geheimer Clientschlüssel	Geheimer Clientschlüssel für Ihre registrierte Anwendung.
Abonnement-ID	Abonnement-ID für Ihre registrierte Anwendung.
Ressourcengruppenname	Ressourcengruppenname für Ihre registrierte Anwendung.
Arbeitsbereichsname	Arbeitsbereichsname für Ihre registrierte Anwendung.

5. Klicken Sie auf **Absenden**.

Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird jede Konfiguration eines Incident-Erfassungsservers auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für Microsoft Azure Sentinel

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform, und bestimmen Sie die Microsoft Azure Sentinel -Incidents, die sich zum Erstellen von Security Incidents eignen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Mit der Integration können Sie verschiedene Arten von Incidents erstellen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Incidents werden basierend auf den Profilen erstellt, die Sie in der Instanz Now Platform konfigurieren. Alle Incidents werden zunächst für einen konfigurierten Incident-Typ in einem Profil erstellt. Erstellte Incidents können dann weiter gefiltert werden, um anzugeben, welche Incidents Security Incidents erstellen.

Alle Incidents, die die Auswahlkriterien in Ihrem Mandanten Microsoft Azure erfüllen und über die API Microsoft Azure Sentinel verfügbar sind, werden zunächst in Ihrer Instanz Now Platform erfasst.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Azure Sentinel Formular „Konfigurationen der Incident-Erfassung“.

Feld	Beschreibung
Name	Name für das Profil Dieser Name hilft Ihnen, den Profiltyp zu identifizieren, und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist.
Aktiv	Indikator, der angibt, dass das Profil aktiv ist. Wenn das Profil aktiv ist, impliziert dies, dass Now Platform Azure Sentinel-Incidents aktiv abfragt und dass entsprechende Security Incidents in SIR erstellt werden, wenn die Filterbedingungen erfüllt sind.
Quelle	Microsoft Azure -Mandanten, den Sie für die Erfassung von Incidents konfiguriert haben. Wenn mehrere Mandanten konfiguriert sind, wählen Sie den entsprechenden Mandanten für die Incident-Typen aus, die für das Profil erfasst werden sollen.
Bestellung	Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Flow mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Beispiel: 100, 200, 300, 400. Der Standardwert ist 100.
Beschreibung	Zusätzlicher Text, mit dem Sie dieses Profil von anderen Profilen unterscheiden können.

4. Um zum Abschnitt „Zuordnung“ zu wechseln, klicken Sie auf **Fortfahren**.

Nächste Maßnahme

Ordnen Sie einzelne Incident-Felder Microsoft Azure Sentinel den Feldern im Security Incident Now Platform SIR zu.

Ordnen Sie die Incident-Felder Microsoft Azure Sentinel zu

Ordnen Sie die einzelnen Incident-Felder Microsoft Azure Sentinel den Feldern im Security Incident SIR zu, um mit den zugeordneten Daten Incidents zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie auf der Zuordnungsseite im Abschnitt „Azure Sentinel-Feldzuordnung“ eine der Beispielerfassungsmethoden aus.

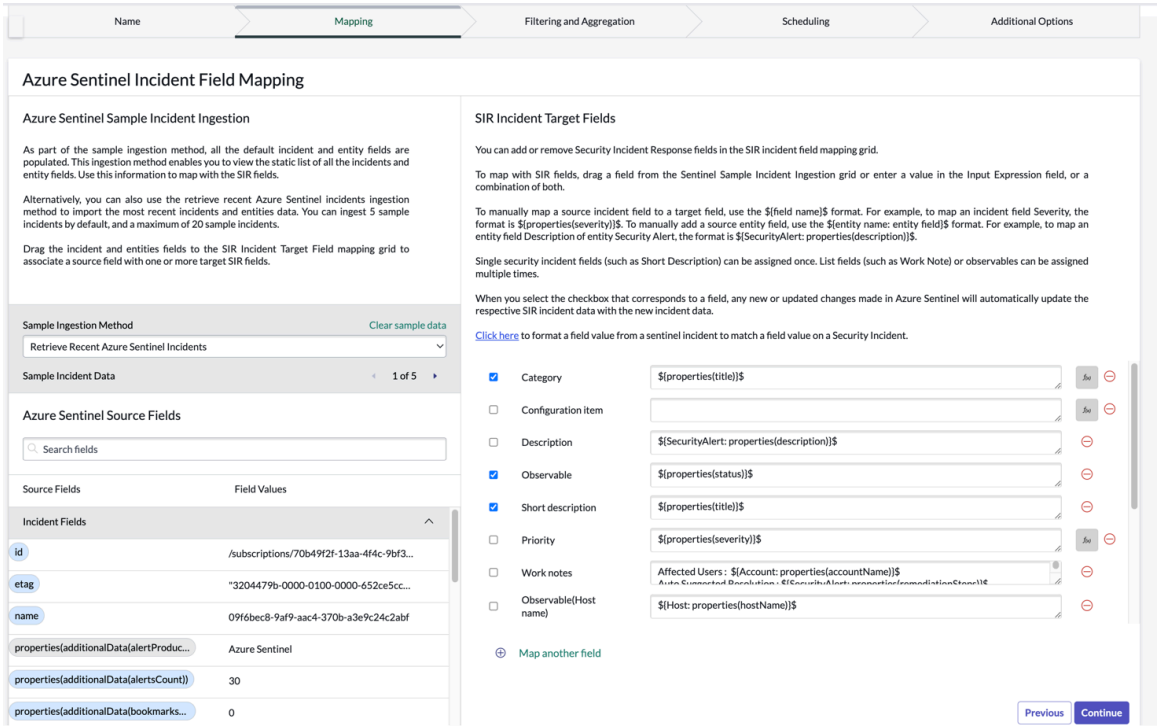
Beispiel für Erfassungsmethoden

Feld	Beschreibung
Alle Standardfelder für Incident und Entität	Verwenden Sie diese Erfassungsmethode, um die statische Liste aller Incident- und Entitätsfelder anzuzeigen. Diese Methode enthält nur Standardfeldnamen ohne Werte. Sie können diese Informationen verwenden, um die Zuordnung zu den Feldern SIR vorzunehmen.
Rufen Sie die neuesten Azure Sentinel-Incidents ab	Verwenden Sie diese Erfassungsmethode, um die neuesten Incident- und Entitätsdaten zu importieren. Wenn der Azure Sentinel-Incident die Entitätsdaten enthält, werden die Entitätsdaten abgerufen und stehen für die Zuordnung im Abschnitt „Azure Sentinel-Quellfelder“ zur Verfügung. Manchmal enthält der Azure Sentinel-Incident die Entitätsdaten möglicherweise nicht, und daher sind die Entitätsfelder in einem solchen Szenario nicht für die Zuordnung verfügbar. Wenn der Azure Sentinel-Incident mehrere Warnungen enthält, wird im Zuordnungsabschnitt die früheste Warnung angezeigt, die Teil des incident ist. Auch während der Erfassung werden die frühesten Feldwerte für Sicherheitswarnungen verwendet. Sie können standardmäßig 5 Beispiel-Incidents und maximal 20 Beispiel-Incidents erfassen. Die Feldwerte für den Beispiel-Incident werden gefüllt, wenn das Profil die Beispiel-Incidents erfasst. Sie können diese Incidents den **SIR-Incident-Zielfeldern**zuordnen. Die Incident-Felder und -Werte werden als einzelne Registerkarten angezeigt.
Importieren Sie Beispieldaten	Klicken Sie auf **Beispieldaten importieren**, um Beispiel-Incidents aus Azure Sentinel zu importieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Diese Schaltfläche wird angezeigt, wenn Sie die Erfassungsmethode Aktuelle Azure Sentinel-Incidents abrufen auswählen. Das Abrufen von Beispiel-Incidents vom Server Microsoft Azure Sentinel kann einen Moment dauern. Ordnen Sie diese abgerufenen Incidents den **SIR-Incident-Zielfeldern**zu. Die Incident-Felder und -Werte werden als einzelne Registerkarten angezeigt.



2. Führen Sie die folgenden Aktionen aus, um den Standardfeldern, die im Security Incident angezeigt werden, Felder hinzuzufügen:

a. Klicken Sie im Abschnitt „SIR-Incident-Zielfelder“ auf die ⊕ Map another field Schaltfläche „Weiteres Feld zuordnen“
Es zeigt eine Liste von Feldern SIR, aus denen Sie ein Feld für ein neues anzuzeigendes Feld auswählen können.

b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie dann ein Feld aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für denselben Security Incident können mehrere erkennbare Elemente angezeigt werden. Beispielsweise kann das Feld „ **Erkennbares Element** “ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder **Konfigurationselement** und **Arbeitsnotizen** mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird eine Fehlermeldung angezeigt, dass dieses Feld nicht mehrere Werte unterstützt. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Ziehen Sie Ihr Feld aus dem Abschnitt „Azure Sentinel-Quellfelder“ per Drag-and-Drop, um es dem neuen Feld zuzuordnen.

d. Wenn Sie das Kontrollkästchen aktivieren, das einem Feld entspricht, werden bei neuen oder aktualisierten Changes, die in Azure Sentinel vorgenommen werden, die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

Hinweis:
Im Basissystem ist die Systemeigenschaft sn_sec_sentinel.incident_updates standardmäßig auf „True“ festgelegt, um die Microsoft Azure Sentinel -Updates im Zusammenhang mit neuen Warnungen zu erhalten, die mit SIR verknüpft sind.

- Standardmäßig sind die Felder Betroffene Anwender, Konfigurationselemente und Erkennbare Elemente aktiviert. Dies bedeutet, dass jedes Mal, wenn dem Incident neue erkennbare Elemente oder zugehörige Konfigurationselemente oder betroffene Benutzer hinzugefügt werden, diese Informationen während dieses Abfrageintervalls automatisch extrahiert und in die entsprechenden zugehörigen Listen in Security Incident Response (SIR) eingetragen werden.
- Für alle anderen Felder müssen Sie das Kontrollkästchen aktivieren, das einem Feld für alle neuen oder aktualisierten Änderungen entspricht, die im Azure Sentinel-Incident-Datensatz in Azure Sentinel vorgenommen werden. Dadurch werden die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

Wichtig:
Vor der Auswahl dieser Funktionalität muss die Sorgfaltspflicht erfüllt werden, da das Überschreiben der vorhandenen Daten zu instabilen Daten führen kann, mit denen der Analyst arbeiten kann, und jede andere Automatisierung, die auch durch die Feldwerte des Security Incident festgelegt wird, betroffen sein kann. Daher ist es sehr wichtig, die Sorgfaltspflicht zu erfüllen, bevor Sie eine Überschreibungsfunktion auswählen.

3. Um ein Feld zu entfernen, klicken Sie auf die Schaltfläche Element entfernen neben dem Eingabeausdrucksfeld im Abschnitt „SIR-Incident-Zielfelder“.

4. Um einen Feldwert aus dem Abschnitt „Azure Sentinel-Quellfelder“ einem Feld im Abschnitt „SIR-Incident-Zielfelder“ zuzuordnen, verwenden Sie eine der folgenden Aktionen:

a. Ziehen Sie den Feldnamen (z. B. ID), und legen Sie ihn neben einem Feldnamen in der Spalte „SIR-Incident-Zielfelder“ ab.

Sie können einen beliebigen Wert aus dem Abschnitt „Azure Sentinel-Quellfelder“ mit einem Feld im Abschnitt „SIR-Incident-Zielfelder“ abgleichen. Felder sind farbcodiert, damit Sie Incident-Felder im Zuordnungsprozess nicht übersehen oder duplizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hellblaue Felder zeigen an, dass ein Incident-Feld noch nicht ausgewählt und dem Security Incident zugeordnet wurde. Unter Umständen möchten Sie ein eingehendes Incident-Feld mehreren Feldern in einem Security Incident zuordnen. Ein graus Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Auf diese Weise können Sie visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob wichtige Incident-Informationen verbleiben.

b. Sie können eine Kombination aus Text und Feld hinzufügen.
Beispiel: Incident-Name ist ${name}$. Hier kann der Incident-Name manuell eingegeben werden, während ${name}$ aus dem Abschnitt „Azure Sentinel-Quellfelder“ zugeordnet wird.

c. Sie können ein Quell-Incident- oder Entitätsfeld direkt manuell eingeben und einem Zielfeld zuordnen.

- Um ein Quell-Incident-Feld manuell zuzuordnen, verwenden Sie das Format ${Feldname}$. Um beispielsweise das Incident-Feld Schweregrad zuzuordnen, lautet das Format${properties(severity)}$.
- Um ein Quellentitätsfeld manuell hinzuzufügen, verwenden Sie das Format ${Entitätsname: Entitätsfeld}$. Um beispielsweise das Entitätsfeld „Beschreibung der Entität „Sicherheitswarnung““ zuzuordnen, lautet das Format ${SecurityAlert: properties(description)}$.

Diese Integration klassifiziert bestimmte Untertypen von erkennbaren Elementen. Wenn Sie ein Azure Sentinel-Feld dem erkennbaren SIR-Feld zuordnen, klassifiziert Now Platform das erkennbare Element automatisch. Wenn Sie das eingehende erkennbare Azure Sentinel-Element generisch dem erkennbaren Elementtyp in SIRzuordnen möchten, ziehen Sie das Feld Azure Sentinel per Drag-and-Drop in das Feld Erkennbares Element. Wenn Sie jedoch den erkennbaren Typ des eingehenden erkennbaren Azure Sentinel-Elements in SIRkennen, ordnen Sie ihn speziell dem Feld „Erkennbarer Typ“ SIR zu. Einige Beispiele für bestimmte erkennbare Elemente in SIR sind „Erkennbares Element“ (Domänenname), „Erkennbares Element“ (E-Mail-Adresse), „Erkennbares Element“ (IP-Adresse (V4)) und „Erkennbares Element“ (Hostname).

Wenn Ihre eingehenden Azure Sentinel-Felder Informationen MITRE-ATT&CK enthalten, ordnen Sie diese dem Feld „Technik“ MITRE-ATT&CK zu. Stellen Sie sicher, dass das eingehende Azure Sentinel-Feld die MITRE-ATT&CK Technik-ID oder den Techniknamen enthält.

Manchmal werden Incident-Feldwerte in Microsoft Azure Sentinel möglicherweise nicht direkt in die Felder im SIR-Security Incident übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten.

5. Um eine Feldübersetzung für ein neues Feld aus einem Azure Sentinel-Incident so zu formatieren, dass sie einem Feldwert in einem Security Incident entspricht, klicken Sie auf den Link **Hier klicken** im Header **„SIR-Incident-Zielfelder“**.

6. Um die Felder zu ändern, die die Feldübersetzung unterstützen, klicken Sie auf das Symbol für .
Die Felder, die die Feldübersetzung unterstützen, sind **Kategorie**, **Konfigurationselement**und **Priorität**.

Klicken Sie beispielsweise auf das Symbol neben der Kategorie. Der Skript-Editor für Azure Sentinel-Feldübersetzung wird geöffnet.

7. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.
Definieren Sie beispielsweise für Kategorie Folgendes im Skript-Editor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
```

Diese Zuordnung stellt sicher, dass ein Profil nur konfigurierte Kategorien verwendet.

8. Setzen Sie Ihre Zuordnung fort, indem Sie Feldwerte hinzufügen oder entfernen.
   Dieselben Feldwerte können Sie im Generator für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Incident erfüllen muss, um einen Security Incident zu erstellen.
9. Um zum Abschnitt „Filtern und Aggregieren“ zu wechseln, klicken Sie auf **Fortsetzen**.

Nächste Maßnahme

Definieren Sie Filterbedingungen, und legen Sie sie fest, um festzulegen, welche Incidents Security Incidents erstellen sollen. Sie können dieselben Feldwerte (definiert im Abschnitt „Zuordnung“) im Generator für Bedingungen für Incident-Generierung (im Abschnitt „Filtern und Zusammenfassung“) verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Incident erfüllen muss, um einen Security Incident zu erstellen.

Definieren von Filter- und Zusammenfassungskriterien

Sie können Filterbedingungen definieren und festlegen, um festzulegen, welche eingehenden Microsoft Azure Sentinel Incidents Security Incidents erstellen sollen. Sie können auch zusätzliche Incident-Feldkriterien definieren, die es ermöglichen, einen eingehenden Incident an einen offenen Security Incident anzuhängen, anstatt einen Incident zu erstellen.

Legen Sie die Filterbedingungen für Security Incidents fest

Legen Sie die Filterbedingungen so fest, dass Security Incidents nur erstellt werden, wenn die Filterbedingungen erfüllt sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Art der Filterung hilft Ihnen, Security Incidents zu isolieren, und begrenzt die Anzahl der von Ihnen erstellten Security Incidents. Wenn Sie zusätzliche Filterkriterien festlegen, werden nur die erforderlichen Incidents erfasst, ohne dass die Abfrage oder die Konfiguration der ausgelösten Incidents geändert werden muss.

Prozedur

1. Um die Kriterien zu definieren, die ein eingehender Incident Microsoft Azure Sentinel erfüllen muss, damit ein Security Incident erstellt wird, wählen Sie **Basierend auf Bedingungen filtern**aus.

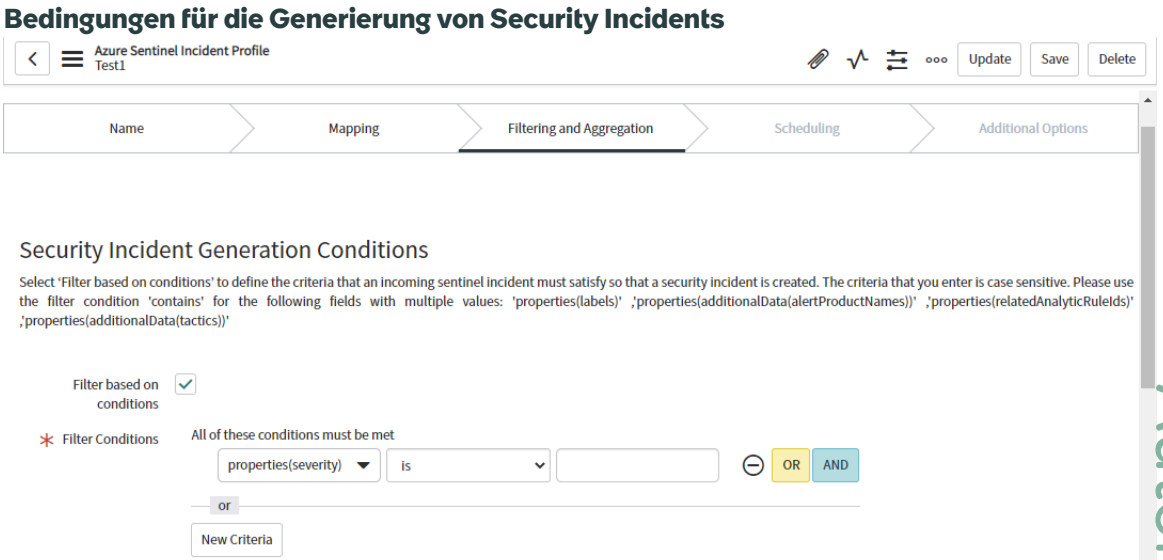
   Die Optionen im ersten Feld der Filterbedingungen entsprechen den Feldern, die im Abschnitt „Azure Sentinel – Beispiel-Incident-Erfassung“ für den von Ihnen erfassten Incident angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach dem von Ihnen erfassten Incident. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des incident übereinstimmen.

   Verwenden Sie die Filterbedingung *`enthält`* für die folgenden Felder mit mehreren Werten:

   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie für die obigen Felder die Filterbedingung „ *Enthält* “ verwenden, um sicherzustellen, dass die Daten ordnungsgemäß gefiltert werden.



2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.
   - Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.
4. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.

Definieren Sie Zusammenfassungsbedingungen

Definieren Sie zusätzliche Kriterien für die Incident-Zusammenfassung, die einen eingehenden Incident zu einem vorhandenen SIR-Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Wenn Sie für jedes Profil Kriterien für Feldabgleichwerte verwenden, kann diese zusätzliche Zusammenfassung die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Incident-Daten in einem einzigen Security Incident zusammengefasst werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein neuer Incident allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird der Incident automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der mit Security Incidents arbeiten, können Sie alle hinzugefügten aggregierten Incidents in einer zugehörigen Liste zu einem Security Incident anzeigen.

Alle aggregierten Incidents für einen Security Incident werden in der zugehörigen Liste „Aggregierte Azure Sentinel-Incidents“ angezeigt. Diese Liste enthält die zugehörigen Zeitstempel und aggregierten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum Incidents zu vorhandenen Security Incidents hinzugefügt werden.

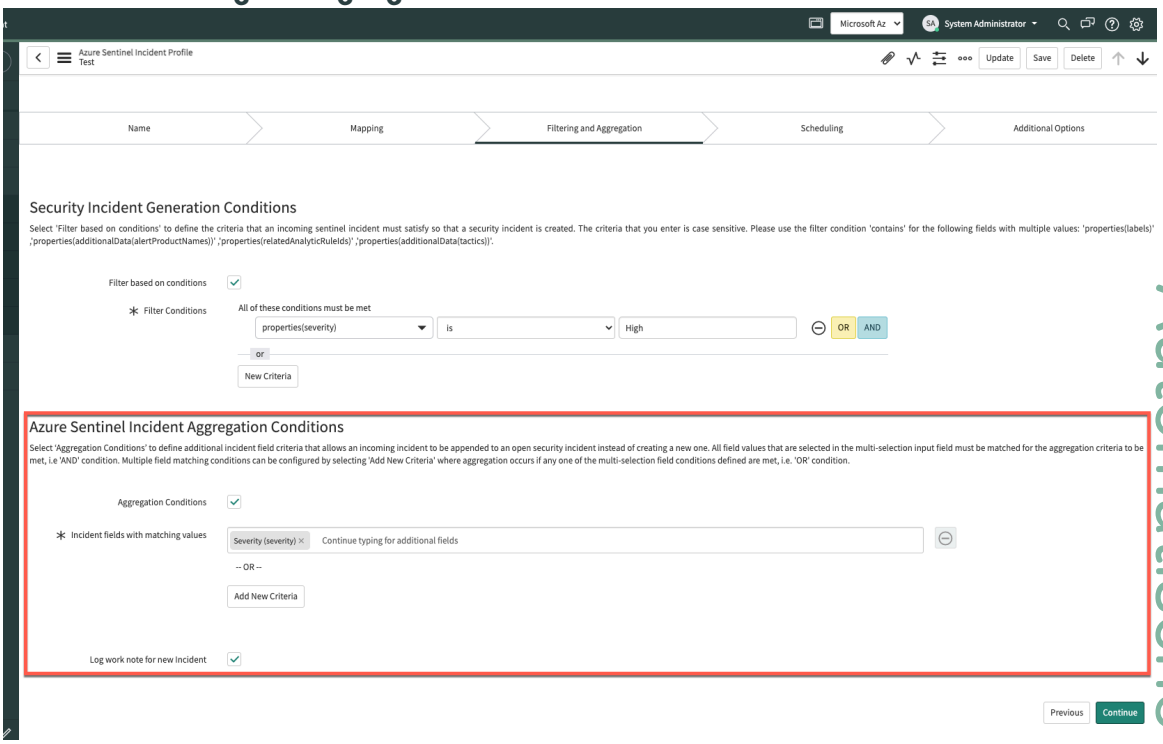
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um zusätzliche Incident-Feldkriterien zu definieren, die es ermöglichen, einen eingehenden Incident Microsoft Azure Sentinel an einen offenen Security Incident anzuhängen, anstatt einen neuen Incident zu erstellen, wählen Sie die Option **Zusammenfassungsbedingungen** (siehe folgende Abbildung).

Zusammenfassungsbedingungen



2. Geben Sie im Feld **Incident-Felder mit übereinstimmenden Werten** die Feldwerte ein, die mit vorhandenen Security Incidents in Ihrer Instanz Now Platform abgeglichen werden sollen.
   Alle Feldwerte, die Sie im Eingabefeld für die Mehrfachauswahl ausgewählt haben, müssen übereinstimmen, damit die Zusammenfassungskriterien erfüllt sind und dieser eingehende Incident an einen vorhandenen Security Incident angehängt werden kann. Diese Auswahl impliziert, dass es sich um eine *UND* -Bedingung handelt, bei der Felder wie erkennbare Elemente und Konfigurationselemente, die mehrere Feldwerte aufweisen können, zugeordnet werden. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Zusammenfassung des Azure Sentinel-Incident nicht erfüllt, und es wird ein neuer Security Incident erstellt.
3. Um mehrere Feldabgleichbedingungen hinzuzufügen, klicken Sie auf **Neues Kriterium hinzufügen**
   Die Zusammenfassung erfolgt, wenn eine der von Ihnen definierten Feldbedingungen für die Mehrfachauswahl erfüllt ist. Diese Auswahl impliziert die *ODER* -Bedingung.
4. Um die Arbeitsnotiz für einen neuen Incident zu aktualisieren, wenn sie einem Security Incident hinzugefügt wird, wählen Sie **Arbeitsnotiz für neuen Incident protokollieren**aus.

   In der Arbeitsnotiz wird protokolliert, dass ein neuer Incident hinzugefügt wurde, und sie enthält einen Link zu den Incident-Details. Die Protokoll-Arbeitsnotiz aktualisiert auch weitere Details, die Sie dem Feld „Arbeitsnotiz“ in Ihrem Zuordnungsabschnitt hinzufügen.
5. Klicken Sie zum Konfigurieren des Zeitplans **auf Fortfahren**.

Nächste Maßnahme

Legen Sie einen Zeitplan fest, um die Incident-Daten und erfassten Incidents abzurufen, die den Kriterien im Profil entsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Planen Sie den Abruf des incident Microsoft Azure Sentinel

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und die Microsoft Azure Sentinel Incidents zu erfassen, die den Kriterien im Profil entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_sni.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft Sie zukünftige Microsoft Azure Sentinel Incidents abfragen möchten, die der Incident-Profilkonfiguration entsprechen.

Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung zu definieren, aktivieren Sie **Zeit für Incident-Erfassung festlegen**. Die nachfolgende Erfassung basiert auf dem Zeitraum des Abfrageintervalls.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die unterschiedlichen Abfrageintervalle können sich auf die Leistung der Incident-Integration Microsoft Azure Sentinel auswirken. Planen Sie bei der Zeitplanung, die Systemlast gegen die Dringlichkeit eines incident abzuwägen. Für alle Profile ist ein Standardwert von einer Minute festgelegt. Sie können diese Einstellung je nach Dringlichkeit des incident und der erwarteten Auslastung Ihres Systems ändern.

Für alle Warnungen, die dem Incident in einem bestimmten Abfrageintervall hinzugefügt werden, wird ein Prozess ausgeführt und dann an die zugehörigen Listen der Azure Sentinel-Warnungen angehängt. Außerdem wird eine Arbeitsnotiz veröffentlicht.

Prozedur

1. Füllen Sie die Felder im Formular „Zeitplanung“ aus.

   Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus dem Mandanten Microsoft Azure abrufen.

   Formular „Zeitplanung“.

Feld	Beschreibung
Fortlaufende Incident-Erfassung	Fortlaufende Incident-Erfassung, bei der die Instanz Now Platform vom Mandanten Microsoft Azure für neue Incidents abruft. Security Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung erfüllt sind.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist.
Incident-Erfassungszeit festlegen	Incident-Erfassung, die auf dem konfigurierten Datum und der konfigurierten Uhrzeit basiert. Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Zeitraum des Abfrageintervalls.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Eingabe Incident-Erfassungszeit	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Einmaliger Abruf	Aktivieren Sie dieses Kontrollkästchen, um den einmaligen Abruf historischer Azure Sentinel-Incidents zuzulassen und dann den Abgleich der Daten durchzuführen. Wenn Sie dieses Kontrollkästchen aktivieren, ruft die Anwendung alle offenen und geschlossenen Azure Sentinel-Incidents für den Zeitraum bis zu etwa 6 Monaten ab. Bei der Verarbeitung der Daten werden sowohl laufende Incidents als auch Verlaufsdaten abgerufen, aber die Verarbeitung der laufenden Incidents hat Vorrang vor dem Verlaufsabruf. Andernfalls kann der Verlaufsabruf je nach Dauer und Anzahl der erfassten Incidents einige Zeit in Anspruch nehmen . **Hinweis:** Die abgerufenen historischen Azure Sentinel-Incidents werden Deduplizierungsprüfungen unterzogen, um Duplikate in der Anwendung Security Incident Response zu verhindern.
Seit Datum	Das Datum, seit dem die historischen Incidents aus Azure Sentinel erfasst wurden. **Hinweis:** Die Incident-Daten werden ungefähr aus den letzten 6 Monaten abgerufen.

Auf der Seite „Zeitplanung“ können Sie definieren, wie und wann Incidents aus dem Mandanten Microsoft Azure abgerufen werden.

2. Um zur Seite „Weitere Optionen“ zu navigieren, klicken Sie auf **Fortfahren**.

Automatisieren Sie die Aktualisierungen und Abschlüsse von Incidents anhand des Incident-Status SIR .

Automatisieren Sie die Aktualisierungen und Abschlüsse von Incidents anhand des Incident-Status SIR. Die Microsoft Azure Sentinel -Integration verfügt über eine bidirektionale Schnittstelle, über die sowohl Incidents Security Incidents erstellen als auch Incidents aktualisiert werden, nachdem der Security Incident erstellt oder geschlossen wurde.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Tragen Sie die Details in das Formular ein.
   Befolgen Sie die Anweisungen zum Abschließen der Konfiguration für die Aktualisierung von Incidents, wenn Sie in SIReinen Security Incident erstellen oder schließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Automatisieren von Incident-Updates“.

Kategorie	Feld	Beschreibung
Aktualisierungen der Incident-Erstellung	Aktualisiert den Status von Azure Sentinel-Incidents bei der Erstellung des SIR-Incidents	Mit dieser Option können Sie die Funktion zur automatisierten Aktualisierung von Incidents verwenden. Der Incident-Status Microsoft Azure Sentinel wird in Incident Microsoft Azure mit den Kommentaren aktualisiert, nachdem der Incident SIR in Now Platformerstellt wurde.
	Anfangsstatusaktualisierung für Incident	Anfänglicher Incident-Status, der in der Umgebung Microsoft Azure Sentinel aktualisiert wird. Sie können **Neu** oder **Aktiv** als Status auswählen.
	Anfangskommentare, die an den Incident zurückgesendet werden	Anfangskommentare, die zum Incident in der Umgebung Microsoft Azure Sentinel veröffentlicht werden. Bearbeiten Sie den Standardtext, der im Kommentarbereich angezeigt wird, indem Sie die Ersetzungsvariablen im Format ${Feldname}$ für ein beliebiges Feld im Incident-Formular SIR hinzufügen oder ändern.
Updates zum Incident-Abschluss	Schließt Azure Sentinel-Incidents bei Abschluss des SIR-Incidents	Option, mit der Sie die automatisierte Funktion zum Aktualisieren des Incident-Status verwenden können. Microsoft Azure Sentinel Incidents werden im Incident Microsoft Azure geschlossen, wobei die Kommentare nach dem Schließen des incident SIR in Now Platformangegeben werden.
	Statusaktualisierung für Abschluss-Incident	Statusaktualisierung im Incident Microsoft Azure Sentinel, wenn der Incident in SIRgeschlossen wird.
	Abschlusskommentare, die an den Incident zurückgesendet werden	Kommentare, die für den Incident im Incident Microsoft Azure Sentinel veröffentlicht werden, wenn der Incident in SIRgeschlossen wird. Bearbeiten Sie den Standardtext, der im Kommentarbereich angezeigt wird, indem Sie die Ersetzungsvariablen im Format ${Feldname}$ für ein beliebiges Feld im Incident-Formular SIR hinzufügen oder ändern.
	Incident-Klassifizierung und Abschlussgrund	Methode für die Incident-Klassifizierung und den Abschlussgrund, die zum

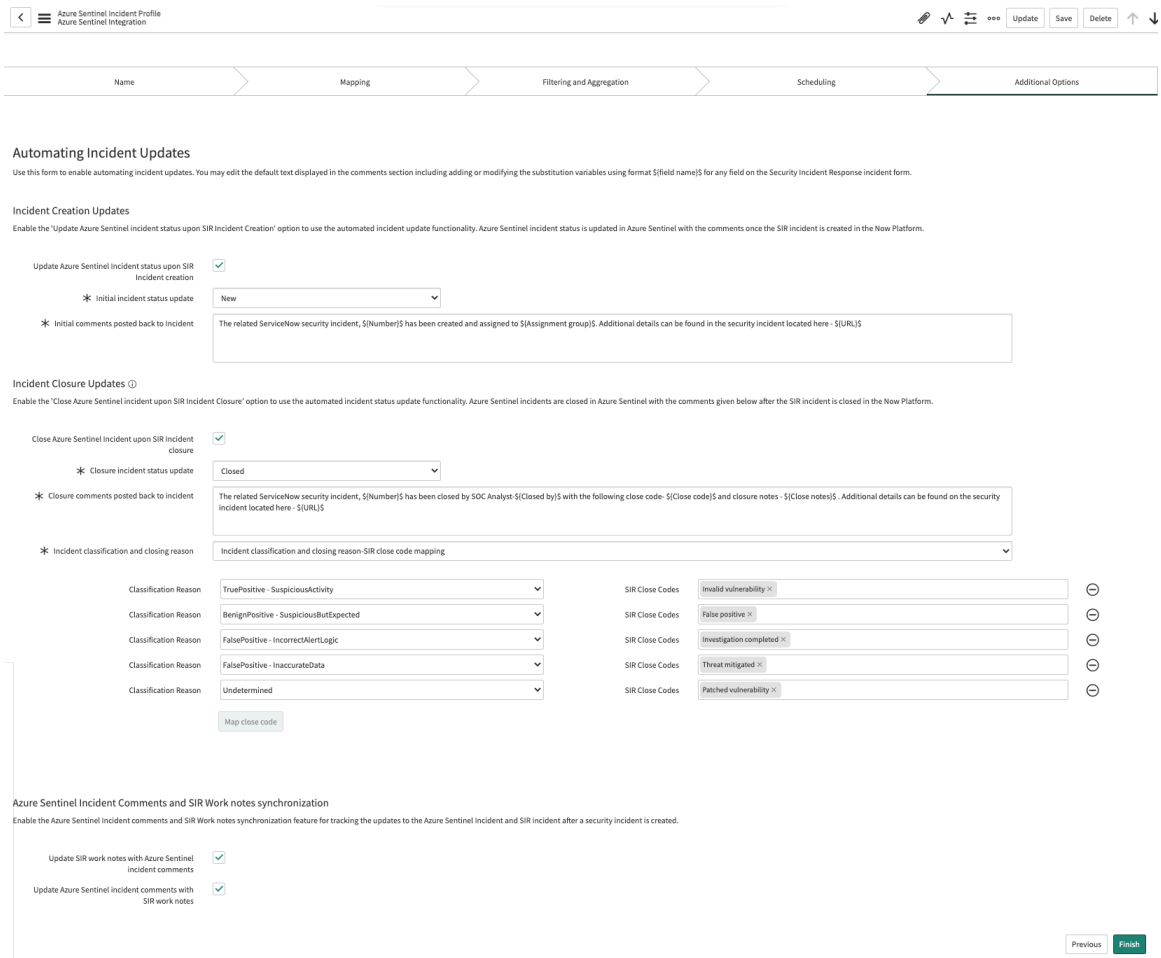
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Feld	Beschreibung
		Schließen des Incidents in der Umgebung Microsoft Azure Sentinel verwendet wird. Wählen Sie die Methode **Standard für Incident-Klassifizierung und Abschlussgrund** aus, um den Incident in der Umgebung Microsoft Azure Sentinel zu schließen. Wenn Sie diese Methode auswählen, müssen Sie die **standardmäßige Incident-Klassifizierung und den Abschlussgrund**definieren. Wenn Sie einen Incident in SIR schließen, wird auch der Incident-Status in Azure Sentinel mit der angegebenen **Standard-Incident-Klassifizierung und dem Abschlussgrund**geschlossen. Wählen Sie die Zuordnungsmethode **Incident-Klassifizierung und Abschlussgrund – SIR-Abschlusscode** aus, um die Incidents zu schließen und die Klassifizierungsgründe den Abschlusscodes SIR zuzuordnen. Sie können einem einzigen Klassifizierungsgrund mehrere SIR Lösungscodes zuordnen. Nachdem Sie einen Incident in SIR mit dem Abschlusscode geschlossen haben, wird der Incident-Status in Azure Sentinel auch mit der zugeordneten Incident-Klassifizierung und dem Abschlussgrund geschlossen. Wenn der Klassifizierungsgrund und SIR die Abschlusscodes nicht zugeordnet sind oder keine Übereinstimmung gefunden wird, wird der Incident mit dem standardmäßigen Klassifizierungsgrund als „Unbestimmt“ in der Umgebung Microsoft Azure Sentinel geschlossen.
Synchronisierung von Azure Sentinel-Incident-Kommentaren und SIR-Arbeitsnotizen	SIR-Arbeitsnotizen mit Azure Sentinel-Incident-Kommentaren aktualisieren	Option, die Sie auswählen können, um Ihre Microsoft Azure Sentinel -Kommentare in den SIR -Arbeitsnotizen zu aktualisieren. Der Kommentar in den Arbeitsnotizen SIR wird mit dem Präfix `Kommentar von`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Feld	Beschreibung
		*Sentinel*angezeigt. Der Kommentar enthält auch die Sentinel-ID, Details zum Analysten und den Zeitstempel.
	Azure Sentinel-Incident-Kommentare mit SIR-Arbeitsnotizen aktualisieren	Option, die Sie auswählen können, um Ihre SIR -Arbeitsnotizen in den Microsoft Azure Sentinel -Incident-Kommentaren zu aktualisieren. Der Kommentar in Microsoft Azure Sentinel wird mit dem Präfix *Kommentar von ServiceNow*angezeigt.

Das folgende Beispiel zeigt die Konfigurationsoptionen, die für die Automatisierung der Incident-Aktualisierung verfügbar sind.



2. Klicken Sie auf **Fertigstellen**.

Nächste Maßnahme

Das Profil wechselt in den Status Warten. Wenn in der Bestätigungsmeldung angezeigt wird, dass das Setup und die Konfiguration abgeschlossen sind, können Sie das Profil aktivieren.

Kopieren Sie ein Microsoft Azure Sentinel -Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt ein Profil zu erstellen. Wenn Sie mehrere Profile erstellen, können Sie die Einstellungen eines vorhandenen Profils wiederverwenden, indem Sie diese Profile kopieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

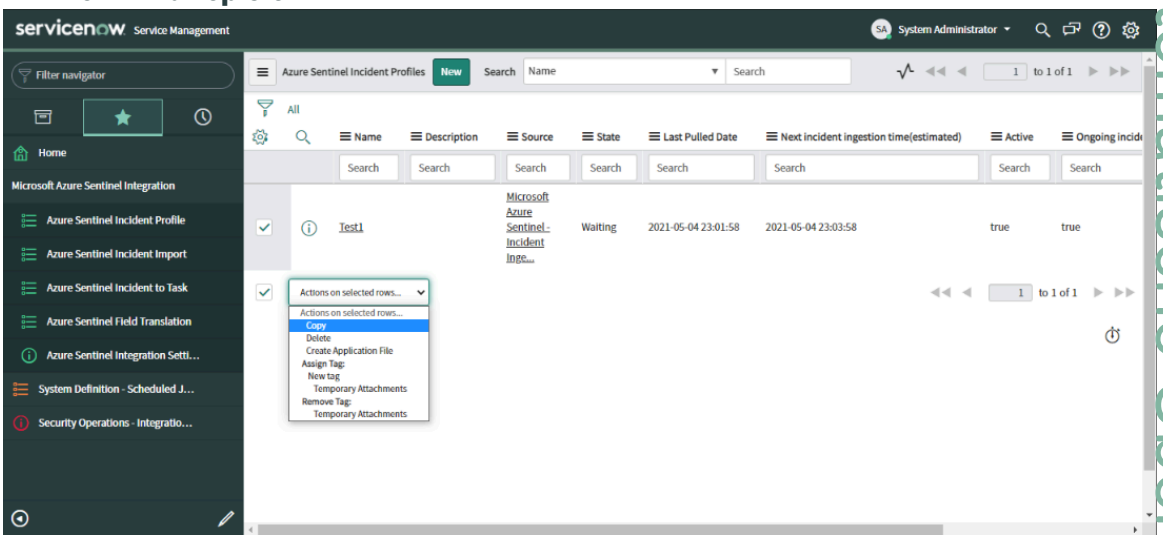
Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie ein Profil kopieren, wird der Profilname zunächst geändert, um zu vermeiden, dass doppelte Profile erstellt werden. Das kopierte Profil ist ebenfalls deaktiviert (auf „falsch“ festgelegt), um sicherzustellen, dass Sie es nicht versehentlich aktivieren, bevor Sie die Konfiguration abgeschlossen haben. Sie können die Profile kopieren und vorhandene Zuordnungen für Security Incidents verwenden, die Sie bereits in der Vorschau angezeigt und überprüft haben.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Profil**.
2. Wählen Sie in der Liste Azure Sentinel-Profile ein Profil aus, das Sie kopieren möchten, und klicken Sie dann in der Liste Aktionen für ausgewählte Zeilen auf **Kopieren**, wie im folgenden Beispiel gezeigt.

Ein Profil wird kopiert

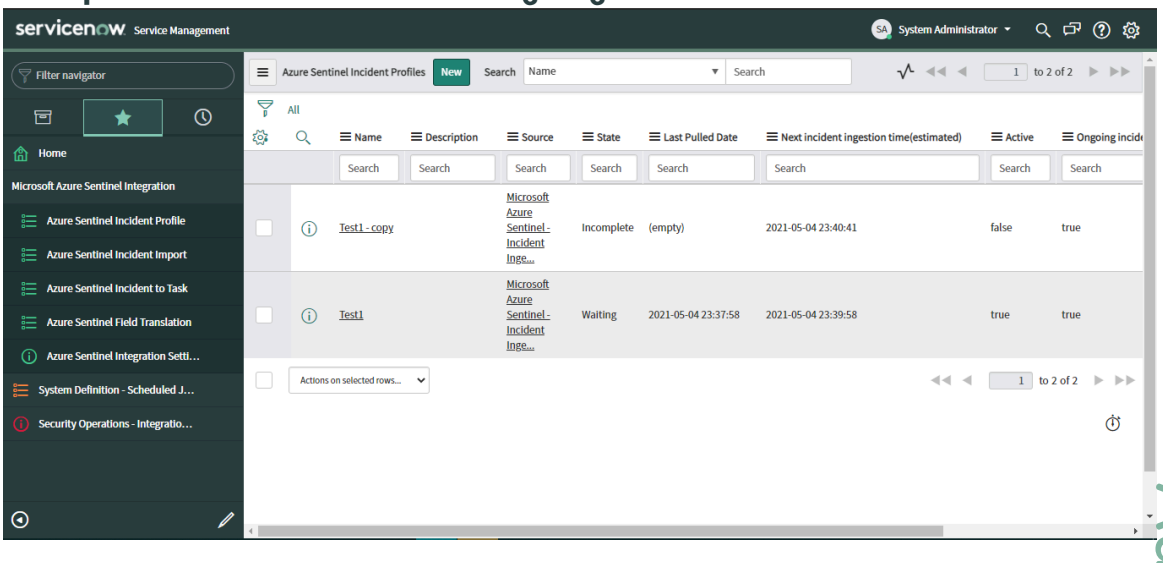


Das Profil wird kopiert und in der Liste angezeigt (siehe folgendes Beispiel). Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Zeitplankonfiguration. Der Name des Profils enthält das Wort „Kopie“. Obwohl das ursprüngliche Profil aktiviert ist (wahr), wird die Kopie an dieser Stelle deaktiviert (falsch). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die kopierten Incident-Profile werden angezeigt



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Der Spaltenstatus „Aktiv“ ist auf „falsch“ festgelegt. Dies bedeutet, dass das Profil aktiviert sein muss.

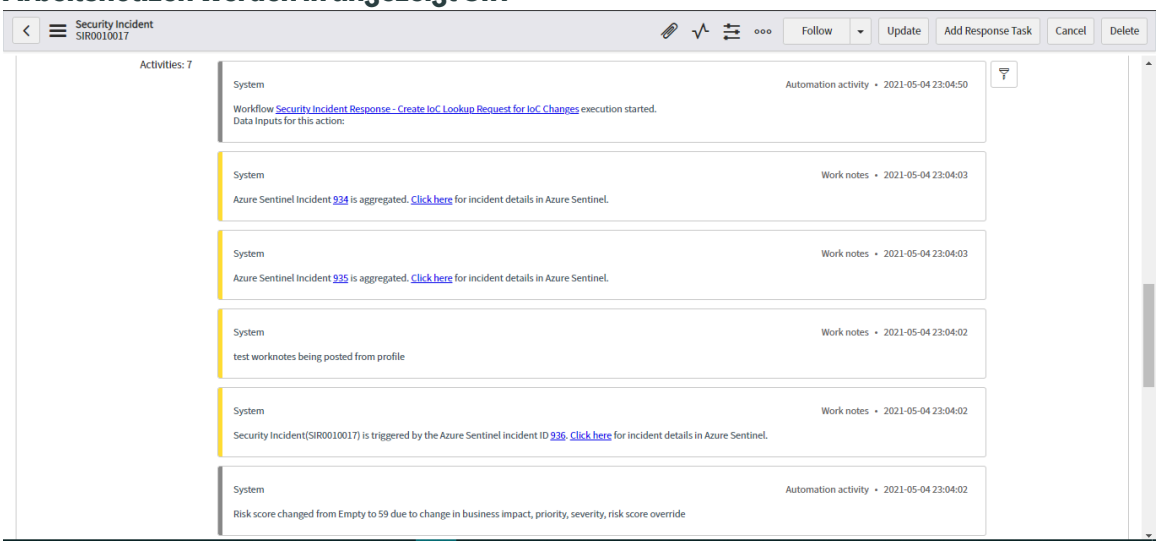
SIR Formular nach einer Incident-Erfassung

Nachdem Now Platform den Incident Microsoft Azure Sentinel erfasst hat, wird ein Security Incident erstellt, und die Aktualisierungen werden an diesem Security Incident-Datensatz vorgenommen.

Arbeitsnotizen

Eine Arbeitsnotiz wird veröffentlicht, wenn ein Incident aggregiert wird und wenn Sie die Option **Arbeitsnotiz für neuen Incident protokollieren** in den Kriterien für die Incident-Zusammenfassungkonfiguriert haben. Das folgende Beispiel zeigt die Arbeitsnotizen in SIR.

Arbeitsnotizen werden in angezeigt SIR



Wenn Sie auf die Incident-Nummer klicken, können Sie den Datensatz für den internen Incident-Import anzeigen, der die Rohdaten zum Incident enthält. Das folgende Beispiel zeigt die Rohdaten zu Incidents in SIR.

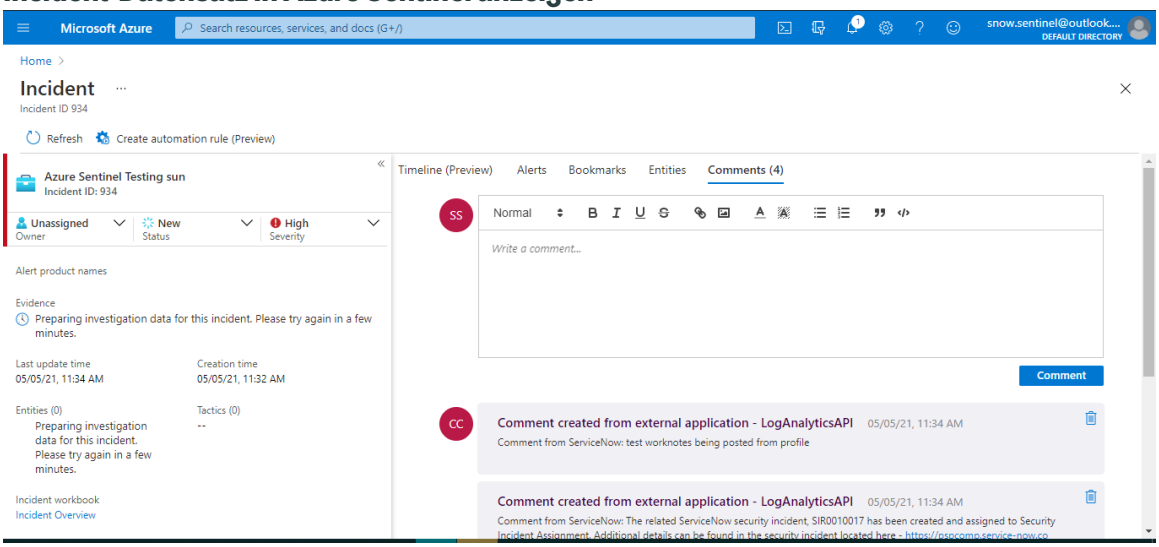
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incident-Rohdaten werden in angezeigt SIR

Wenn Sie auf den Link **Hier klicken** klicken, können Sie den Datensatz in der Umgebung Microsoft Azure Sentinel anzeigen. Das folgende Beispiel zeigt den Datensatz in der Umgebung Microsoft Azure Sentinel.

Incident-Datensatz in Azure Sentinel anzeigen

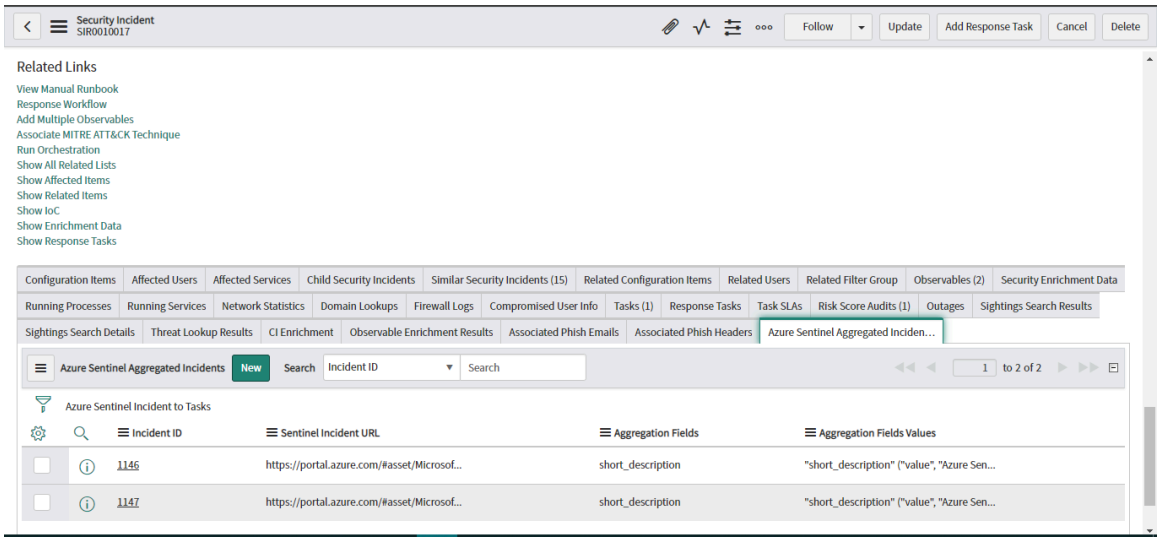


Aggregierte Sentinel Incidents

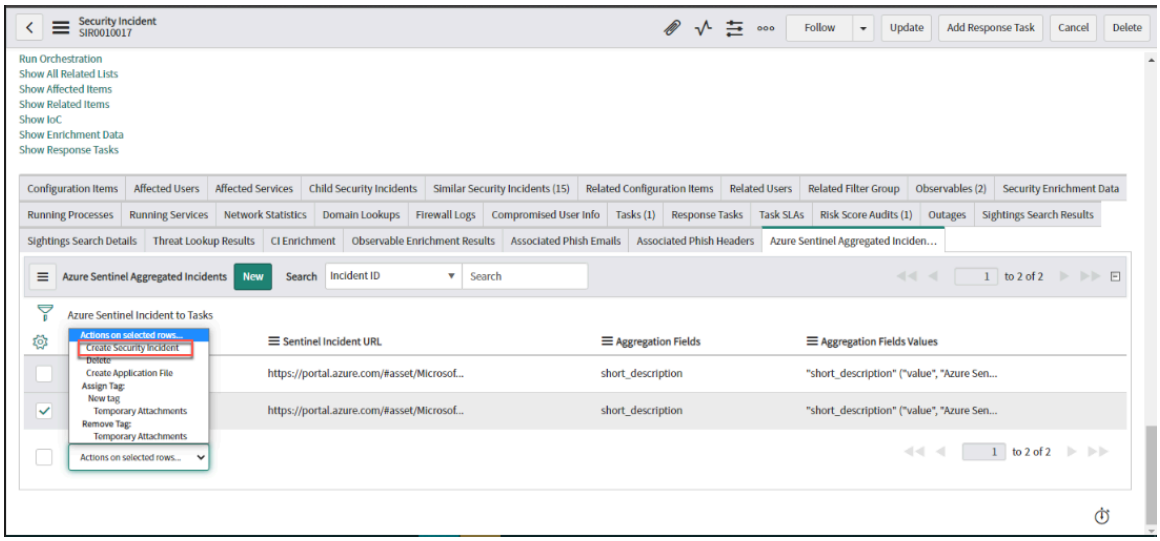
Aggregierte Sentinel-Incidents anzeigen: Zeigen Sie die Incidents an, die zum Security Incident aggregiert wurden. Navigieren zu **Alle zugehörigen Listen anzeigen** > **Aggregierte Microsoft Azure Sentinel-Incidents**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Security Incident erstellen: Wählen Sie einen Incident aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie dann auf **Security Incident erstellen**. Durch diese Option wird ein neuer Security Incident für den Incident erstellt. Dieser Incident wird aus dem übergeordneten Security Incident deaggregatiert.

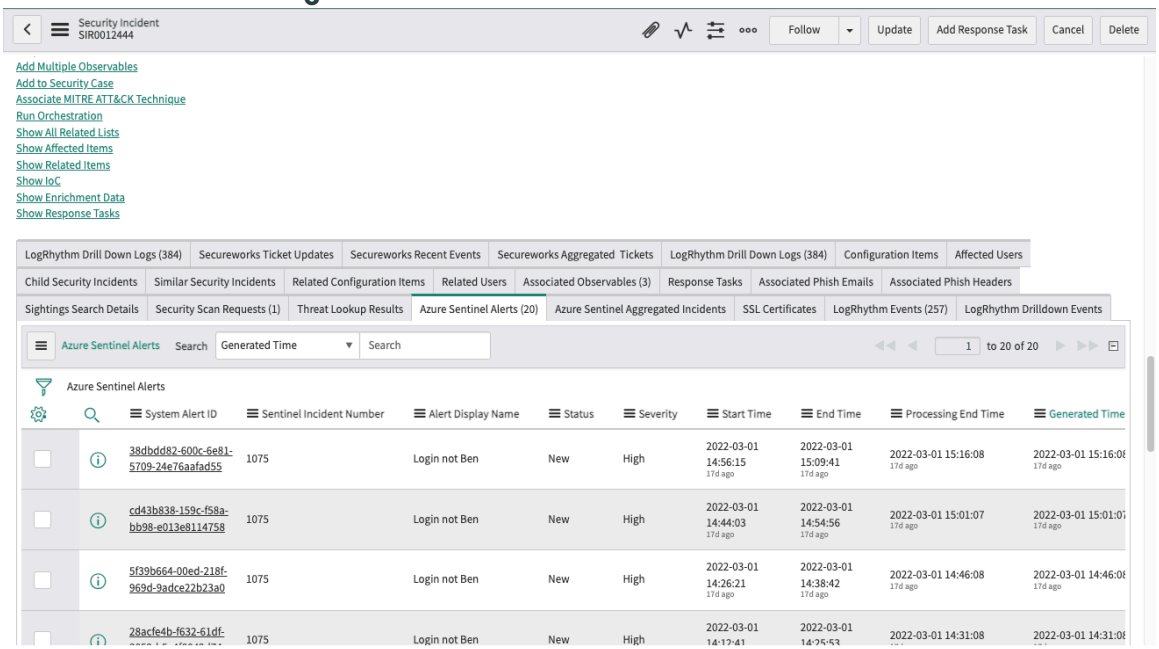


Azure Sentinel-Warnungen

Um die Warnungen anzuzeigen, die dem Sentinel Incident zugeordnet sind, der den Security Incident ausgelöst hat, navigieren Sie zu **Alle zugehörigen Listen anzeigen** > **Azure Sentinel-Warnungen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Sentinel-Warnungen



Überprüfen Sie die Integrationseinstellungen für Microsoft Azure Sentinel .

Überprüfen Sie die Integrationseinstellungen Microsoft Azure Sentinel für [], damit Sie die Systemeigenschaften an Ihre Umgebung anpassen können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Integration: Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

Microsoft Azure Sentinel Integrationseinstellungen

Eigenschaftsname	Beschreibung
Erzwingt einen Grenzwert für die Anzahl der Tage, für die Beispieldaten abgerufen werden können. sn_sec_sentinel.max_num_of_days_for_sample_data	Maximale Anzahl von Tagen, für die Sie Beispieldaten aus der Umgebung Microsoft Azure Sentinel abrufen können. Typ: Ganzzahl Standardwert: 7
Erhalten Sie Updates zu neuen Warnungen, die mit SIR verknüpft sind. sn_sec_sentinel.incident_updates	Aktivieren Sie die Option, um Incident-Updates zu erhalten. Typ: Boolesch Standardwert: True
Das Trennzeichen zum Teilen der Werte in Feldzuordnungen Microsoft Azure Sentinel	Das Trennzeichen zum Teilen der Werte in Feldzuordnungen Microsoft Azure Sentinel

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung
sn_sec_sentinel.delimiter	Typ: Zeichenfolge Standardwert: ', ' (Komma mit Leerzeichen)
Erzwingt einen Grenzwert für die Anzahl der Beispiel-Incidents, die abgerufen werden können. sn_sec_sentinel.max_num_of_sample_incidents_per_call	Maximale Anzahl von Beispiel-Incidents, die Sie zur Erfassung aus der Umgebung Microsoft Azure Sentinel abrufen. Typ: Ganzzahl Standardwert: 5 Maximaler Stichprobenwert: 20
Erzwingt einen Grenzwert für die Anzahl von Sentinel-Incidents, die zu einem einzelnen Incident zusammengefasst werden können. sn_sec_sentinel.max_aggregations_per_si	Grenzwert für die Incident-Zusammenfassung für einen Security Incident. Wenn beispielsweise 102 Incidents vorhanden sind, werden die ersten 100 zu Security Incident_1 und die verbleibenden 2 zu Security Incident_2 zusammengefasst. Typ: Ganzzahl Standardwert: 100
Erzwingt einen Grenzwert für die Anzahl von Security Incidents, die innerhalb von 24 Stunden erstellt werden können. sn_sec_sentinel.max_si_per_day	Maximale Anzahl der Security Incidents, die innerhalb von 24 Stunden im Now Platformerstellt werden können. Typ: Ganzzahl Standardwert: 1000
Maximaler Paginierungsgrenzwert für das Abrufen der Incident-Daten in einem REST-Aufruf. sn_sec_sentinel.max_page_size	Paginierungsgrenze für das Abrufen der Incident-Daten in einem REST-Aufruf aus der Umgebung Microsoft Azure Sentinel. Typ: Ganzzahl Standardwert: 100
API-Versionswert für Incidents. sn_sec_sentinel.sentinel_security_incident_api_version	Die Microsoft API-Version zum Abrufen von Sentinel-Incidents. Standardwert: 01.10.2021
API-Versionswert für Warnungen. sn_sec_sentinel.sentinel_security_alert_api_version	Die Microsoft API-Version zum Abrufen von Sentinel-Warnungen. Standardwert: 01.10.2021
API-Versionswert für Entitäten. sn_sec_sentinel.sentinel_security_entities_api_version	Die Microsoft API-Version zum Abrufen von Sentinel-Entitäten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung
	Standardwert: 01.10.2021
sn_sec_sentinel.ging.verbosity	Die Protokollausführlichkeitsstufe der Anwendung, d. h. den Namen des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **Fehler** ○ **warnen** ○ **Info** ○ **debuggen** Standardwert: **info**.

3. Klicken Sie auf **Speichern**.
   Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Domain Separation und die Microsoft Azure Sentinel -Integration

Domänentrennung wird für diese Anwendung unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Funktionsweise der Domänentrennung in der Microsoft Azure Sentinel -Integration

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie in der entsprechenden Domäne einen Benutzer mit der Rolle sn_si.admin.

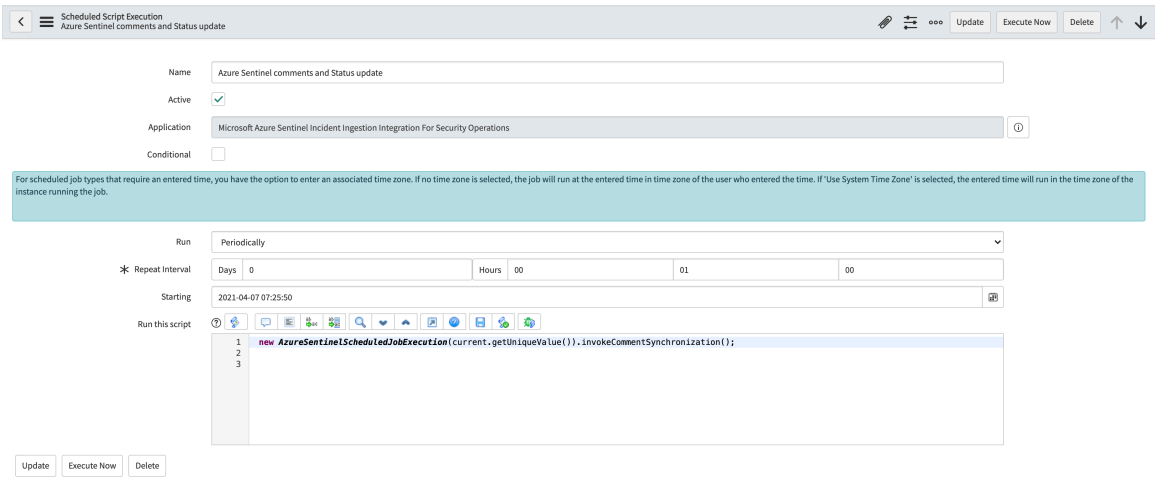
  Hinweis:
  Verwenden Sie beim Erstellen des Profils die Domänenauswahl, um eine Domäne auszuwählen. Erstellen Sie den Benutzer nicht in der übergeordneten Domäne, und ändern Sie später die Domäne des Profils. Sie müssen für jede Domäne einen Benutzer für Ihr Profil mit der Rolle sn_si.admin haben. Verwenden Sie diesen Anwender, um Einstellungen im Profil zu erstellen oder zu ändern.

- Deaktivieren Sie vorhandene geplante Aufgaben.
- Replizieren Sie die folgenden geplanten Aufgaben für jede Domäne:
  - Azure Sentinel – Warnungen und Entitäten werden abgerufen
  - Synchronisierung von Azure Sentinel-Kommentaren
  - Azure Sentinel-Statusaktualisierung
  - Azure Sentinel – Profilprozess
  - Azure Sentinel – Prozessrohdaten
  - Azure Sentinel-Datenbereinigung
  - Historischer Kommentarabruf von Azure Sentinel

  Hinweis:
  Nachdem Sie die geplanten Aufgaben repliziert haben, verwenden Sie den Navigator, und suchen Sie nach dem Modul „Modulzugriffsrichtlinien“, um die kürzlich erstellten Datensätze anzuzeigen, in deren **Zielskript** die neu erstellten geplanten Aufgaben angezeigt werden. Ändern Sie den Feldwert **Ergebnis** in **Nachverfolgen**.

- Ändern Sie **Ausführen als** vom Systembenutzer in den Benutzer mit der Rolle sn_si.admin in der entsprechenden Domäne, und führen Sie dann die geplante Aufgabe aus.

Das folgende Beispiel zeigt, wie Sie den Auftrag zur Azure Sentinel-Kommentare und Statusaktualisierung replizieren und als Systembenutzer ausführen.



Zugehörige Informationen

Domänentrennung für Service Provider

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der Integrationen Microsoft Azure Sentinel und Microsoft Graph-Sicherheits-API mit SIR

Sie können die Unterschiede zwischen den Integrationen Microsoft Azure Sentinel und Microsoft Graph-Sicherheits-API anzeigen und die richtige Integration mit Ihrer Instanz Now Platform von auswählen.

Microsoft Azure Sentinel – Incident Ingestion – Übersicht

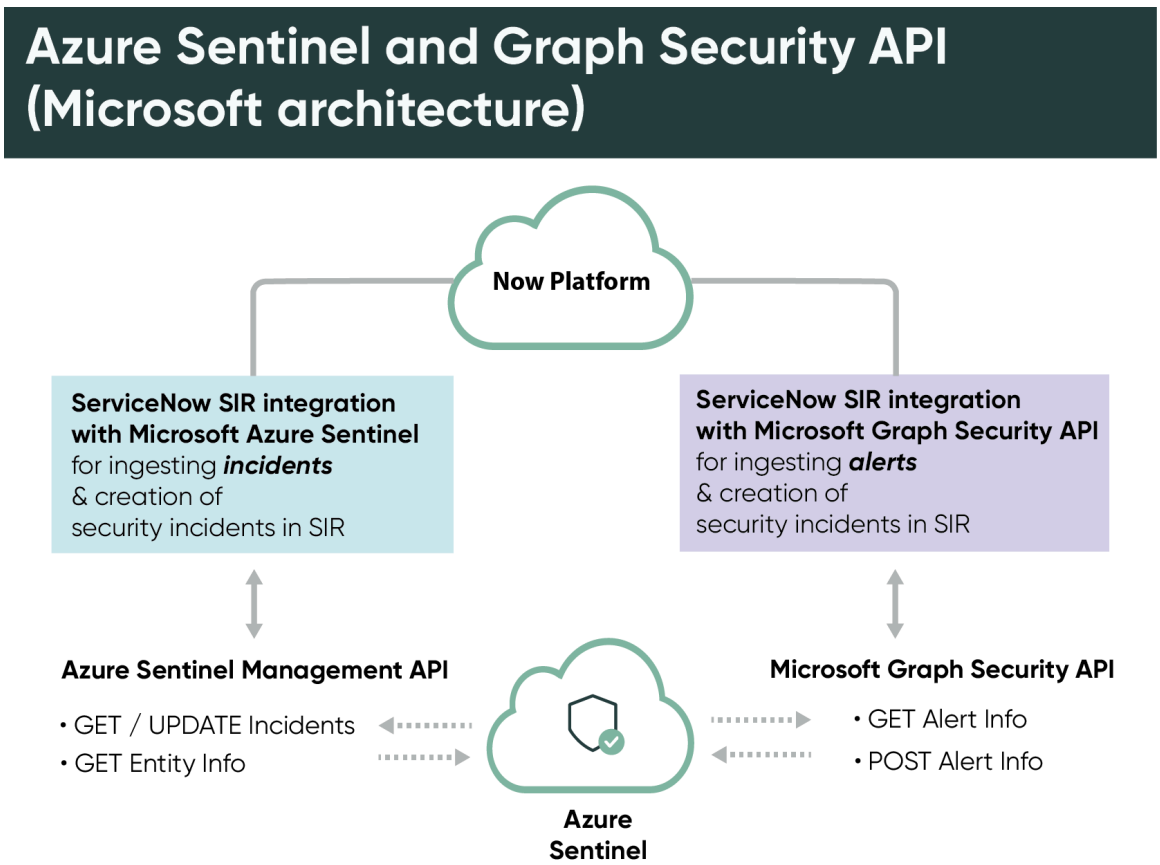
Microsoft Azure Sentinel ist eine cloudbasierte Lösung für Security Information Event Management (SIEM) und Security Orchestration Automated Response (SOAR). Microsoft Azure Sentinel bietet intelligente Sicherheitsanalysen und Threat Intelligence für das gesamte Unternehmen. Sie bietet eine einzige Lösung für Warnungserkennung, Bedrohungstransparenz, proaktive Suche und Reaktion auf Bedrohungen.

Microsoft Graph-Sicherheits-API – Übersicht

Microsoft Graph-Sicherheits-API ist ein intermediärer Service (oder Broker), der eine einzige programmgesteuerte Schnittstelle für die Verbindung mehrerer Sicherheitsanbieter (native zu Microsoft sowie ServiceNow Partner) bereitstellt.

Die Microsoft Graph-Sicherheits-API -Integration behebt diese Probleme, indem sie Microsoft Graph-Sicherheits-API verwendet, um eine Verbindung mit verschiedenen Microsoft-Sicherheitstechnologien wie Azure Sentinel, Microsoft Defender Advanced Threat Protection und Azure Advanced Threat Protection herzustellen. In Security Incident Responsewerden Warnungen von Microsoft-Sicherheitsanbietern erfasst, und Security Incidents werden automatisch erstellt.

Zusammenfassung der Funktionsunterschiede



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Azure Sentinel vs Microsoft Graph-Sicherheits-API

Microsoft Azure Sentinel	Microsoft Graph-Sicherheits-API
Erfasst Microsoft Azure Sentinel Incidents zusammen mit Entitätsinformationen (falls verfügbar) und automatisiert die Erstellung von Security Incidents in SIR.	Erfasst Warnungen von mehreren Sicherheitsanbietern (einschließlich Azure Sentinel) in einem Standardschema und automatisiert die Erstellung von Security Incidents in SIR.
Automatisiert Microsoft Azure Sentinel Incident-Statusaktualisierungen für Security Incident Response, sodass Sie Security Incidents erstellen und schließen können. **Hinweis:** ServiceNow aktualisiert den Status von Microsoft Azure Sentinel Incidents basierend auf der Erstellung oder dem Abschluss des Security Incidents.	Unterstützt Warnungsaktualisierungen (Änderung des Warnungsstatus und Warnungsabschluss) für ausgewählte Sicherheitsanbieter. **Hinweis:** Weitere Informationen zu den von Microsoft Graph-Sicherheits-API unterstützten Sicherheitsanbietern finden Sie in der Microsoft-Dokumentation .
Verwenden Sie diese Integration, wenn Ihr Szenario die folgenden Bedingungen enthält: • Die vorläufige Incident-Untersuchung befindet sich in Microsoft Azure Sentinel, die nachfolgende Untersuchung befindet sich in SIR. • Microsoft Azure Sentinel Incidents in SIRaufnehmen	Verwenden Sie diese Integration, wenn Ihr Szenario die folgenden Bedingungen enthält: • Führen Sie eine Incident-Untersuchung in SIRdurch. • Microsoft Azure Sentinel Warnungen in SIRerfassen. • In Microsoft Azure Sentinelwerden keine Incidents erstellt.
Warnung ist eine Entität in Microsoft Azure Sentinel. Mit der Management-API Microsoft Azure Sentinel können Sie keine eigenständigen oder spezifischen Warnungen abrufen. Sie können nur die Warnungsdaten abrufen, die einem Incident zugeordnet sind. Die mit dieser Integration verfügbaren Warnungsdaten sind umfangreicher als die mit Microsoft Graph-Sicherheits-APIverfügbaren Warnungsdaten.	Die normalisierten Warnungsdaten für Microsoft Azure Sentinel sind verfügbar. Die Warnungsfelder Microsoft Azure Sentinel, die intern in Microsoft Graph-Sicherheits-APIzugeordnet sind und in Microsoft Graph-Sicherheits-APIverfügbar sind, können in dieser Integration verwendet werden.
	Sie können mit dieser Integration keine Warnungen in Microsoft Azure Sentinel aktualisieren.

Microsoft Defender for Endpoint Integration

Mit Microsoft Defender for Endpoint können Sie bekannte und unbekannte Bedrohungen auf jedem Endpunkt proaktiv überprüfen, analysieren und eindämmen.

Die Microsoft Defender for Endpoint -Integration hilft Sicherheitsanalysten, Security Incidents effizient zu untersuchen und zu beheben, ohne zwischen Tools wechseln zu müssen.

Sie können diese Integration verwenden, um Konfigurationen zu erstellen, um Hostdetails, Details angemeldeter Benutzer, Details zu zugehörigen Computern und andere Ergänzungsfunktionen abzurufen. Sie können anfordern, jeden Computer vom Zugriff auf die Netzwerke zu isolieren oder die Computer aus der Isolation zu entfernen. Anforderungen können von den Genehmigern akzeptiert oder abgelehnt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Schlüsselfunktionen

Microsoft Defender for Endpoint besitzt die folgenden Schlüsselfunktionen:

- Führen Sie eine Enterprise Security-Suche durch, um potenziell schädliche erkennbare Elemente über Endpunkte hinweg zu erkennen und Gegenmaßnahmen zu ergreifen.
- Führen Sie Antwortaktionen aus, z. B. Host isolieren, Isolation entfernen, App-Ausführung einschränken, Antivirenprüfung ausführen, App-Einschränkung entfernen und Datei anhalten und unter Quarantäne stellen.
- Erstellen oder aktualisieren Sie Indikatoren.
- Führen Sie eine Anreicherung erkennbarer Elemente durch, und rufen Sie Daten im Zusammenhang mit Indikatoren ab.

Microsoft Defender for Endpoint

Untersuchen Erste Schritte mit Microsoft Defender für Endpunkt	**Installieren** Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration	**Konfigurieren** Konfigurieren Sie Profile und Security Incidents für Microsoft Defender für Endpunkt
Fähigkeitsprofil Erstellen Sie ein Fähigkeitsprofil für die Microsoft Defender für Endpunkt-Integration.	**Zusätzliche Konfigurationen** Zusätzliche Konfigurationen, die Sie in Microsoft Defender für Endpunkt durchführen können	**Verschiedenes** Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche und Indikatoren mit Microsoft Defender für Endpunkt.

Registrieren Sie, und konfigurieren Sie den Microsoft Defender for Endpoint im -Portal Microsoft Azure .

Registrieren Sie die Anwendung Microsoft Defender for Endpoint im Microsoft Azure-Portal, und gewähren Sie der Anwendung Lese- und Schreibzugriff.

Vorbereitungen
Erforderliche Rolle: Anwendungsentwickler, Mandantenadministrator.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich beim Microsoft Azure-Portal an.
2. Geben Sie im Suchfeld App-Registrierungen ein, und klicken Sie **auf Neue Registrierung**.
3. Geben Sie einen Namen für Ihre Anwendung und den Umleitungs-URI ein, und klicken Sie auf **Registrieren**.
   Ein Beispielname ist Microsoft Defender für Endpunkt. Der Umleitungs-URI wird verwendet, wenn die Administratoreinwilligung für die Anwendung erteilt wird.
4. Wählen Sie auf der Seite **App-Registrierungen** die Anwendung aus, die Sie in Schritt 3 registriert haben.
5. Wählen Sie unter Verwalten die Option **Zertifikate und Geheimnisse**aus.
6. Um einen geheimen Clientschlüssel zu erstellen, wählen Sie **Neuer geheimer Clientschlüssel**aus.
7. Kopieren Sie den geheimen Clientschlüssel, und speichern Sie ihn.

   Falls Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen geheimen Clientschlüssel generieren.
8. Navigieren zu **Verwalten** > **API-Berechtigungen**.
9. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
10. Klicken Sie im Fenster API-Berechtigungen anfordern auf die Registerkarte **Von meiner Organisation verwendete APIs**.
11. Suchen Sie nach **WindowsDefenderATP**, und wählen Sie den Eintrag aus.
12. Wählen Sie in den WindowsDefenderATP-Berechtigungen **Anwendungsberechtigungen**aus.
    Durch Aktivieren dieser Berechtigung wird sichergestellt, dass die Anwendung als Hintergrundservice oder Daemon ohne angemeldeten Benutzer ausgeführt wird.
13. Fügen Sie die folgenden Berechtigungen auf Anwendungsebene hinzu, und erteilen Sie die Administratorzustimmung für die neu hinzugefügten API-Berechtigungen.

Berechtigung	Anzeigename der Berechtigung
Machine.Read.All	Alle Rechnerprofile lesen
Benutzer.Lesen.Alle	Anwenderprofile zum Lesen
Rechner.Isolieren	Computer isolieren
Rechner.AusführungEinschränken	Beschränken Sie die Codeausführung
Machine.Scan	Computer scannen
Rechner.StoppUndQuarantäne	Anhalten und unter Quarantäne stellen
URL.Lesen.Alle	URLs lesen
Datei.Lesen.Alle	Dateiprofile lesen
Ip.Lesen.Alle	IP-Adressprofile lesen
Ti.LesenSchreiben.Alle	Indikatoren mit Lese- und Schreibzugriff

Erste Schritte mit der Microsoft Defender for Endpoint -Integration

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung Microsoft Defender for Endpoint aus dem ServiceNow Store installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Sehen Sie sich die folgende Tabelle an, und vergewissern Sie sich, dass Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen für Now Platform und Security Incident Response (SIR) zugewiesen haben.	Die folgenden Rollen sind erforderlich: **1.** Sie müssen die Rolle eines Systemadministrators (admin) innehaben, um die Anwendung für die Integration zu installieren. **2.** Um die Integration zu konfigurieren sowie Profile zu erstellen, zu aktivieren und zu entfernen, müssen Sie über die Rolle „Security Incident-Administrator“ (sn_si.admin) verfügen. **3.** Um mit Security Incidents arbeiten zu können, benötigen Sie die Rolle „Security Incident Analyst“ (sn_si.analyst). Ein Benutzer mit dieser Rolle kann alle in der Integration verfügbaren Fähigkeiten initiieren.
Stellen Sie sicher, dass die ServiceNow Core-Anwendungen, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung installieren.	Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie sie einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation zu gewährleisten: **1.** Security Incident Response **2.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **3.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Bevor Sie die Genehmigungsoption für Profile aktivieren, vergewissern Sie sich, dass Sie eine Genehmigungsgruppe erstellt haben.	Ein optionaler Genehmigungsworkflow ist verfügbar, um Hostcomputer zu isolieren, sie wieder in das Netzwerk zu integrieren und zusätzliche Aktionen für den Endpunkt auszuführen. Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünscht, aktivieren Sie bei der Konfiguration der Profile die Option Genehmigung erforderlich. In einem Szenario, in dem das Profil verfügbar ist, hat die Profilkonfiguration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	für die Genehmigung Vorrang. In einem Szenario, in dem das Profil nicht verfügbar ist, werden die Genehmigungen basierend auf den Standardeinstellungen behandelt. Als Sicherheitsadministrator können Sie Genehmigungen einrichten, während Sie die Profile und Standardeinstellungen konfigurieren. Eine Genehmigungsgruppe muss in der Gruppenliste in Ihrer Instanz verfügbar sein. Zur Überwachung und Verarbeitung von Anforderungen, die von Benutzern mit der Rolle sn_si.analyst übermittelt wurden, müssen alle Mitglieder der Genehmigungsgruppe zu Meine Genehmigungen in Now Platform®navigieren. Alternativ finden Genehmiger die Anforderungen, die ausschließlich für die Integration Microsoft Defender for Endpoint übermittelt wurden, im Modul Approvals (Genehmigungen). Weitere Informationen zum Erstellen von -Benutzergruppen finden Sie unter Benutzergruppen erstellen .

Nächste Maßnahme

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration Microsoft Defender for Endpoint eingerichtet. Der nächste Schritt besteht in der Installation der Anwendung Microsoft Defender for Endpoint aus dem ServiceNow Store für die Integration.

Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration

Installieren und konfigurieren Sie die Microsoft Defender for Endpoint -Integration von ServiceNow Store in Ihrer Instanz Now Platform von . Beginnen Sie mit der Erstellung von Fähigkeitsprofilen mithilfe von -Konfigurationen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie die Microsoft Defender für Endpunkt-Integration von ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel Microsoft Defender für Endpunkt, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die folgenden Felder des Formulars aus.

Konfigurieren Sie Microsoft Defender für Endpunkt

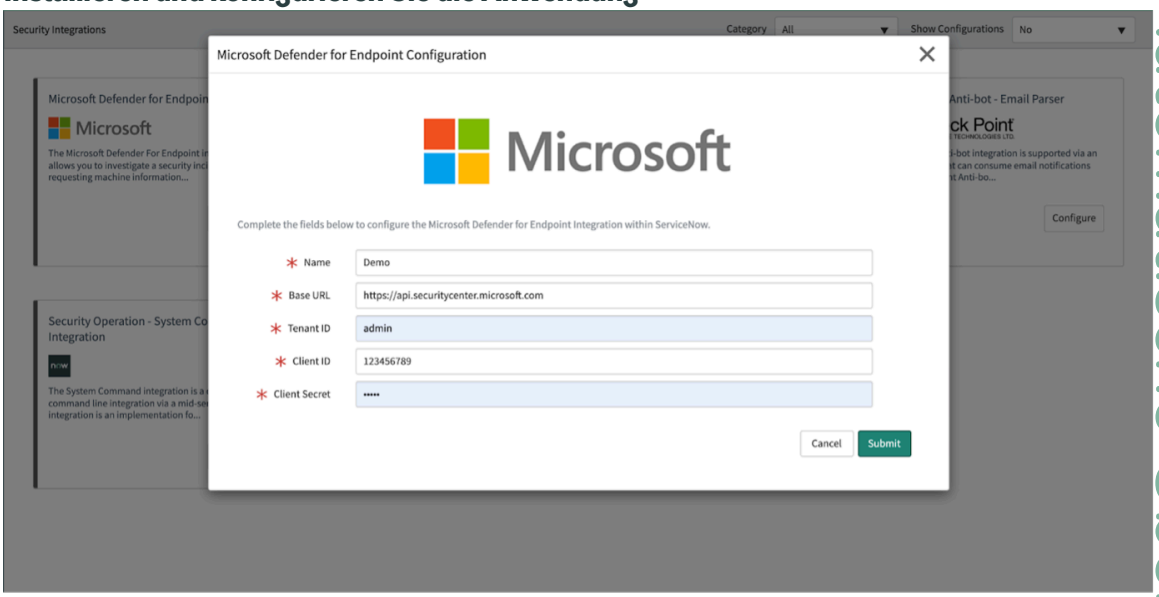
Name	Name für die Konfiguration der Instanz Microsoft Defender for Endpoint

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basis-URL	Die Servicebasis-URL für Microsoft Defender for Endpoint
Mandanten-ID	Die Microsoft Defender for Endpoint Mandanten-ID. Alle Aktionen werden in dieser Instanz ausgeführt.
Client-ID	Client-ID für die Anwendung, die Sie im Microsoft Azure-Portal registriert haben.
Geheimer Clientschlüssel	Geheimer Clientschlüssel für Ihre registrierte Anwendung.

5. Klicken Sie auf **Absenden**.

Installieren und konfigurieren Sie die Anwendung



Ergebnisse

Die Konfigurationsliste Microsoft Defender for Endpoint wird mit dem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für Microsoft Defender for Endpointabgeschlossen.

Microsoft Defender for Endpoint Standardeinstellungen

Nach Abschluss der Installation müssen Sie zusätzliche Konfigurationseinstellungen vornehmen.

Nachdem Sie die Installation abgeschlossen haben, finden Sie das Modul „Standardeinstellungen“ unter der Anwendung Microsoft Defender for Endpoint im linken Navigationsbereich. Sie enthält die Standardeinstellungen für verschiedene Microsoft Defender for Endpoint -Funktionalitäten.

Erforderliche Rolle: sn_si.admin, sn_si.analyst (schreibgeschützt).

Zusätzliche Konfigurationen

Im Folgenden finden Sie zusätzliche Konfigurationseinstellungen:

- **Genehmigung**: Diese Genehmigung gilt speziell für die Aktion „Host isolieren“, die Aktion „Hostisolierung entfernen“ und zusätzliche Aktionen wie „Ausführung der App einschränken“, „App-Beschränkung entfernen“ und „Antivirus-Scan ausführen“. Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

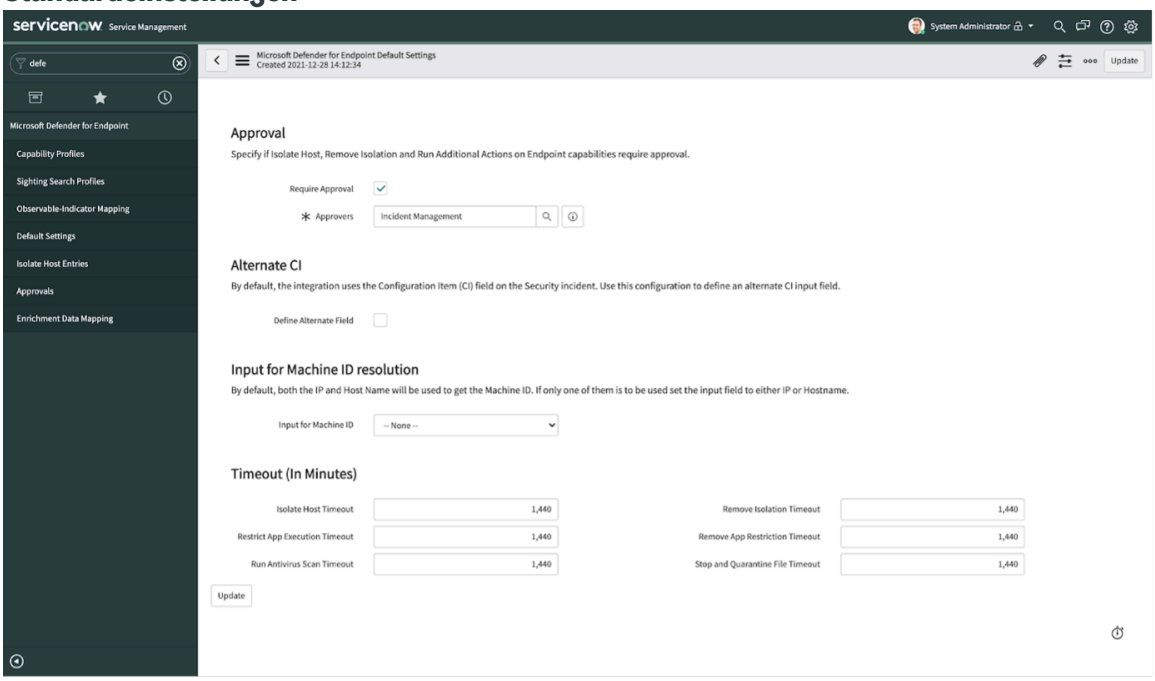
können diese Genehmigung nur verwenden, wenn Aktionen direkt von der zugehörigen Liste ausgelöst werden und keine Profile vorhanden sind. Wenn für diese Fähigkeiten Profile vorhanden sind, hat die Genehmigungskonfiguration im Profil Vorrang.

  - **Genehmigung erforderlich**: Wenn Sie **„Genehmigung erforderlich“**aktivieren, ist das Feld Genehmiger im Formular verfügbar.
  - **Genehmiger**: Liste der Genehmigergruppen. Nachdem Sie eine Anforderung übermittelt haben, ist zum Abschließen der Anforderung eine Genehmigung durch die Gruppe erforderlich.

- **Alternatives CI**: Durch Aktivieren dieses Kontrollkästchens wird die Liste der Felder angezeigt, in denen ein alternatives CI an die Fähigkeit übergeben werden kann. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Diese Konfiguration gilt nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“. Verwenden Sie diese Konfiguration, um ein alternatives CI-Eingabefeld nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“ zu definieren. Verwenden Sie für die anderen Fähigkeiten die Konfiguration im Profilabschnitt. Wenn die Profile kein alternatives CI definieren, übernehmen die Fähigkeiten das CI-Feld aus dem Formular „Security Incident“.
- **Eingabe für die Auflösung der Agent-ID**: Standardmäßig werden IP und Hostname zum Abrufen der Agent-ID verwendet. Wenn Sie nur eine davon verwenden möchten, legen Sie das Eingabefeld entweder auf „IP“ oder „Hostname“ fest.
- **Zeitüberschreitung**:
  - **Zeitüberschreitung bei Host-Isolierung (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeiten „Host isolieren“ an.
  - **Zeitüberschreitung für Isolation entfernen (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „Zeitüberschreitung für Isolierung entfernen“ an.
  - **Zeitüberschreitung bei der Ausführung von Apps einschränken (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „Ausführung von Apps einschränken“ an.
  - **Zeitüberschreitung beim Entfernen der App-Beschränkung (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „App-Beschränkung entfernen“ an.
  - **Zeitüberschreitung bei der Ausführung des Antivirus-Scans (in Minuten):** Gibt den Ausführungsschwellenwert für die Funktion „Antivirus-Scan ausführen“ an.
  - **Zeitüberschreitung beim Stoppen und Platzieren von Dateien (in Minuten):** Gibt den Ausführungsschwellenwert für die Funktion „Datei anhalten und unter Quarantäne stellen“ an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardeinstellungen



Ordnen Sie die Indikatortypen Microsoft Defender for Endpoint zu

Ordnen Sie den erkennbaren Elementtyp ServiceNow dem Indikatortyp Microsoft Defender for Endpoint zu. Diese Zuordnung wird in Microsoft Defender in den Aktionen „Anreicherung erkennbarer Elemente“ und „Indikator erstellen“ verwendet.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst (schreibgeschützt)

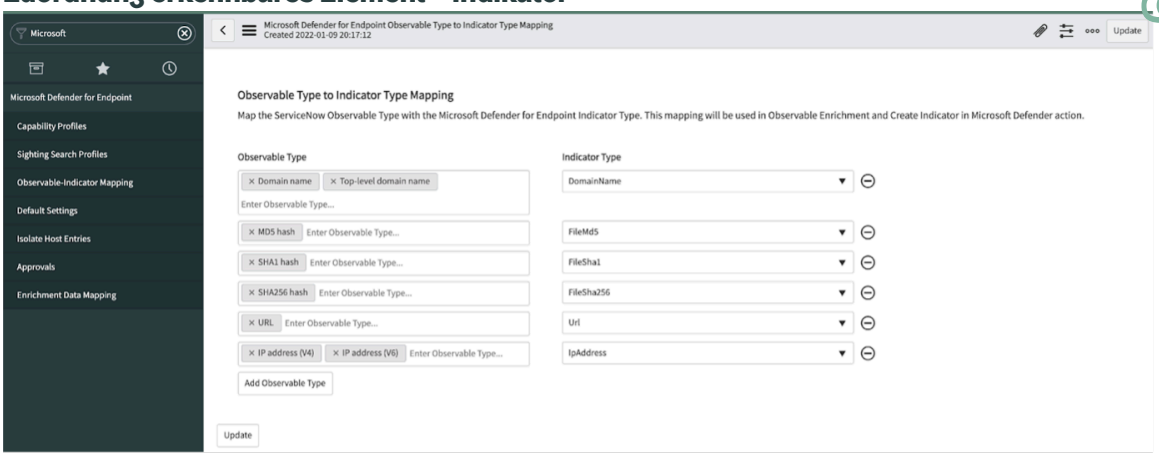
Warum und wann dieser Vorgang ausgeführt wird

In einem Szenario, in dem der Typ des erkennbaren Elements keinem Indikatortyp zugeordnet ist, sind diese erkennbaren Elemente nicht für die Ergänzung erkennbarer Elemente und die Indikatorerstellung in Microsoft Defender für Endpunkt geeignet.

Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Zuordnung erkennbares Element – Indikator**.

Zuordnung erkennbares Element – Indikator



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Fügen Sie einen erkennbaren Elementtyp auf eine der folgenden Arten hinzu, oder aktualisieren Sie ihn:
   - Um eine neue Zuordnung hinzuzufügen, klicken Sie auf **Add Observable Type (Erkennbaren Typ hinzufügen)**.
   - Um das erkennbare Element für die Zuordnung des Indikatortyps zu aktualisieren, klicken Sie auf eine vorhandene Zeile.
3. Klicken Sie auf **Aktualisieren**, um die Zuordnung zu speichern.

Erstellen Sie ein Fähigkeitsprofil für die Integration Microsoft Defender for Endpoint .

Erstellen Sie ein Profil, und wählen Sie die Microsoft Defender for Endpoint -Fähigkeiten aus, die das Profil ausführen soll.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Profile werden erstellt, um die Fähigkeiten zu vereinen oder zu gruppieren, was Analysten helfen würde, die Untersuchung oder Nachbesserung einfach durchzuführen. Sie können dem Profil die folgenden Fähigkeiten hinzufügen:

- Hostdetails abrufen
- Angemeldete Anwender abrufen
- Host isolieren
- Isolation entfernen

Sie können die Fähigkeiten „Host isolieren“ und „Hostisolierung entfernen“ nicht mit anderen Fähigkeiten in Zusammenhang bringen, während Sie ein Profil erstellen. Profile für diese Fähigkeiten müssen einzeln erstellt werden. Die Funktionen „Hostdetails abrufen“ und „Angemeldete Anwender abrufen“ können hingegen zusammengefasst werden. Sie können Profile einzeln erstellen oder sie je nach Bedarf ganz oder teilweise zusammenstellen.

Hinweis:
Nachdem eine Fähigkeit in ein Profil aufgenommen wurde, kann sie in keinem anderen Profil aus derselben Quelle enthalten sein.

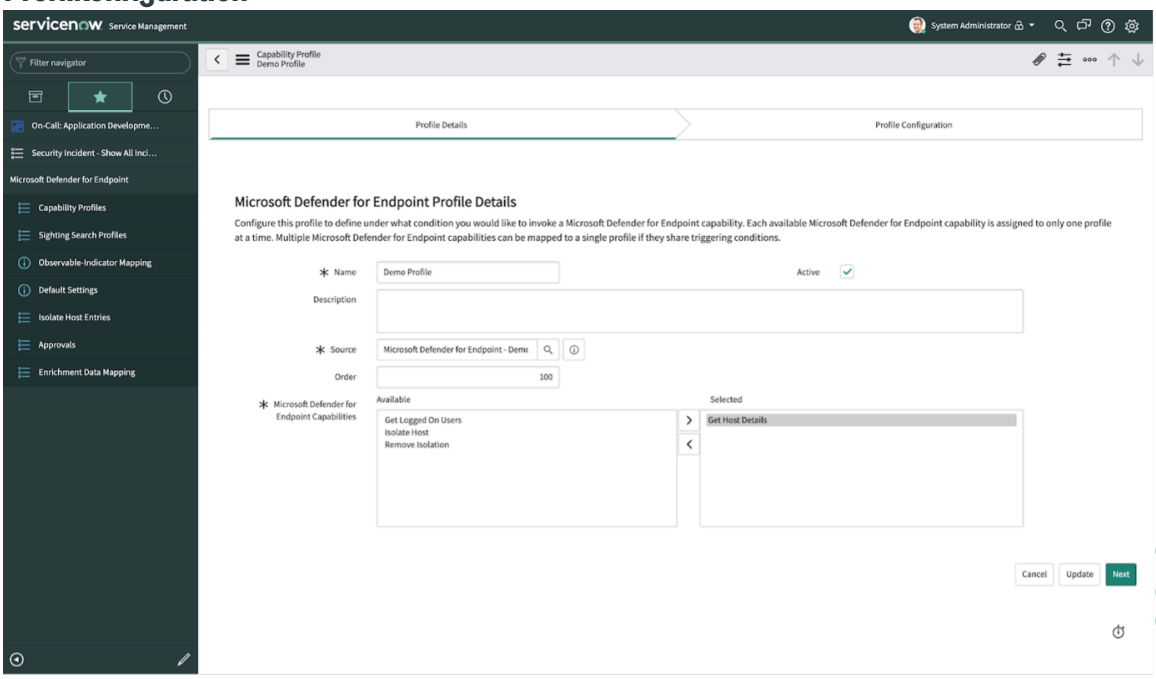
Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Fähigkeitsprofile**.

   Die Liste der Microsoft Defender für Endpunkt-Fähigkeitenprofile wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Profilkonfiguration



2. Klicken **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Fähigkeitsprofil“.

Feld	Beschreibung
Name	Name für das Fähigkeitsprofil Microsoft Defender for Endpoint. Mit diesem Namen können Sie den Profiltyp identifizieren und beschreiben.
Beschreibung	Zusätzliche Informationen zum Profil, die das Profil weiter beschreiben.
Quelle	Name der Microsoft Defender for Endpoint -Quelle. Nur konfigurierte Quellen sind in der Liste verfügbar.
Microsoft Defender für Endpunkt-Funktionen	Fähigkeiten des Profils Microsoft Defender for Endpoint. Wählen Sie die gewünschten Fähigkeiten für dieses Profil aus der Spalte Verfügbar aus, und verschieben Sie sie in die Spalte Ausgewählt.
Bestellung	Flow-Priorität. Der Standardwert ist 100. Der Wert dieses Felds gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Flow mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Beispiel: 100, 200, 300, 400.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option, um anzugeben, dass das Profil aktiv ist. Nach wird das Profil automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den Filterbedingungen entspricht, die Sie in der Konfiguration angegeben haben.

4. Klicken Sie auf, um mit Profilkonfiguration fortzufahren **Weiter**.

Nächste Maßnahme

Im nächsten Schritt konfigurieren Sie Ihr Profil. Bevor Sie die Einstellungen für das Profil konfigurieren, möchten Sie möglicherweise überprüfen, wie Profile sowie Bedingungen konfiguriert und auslösen. Weitere Informationen finden Sie unter Auslösebedingungen in einem Configuration Item.

Auslösebedingungen in einem Configuration Item

Nachdem Sie ein Profil erstellt und die Microsoft Defender for Endpoint -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Profileinstellungen so, dass das Profil nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt ist.

Wie Bedingungen in einem Konfigurationselement ausgelöst werden

Sie können Auslöserbedingungen festlegen, sodass das Profil automatisch ausgeführt wird, wenn ein Security Incident erstellt wird, der den Auslöserbedingungen entspricht. Wenn die Auslösebedingung nicht festgelegt ist, können diese Profile manuell ausgeführt werden, indem Sie im Security Incident auf das Formular „EDR-Profil(e) ausführen“ klicken und das Profil auswählen.

Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in Now Platform Configuration Management Database (CMDB)gespeicherten Informationen abzugleichen. Wenn ein Security Incident erstellt wird und ein Profil entweder automatisch oder manuell ausgeführt wird, wird CMDB durchsucht, um den Hostnamen oder die IP-Adresse basierend auf dem Wert des CI-Felds abzurufen. Der Hostname oder die IP wird verwendet, um die Agent-ID auf Microsoft Defender for Endpoint aufzulösen und den Endpunkt zu identifizieren.

In einem idealen Szenario wird ein übereinstimmender Wert in der -Datenbank gefunden, und Daten werden in der Konsole Microsoft Defender for Endpoint für das übereinstimmende Asset gesammelt. Die Daten für verschiedene Fähigkeiten werden in Ihre Instanz Now Platform Configuration Management Database (CMDB) abgerufen und in den zugehörigen Listen eines Security Incident angezeigt. Wenn das Feld Configuration Item (CI) im Security Incident mit einem Hostnamen mit oder einer IP-Adresse, die der -Datenbank entspricht, nicht ausgefüllt ist, können Sie im Security Incident ein alternatives Feld auswählen, das entweder den Hostnamen oder die auszuführende IP-Adresse enthält die Agent-ID-Auflösung.

Während des Konfigurationsschritts des Profil-Setups können Sie ein alternatives CI-Feld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass Sie den Endpunkt unter Microsoft Defender for Endpointidentifizieren können. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Durch Auswahl dieses alternativen CI-Felds als Sicherung stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld im zugehörigen Security Incident bei der Incident-Erstellung nicht ausgefüllt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die alternativen CI-Felder werden nur für Fähigkeiten berücksichtigt, die einem Profil hinzugefügt werden können. Zu diesen Fähigkeiten gehören „Hostdetails abrufen“, „Angemeldete Benutzer abrufen“, „Host isolieren“ und „Isolierung entfernen“. Für alle zusätzlichen Aktionen muss das alternative CI im Modul „Standardeinstellungen“ konfiguriert sein.

Konfigurieren Sie Profile und Security Incidents für die -Integration Microsoft Defender for Endpoint .

Erstellen Sie ein Profil, und wählen Sie die Microsoft Defender for Endpoint -Fähigkeiten aus, die das Profil ausführen soll. Sie müssen die Einstellungen so konfigurieren, dass das Profil nur unter den definierten Bedingungen ausgelöst werden kann.

Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.analyst (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie das Profil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Bei Bedarf können Sie ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen und Filterbedingungen festlegen, damit das Profil automatisch ausgelöst wird, wenn ein Security Incident erstellt wird, der die Auslöserbedingungen erfüllt.

Hinweis:
Sie können zur Seite „Profilkonfiguration“ nur navigieren, nachdem Sie die Seite „Profildetails“ aufgerufen haben.

Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Fähigkeitsprofile**.
2. Klicken Sie, nachdem Sie den Abschnitt Profildetails abgeschlossen haben, auf **Weiter**.
   Überprüfen und konfigurieren Sie die Abschnitte.
3. Wählen Sie im Abschnitt „Kriterien für Incidents definieren (Automatisierung)“ die Option **„Kriterien für Incidents definieren“** aus, um Microsoft Defender for Endpoint -Funktionen im Profil automatisch auszulösen.
   Incident-Kriterien definieren (Automatisierung): Definieren Sie die Bedingungen für Security Incidents, die automatisch die Microsoft Defender for Endpoint-Fähigkeiten für das Profil auslösen. Wenn Sie die Option **„Incident-Kriterien definieren“** nicht auswählen, können das Profil und die zugrunde liegenden Fähigkeiten manuell über den Security Incident aufgerufen werden.

   Hinweis:
   Die Funktionen „Host isolieren“ und „Host isolieren“ können nicht automatisch ausgelöst werden.

   a. Wählen Sie in den **Filterbedingungen**das Pflichtfeld aus.
   b. Fügen Sie **neue Kriterien** hinzu, und definieren Sie auch die **ODER-** oder die **UND-** Bedingung.
4. Aktivieren Sie im Abschnitt „Genehmigungen“ das Kontrollkästchen **Genehmigung erforderlich**, um eine zusätzliche Kontrollebene bereitzustellen.

   Wenn Sie diese Option auswählen, haben Sie mehr Kontrolle, wenn Sie die Microsoft Defender für Endpunkt-Fähigkeiten zum Isolieren von Hostcomputern, Wiederherstellen im Netzwerk oder Abrufen von Dateien verwenden.

   Die Option „Genehmigungen“ in der Profilkonfiguration wird nur für die Funktionen „Host isolieren“ und „Hostisolierung entfernen“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Abschnitt „Zusätzliche Konfiguration“ die Option **Alternatives Feld definieren aus**, um ein alternatives Eingabefeld zu definieren.
   Zusätzliche Konfiguration: Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, um die Microsoft Defender für Endpunkt-APIs abzufragen .

   Hinweis:
   Weitere Informationen finden Sie unter Auslösebedingungen in einem Configuration Item.

   a. Wählen Sie die Option **Alternatives Feld definieren** aus.

   b. Wählen Sie das Eingabefeld aus **Alternatives CI-Auslöserfeld**.

6. Aktivieren Sie im Abschnitt „Tags“ das Kontrollkästchen **Tag anzeigen**, um die Kennzeichnung von Security Incidents zu aktivieren. Bei Aktivierung des Tags wird der Profilname vorangestellt.

   Optional können Sie Security Incidents mit Tags für „Profil initiiert“, „Profil abgeschlossen“ und „Profil fehlgeschlagen“ kennzeichnen. Standardmäßig ist diese Option für alle Profile deaktiviert.

7. Klicken **Fertig**.

Verifiziert die Auslöserbedingungsfilter

Validieren Sie das Profil und vergewissern Sie sich, dass die von Ihnen konfigurierten Auslöserbedingungsfilter wie erwartet funktionieren.

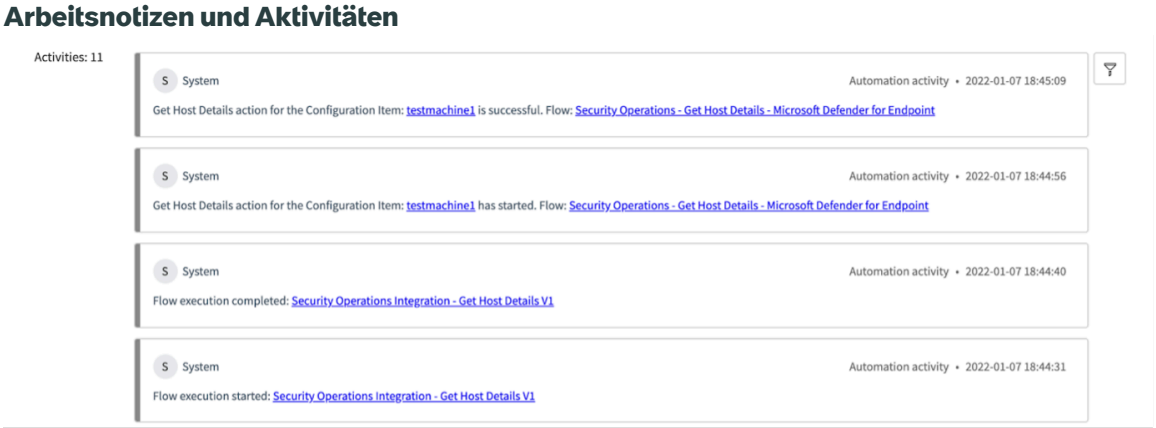
Vorbereitungen
Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Nachdem Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in den Security Incidents Now Platform® anzeigen.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Um einen neuen Security Incident zu erstellen, wählen Sie **Neu**.
3. Um das jeweilige Profil auszulösen, geben Sie die im Fähigkeitsprofil angegebenen Filterbedingungen an.
4. Klicken **Speichern**.
5. Um den Abschnitt „Arbeitsnotizen und Aktivitäten“ zu validieren, zeigen Sie die Datensätze an, die mit den Tags „Profil initiiert“, „Profil abgeschlossen“ oder „Profil fehlgeschlagen“ gekennzeichnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Um alle Daten in den zugehörigen Listen zu validieren, klicken Sie **auf Alle zugehörigen Listen anzeigen**.
7. Klicken Sie auf eine beliebige Registerkarte **der zugehörigen Liste**, um die Details zu validieren. Beispiel: Hostdetails.

Lösen Sie die Microsoft Defender for Endpoint -Fähigkeiten über zugehörige Links aus

Lösen Sie ein Fähigkeitsprofil manuell aus, nachdem Sie einen Security Incident über zugehörige Links überprüft haben.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

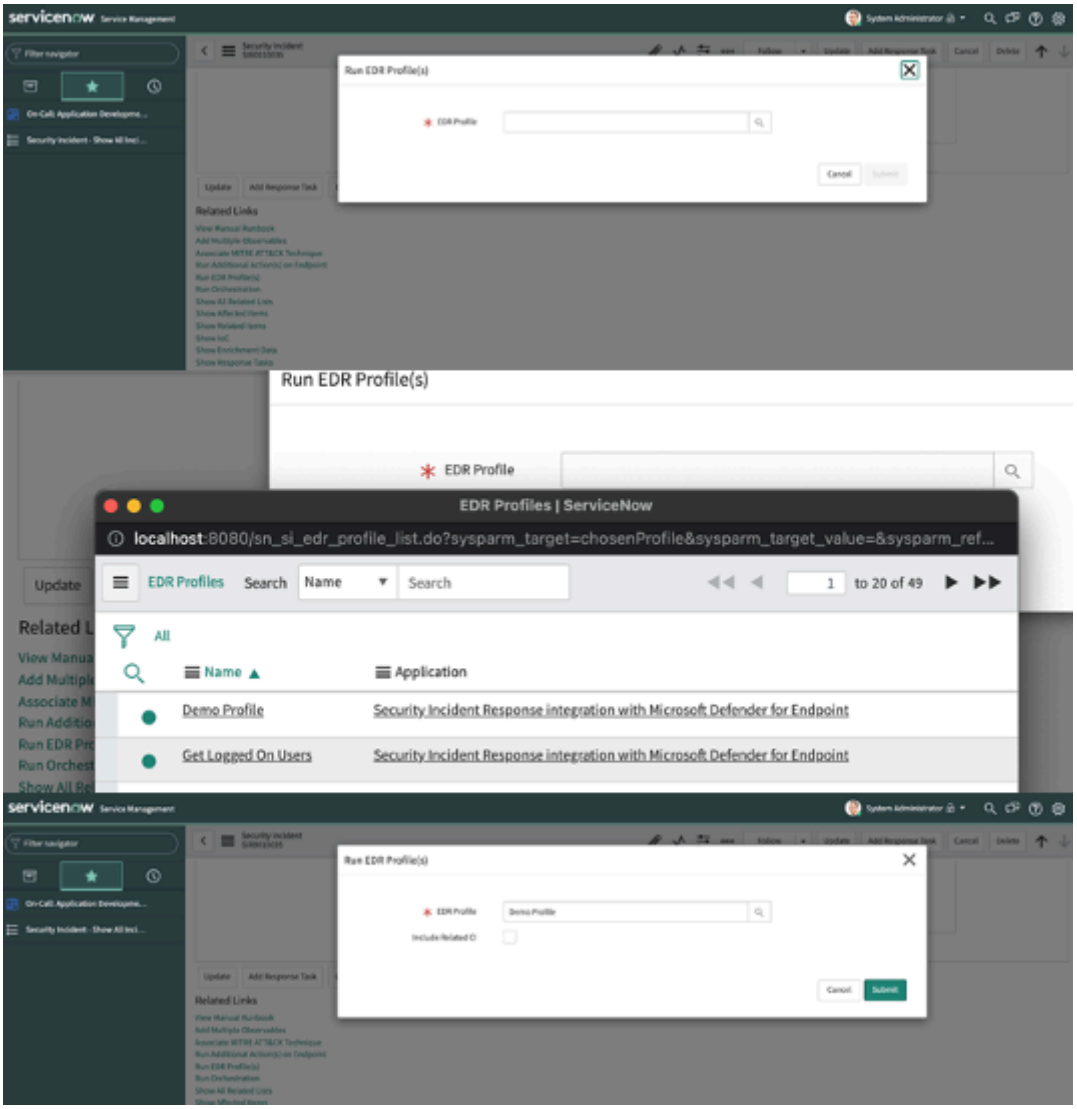
Sie können das Profil nicht nur für das CI oder das alternative CI des Security Incident ausführen, sondern auch für CI-Werte, die in der zugehörigen Liste „Konfigurationselement“ vorhanden sind, indem Sie im Dialogfeld **„Zugehöriges CI einbeziehen“** auswählen. Dadurch werden auch die Daten für die CI-Werte abgerufen, die in der zugehörigen Liste vorhanden sind. Alternativ können Sie das Profil nur für die CI-Werte ausführen, die in der zugehörigen Liste vorhanden sind.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen Microsoft Defender for Endpoint aus.
3. Klicken Sie im Abschnitt „Zugehörige Links **“ auf EDR-Profil(e) ausführen**.
4. Suchen Sie in der Liste der verfügbaren Profile nach einem Profil, und klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie ein Profil aus



Das ausgewählte Profil wird manuell ausgelöst.

5. Validieren Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
6. Zeigen Sie die Tags an, und validieren Sie die Daten in den zugehörigen Listen.

Lösen Sie die Microsoft Defender for Endpoint in der zugehörigen Liste „Configuration Item“ aus

Lösen Sie ein Fähigkeitsprofil manuell über die zugehörige Liste des Konfigurationselements aus.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen Microsoft Defender for Endpoint aus.
3. Klicken **Alle zugehörigen Listen anzeigen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die zugehörige Liste Configuration Item.
5. Wählen Sie die hinzugefügten Configuration Items aus.
6. Wählen Sie unter **Aktionen** für ausgewählte Zeilen eine Fähigkeit aus.
   Die ausgewählte Fähigkeit wird manuell ausgelöst.
7. Validieren Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
8. Zeigen Sie die Tags an, und validieren Sie die Daten in den zugehörigen Listen.

Zusätzliche Konfigurationen in Microsoft Defender for Endpoint

Die Microsoft Defender for Endpoint -Integration unterstützt die Ausführung zusätzlicher Aktionen, die über die Standardaktionen hinausgehen.

Microsoft Defender for Endpoint unterstützt die folgenden zusätzlichen Konfigurationen:

Konfigurieren Sie die Fähigkeit „Host isolieren“ in Microsoft Defender for Endpoint

Isolieren Sie den Host vom Zugriff auf das Netzwerk in Microsoft Defender for Endpoint basierend auf dem Schweregrad des Angriffs. Durch das Isolieren des Hosts vom Netzwerk können Sie andere schädliche Aktivitäten oder potenzielle Angriffe auf andere Hosts verhindern.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Anforderungen für die Fähigkeit „Host isolieren“.

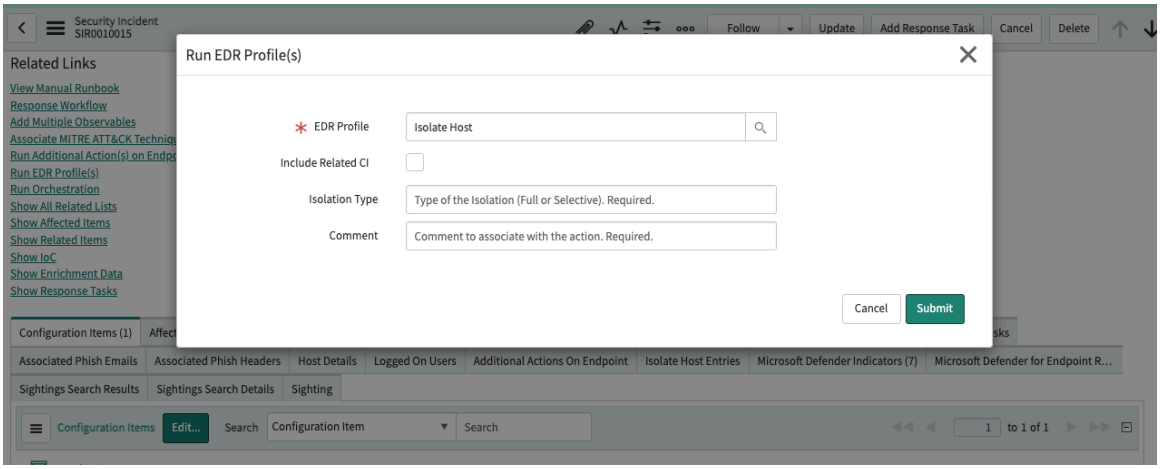
Fähigkeit	Erforderlich	Beschreibung
Host isolieren	Isolierungstyp	(Erforderlich) Typ der Isolierung (vollständig oder selektiv).
	Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.
3. Klicken Sie im Abschnitt „Zugehörige Links **“ auf EDR-Profil(e) ausführen**.
4. Suchen und wählen Sie in der Liste der verfügbaren Profile ein Profil mit **der Fähigkeit „Host isolieren“** aus, und klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Host isolieren



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt „Zugehörige Listen“ **auf Alle zugehörigen Listen anzeigen**.

b. Klicken Sie auf die zugehörige Liste **Configuration Item**.

c. Wählen Sie **Host isolieren** aus, und wählen Sie die entsprechenden Fähigkeiten aus.

5. Validieren Sie die Automatisierungsaktivität und den Abschnitt „Aktivitäten“, und stellen Sie sicher, dass die Daten den Erwartungen entsprechen.
6. Zeigen Sie die Daten an, und validieren Sie die Details der Hostisolierung in den zugehörigen Listen.

Konfigurieren Sie die Funktion „Hostisolierung entfernen“ in Microsoft Defender for Endpoint

Entfernen Sie bei Bedarf die Isolation eines Hosts, der zuvor vom Netzwerk in Microsoft Defender for Endpointisoliert war. Sie können andere schädliche Aktivitäten oder potenzielle Angriffe auf andere Hosts verhindern.

Vorbereitungen

Anforderungen für die Fähigkeit „Isolation entfernen“.

Fähigkeit	Erforderliche Eingabe	Beschreibung
Isolation entfernen	Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll.

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

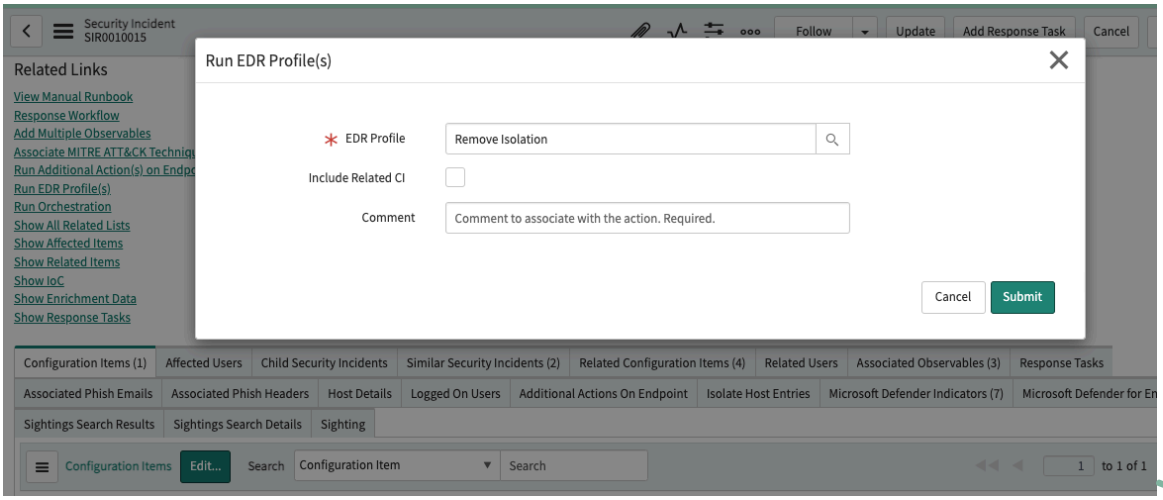
Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.
3. Klicken Sie im Abschnitt „Zugehörige Links **“ auf EDR-Profil(e) ausführen**.
4. Suchen und wählen Sie ein Profil mit **der Fähigkeit Isolation entfernen** aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Isolation entfernen



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt „Zugehörige Listen“ auf **Alle zugehörigen Listen anzeigen**.

b. Klicken Sie auf die zugehörige Liste **Configuration Item**.

c. Wählen Sie **Isolation entfernen** und anschließend die entsprechenden Fähigkeiten aus.

5. Validieren Sie die Automatisierungsaktivität und den Abschnitt „Aktivitäten“.
6. Zeigen Sie die Daten an, und validieren Sie die Details der Hostisolierung in den zugehörigen Listen.
7. Validiert die Automatisierungsaktivitäten der -Ausführung.

Konfigurieren Sie die Funktion Antivirus-Scan ausführen in Microsoft Defender for Endpoint

Initiieren Sie remote einen Virenscan, um Malware zu identifizieren und zu beheben, die möglicherweise auf einem gefährdeten Gerät vorhanden ist. Führen Sie den Scan als Teil des Untersuchungs- oder Antwortprozesses aus.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Anforderungen für die Funktion „Antivirus-Scan ausführen“.

Eingabe	Beschreibung
Scantyp	(Erforderlich) Typ des Scans (vollständig oder schnell).
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll.

Prozedur

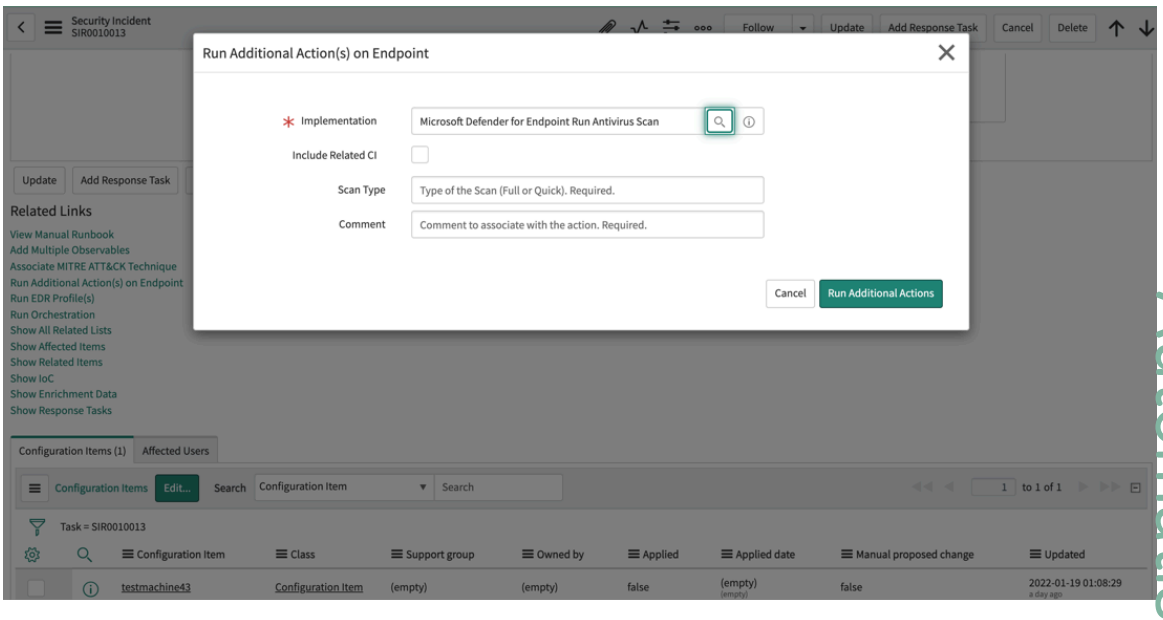
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.

b. Durchsuchen und die gewünschte Fähigkeit auswählen
Klicken Sie beispielsweise auf die Fähigkeit **Antivirus-Scan ausführen**.

Antivirus-Scan ausführen



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt „Zugehörige Listen“ **auf Alle zugehörigen Listen anzeigen**.

b. Klicken Sie auf die zugehörige Liste **Configuration Item**.

c. Wählen Sie die hinzugefügten Konfigurationselemente aus, und wählen Sie unter Aktionen für ausgewählte Zeilen die Option **Zusätzliche Aktionen für Endpunkt ausführen aus**.

Nachdem Sie die Implementierung der Fähigkeit **Antivirus-Scan ausführen** ausgewählt haben, werden die Eingabefelder **Zusätzlicher Scantyp** und **Kommentar** angezeigt.

3. Wählen Sie den **Scantyp** aus, den Sie ausführen möchten (Schnell oder Vollständig), und fügen Sie einen Kommentar hinzu, bevor Sie den Scan ausführen.
4. Um die Virenprüfung zu initiieren, klicken Sie auf **Zusätzliche Aktion ausführen**.
5. Zeigen Sie die Automatisierungsaktivitäten der -Ausführung an, und validieren Sie sie.
6. Validiert den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

Konfigurieren Sie die Funktion „App-Ausführung einschränken“ in Microsoft Defender for Endpoint

Um einen Angriff einzudämmen, schränken Sie ein Gerät ein oder sperren Sie es, und verhindern Sie, dass nachfolgende Versuche potenziell schädlicher Programme ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Anforderungen für die Fähigkeit „App-Ausführung einschränken“.

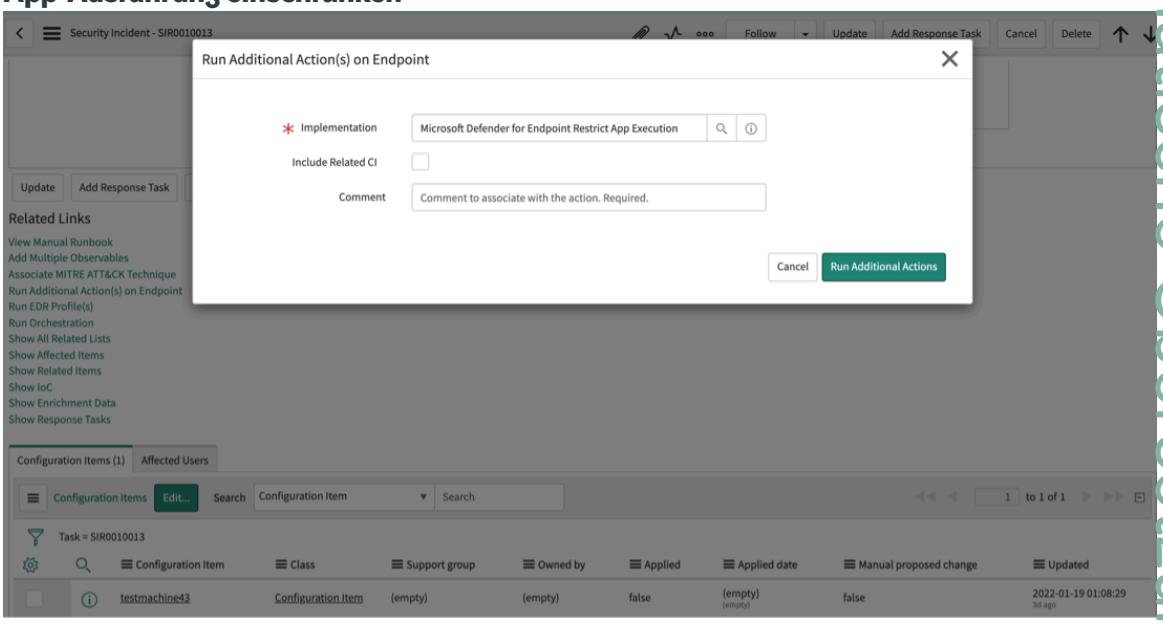
Eingabe	Beschreibung
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll)

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.
   a. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.
   b. Navigieren Sie zur Fähigkeit **App-Ausführung einschränken**, und wählen Sie sie aus.

App-Ausführung einschränken



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt „Zugehörige Listen“ **auf Alle zugehörigen Listen anzeigen**.
b. Klicken Sie auf die zugehörige Liste **Configuration Item**.
c. Wählen Sie die hinzugefügten Configuration Items aus.
d. Wählen Sie unter Aktionen für ausgewählte Zeilen **die Option Zusätzliche Aktionen für Endpunkt ausführen aus**.

3. Klicken Sie auf **Zusätzliche Aktion ausführen**, um die Option Ausführung von Apps einschränken auf dem Computer zu aktivieren.
4. Zeigen Sie die Automatisierungsaktivitäten der -Ausführung an, und validieren Sie sie.
5. Validiert den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Funktion „App-Beschränkung entfernen“ in Microsoft Defender for Endpoint

Entfernen Sie bei Bedarf die Einschränkungen aller Anwendungen auf dem Gerät.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

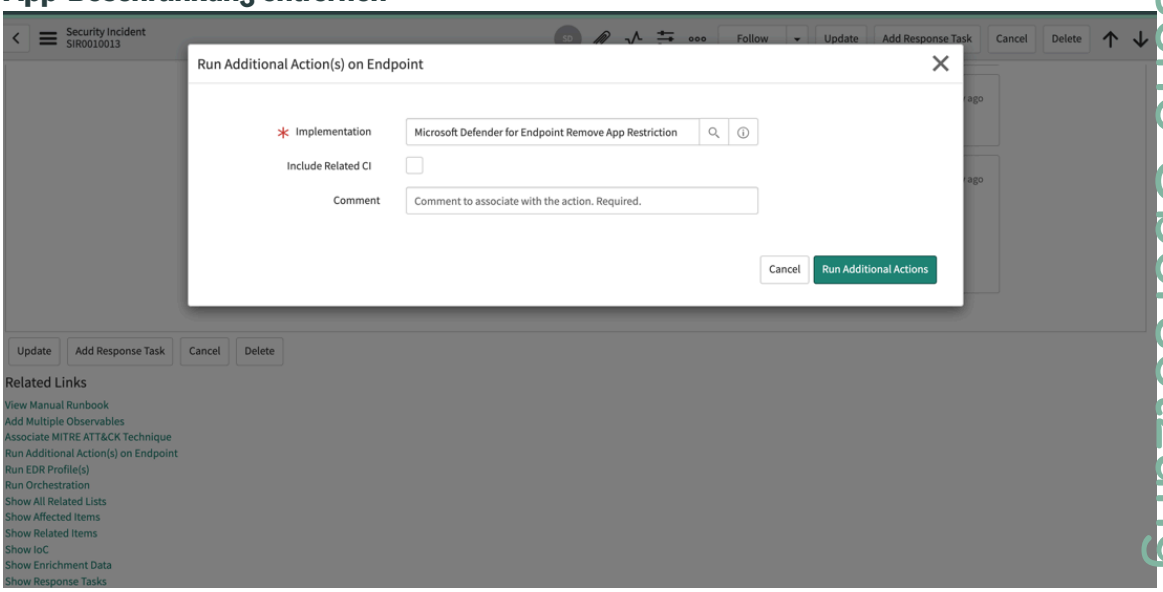
Anforderungen für die Fähigkeit „App-Beschränkung entfernen“.

Eingabe	Beschreibung
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll)

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.
   a. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.
   b. Navigieren Sie zu der Funktion **App-Beschränkung entfernen,** und wählen Sie sie aus.

App-Beschränkung entfernen



Alternativ können Sie die folgenden Schritte ausführen:

   a. Klicken Sie im Abschnitt „Zugehörige Listen“ **auf Alle zugehörigen Listen anzeigen**.
   b. Klicken Sie auf die zugehörige Liste **Configuration Item**.
   c. Wählen Sie die hinzugefügten Configuration Items aus.
   d. Wählen Sie **Zusätzliche Aktionen für Endpunkt ausführen aus**.
   Das Eingabefeld Zusätzlicher Kommentar wird angezeigt.
3. Um die App-Einschränkung aufzuheben, klicken Sie auf **Zusätzliche Aktion ausführen**.
4. Zeigen Sie die Automatisierungsaktivitäten der -Ausführung an, und validieren Sie sie.
5. Validiert den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Fähigkeit „Zugehörige Computer aus Defender abrufen“ in Microsoft Defender for Endpoint

Ruft die Liste der zugehörigen Computer bestimmter erkennbarer Elemente ab.

Vorbereitungen

Hinweis:
Unterstützte erkennbare Typen sind Domänenname, SHA1-Hash und Anwendername.

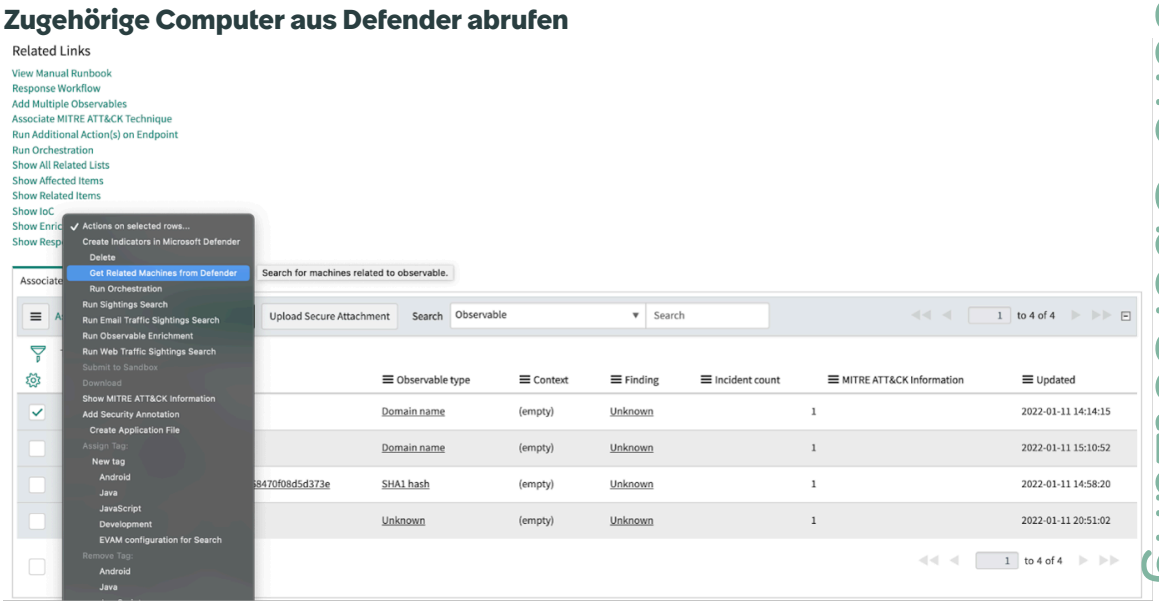
Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Liste der Computer abrufen, die auf die jeweiligen erkennbaren Elemente zugegriffen haben. Sie können die Liste in der Detailtabelle zugehöriger Computer von Microsoft Defender für Endpunkt speichern. Sie können die Funktion „Zugehörige Computer aus Defender abrufen“ über die zugehörige Liste „Zugeordnete erkennbare Elemente“ auslösen.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.



3. Klicken Sie im Abschnitt „Zugehörige Links“ **auf IoC anzeigen**.
4. Klicken Sie auf die zugehörige Liste Zugeordnete erkennbare Elemente.
5. Wählen Sie die zugehörigen erkennbaren Elemente aus.
6. Wählen Sie in der Liste Aktionen die **Funktion Zugehörige Computer aus Defender** abrufen.
7. Validieren Sie die Automatisierungsaktivität und den Abschnitt „Aktivitäten“.
8. Zeigen Sie die Daten an, und validieren Sie die Details der Microsoft Defender für Endpunkt-bezogenen Computer in den zugehörigen Listen.
9. Zeigen Sie die Automatisierungsaktivitäten der -Ausführung an, und validieren Sie sie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Funktion zum Anhalten und Quarantänen von Dateien in Microsoft Defender for Endpoint

Dateien von der Microsoft Defender-Plattform anhalten und unter Quarantäne stellen.

Vorbereitungen

Unterstützte erkennbare Typen: SHA1-Hash

Anforderungen für die Funktion „Datei anhalten und in Quarantäne stellen“

Eingabe	Beschreibung
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll)

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Aktion „Datei anhalten und in Quarantäne stellen“ nur für bestimmte erkennbare Elemente vom Typ SHA1 ausführen. Speichern Sie die Details in der Tabelle „Zusätzliche Aktionen für Endpunkt“. Sie können die Fähigkeit „Datei anhalten und unter Quarantäne stellen“ über die zugehörige Liste Microsoft Defender für Endpunkt zugehörige Computer auslösen.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.
3. Klicken Sie im Abschnitt „Zugehörige Links **“ auf Alle zugehörigen Listen anzeigen**.
4. Klicken Sie auf die zugehörige Liste Details zu Microsoft Defender für Endpunkt-Computer.
5. Wählen Sie einen oder mehrere Datensätze aus.
6. Wählen Sie unter „ **Aktionen** für ausgewählte Zeilen“ die Fähigkeit **Datei anhalten und in Quarantäne stellen**.
7. Validieren Sie die Automatisierungsaktivität und den Abschnitt „Aktivitäten“.
8. Zeigen Sie die Daten an, und validieren Sie die Daten in den zugehörigen Listen.
9. Zeigen Sie die Automatisierungsaktivitäten der -Ausführung an, und validieren Sie sie.

Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche mit der Microsoft Defender for Endpoint -Integration

Sichtungssuchprofil automatisch mit Microsoft Defender for Endpointerstellen und konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können den Workflow für die Sichtungssuche verwenden, um Sichtungssuchen durchzuführen. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, sucht nach implementierenden Fähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchen aus, die auf dem konfigurierten Workflow basieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Defender for Endpoint stellt ein Sichtungssuchprofil für das Basissystem bereit, mit dem Sie die automatischen Sichtungssuchen konfigurieren können. Mit diesem Profil können Sie auf die zugehörigen Sichtungsinformationen für erkennbare Elemente einer Organisation zugreifen und auch die Sichtungen anderer Organisationen anzeigen.

Prozedur

1. Navigieren zu **Integrationen** > **Sichtungssuche: Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die folgenden Felder des Formulars aus.

Formular „Konfigurationen für Sichtungssuche“.

Feld	Beschreibung
Name	Name für das Sichtungssuchprofil.
Ist gespeicherte Suche	Option zum Speichern der Suchkonfiguration. Die gespeicherten Suchkonfigurationsabfragen sind Beispielabfragen. Sie können sie durch die Parameter für Ihre Umgebung ersetzen und nach Bedarf zusätzliche gespeicherte Suchkonfigurationen erstellen.
Sichtungssuchquelle	Die Quelle, die für die Sichtungssuche in der Integration Microsoft Defender for Endpoint konfiguriert ist.
Suchen	Native Suchzeichenfolge, die eine Abfrage formt.
Aktiv	Option zum Aktivieren der gespeicherten Suchkonfiguration. Nur aktive Suchkonfigurationen können eine Sichtungssuche durchführen.
Erkennbarer Typ	Typ der Kategorie erkennbarer Elemente. Zum Beispiel IP-Adresse, Hash-Wert, URL und Domänenname.
Maximales erkennbares Element pro Suche	Maximale Anzahl erkennbarer Elemente, die Sie in einer Suchabfrage anzeigen können. Legen Sie diesen Wert für diese Integration auf 1 fest.
Sichtungssuchparameter	Parameter zum Definieren komplexerer Abfragen, die Logik und andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden.

4. Klicken Sie auf **Absenden**.

Führen Sie eine manuelle Sichtungssuche in durch Microsoft Defender for Endpoint

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in Microsoft Defender for Endpoint durch, um die Verbreitung einer Bedrohung im Zeitverlauf zu bestimmen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden erkennbaren Elemente werden unterstützt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Domänenname
- IP-Adresse (V4)
- IP-Adresse (V6)
- MD5-Hash
- SHA1-Hash
- SHA256-Hash

Prozedur

1. Navigieren Sie zu **Security Incidents**.
2. Öffnen Sie einen vorhandenen SIR, oder erstellen Sie einen neuen SIR.
3. Klicken Sie in den zugehörigen Links **auf IoC anzeigen**.
4. Klicken Sie auf die zugehörigen Listen Zugeordnete erkennbare Elemente.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in der Liste „Aktionen“ **auf Ergänzung erkennbarer Elemente ausführen**.
7. Wählen Sie die erkennbaren Elemente unter **Aktion** für ausgewählte Zeilen aus, und klicken Sie auf **Sichtungssuche ausführen**.

   Hinweis:
   Die Sichtungssuche wird für die erkennbaren Elementtypen Domänenname, IP-Adresse (V4), IP-Adresse (V6), MD5-Hash, SHA1-Hash bzw. SHA256-Hash unterstützt.

8. Geben Sie den Zeitrahmen für die Suche an, und klicken Sie auf **Suchen**.

   Hinweis:
   Microsoft Defender für Endpunkt unterstützt nur die Sichtungssuche für die letzten 30 Tage. Wenn Ihre Bereichsabfrage vor den letzten 30 Tagen liegt, ruft die Sichtungssuche keine Daten ab. Wenn sich Ihre Bereichsabfrage mit den letzten 30 Tagen überschneidet, werden nur die Sichtungen der letzten 30 Tage abgerufen. Wenn Ihre Bereichsabfrage innerhalb der letzten 30 Tage liegt, werden die Sichtungen ab der definierten Startzeit bis zur aktuellen Zeit abgerufen.

9. Validieren Sie nach Abschluss der Suche die Ergebnisse und Details in den zugehörigen Listen.
10. Klicken Sie auf **Sichtungssuchdetails,** um die Details der Sichtungssuche anzuzeigen.
11. Klicken Sie auf die Registerkarte **Sichtung**, um Details und die Registerkarte **Sichtungssuchergebnisse zu erhalten,** um die Suchergebnisse anzuzeigen.

    Zusätzliche Informationen zu der jeweiligen Sichtung können Sie im Feld **Zusammenfassung** anzeigen.

Führen Sie eine automatische Anreicherung erkennbarer Elemente in durch Microsoft Defender for Endpoint

Führen Sie eine automatische Anreicherung erkennbarer Elemente in Microsoft Defender for Endpoint durch, um erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen Quellen anzureichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass die Systemeigenschaft **Security Incident Response** aktiviert ist. Diese Option löst die Fähigkeit zur Ergänzung erkennbarer Elemente in SIR aus, wenn ein erkennbares Element einem Security Incident zugeordnet wird.

Erforderliche Rolle: sn_si.admin, sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können diese Funktionalität während bei der Reaktion auf Incidents während Untersuchungen verwenden, um eine identifizierte Bedrohung einzudämmen. Wenn dem Security Incident neue erkennbare Elemente zugeordnet werden, können Sie die automatische Ausführung der Ergänzung erkennbarer Elemente in Microsoft Defender für Endpoint aktivieren.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.
3. Validiert die Automatisierungsaktivität, sobald die neuen erkennbaren Elemente dem Security Incident zugeordnet wurden.
4. Zeigen Sie die Ergebnisse der Ergänzung in der zugehörigen Liste „Indikatoren“ des Security Incident an. Weitere Informationen zur Ergänzung erkennbarer Elemente finden Sie in der folgenden Tabelle.

Microsoft Defender-Indikator

Feld	Beschreibung
Indikator-ID	Identität der Indikatorentität. Klicken Sie auf **Öffnen**, um den Datensatz in Details in der Instanz Now Platform anzuzeigen
Erkennbares Element	Das dem Ergebnis zugeordnete erkennbare Element.
Titel	Titel für den Indikator.
Indikatortyp	Typ des Indikators.
Aktion	Vom Indikator durchgeführte Aktion.
Empfohlene Aktion	Empfohlene Aktionen für den Indikator.
Integrationslieferant	Integration der Defender-Quelle, aus der die Daten abgerufen werden.
Ablaufdatum	Ablaufzeit für den Indikator.
Abrufdatum	Datum, an dem der Ergänzungsdatensatz erstellt wird.

Führen Sie eine manuelle Anreicherung erkennbarer Elemente in durch Microsoft Defender for Endpoint

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Anreicherung erkennbarer Elemente durch, um erkennbare Elemente mit zusätzlichen Informationen aus Microsoft Defender for Endpointanzureichern.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die Microsoft Defender for Endpoint -Integration ermöglicht die Anreicherung erkennbarer Elemente für alle Typen erkennbarer Elemente, die im Modul „Erkennbares Element – Indikatorzuordnung“ zugeordnet sind.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender für Endpunkt-Informationen überprüfen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen**.
4. Klicken Sie auf die Registerkarte **Zugeordnete erkennbare Elemente**.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in der Liste „Aktionen“ **auf Ergänzung erkennbarer Elemente ausführen**.
7. Wählen Sie eine Microsoft Defender für Endpunkt **-Quelle** aus, und verschieben Sie sie in die Spalte **Ausgewählt**, um anzugeben, welche Implementierung Sie zum Anreichern der ausgewählten erkennbaren Elemente verwenden möchten.
8. Klicken Sie auf **Absenden**.
9. Um den Status der Ausführung zu validieren, zeigen Sie die Arbeitsnotizen an.
10. Um die Ergebnisse anzuzeigen, klicken Sie auf die Registerkarte **Microsoft Defender-Indikator**. Weitere Informationen zur Ergänzung erkennbarer Elemente finden Sie in der folgenden Tabelle.

Microsoft Defender-Indikator

Feld	Beschreibung
Indikator-ID	Identität der Indikatorentität. Klicken Sie auf **Öffnen**, um den Datensatz in Details in der Instanz Now Platform anzuzeigen
Erkennbares Element	Das dem Ergebnis zugeordnete erkennbare Element.
Titel	Titel für den Indikator.
Indikatortyp	Typ des Indikators.
Aktion	Vom Indikator durchgeführte Aktion.
Empfohlene Aktion	Empfohlene Aktionen für den Indikator.
Integrationslieferant	Integration der Defender-Quelle, aus der die Daten abgerufen werden.
Ablaufdatum	Ablaufzeit für den Indikator.
Abrufdatum	Datum, an dem der Ergänzungsdatensatz erstellt wird.

Indikatoren in Microsoft Defender for Endpoint erstellen

Erstellen Sie mit Microsoft Defender for EndpointIndikatoren aus zugehörigen erkennbaren Elementen des Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

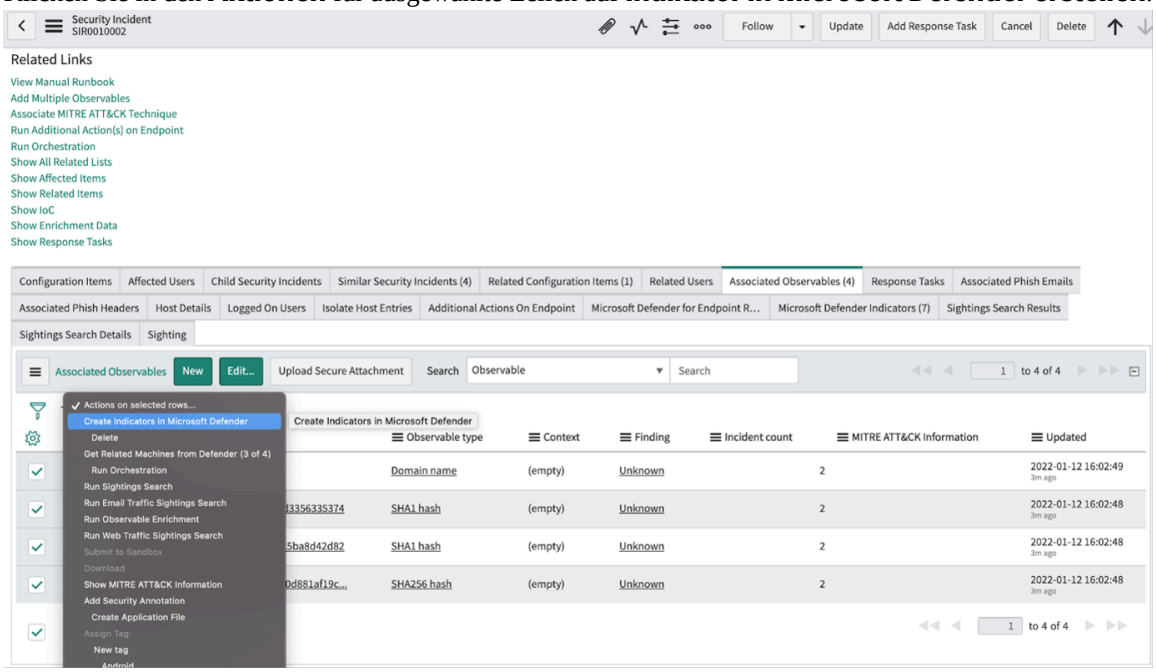
Warum und wann dieser Vorgang ausgeführt wird

Die Microsoft Defender for Endpoint -Integration ermöglicht die Anreicherung erkennbarer Elemente für alle Typen erkennbarer Elemente, die im Zuordnungsmodul „Erkennbares Element – Indikator“ zugeordnet sind.

Das Erstellen von Indikatoren bietet Ihnen die Möglichkeit, eine Liste von Indikatoren für die Erkennung und das Blockieren von Prävention und Reaktionen festzulegen. Sie können die Indikatoren aus dem zugehörigen erkennbaren Element des Security Incident erstellen.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie Indikatoren in Microsoft Defender für Endpunkt erstellen möchten.
3. Klicken Sie auf die zugehörigen Listen Zugeordnete erkennbare Elemente.
4. Fügen Sie vorhandene erkennbare Elemente hinzu, oder erstellen Sie neue erkennbare Elemente.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in den **Aktionen** für ausgewählte Zeilen auf **Indikator in Microsoft Defender erstellen**.



7. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Ausgewählte erkennbare Elemente	Betroffene erkennbare Elemente. Diese Aktion kann verwendet werden, um Indikatoren für mehrere erkennbare Elemente zu erstellen. Wenn Sie die Auswahl eines erkennbaren Elements aufheben möchten, können Sie dies tun, indem Sie die Auswahl der erkennbaren Elemente aus der Liste aufheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn die unterstützten erkennbaren Elemente nicht zugeordnet sind, werden die Indikatoren für solche erkennbaren Elemente nicht in Microsoft Defender erstellt.
Titel	Titel für den Indikator.
Beschreibung	Beschreibung für den Indikator.
Ablaufzeit	Ablaufzeit für den Indikator.
Empfohlene Aktionen	Empfohlene Aktionen, die für den Indikator ausgeführt werden müssen.
Quelle	Integrationskonfiguration zum Erstellen des Indikators.
Aktion	Aktionen, die ausgeführt werden, wenn der Indikator in der Organisation erkannt wird. Die möglichen Werte lauten wie folgt: ○ **Warnen** ○ **Blockieren** ○ **Audit** ○ **BlockierenUndNachbessern** ○ **Zulässig**
Anwendung	Die Microsoft Defender für Endpunkt-Anwendung, die dem Indikator zugeordnet ist. Dieses Feld gilt nur für einen neuen Indikator und kann nicht für einen vorhandenen Indikator verwendet werden.
Schweregrad	Schweregrad des Indikators. Die möglichen Werte lauten wie folgt: ○ **Niedrig** ○ **Zuverlässige Anzeige** ○ **Hoch**
RBAC-Gruppennamen	RBAC-Gruppennamen, auf die der Indikator angewendet würde. Die Namen befinden sich in einer durch Kommas getrennten Liste.

8. Klicken Sie auf **Indikator erstellen**
9. Validieren Sie die Aktivität und die UI-Nachrichten.
10. Klicken Sie auf die Registerkarte **Microsoft Defender-Indikator,** um die Ergebnisse anzuzeigen.

Aktualisieren Sie Indikatoren in Microsoft Defender for Endpoint

Aktualisieren Sie die vorhandenen Indikatoren in Microsoft Defender for Endpoint über das Listenkontextmenü bzw. über die Formularansicht des Microsoft Defender-Indikators.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.analyst

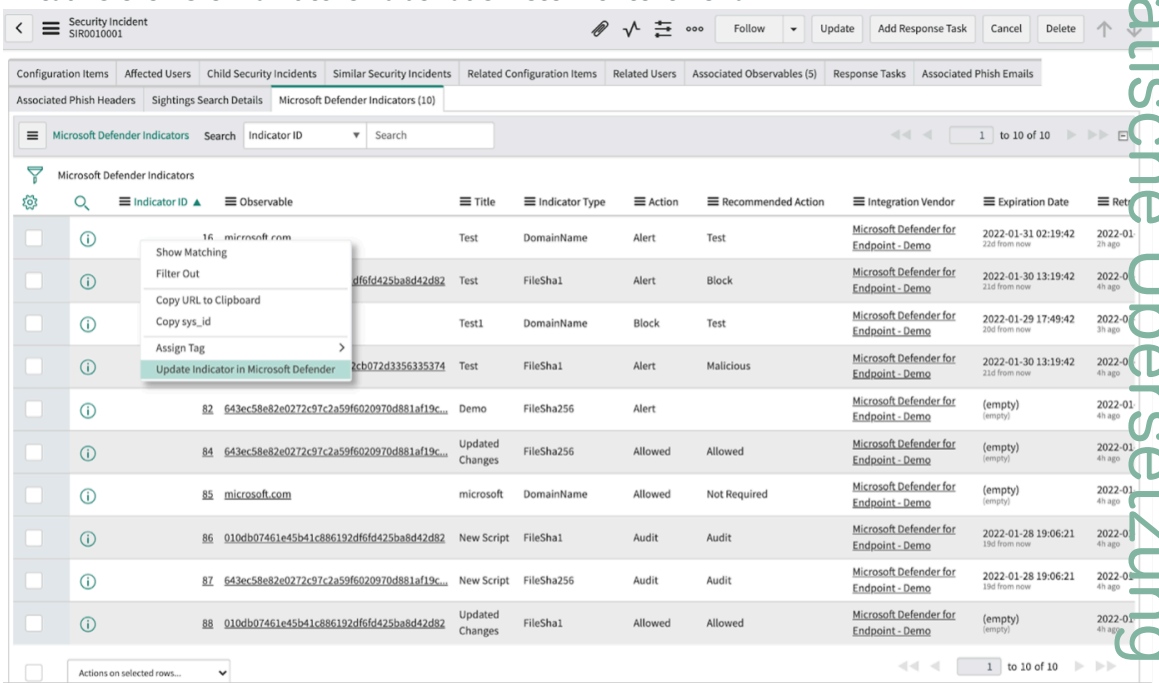
Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und dann auf die Registerkarte **Microsoft Defender-Indikatoren**.

> **Hinweis:**
>
> Sie müssen die zugehörige Liste für die Microsoft Defender-Indikatoren konfigurieren, die in den zugehörigen Listen für Security Incidents angezeigt werden. Weitere Informationen finden Sie unter UI-Aktionen für Formulare.

3. Aktualisieren Sie die Microsoft Defender für Endpunkt-Indikatoren auf eine der folgenden Arten:
   - Um die Indikatoren über das Listenkontextmenü zu aktualisieren, wählen Sie die Zeile des Indikators aus, den Sie aktualisieren möchten, und klicken Sie **in der Option Microsoft Defender auf Indikator aktualisieren**.

Aktualisieren Sie Indikatoren über das Listenkontextmenü

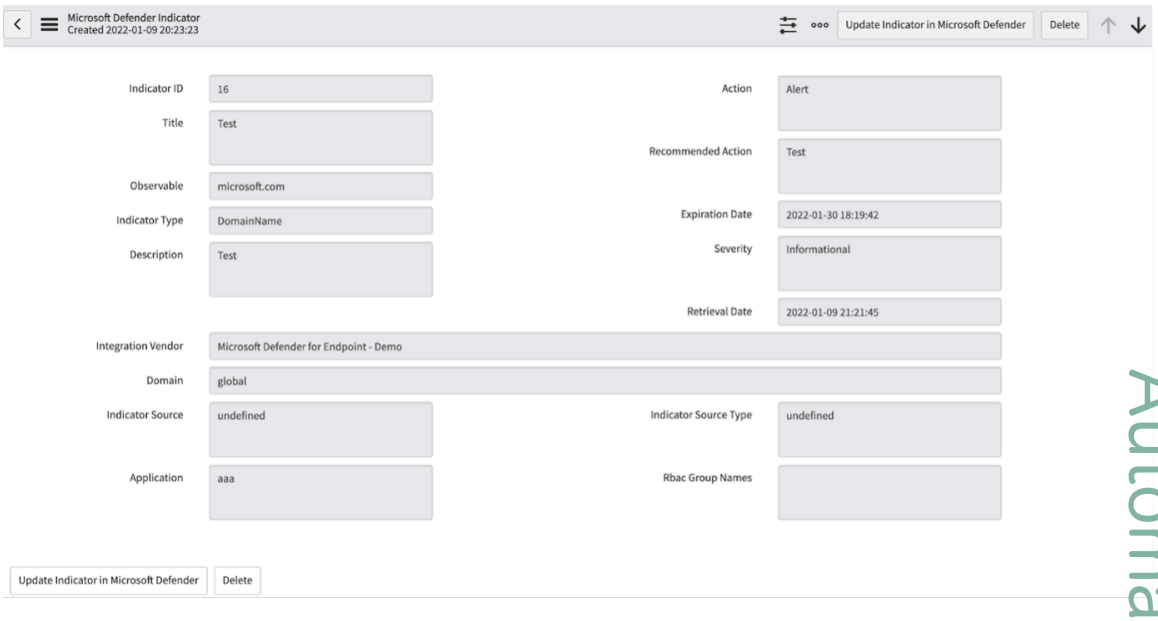


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Indikatoren aus der Formularansicht zu aktualisieren, klicken Sie in der Formularansicht **in Microsoft Defender auf Indikator aktualisieren**.

Aktualisieren Sie Indikatoren in der Formularansicht



4. Füllen Sie die Felder des Formulars aus.

Formular „Microsoft Defender-Indikator“.

Feld	Beschreibung
Titel	Titel für den Indikator.
Beschreibung	Beschreibung für den Indikator.
Ablaufzeit	Ablaufzeit für den Indikator.
Empfohlene Aktionen	Empfohlene Aktionen, die für den Indikator ausgeführt werden sollen.
Quelle	Integrationskonfiguration zum Erstellen des Indikators.
Aktion	Aktionen, die ausgeführt werden, wenn der Indikator in der Organisation erkannt wird. Die möglichen Werte lauten wie folgt: ○ **Warnen** ○ **Blockieren** ○ **Audit** ○ **BlockierenUndNachbessern** ○ **Zulässig**
Anwendung	Die Microsoft Defender für Endpunkt-Anwendung, die dem Indikator zugeordnet ist. Dieses Feld gilt nur für einen neuen Indikator und kann nicht für einen vorhandenen Indikator verwendet werden.
Schweregrad	Schweregrad des Indikators. Mögliche Werte:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Niedrig** ○ **Zuverlässige Anzeige** ○ **Hoch**
RBAC-Gruppennamen	Namen der RBAC-Gruppe, auf die der Indikator angewendet wird. Die Namen befinden sich in einer durch Kommas getrennten Liste.

5. Klicken Sie auf **Indikator aktualisieren**.
6. Validieren Sie die Aktivität und die UI-Nachrichten.

Domain Separation in Microsoft Defender for Endpoint der -Integration

Domänentrennung wird in der Microsoft Defender for Endpoint -Integration unterstützt. Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe

Support: Standard

Verwenden Sie die folgenden Schritte für Domain Separation:

1. Erstellen Sie in der entsprechenden Domäne einen Benutzer mit der Rolle sn_si.admin.
2. Führen Sie die Microsoft Defender for Endpoint Integrationsverfahren in der entsprechenden Domäne durch.

Konfiguration der Quotenbegrenzung in Integration Microsoft Defender for Endpoint

Konfigurieren Sie die Quotengrenze der API und die Zeitüberschreitung für die Quotengrenze für Microsoft Defender for Endpoint die -Integration.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.analyst (schreibgeschützt)

Prozedur

1. Geben Sie im Navigationsfilter sys.properties.listein.
   Die gesamte Liste der Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties] wird angezeigt.
2. Suchen und ändern Sie die folgenden Eigenschaften entsprechend Ihren Anforderungen.

Eigenschaftsname	Beschreibung
sn_sec_defender_ep.rate_limit_timeout_in_minutes	Wenn eine Anforderung nicht innerhalb des angegebenen Zeitrahmens ausgeführt wird, wird die Ausführung angehalten und eine entsprechende Fehlermeldung angezeigt. Standardwert: 75.
sn_sec_defender_ep.request_per_hour_limit	Wenn der konfigurierte API-Aufruf innerhalb von einer Stunde am selben Endpunkt erfolgt, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung
	die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist. Standardwert: 1500.
sn_sec_defender_ep.request_per_minute_limit	Wenn der konfigurierte API-Aufruf innerhalb einer Minute am selben Endpunkt erfolgt, wird die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist. Standardwert: 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	Wenn der konfigurierte API-Aufruf innerhalb einer Minute am Endpunkt erfolgt, wird die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist. Standardwert: 30.

Microsoft Exchange Online Integration

Bei der Integrationsanwendung Microsoft Exchange Online von ServiceNowwird das Produkt Now Platform® Security Incident Response (SIR) in den Service Microsoft Exchange Online integriert, einen der cloudbasierten Services in der Office 365-Produktsuite MicrosoftMicrosoft Azure Event Hubs. Ihr SOC-Analyst (Security Operation Center) kann die E-Mail-Umgebung Ihres Unternehmens nach sicherheitsbezogenen Bedrohungen durchsuchen und Phishing-E-Mails mit E-Mail-Such- und -Löschfunktionen entfernen und korrigieren.

Übersicht

Als Security Incident-Analyst führen Sie die Integration über die Schnittstelle für Sicherheitsanalysten aus, und der Workflow gibt E-Mail-Nachrichtendetails zurück, die den Suchkriterien entsprechen. E-Mail-Suchvorgänge basieren auf Kriterien wie Betreffzeilen sowie E-Mail-Adressen von Absendern und Empfängern. Nachdem die E-Mail-Suche abgeschlossen ist, können Sie verdächtige E-Mails aus dem Service Microsoft Exchange Online löschen. Außerdem kann ein optionaler Genehmigungsprozess konfiguriert werden, um vor dem Löschen von E-Mails eine Genehmigung anzufordern.

Diese Integration zum Suchen und Löschen von E-Mails kann mit einem umfassenderen Workflow oder Runbook für Incidents zur Reaktion auf Phishing verwendet werden. Nachdem ein Unternehmensbenutzer oder Mitarbeiter eine verdächtige E-Mail erhalten und dem Phishing-Reaktionsteam oder dem Posteingang des Unternehmens gemeldet hat, wird die gemeldete E-Mail an Now Platform weitergeleitet und als Security Incident kategorisiert. Nachdem Sie verifiziert haben, dass es sich bei einer E-Mail um einen Phishing-Angriff handelt, können Sie als Analyst, der für die Untersuchung von Phishing-Incidents verantwortlich ist, eine E-Mail-Suche starten, um festzustellen, ob andere Unternehmensanwender diese Phishing-E-Mail erhalten haben. Mit der Suche können Sie zugehörige E-Mails aus derselben Phishing-Kampagne finden und andere potenzielle Opfer identifizieren, die die E-Mail möglicherweise erhalten und gelesen haben und möglicherweise auch auf eine schädliche URL geklickt oder einen Anhang geöffnet haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

Die Integration umfasst die folgenden Schlüsselfunktionen:

- Konfigurieren Sie Suchkriterien für Phishing-Bedrohungen in Security Incident Response basierend auf Kombinationen der Felder „Absender“, „Empfänger“ und „Betreff“ in E-Mail-Nachrichten.
- Bei großen und langen E-Mail-Suchen wird der Security Incident-Analyst per E-Mail benachrichtigt, wenn die Suche erfolgreich abgeschlossen wurde, zusammen mit der Anzahl der übereinstimmenden Nachrichten.
- Der Status für einzelne Nachrichten informiert Sie, wenn Empfänger verdächtige E-Mails gelesen oder gelöscht haben.
- Wenn konfiguriert, stellen optionale Genehmigungsprozesse sicher, dass verdächtige E-Mails nicht ohne vorherige Genehmigung gelöscht werden.
- Ein vollständiger Audit-Pfad für Löschanforderungen, der die Anzahl der gelöschten E-Mails enthält, wird in den Arbeitsnotizen von Security Incidents protokolliert.
- Wenn Tagging konfiguriert ist, werden Sicherheits-Tags aufgezeichnet, wenn E-Mail-Such- und -Lösch-Workflows für Security Incidents initiiert und erfolgreich abgeschlossen werden.

Unterstützte Versionen Microsoft Exchange Online.

Diese Integration unterstützt Services vom Microsoft Exchange Online Typ , die Teil der Office 365-Suite MicrosoftMicrosoft Azure Event Hubs sind. Die Integration unterstützt keine gehosteten MicrosoftMicrosoft Azure Event Hubs Exchange-Umgebungen. MicrosoftMicrosoft Azure Event Hubs führt die Services Microsoft Exchange Online in der Exchange 2016-Version aus.

Voraussetzungen

Das Plugin „com.snc.si_dep“ ist für jede Now Platform -Version erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations -Anwendungen müssen über ServiceNow Storeinstalliert und aktiviert werden. Installieren Sie eine Anwendung nach der anderen in der unten aufgeführten Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

Integrationsarchitektur und Systemverbindung

Weitere Informationen zur Architektur der Integration, einschließlich wichtiger Begriffe und Details zu Verbindungen externer Systeme, finden Sie unter Integrationsarchitektur und externe Systemverbindung für die Microsoft Exchange Online -Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Die folgenden Themen sind nummeriert. Befolgen Sie die unten in der Reihenfolge aufgeführten Themen, um eine reibungslose Installation und Konfiguration der Anwendung zu gewährleisten.

Eine Prüfliste dieser Schritte zum Ausdrucken finden Sie unter Prüfliste für die Microsoft Exchange Online -Integration. Anhand dieser Liste können Sie Ihren Fortschritt überwachen, während Sie die End-to-End-Aufgaben der Einrichtung, Konfiguration und Überprüfung der Ergebnisse der Integration durchführen.

Richten Sie Ihr MicrosoftMicrosoft Azure Event Hubs Azure-Konto für die ServiceNow Microsoft Exchange Online -Integration ein

Führen Sie die folgenden Setupaufgaben im Azure-Portal MicrosoftMicrosoft Azure Event Hubs aus, bevor Sie die Anwendung ServiceNow für diese Integration installieren. Dieser Account ermöglicht den Zugriff auf den -Mandanten Microsoft Exchange Online für E-Mail-Nachrichtendetails.

Vorbereitungen

Erforderliche Rolle: MicrosoftMicrosoft Azure Event Hubs Azure-Portaladministrator

Dieser Account ist erforderlich, um auf den -Mandanten Microsoft Exchange Online zuzugreifen, zusätzliche E-Mail-Nachrichtendetails zu sammeln und E-Mail-Nachrichten zu löschen. Dieser Account wird im Azure-Portal MicrosoftMicrosoft Azure Event Hubs eingerichtet.

Die Bilder in den folgenden Aufgaben sind privilegiert und proprietär und werden mit Genehmigung von MicrosoftMicrosoft Azure Event Hubsverwendet. Dieser Inhalt kann bis zum MicrosoftMicrosoft Azure Event Hubsaktualisiert werden. Um sicherzustellen, dass Sie Zugriff auf die neuesten Inhalte haben, konsultieren Sie die Microsoft-Dokument -Website.

In den folgenden Abbildungen wird ServiceNow Inc. als Accountname in den Beispielen für das Azure-Portal angezeigt. In Ihrem Azure-Portal-Account wird der Unternehmensname für Ihren Account im Azure-Portal angezeigt.

Prozedur

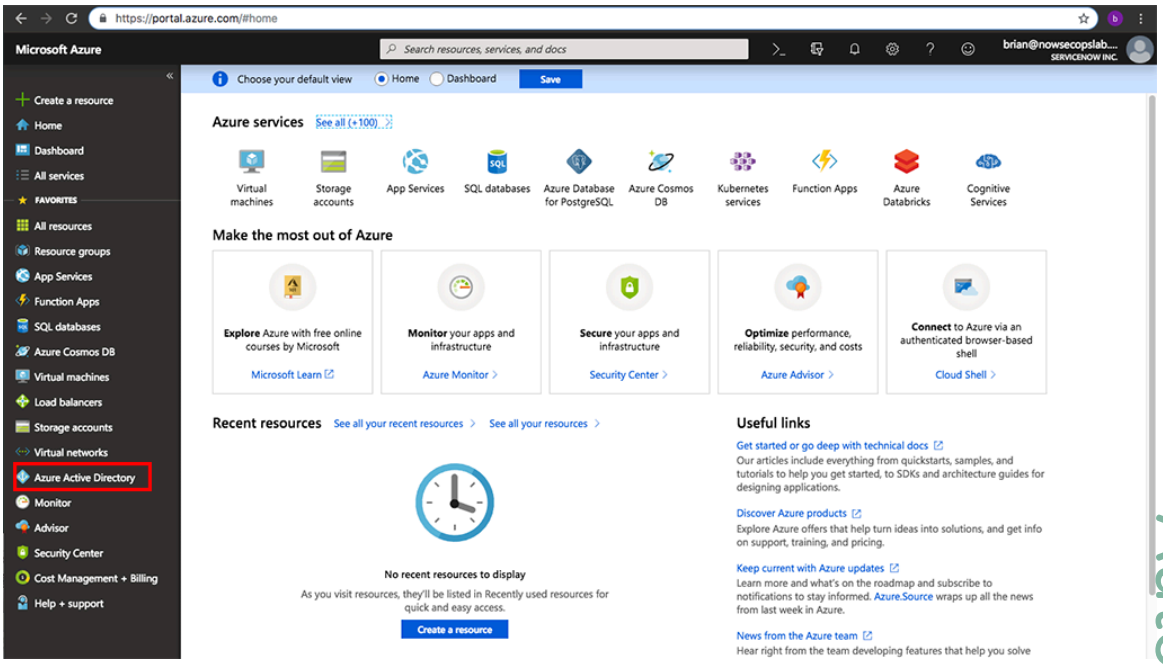
Wenn Sie im Azure-Portal MicrosoftMicrosoft Azure Event Hubs keine Anwendungs-ID für die OAuth-Authentifizierung erstellt haben, führen Sie die folgenden Schritte aus.

a. Melden Sie sich beim Azure-Portal MicrosoftMicrosoft Azure Event Hubs mit den Anmeldeinformationen Ihres Azure-Portal-Administrators an.

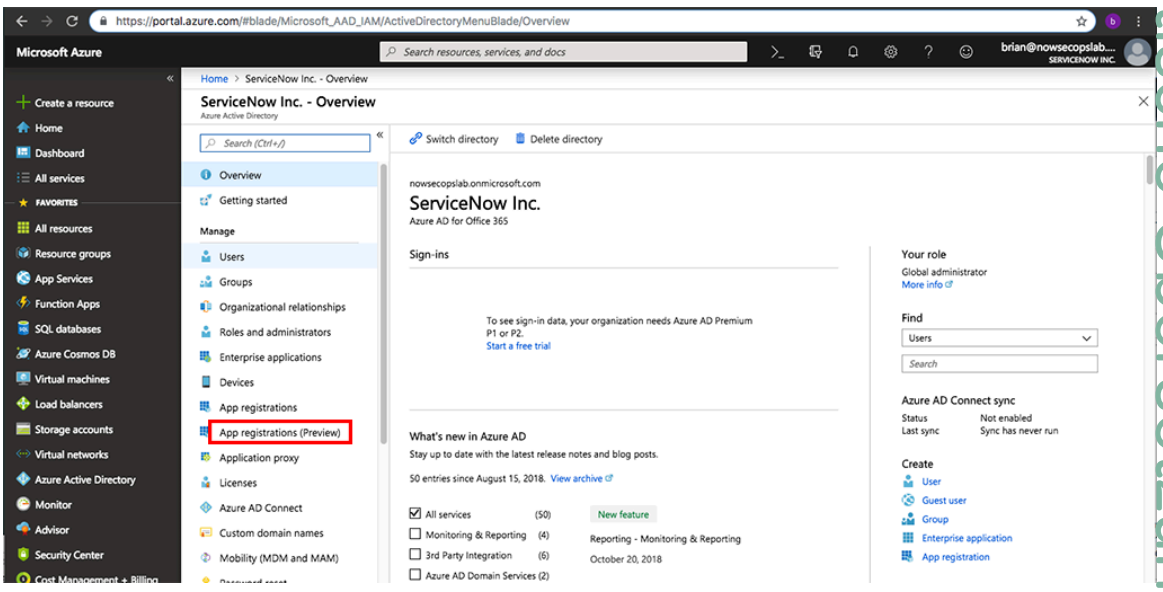
b. Klicken Sie im linken Navigationsbereich der Startseite auf **Azure Active Directory**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



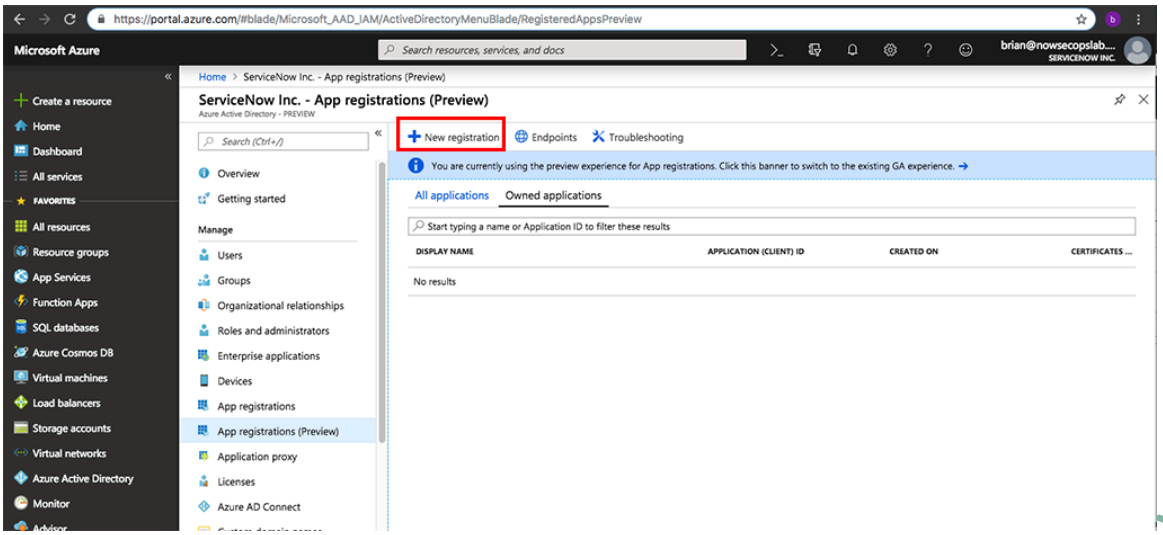
c. Klicken Sie im angezeigten Fenster Übersicht auf **App-Registrierungen (Vorschau)**.



d. Klicken Sie im angezeigten Bereich App-Registrierungen (Vorschau) auf **Neue Registrierung**.

Automatische Übersetzung

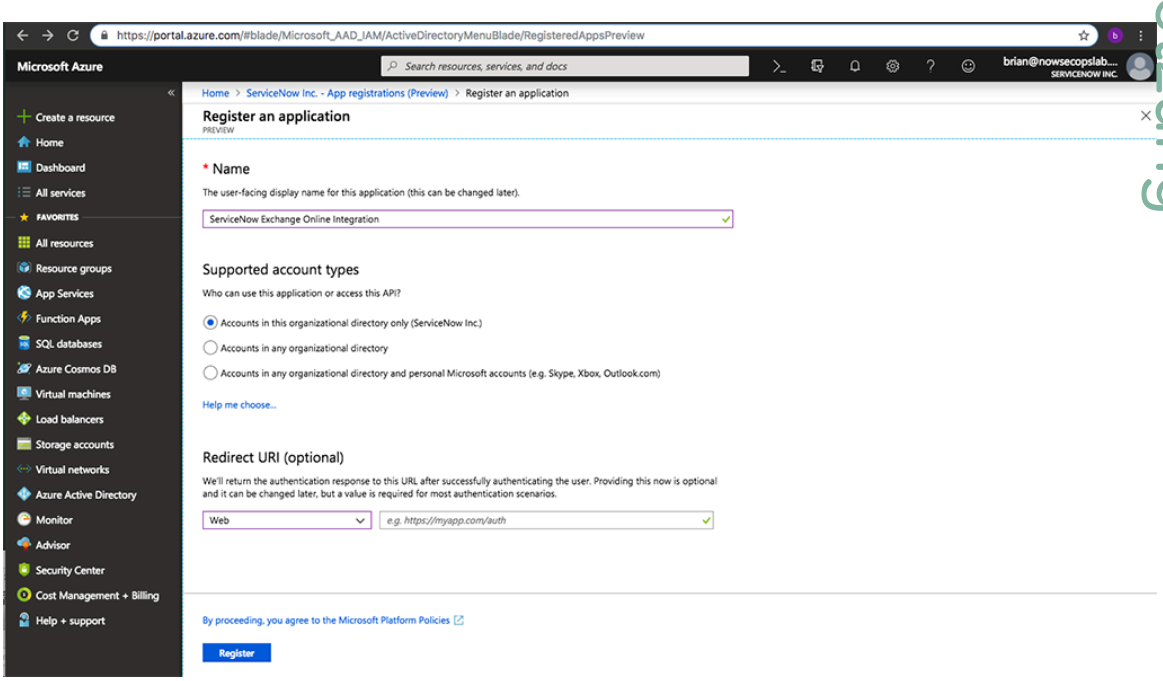
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Füllen Sie das angezeigte Formular Anwendung registrieren aus.

Ein Beispiel für ein ausgefülltes Formular wird nach der Tabelle angezeigt.

Feld	Beschreibung
Name	Name für die Anwendung. In diesem Beispiel wird ServiceNow Exchange Online Integration eingegeben.
Unterstützte Account-Typen	Klicken Sie für diesen Account unter Unterstützte Accounttypen auf **Accounts in diesem Organisationsverzeichnis (nur ServiceNow Inc.)**. Diese Domäne wird für E-Mail-Suchen verwendet.
Umleitungs-URL (optional)	Wenn Sie einen Wert für dieses Feld eingeben, wird es von der Integration nicht verwendet.

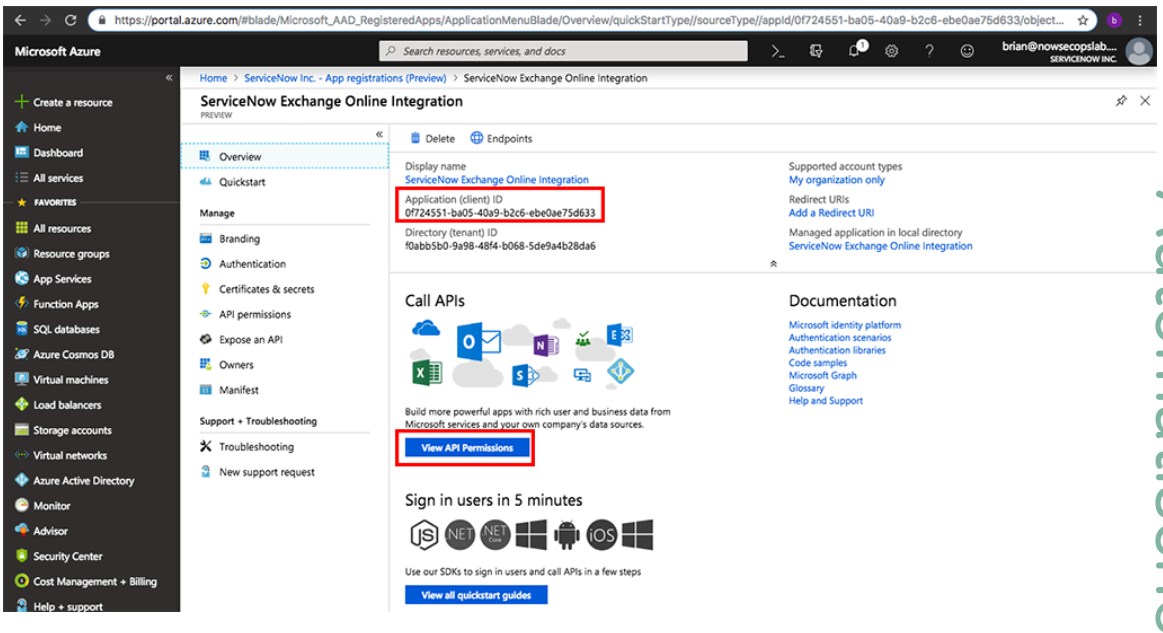


Automatische Übersetzung

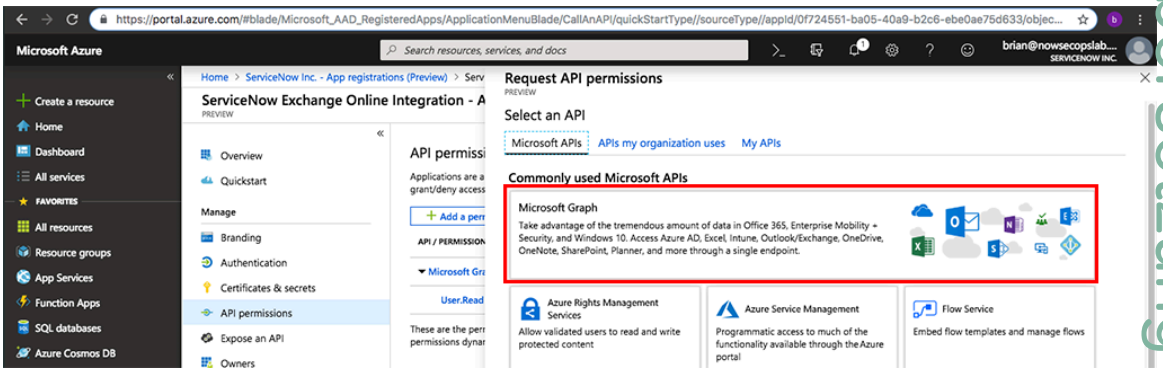
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Klicken Sie auf **registrieren**.
Eine Anwendungs-ID wird erstellt. Diese ID ähnelt einem Anwendernamen. Sie geben diesen Wert auf der Konfigurationsseite im Feld **OAuth-Anwendungs-ID** während des Konfigurationsschritts in Ihrer Instanz Now Platform ein, der in Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform .beschrieben wird.

g. Klicken Sie bei angezeigter Anwendungs-ID (Client) im Bereich ServiceNow Exchange Online-Integration **auf API-Berechtigungen anzeigen**.



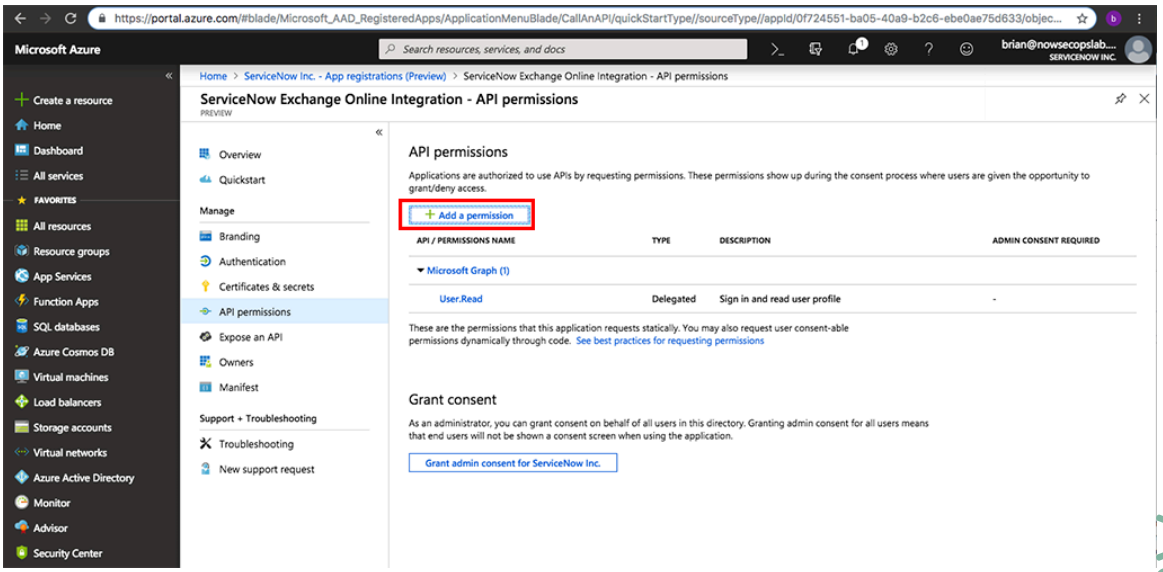
h. Klicken Sie im angezeigten Bereich „API-Berechtigungen anfordern“ auf **Microsoft Graph**.



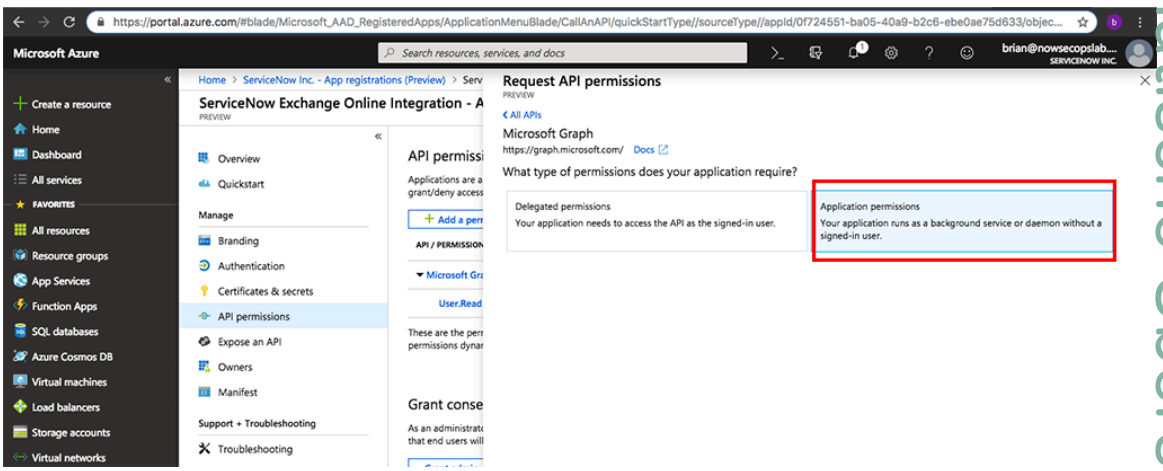
i. Klicken Sie im angezeigten Bereich ServiceNow Exchange Online-Integration – API-Berechtigungen auf **Add a Permission (Berechtigung hinzufügen)**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



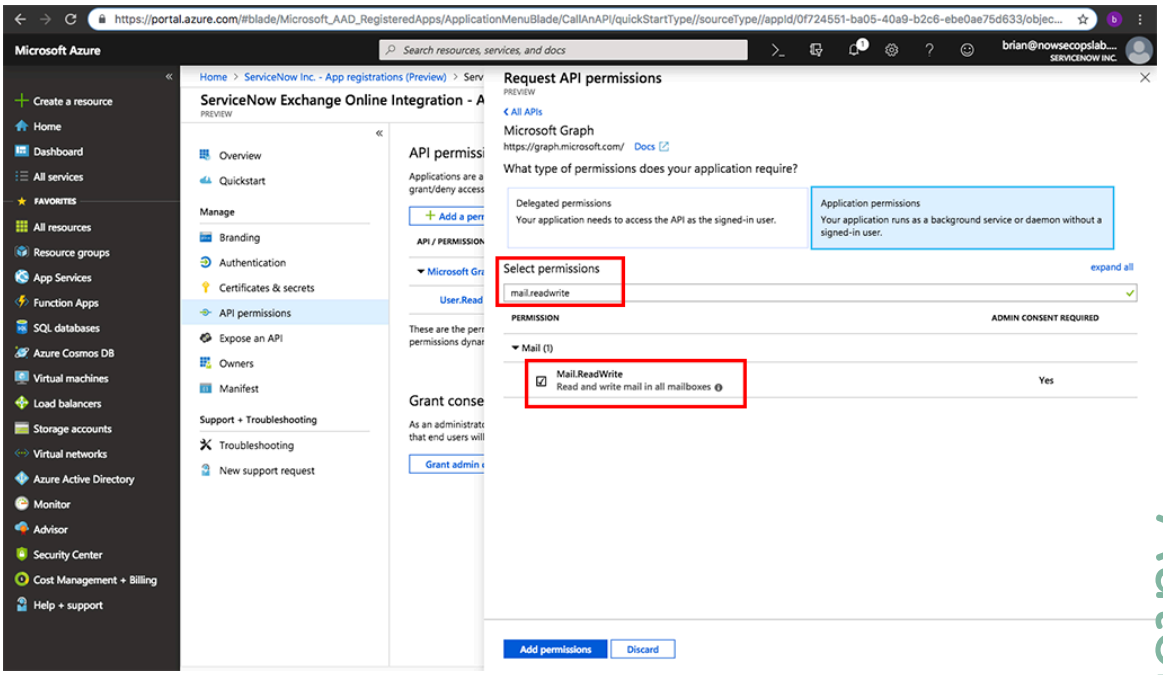
j. Klicken Sie im angezeigten Fenster „API-Berechtigungen anfordern“ **auf Anwendungsberechtigungen**.



k. Geben Sie im Feld Berechtigungen auswählen, das angezeigt wird, **Mail.ReadWrite** ein, und aktivieren Sie das Kontrollkästchen **Mail.ReadWrite**.

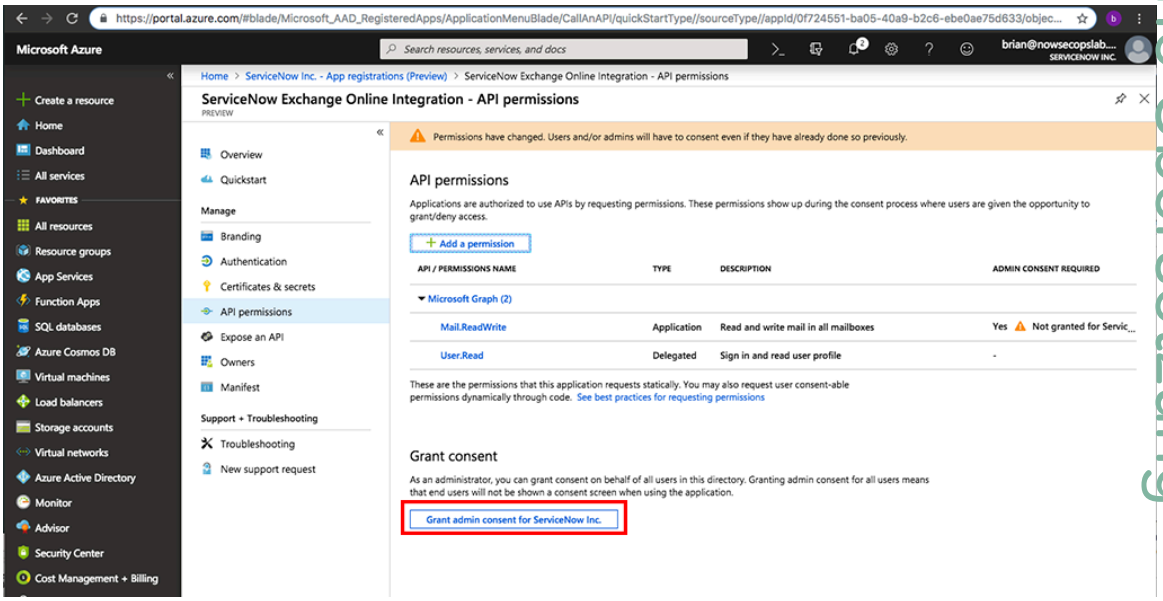
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



l. Klicken Sie auf **Berechtigungen hinzufügen**.

m. Klicken Sie im angezeigten Bereich ServiceNow Exchange Online-Integration – API-Berechtigungen **auf Admin-Zustimmung gewähren für**<your organization name> .

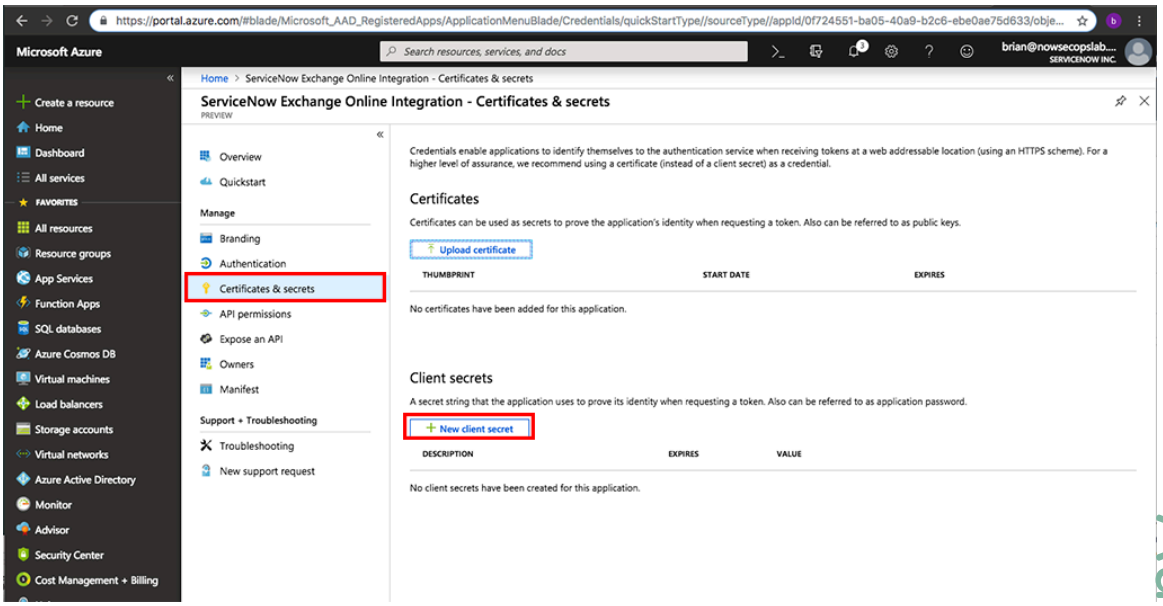


n. Um die zuvor eingegebene API-Auswahl (MicrosoftMicrosoft Azure Event Hubs Graph API) zu bestätigen, klicken Sie auf **Bestätigen**.

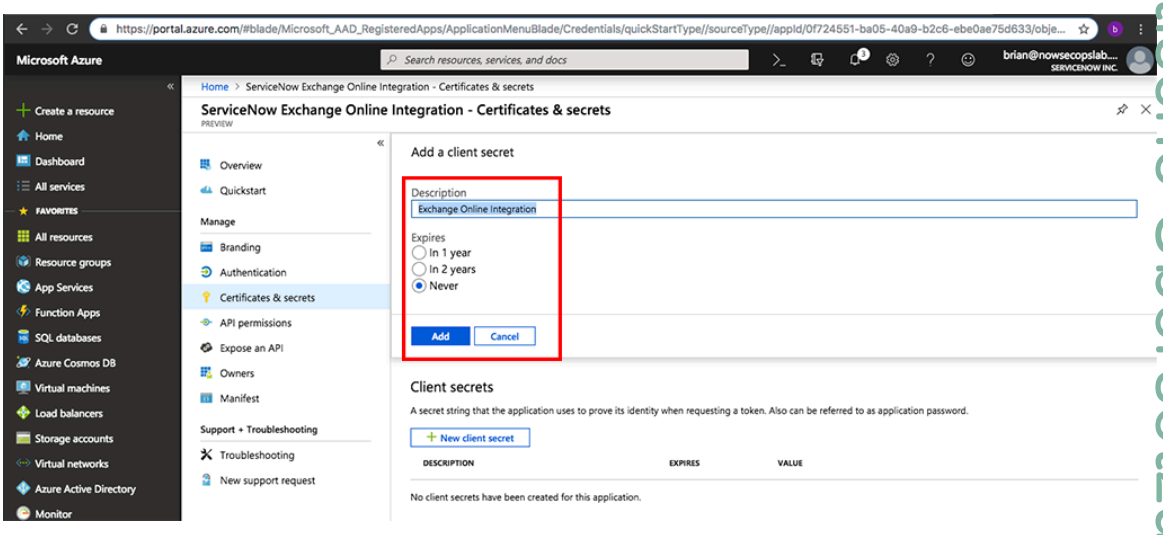
o. Klicken Sie im Bereich ServiceNow Exchange Online-Integration – Zertifikate und Geheimnisse auf **Zertifikate und Geheimnisse** und anschließend auf **Neuer geheimer Clientschlüssel** (Passwort).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



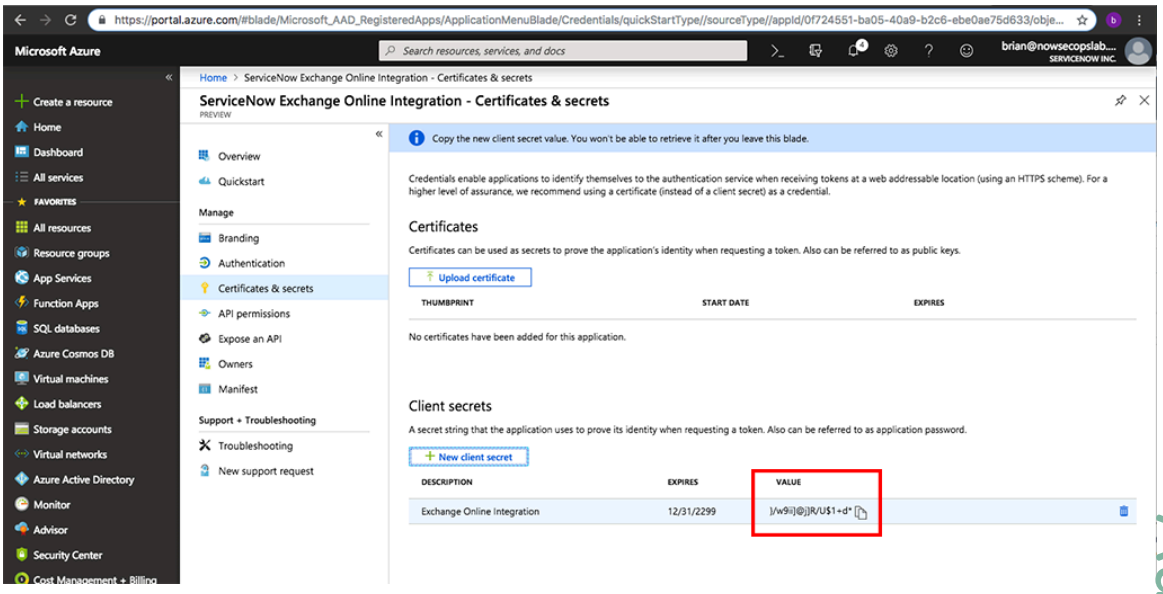
p. Geben Sie im Formular, das im Bereich ServiceNow Exchange Online-Integration – Zertifikate und Geheimnisse angezeigt wird, im Feld Beschreibung den Namen der Anwendung ein, klicken Sie auf eine Option für Ablauf und klicken Sie auf **Hinzufügen**.



Im angezeigten Bereich Zertifikate und Geheimnisse im Abschnitt **Client-Geheimnisse** unter Wertwird die Zeile mit dem neuen Client-Geheimnis (Passwort) ausgefüllt. Speichern Sie dieses Passwort an einem sicheren Ort. Nachdem Sie diese Seite verlassen haben, ist dieser Passwortwert nicht mehr sichtbar. Dieses Passwort geben Sie auf der Konfigurationsseite während des Konfigurationsschritts für die Integration in Ihrer Instanz Now Platform im Feld **OAuth-Client-Geheimnis** ein. Die Konfigurationsschritte für die Integration sind unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform .beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie haben erfolgreich eine Anwendungs-ID für die OAuth-Authentifizierung im Azure-Portal MicrosoftMicrosoft Azure Event Hubs erstellt.

Nächste Maßnahme

Sie sind bereit, Ihre Instanz Now Platform® für die Integration einzurichten.

Richten Sie die zertifikatbasierte Authentifizierung oder die Nur-App-Authentifizierung ein

Für die Authentifizierung mithilfe von Anwendungsobjekten ist ein anfängliches Onboarding erforderlich. Anwendung und Serviceprinzipal werden austauschbar verwendet, aber eine Anwendung ist wie ein Klassenobjekt, während ein Serviceprinzipal eine Instanz der Klasse ist.

Weitere Informationen zu Anwendungs- und Serviceprinzipalobjekten in Azure Active Directory finden Sie unter Anwendungs- und Serviceprinzipalobjekte in Azure Active Directory . Einen detaillierten visuellen Flow zum Erstellen von Anwendungen in Azure AD finden Sie unter Azure Active Directory-Anwendung und -Serviceprinzipal erstellen, die auf Ressourcen zugreifen können .

Um die zertifikatbasierte oder die App-reine Authentifizierung einzurichten, gehen Sie wie folgt vor:

1. Registrieren Sie die Anwendung in Azure AD.
2. Weisen Sie der Anwendung API-Berechtigungen zu.

   Damit das Anwendungsobjekt auf -Ressourcen zugreifen kann, muss es über die Anwendungsberechtigung `Exchange.ManageAsApp` und `Mail.ReadWrite`verfügen.

3. Generieren Sie ein selbstsigniertes Zertifikat, und gewähren Sie Zugriff auf den privaten Schlüssel.

   Erstellen und konfigurieren Sie ein selbstsigniertes X.509-Zertifikat, das zur Authentifizierung Ihrer Anwendung bei Azure AD verwendet wird, während das Nur-App-Zugriffstoken angefordert wird. Next Generation-Zertifikate (CNG) werden für die reine App-Authentifizierung mit Exchange nicht unterstützt. CNG-Zertifikate werden in modernen Windows-Versionen standardmäßig erstellt. Sie müssen ein Zertifikat von einem CSP-Schlüsselanbieter verwenden. (`-Provider = 'Microsoft Starker Kryptografieanbieter'`).

4. Hängen Sie das Zertifikat an die Azure AD-Anwendung an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Weisen Sie der Anwendung Azure AD-Rollen zu.

   Der Anwendung muss die Azure AD-Rolle „Compliance-Administrator“ zugewiesen sein.

6. Erstellen Sie einen neuen Serviceprinzipal.

Schritt 1: Registrieren der Anwendung in Azure AD

1. Öffnen Sie das Azure AD-Portal .
2. Geben Sie im **Suchfeld** oben auf der Seite **App-Registrierungen**ein.
3. Wählen Sie in den Ergebnissen im Abschnitt „Services“ **die Option App-Registrierungen** aus.

   Alternativ können Sie mithilfe von https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade zur **App-Registrierungsseite**navigieren.

4. Wählen Sie auf der Seite **„App-Registrierungen“Neue Registrierung**aus.
5. Konfigurieren Sie auf der Seite**„Anwendung registrieren“** die folgenden Einstellungen:

Feld	Beschreibung
Name	Geben Sie etwas Beschreibendes ein. Beispiel: ExO PowerShell CBA.
Unterstützte Account-Typen	Stellen Sie sicher, dass **nur Accounts in diesem Organisationsverzeichnis** (<YourOrganizationName> ist ausgewählt . Um die Anwendung für delegierte Exchange Online-Szenarien mehrinstanzenfähig zu machen, wählen Sie den Wert Accounts in jedem Organisationsverzeichnis (Beliebiges Azure AD-Verzeichnis – Mehrinstanzenfähig) aus.

6. Wählen Sie nach Abschluss der App-Registrierung **Registrieren** aus, und schließen Sie die App-Seite.

Schritt 2: Weisen Sie der Anwendung API-Berechtigungen zu

Die Verfahren in diesem Abschnitt ersetzen alle Standardberechtigungen, die automatisch für die neue App konfiguriert wurden. Die App benötigt die Standardberechtigungen nicht, die ersetzt wurden.

1. Wählen Sie auf der App-Seite **Manifest** unter Verwaltung.
2. Suchen Sie auf der Seite „Manifest“ nach dem Eintrag „requiredResourceAccess“ (in oder um Zeile 47).
3. Ändern Sie die Werte für resourceAppId, resourceAccess idund resourceAccess type wie im folgenden Codeausschnitt gezeigt:

```
"requiredResourceAccess": [
 {
  "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "resourceAccess": [
   {
    "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
    "type": "Role"
   }
  ]
 },
 {
  "resourceAppId": "00000003-0000-0000-c000-000000000000",
  "resourceAccess": [
   {
    "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
    "type": "Role"
   }
  ]
 }
],
```

4. Wählen Sie **Speichern**.
5. Wählen Sie auf der **Manifest** -Seite unter Verwaltung **die Option API-Berechtigungen** aus.
6. Füllen Sie die Felder auf der Seite **„API-Berechtigungen“** aus.

Feld	Beschreibung
API-/Berechtigungsname	Überprüfen Sie, ob der Wert „Exchange.ManageAsApp and Mail.ReadWrite“ angezeigt wird.
Status	Der derzeit falsche Wert ist **„Nicht gewährt für“.**<Organization> , und dieser Wert muss geändert werden. Wählen Sie **Administratorzustimmung erteilen für aus**<Organization> , lesen Sie den Bestätigungsdialog, der geöffnet wird, und wählen Sie **Ja**aus. Der Statuswert sollte jetzt **Gewährt für lauten**<Organization> .

7. Schließen Sie die aktuelle API-Berechtigungsseite (nicht die Registerkarte im Browser), um zur Seite für die App-Registrierungen zurückzukehren.

Schritt 3: Generieren Sie ein selbstsigniertes Zertifikat, und gewähren Sie Zugriff auf den privaten Schlüssel

Erstellen Sie ein selbstsigniertes x.509-Zertifikat, indem Sie wie folgt vorgehen:

- Verwenden Sie die Cmdlets New-SelfSignedCertificate , Export-Certificate und Export-PfxCertificate in einer Windows PowerShell-Sitzung mit erhöhten Rechten (als Administrator ausführen), um ein selbstsigniertes Zertifikat anzufordern und in .cer und .pfx (standardmäßig SHA1) zu exportieren. Zum Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
# Create certificate
$mycert = New-SelfSignedCertificate -DnsName "snowsecops.onmicrosoft.com"
 -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(2) -KeySpec
 KeyExchange -Provider "Microsoft Strong Cryptographic Provider"

# Generate password fro private key
$mypwd = ConvertTo-SecureString -String '<password>' -Force -AsPlainText

# Export certificate to .pfx file
$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $mypwd

# Export certificate to .cer file
$mycert | Export-Certificate -FilePath mycert.cer
```

- Gewähren Sie dem MID-Serviceanwender Zugriff mit dem privaten Schlüssel, indem Sie die folgenden Schritte ausführen:

  1. Öffnen Sie **die MMC (Microsoft Management Console)**.
  2. Navigieren Sie in der Microsoft Management Console (MMC) zu **Zertifikate (lokaler Computer)** > **Persönlich** > **Zertifikate**.

     (Wenn MMC kein Menüelement hat, fügen Sie es hinzu, indem Sie zu navigieren **Datei** > **Snap-in „Hinzufügen/Entfernen“**.
  3. Klicken Sie mit der rechten Maustaste auf das von Ihnen generierte Zertifikat.
  4. Erweitern **Alle Aufgaben** > **Private Schlüssel verwalten**
  5. Fügen Sie den **MID-Serviceanwender** der Liste der Zugriffsberechtigten hinzu.

Schritt 4: Hängen Sie das Zertifikat an die Azure AD-Anwendung an

Nachdem Sie das Zertifikat bei Ihrer Anwendung registriert haben, können Sie den Fingerabdruck zur Authentifizierung verwenden.

1. Wählen Sie auf der Registerkarte **Eigene Anwendungen** auf der Seite **„Apps-Registrierung“** am Ende von Schritt 2 Ihre Anwendung aus.

   Wenn Sie zur Registrierungsseite **für Apps** zurückkehren müssen, verwenden Sie https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/%7E/RegisteredApps , vergewissern Sie sich, dass die Registerkarte **Eigene Anwendungen** ausgewählt ist, und wählen Sie dann Ihre Anwendung aus.
2. Wählen Sie **Zertifikate und Geheimnisse** unter Verwalten aus.
3. Wählen Sie auf der Seite **„Zertifikate und Geheimnisse“**, die sich öffnet, **Zertifikat hochladen**aus.
4. Navigieren Sie zu dem selbstsignierten Zertifikat (`.cer`- Datei), das Sie in Schritt 3erstellt haben.
5. Wählen Sie nach Abschluss **Hinzufügen aus**.

   Das Zertifikat wird jetzt im Abschnitt „Zertifikate“ angezeigt.
6. Notieren Sie sich `CertificateThumbprint`, und schließen Sie die aktuelle Seite **für Zertifikate und Geheimnisse**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt 5: Weisen Sie der Anwendung Azure AD-Rollen zu

1. Öffnen Sie das Azure AD-Portal .
2. Suchen Sie im **Suchfeld** oben auf der Seite nach **Rollen und Administratoren**.
3. Wählen Sie aus den Ergebnissen im Abschnitt „Services“ **Azure AD-Rollen und -Administratoren** aus.

   Alternativ können Sie mithilfe von https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade zur Seite für **Azure AD-Rollen und Administratoren**navigieren.
4. Suchen Sie auf der Seite **„Azure AD-Rollen und Administratoren“** eine der unterstützten Rollen, und wählen Sie sie aus, indem Sie in den Ergebnissen auf den Namen der Rolle (nicht auf das Kontrollkästchen) klicken.

   Suchen Sie die Rolle **Compliance-Administrator**, und wählen Sie sie aus.
5. Wählen Sie auf der Seite **„Zuweisungen“Zuweisung hinzufügen**.
6. Suchen Sie im Popup-Fenster „ **Zuweisungen hinzufügen“** die App, die Sie in Schritt 1erstellt haben, und wählen Sie sie aus.
7. Wählen Sie nach Abschluss **Hinzufügen aus**.
8. Kehren Sie zur Seite **„Zuweisungen“** zurück, und vergewissern Sie sich, dass die Rolle der App zugewiesen wurde.

Schritt *6*: Erstellen Sie einen neuen Serviceprinzipal

Wichtig:
Stellen Sie sicher, dass eine Verbindung zu **Security & Compliance PowerShell** hergestellt wurde, bevor Sie die Schritte zum Erstellen eines neuen Serviceprinzipals ausführen. Das Erstellen eines neuen Serviceprinzipals ohne Verbindung mit PowerShell funktioniert nicht (Ihre Azure-App-ID und Objekt-ID sind erforderlich, um das neue Serviceprinzipal zu erstellen).

1. Führen Sie den folgenden Befehl aus, um die Details der Azure-Anwendung zu speichern, die Sie in Schritt 1 registriert haben (<AppName>) in einer Variablen:

```
Install-Module -Name AzureAD
Import-Module -Name AzureAD
Connect-AzureAD
$AADApp = Get-AzureADServicePrincipal -SearchString"<AppName>"
```

   Ausführliche Informationen zu Syntax und Parametern finden Sie unter Get-AzureADServicePrincipal .
2. Stellen Sie im selben PowerShell-Fenster eine Verbindung zu Security & Compliance PowerShell her :

```
Import-Module ExchangeOnlineManagement
Connect-IPPSSession -CertificateThumbPrint "<Your_Certificate_ThumbPrint>" -AppID
 $AADApp.AppId -Organization "<Your_organization>
```

   Führen Sie die folgenden Befehle aus, um ein Dienstprinzipalobjekt für die Azure-Anwendung zu erstellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
New-ServicePrincipal -AppId $AADApp.AppId -ObjectId $AADApp.ObjectId -DisplayName
"<Descriptive Name>"
```

Detaillierte Syntax- und Parameterinformationen finden Sie unter New-ServicePrincipal .

Richten Sie Ihre Instanz Now Platform® für die Integration Microsoft Exchange Online ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in der Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung Microsoft Exchange Online installieren. Sehen Sie sich die Prüfliste an, und vergewissern Sie sich, dass Sie diese Aufgaben abgeschlossen haben, bevor Sie die Anwendung Microsoft Exchange Online für die Integration herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

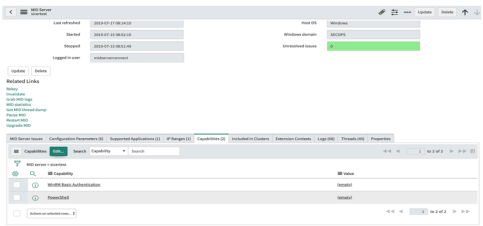
Vorbereitungen

Setupaufgabe	Beschreibung
Vergewissern Sie sich, dass die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen wurden.	Die folgenden ServiceNow Rollen sind erforderlich: • Der Systemadministrator (admin) installiert Anwendungen und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) konfiguriert die Anwendung für die Integration. Bei Bedarf weist die Rolle des Security Incident-Administrators dem Security Incident-Analysten (sn_si.analyst) auch die E-Mail-Lese- und Schreibrollen (sn_sec_cmn.cap_email_write und sn_sec_cmn.cap_email_read) zu. Die Rollen (sn_sec_cmn.cap_email_read) und (com.snc.security_incident) werden mit dem Produkt Security Incident Response installiert. Sie sind dem Security Incident-Administrator standardmäßig zugewiesen und können bei Bedarf neu zugewiesen werden. • Der Security Incident-Analyst (sn_si.analyst) führt E-Mail-Suchen durch und löscht E-Mails. Diese Rolle verifiziert auch, ob E-Mails gelöscht wurden, und arbeitet mit Security Incidents. ○ Die Schreibrolle ermöglicht dem sn_si.analyst das Bearbeiten, Erstellen und Durchführen von E-Mail-Suchen sowie das Löschen von Nachrichten. Zum Löschen von Nachrichten ist keine separate Rolle erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	○ Mit der Leserolle kann der sn_si.analyst die Ergebnisse in zugehörigen Listen für Security Incidents anzeigen. **Hinweis:** Der sn_si.analyst muss über die Rollen (sn_sec_cmn.cap_email_read) und (sn_sec_cmn.cap_email_write) verfügen, um E-Mail-Suchergebnisse anzuzeigen und E-Mail-Suchabfragen zu erstellen und durchzuführen. Wenn die Rollen (sn_sec_cmn.cap_email_read) und (sn_sec_cmn.cap_email_write) dem Security Incident-Analysten nicht zugewiesen werden. Weitere Informationen zum Zuweisen von Rollen in Security Incident Responsefinden Sie unter Mit SIR installierte Rollen.
Stellen Sie sicher, dass Sie einen Windows MID-Server in Ihrer Now Platform -Instanz eingerichtet haben.	Der MID Server wird in Ihrer Umgebung Now Platform benötigt. Obwohl sowohl das Produkt Microsoft Exchange Online als auch Now Platform Cloud-Angebote sind, ist für diese Integration ein MID-Server erforderlich. Das PowerShell-Skript wird von einem Server Windows in der Kundenumgebung ausgeführt, um über einen MID-Server eine Verbindung zum Server Microsoft Exchange Online herzustellen. Ab Version 10.5 der Integration Microsoft Exchange Online für Security Operations müssen Sie das Exchange Online PowerShell V2-Modul im MID Server installieren. Weitere Informationen finden Sie in der Microsoft-Dokumentation zum Exchange Online PowerShell V2-Modul . Eine ausgehende HTTPS-Verbindung vom MID-Server ist erforderlich, damit die Integration Informationen vom Servicemandanten Microsoft Exchange Online abrufen kann. Weitere Informationen zum MID-Server finden Sie unter MID-Server Sie testen die Verbindung zwischen Ihrer -Instanz und dem Windows-MID-Server, nachdem Sie die Anwendung während des Konfigurationsschritts der Integration installiert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

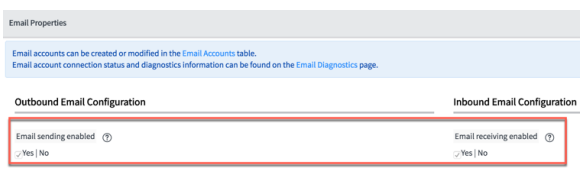
Setupaufgabe	Beschreibung
Richten Sie Windows MID-Server für die Verarbeitung von Microsoft Exchange Online -Abfragen ein	• Richten Sie die zertifikatsbasierte Exchange Online-Authentifizierung für MID Serversein. • Weisen Sie den festgelegten MID-Servern die zertifikatbasierte Exchange Online-Authentifizierung und PowerShell-Funktionen zu.
	
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Das Plugin Security Incident Response „ Dependency (com.snc.si_dep) ist erforderlich und installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.

Wenn Sie in Ihrer aktuellen MID-Server-Umgebung die Funktionen für jeden MID-Server auf **ALLE** festgelegt haben, wird die **zertifikatbasierte Exchange Online-Authentifizierung** automatisch für alle MID-Server hinzugefügt. In diesem Fall kann jeder der MID-Server in Ihrer Umgebung Anforderungen für Microsoft Exchange Online die -Integrationssuche empfangen.

Um sicherzustellen, dass die Suchanforderungen nur an die festgelegten MID-Server gesendet werden, und um eine falsche Weiterleitung der Suche zu verhindern, klicken Sie auf **Bearbeiten** und gehen Sie wie folgt vor:

- Entfernen Sie die Fähigkeit **„ALLE“** von jedem MID-Server, der nicht über die erforderliche **zertifikatbasierte Authentifizierungsfunktion für Exchange Online** verfügt.
- Wählen Sie die erforderlichen Fähigkeiten aus (siehe unten), und klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	1. Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.
Wenn Ihre Organisation E-Mail-Benachrichtigungen vom Now Platform Typ verwenden möchte, vergewissern Sie sich, dass die Funktion zum Senden/Empfangen von E-Mails aktiviert ist.	Führen Sie diese Schritte aus, um sicherzustellen, dass die Funktion zum Senden und Empfangen von E-Mails in Ihrer Instanz Now Platform® aktiviert ist. Diese Funktion benachrichtigt Benutzer per E-Mail, wenn Such- und Löschanforderungen initiiert und erfolgreich abgeschlossen wurden. **1.** Navigieren zu **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**. **2.** Überprüfen Sie unter Konfiguration ausgehender E-Mails, ob E-Mail-Versand aktiviert und Empfangen von E-Mail aktiviert sind. Diese Funktion zum Senden/Empfangen von E-Mails ist erforderlich, damit Ihr Security Incident-Analyst E-Mail-Benachrichtigungen erhält, die von Now Platform®gesendet werden. Wenn die Funktion zum Löschen der Genehmigung aktiviert ist, werden Anforderungen zum Löschen von E-Mails auch per E-Mail an genehmigende Personen gesendet. Außer der Aktivierung dieser E-Mail-Eigenschaft ist kein weiteres Setup erforderlich, um E-Mails in Now Platform®zu senden und zu empfangen.
	

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Als Security Incident-Administrator Now Platform für (sn_si.admin) werden Ihnen die Rollen zum Lesen und Schreiben von E-Mails (sn_sec_cmn.cap_email_read) und (sn_sec_cmn.cap_email_write) automatisch zugewiesen, wenn Sie das Produkt Security

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

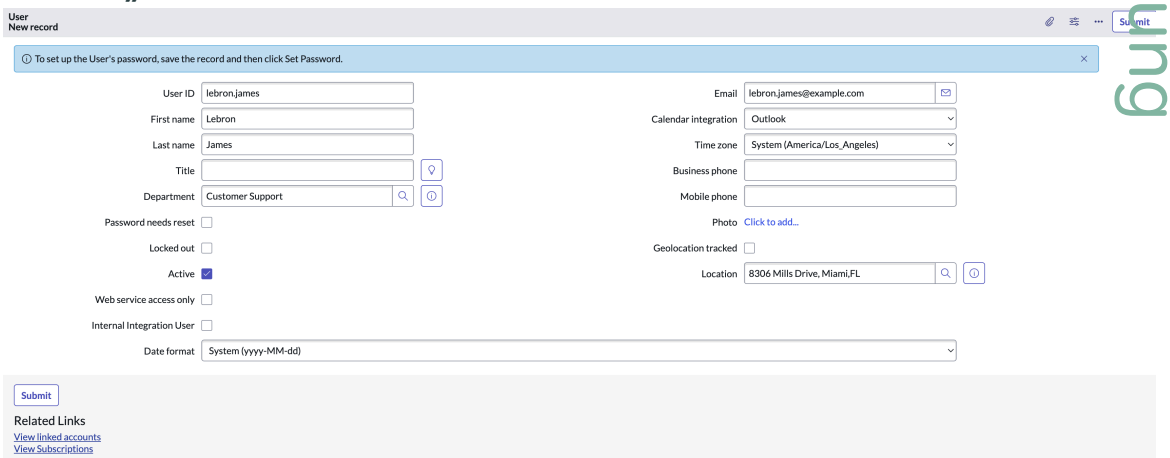
Incident Response (SIR) herunterladen. Als Security Incident-Administrator weisen Sie diese Rollen dem Security Incident-Analysten (sn_si.analyst) oder einer anderen Rolle zu. Wenn Sie diese Rollen nicht dem Security Incident-Analysten oder einer anderen Rolle zugewiesen haben, führen Sie die folgenden Schritte aus, um sie zuzuweisen.

Prozedur

1. Navigieren zu **Organisation** > **Anwender**.
2. Klicken Sie auf das Modul **Benutzer**.
   a. Klicken Sie in der angezeigten Benutzerliste auf **Neu**.
   b. Füllen Sie das angezeigte Formular für neue Anwender aus.

Feld	Beschreibung
Anwender-ID	Anwender-ID für die Rolle „Security Incident-Analyst“ Now Platform, z. B. jferguson.
E-Mail	Unternehmens-E-Mail-Adresse. An diese E-Mail-Adresse werden die Benachrichtigungen für E-Mail-Suchergebnisse und Bestätigungen für das Löschen von E-Mails gesendet. In diesem Beispiel wird jferguson@servicenow.com verwendet, aber jede Unternehmens-E-Mail-Adresse kann je nach Anforderung Ihrer Organisation zum Empfangen dieser E-Mail-Benachrichtigungen verwendet werden.
Vorname	Vorname
Nachname	Nachname
Titel	Beispiel:Security Incident-Analyst, Sicherheitsanalystoder Security Operations Center-Analyst (SOC).

Formular „Neuer Anwender“.



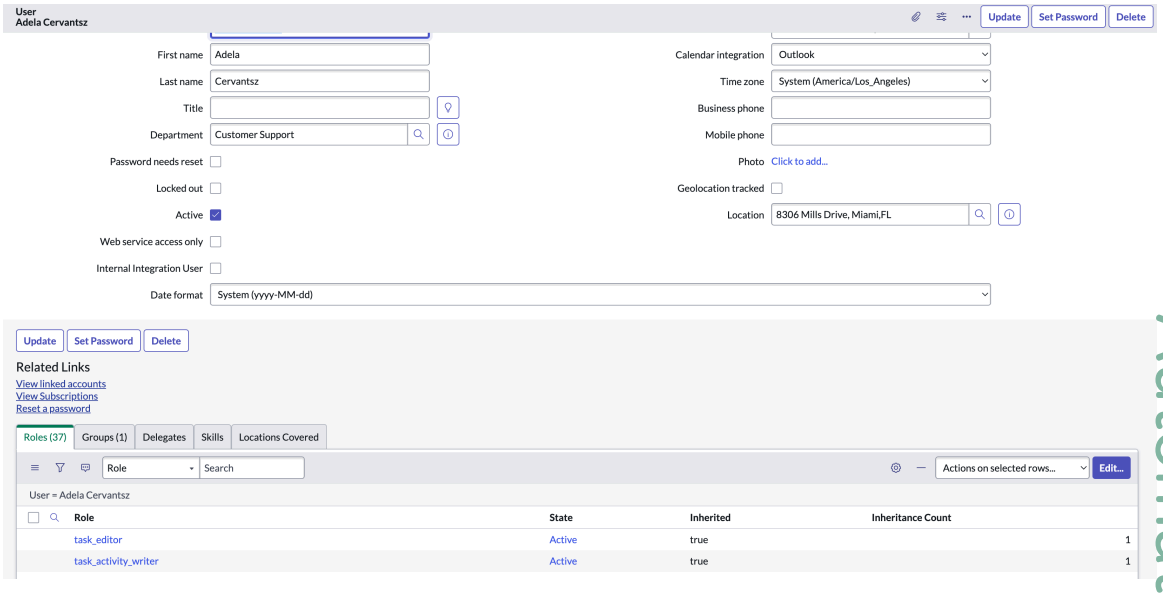
   c. Klicken Sie auf **Absenden**.
   Der neue Benutzer wird in der Benutzerliste angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie in der Liste „Benutzer“ in der Spalte „Benutzer-ID“ auf den Namen des Benutzers, dem Sie die Rollen sn_sec_cmn.cap_email_read und sn_sec_cmn.cap_email_read zuweisen möchten.
4. Klicken Sie im geöffneten Datensatz im Abschnitt „Zugehörige Links“ auf **Bearbeiten**.

Formular „Benutzer bearbeiten“.



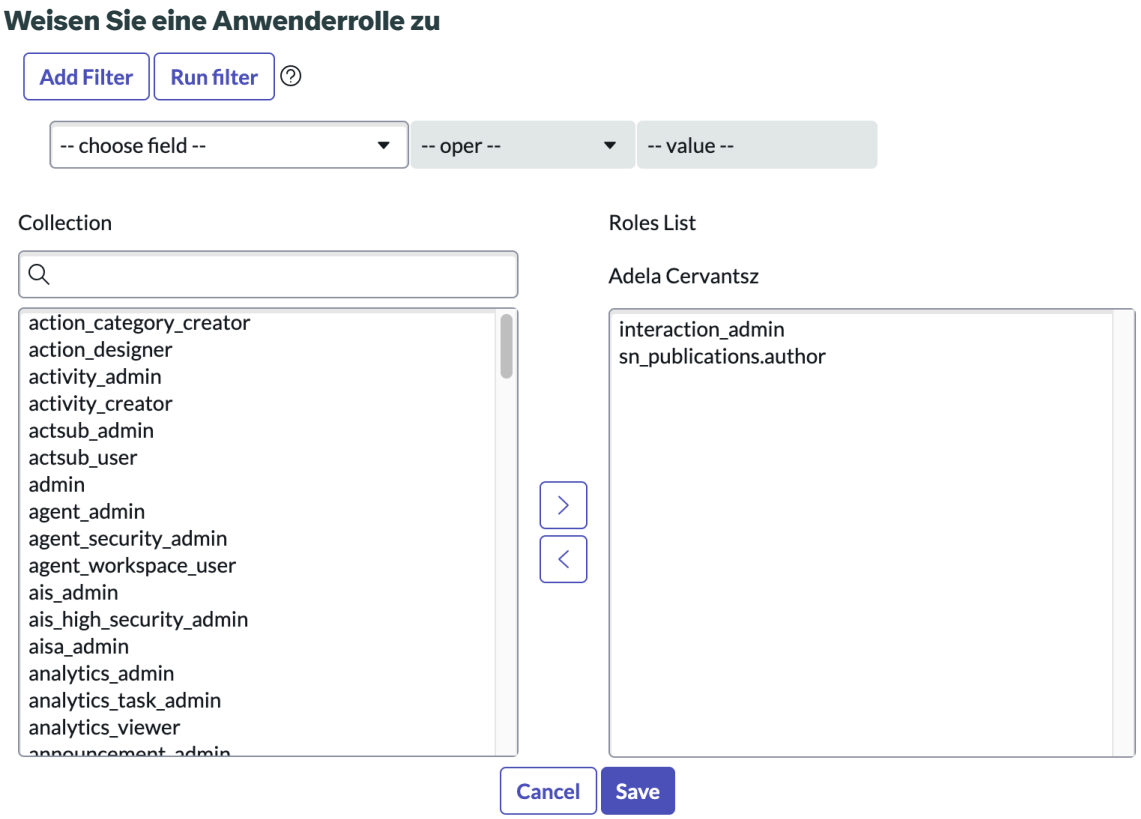
5. Geben Sie im angezeigten Formular „Mitglieder bearbeiten“ im Feld Sammlung den Wert sn_sec_cmn.cap_email_read ein.

> **Hinweis:**
> Die Spalte unter dem Feld wird automatisch ausgefüllt. Wenn dem Benutzer die Rolle sn_si.analyst nicht zugewiesen wurde, geben Sie auch sn_si.analyst im Feld Sammlung ein. In der folgenden Abbildung wurde die Rolle sn_si.analyst bereits Joe Perguson zugewiesen.

6. Wählen Sie in der Spalte Sammlung die Option aus, und verschieben Sie sn_sec_cmn.cap_email_read, sn_sec_cmn.cap_email_read und sn_si.analyst (falls nicht bereits zugewiesen) in die Rollenliste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Speichern**.
   Die Rollen `sn_sec_cmn.cap_email_read` und `sn_sec_cmn.cap_email_read` werden dem Sicherheitsanalysten (jferguson) zugewiesen.
8. Fügen Sie Anwender hinzu, und weisen Sie Rollen nach Bedarf für Ihre Organisation zu.
9. **Wahlweise:** Wenn Sie die Genehmigungsfunktion für E-Mail-Löschanforderungen aktivieren möchten, führen Sie die folgenden Schritte aus, um eine Genehmigungsgruppe zu erstellen.

   a. Navigieren zu **Anwenderadministration** > **Gruppen**.

   b. Klicken Sie in der angezeigten Liste Gruppen auf **Neu**.

   c. Füllen Sie die Felder im Formular aus.

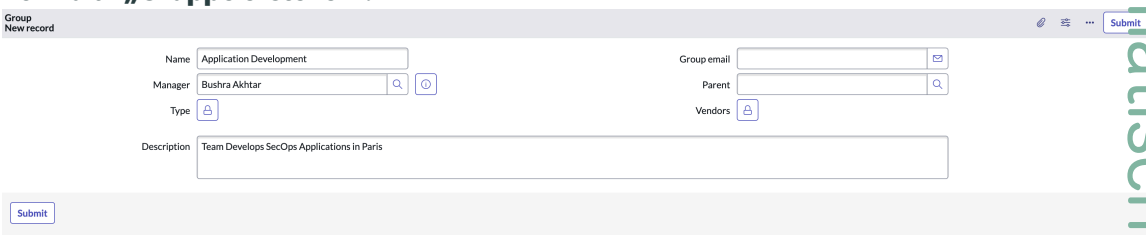
Feld	Beschreibung
Name	Name der Gruppe, die eine Genehmigung verarbeitet, wenn eine E-Mail-Löschanforderung übermittelt wird, z. B. `Exchange Online-Genehmiger`.
Gruppen-E-Mail	Geben Sie eine E-Mail-Adresse ein, wenn Sie eine Gruppen-E-Mail-Verteilerliste möchten, oder die E-Mail-Adresse des Kontaktpunkts, z. B. den Gruppenmanager. (Optional) Lassen Sie dieses Feld leer, wenn Sie möchten, dass E-Mail-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Benachrichtigungen an die einzelnen E-Mail-Adressen für jeden Anwender in der Gruppe gesendet werden.
Manager	(Optional) Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen.
Übergeordnet	(Optional) Wenn diese Gruppe ein übergeordnetes Element hat, ist dies die andere Gruppe, in der diese Gruppe Mitglied ist.
Typ	(Optional) Definieren Sie Kategorien von Gruppen.
Lieferanten	(Optional) Weisen Sie die Rolle vendor_manager Anwendern zu, die am Lieferantenverwaltungsprozess Ihrer Organisation beteiligt sind.
Beschreibung	(Optional) Zusätzliche Informationen zur Gruppe.

Formular „Gruppe erstellen“.



Weitere Informationen zum Erstellen von Gruppen und zum Zuweisen von Rollen finden Sie unter Benutzergruppen erstellen .

d. Klicken Sie auf **Absenden**.
In der Spalte Name wird die neue Gruppe in der Gruppenliste angezeigt.

Sie können dieser Gruppe weitere Anwender hinzufügen. Ein Benutzer erbt Rollen von allen Gruppen, denen er angehört. Sie können Rollen auch direkt einem Benutzer zuweisen. Weitere Informationen finden Sie unter Managing roles . Jeder Benutzer kann vom Sicherheitsanalysten übermittelte E-Mail-Löschanforderungen genehmigen. Es ist nur ein Anwender erforderlich, um die Anforderung zu genehmigen oder abzulehnen.

Wenn Ihre Organisation mit dieser Integration eine zusätzliche Kontrolle über das Löschen von E-Mails haben möchte, aktivieren Sie die optionale Genehmigungsfunktion. Aktivieren Sie während des Konfigurationsschritts auf der Registerkarte Zusätzliche Einstellungen das Kontrollkästchen **Aktivieren**, um Genehmigungen zu aktivieren. Im vorherigen Beispiel ist jeder Benutzer der Exchange Online- Genehmigergruppe verfügbar, um Löschanforderungen per E-Mail-Benachrichtigung zu verarbeiten.

Installieren Sie die Anwendung Microsoft Exchange Online für die Integration ServiceNow Microsoft Exchange Online .

Bevor Sie die Integration in Ihrer -Instanz ausführen, installieren Sie die Anwendung Microsoft Exchange Online für die Integration aus dem ServiceNow Store.

Vorbereitungen

Bevor Sie die Anwendung aus ServiceNow Store in Ihrer Instanz Now Platform installieren, führen Sie alle in den erforderlichen Prüflisten aufgeführten Aufgaben aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Administrator

Wichtig:

- Die zertifikatbasierte Microsoft Exchange Online-Authentifizierung wird ab Microsoft Exchange Online for Security Operations Version 10.5.4 unterstützt.
- Wenn Sie Demodaten installieren, wird automatisch eine Demokonfiguration ohne Anmeldeinformationen erstellt. Dies kann zu Fehlern führen. Weitere Informationen finden Sie unter KB0755880 .

Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Nachdem Sie die Anwendung aus ServiceNow Storeinstalliert haben, konfigurieren Sie sie so, dass eine Verbindung zu Ihrer Instanz Now Platform hergestellt wird.

Zugehörige Informationen

Richten Sie Ihr MicrosoftMicrosoft Azure Event Hubs Azure-Konto für die ServiceNow Microsoft Exchange Online -Integration ein

Richten Sie die zertifikatbasierte Authentifizierung oder die Nur-App-Authentifizierung ein

Richten Sie Ihre Instanz Now Platform für die Integration Microsoft Exchange Online ein

Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform .

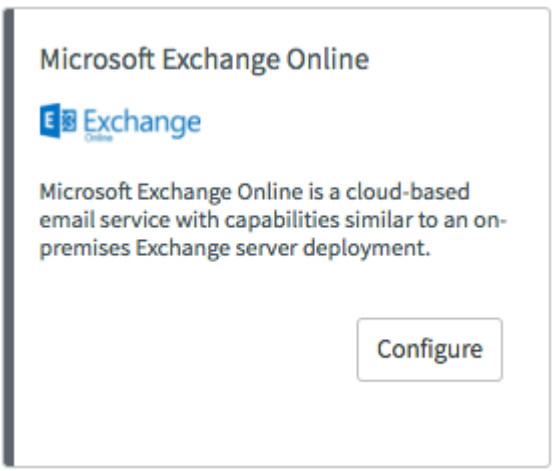
Nachdem Sie die Anwendung aus ServiceNow Storeinstalliert haben, konfigurieren Sie sie so, dass eine Verbindung zu Ihrer Instanz Now Platform hergestellt wird. Mit dieser Aktivierung werden die Such- und Lösch-Workflows aktiviert.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren Sie in Ihrer Instanz von Now Platform zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
2. Suchen Sie die Kachel Microsoft Exchange Online.
3. Klicken Sie auf **Konfigurieren**.



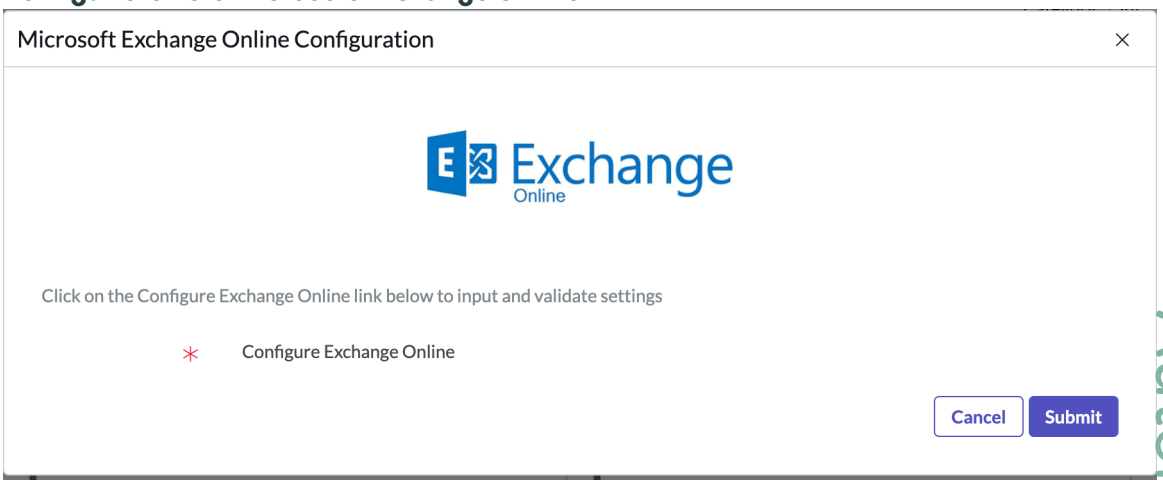
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

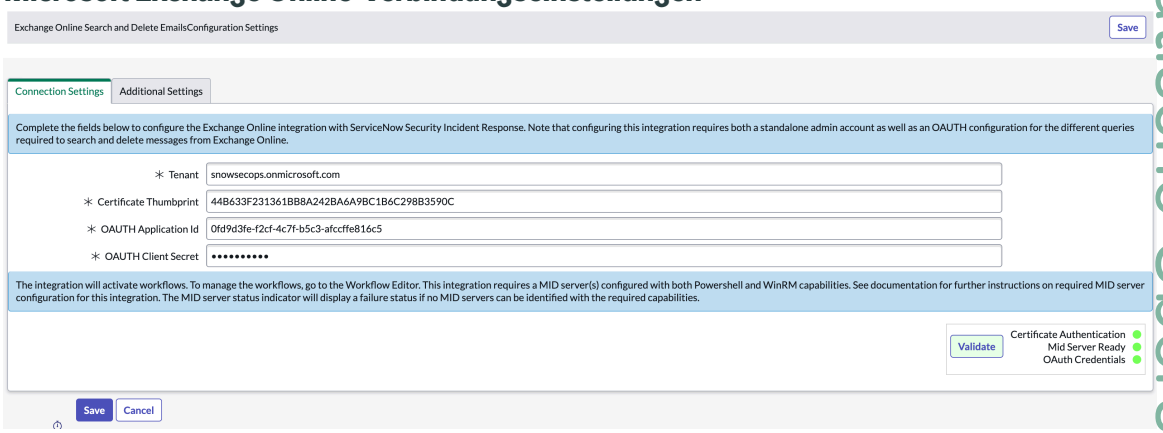
4. Klicken Sie im angezeigten Dialogfeld Microsoft Exchange Online Konfiguration **auf Exchange Online konfigurieren**.

   Ein Beispiel für ein ausgefülltes und validiertes Formular folgt der Tabelle.

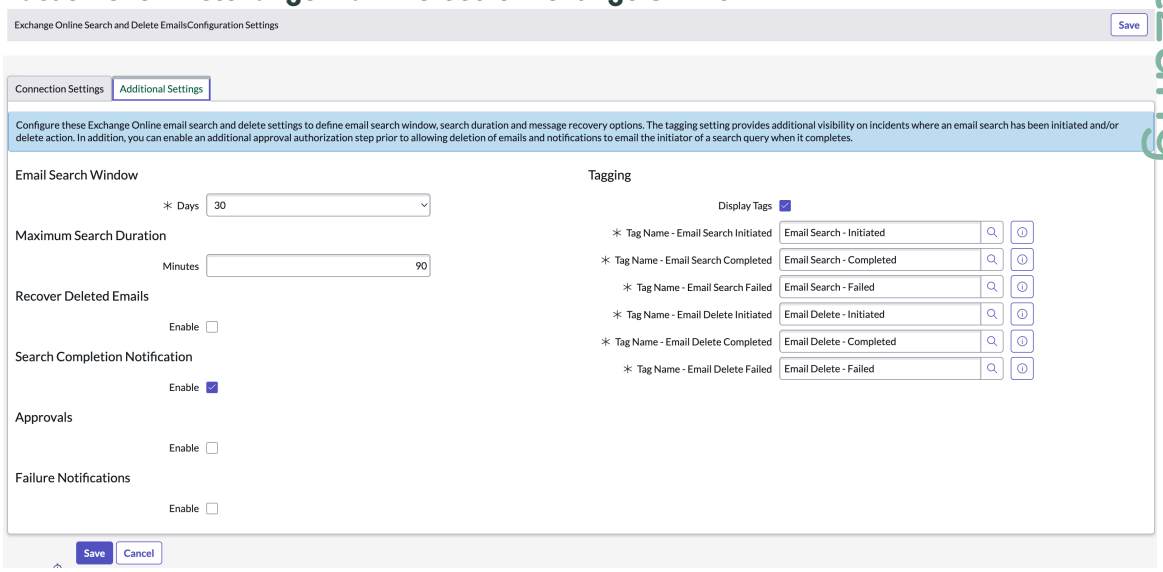
Konfigurieren Sie Microsoft Exchange Online



Microsoft Exchange Online-Verbindungseinstellungen



Zusätzliche Einstellungen für Microsoft Exchange Online



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie eine, um fortzufahren.

Trouble?
Wenn eine Fehlermeldung angezeigt wird oder einer oder mehrere Indikatoren rechts neben der Schaltfläche Validate (Validieren) rot sind, vergewissern Sie sich, dass die von Ihnen eingegebenen Anmeldeinformationen für das Benutzerkonto gültig sind. Geben Sie Ihre Anmeldeinformationen ein, und klicken Sie erneut auf **Speichern**.

Validierung nicht erfolgreich

In der folgenden Tabelle finden Sie weitere Informationen zur Schaltfläche **Validieren** und zu den Farbsymbolen.

Status der Schaltflächen und Indikatoren zum Validieren	Beschreibung
Die Schaltfläche „Validieren“ ist grün und alle kleinen farbigen Indikatoren sind grün.	Gibt an, dass die MID-Serververbindung und die Anmeldeinformationen (Zertifikatauthentifizierung und OAuth) gültig sind.
Die Schaltfläche zum Validieren ist hellrot mit einem blauen Rahmen, und mindestens ein kleiner Farbindikator ist orange.	Die Validierung wird durchgeführt. Die Validierung kann einige Minuten dauern.
Die Schaltfläche „Validieren“ ist hellrot, und mindestens einer der kleinen Farbindikatoren ist rot.	• Die Schaltfläche für die zertifikatsbasierte Authentifizierung von Exchange Online oder OAuth-Anmeldeinformationen ist rot: Gibt an, dass die zertifikatsbasierte Authentifizierung von Exchange Online oder die OAuth-Anmeldeinformationen ungültig sind. • Die Schaltflächen für die zertifikatbasierte Exchange Online-Authentifizierung und „MID-Server bereit“ sind rot: Gibt an, dass der MID-Server nicht erreichbar ist und daher die zertifikatbasierte Exchange Online-Authentifizierung über den MID-Server fehlgeschlagen ist. • Der Indikator für die zertifikatbasierte Exchange Online-Authentifizierung ist rot, die Schaltfläche „MID-Server bereit“ ist jedoch grün: Zeigt an, dass der MID-Server aktiv und ordnungsgemäß konfiguriert ist, die zertifikatbasierte Exchange Online-Authentifizierung jedoch falsch ist.

Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im Service Microsoft Exchange Online an

Definieren Sie als Benutzer mit der Rolle sn_si.analyst Suchkriterien, und senden Sie eine E-Mail-Suchanforderung basierend auf Incident-Details in einem Security Incident-Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Die Zahlen in diesem Verfahren werden mit in den Systemeinstellungen ausgewählten **Formularen mit Registerkarten** angezeigt. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt mit der Bezeichnung Formulare mit Registerkarten anzeigen in Formularlayout konfigurieren auf der Website der Produktdokumentation von ServiceNow .

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Der Status einzelner Nachrichten, die der Suchabfrage entsprechen, und die Ergebnisse der Suche werden im Security Incident-Datensatz gemeldet. Wenn E-Mail-Benachrichtigungen aktiviert sind, können Sie die Suchergebnisse aus einer E-Mail-Nachricht anzeigen.

Suchkriterien können Absenderadressen, Empfängeradressen oder Betreffnamen der Nachricht sein. Die folgenden Kombinationen aus Suchparametern für Nachrichtenbetreff, Absender und Empfänger werden häufig verwendet, um Phishing-bezogene E-Mail-Nachrichten zu finden, die Teil einer einzelnen Phishing-Kampagne sein können:

- Finden Sie alle ursprünglichen E-Mails, die von einem Phishing-Account gesendet wurden: Suche nach Absender.
- Alle ursprünglichen E-Mails für eine einzelne Phishing-Kampagne finden: Suchen Sie nach Betreff und Absender.
- Suchen Sie alle E-Mails, die für eine einzelne Phishing-Kampagne empfangen wurden (ursprüngliche und weitergeleitete E-Mails, beliebiger Absender): Suche nach Betreff.
- Alle weitergeleiteten E-Mails für eine einzelne Phishing-E-Mail von einem einzelnen Anwender finden: Suche nach Empfänger + Betreff.
- Finden Sie alle Phishing-bezogenen E-Mails, die an einen einzelnen Anwender gesendet wurden: Suchen Sie nach Absender und Empfänger.

Hinweis:
Suchen werden nach E-Mails durchgeführt, die innerhalb der letzten 30 Kalendertage gesendet oder empfangen wurden, es sei denn, während der Ersteinrichtung wurde ein kürzeres Suchfenster konfiguriert. Eine erfolgreiche E-Mail-Suche ist erforderlich, bevor Sie E-Mails löschen können.

Das folgende Beispiel zeigt, wie Sie eine Suche aus einem Security Incident Now Platform initiieren. Ein Security Incident wird basierend auf der ursprünglichen E-Mail eines mutmaßlichen Phishing-Angriffs auf dem Server Microsoft Exchange Online Ihrer Organisation erstellt. In diesem Beispiel lauten die Suchkriterien Absender (Von) plus Betreff, wobei Vonphisher@cbazyx.comund BetreffAnmelden bei Ihrem Konto lauten.

Ergebnisse für Suchen nach Themen werden zurückgegeben, wenn die Suche Textzeichenfolgen findet, die Schlüsselwörter enthalten, die den eingegebenen Suchkriterien entsprechen. In diesem Beispiel lautet der Betreff Anmelden bei Ihrem Account. Verwenden Sie den Operator **AND**, um die Suchbedingungen Von und Betreff zu trennen und Ergebnisse für alle E-Mail-Nachrichten zurückzugeben, die diese angegebenen Suchkriterien enthalten. In den folgenden Schritten wird beschrieben, wie Sie eine Suche einrichten, die nur E-Mails findet, die Betreffzeilentext enthalten, der von einem bestimmten Phishing-Account gesendet wurde.

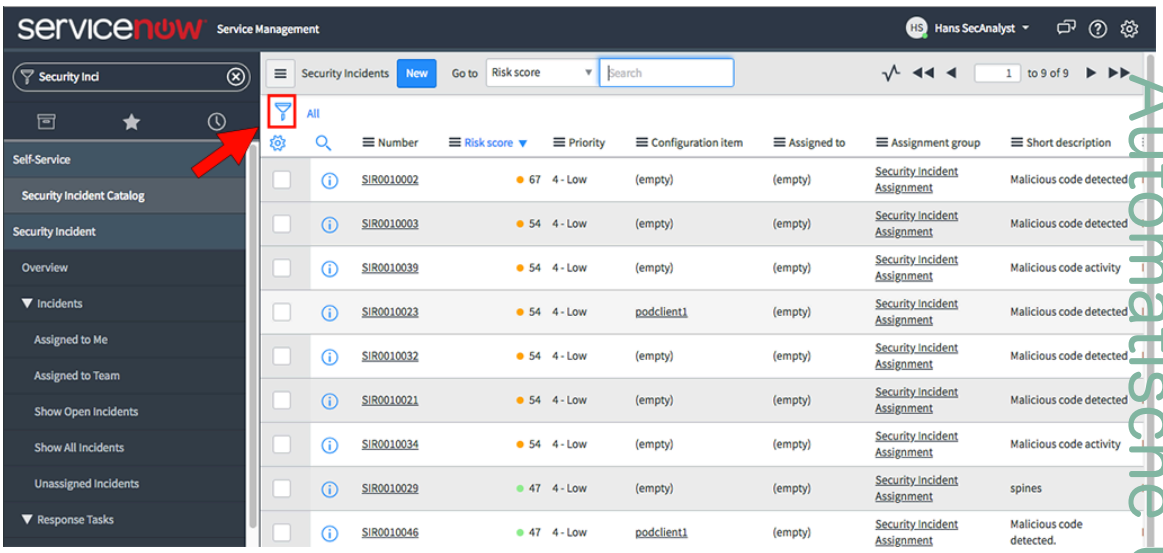
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen** und suchen Sie den Security Incident, mit dem Sie arbeiten.
2. Befolgen Sie alternativ diese Schritte, um einen Filter festzulegen und auszuführen, sodass nur Security Incidents angezeigt werden, die durch Phishing-Ereignisse erstellt wurden.

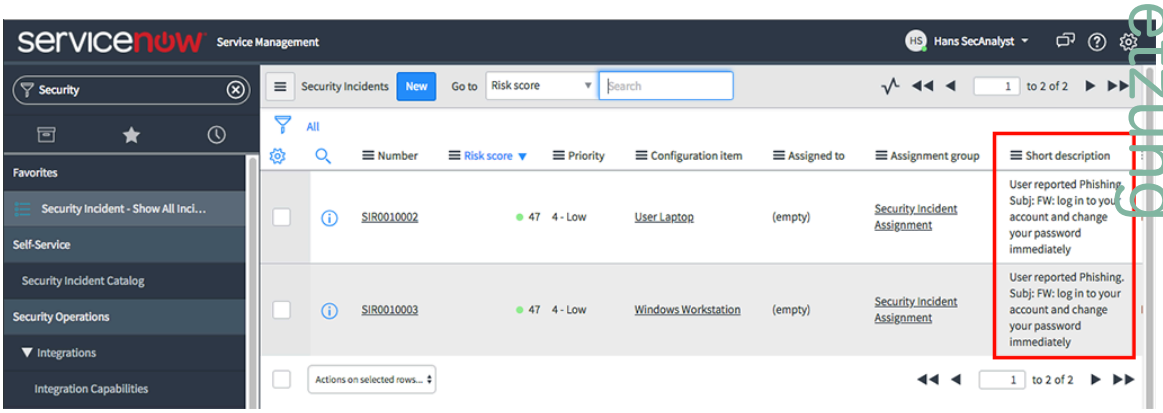
   a. Navigieren zu **Security Incident** > **Alle Incidents anzeigen** um die Liste der Security Incidents zu öffnen.

   b. Klicken Sie in der oberen linken Ecke der angezeigten Liste auf das Filtersymbol.



   c. Wählen Sie in den angezeigten Feldern aus **Kurzbeschreibung** > **enthält** Geben Sie in den Auswahllisten Vom **Anwender gemeldetes Phishing** ein, und klicken Sie auf **Ausführen**.

   Die Security Incidents im Zusammenhang mit Phishing werden angezeigt.



   d. Verwenden Sie den Text in der Spalte Kurzbeschreibung, um den Security Incident zu finden, mit dem Sie arbeiten.

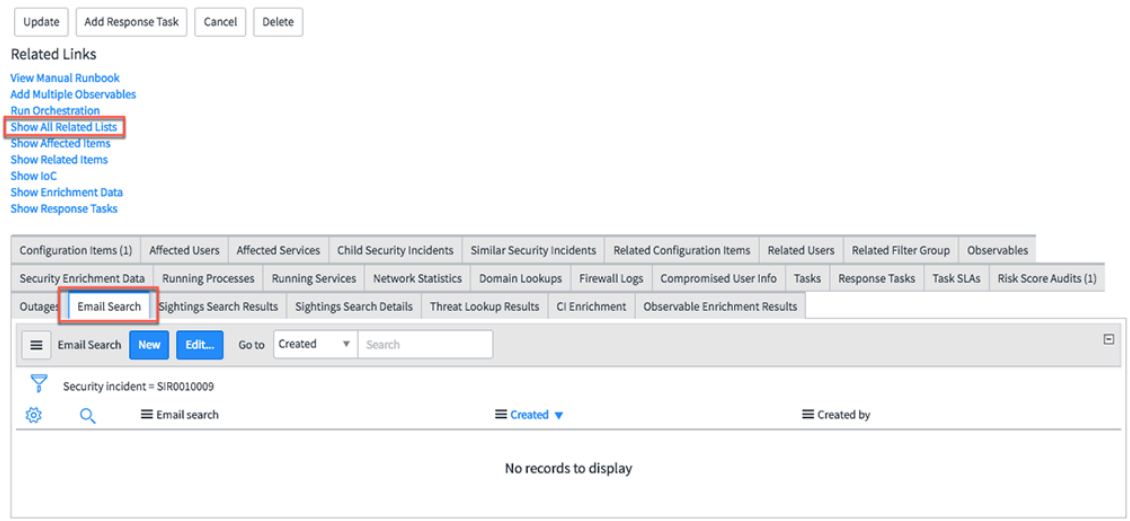
   e. Klicken Sie in der Spalte Nummer auf einen Security Incident, um einen Datensatz zu öffnen.

3. Scrollen Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf die zugehörige Liste E-Mail-Suche.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die zugehörige Liste E-Mail-Suche nicht angezeigt wird, klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**, um diese zugehörige Liste anzuzeigen.

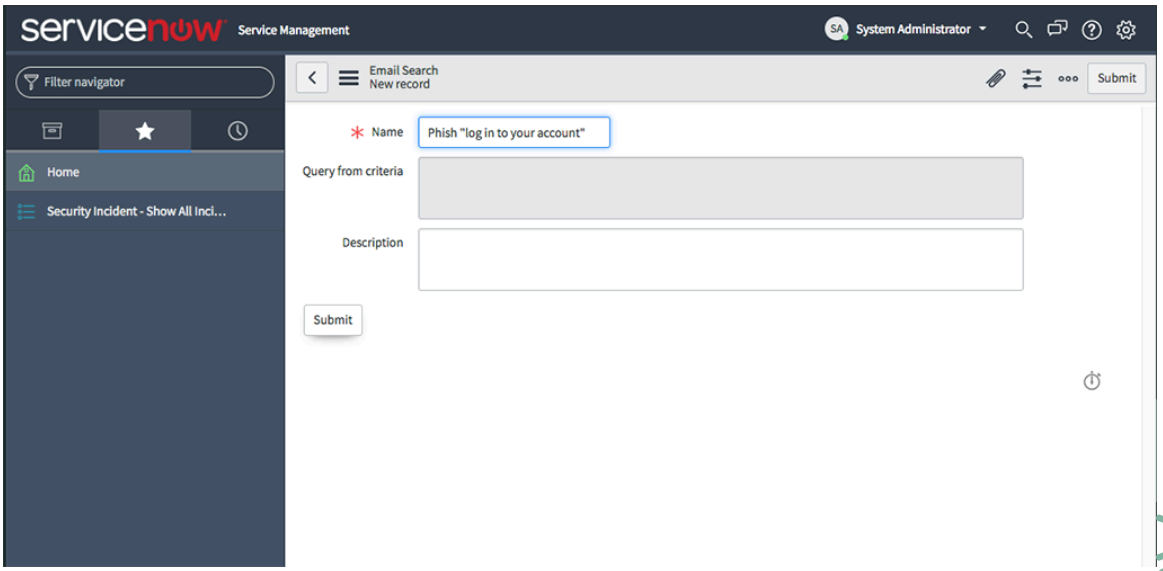


4. Klicken Sie in der zugehörigen Liste „E-Mail-Suche“ auf **Neu**, um einen neuen E-Mail-Suchdatensatz zu erstellen.
   Das Formular „E-Mail-Suche“ wird angezeigt. Wenn Sie diese Suchabfrage für denselben Phishing-bezogenen Incident mit geringfügigen Änderungen erneut ausführen möchten, können Sie diesen Suchabfrage-Datensatz erneut verwenden. Es ist jedoch unwahrscheinlich, dass Sie diese Suche für einen anderen Incident im Zusammenhang mit Phishing verwenden, da Phishing-Kampagnen dynamisch sind und sich die Felder „Absender“ und „Nachricht“ häufig ändern.
5. **Wahlweise:** Um einen vorhandenen Suchabfrage-Datensatz zu bearbeiten, klicken Sie auf **Bearbeiten**.
6. Füllen Sie die Felder im Formular „E-Mail-Suche“ aus.

Feld	Beschreibung
Name	Informationen zur Beschreibung des Suchtyps. In diesem Beispiel lautet ein Name für eine Suche unter „Von + Betreff “ Phishing "log in to your account".
Beschreibung	Informationen zur Suche im E-Mail-Server. Ein Beispiel für diese Suche ist Von=phisher@cbazyx.com + Betreff=an Ihrem Account anmelden.

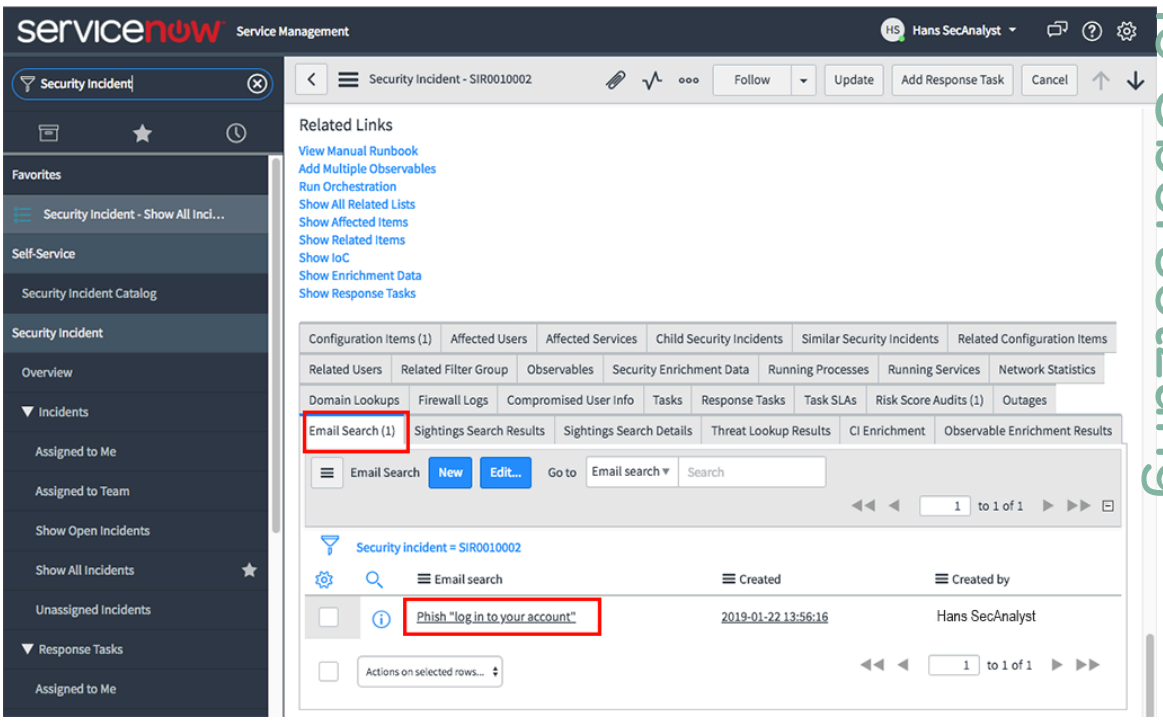
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.
   Der Security Incident wird angezeigt, und der Name der E-Mail-Suche wird in der Spalte E-Mail-Suche in der zugehörigen Liste „E-Mail-Suche“ angezeigt. Bevor Sie diese neue Suchabfrage verwenden können, müssen Suchkriterien für den Suchdatensatz definiert werden.

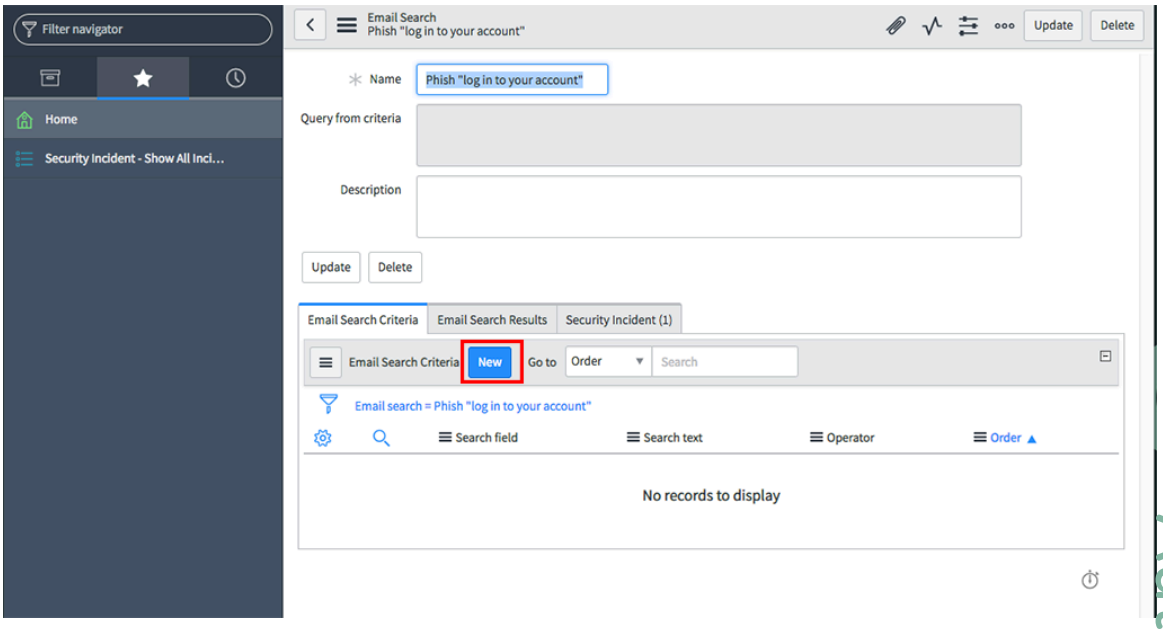
8. Um Suchkriterien zu definieren, klicken Sie bei ausgewählter zugehöriger Liste E-Mail-Suche in der Spalte E-Mail-Suche auf **Phishing "log in to your account" (Bei Ihrem Account anmelden) auf Phishing**.



9. Klicken Sie im angezeigten E-Mail-Suchdatensatz auf die zugehörige Liste E-Mail-Suchkriterien, und klicken Sie dann auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Füllen Sie die Felder im Formular „E-Mail-Suchkriterien“ aus.

Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
E-Mail-Suche	Das Feld wird automatisch mit dem Namen ausgefüllt, den Sie für den E-Mail-Suchdatensatz eingegeben haben.
Suchsymbol	Suche mithilfe von Liste. Eine Liste der gespeicherten Suchen. Klicken Sie auf das Symbol, um eine Liste der gespeicherten E-Mail-Suchen zu öffnen. Klicken Sie auf ein Element in dieser Liste, um die aktuelle Suche zu entfernen und eine zuvor gespeicherte E-Mail-Suche auszuwählen.
Informationssymbol	Symbol zum Anzeigen des Datensatzes „E-Mail-Suche“. Klicken Sie auf das Symbol, um den E-Mail-Suchdatensatz anzuzeigen.
Suchfeld	Suchkriterium (**Betreff**, **Von**oder **Empfänger**). Wählen Sie das Suchkriterium aus der Auswahlliste aus, und definieren Sie im Textfeld einen Wert, nach dem Sie suchen möchten. Beginnen Sie in diesem Beispiel mit Von phisher@cbazyx.com (der E-Mail-Adresse des Absenders der Phishing-E-Mail).
Aktiv	Option zum Aktivieren der Suche. Die Suche ist standardmäßig aktiviert.

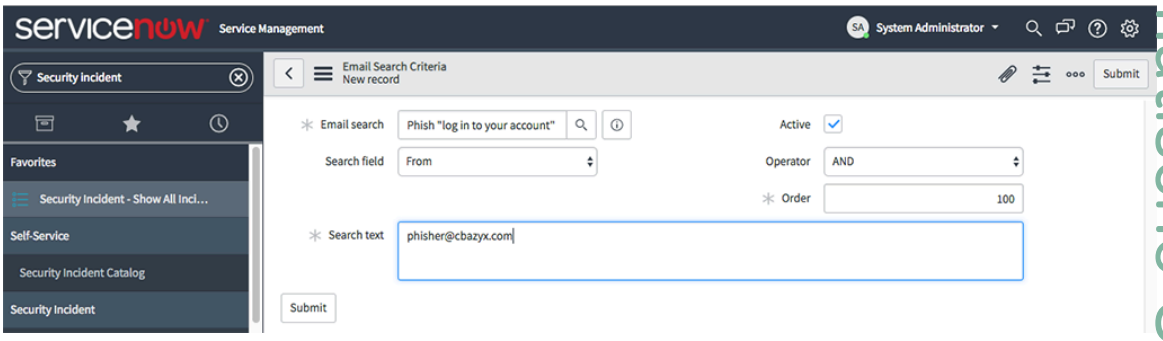
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

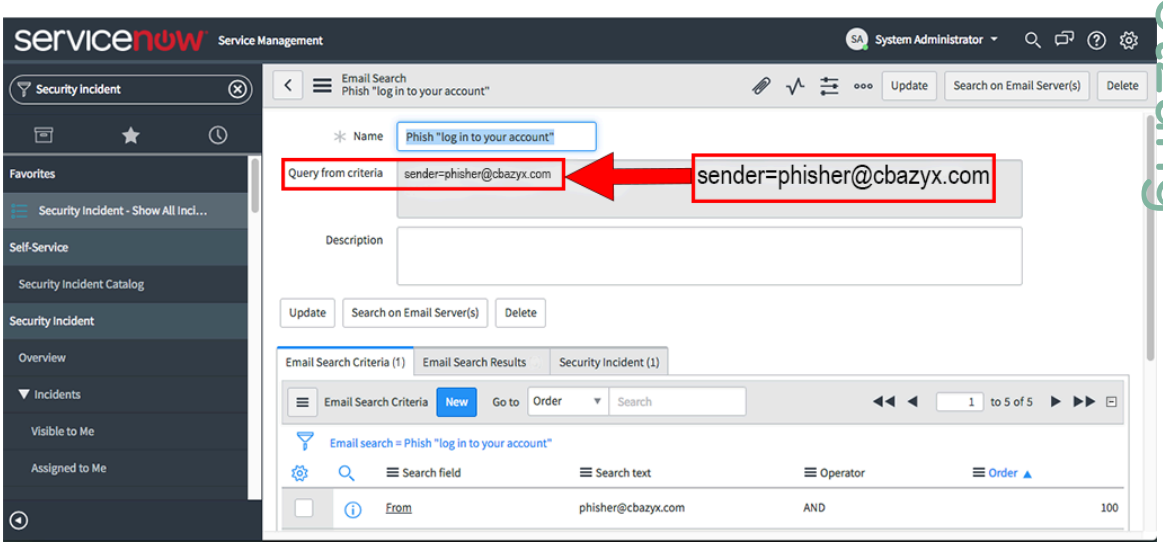
Feld	Beschreibung
	Wenn Sie diese Option deaktivieren, wird dieser Datensatz nicht in eine Suche einbezogen.
Betreiber	Operatoren (**AND**, **OR**) zur weiteren Definition Ihrer Suche. **AND**: Das System sucht nach den durch **AND** getrennten Bedingungen und gibt nur dann Ergebnisse zurück, wenn alle Bedingungen erfüllt sind. Verwenden Sie für die Suche nach Absender und Betreff den **AND-** Operator, damit beide Suchbedingungen während der E-Mail-Suche erfüllt werden. Verwenden Sie in diesem Beispiel den **AND-** Operator, sodass die Abfrage „Von (Absender) = phisher@cbazyx.com **UND** Betreff = bei Ihrem Account anmelden“lautet. **ODER**: Das System sucht und gibt Ergebnisse zurück, wenn eine der durch **ODER** getrennten Bedingungen erfüllt ist. Ein Beispiel ist Von (Absender) = phisher@cbazyx.com **ODER** Von (Absender) = phisher-2@cbazyx.com.
Bestellung	Wenn Sie mehr als zwei Suchbedingungen eingeben, verwenden Sie die Reihenfolge, um die Bedingungen zu priorisieren. 100 ist der Standardwert. Geben Sie für jede Bedingung einen Wert zwischen 1 und 100 ein, z. B. 100, 95, 90, 80. Die Bedingung mit der niedrigsten zugewiesenen Nummer hat die höchste Suchpriorität innerhalb einer Gruppe von Bedingungen.
Suchtext	Die Textwerte (Stichwörter) für die Suche (E-Mail-Adressen oder Betreffzeilen). Das Suchfeld enthält den bei der Suche verwendeten Text, z. B. phisher@cbazyx.com. Damit die Suche für die Suche nach Absender (Von) und Empfänger genaue Ergebnisse liefert, müssen die Suchzeichenfolgen genau übereinstimmen. Bei Betreffsuchen kann die Suchzeichenfolge Schlüsselwörter enthalten, die Teil einer größeren Zeichenfolge sind. Beispielsweise kann ein Betreff die genaue Suchzeichenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	enthalten, die in einem weitergeleiteten oder einem Antwortnachrichtenheader wie FW abgeglichen wird: Melden Sie sich bei Ihrem -Konto an, und ändern Sie sofort Ihr Passwort. Beispiel: Melden Sie sich bei Ihrem Account an sind genaue Schlüsselwörter in der Zeichenfolge Melden Sie sich bei Ihrem Account an und ändern Sie sofort Ihr Passwort. Es ist keine Platzhalterbezeichnung (*) erforderlich, um den Suchtyp „*enthält*“ zu unterstützen. Derzeit ist keine Filtermethode zum Abgleichen einer exakten Suchzeichenfolge vorhanden, die nicht Teil einer größeren Textzeichenfolge ist.



11. Klicken Sie auf **Absenden**.
Der Datensatz „E-Mail-Suche“ wird angezeigt. Im Feld **Abfragekriterien** werden die Suchkriterien angezeigt, die Sie für Absender (Von) hinzugefügt haben.

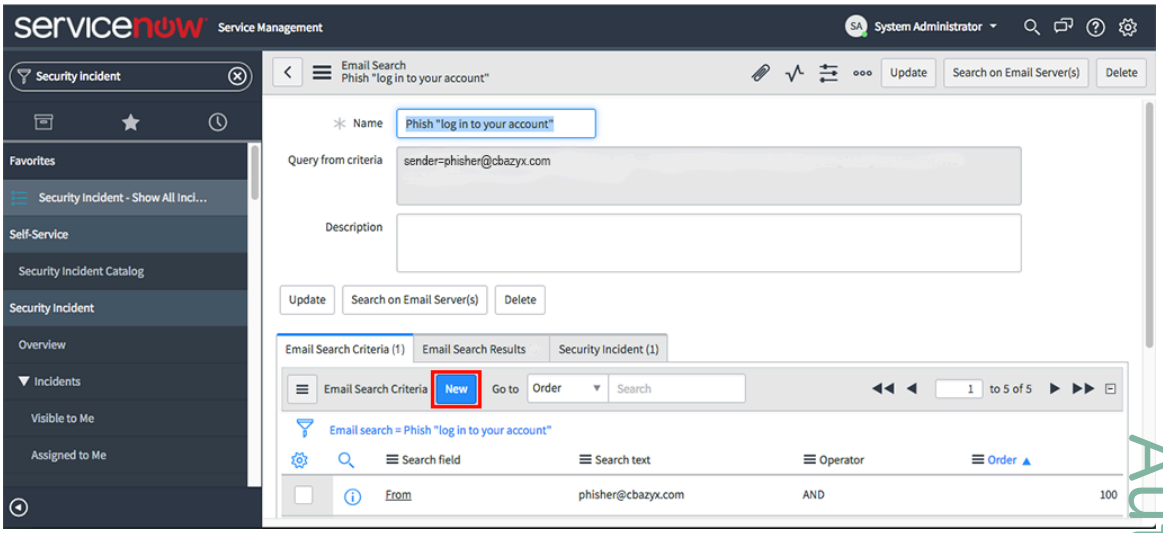


12. Um diese E-Mail-Suchkriterien mit weiteren Informationen zu aktualisieren, damit die Abfrage die gewünschte Bedingung für Betreff und Absender enthält, führen Sie die Schritte zum Hinzufügen einer weiteren Suchbedingung aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

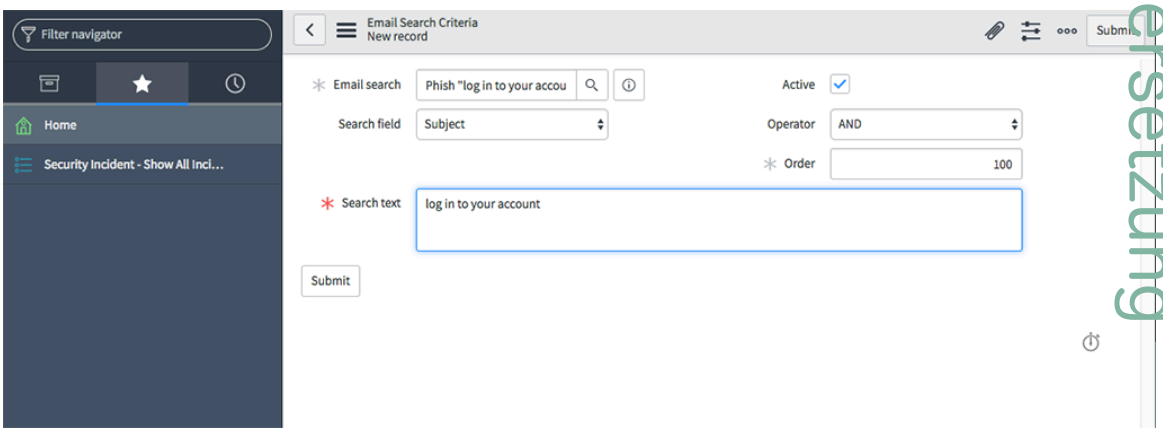
a. Klicken Sie in der zugehörigen Liste E-Mail-Suchkriterien **auf Neu**.



b. Wählen Sie in der Liste **Suchfeld**im angezeigten Datensatz „E-Mail-Suchkriterien“ die **Option Betreff**aus.

c. Wählen Sie in der Liste Operatoren**AND** oder **OR**aus.
Wenn Sie **ODER**auswählen, gibt die Suche Ergebnisse zurück, wenn entweder Schlüsselwörter in der Textzeichenfolge in der Betreffzeile übereinstimmen oder die E-Mail-Adressbedingung erfüllt ist. **UND** ist für dieses Beispiel ausgewählt, damit die Suche Ergebnisse nur für E-Mails zurückgibt, die die Stichwörter der Betreffzeichenfolge enthalten und mit der E-Mail-Adresse des Absenders übereinstimmen.

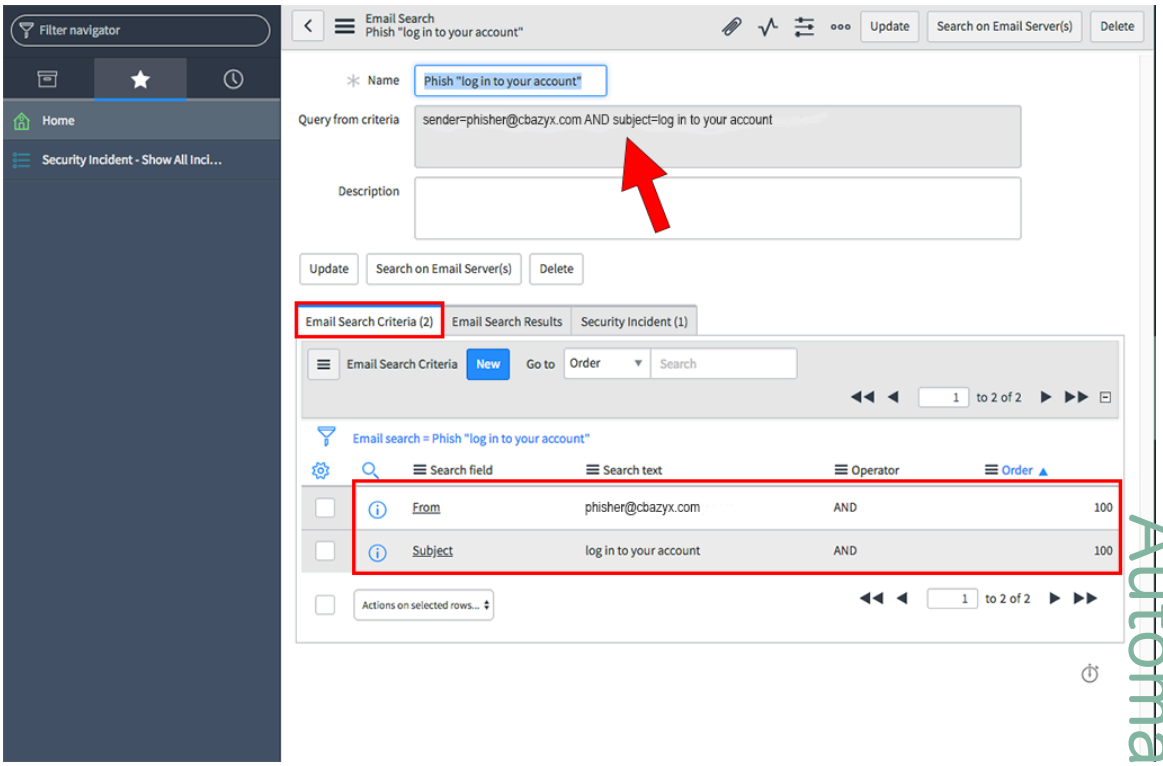
d. Geben Sie im Feld **Suchtext** den Wert für den Betreffzeilentext ein, und melden Sie sich bei Ihrem Account an.



e. Klicken Sie auf **Absenden**.
Die neue Bedingung wird in der zugehörigen Liste E-Mail-Suchkriterien angezeigt, und beide Bedingungen werden im Feld **Abfragekriterien** durch den **UND-** Operator getrennt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



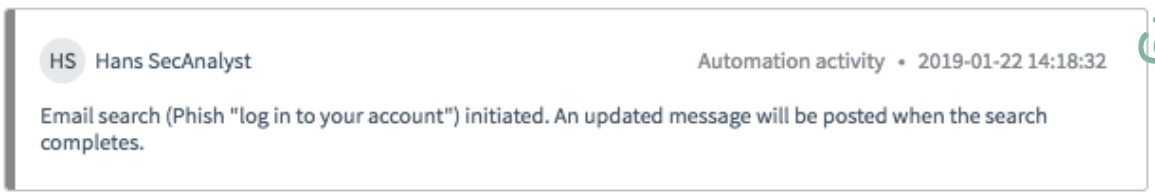
f. Wahlweise: Wenn Sie mehr als zwei Suchbedingungen haben und **UND** auswählen, um jede Bedingung zu trennen, legen Sie den Reihenfolgewert fest, um sie zu priorisieren.

g. Fügen Sie nach Bedarf Suchkriterien hinzu, ändern oder entfernen Sie sie, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen im Datensatz zu speichern.

13. Wählen Sie eine Option aus, um fortzufahren.

14. Um eine E-Mail-Suche zu starten, klicken Sie im E-Mail-Suchdatensatz **auf Auf E-Mail-Servern suchen**. Es wird eine Meldung angezeigt, dass die Suchanforderung gesendet wurde.

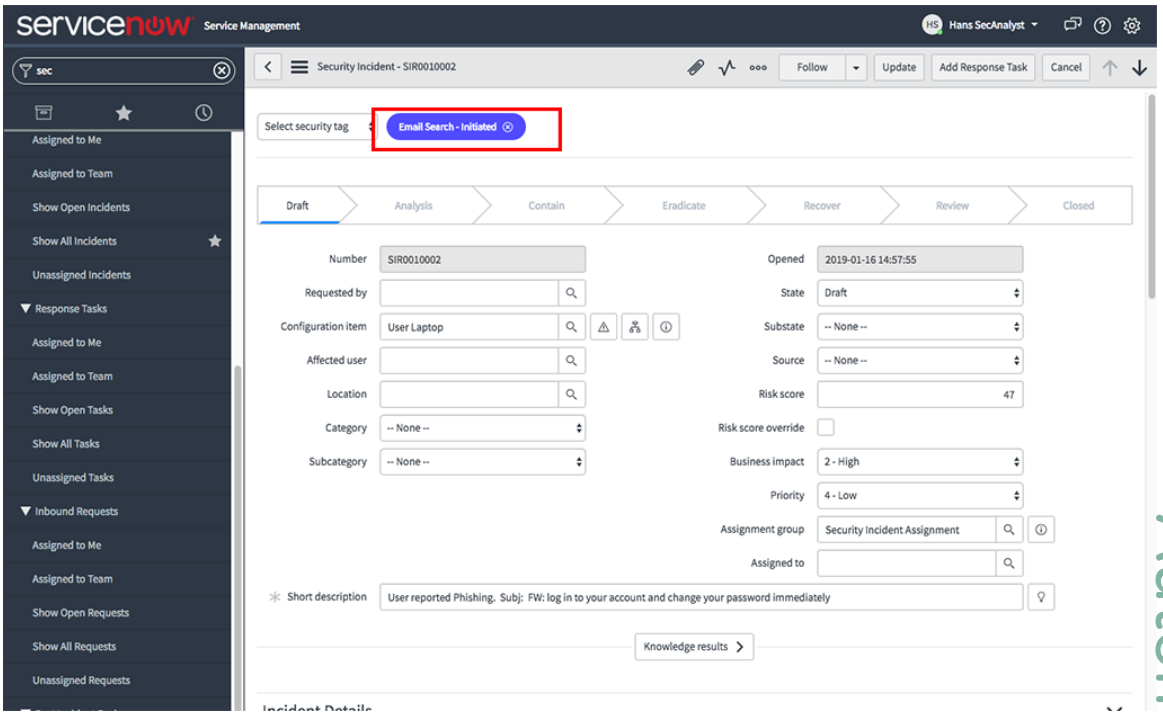
Im Security Incident-Datensatz wird eine Arbeitsnotiz angezeigt, die angibt, dass eine Suche initiiert wurde.



Wenn Tagging aktiviert ist, wird oben im Security Incident-Datensatz das Sicherheits-Tag E-Mail-Suche – Initiiert angezeigt.

Automatische Übersetzung

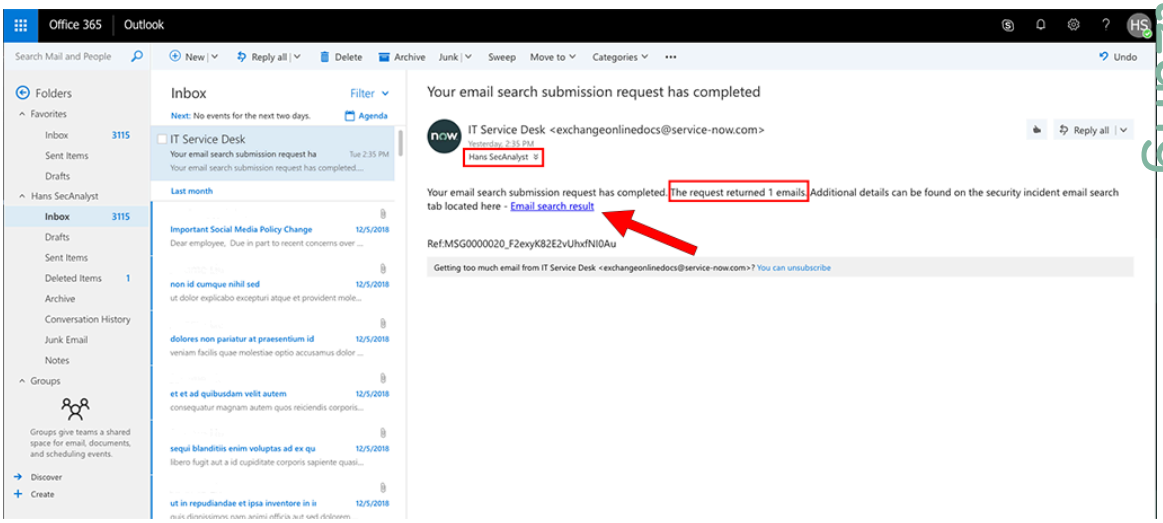
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem die Suche erfolgreich abgeschlossen wurde und E-Mail-Benachrichtigungen aktiviert sind, wird eine E-Mail an die E-Mail-Adresse der Person gesendet, die die Suche initiiert hat.

In diesem Beispiel hat der Benutzer mit der Rolle sn_si.analyst, Häns SecAnalyst, diese Suche übermittelt. Die folgende Abbildung zeigt, dass diese Benachrichtigung an einen Account in Microsoft Exchange Onlinegesendet wird. Diese Benachrichtigungen können jedoch bei Bedarf an einen anderen E-Mail-Service gesendet werden.

Mit dieser Benachrichtigung können Sie alle übereinstimmenden Ergebnisse anzeigen, die nachverfolgt und gelöscht werden müssen. Das folgende Beispiel zeigt, dass eine E-Mail den Suchkriterien entspricht. Ein E-Mail-Suchergebnis-Link zum E-Mail-Suchergebnis-Datensatz in Ihrer Instanz Now Platform wird ebenfalls bereitgestellt. Wenn Sie den Suchdatensatz anzeigen möchten, klicken Sie auf diesen Link.



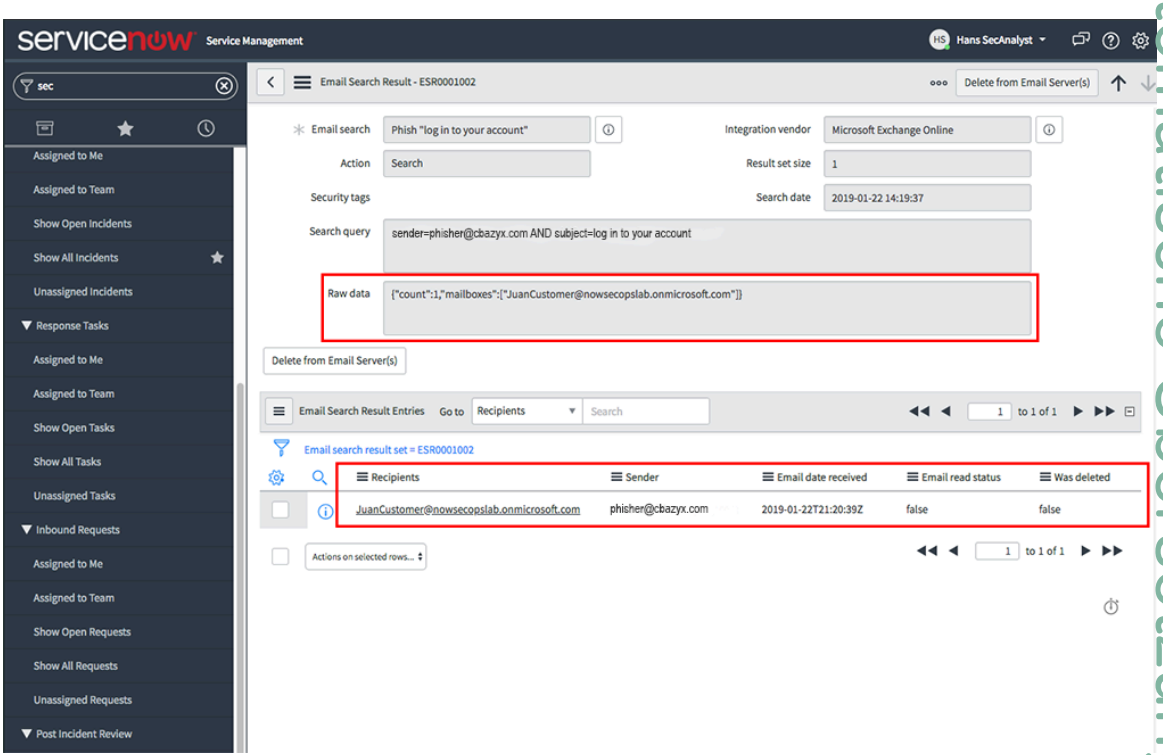
15. Um die Suchergebnisse anzuzeigen, klicken Sie in dieser E-Mail auf den Link **Suchergebnis senden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Datensatz für das E-Mail-Suchergebnis wird angezeigt. In diesem Datensatz können Sie die folgenden Daten überprüfen.

- Im Feld **Rohdaten** werden die E-Mail-Anzahl für die Anzahl der E-Mails, die den Suchkriterien {"count":1}entsprechen, und die Postfachadressen, unter denen die E-Mails gefunden wurden, angezeigt ["JuanCustomer@nowsecopslab.onmicrosoft.com"].
- In der Spalte Empfänger ist der Empfänger der (JuanCustomer@nowsecopslab.onmicrosoft.com).
- In der Spalte Absender wird die Quelle der E-Mail angezeigt.
- In der Spalte Empfangsdatum der E-Mail werden das Datum und die Uhrzeit des Empfangs der E-Mail angezeigt, damit Sie die Zeitleisten für Phishing-Kampagnen nachverfolgen können.
- In der Spalte Lesestatus der E-Mail wird angegeben, dass die E-Mail in diesem Beispiel nicht gelesen wurde (false). Wenn eine E-Mail gelesen wurde, wird true angezeigt.
- In der Spalte Was gelöscht wurde die E-Mail in diesem Beispiel nicht gelöscht. Wenn eine E-Mail gelöscht wurde, wird „wahr“ angezeigt.

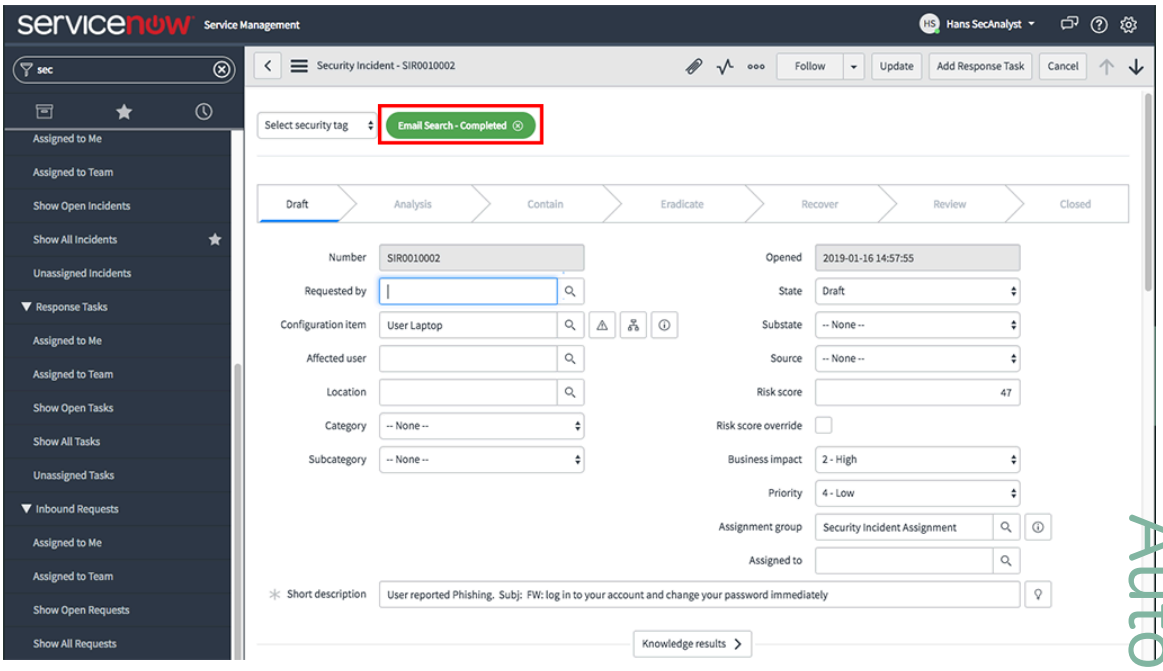


16. Alternativ können Sie die Suchergebnisse aus dem Security Incident anzeigen, indem Sie die folgenden Schritte ausführen.

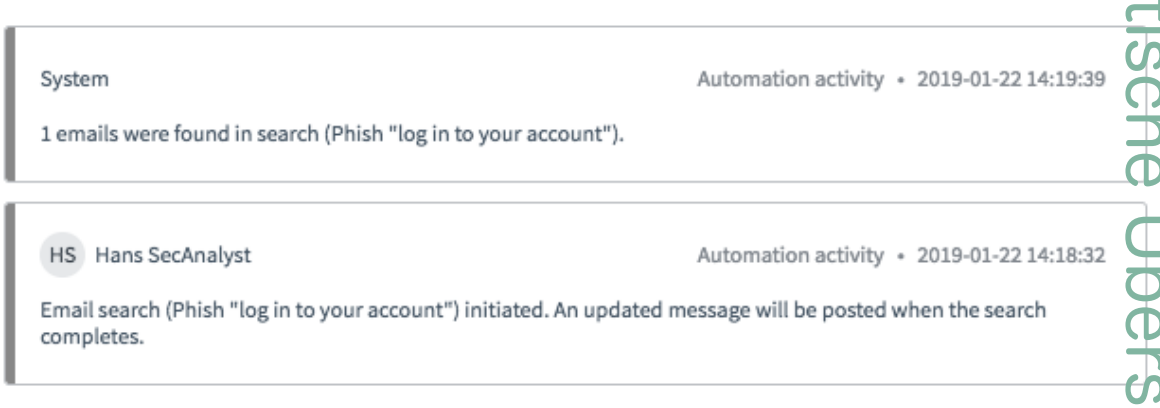
a. Navigieren zu **Security Incident** > **Incidents** und öffnen Sie den Security Incident, mit dem Sie arbeiten.
Wenn die Suche erfolgreich abgeschlossen wird, ersetzt oben im Datensatz das Sicherheits-Tag E-Mail-Suche – Abgeschlossen das Sicherheits-Tag E-Mail-Suche – Initiiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Es werden Arbeitsnotizen angezeigt, dass die Suche erfolgreich abgeschlossen wurde und dass eine übereinstimmende E-Mail-Adresse gefunden wurde.

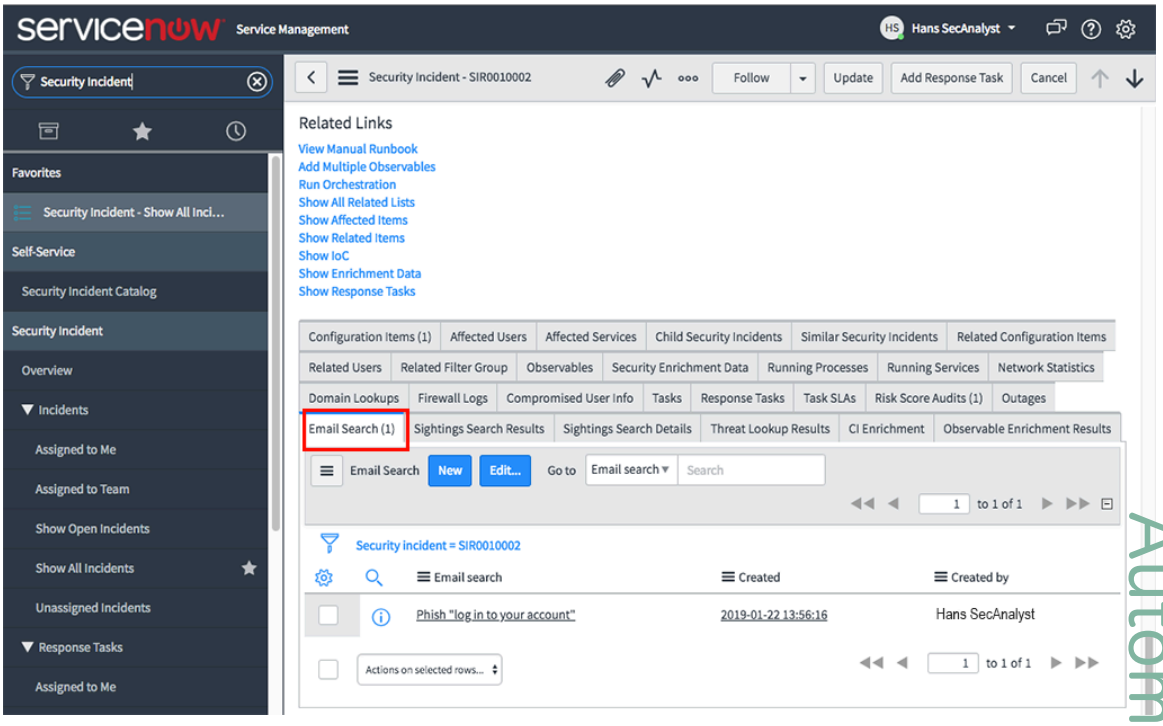


b. Scrollen Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf die zugehörige Liste E-Mail-Suche.

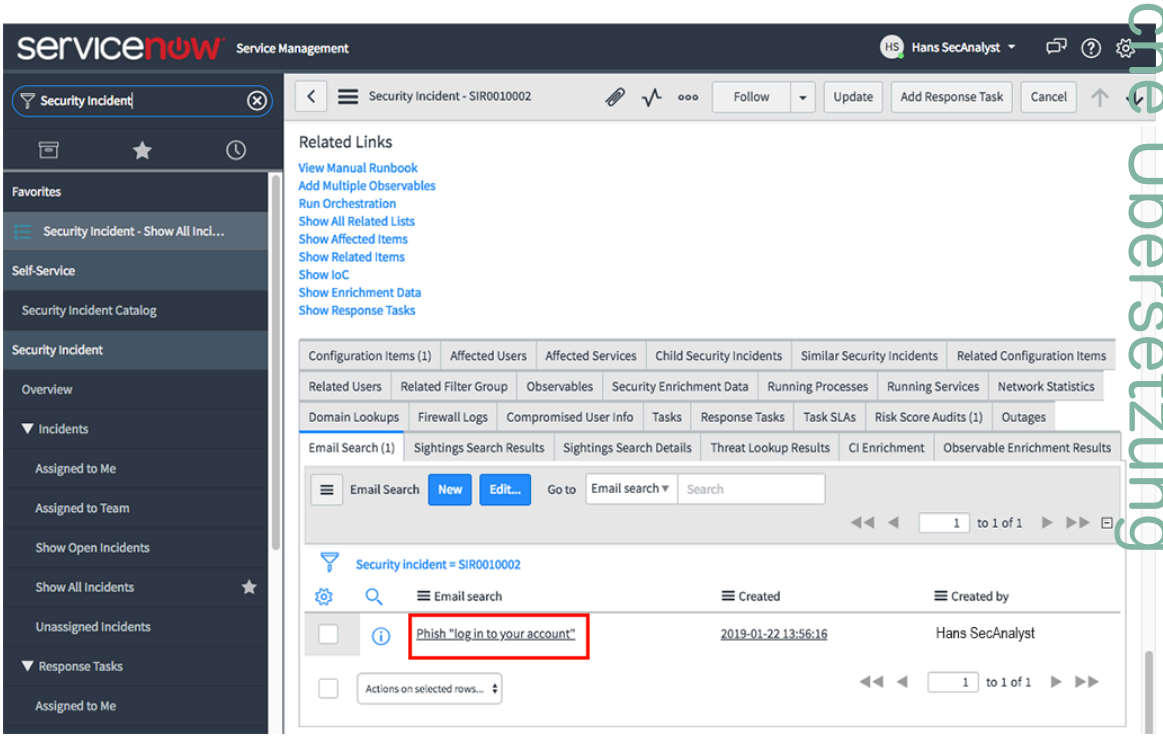
Wenn die zugehörige Liste E-Mail-Suche nicht angezeigt wird, klicken Sie auf den zugehörigen Link**Alle zugehörigen Listen anzeigen**, um diese zugehörige Liste anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Wählen Sie die zugehörige Liste „E-Mail-Suche“ aus, und klicken Sie in der Spalte „E-Mail-Suche“ auf den Namen Ihrer Suche.



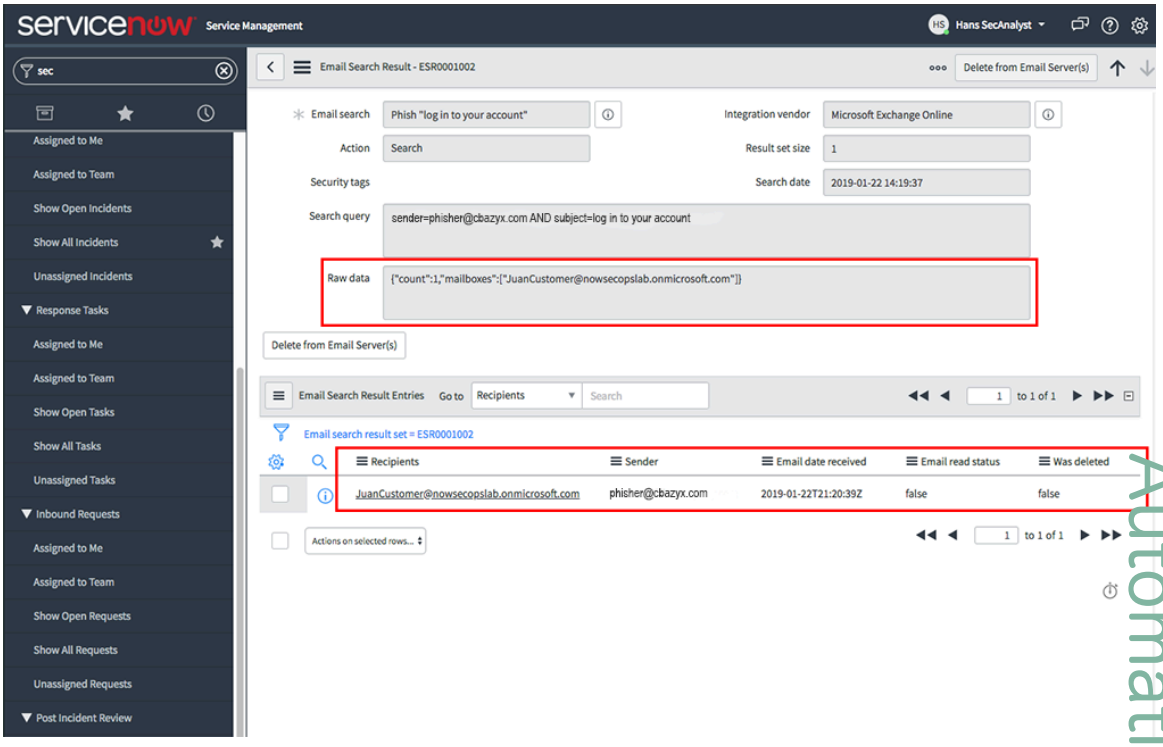
d. Klicken Sie im Datensatz „E-Mail-Suche“ auf die zugehörige Liste „E-Mail-Suchergebnisse“.

e. Klicken Sie in der Spalte Suchdatum auf das Datum Ihrer Suche, um die Daten anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Datensatz für das E-Mail-Suchergebnis wird angezeigt.



Nachdem eine E-Mail-Suche erfolgreich abgeschlossen wurde, werten Sie die Ergebnisse aus. Wenn Sie feststellen, dass E-Mails korrigiert werden müssen, können Sie jetzt E-Mails löschen oder die Löschgenehmigung anfordern.

Fordern Sie die Löschgenehmigung für E-Mails im Microsoft Exchange Online-Service an

Nachdem eine E-Mail-Suche erfolgreich abgeschlossen wurde und übereinstimmende Nachrichten identifiziert wurden, können Sie alle verdächtigen E-Mails, die mit dem Security Incident und der Phishing-Kampagne in Zusammenhang stehen, endgültig aus dem Microsoft Exchange Online-Service löschen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Das System löscht Ihre letzten erfolgreichen Suchergebnisse.

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Genehmigungen und E-Mail-Benachrichtigungen aktiviert sind, senden Sie vor dem Entfernen der E-Mail eine Anforderung zum Löschen von E-Mails an eine Genehmigungsgruppe.

E-Mail-Suchergebnisse werden mit allen empfangenen Nachrichten angezeigt. Um sicherzustellen, dass Phishing-E-Mails erfolgreich gelöscht werden, werden die Löschergebnisse in den Arbeitsnotizen des zugehörigen Security Incident veröffentlicht. Wenn Tagging aktiviert ist, wird auch ein Sicherheits-Tag für den zugehörigen Security Incident angezeigt. Wenn die E-Mail nicht erfolgreich gelöscht wird, werden Sie auch in den Arbeitsnotizen benachrichtigt.

Abhängig von Ihren Organisationsrichtlinien müssen Sie möglicherweise eine Genehmigung anfordern, bevor Sie Phishing-E-Mails löschen. Für den Löschgenehmigungsprozess sind Informationen zur Anzahl der zu löschenden E-Mails und möglicherweise Zugriff auf weitere Nachrichtendetails erforderlich. Für die Verarbeitung der Löschanforderung werden in einer E-Mail-Benachrichtigung einem Genehmiger die entsprechende Anzahl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

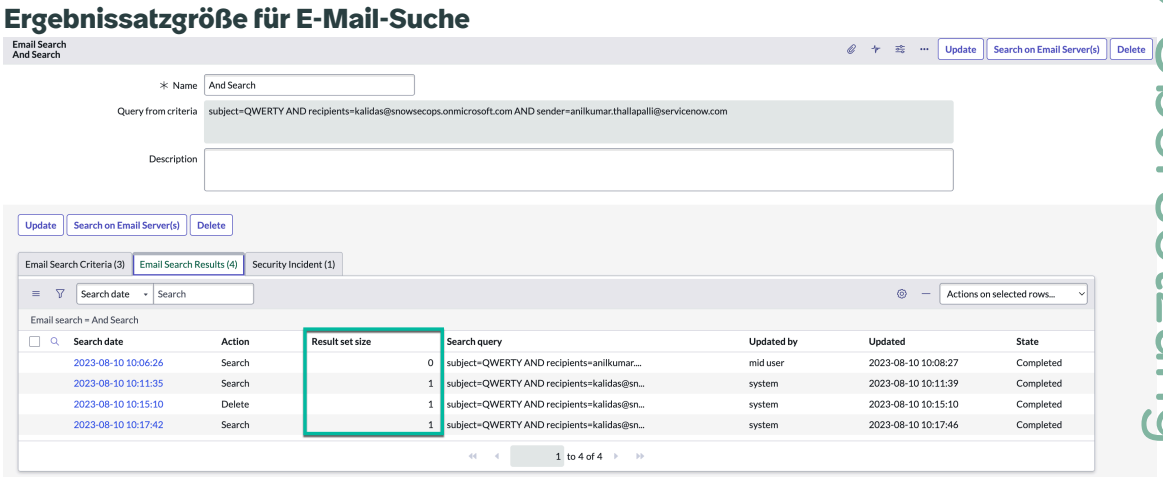
der E-Mail-Nachrichten, der Security Incident-Link für den Zugriff auf vollständige Nachrichtendetails und Links zum Genehmigen oder Ablehnen bereitgestellt. Die Links in dieser E-Mail ermöglichen es einem Genehmiger, die Löschanforderung in der E-Mail-Benachrichtigung anzunehmen oder abzulehnen. Es ist auch ein vollständiger Audit-Pfad mit einem Zeitstempel verfügbar, der nachverfolgt, wann sich der Genehmigungsstatus in den Arbeitsnotizen geändert hat. Wenn eine Genehmigungsgruppe zugewiesen ist, kann ein Benutzer in der Gruppe die Anforderung für die gesamte Gruppe verarbeiten. Jedes Mitglied der Genehmigungsgruppe erhält eine E-Mail-Benachrichtigung über die Anforderung.

Wenn Sie als Benutzer mit der Rolle sn_si.analyst feststellen, dass E-Mails korrigiert werden müssen, führen Sie die erforderlichen Schritte zum Löschen von E-Mails aus. Wenn Genehmigungen aktiviert sind, fordern Sie die Genehmigung zum Löschen von E-Mails aus dem Service Microsoft Exchange Online an.

Prozedur

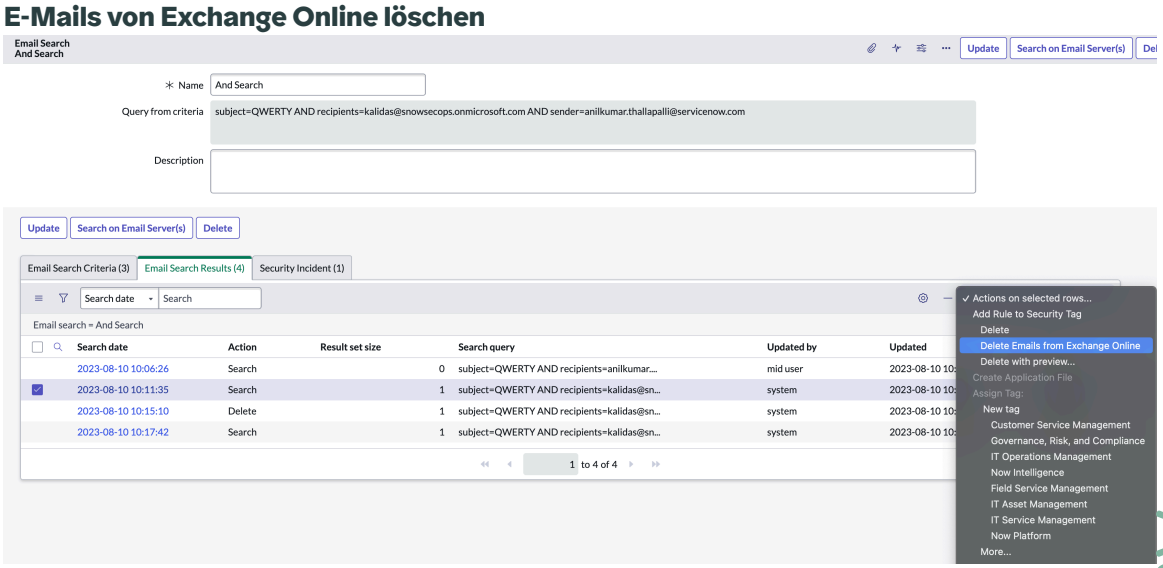
1. Navigieren zu **Alle** > **Security Incident > Alle Incidents anzeigen**.
2. Klicken Sie auf die zugehörige Liste **E-Mail-Suche**.
3. Wählen Sie die zugehörige Liste „E-Mail-Suche“ aus, und klicken Sie in der Spalte „E-Mail-Suche“ auf den Namen Ihrer Suche.
   Die Suchergebnisse werden in der zugehörigen Liste E-Mail-Suchergebnisse angezeigt.

   In diesem Beispiel hat diese Suche E-Mails gefunden, die Ihren Suchkriterien entsprechen. Im Datensatz sind zwei Suchaktionen aufgeführt. Eine Suche hat keine Übereinstimmungen (0) und die andere Suche hat eine übereinstimmende E-Mail-Adresse (1).



4. Um E-Mail-Elemente zu löschen, die einer Suche zugeordnet sind, aktivieren Sie links neben der Spalte Suchdatum das Kontrollkästchen eines Suchergebnissatzes.
   Sie können einen einzelnen Ergebnissatz oder mehrere Ergebnissätze aus der Liste auswählen.
5. Wählen Sie die Ergebnissätze aus, die Sie löschen möchten.

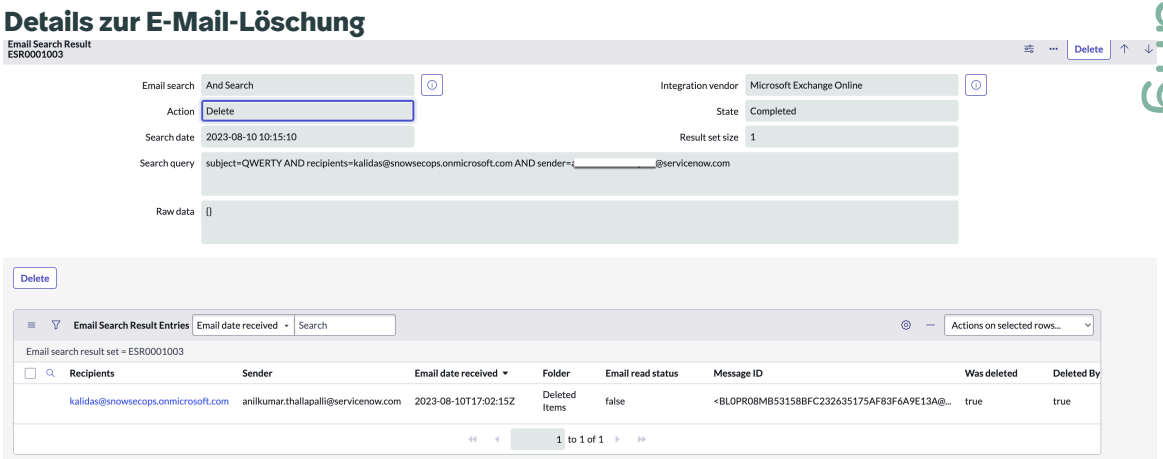
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie unten in der zugehörigen Liste „E-Mail-Suchergebnisse“ in der Liste „Aktionen für ausgewählte Zeilen“ die **Option E-Mails aus Exchange Online löschen aus**, um alle E-Mail-Elemente zu löschen, die einem oder mehreren Ergebnissätzen zugeordnet sind, vom Exchange Online-Server.
Wenn ein Ergebnissatz mehr als eine E-Mail enthält, müssen Sie den Datensatz „E-Mail-Suchergebnis“ nicht öffnen und einzelne E-Mails auswählen, um sie zu löschen. Alle E-Mail-Elemente mit dem Status „ false“ in der Spalte „Wurde gelöscht“ im Datensatz „E-Mail-Suchergebnis“ werden gelöscht, nachdem Sie **E-Mails aus Exchange Online löschen**ausgewählt haben.

   Wenn ein E-Mail-Element in einem Ergebnissatz bereits gelöscht wurde, lautet der Status in der Spalte Wurde gelöscht im Datensatz E-Mail-Suchergebnis „ true“. Diese Elemente werden nicht erneut gelöscht.

   Wenn die Genehmigungsoption während des Konfigurationsschritts deaktiviert ist, werden die dem Ergebnissatz zugeordneten E-Mails gelöscht, nachdem Sie **E-Mails aus Exchange Online löschen**ausgewählt haben. Der Ergebnissatz selbst wird nicht gelöscht. Der Status aller gelöschten E-Mail-Elemente des Ergebnissatzes wird jedoch in der Spalte Wurde gelöscht des Datensatzes E-Mail-Suchergebnis auf „True“ aktualisiert. Weitere Informationen zur Genehmigungsfunktion finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform ..



   Diese E-Mails werden aus dem Mandanten Microsoft Exchange Online gelöscht, in dem Sie die Suchen durchgeführt haben. Wenn die E-Mails erfolgreich gelöscht wurden, wird eine Arbeitsnotiz angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

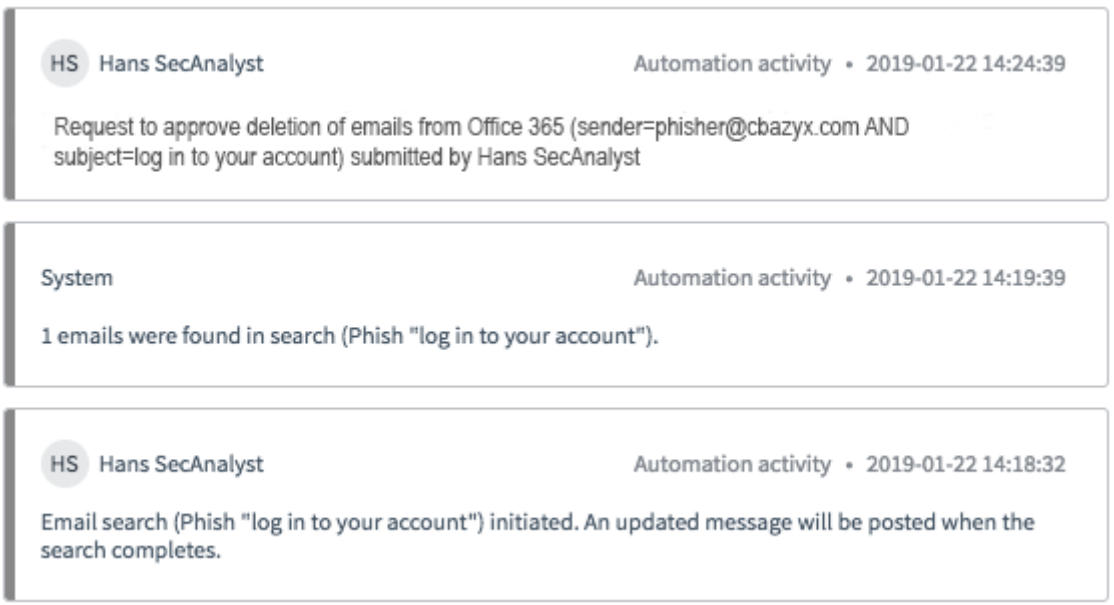
Im Security Incident-Datensatz wird das Sicherheits-Tag E-Mail-Löschung abgeschlossen angezeigt.

Wenn Genehmigungen für Löschanforderungen deaktiviert sind, haben Sie erfolgreich E-Mails aus dem Mandanten Microsoft Exchange Online gelöscht.

Wenn während des Konfigurationsschritts Genehmigungen für Löschanforderungen aktiviert sind, wird nach der Auswahl **von E-Mails löschen aus Exchange Online**eine E-Mail-Benachrichtigung an jedes Mitglied der Genehmigungsgruppe gesendet, die Sie im Konfigurationsschritt ausgewählt haben.

Wenn Tagging während des Konfigurationsschritts aktiviert wird, wird das Sicherheits-Tag E-Mail-Löschung – Initiiert im zugehörigen Security Incident-Datensatz angezeigt. Weitere Informationen zum Tagging finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform ..

Arbeitsnotizen werden angezeigt, wenn ein Benutzer mit der Rolle sn_si.analyst (Hans SecAnalyst) eine Anforderung zum Löschen von E-Mails übermittelt.

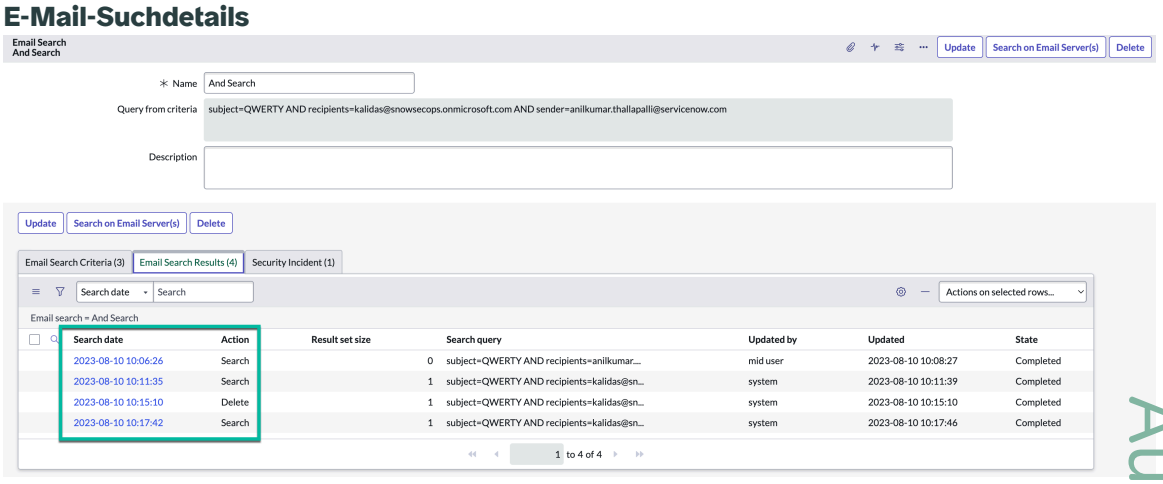


Wenn Genehmigungen aktiviert sind, besteht der nächste Schritt in der Verarbeitung der Löschanforderung.

7. Wenn Sie alternativ die Details und einzelnen E-Mail-Elemente eines Suchdatensatzes anzeigen möchten, bevor Sie ihn löschen oder eine Löschanforderung senden, führen Sie die folgenden Schritte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie bei ausgewählter zugehöriger Liste E-Mail-Suchergebnisse in der Spalte Suchdatum auf das Datum einer Suche, die Sie überprüfen möchten.



Die folgenden Informationen zu den E-Mails werden angezeigt:

- Empfänger
- Absender
- Empfangsdatum der E-Mail
- Lesestatus der E-Mail (wahr oder falsch)
- Wurde gelöscht (wahr oder falsch)
- Von Integration gelöscht (wahr oder falsch)

Hinweis:

Der Wert wird auf „wahr“ festgelegt, wenn die E-Mail gelöscht wird, wenn der Analyst die Aktion „Von E-Mail-Servern löschen“ initiiert.

Die Arbeitsnotizen werden mit der Gesamtzahl der gelöschten Datensätze aktualisiert, einschließlich der nach Integration und Anwender gelöschten Datensätze.

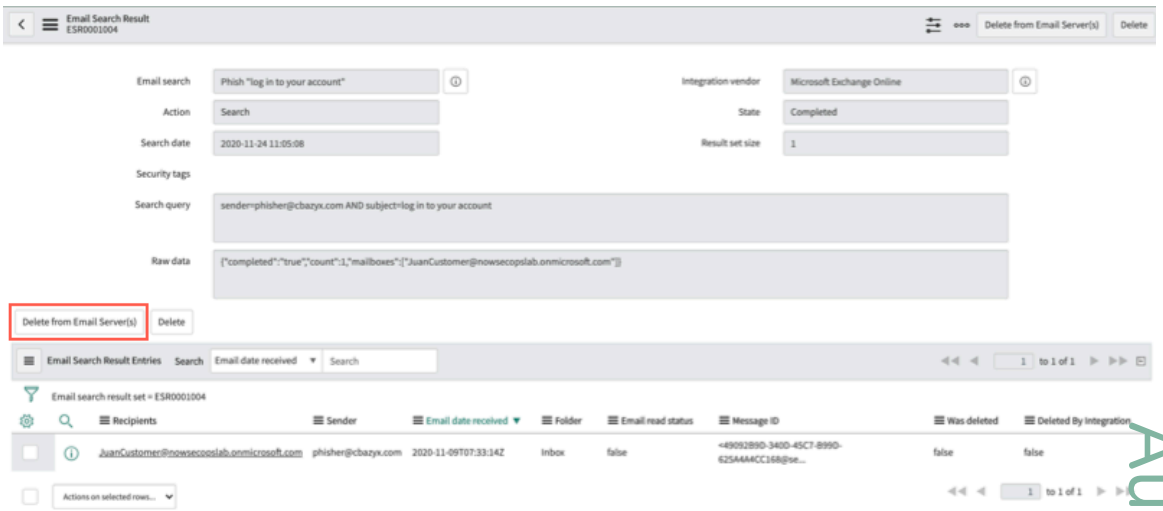
b. Nachdem Sie die Daten überprüft haben, klicken Sie auf **Von E-Mail-Server(n) löschen**, um alle E-Mails zu löschen oder eine Anforderung zum Löschen aller E-Mails zu senden.

Wenn im Suchergebnisdatensatz mehrere E-Mail-Adressen aufgeführt sind, müssen Sie, wie im vorherigen Beispiel beschrieben, die einzelnen E-Mail-Adressen nicht auswählen, um sie zu entfernen. Die Löschanforderung entfernt alle mit der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suche verknüpften E-Mails, wenn in der Spalte Wurde gelöscht aus den aktuellen Suchergebnissen falsch angezeigt wird.



Wenn Genehmigungen aktiviert sind, haben Sie erfolgreich eine Anforderung zum Löschen von E-Mails gesendet. Die Sicherheits-Tags und Arbeitsnotizen werden im zugehörigen Security Incident-Datensatz angezeigt (siehe vorheriges Beispiel). Als Genehmiger besteht der nächste Schritt in der Verarbeitung der Löschanforderung.

Genehmigen Sie E-Mail-Löschungsanforderungen für die Integration Microsoft Exchange Online .

Wenn die Genehmigungsoption in Ihrer Instanz Now Platform aktiviert ist, werden Anforderungen zum Löschen von E-Mails per E-Mail an jedes Mitglied der Genehmigungsgruppe gesendet. Die Genehmigungsgruppe wählen Sie im Konfigurationsschritt aus. Genehmigungen bieten Ihrer Organisation eine zusätzliche Kontrollebene für die Löschung von E-Mails.

Vorbereitungen

Vergewissern Sie sich, dass im Formular „Konfigurationseinstellungen für das Suchen und Löschen von E-Mails“ von Exchange Online auf der Registerkarte „Zusätzliche Einstellungen“ die Option **„Genehmigungen“** ausgewählt ist.

Stellen Sie sicher, dass Sie die Optionen **Senden von E-Mails aktiviert**und **Empfangen von E-Mails** in Ihrer Instanz Now Platform für Genehmigungsanforderungen aktiviert haben. Weitere Informationen finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration Microsoft Exchange Online ein.

Wenn ein Benutzer mit der Rolle sn_si.analyst E-Mail-Löschungsanforderungen sendet, werden diese Anforderungen standardmäßig per E-Mail an sn_si.admin gesendet. Wenn Sie eine Genehmigungsgruppe erstellt haben, erhält jedes Gruppenmitglied eine Benachrichtigung. Genehmiger können E-Mail-Löschanforderungen direkt aus der E-Mail-Benachrichtigung verarbeiten. Alternativ können Anforderungen aus den E-Mail-Suchergebnisdatensätzen in Instanzen Now Platform verarbeitet werden. In diesem Thema werden beide Genehmigungsmethoden behandelt.

Die folgenden Informationen beschreiben die Anforderung in der E-Mail-Benachrichtigung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatznummer des E-Mail-Suchergebnisses

Eindeutige Nummer, die dem Suchdatensatz von Now Platform als Teil des Audit-Trails zugewiesen wurde.

Name des Analysten, der die Anforderung gesendet hat

Name der Person, die die Anforderung als Teil des Audit-Trails übermittelt hat.

Link zum Security Incident

Ein Link zum Security Incident im Zusammenhang mit dem Phishing-Ereignis Zeigen Sie den Security Incident mit den Arbeitsnotizen, E-Mail-Suchergebnissen und E-Mail-Suchergebnissen direkt aus der E-Mail an.

Links zum Genehmigen oder Ablehnen

Links zum Genehmigen oder Ablehnen der Anforderung aus der E-Mail-Benachrichtigung. Nachdem Sie auf einen der Links geklickt haben, initiiert das System automatisch den zugehörigen Workflow, und im Datensatz des Security Incident wird eine Arbeitsnotiz veröffentlicht.

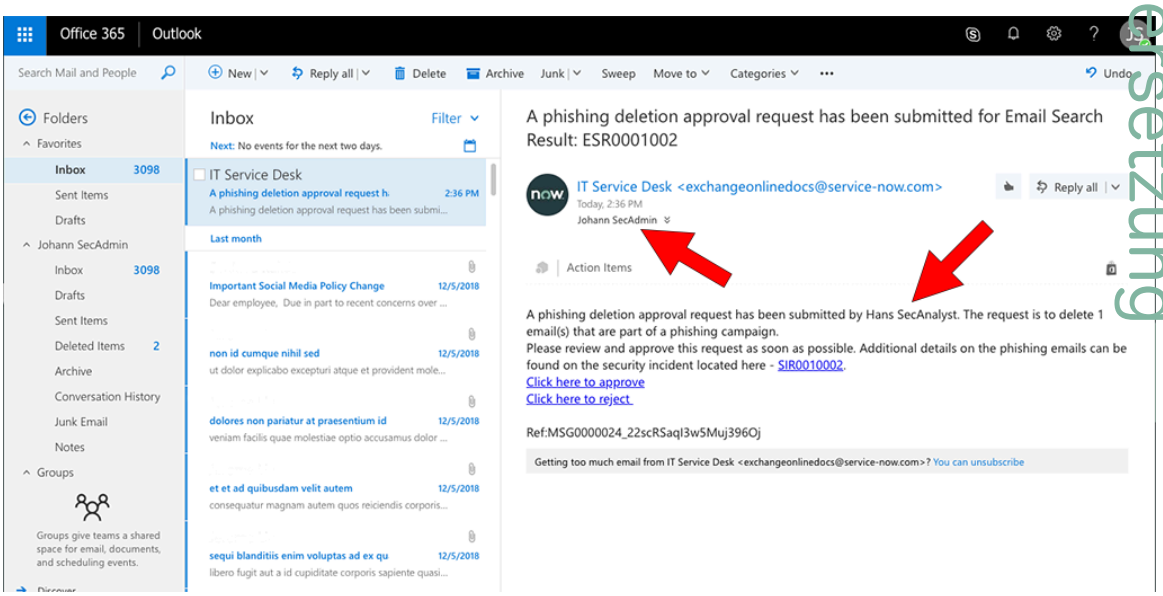
Erforderliche Rolle: sn_si.admin oder alle Mitglieder einer zugewiesenen Genehmigungsgruppe.

Prozedur

1. Führen Sie die folgenden Schritte aus, um die Löschanforderung aus der E-Mail-Benachrichtigung zu verarbeiten.

   a. Suchen Sie als Genehmiger die Benachrichtigungs-E-Mail in dem E-Mail-Konto, das Sie in Ihrem Benutzerkonto Now Platform konfiguriert haben.

   In diesem Beispiel sendet der Benutzer mit der Rolle sn_si.analyst (Hans SecAnalyst) eine Anforderung zum Löschen einer E-Mail. August SecAdmin ist Mitglied der Genehmigungsgruppe.



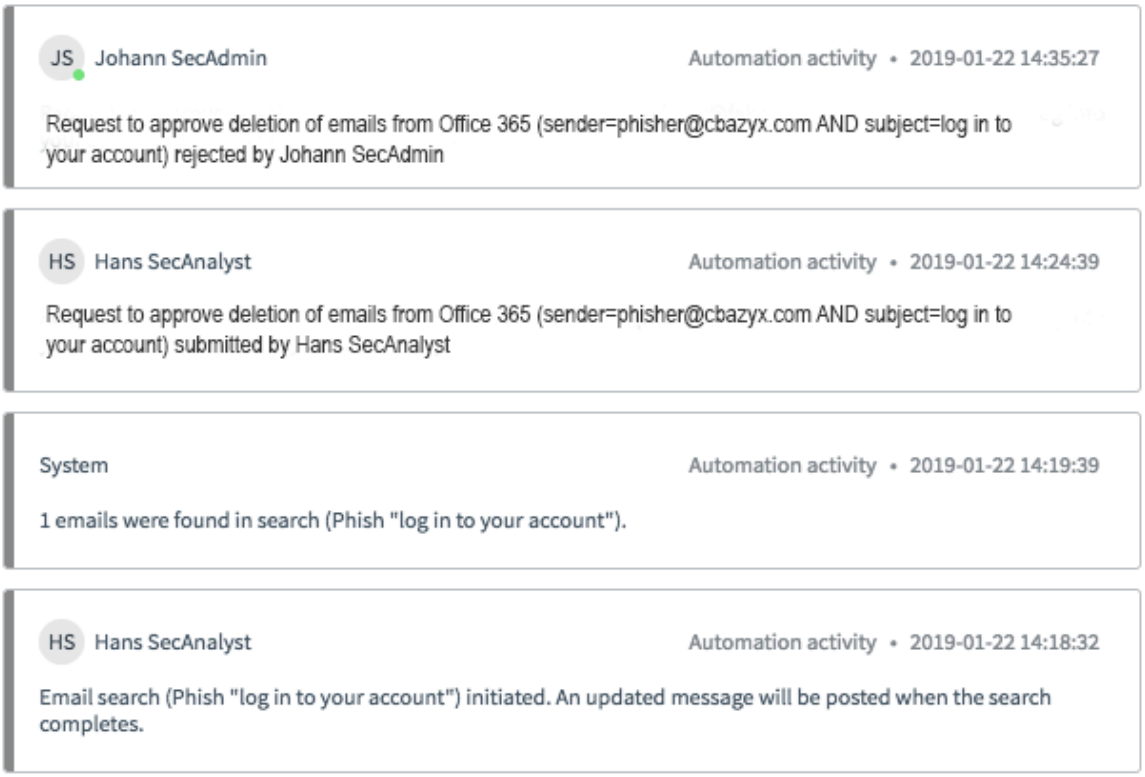
   b. Wählen Sie in der E-Mail-Benachrichtigung eine Option aus, um fortzufahren.

   Die folgende Abbildung zeigt ein Beispiel für den Audit-Pfad, der von den Arbeitsnotizen im zugehörigen Security Incident-Datensatz für dieses Beispiel erstellt wurde. Wenn die Anforderung von einem Genehmiger in der E-Mail-Benachrichtigung abgelehnt wird, wird

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von der Person, die die Anforderung abgelehnt hat, eine Arbeitsnotiz mit veröffentlicht. Pfr. SecAdmin lehnt diese Anforderung ab.



In der Instanz Now Platform der Person, die die Anforderung abgelehnt hat (Johann SecAdmin), in **Selfservice > Meine Genehmigungen**, in der Spalte Status wird „Abgelehnt“ angezeigt.

Nachdem eine Anforderung von einem einzelnen Mitglied der Genehmigungsgruppe abgelehnt wurde, müssen Sie als Benutzer mit der Rolle sn_si.analyst eine neue Anforderung zum Löschen dieser E-Mails senden, wenn Sie feststellen, dass sie gelöscht werden sollen.

In diesem Beispiel sendet der Benutzer mit der Rolle sn_si.analyst eine neue Anforderung, nachdem die Anforderung abgelehnt wurde.

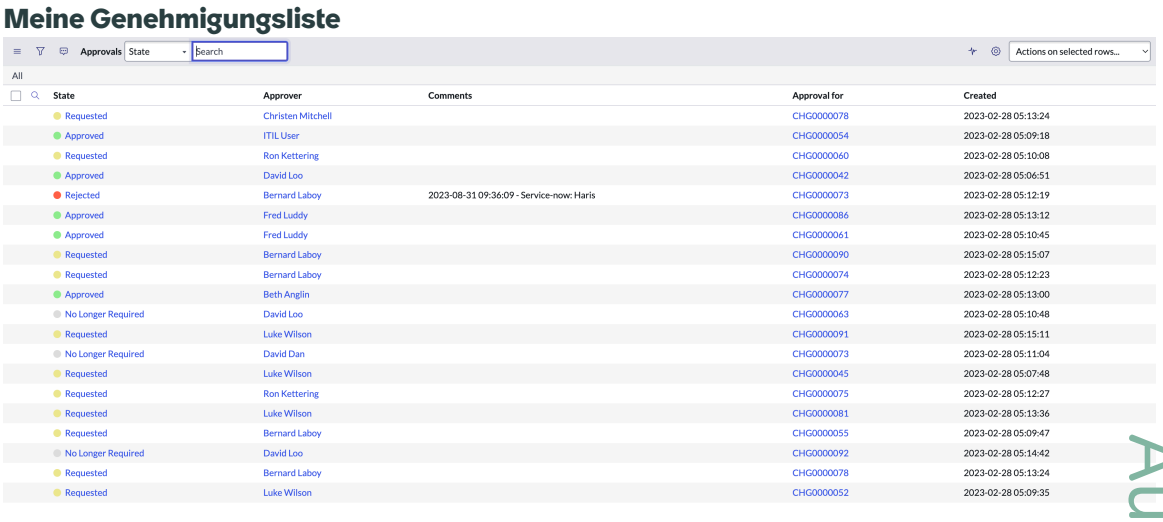
Ein anderes Mitglied der Genehmigungsgruppe, Max Genehmiger, erhält eine ähnliche E-Mail wie im vorherigen Beispiel. John-Genehmiger kann diese Anforderung auch verarbeiten.

2. Alternativ können Genehmiger zu navigieren **Selfservice > Meine Genehmigungen** in ihren Instanzen Now Platform, um Löschanforderungen anzuzeigen und zu verarbeiten.
   Führen Sie die folgenden Schritte aus, um eine -Anforderung aus **„Meine Genehmigungen“**zu verarbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

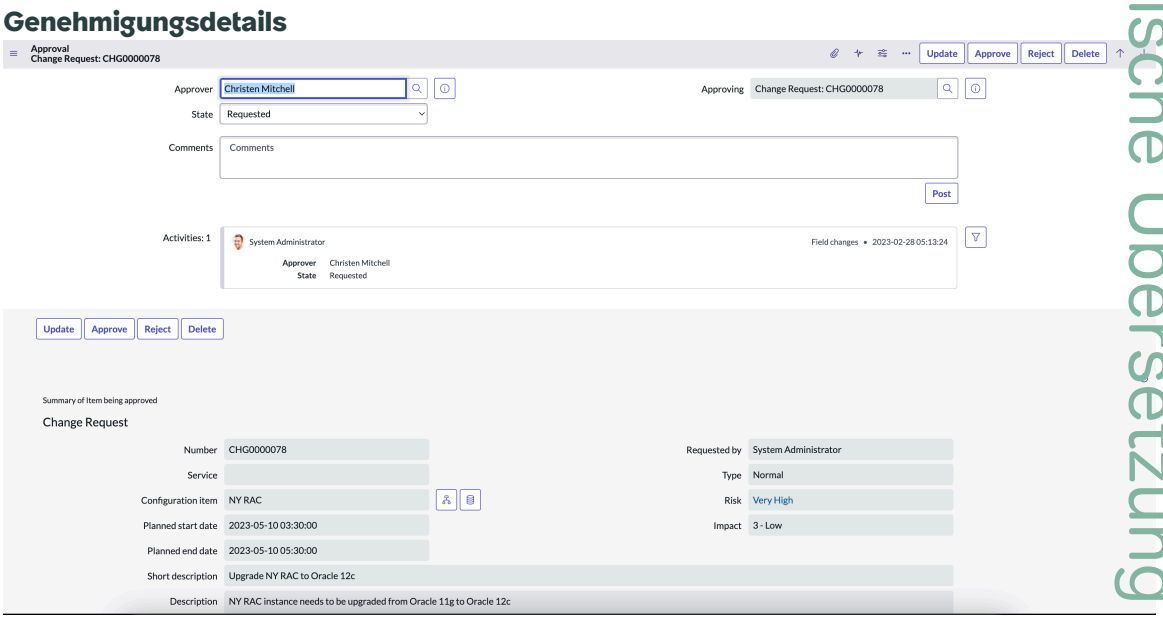
a. Navigieren zu **Selfservice > Meine Genehmigungen**.



State	Approver	Comments	Approval for	Created
Requested	Christen Mitchell		CHG0000078	2023-02-28 05:13:24
Approved	ITIL User		CHG0000054	2023-02-28 05:09:18
Requested	Ron Kettering		CHG0000060	2023-02-28 05:10:08
Approved	David Loo		CHG0000042	2023-02-28 05:06:51
Rejected	Bernard Laboy	2023-08-31 09:36:09 - Service-now: Haris	CHG0000073	2023-02-28 05:12:19
Approved	Fred Luddy		CHG0000086	2023-02-28 05:13:12
Approved	Fred Luddy		CHG0000061	2023-02-28 05:10:45
Requested	Bernard Laboy		CHG0000090	2023-02-28 05:15:07
Requested	Bernard Laboy		CHG0000074	2023-02-28 05:12:23
Approved	Beth Anglin		CHG0000077	2023-02-28 05:13:00
No Longer Required	David Loo		CHG0000063	2023-02-28 05:10:48
Requested	Luke Wilson		CHG0000091	2023-02-28 05:15:11
No Longer Required	David Dan		CHG0000073	2023-02-28 05:11:04
Requested	Luke Wilson		CHG0000045	2023-02-28 05:07:48
Requested	Ron Kettering		CHG0000075	2023-02-28 05:12:27
Requested	Luke Wilson		CHG0000081	2023-02-28 05:13:36
Requested	Bernard Laboy		CHG0000055	2023-02-28 05:09:47
No Longer Required	David Loo		CHG0000092	2023-02-28 05:14:42
Requested	Bernard Laboy		CHG0000078	2023-02-28 05:13:24
Requested	Luke Wilson		CHG0000052	2023-02-28 05:09:35

b. Klicken Sie in der Spalte Status auf das angeforderte Element.

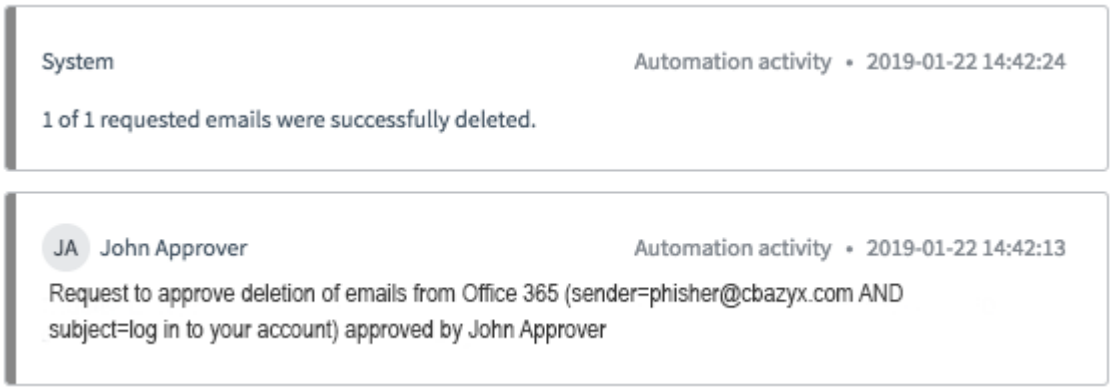
Im angezeigten Genehmigungsdatensatz werden Daten zur Suche, zur Suchanforderung und zu den Suchergebnissen aufgelistet.



c. Klicken Sie in diesem Datensatz auf **„Genehmigen“**, um die Anforderung zu genehmigen. Nachdem die Anforderung genehmigt wurde, initiiert das System den Lösch-Workflow, um die E-Mails zu entfernen. Die folgende Abbildung zeigt ein Beispiel für den Audit-Pfad, der von den Arbeitsnotizen im zugehörigen Security Incident-Datensatz für dieses Beispiel erstellt wurde. Nachdem diese Löschanforderung erneut übermittelt wurde, wird sie genehmigt. Unabhängig davon, welche Methode zum Genehmigen einer Anforderung verwendet wird, wird die Anzahl der erfolgreich gelöschten E-Mails in einer Arbeitsnotiz veröffentlicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem die E-Mails im zugehörigen Security Incident-Datensatz erfolgreich gelöscht wurden und Tagging aktiviert ist, ersetzt das Tag E-Mail-Löschung – Abgeschlossen das Tag E-Mail-Löschung – Initiiert.

Ein **Selfservice > Meine Genehmigungen** Für den Genehmiger (John Approver) ändert sich der Status von Angefordert in Genehmigt.

Ein **Selfservice > Meine Genehmigungen** Für andere Mitglieder der Genehmigungsgruppe, z. B. Jakob SecAdmin, ändert sich der Status in Nicht mehr erforderlich, nachdem die Anforderung genehmigt wurde.

3. Führen Sie alternativ die folgenden Schritte aus, um zu bestätigen, dass E-Mails im Datensatz „E-Mail-Suchergebnis“ im zugehörigen Security Incident-Datensatz gelöscht werden.

a. Navigieren zu **Security Incidents > Alle Incidents anzeigen** und lokalisieren Sie den Security Incident mit Phishing-Bezug.
Am Ende des Datensatzes werden die zugehörigen Listen angezeigt.

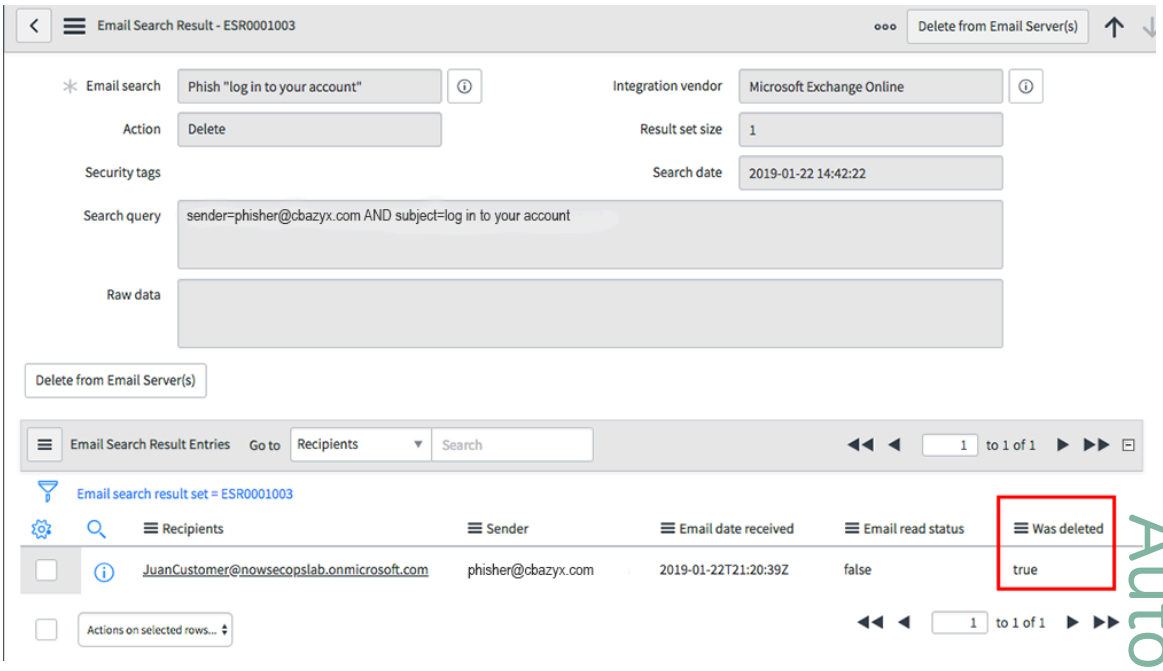
b. Klicken Sie auf die zugehörige Liste **E-Mail-Suche**.

c. Klicken Sie auf den Namen der Suche in der E-Mail-Suchspalte (Phishing „Anmelden bei Ihrem Account“).
Der Datensatz „E-Mail-Suche“ wird angezeigt. Wenn die zugehörige Liste „E-Mail-Suche“ nicht sichtbar ist, klicken Sie auf den Link **Alle zugehörigen Listen anzeigen**.

d. Klicken Sie auf die zugehörige Liste **E-Mail-Suchergebnisse**.
In der Spalte Suchdatum werden die Aktionen zum Suchen und Löschen von E-Mails mit entsprechenden Datumsangaben angezeigt.

e. Klicken Sie in der Spalte Suchdatum auf das Element, das der Löschaktion entspricht.
Im angezeigten Datensatz „E-Mail-Suchergebnis“, der angezeigt wird, zeigt der Status der Spalte Wurde gelöscht an, dass die E-Mail gelöscht ist (true).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie haben Anforderungen zum Löschen von E-Mails sowohl aus einer E-Mail-Benachrichtigung als auch aus einem Genehmigungsdatensatz erfolgreich genehmigt und bestätigt, dass E-Mails gelöscht werden. Weitere Informationen zum Auffinden des Datensatzes „E-Mail-Suchergebnis“ finden Sie unter Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im Service Microsoft Exchange Online an.

Integrationsarchitektur und externe Systemverbindung für die Microsoft Exchange Online -Integration

Die Microsoft Exchange Online -Integrationsarchitektur wurde entwickelt, um die Such- und Löschfunktionen für E-Mail-Bedrohungen im Service Microsoft Exchange Online zu unterstützen. In dieser Einführung wird erläutert, warum Sie in Ihren MicrosoftMicrosoft Azure Event Hubs -Accounts einige Setup-Schritte ausführen müssen, bevor Sie die Anwendung ServiceNow installieren.

Die Integrationsarchitektur basiert auf Bewertungen der derzeit verfügbaren Anwendungsprogrammierschnittstellen und auf Grundlage der Beratung durch das -Integrationspersonal von MicrosoftMicrosoft Azure Event Hubs. Diese Informationen sowie wichtige Begriffe zu den Services Now Platform und Microsoft Exchange Online werden bereitgestellt, um den konzeptionellen Betrieb der Integration zu verdeutlichen.

Für diese Integration verwendete Schlüsselbegriffe

Die folgenden Schlüsselbegriffe werden während der Installation und Konfiguration von verwendet. Weitere Informationen zu den folgenden Begriffen finden Sie auf der Website der ServiceNow-Produktdokumentation und auf der Microsoft-Dokumentationswebsite .

Now Platform

Ein Produkt des Unternehmens ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management (ITSM) und andere -Produkte aufbauen.

Security Incident Response (SIR)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Anwendung Now Platform, die den Fortschritt von Security Incidents von der Erkennung und ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur abschließenden Überprüfung und Schließung nach Incident verfolgt.

Microsoft Exchange Online

Das E-Mail-Serviceangebot für Microsoft Exchange Online, das Teil der Office 365-Suite von MicrosoftMicrosoft Azure Event Hubs -Produkten ist.

Global Graph API

Die von MicrosoftMicrosoft Azure Event Hubs bereitgestellte API, die für den Zugriff auf Postfachinformationen in Microsoft Exchange Onlineverwendet wird.

Zertifikatbasierte Authentifizierung

Mit dieser Authentifizierung können Kunden zulassen oder von Anwendern die direkte Authentifizierung mit X.509-Zertifikaten bei Azure Active Directory (Azure AD) für Anwendungen und die Browseranmeldung verlangen.

OAuth-Authentifizierung

Eine im Azure-Portal MicrosoftMicrosoft Azure Event Hubs erstellte ID, die zum Sammeln zusätzlicher E-Mail-Nachrichtendetails und zum Löschen von E-Mails in Microsoft Exchange Onlineverwendet wird.

Windows-Host

Spezifischer Typ des virtuellen Computers, der in dieser Integration verwendet wird.

MID-Server

Eine Anwendung Now Platform erleichtert die Kommunikation und das Verschieben von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services. Ein MID-Server ist normalerweise für die Integration mit lokalen Technologien erforderlich. In bestimmten Fällen kann jedoch ein MID-Server zwischen Now Platform und einem cloudbasierten Angebot bereitgestellt werden, wenn für die Integration eine vom Kunden bereitgestellte Komponente erforderlich ist. Bei dieser Microsoft Exchange Online -Serviceintegration erleichtert der MID-Server die Kommunikation zwischen dem Now Platform und dem PowerShell-Server.

PowerShell-Server

Der PowerShell-Server ist eine Microsoft-Anwendung, die Ihre Microsoft-Anmeldeinformationen erfordert.

Security Incident-Administrator (sn_si.admin)

Der Benutzer mit der Rolle sn_si.admin überwacht die Konfiguration der Integration mit dem SIR-Produkt in Ihrer Instanz Now Platform. Benutzer mit dieser Rolle genehmigen standardmäßig auch Löschanforderungen für E-Mails und weisen bei Bedarf die Rolle sn_si.analyst zu. Der Benutzer mit dieser Rolle hat auch vollständige Kontrolle über alle Servicemanagement -Daten.

Security Incident-Analyst (sn_si.analyst)

Der Benutzer mit der Rolle sn_si.analyst interagiert mit Security Incidents im Produkt SIR und analysiert sie.

Externe Systemverbindung zum Suchen und Löschen von E-Mails

Diese Anwendung verwendet den PowerShell-Service „Office 365 Security and Compliance Center“ und den Global Graph API-Service, um Informationen vom Servicemandanten von Office 365 Exchange Online abzurufen. Eine ausgehende HTTPS-Verbindung vom MID-Server zu dieser Umgebung ist erforderlich, damit die Integration ordnungsgemäß funktioniert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die -Integrationsarchitektur unterstützt die Funktion zum Suchen und Löschen von E-Mails im Service Microsoft Exchange Online. Die -Integrationsarchitektur zielt auf Phishing-E-Mails und andere E-Mail-Bedrohungen ab, die die Sicherheit Ihres Unternehmens gefährden können. Um E-Mails zu erhalten, die bestimmten Suchkriterien entsprechen, stellt der Now Platform eine Verbindung zu einem Microsoft Exchange Online -Servicemandanten her, der einen MID-Server verwendet, der PowerShell auf einem Windows-Server ausführt.

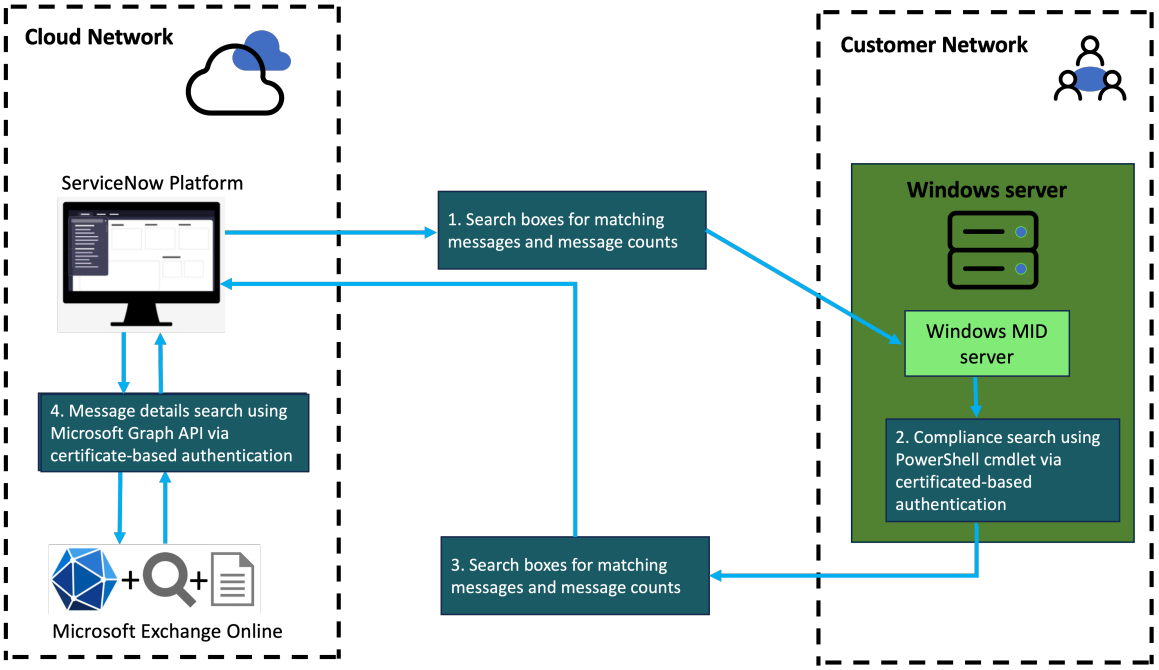
Nachdem Now Platform mit dem Service Microsoft Exchange Online verbunden wurde, unterstützt die Integration die folgenden Ebenen der E-Mail-Suche:

- Die übereinstimmenden Nachrichten: Diese Suche wird über das Microsoft PowerShell-Cmdlet über einen Windows-MID-Server durchgeführt, der eine Komponente von Now Platformist. Diese Suche basiert auf Kriterien, die Sie in Now Platform aus einem Security Incident konfigurieren. Die erste Komponente der Suche gibt alle E-Mail-Nachrichten zurück, die den von Ihnen konfigurierten Suchkriterien entsprechen, zusätzlich zu den spezifischen Postfachadressen, unter denen diese Nachrichten in Microsoft Exchange Onlinezu finden sind. Die unterstützten Suchparameter sind Betreff, Absender und Empfänger der E-Mail-Nachricht (der Wert, der im Feld An in einer E-Mail-Nachricht angezeigt wird).
- Die Nachrichtendetails: Nachdem die anfängliche Suche auf Basis von PowerShell-Cmdlets die übereinstimmenden Nachrichten identifiziert hat, ruft diese Suche mithilfe der Global Graph API MicrosoftMicrosoft Azure Event Hubs zusätzliche Nachrichteninformationen ab. Die zurückgegebenen E-Mail-Ergebnisse enthalten die folgenden Nachrichtendetails:
  - Lesestatus: Der Status „Wahr“ oder „falsch“ verfolgt, wenn Anwender E-Mails gelesen haben.
  - Absenderadresse.
  - Empfängeradresse: Diese Adressen umfassen Einzelpersonen, eine Gruppe und Personen, die in Nachrichten auf CC gesetzt und auf BCC gesetzt werden.
  - Löschstatus: Der Status „Wahr“ oder „falsch“ verfolgt gelöschte E-Mails.
  - Nachrichten-ID: Der alphanumerische Bezeichner von E-Mail-Nachrichten.

In der folgenden Abbildung ist der grundlegende Daten-Flow der E-Mail-Suche nach Nachrichtenanzahl und Nachrichtendetails dargestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Suche nach Anzahl der Nachrichten und Nachrichtendetails



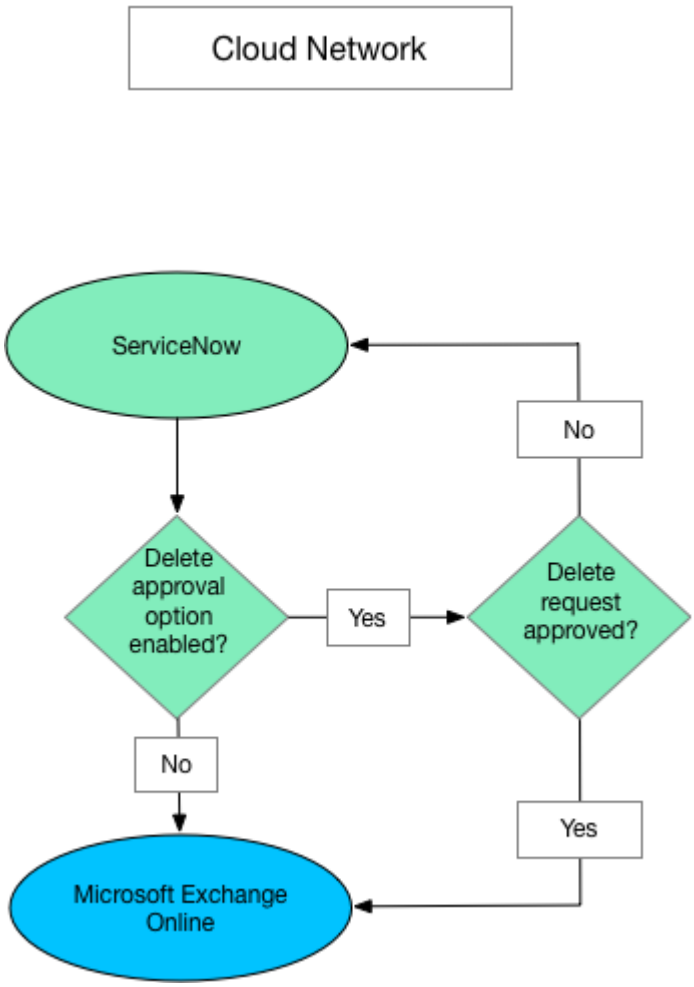
Zum Löschen von E-Mails verwendet die Integration die Global Graph API. Die Wiederherstellung gelöschter E-Mails ist als Option während des Konfigurationsschritts verfügbar und wird ausführlicher unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform .beschrieben.

In der folgenden Abbildung ist der Datenfluss zum Löschen von E-Mails mit dem vorkonfigurierten Genehmigungsprozess dargestellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail löschen



Flows

Die Anwendung Microsoft Exchange Online zum Suchen und Löschen von E-Mails enthält die folgenden Flows:

- Exchange online – E-Mails löschen.
- Ruft Exchange Online-E-Mail-Details ab.
- Microsoft Exchange Online -E-Mails suchen und löschen.

Sie können jetzt die für die Integration erforderlichen Accounts einrichten.

Stellen Sie gelöschte E-Mails im Service Microsoft Exchange Online wieder her

(Optional) Als Microsoft Exchange-Administrator können Sie gelöschte E-Mails wiederherstellen, wenn die Incident-Korrektur erfordert, dass Sie die vom Workflow dieser Integration gelöschten E-Mails wiederherstellen.

Vorbereitungen

Weitere Informationen zum Löschen von E-Mails durch diese Integration finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform ..

Weitere Informationen zur Administratorrolle im Produkt MicrosoftMicrosoft Azure Event Hubs Office 365, einschließlich Informationen zum Wiederherstellen gelöschter Elemente in einem -Benutzerpostfach, finden Sie unter Informationen zur Rolle „Exchange Online-Administrator“ .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin, Microsoft Exchange-Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie während des Konfigurationsschritts auf der Registerkarte Zusätzliche Einstellungen die Option **Gelöschte E-Mails wiederherstellen** auswählen, aktivieren Sie die Wiederherstellung gelöschter E-Mails in Ihrem Mandanten Microsoft Exchange Online. E-Mails, die mit dem Lösch-Workflow dieser Integration gelöscht wurden, werden im Unterordner „Gelöschte Elemente“ des Ordners „Wiederherstellbare Elemente“ im Postfach des Anwenders im Service Microsoft Exchange Online platziert. Wenn der Account des Benutzers im Mandanten Microsoft Exchange Online so konfiguriert ist, dass der Benutzer den Ordner „Gelöschte Elemente“ anzeigen kann, kann er diese E-Mails mithilfe des Outlook-Service MicrosoftMicrosoft Azure Event Hubs im Web wiederherstellen. Alternativ kann der Administrator Microsoft Exchange Online gelöschte E-Mails aus dem Ordner „Gelöschte Elemente“ eines Benutzers wiederherstellen. Weitere Informationen finden Sie unter Gelöschte Elemente oder E-Mails in Outlook Web App wiederherstellen .

Erforderliche Rolle: Microsoft Exchange Online Administrator oder MicrosoftMicrosoft Azure Event Hubs Globaler Administrator zur Wiederherstellung gelöschter E-Mails.

Erforderliche Rolle: sn_si.admin in Now Platform, um die Option Gelöschte E-Mails wiederherstellen zu aktivieren.

Erforderliche Rolle: sn_si.analyst in Now Platform, um eine erfolgreiche Suche nach E-Mails abzuschließen und zu überprüfen, ob E-Mails vor der Wiederherstellung erfolgreich gelöscht wurden.

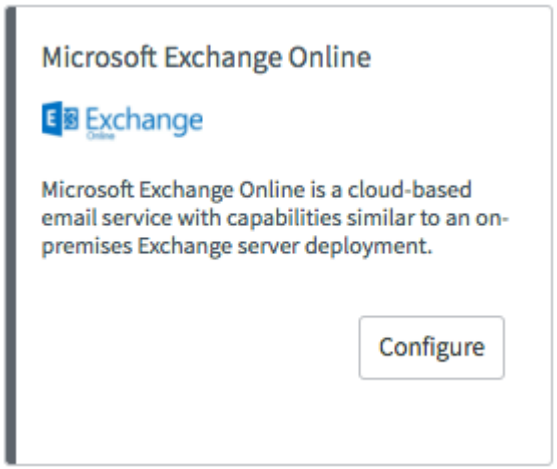
Prozedur

Führen Sie die folgenden Schritte aus, um die Option zur E-Mail-Wiederherstellung zu aktivieren.

a. Navigieren zu **Security Operations** > **Integrationen** > **Konfigurationen**.

b. Suchen Sie die Kachel Microsoft Exchange Online.

c. Klicken Sie auf **Konfigurieren**.

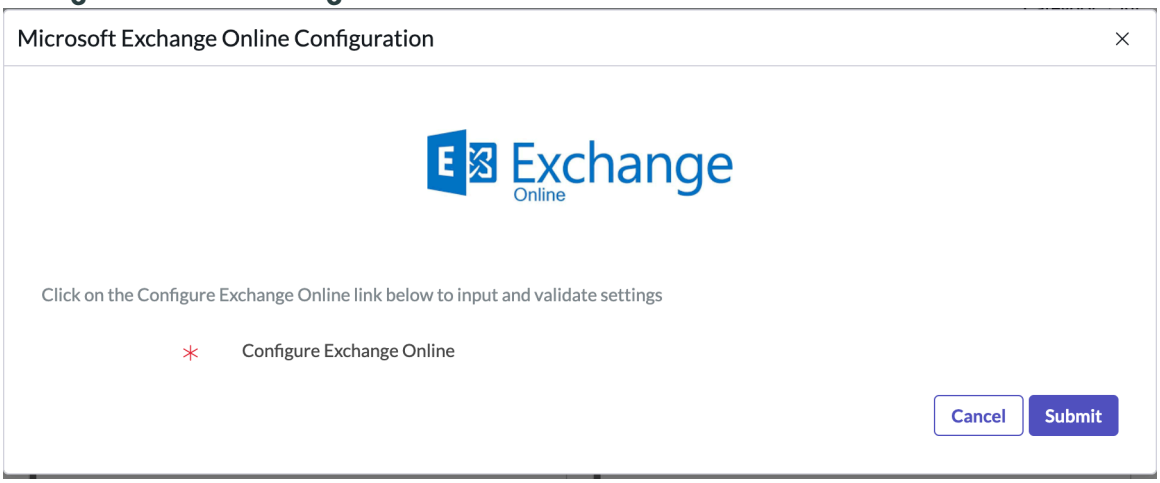


d. Klicken Sie im Dialogfeld Microsoft Exchange Online Konfiguration, das angezeigt wird, **auf Exchange Online konfigurieren**.

Automatische Übersetzung

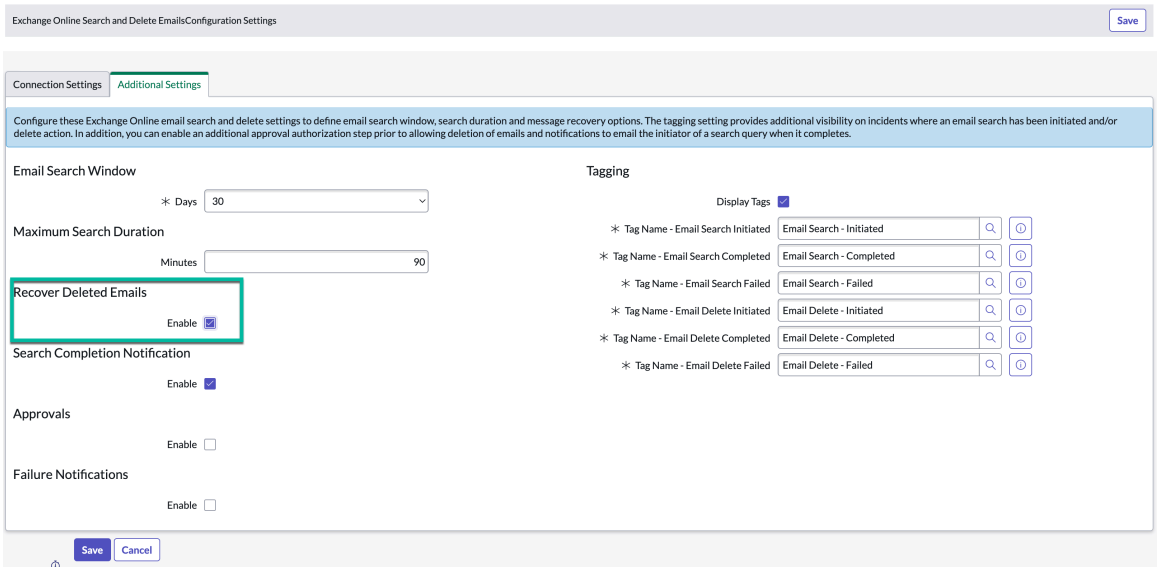
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Exchange Online



e. Aktivieren Sie auf der Registerkarte Zusätzliche Einstellungen unter Gelöschte E-Mailswiederherstellen das Kontrollkästchen **Aktivieren**.

Gelöschte E-Mails wiederherstellen



f. Überprüfen Sie alle anderen Einstellungen, und klicken Sie auf **Absenden**.

g. Um zu überprüfen, ob das Suchen und Löschen von E-Mail-Nachrichten für die wiederherzustellenden E-Mail-Nachrichten erfolgreich abgeschlossen wurden, navigieren Sie zu dem Security Incident, der die Workflows zum Suchen und Löschen von E-Mails protokolliert hat.

h. Suchen Sie die Arbeitsnotizen, und vergewissern Sie sich, dass das System die Nachrichten erfolgreich gelöscht hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Melden Sie sich als Microsoft Exchange Online -Administrator oder globaler Administrator bei Ihrem MicrosoftMicrosoft Azure Event Hubs Office 365-Konto an.

j. Führen Sie die unter Gelöschte Elemente oder E-Mails in Outlook Web App wiederherstellen auf der Dokumentationswebsite MicrosoftMicrosoft Azure Event Hubs beschrieben aus.

Bearbeiten Sie Sicherheits-Tags auf der Now Platform für die Microsoft Exchange Online -Integration

Sie können die Namen und Farben der Sicherheits-Tags in Ihrer Instanz Now Platform® für die Integration Microsoft Exchange Online bearbeiten. Mithilfe dieser Sicherheits-Tags können Sie schnell erkennen, wann die E-Mail-Suche abgeschlossen wird oder fehlschlägt. Sie identifizieren auch, wenn Anforderungen zum Löschen von E-Mails initiiert werden und wenn die E-Mail-Elemente erfolgreich gelöscht werden.

Vorbereitungen

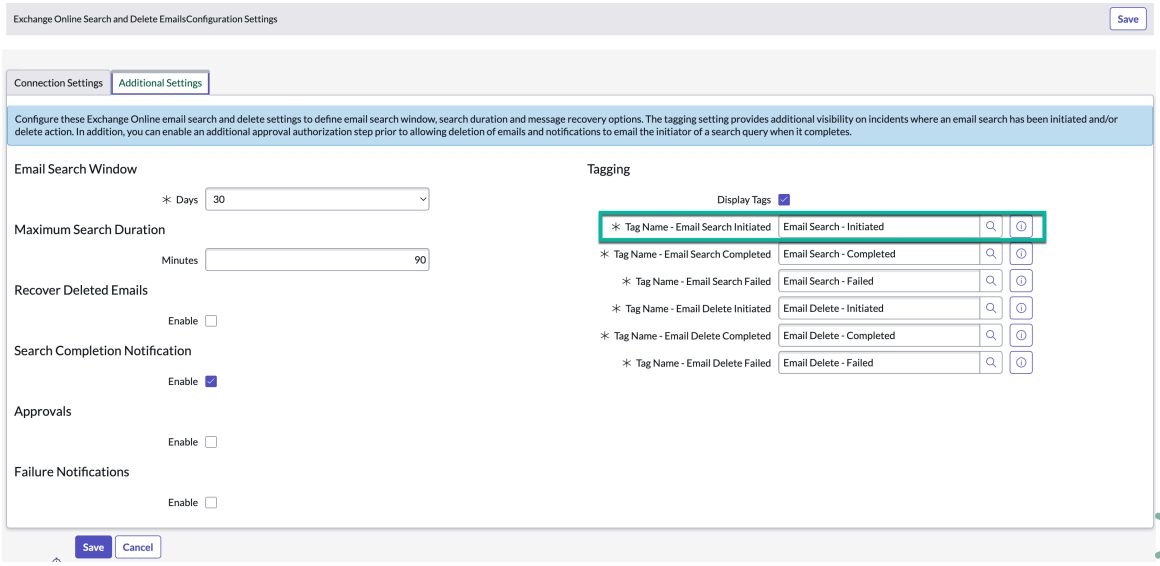
Standardmäßig sind die Sicherheits-Tags in Ihrer Instanz Now Platform® aktiviert, wenn Sie während des Konfigurationsschritts die Option **Tags anzeigen** auswählen. Sie können Tag-Farben und -Namen bearbeiten und Sicherheits-Tag-Gruppen Tags zuweisen, um sie in Ihrer Instanz Now Platform® zu organisieren. Sie können beispielsweise die Farben der Tags so ändern, dass das Start-Tag einer Fähigkeit eine Farbe und das Abschluss-Tag eine andere Farbe aufweist, um sie an die anderen in Ihrer Instanz Now Platform® aktivierten Sicherheits-Tags anzupassen. Anhand dieser verschiedenen Farben können Sie schnell erkennen, wann Workflows gestartet und erfolgreich abgeschlossen wurden. Wenn Sie entscheiden, dass Sie ein bestimmtes Tag nicht benötigen, ohne das Tagging für die Integration zu deaktivieren, können Sie auch ein einzelnes Tag im Tag-Datensatz deaktivieren. Wenn die Option deaktiviert ist, wird dieses Tag nicht mehr in den zugehörigen Security Incidents angezeigt. Weitere Informationen zum Einrichten von Sicherheits-Tag-Gruppen und Tags finden Sie unter Sicherheits-Tag-Gruppen und Tags einrichten auf der Website der ServiceNow-Produktdokumentation .

Erforderliche Rolle: sn_si.admin

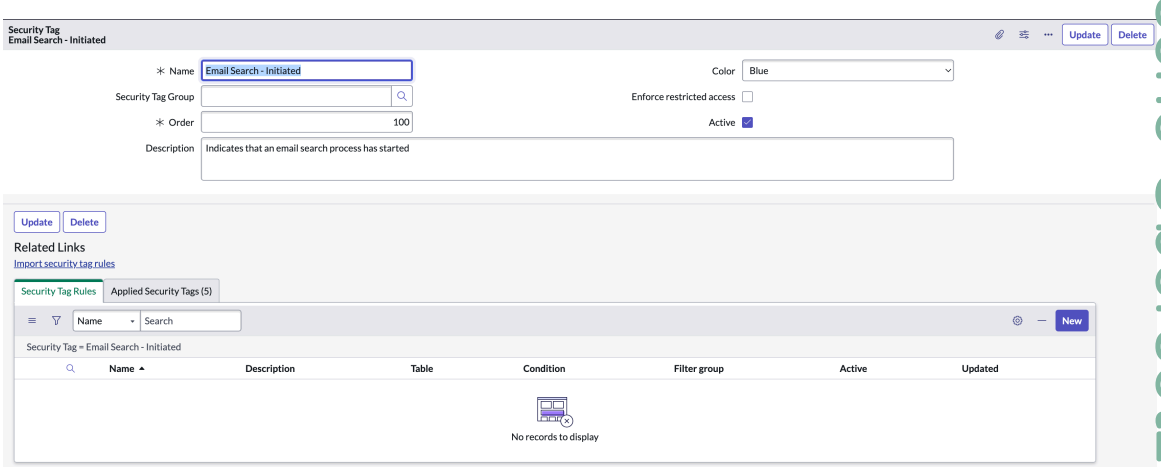
Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Exchange Online-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Zusätzliche Einstellungen**, um sie auszuwählen.
3. Wenn die Option **Tags anzeigen** auf der angezeigten Registerkarte deaktiviert ist, wählen Sie sie aus, um Tag-Namen anzuzeigen.
4. Klicken Sie bei angezeigten Tag-Namen rechts neben einem Tag auf das Informationssymbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie im angezeigten Dialogfeld „Sicherheits-Tag“ **auf Datensatz öffnen**.
6. Bearbeiten Sie im angezeigten Datensatz die Felder.
7. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.



Sie haben jetzt den Tag-Datensatz für ein Sicherheits-Tag erfolgreich bearbeitet.

Prüfliste für die Microsoft Exchange Online -Integration

Verwenden Sie diese Prüfliste, um sich durch die End-to-End-Aufgaben der Integration führen zu lassen. Die folgende Prüfliste enthält Einrichtungs- und Installationsaufgaben sowie Beispiele für Anwendungsfälle und erwartete Ergebnisse für die Anwendung.

Vorbereitungen

Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration anhand der folgenden Tabelle. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jeder Schritt identifiziert die Rollen, die zum Ausführen der Aufgaben erforderlich sind, und verweist auf die nummerierten Themen im Installations- und Konfigurationsleitfaden für diese Integration.

Erforderliche Rollen: In der folgenden Tabelle werden für jeden Schritt Rollen aufgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Um Ihren Fortschritt für die Integration nachzuverfolgen, folgen Sie den Schritten in der Tabelle in der Reihenfolge, in der sie angezeigt werden

Prüfliste

☐	Richten Sie als MicrosoftMicrosoft Azure Event Hubs Office 365-Administrator Ihr MicrosoftMicrosoft Azure Event Hubs Office 365-Konto ein. Erstellen Sie ein API-Konto, das den Zugriff auf das Security and Compliance Center in MicrosoftMicrosoft Azure Event Hubs Office 365 ermöglicht.
☐	Richten Sie als MicrosoftMicrosoft Azure Event Hubs Azure-Administrator Ihr MicrosoftMicrosoft Azure Event Hubs Azure-Konto ein. Erstellen Sie ein Konto, das eine Anwendungs-ID verwendet, um zusätzliche Details von E-Mail-Nachrichten zu sammeln und E-Mail-Nachrichten zu löschen. Schritte zum Einrichten des Kontos finden Sie unter Richten Sie Ihr MicrosoftMicrosoft Azure Event Hubs Azure-Konto für die ServiceNow Microsoft Exchange Online -Integration ein.
☐	Richten Sie als Now Platform -Administrator Ihre Instanz Now Platform für die Integration ein. Aufgaben und weitere Informationen finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration Microsoft Exchange Online ein. **a.** Weisen Sie Now Platform Rollen zu. **b.** Richten Sie einen MID-Server in Ihrer Instanz Now Platform ein. **c.** Installieren Sie die Anwendungen Now Platform (SIR) und Security Operations aus dem ServiceNow Store, und aktivieren Sie sie in Ihrer -Instanz. **d.** Aktivieren Sie die Funktionen zum Senden und Empfangen von E-Mails. **e.** Weisen Sie sn_si.analyst die Rolle zum Lesen und Schreiben von E-Mails zu. **f.** Erstellen Sie eine Genehmigungsgruppe.
☐	Als Now Platform -Administrator installieren Sie die Anwendung für die Integration aus dem ServiceNow Store. Schritte zur Installation finden Sie unter Installieren Sie die Anwendung Microsoft Exchange Online für die Integration ServiceNow Microsoft Exchange Online ..
☐	Füllen Sie als sn_si.admin die Registerkarten mit Konfigurationseinstellungen aus, um Verbindungen herzustellen und die Such- und Lösch-Workflows zu aktivieren. Informationen zu Verbindungs- und Konfigurationseinstellungen finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer -Instanz Now Platform ..

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

☐	Richten Sie als sn_si.analyst E-Mail-Suchkriterien ein, und fordern Sie eine Suche nach übereinstimmenden E-Mails auf dem Server Microsoft Exchange Online an. Ein Beispiel finden Sie unter Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im Service Microsoft Exchange Online an. **a.** Suchen Sie Security Incidents im Zusammenhang mit Phishing-Ereignissen. **b.** Richten Sie E-Mail-Suchkriterien ein. **c.** Fordern Sie eine Suche nach E-Mails an. **d.** Suchen Sie Suchergebnisse und Nachrichtendetails in den zugehörigen Listen im Security Incident.
☐	Löschen Sie als sn_si.analyst E-Mails vom Server Microsoft Exchange Online. Ein Beispiel finden Sie unter Fordern Sie die Löschgenehmigung für E-Mails im Microsoft Exchange Online-Service an. **a.** Suchen Sie Security Incidents mithilfe von Suchergebnissen. **b.** Löschen Sie E-Mails, oder fordern Sie die Genehmigung zum Löschen von E-Mails an. **c.** Verifiziert, ob E-Mails aus den Ergebnissen gelöscht werden, die in den Arbeitsnotizen und zugehörigen Listen im Security Incident veröffentlicht werden.
☐	Als sn_si.admin oder als Mitglied einer Genehmigungsgruppe verarbeiten Sie Anforderungen zum Löschen von E-Mails über E-Mail-Benachrichtigungen. Ein Beispiel finden Sie unter Genehmigen Sie E-Mail-Löschungsanforderungen für die Integration Microsoft Exchange Online ..

Sie haben die Einrichtungsschritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration verifiziert.

Problembehandlung bei der Microsoft Exchange Online-Integration

Nachdem Sie die Anwendung Microsoft Exchange Online erfolgreich konfiguriert und Ihre Instanz Now Platform eingerichtet haben, können Sie bei E-Mail-Suchproblemen Diagnosetests basierend auf bestimmten Kriterien ausführen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Ergebnisse dieser Tests können dem Kundensupport ServiceNow von helfen, die Probleme zu identifizieren und zu beheben.

Prozedur

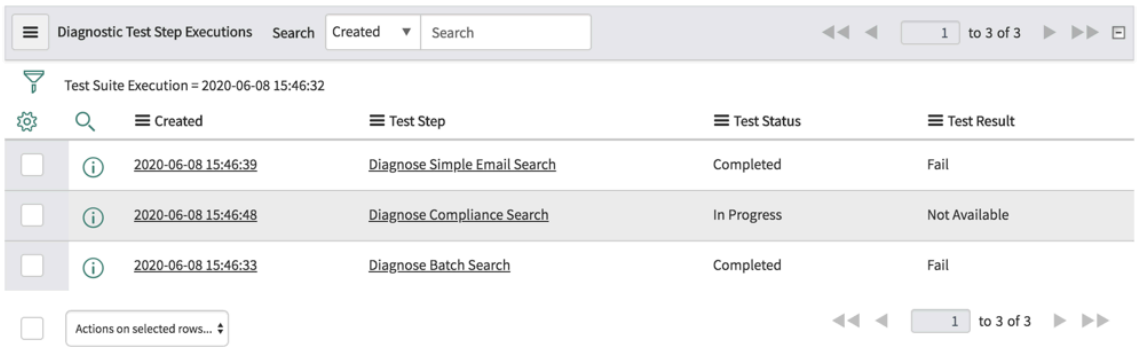
1. Navigieren zu **Alle** > **Exchange Online-Diagnose** > **Diagnosetests initiieren**.
2. Geben Sie die folgenden Details ein:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geben Sie den Absender und eine oder mehrere Empfänger-E-Mail-Adressen ein, um die Suchkriterien einzugrenzen und genauere Ergebnisse zu erhalten.
- Geben Sie den Betreff an, für den die Diagnosetests durchgeführt werden. Das ist ein Pflichtfeld.

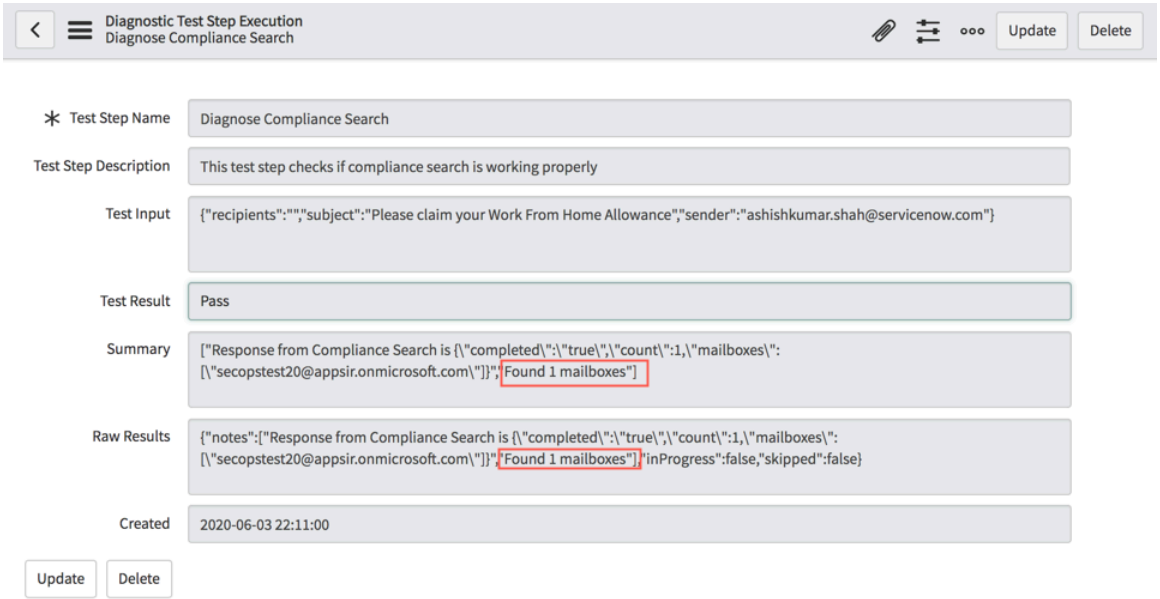
3. Klicken Sie auf **Absenden**.
4. Um die Ergebnisse der Diagnosetests anzuzeigen, navigieren Sie zu **Exchange Online-Diagnose** > **Ergebnisse der Diagnosetests anzeigen**.
   Die Spalte „Status“ zeigt die folgenden Status an:
   - Abgeschlossen – Bestanden: Die Tests wurden erfolgreich abgeschlossen.
   - Abgeschlossen – Fehler: Die Tests wurden mit einigen Fehlern abgeschlossen.
   - In Bearbeitung: Die Tests werden noch ausgeführt und wurden nicht abgeschlossen.
5. Klicken Sie auf die Ausführung der Diagnosetest-Suite, um die Details zur Testausführung anzuzeigen.



   Die folgenden Arten von Diagnosetests werden ausgeführt:
   - Diagnose-Compliance-Suche: Generiert eine Liste von Empfänger-E-Mail-Postfächern, indem eine Compliance-Suche durchgeführt wird.
   - Einfache E-Mail-Suche diagnostizieren: Durchsucht E-Mail-Postfächer durch separate REST-Aufrufe, um jeden Ordner des Empfängers zu durchsuchen.
   - Diagnose-Batch-Suche: Durchsucht Postfächer in einer Batch-Abfrage, indem mehrere Suchvorgänge in einem REST-Aufruf kombiniert werden.

   Um die Tests 2 und 3 durchzuführen, müssen Sie die Empfänger-E-Mail-Adressen auf der Seite Diagnosetests initiieren angeben. Wenn sie nicht angegeben sind, werden die Tests nicht durchgeführt.
6. Klicken Sie auf den Link Erstellt auf der Seite Ausführung der Diagnose-Test-Suite, um die Testergebnisse im Detail anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die obige Abbildung zeigt die detaillierten Ergebnisse der Ausführung des Testschritts „Diagnose-Compliance-Suchtest“ sowie die Anzahl der bei der Suche gefundenen Postfächer.

Wichtig:
Zusätzliche Problembehandlungsszenarien und -probleme finden Sie unter KB1501969: Einrichtung und Problembehandlung der zertifikatsbasierten Authentifizierung für die Exchange Online-Integration

Integration mit Microsoft Exchange lokal

Die lokale Integration Microsoft Exchange von bietet Sicherheitsanalysten Tools, um Phishing- und Spear-Phishing-E-Mail-Bedrohungen in lokalen Instanzen einzudämmen und zu beseitigen.

Erkunden

Security Incident Response-Integrationen

Einrichten

Erste Schritte mit der Integration von Microsoft Exchange On-Premises

Verwenden

Suchen und löschen Sie Phishing-E-Mails

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der Integration von Microsoft Exchange On-Premises

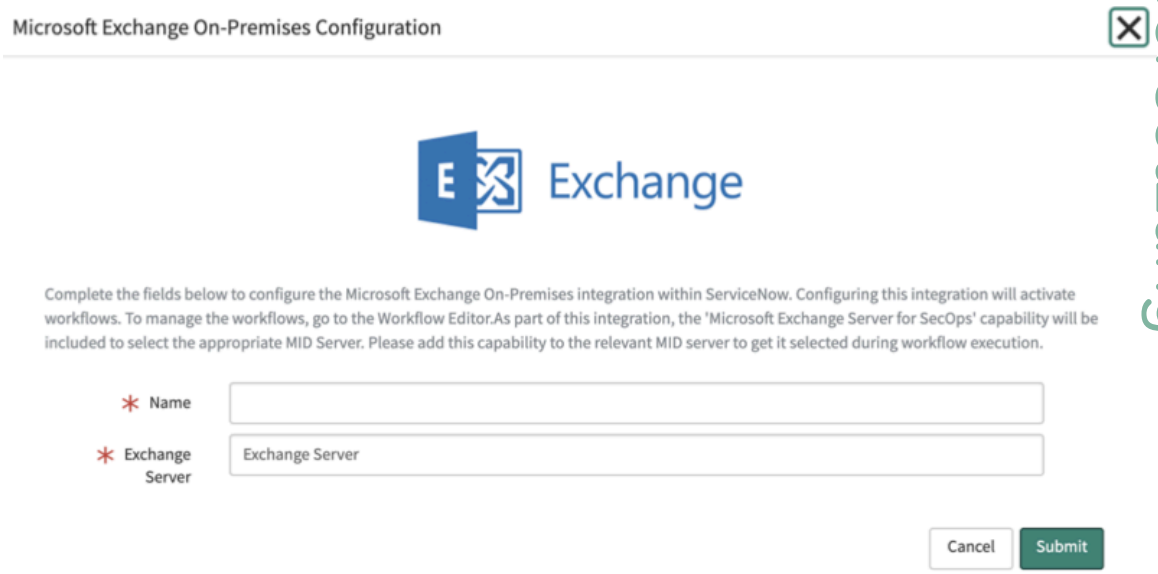
Die lokale Integration Microsoft Exchange von bietet Sicherheitsanalysten Tools zum Eindämmen und Beheben von Phishing- und Spear-Phishing-E-Mail-Bedrohungen in lokalen Instanzen. Bevor Sie die lokale Integration Microsoft Exchange verwenden können, müssen Sie sie von ServiceNow Store herunterladen und die entsprechenden Exchange- und MID-Server identifizieren.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte Microsoft Exchange Lokal auf **New (Neu)**.



4. Füllen Sie die Felder nach Bedarf aus.

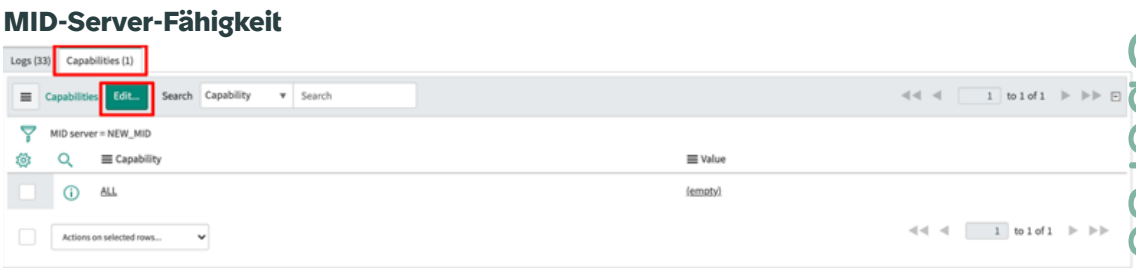
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Exchange Server	Geben Sie den zu verwendenden Exchange-Server an.

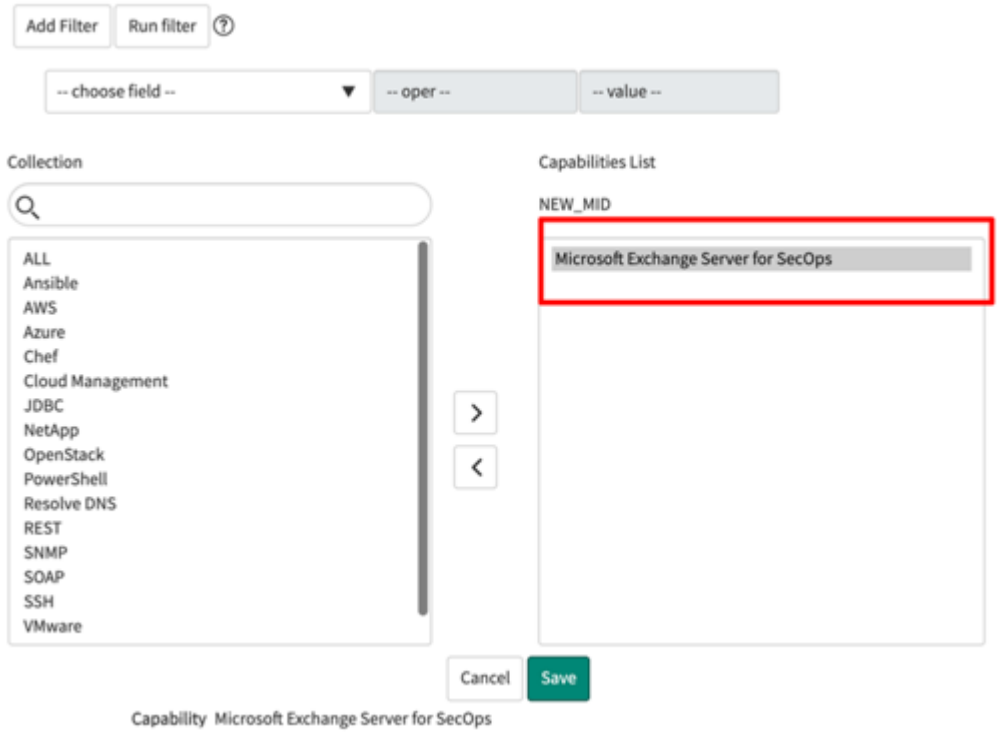
Hinweis:
Durch die Konfiguration dieser Integration werden Flows aktiviert. Um die Flows zu verwalten, navigieren Sie zu **Workflow-Studio/Flow Designer.**.

5. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern bzw. zu löschen.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.
8. Navigieren zu **Orchestration** > **MID-Server**.
9. Öffnen Sie den Datensatz, und überprüfen Sie, ob der Status des MID-Servers erreichbar ist, der für den Exchange-Server erreichbar ist, und dass die Option **Status** auf **In Betrieb** und **Validiert** auf **Ja**festgelegt ist.
10. Fügen Sie die MID-Server-Fähigkeit hinzu:
    - Wählen Sie den entsprechenden MID-Server aus, um die Fähigkeit hinzuzufügen.
    - Klicken Sie auf die zugehörige Liste **Fähigkeiten** und klicken Sie auf **Bearbeiten**.



    - Entfernen Sie **Alle**, und fügen Sie **Microsoft Exchange Server for SecOps**hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Wählen Sie im Abschnitt **„Zugehörige Listen“** die **IP-Bereiche** aus, und legen Sie den Wert entweder auf **ALLE** oder einen beliebigen Wert fest.
- Wählen Sie im Abschnitt **„Zugehörige Listen“** die **unterstützten Anwendungen** aus, und legen Sie den Wert entweder auf ALLE oder Orchestration fest.
- **Speichern Sie** den Datensatz.

11. Validieren Sie die Verbindungen und Anmeldeinformationen.
12. Sobald die Anmeldeinformationen validiert wurden, ist die Konfiguration in der ServiceNow-Instanz abgeschlossen und bereit, E-Mail-Such- und Löschvorgänge mit dieser Integration auszuführen.

Microsoft Exchange – Flow zum Suchen und Löschen von E-Mails

Wenn der Flow **„Microsoft Exchange – E-Mail-Suche und -Löschung durchführen“** ausgeführt wird, wird der Exchange-Server mit der angegebenen Suchabfrage durchsucht, und die Details werden an die lokale Instanz zurückgegeben.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Der Flow **„Microsoft Exchange – E-Mail-Suche und -Löschung durchführen“** wird ausgeführt, wenn E-Mail-Suchen eingerichtet sind und die Schaltfläche **„Aus E-Mail-Servern löschen“** oder **„Auf E-Mail-Servern suchen“** angeklickt wird.

Spezifische Aktionen für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Die Flow-Aktionen umfassen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie eine Compliance-Suchaktion
- Aktion zum Überprüfen des Compliance-Suchstatus

Vorschau-Aktion für Compliance-Suche erstellen

Mit der Vorschauaktion für Compliance-Suche erstellen wird eine neue Compliance-Suchaktion vom Typ „Vorschau“ auf dem Exchange-Server für die erstellte Compliance-Suche erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Pflichtfeld für den Zielhostbezeichner, an dem sich der Exchange-Server befindet.
searchName	Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Abgeschlossen	Wenn die Compliance-Suchaktion erfolgreich erstellt wurde.
Fehler beim Erstellen der Aktion	Wenn die Erstellung der Compliance-Suchaktion aufgrund einer Ausnahme in Exchange Server fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Status der Vorschauaktion überprüfen

Der Status der Vorschauaktion überprüft den Status der Compliance-Suchaktion vom Typ Vorschau und gibt die Vorschauinformationen der gefundenen E-Mails zurück, z. B. Empfänger, Absender, Betreff, Empfangsdatum der E-Mail.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
targetId	Pflichtfeld für den Zielhostbezeichner, an dem sich der Exchange-Server befindet.
searchName	Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
response	Enthält den Status der Compliance-Suchaktion und die Vorschauinformationen der als Teil der Compliance-Suche gefundenen E-Mail.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Vorschau in Bearbeitung	Wenn der Status der Compliance-Suchaktion ausgeführt wird.
Keine E-Mail gefunden	Wenn der Status der Compliance-Suchaktion abgeschlossen ist und keine E-Mails als Teil der Compliance-Suche gefunden wurden.
Vorschau abgeschlossen	Wenn der Status der Compliance-Suchaktion abgeschlossen ist und E-Mails als Teil der Compliance-Suche gefunden werden.
Fehler beim Überprüfen des Status	Wenn die Statusüberprüfung aufgrund einer Ausnahme in Exchange Server fehlschlägt.
Fehler	Wenn in der Workflow-Aktivität eine Ausnahme auftritt.

Lösch-Aktion für Compliance-Suche erstellen

Mit der Löschaktion „Compliance-Suche erstellen“ wird auf dem Exchange-Server für die erstellte Compliance-Suche eine neue Compliance-Suchaktion vom Typ „löschen“ erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Pflichtfeld für den Zielhostbezeichner, an dem sich der Exchange-Server befindet.
searchName	Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Abgeschlossen	Wenn die Compliance-Suchaktion erfolgreich erstellt wurde.
Fehler beim Erstellen der Aktion	Wenn die Erstellung der Compliance-Suchaktion aufgrund einer Ausnahme in Exchange Server fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Löschaktion überprüfen

Die Status der Löschaktion überprüfen überprüft den Status der Compliance-Suchaktion vom Typ „Löschen“ und führt einen vorläufigen Löschvorgang auf dem Exchange-Server für die als Teil der Compliance-Suche gefundenen E-Mails aus.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Pflichtfeld für den Zielhostbezeichner, an dem sich der Exchange-Server befindet.
searchName	Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Enthält den Status der Compliance-Suchaktion und die Anzahl der gelöschten E-Mails, die als Teil der Compliance-Suche gefunden wurden.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Löschen in Bearbeitung	Wenn der Status der Compliance-Suchaktion ausgeführt wird.
Keine E-Mail gefunden	Wenn der Status der Compliance-Suchaktion abgeschlossen ist und keine E-Mails als Teil der Compliance-Suche gelöscht werden.
Löschen abgeschlossen	Wenn der Status der Compliance-Suchaktion abgeschlossen ist, werden E-Mails als Teil der Compliance-Suche gelöscht.
Fehler beim Überprüfen des Status	Wenn die Statusüberprüfung aufgrund einer Ausnahme in Exchange Server fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Compliance-Suchaktion entfernen

Mit der Aktion „Compliance-Suche entfernen“ wird die erstellte Compliance-Suche aus Exchange Server entfernt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
targetId	Pflichtfeld für den Zielhostbezeichner, an dem sich der Exchange-Server befindet.
searchName	Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche.

Integration der Microsoft Graph-Sicherheits-API zur Warnungserfassung

Verwenden Sie die -Integration Microsoft Graph-Sicherheits-API, um Warnungen von Microsoft Graph-Sicherheitsanbietern zu erfassen und automatisch Security Incidents zu erstellen.

Übersicht

Microsoft Graph-Sicherheits-API ist ein intermediärer Service (oder Broker), der eine einzige programmgesteuerte Schnittstelle für die Verbindung mehrerer Sicherheitsanbieter (native zu Microsoft sowie ServiceNow-Partner) bereitstellt.

Die Microsoft Graph-Sicherheits-API -Integration behebt diese Probleme, indem sie Microsoft Graph-Sicherheits-API verwendet, um eine Verbindung mit verschiedenen Microsoft-Sicherheitstechnologien wie Azure Sentinel, Microsoft Defender Advanced Threat Protection und Azure Advanced Threat Protection herzustellen. In Security Incident Responsewerden Warnungen von Microsoft-Sicherheitsanbietern erfasst, und Security Incidents werden automatisch erstellt.

Schlüsselfunktionen

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Erkennung von Microsoft Graph-Sicherheits-API -Warnungen, die Kandidaten für Security Incidents sind, und Automatisierung der Erstellung von -Security Incidents.
- Zuordnung von Warnungsfeldern zu Security Incident-Feldern.
- Zusammenfassung ähnlicher Warnungen zu vorhandenen offenen Security Incidents, anstatt doppelte Security Incidents zu erstellen.
- Zeigen Sie eine Vorschau der Warnungsfeldwerte an, und validieren Sie ihre Zuordnungen im Security Incident.
- Automatische Aktualisierung des Warnungsstatus für die Erstellung und den Abschluss von Security Incidents.
- Richten Sie eine geplante Erfassung von Warnungen ein, um regelmäßig Security Incidents zu erstellen.

Richten Sie Ihre Now Platform-Instanz für die Integration der Microsoft Graph-Sicherheits-API ein

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in der Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung von ServiceNow Storeinstallieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sehen Sie sich die folgende Tabelle an, und vergewissern Sie sich, dass Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response zugewiesen haben.	Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Instanz Now Platform® von erforderlich. • Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Ein Benutzer mit der Rolle sn_si.admin überwacht die folgenden Aufgaben in Now Platform®: ◦ Benennt, erstellt und bearbeitet Warnungsprofile. ◦ Wählt Warnungsdatenfelder der Microsoft Graph-Sicherheits-API aus und ordnet sie den Feldern für Security Incidents zu. ◦ Zeigt eine Vorschau der Details von Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird. ◦ Plant die laufende Warnungserfassung. ◦ Aktiviert Warnungsaktualisierungen, wenn der Incident Security Incident Response erstellt und geschlossen wird. ◦ Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu. ◦ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Rollen auf der Website der ServiceNow-Produktdokumentation .
Registrieren Sie Ihre -Anwendung im -Portal Microsoft Azure.	Bevor Sie Warnungen erfassen können, müssen Sie Ihre Anwendung im -Portal Microsoft Azure konfigurieren. Details siehe Konfigurieren Sie das Microsoft Azure-Portal.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Event and Alert Ingestion for Security Operations: Diese Anwendung benötigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST **Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Ereignis- und Warnungserfassung“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport. Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Konfigurieren Sie das Microsoft Azure-Portal

Um Sicherheitswarnungen für eine Anwendung abzurufen, die im Microsoft Azure-Mandanten mit Microsoft Graph-Sicherheits-APIverfügbar ist, müssen Sie die Anwendung im Portal Microsoft Azure registrieren und der Anwendung Lese- und Schreibzugriff für Sicherheitsereignisse gewähren.

Vorbereitungen

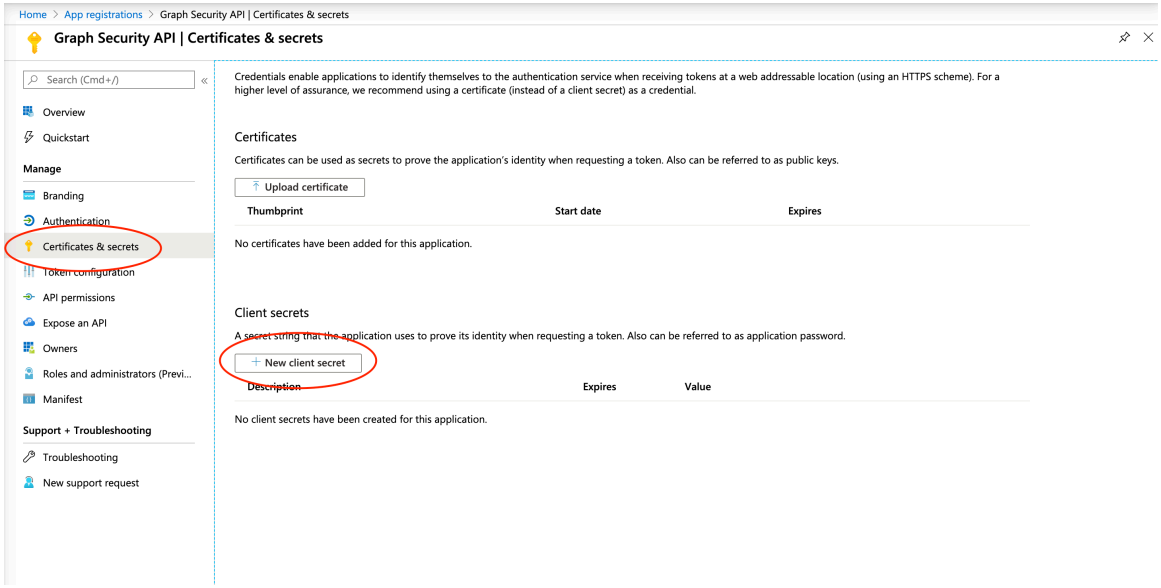
Erforderliche Rolle:

- Anwendungsentwickler: Erforderlich für die Registrierung der Anwendung.
- Mandantenadministrator: Der Mandantenadministrator Microsoft Azure muss der Anwendung Berechtigungen für erteilen, indem er einen Aufruf an den Endpunkt der Administratoreinwilligung durchführt.

Prozedur

1. Melden Sie sich beim -Portal Microsoft Azure an.
2. Geben Sie im **SuchfeldApp-Registrierungen** ein.
3. Klicken Sie auf **New registration (Neue Registrierung)**.
4. Geben Sie einen Namen für Ihre Anwendung und den Umleitungs-URI ein, z. B. http://localhost, und klicken Sie auf **Registrieren**.
   Der Umleitungs-URI wird verwendet, wenn die Administratoreinwilligung für die Anwendung erteilt wird.
5. Wählen Sie auf der Seite „App-Registrierungen“ die Anwendung aus, die Sie registriert haben, z. B. Graph Security Demo.
6. Wählen Sie unter **Verwalten**die Option **Zertifikate und Geheimnisse**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

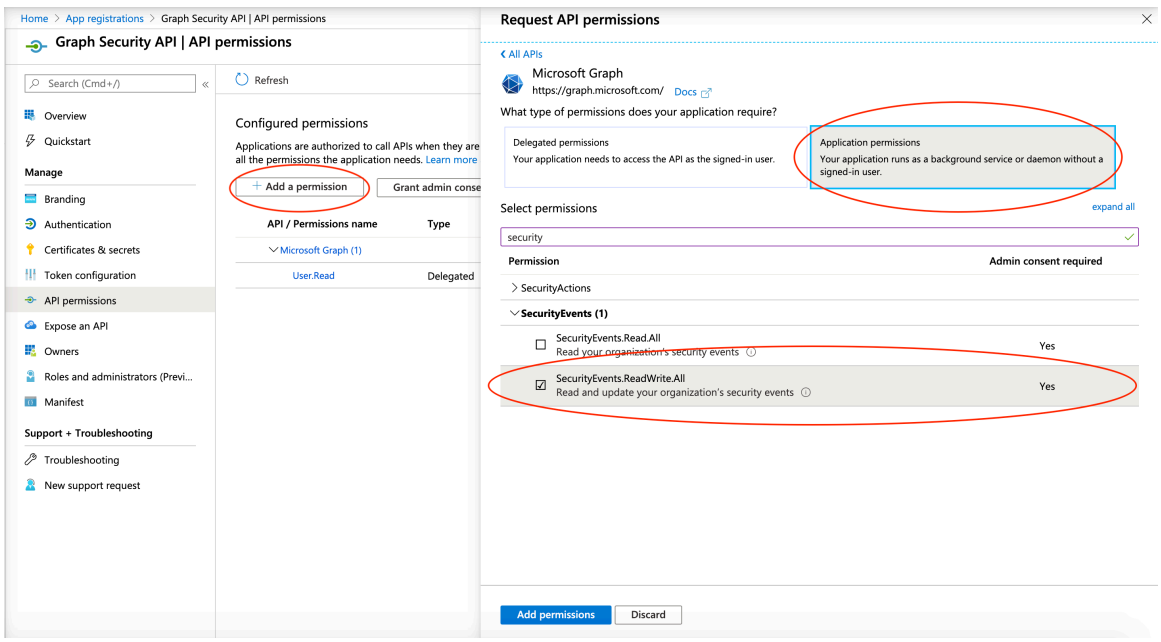


7. Wählen Sie **Neuer geheimer Clientschlüssel** aus, um einen geheimen Clientschlüssel zu erstellen. Kopieren Sie den geheimen Clientschlüssel, und speichern Sie ihn, da er später nicht sichtbar ist. Falls Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen geheimen Clientschlüssel generieren.

   Hinweis:
   Wenn Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen generieren, indem Sie die Anweisungen in den Schritten 4 und 5 befolgen.

8. Klicken Sie auf der Seite Übersicht **auf API-Berechtigungen anzeigen**.

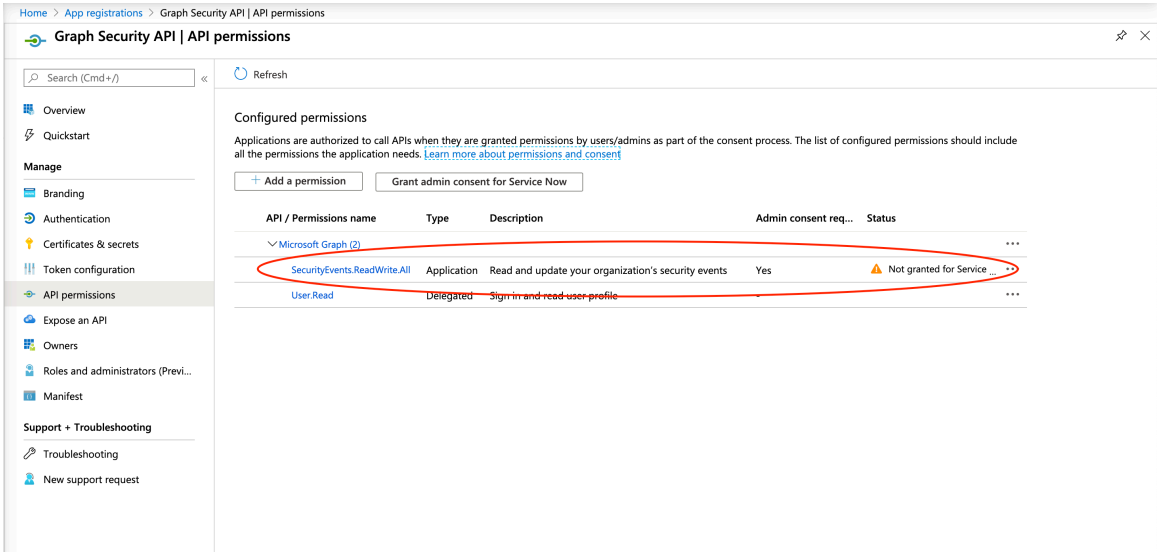
9. Fügen Sie neue API-Berechtigungen auf Anwendungsebene für SecurityEvents.ReadWrite.All Sicherheitsereignisse hinzu.



10. Erteilen Sie die Administratorzustimmung für die neu hinzugefügten API-Berechtigungen.
    Weitere Informationen finden Sie in der Referenz zu Microsoft Graph-Berechtigungen Microsoft Graph-Berechtigungsmodell.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Melden Sie sich als Mandantenadministrator an, und erteilen Sie die Einwilligung für die Anwendung. Die Schritte sind unten aufgeführt:

    a. Navigieren Sie zur folgenden URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

    Geben Sie die APPLICATION_ID der Anwendung ein, die Sie registriert haben.

12. Klicken Sie auf **„Akzeptieren“**, um die von der oben erstellten Anwendung angeforderten Berechtigungen zu akzeptieren.
    Anschließend können Sie die Anwendung zum Lesen von Sicherheitsereignissen verwenden. Weitere Informationen finden Sie in der Microsoft Graph-Sicherheitsautorisierungsdokumentation .

Installieren und konfigurieren Sie die ServiceNow-Anwendung für die Microsoft Graph-Sicherheits-API-Integration zur Warnungserfassung

Bevor Sie die -Integration in Ihrer Instanz Now Platform® ausführen, führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in die -Produkte Security Incident Response und Security Operations in Ihrer Instanz Now Platform integriert werden kann.

Vorbereitungen

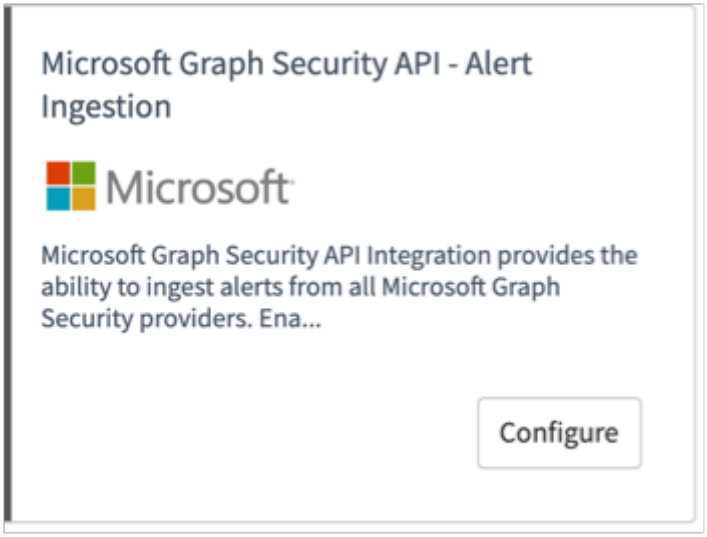
Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn Sie die Anwendung Microsoft Graph-Sicherheits-API für die Integration nicht aus ServiceNow Store installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Microsoft Graph-Sicherheits-API – Warnungserfassung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie zum Konfigurieren der Anwendung auf **Konfigurieren**.
4. Füllen Sie im angezeigten Dialogfeld „Konfiguration der Warnungserfassungen“ die Felder aus.
5. Klicken Sie auf **Absenden**.
   Nach der erfolgreichen Validierung und Übermittlung wird jede Serverkonfiguration für Warnungserfassungen auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite mit den Sicherheitsintegrationen angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.

Nächste Maßnahme
Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht im Erstellen eines Warnungsprofils.

Erstellen Sie ein Profil für die Microsoft Graph-Sicherheits-API-Integration zur Warnungserfassung

Als Benutzer mit der Rolle sn_si.admin erstellen Sie ein Warnungsprofil in Ihrer Instanz Now Platform und bestimmen, welche Warnungen Security Incidents generieren. Bevor Security Incidents aus erfassten Warnungen erstellt werden, werden die Feldwerte aus Warnungen in einem Layout eines Now Platform -Security Incidents angezeigt, sodass Sie eine Vorschau auf die Darstellung des tatsächlichen Security Incidents anzeigen können.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die Integration ermöglicht es Ihnen, verschiedene Arten von Warnungen zu erfassen, z. B. zu nicht autorisierten Zugriffsversuchen und Malware. Diese Warnungen werden basierend auf den Profilen erfasst, die Sie in der Umgebung Security Operations Ihrer -Instanz konfigurieren. Alle Warnungen werden anfänglich für einen konfigurierten Warnungstyp in einem Profil erfasst. Erfasste Warnungen können dann weiter gefiltert werden, um anzugeben, welche Warnungen Security Incidents erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise können Sie Filter bevorzugen, die Security Incidents nur für Warnungen erstellen, die als hoch riskant eingestuft werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Warnungen erstellt, werden einzelne Feldwerte in den gefilterten Warnungen für eine Vorschau den entsprechenden Feldern in einem Layout von Security Incidents zugeordnet. Alle Warnungen, die die Auswahlkriterien in Ihrem Mandanten Microsoft Azure erfüllen und über den Microsoft Graph-Sicherheits-API verfügbar sind, werden zunächst in Ihrer Instanz Now Platform erfasst.

Identifizieren Sie die Quelle für das Profil

Geben Sie den Namen und die Quelle für das Profil an.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Um ein Profil für eine Warnung in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **Microsoft Graph-Sicherheits-API – Integration** > **Microsoft Graph-Sicherheits-API-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

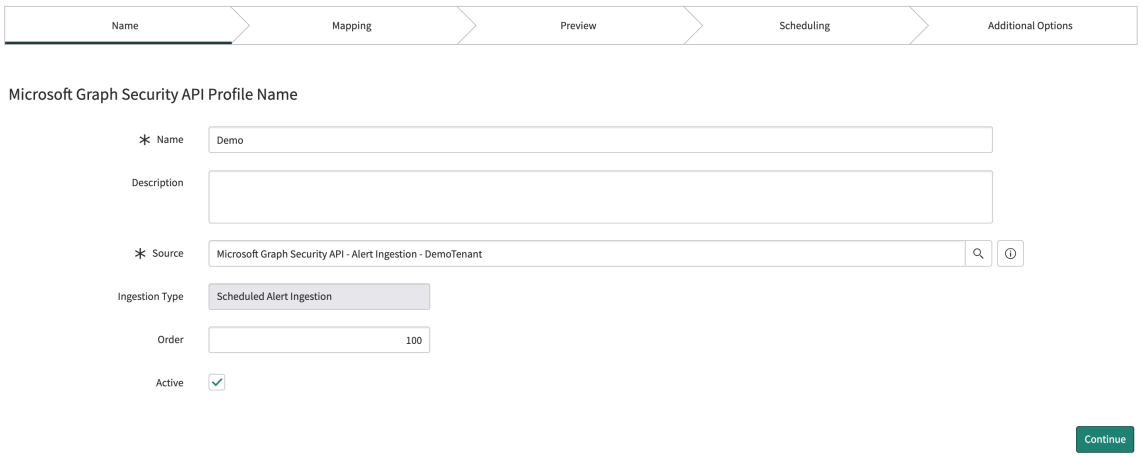
   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn die Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert. Profilnamen in Ihrer Instanz Now Platform müssen eindeutig sein.
Aktiv	Checkbox ist standardmäßig deaktiviert. Wenn diese Option deaktiviert ist, ist das Profil nicht aktiv. **Hinweis:** Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.
Quelle	Der -Mandant Microsoft Azure, den Sie für die Erfassung von Warnungen konfiguriert haben. Wenn Sie mehrere Mandanten konfiguriert haben, wählen Sie den entsprechenden Mandanten für die Warnungstypen aus, die für das Profil erfasst werden sollen. Sie müssen einen Wert eingeben.
Bestellung	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile dieselben Auslösebedingungen verwenden. Je niedriger der Reihenfolgenwert, desto höher die Priorität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
(Optional) Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



Nächste Maßnahme

Der nächste Schritt besteht im Zuordnen der Warnungsfelder.

Zuordnung von Warnungsfeldern für die Microsoft Graph-Sicherheits-API-Integration zur Warnungserfassung

Nachdem Sie die Quellen für die geplante Warnungserfassung identifiziert haben, besteht der nächste Schritt in der Zuordnung einzelner Warnungsfelder zu den Feldern in einem Security Incident Now Platform SIR.

Für den Zuordnungsschritt müssen Sie zuerst Beispielwarnungen aus dem -Mandanten Microsoft Azure erfassen. Dann müssen Sie sicherstellen, dass alle relevanten Warnungsfelddaten an der entsprechenden Stelle im Incident-Formular SIR zugeordnet sind, und dann den Incident SIR im Vorschaubereich visualisieren.

Die Zuordnung der Beispielwarnungsfelder umfasst Folgendes:

- Erfassung von Microsoft Graph-Sicherheits-API-Beispielwarnungen
- Zuordnung von Warnungen zu Security Incident Response-Feldern

Erfassung von Microsoft Graph-Sicherheits-API-Beispielwarnungen

Nehmen Sie Beispielwarnungen von Ihrem -Mandanten Microsoft Azure auf.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

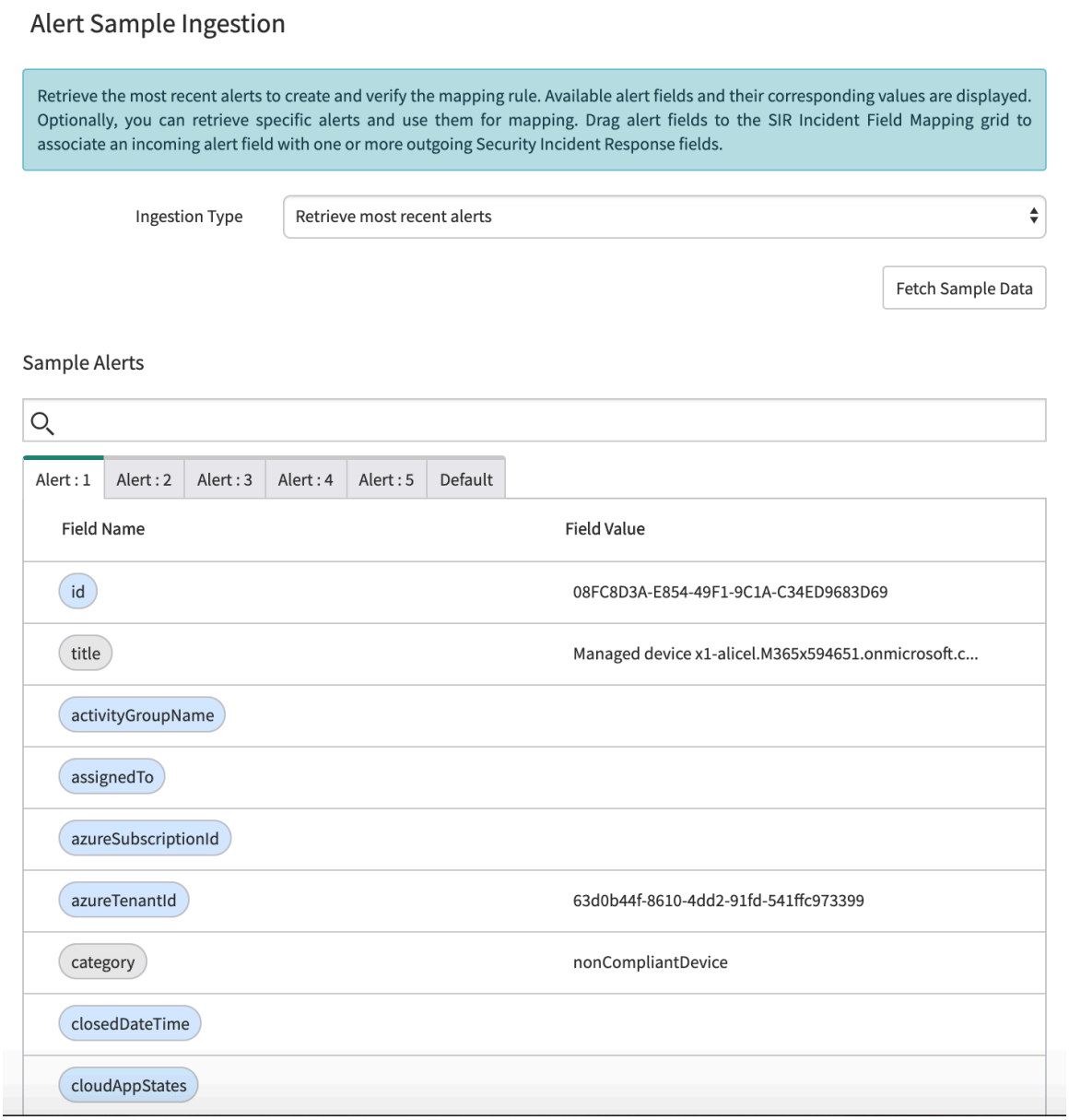
1. Sie können entweder die 5 neuesten Beispielwarnungen abrufen oder die eindeutigen Warnungs-IDs für die spezifischen Warnungen angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   Wählen Sie in der Auswahlliste **Erfassungseinstellung** eine der folgenden Optionen aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Neueste Warnungen abrufen: Es werden die 5 neuesten Warnungen abgerufen.
- Wählen Sie Warnungen basierend auf der Warnungs-ID aus: Geben Sie die Warnungs-ID für die abzurufenden Warnungen an. Sie können maximal 5 durch Kommas getrennte Warnungs-IDs angeben.

2. Klicken Sie **auf Beispieldaten abrufen**, um die neuesten Beispielwarnungsdaten aus dem Mandanten Microsoft Azure abzurufen.
   Das Abrufen von Beispielwarnungen kann einige Minuten dauern.

   Die Feldwerte für die Beispielwarnung werden auf der linken Seite des Formulars ausgefüllt, wenn Beispielwarnungen vom Profil erfasst werden. Dies sind die Warnungen, die Sie den Security Incident-Feldern SIR zuordnen. Die Warnungsfelder und -wertergebnisse werden als einzelne Registerkarten angezeigt.



Nächste Maßnahme

Nachdem Sie die Beispieldaten abgerufen haben, besteht der nächste Schritt darin, die Warnungsfelder dem Security Incident zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnung von Warnungen zu Security Incident Response-Feldern

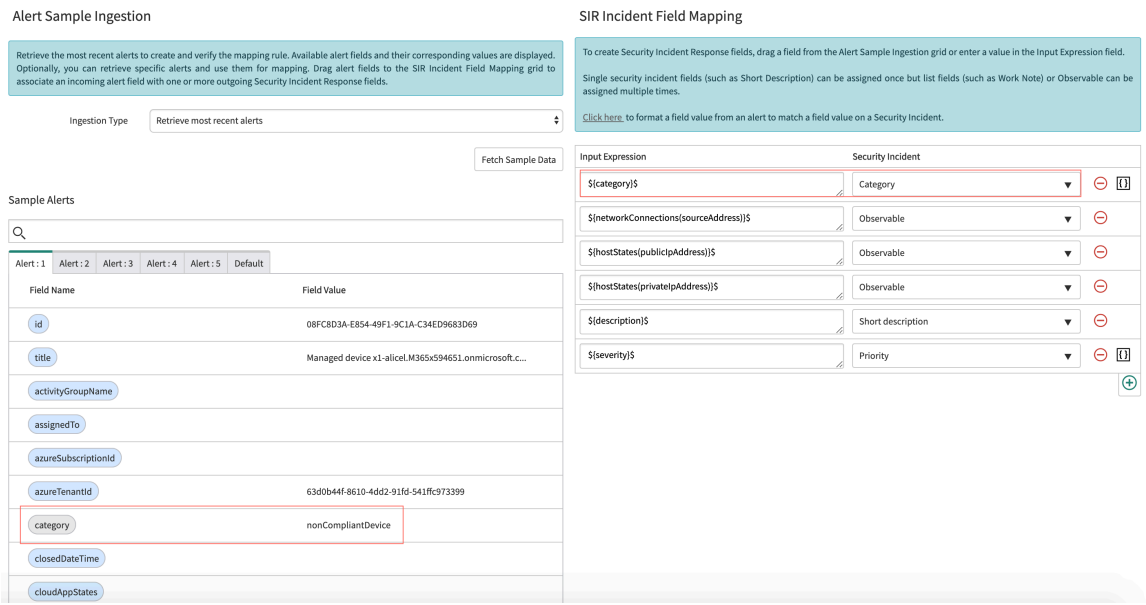
Ordnen Sie einzelne Warnungsfelder aus ausgelösten Warnungen Feldern in einem Security Incident Now Platform zu.

Warnungsfeldzuordnung

Als Benutzer mit der Rolle sn_si.admin verwenden Sie die Felder aus dem Abschnitt Beispielwarnungen auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ im rechten Bereich zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Warnungsfelder aus der linken Seite ziehen und sie im Abschnitt SIR Incident-Zuordnung auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das Feld für eingehende Warnungen einem Feld für ausgehende Security Incidents zu.

1. Nachdem Sie die Beispieldaten abgerufen haben, besteht der nächste Schritt darin, die Warnungsfelder dem Security Incident zuzuordnen. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf einen blauen Feldnamen auf der linken Seite des Formulars.
2. Ziehen Sie den Feldnamen, z. B. Kategorie, in ein Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“.

   Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird die Kategorie dem Feld Kategorie im Security Incident zugeordnet.



   Sie können jedoch jeden Wert auf der linken Seite mit einem Feld auf der rechten Seite abgleichen. Vergewissern Sie sich, dass der Wert dem Security Incident während des Vorschauschritts korrekt zugeordnet wurde.

   Um sicherzustellen, dass im Zuordnungsprozess keine Warnungsfelder übersehen oder dupliziert werden, sind Felder farbcodiert. Die Farbcodierung der Warnungsfelder hilft Ihnen, die bereits zugeordneten Warnungswerte nachzuverfolgen, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Warnungsinformationen nicht zugeordnet bleiben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Warnungsfeld ausgewählt und dem Security Incident zugeordnet wurde. Unter Umständen möchten Sie ein Feld für eingehende Warnungen mehreren Feldern in einem Security Incident zuordnen. Ein graus Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

Hinweis:

a. Um manuell einen Wert in das Feld Eingabeausdruck einzugeben, geben Sie ihn im Format ${fieldname}$ ein. Das Warnungsfeld wird dem Feld „Security Incident“ zugeordnet.

b. Sie können erfasste Warnungen nicht den Feldern des Frameworks MITRE-ATT&CK im Abschnitt „Zuordnung von Security Incidents“ zuordnen. Wenn Sie die Felder trotzdem zuordnen, sind die Informationen nicht als Teil der Karte MITRE-ATT&CK im Abschnitt „Framework“ MITRE-ATT&CK im Formular „Security Incident“ verfügbar. Um die Techniken MITRE-ATT&CK zuzuordnen, verwenden Sie die Funktion Automatische Extraktion, die als Teil des Frameworks MITRE-ATT&CK im Modul Threat Intelligence verfügbar ist.

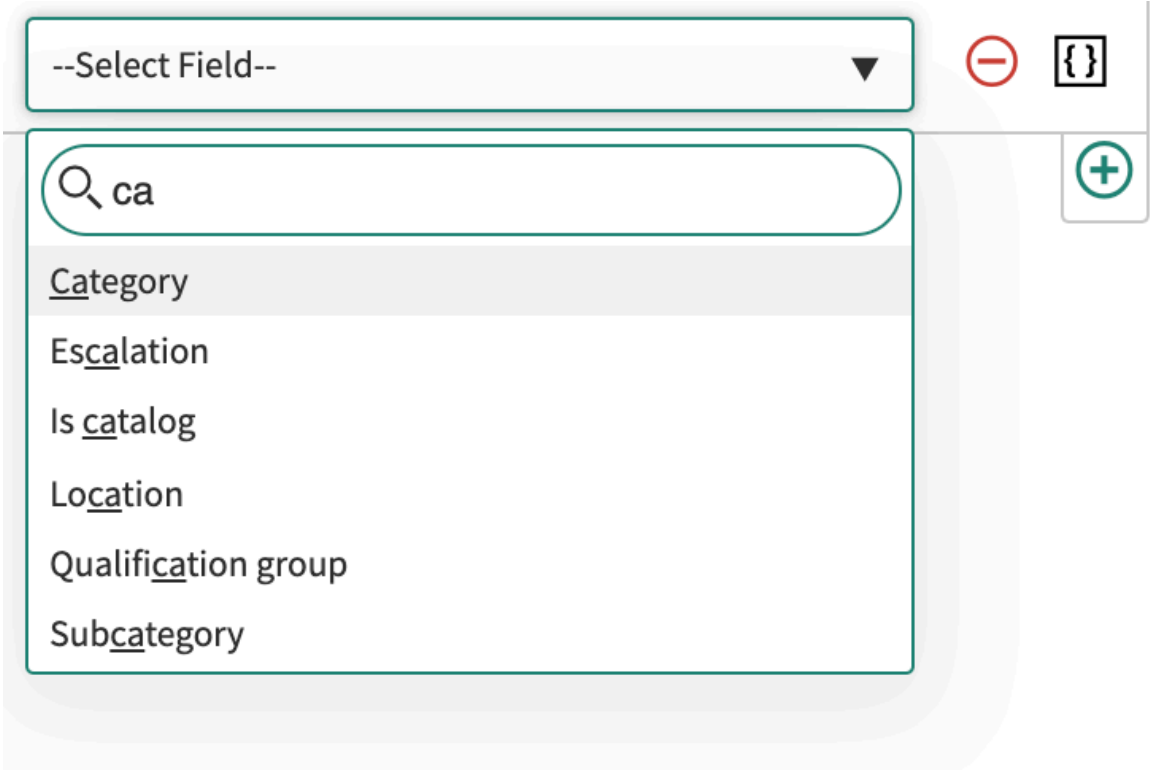
3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

a. Klicken Sie rechts im Formular im Abschnitt SIR Incident-Feldzuordnung unten im Raster auf das Pluszeichen (+). Ein neues Feld wird angezeigt.

b. Erweitern Sie in der Spalte „Security Incident“ die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung ist die Kategorie grau hinterlegt, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Warnungsfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Felder für Security Incidents auf der rechten Seite beim Nachverfolgen der bereits zugeordneten Incident-Felder SIR.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Da für denselben Security Incident mehrere erkennbare Elemente angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der mehrere Optionen ausgewählt werden können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident ebenfalls nicht ausgefüllt.

c. Geben Sie alternativ einen Wert in das Feld Suchen für die neue Zeile ein.

d. Wählen Sie auf der linken Seite des Formulars mit der linken Maustaste die Warnungs-ID aus, die Sie im Feld Eingabeausdruck verwenden möchten. Ordnen Sie es per Drag-and-Drop neben Ihrem neuen Feld zu.

4. Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.

5. Nachdem Sie die vorhergehenden Feldzuordnungsschritte abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

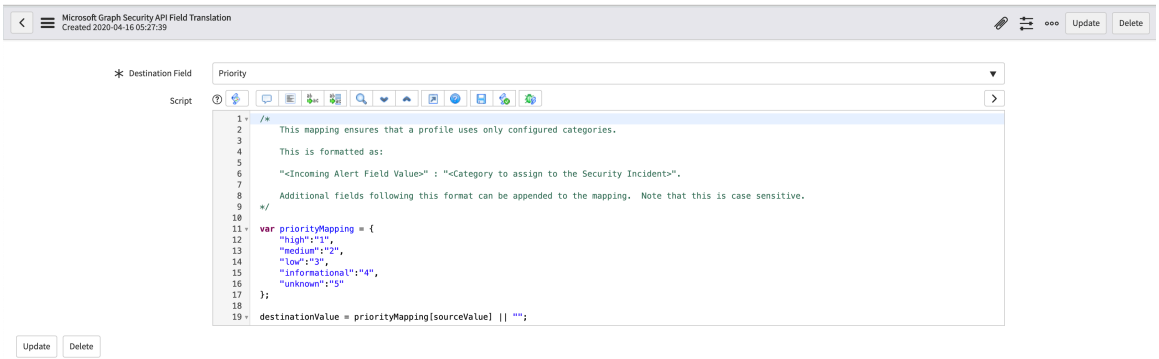
Formatfeldübersetzung

In bestimmten Fällen werden Warnungsfeldwerte in Microsoft Graph-Sicherheits-API möglicherweise nicht direkt in die Felder im SIR-Security Incident übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten. Beispielsweise können mit dem Skript-Editor die Kategoriewerte „Malware-Warnung“ und „Virusinfizierung“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mithilfe des Formats in eine gemeinsame böswillige Code-Aktivität im Feld „Kategorie“ des SIR-Security Incident übersetzt werden Feldübersetzungsfunktion.

Klicken Sie auf das Symbol {}, um den Skript-Editor zu verwenden. Der Skript-Editor wird angezeigt.



Bedingungen für Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um festzulegen, welche Warnungen Security Incidents erstellen und welche Warnungen herausgefiltert werden sollen (z. B. Warnungen mit niedriger Priorität). Dieselben Feldwerte können Sie im Builder für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

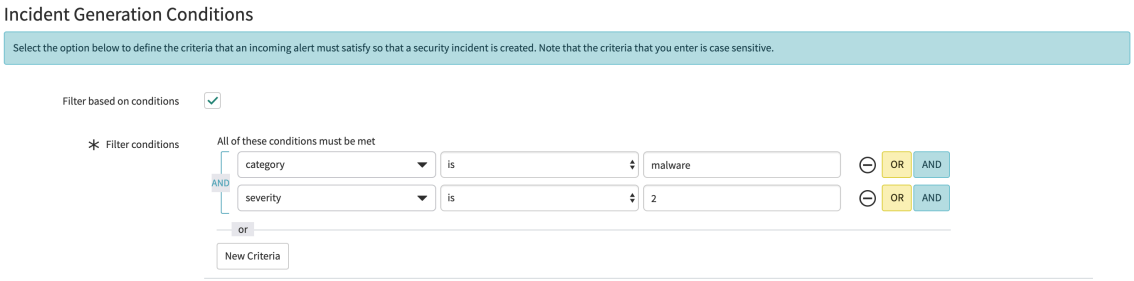
1. Scrollen Sie im Formular zum Abschnitt Bedingungen für Incident-Generierung, und wählen Sie die Option Basierend auf Bedingungen filtern aus. Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt „Erfassung des Warnungsbeispiels“ für die von Ihnen erfasste Warnung angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach der von Ihnen erfassten Warnung. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau den Werten der Warnung entsprechen. Wenn Sie sich bei den Werten, die Sie in die Filterfelder eingeben sollen, nicht sicher sind, kehren Sie möglicherweise zu Ihrem Microsoft Azure-Mandanten zurück und überprüfen Ihre Warnungen auf die Stichwörter.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **AND** oder **OR**.
   - Wenn **AND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER**ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.
4. Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest

   Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



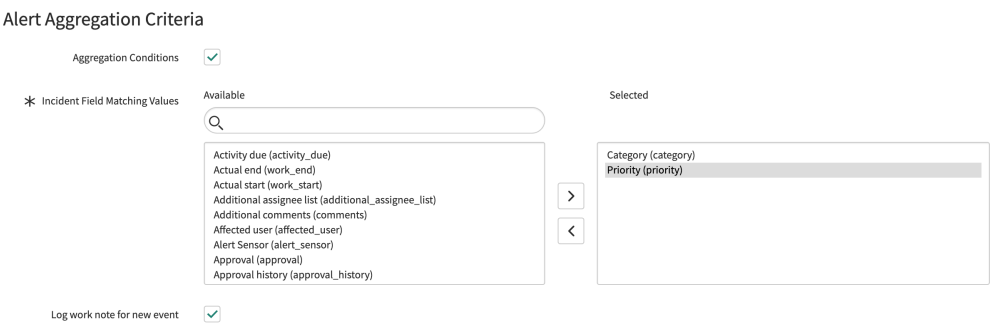
Sie haben die Auslösebedingungen so festgelegt, dass Security Incidents nur erstellt werden, wenn die beiden von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Filterung hilft Ihnen, Sicherheitswarnungen zu isolieren, und begrenzt die Anzahl der von Ihnen erstellten Security Incidents. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur erforderliche Warnungen erfasst, ohne dass die Abfrage oder die Konfiguration der ausgelösten Warnung geändert werden muss.

Kriterien für die Zusammenfassung von Warnungen, um ähnliche Warnungen zu verarbeiten und doppelte Incidents zu vermeiden

Definieren Sie zusätzliche Kriterien für die Warnungszusammenfassung, die eine eingehende Warnung zu einem vorhandenen Security Incident SIR zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Durch die Verwendung von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Warnungsdaten in einem einzigen Security Incident platziert werden. Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:

1. Scrollen Sie im Formular zum Abschnitt Kriterien für Warnungszusammenfassung, und wählen Sie die Option Zusammenfassungsbedingungen aus. Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die im Security Incident SIR konfiguriert sind.
2. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Ihrer Now Platform abgleichen möchten, und verschieben Sie sie in die Liste Ausgewählt. Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, damit diese eingehende Warnung an einen vorhandenen Security Incident angehängt wird. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Warnungsfeldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Warnungszusammenfassung nicht erfüllt, und es wird ein neuer Security Incident erstellt. Screenshot unten für Feldzuordnung mit mehreren Werten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine neue Warnung allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird die Warnung automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, die mit Security Incidents arbeiten, können Sie alle hinzugefügten aggregierten Warnungen in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle aggregierten Warnungen zu einem Security Incident werden in der zugehörigen Liste „Aggregierte Microsoft Graph-Warnungen“ angezeigt. Diese Liste enthält Details zu zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum Warnungen zu vorhandenen Security Incidents hinzugefügt werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter „Zugehörige Links“ zur linken Seite des Datensatzes, und klicken Sie auf den Link **Alle zugehörigen Listen anzeigen**.

3. (Optional) Um eine Arbeitsnotiz für eine neue Warnung zu protokollieren, die dem Security Incident kürzlich hinzugefügt wurde, aktivieren Sie das Kontrollkästchen zum Aktivieren dieser Option. Die Arbeitsnotiz protokolliert, dass eine neue Warnung hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails und allen anderen Details, die dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben erfolgreich Werte aus einer Warnung Feldern in einem Security Incident SIR zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents anhand von Filterkriterien einzuschränken. Sie haben Warnungen oder Ereignisse auch an vorhandene SIR Security Incidents angehängt.

4. Klicken Sie auf **„Fortsetzen** “, um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht darin, eine Vorschau der Felder anzuzeigen, die Sie einem SIR-Security Incident zugeordnet haben

Zeigen Sie eine Vorschau des Security Incident für die Microsoft Graph-Sicherheits-API-Integration an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Security Incident Now Platform SIR zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Warnungsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

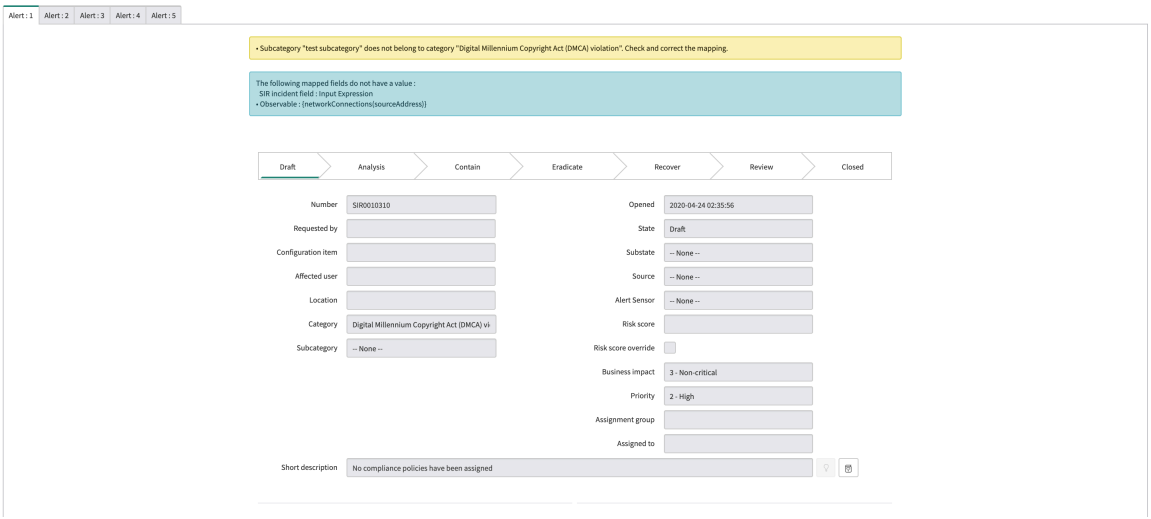
Warum und wann dieser Vorgang ausgeführt wird

Als Benutzer mit der Rolle sn_si.admin können Sie die Vorschau eines Security Incident anzeigen und die Zuordnung nach Bedarf erneut bearbeiten, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wird, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen auf Security Incidents SIR werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

Prozedur

1. Wenn die Vorschau des Security Incidents nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Vorschau**.
   Alle erfassten Warnungen und die auf der Zuordnungsseite definierten Feldzuordnungen werden angezeigt.
2. Klicken Sie auf eine Warnungs-ID, um eine Vorschau des Security Incident anzuzeigen.
   Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Warnungswerte für den Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in den -Fehlermeldungen beschrieben werden.

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung im Security Incident zufrieden sind, besteht der nächste Schritt in der Definition des Zeitplans.

Definieren Sie einen Zeitplan für die Integration der Microsoft Graph-Sicherheits-API

Überprüfen Sie die Standardeinstellungen für den Abruf von Warnungen, oder ändern Sie die Zeitplanung nach Bedarf. Mit diesem Schritt können Sie den Abruf Ihrer Warnung basierend auf einem Datumsbereich filtern.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch auswählen, wie häufig zukünftige Warnungen abgefragt werden, die der Konfiguration des Warnungsprofils entsprechen. Bei Profilen zur automatisierten Warnungserfassung überprüfen und ändern Sie vor der Aktivierung des Profils die Zeitplanung und den Warnungsabruf. Dieser Schritt ist für geplante Warnungsprofile erforderlich.

Als Benutzer mit der Rolle sn_si.admin konfigurieren Sie diese Abfrageintervalle für einzelne Profile. Die Leistung der Integration zur Microsoft Graph-Sicherheits-API -Warnungserfassung wird durch die verschiedenen Abfrageintervalle beeinflusst. Bei der Planung möchten Sie möglicherweise die Systemlast gegen die Dringlichkeit des incident abwägen. Für jedes Profil ist ein Standardwert von fünf Minuten festgelegt. Sie können diese Einstellung jedoch je nach Dringlichkeit des incident und der erwarteten Auslastung Ihres Systems ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **„Zeitplanung“**aus.
2. Wählen Sie eine aus, um zu planen, wie und wann Warnungen aus dem Mandanten Microsoft Azure abgerufen werden.
3. Klicken Sie auf **„Fortsetzen** “, um zur Seite „Zusätzliche Optionen“ zu navigieren.

Automatisieren Sie die Aktualisierung und den Abschluss von Warnungen basierend auf dem SIR-Incident-Status

Die Integration zur Erfassung von -Warnungen Microsoft Graph-Sicherheits-API für verfügt über eine bidirektionale Schnittstelle, über die sowohl Warnungen als auch Security Incidents erstellt werden können. Außerdem können die Warnungen aktualisiert werden, sobald der Security Incident mit relevanten Incident-Details wie dem Incident SIR erstellt und/oder geschlossen wurde Nummer, Zuweisungsgruppe, SIR Incident-URL usw. T

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Hinweis:
Der anfängliche und der Abschlussstatus der Warnung werden nur aktualisiert, wenn diese Funktionalität vom Service Provider unterstützt wird. Einzelheiten finden Sie in der Dokumentation Microsoft Graph-Sicherheits-API und in der Dokumentation des Sicherheitsanbieters.

Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration für die Aktualisierung von Warnungen abzuschließen, wenn der Security Incident erstellt wird.
3. Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen und das Profil in den Status **Warten** zu versetzen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um -Warnungen basierend auf Ihrer Planung aus dem -Mandanten Microsoft Azure abzurufen. Innerhalb von 24 Stunden können maximal 1.000 Security Incidents erstellt werden.

Konfigurationseinstellungen für die Microsoft Graph-Sicherheits-API-Integration

Verwenden Sie diese Option, um die Standardsystemeigenschaften der Microsoft Graph-Sicherheits-API -Erfassungsintegration zu ändern.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

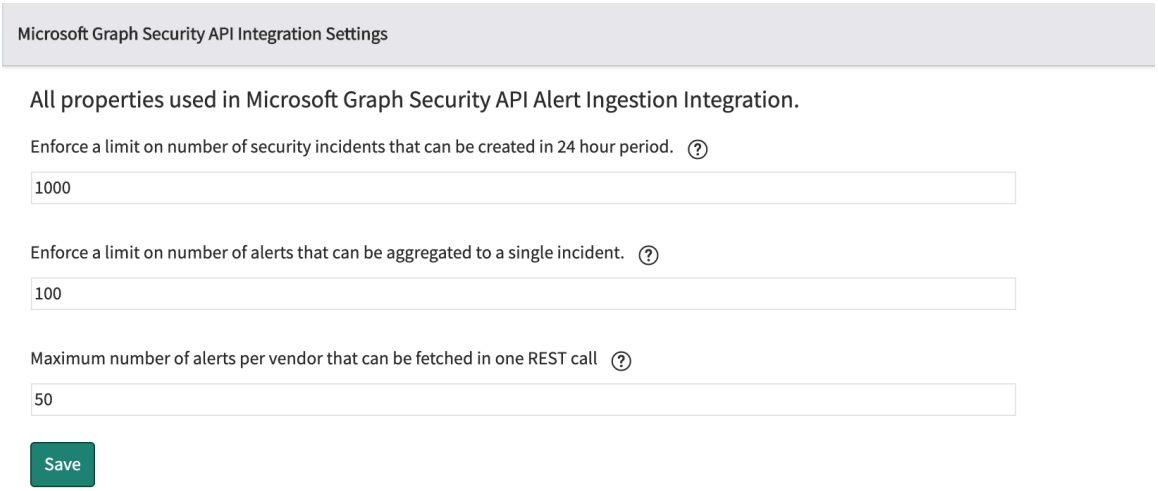
Warum und wann dieser Vorgang ausgeführt wird

Ändern Sie die Standardkonfigurationseigenschaften, um die Anzahl der Security Incidents zu begrenzen, die innerhalb von 24 Stunden erstellt werden können, oder die Anzahl der Warnungen, die in einem Security Incident zusammengefasst werden können.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **Microsoft Graph-Sicherheits-API – Integration** > **Microsoft Graph-Sicherheits-API – Integrationseinstellungen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.



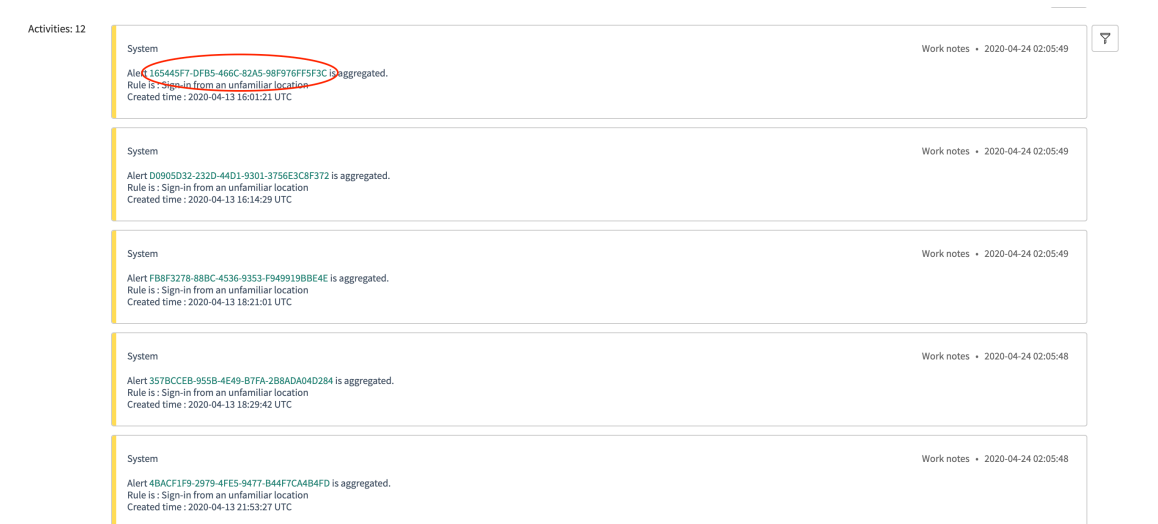
Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

Security Incident Response-Formular nach Erfassung von Warnungen

Nachdem eine Microsoft Graph-Sicherheits-API -Warnung erfasst wurde, wird ein Security Incident erstellt, und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

Arbeitsnotiz

Wenn Sie die Option **Arbeitsnotiz für neue Warnung** protokollieren in den Zusammenfassungskriterien der Warnung ausgewählt hatten, wie in Zuordnung von Warnungen zu Security Incident Response-Feldernbeschrieben, wird beim Aggregieren der Warnung eine Arbeitsnotiz veröffentlicht.



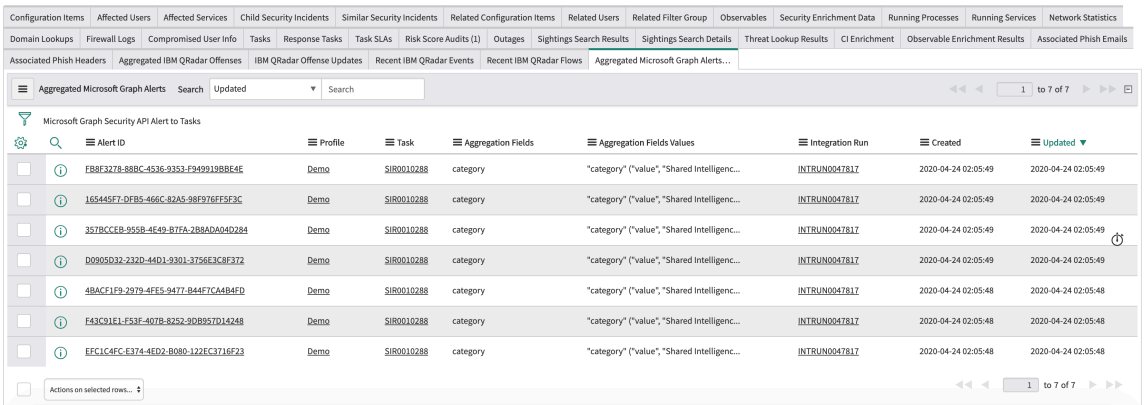
Klicken Sie auf den Warnungslink, um zum Datensatz des internen Warnungsimports zu navigieren, der Rohwarnungsdaten enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aggregierte Warnungen

Klicken **Zugehörige Listen** > **Aggregierte Microsoft Graph-Sicherheitswarnungen** um die für den Security Incident aggregierten Warnungen anzuzeigen.



- **Security Incident erstellen**: Wählen Sie eine Warnung aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie dann auf **Security Incident erstellen**. Durch diese Option wird ein neuer Security Incident für die Warnung erstellt, und für diese Warnung wird die Zusammenfassung aus dem übergeordneten Security Incident aufgehoben.
- **Warnungsdatensatz löschen**: Wählen Sie eine Warnung aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie auf **Löschen**. Mit dieser Option wird der Warnungsdatensatz gelöscht.

Optional: Kopieren Sie ein Microsoft Graph-Sicherheits-API-Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich möglicherweise, Profile zu kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname zunächst geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es nicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

versehentlich aktiviert wird, bevor die Konfiguration abgeschlossen wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Graph-Sicherheits-API – Integration** > **Microsoft Graph-Sicherheits-API-Profil**.
2. Wählen Sie in der angezeigten Liste Microsoft Graph-Sicherheits-API Profile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.
   Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Zeitplankonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie an dieser Stelle deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.

   Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **„Aktiv“** auf „falsch“ festgelegt ist, da das Profil aktiviert werden muss.

Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren, nachdem Sie die Konfigurationsschritte abgeschlossen haben.

Domain Separation und Microsoft Graph-Sicherheits-API Warnungserfassung

Domänentrennung wird für diese Anwendung unterstützt. Die Microsoft Graph-Sicherheits-API -Integration erfasst Warnungen von Microsoft Graph-Sicherheitsanbietern und erstellt automatisch Security Incidents. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

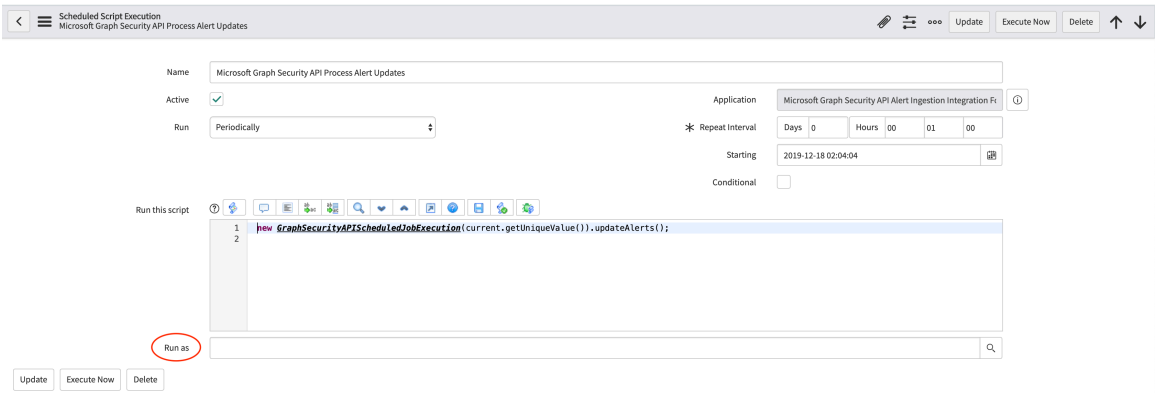
So funktioniert Domain Separation in Microsoft Graph-Sicherheits-API

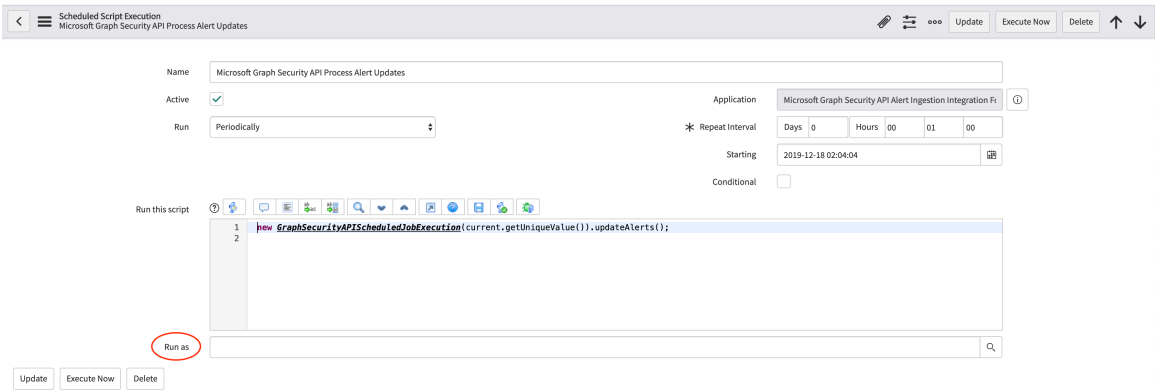
Um Domain Separation zu erreichen, replizieren Sie die geplanten Aufgaben Profilprozess Microsoft Graph-Sicherheits-API und SIR Prozesswarnungsaktualisierungen, und ändern Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die **Option Ausführen als** Benutzer. Standardmäßig führen die Systembenutzer diese regelmäßigen Aufgaben aus. Ändern Sie **Ausführen als** in einen Benutzer mit der Rolle sn_si.admin in der entsprechenden Domäne, und führen Sie die geplante Aufgabe aus.





Zugehörige Informationen

Domänentrennung für Service Provider

Verwendung von Flow Designer und Integration Hub in der Microsoft Graph-Sicherheits-API-Integration

Unter Verwendung der Funktionalität von Flow Designer und Integration Hub wurden mehrere Subflows und Aktionen als Teil der Microsoft Graph-Sicherheits-API -Integration erstellt.

Die folgenden Subflows sind verfügbar:

- Microsoft Graph-Sicherheits-API Konfigurationsvalidierung: Dies wird in der Konfigurationskachel verwendet, um die Anmeldeinformationen beim ersten Setup zu validieren.
- REST-Aufruf für Microsoft Graph-Sicherheits-API: Dies wird für alle Interaktionen mit der Microsoft Graph-Sicherheits-API mithilfe von REST-Aufrufen verwendet.
- Beispielwarnungen abrufen: Wird im Abschnitt „Zuordnung“ des Profil-Setups verwendet, um Beispieldaten abzurufen. Dieser Subflow wird asynchron ausgelöst.

Problembehandlung bei der Microsoft Graph-Sicherheits-API-Integration

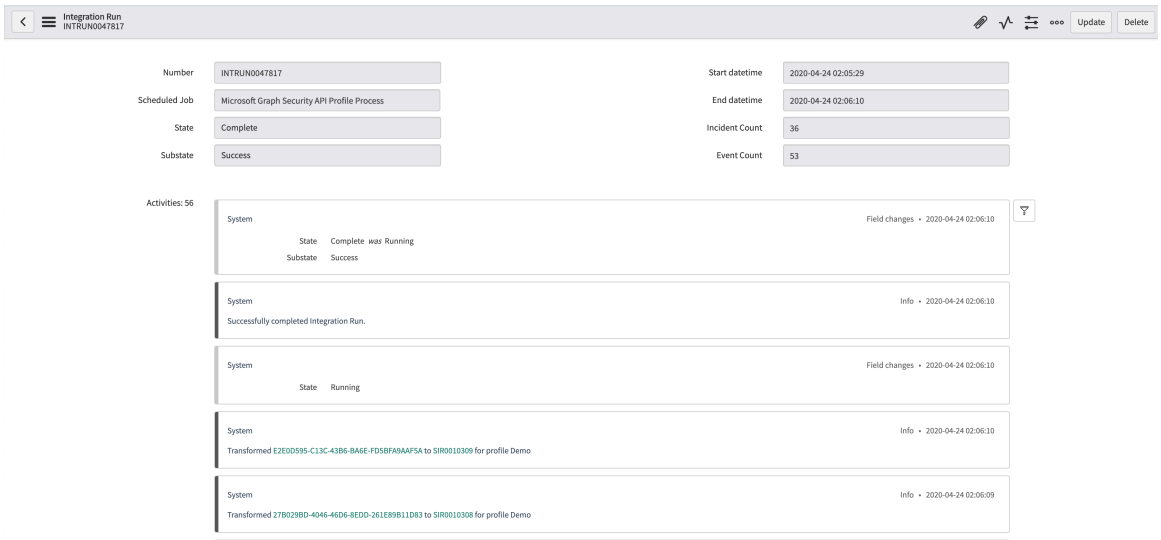
Dieser Abschnitt enthält wichtige Problembehandlungstipps und häufig gestellte Fragen im Zusammenhang mit der Integration der Microsoft Graph-Sicherheits-API -Warnungserfassung.

- **Integrationsausführung**: Wenn die Ausführung einer geplanten Aufgabe beginnt, wird ein Datensatz für die Integrationsausführung mit Protokollen, Fehlern und Warnungen angezeigt. Die Anzahl der abgerufenen Warnungen und die Anzahl der Incidents,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die in einer Ausführung einer geplanten Aufgabe erstellt wurden, werden ebenfalls angezeigt. Benutzer mit der Rolle sn_si.analyst können sehen, ob das Abrufen von Fehlern/Profilen während der Integrationsausführung fehlgeschlagen ist. Benutzer mit der Rolle sn_si.analyst können die Tabelle sn_event_ingestion_integration_run auf aufgetretene Fehler überprüfen. Um Integrationsprobleme zu beheben, müssen Sie zuerst die Integrationsausführung überprüfen. Fehler werden als Arbeitsnotizen in den Datensätzen der Integrationsausführung für jede Ausführung einer geplanten Aufgabe protokolliert.



- **Unvollständiges Profil**: Klicken Sie bei der Konfiguration des Profils im Abschnitt „Zusätzliche Optionen“ (Automatisieren Sie die Aktualisierung und den Abschluss von Warnungen basierend auf dem SIR-Incident-Status) auf die Schaltfläche **„Fertigstellen“**, um sicherzustellen, dass das Profil in den Status „Warten“ versetzt wird und damit auf die Erfassung wartet.
- **Profil validieren**: Um zu validieren, ob die Integration ordnungsgemäß funktioniert, überprüfen Sie die Profilstatus, das Datum des letzten Abrufs des Profils, die Warnungsimporttabelle und die Datensätze der Warnungs-zu-Aufgaben-Tabelle.
- **SSL-Probleme**: Wenn Sie eine Verbindung über Microsoft Graph-Sicherheits-APIherstellen, vergewissern Sie sich, dass die Instanz über ein gültiges CA-Zertifikat verfügt, das nicht abgelaufen ist. Sie können RSA-Zertifikate oder eigene Zertifikate in die Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Weitere Informationen finden Sie in KB0778285 .

Palo Alto Networks – AutoFocus Integration

Das Basissystem für Palo Alto Networks – AutoFocus die -Integration enthält einen Workflow und eine Reihe von Workflow-Aktivitäten, mit denen Sie Palo Alto Networks – AutoFocus in Ihre -Instanz integrieren können.

Erkunden

Security Incident Response-Integrationen

Einrichten

Aktivieren und konfigurieren Sie die Palo Alto Networks – AutoFocus Integration

---

Verwenden

Entwickeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Security Operations Palo Alto Networks: Wert-Workflow zum Überprüfen und Blockieren
- Ruft den Flow zur Ergänzung der AutoFocus-Sitzungsinformationen ab
- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Aktivieren und konfigurieren Sie die Palo Alto Networks – AutoFocus Integration

Mit der Funktion „Integrationskonfiguration“ können Sie die Sicherheitsintegrationen von Drittparteien, einschließlich Palo Alto Networks – AutoFocus, schnell aktivieren und einrichten. Bevor Sie Palo Alto Networks – AutoFocusverwenden können, müssen Sie es von ServiceNow Storeherunterladen.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie eine Anwendung zum ersten Mal von ServiceNow Store herunter.
2. Wenn die Installation abgeschlossen ist, rufen Sie die Support-Website von Palo Alto Networks auf, und rufen Sie den API-Schlüssel ab.
3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationskonfiguration**.
4. Klicken Sie auf der Karte Palo Alto Networks AutoFocus auf **Konfigurieren**.
5. Geben Sie den **API-Schlüssel** ein, den Sie auf der Support-Website von Palo Alto Networks erworben haben, oder fügen Sie ihn ein.
6. Klicken Sie auf **Absenden**.

Ruft den Flow zur Ergänzung der AutoFocus-Sitzungsinformationen ab

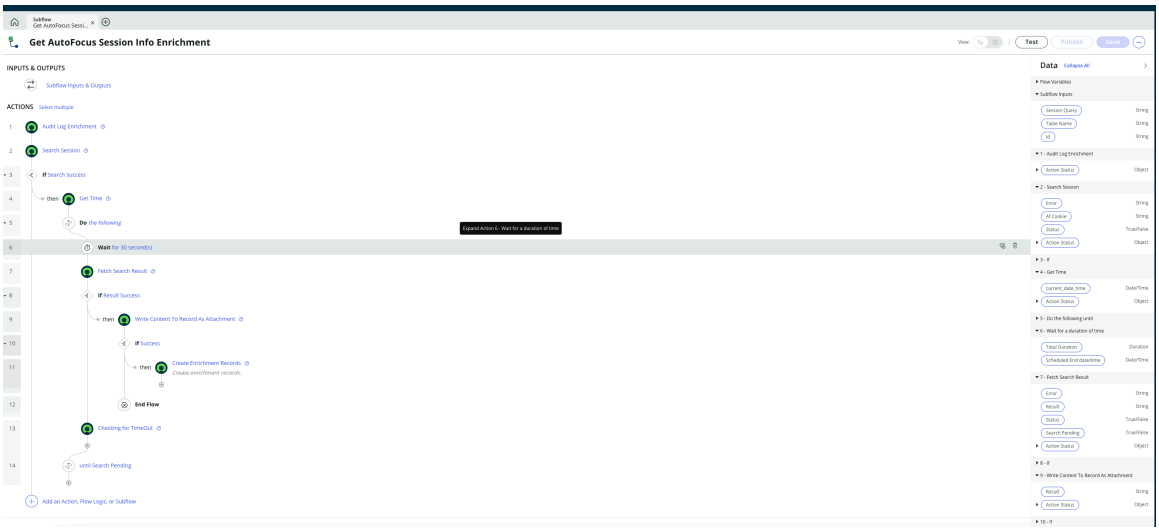
Wenn der Flow **„Security Operations Palo Alto Networks – Anreicherung von AutoFocus-Sitzungsinformationen abrufen“** ausgeführt wird, wird eine Suchabfrage bei AutoFocus in die Warteschlange gestellt, um Informationen zu einer angegebenen Quell-IP zu sammeln. Wenn AutoFocus Kenntnisse über vorherige Sitzungen hat, die von dieser IP-Adresse stammen, wird ein Bericht im JSON-Format zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Der Flow **„Security Operations Palo Alto Networks – Anreicherung von AutoFocus-Sitzungsinformationen abrufen“** wird ausgeführt, wenn das Feld **Quell-IP** in einem Security Incident geändert und der Datensatz aktualisiert wird. Der Flow ruft die IP-Adresse ab und sendet eine Abfrageanforderung an AutoFocus. Wenn AutoFocus zuvor Sitzungen identifiziert hat, die von der IP-Adresse stammen, wird ein Bericht im JSON-Format zurückgegeben.

Security Operations Palo Alto Networks – WildFire-Datenanreicherungs-Flow abrufen



Prozedur
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Klicken Sie auf die Registerkarte **Indicators of Compromise (Indikatoren der Gefährdung)**, und füllen Sie das Feld **Quell-IP** aus.
3. Klicken Sie auf **Aktualisieren**.
   AutoFocus scannt die Informationen aus der IP-Adresse, und an den Security Incident wird eine Textdatei im JSON-Format angehängt.

   Spezifische Aktionen für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Aktion „AutoFocus-Suchsitzung“.
Die Flow-Aktion **AutoFocus-Suchsitzung** lädt Informationen von einer IP-Adresse, die einem Security Incident zugewiesen ist, zu AutoFocus und stellt sie für eine Suchabfrage in die Warteschlange.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Hinweis:

Wenn die Aktion ausgeführt wird, wird eine Suchabfrage mit AutoFocus in die Warteschlange gestellt, um Informationen für eine angegebene Quell-IP zu sammeln. Wenn AutoFocus zuvor Sitzungen identifiziert hat, die von dieser IP-Adresse stammen, wird ein Bericht im JSON-Format zurückgegeben.

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
searchSessionQuery [Zeichenfolge]	Die Suchabfrage für Sitzungsinformationen.

Aktion „Suchergebnisse abrufen“.

Die Flow-Aktion **Suchergebnisse** abrufen ruft Suchergebnisse ab, die durch ein Cookie für die Suchabfrage identifiziert wurden, die von der Aktion **AutoFocus-Suchsitzung** initiiert wurde.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
afcookie [Zeichenfolge]	Das AutoFocus-Cookie für die von Aktion „AutoFocus-Suchsitzung“.generierte Suchanforderung.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
searchPending [Boolean]	„Wahr“, wenn die Suchanforderung noch in AutoFocus verarbeitet wird.
Ergebnis [Zeichenfolge]	Die Suchergebnisdaten.
status [Boolesch]	„Wahr“, wenn die Suche abgeschlossen ist und Ergebnisse erfolgreich generiert wurden.
Fehler [Zeichenfolge]	Der Fehler, der in der Aktion aufgetreten ist, falls vorhanden.

Palo Alto Networks – Firewall Integration

Stellen Sie zum Durchführen Palo Alto Networks – Firewall der -Integration sicher, dass Sie ein MID-Server mit SSH-Anmeldeinformationen eingerichtet haben. Wenn noch keine Firewall eingerichtet ist, fügen Sie eine hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden	Einrichten
Security Incident Response-Integrationen	• Palo Alto Networks-Firewall-Integration aktivieren und konfigurieren • Richten Sie SSH-Anmeldeinformationen für den MID-Server ein

Verwenden	Entwickeln
Workflow für das Firewall-Startprogramm für Security Operations-Integration Palo Alto Networks .	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Richten Sie SSH-Anmeldeinformationen für den MID-Server ein

Die Palo Alto Networks-Firewall sendet API-Aufrufe an den MID Server. Stellen Sie daher sicher, dass SSH-Anmeldeinformationen für den MID Server erstellt wurden.

Vorbereitungen

- Das Orchestration-Plugin muss aktiviert sein.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Orchestration** > **Anmeldeinformationen und Verbindungen** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie im Bildschirm „Interceptor“ auf **SSH-Anmeldeinformationen**.
4. Füllen Sie die Felder nach Bedarf aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSH-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen Namen für die Anmeldeinformationen ein.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese Anmeldeinformationen zu aktivieren.
Betrifft	Wählen Sie **Alle MID-Server** oder **Bestimmte MID-Server**aus.
MID-Server	Wenn Sie **Bestimmte MID-Server**ausgewählt haben, klicken Sie auf das Schlosssymbol, und wählen Sie die MID-Server aus, auf die diese Anmeldeinformationen angewendet werden sollen.
Bestellung	Wählen Sie die Reihenfolge aus, für die die Anmeldeinformationen vom Server getestet werden. Kleinere Zahlen werden zuerst versucht.
Anwendername	Geben Sie den Anwendernamen des Anwenders ein, der diesen Anmeldeinformationen zugeordnet ist, falls vorhanden.
Passwort	Wenn Sie einen **Anwendernamen**eingegeben haben, geben Sie das Passwort des Anwenders ein.
Tag	Geben Sie ein Tag ein, das für Suchkriterien verwendet werden soll. Das Feld **Tag** muss denselben Wert wie der **Name**enthalten.

Palo Alto Networks-Firewall-Integration aktivieren und konfigurieren

Mit der Funktion „Integrationskonfiguration“ können Sie die Sicherheitsintegrationen von Drittparteien, einschließlich Palo Alto Networks – Firewall, schnell aktivieren und einrichten. Bevor Sie Palo Alto Networks – Firewallverwenden können, müssen Sie es von ServiceNow Storeherunterladen.

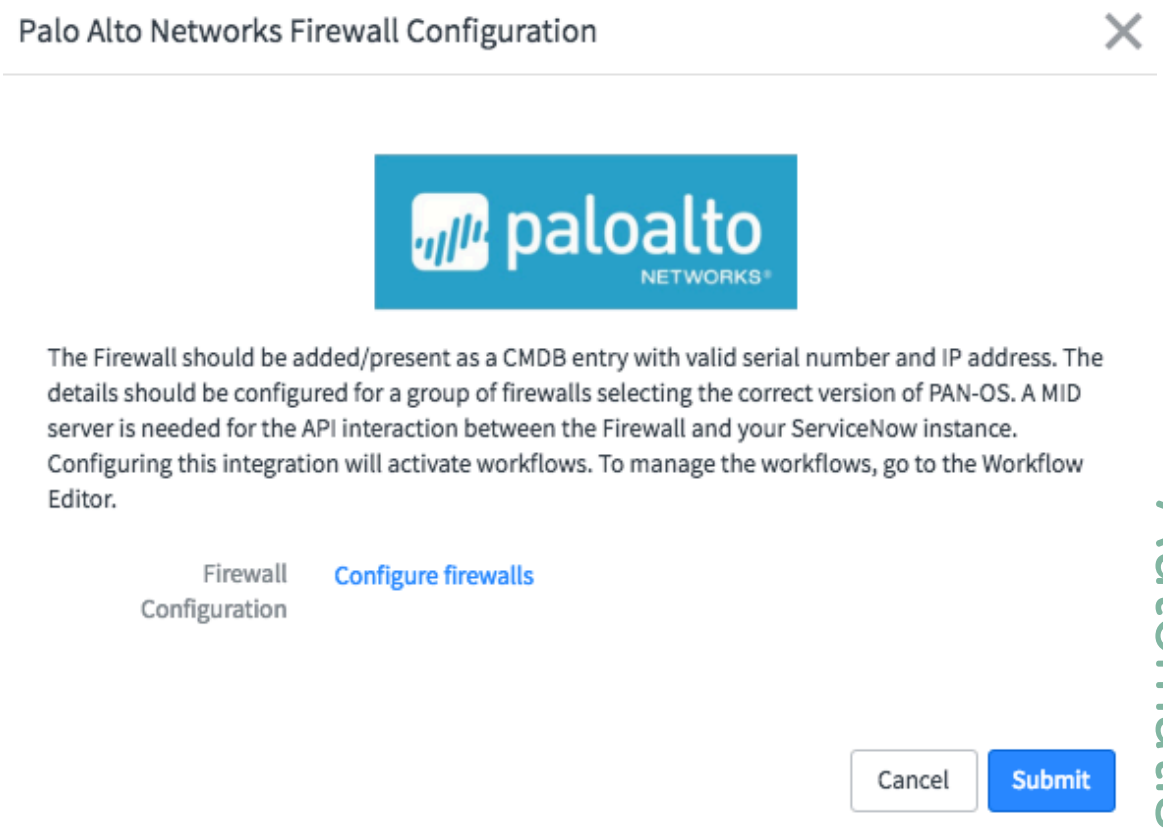
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Greifen Sie vor dem Aktivieren und Konfigurieren der Integration auf das Palo Alto Networks-Firewall-Dashboard zu.
   Notieren Sie sich die Namen der dynamischen IP-Liste, der dynamischen URL-Liste oder der dynamischen Domänenliste, die Sie für die Firewall-Blockierung verwenden.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.
3. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte Palo Alto Networks-Firewall auf **Konfigurieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Firewalls konfigurieren**.
6. Klicken Sie im Bildschirm Firewall-Konfigurationen auf **Neu**.
7. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Firewalls	Klicken Sie auf das Schlosssymbol, und wählen Sie die zu konfigurierende Firewall aus.
Firewall-Version	Wählen Sie die Palo Alto Networks-Firewall-Version aus.**PAN-OS-7.1** ist die empfohlene Version. Die Auswahl früherer Versionen kann zu inkonsistenten Ergebnissen führen.
Anwendername	Geben Sie den Anwendernamen ein, der beim Herstellen einer Verbindung zur Firewall über REST-Endpunkte verwendet werden soll.
Passwort	Geben Sie das Passwort für den verbindenden Anwender ein.
Dynamische IP-Liste	Geben Sie den Namen der externen dynamischen Liste oder dynamischen Sperrliste ein, die Sie für IP-Adressen verwenden.
Dynamische URL-Liste	Geben Sie den Namen der externen dynamischen Liste oder der dynamischen Sperrliste ein, die Sie für URLs verwenden.
Dynamische Domänenliste	Geben Sie den Namen der externen dynamischen Liste oder der dynamischen Sperrliste ein, die Sie für Domänen verwenden.

8. Klicken Sie auf **Absenden**.

Automatische Übersetzung

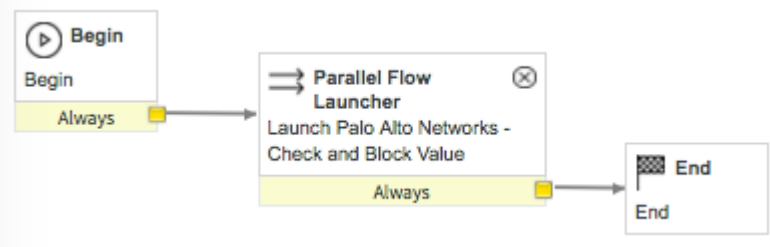
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow für das Firewall-Startprogramm für Security Operations-Integration Palo Alto Networks .

Der Workflow**„Security Operations Integration Palo Alto Networks Firewall Launcher“** ist die Palo Alto Networks-Firewall-Implementierung, die vom Workflow der Funktionalität **„Security Operations Integration – Blockierungsanforderung“** gestartet wird.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Der Workflow-Prozess umfasst folgende Aktivitäten:Security Operations Palo Alto Networks: Wert-Workflow zum Überprüfen und Blockieren.



Security Operations Palo Alto Networks: Wert-Workflow zum Überprüfen und Blockieren

Wenn Security Incidents erstellt und selektiert werden, um potenzielle Bedrohungen zu identifizieren, können Sie den Workflow **„Security Operations Palo Alto Networks – Werte überprüfen und sperren“** verwenden, um IP-Adressen, URLs und Domänen mithilfe von in Palo Alto Networks – Firewalldefinierten externen dynamischen Listen automatisch zu überprüfen und zu aktualisieren.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

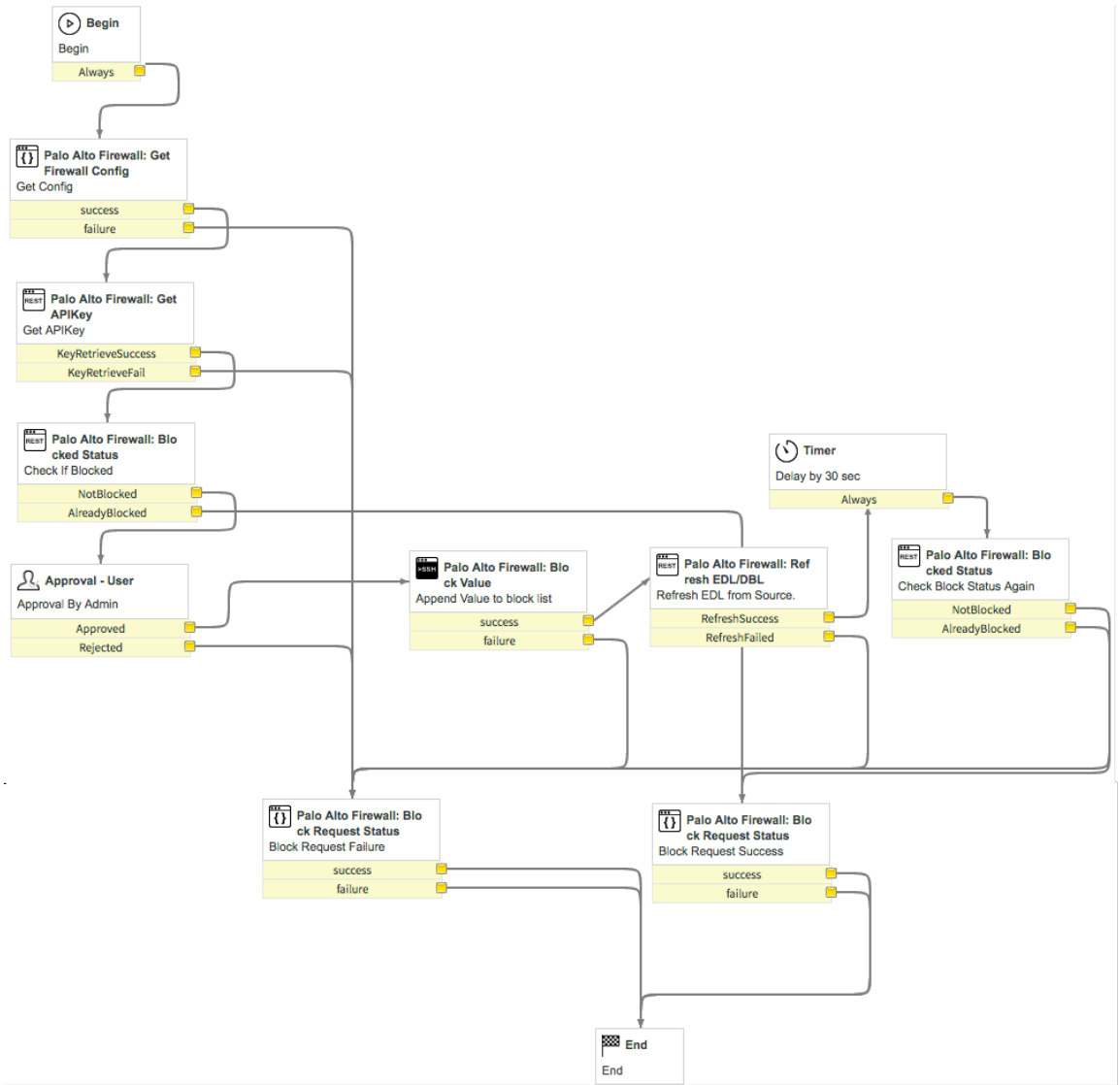
Warum und wann dieser Vorgang ausgeführt wird
Der Workflow **„Security Operations Palo Alto Networks – Wert überprüfen und blockieren“** wird ausgeführt, wenn Firewall-Blockierungsanforderungen übermittelt werden. Die Blockierungsanforderung gibt die zu verwendende Firewall, den Typ des zu überprüfenden und zu blockierenden (falls erforderlich) erkennbaren Elements und den Blockwert an. Das heißt die betreffende IP-Adresse, URL oder Domäne.

Während der Workflow-Ausführung werden die unter definierten Befehle als **Integration mit Palo Alto Networks** > **Firewall** > **Befehle** werden ausgeführt. Die Befehle vom Typ „Anzeigetyp“ (z. B. Show-IP-ExternalDynamicList) bestimmen, ob der Wert in der Firewall vorhanden ist. Die Befehle vom Typ „Aktualisieren“ (z. B. Refresh-IP-ExternalDynamicList) fügen der Sperrliste Werte hinzu, die in der Firewall nicht vorhanden sind.

Nach der Ausführung der Aktivität „Blockierter Status“ ist die Genehmigung durch einen Systemadministrator erforderlich, bevor der Workflow fortgesetzt werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations Palo Alto Networks: Workflow zum Überprüfen und Blockieren von Werten



Prozedur

1. Navigieren zu **Integration mit Palo Alto Networks** > **Firewall** > **Anforderungen blockieren**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Firewall	Wählen Sie die zu verwendende Firewall aus.
Blocktyp	Wählen Sie den Typ des zu überprüfenden Werts aus: ○ IP ○ URL ○ DOMAIN

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Blockwert	Geben Sie den Wert des ausgewählten Typs ein, der in der Firewall überprüft werden soll.

4. Klicken Sie auf **Absenden**.

Palo Alto-Firewall: Aktivität „Status der Anforderung blockieren".

Diese Aktivität wird von anderen Aktivitäten aufgerufen, um den Status der Firewall-Blockanforderung auf „Erfolg" oder „Fehler" festzulegen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
FirewallBlockRequestSysid [Zeichenfolge]	Die System-ID der Firewall-Block-Anforderung. Diese Eingabevariable ist obligatorisch.
Status [Zeichenfolge]	Gibt an, ob der Aktualisierungsauftrag ausgeführt wurde: Erfolg oder Fehler.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Gibt an, ob der Aktualisierungsauftrag erfolgreich war oder fehlgeschlagen ist.

Palo Alto-Firewall: Aktivität zum Blockieren des Werts

Nachdem der Workflow einen Wert identifiziert hat, der sich nicht in der Firewall befindet, wird der Datensatz zur Genehmigung weitergeleitet. Nach der Genehmigung stellt diese Aktivität über Ihre SSH-Anmeldeinformationen eine Verbindung zum MID-Server her und ruft ein Skript auf, das den Wert zur externen Sperrliste der Firewall hinzufügt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Hinweis:
Sie müssen die Eingabevariablen für diese Aktivität manuell eingeben und dann den Workflow veröffentlichen. Wenn der Workflow nicht veröffentlicht wird, werden die Eingabevariablen für Nicht-Administratoren nicht gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
toBeBlockedValue [Zeichenfolge]	Der Wert, der der EDL hinzugefügt werden soll, falls noch nicht vorhanden. Diese Eingabevariable ist obligatorisch.
typeToBeBlocked [Zeichenfolge]	Der Werttyp, der blockiert werden soll: IP, URL oder Domäne. Diese Eingabevariable ist obligatorisch.
targetHost [Zeichenfolge]	Der MID-Server, auf dem das Skript ausgeführt wird.
SSHCredentialTag [Zeichenfolge]	Das auf dem MID-Server definierte SSH-Anmeldeinformations-Tag.
scriptCommand [Zeichenfolge]	Das AppendValueToList.sh-Skript, das zum Hinzufügen des Werts zur EDL verwendet wird. Erfordert den vollständigen Pfad zum MID Server.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Das Ergebnis wurde an die EDL übergeben.

Palo Alto-Firewall: Aktivität „Status blockiert“.

Diese Aktivität überprüft, ob der Wert (IP, URL oder Domäne) in der entsprechenden externen dynamischen Liste/dynamischen Sperrliste (EDL/DBL) in der Firewall enthalten ist. Die EDL/DBL-Details werden mit einem Betriebsbefehl von der Firewall abgerufen, und es wird eine Routine ausgeführt, um zu überprüfen, ob der Wert in der Firewall blockiert ist.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgelisteten Eingabevariablen-Einträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
valueToBeChecked [Zeichenfolge]	Der Wert in der Blockanforderung.
anzeigenEDLDetailsCommand [Zeichenfolge]	Der Befehl für die externe dynamische Liste, mit dem bestimmt wird, ob der Wert in der Firewall vorhanden ist.
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der verwendeten Firewall.
FirewallApiKey [Zeichenfolge]	Der Firewall-API-Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie Daten, die dynamisch mit der Nachricht der Palo Alto-Firewall-Funktionsbefehls-API generiert werden.

Ausgabevariablen

Variable	Beschreibung
kommandoergebnis [Zeichenfolge]	Die Ergebnisse aus der Firewall für den Befehl zum Anzeigen von EDL-Details.
blockiertStatus [Boolesch]	„True“ gibt an, dass blockiert ist. „Falsch“ gibt an, dass nicht blockiert ist.
Befehlsantwort [Zeichenfolge]	Der von der Firewall für den Befehl zum Anzeigen von EDL-Details abgerufene Antwortstatus.

Palo Alto-Firewall: Aktion „API-Schlüssel abrufen“.

Diese Aktion ruft den API-Schlüssel von der Firewall ab.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion. Alle aufgelisteten Eingabevariablen-Einträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
Anwendername [Zeichenfolge]	Der Anwendername des Firewall-Administrators.
Passwort [Zeichenfolge]	Das Passwort des Firewall-Administrators.
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
APIKey [Zeichenfolge]	Der Firewall-API-Schlüssel.

Palo Alto-Firewall: Aktion zum Abrufen der Firewall-Konfiguration

Die Flow-Aktion **Palo Alto Firewall: Firewall-Konfiguration abrufen** ruft alle zugehörigen Firewall-Konfigurationsinformationen aus der -Datenbank ab und stellt sie für die Verwendung durch die nachfolgende Aktion bereit.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
FirewallSysid [Zeichenfolge]	Die System-ID der Firewall. Diese Eingabevariable ist obligatorisch.
typeOfValueToBeBlocked [Zeichenfolge]	Werttyp, der in der Firewall blockiert werden soll: IP, URL oder Domäne.
Firewall-IPAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
ipEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für IP-Adressen.
urlEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für URLs.
domainEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für Domänen.
FirewallVersionSysId [Zeichenfolge]	Die System-ID für die Firewall-Version.
refreshEDLCommand [Zeichenfolge]	Der zum Aktualisieren der EDL aus der Quelle zu verwendende Befehl.
ShowEDLDetailsCommand [Zeichenfolge]	Der zum Abrufen der EDL-Details zu verwendende Befehl.
status [Boolesch]	„Wahr“ bedeutet Erfolg. „Falsch“ gibt einen Fehler an.
Fehler [Zeichenfolge]	Der Fehler, der in der Aktion aufgetreten ist, falls vorhanden.
Endpunkt [Verschlüsselt]	Der verschlüsselte Endpunkt aus der Datenbank.

Palo Alto-Firewall: EDL-/DBL-Aktivität aktualisieren

Diese Aktivität führt einen operativen Befehl in der Firewall aus, um die externe dynamische Liste aus der in der Firewall konfigurierten Quelle zu aktualisieren. Die Ausgabe dieser Aktivität gibt an, ob der Aktualisierungsauftrag in die Warteschlange gestellt wurde.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgelisteten Eingabevariablen-Einträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall, die aktualisiert wird.
FirewallApiKey [Zeichenfolge]	Der aktualisierte Firewall-API-Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen (Fortsetzung)

Variable	Beschreibung
FirewallCommand [Zeichenfolge]	Der Betriebsbefehl, der ausgeführt werden soll, um den Aktualisierungsauftrag in die Warteschlange zu stellen.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
Aktivität.Ausgabe.Ergebnis [Zeichenfolge]	Eine Textzeichenfolge, die angibt, ob der Aktualisierungsauftrag in die Warteschlange gestellt wurde: Erfolg oder Fehler.

Protokolldaten-Flow abrufen

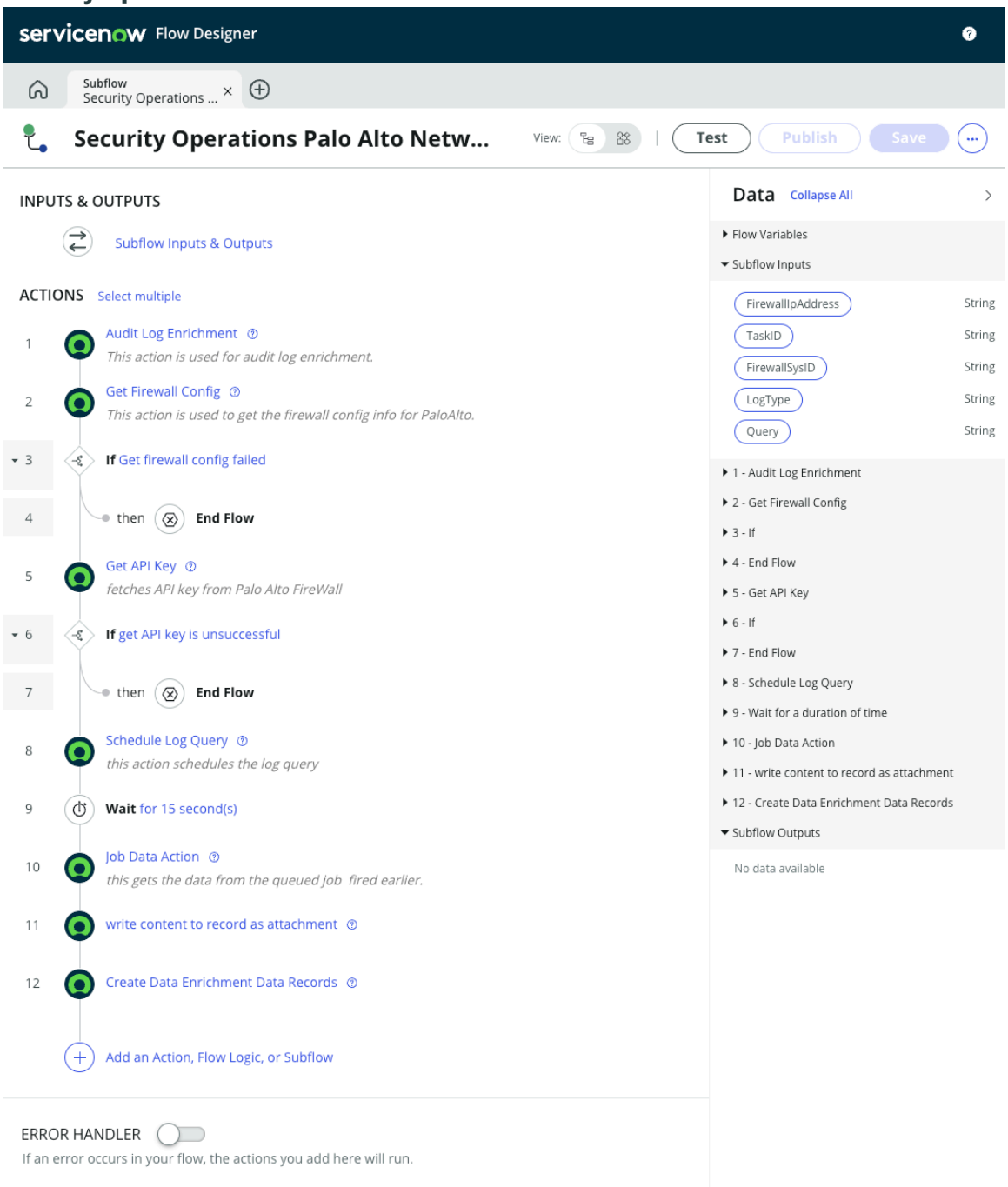
Wenn Security Incident Response, Threat Intelligenceund Palo Alto Networks – Firewall aktiviert sind, wird der Flow **„Security Operations Palo Alto Networks – Protokolldaten abrufen“** automatisch ausgeführt, wenn die Quell-IP für erkennbare Elemente in einem Security Incident geändert wird.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Während der Flow-Ausführung werden Firewall-Konfigurationsinformationen aus der -Datenbank abgerufen, und der API-Schlüssel wird von der Firewall abgerufen. Die Aktion „Protokoll abrufen“ stellt eine Suchabfrage in der Firewall bereit. Wenn die Abfrage ausgeführt wird, gibt sie eine Auftrags-ID zurück, die zum Abrufen von Bedrohungsprotokolldaten von der Firewall verwendet wird. Die Protokolldaten werden als XML-Datei an den Security Incident angehängt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations Palo Alto Networks: Flow zum Abrufen von Protokolldaten



Automatische Übersetzung

Prozedur

1. Navigieren Sie zu einem Security Incident, der erkennbare Elemente enthält.
2. Klicken Sie auf die Registerkarte **Erkennbare Elemente des Security Incidents**.
3. Fügen Sie unter **Quell-IP**die IP-Adresse hinzu, oder ändern Sie sie.
4. Klicken Sie auf **Aktualisieren**.
   Der Flow **„Security Operations Palo Alto Networks – Protokolldaten abrufen“** wird ausgeführt, und dem Security Incident werden angereicherte Bedrohungsprotokolldaten angehängt. Die Informationen werden auch analysiert und im Abschnitt **„Firewall-Protokolle“** auf der Registerkarte **Ergänzungsdaten** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Palo Alto-Firewall: Aktion „API-Schlüssel abrufen“.

Diese Aktion ruft den API-Schlüssel von der Firewall ab.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion. Alle aufgelisteten Eingabevariablen-Einträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
Anwendername [Zeichenfolge]	Der Anwendername des Firewall-Administrators.
Passwort [Zeichenfolge]	Das Passwort des Firewall-Administrators.
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
APIKey [Zeichenfolge]	Der Firewall-API-Schlüssel.

Palo Alto-Firewall: Aktion zum Abrufen der Firewall-Konfiguration

Die Flow-Aktion **Palo Alto Firewall: Firewall-Konfiguration abrufen** ruft alle zugehörigen Firewall-Konfigurationsinformationen aus der -Datenbank ab und stellt sie für die Verwendung durch die nachfolgende Aktion bereit.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
FirewallSysid [Zeichenfolge]	Die System-ID der Firewall. Diese Eingabevariable ist obligatorisch.
typeOfValueToBeBlocked [Zeichenfolge]	Werttyp, der in der Firewall blockiert werden soll: IP, URL oder Domäne.
Firewall-IPAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
ipEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für IP-Adressen.
urlEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für URLs.
domainEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für Domänen.
FirewallVersionSysId [Zeichenfolge]	Die System-ID für die Firewall-Version.
refreshEDLCommand [Zeichenfolge]	Der zum Aktualisieren der EDL aus der Quelle zu verwendende Befehl.
ShowEDLDetailsCommand [Zeichenfolge]	Der zum Abrufen der EDL-Details zu verwendende Befehl.
status [Boolesch]	„Wahr“ bedeutet Erfolg. „Falsch“ gibt einen Fehler an.
Fehler [Zeichenfolge]	Der Fehler, der in der Aktion aufgetreten ist, falls vorhanden.
Endpunkt [Verschlüsselt]	Der verschlüsselte Endpunkt aus der Datenbank.

Palo Alto-Firewall: Protokollaktion abrufen

Die Flow-Aktion **„Palo Alto-Firewall: Protokoll abrufen“** plant eine Abfrage auf der Firewall, um Protokolle abzurufen, und gibt eine JobID zurück, die zum Abrufen der Protokolldaten verwendet wird.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall. Diese Eingabevariable ist obligatorisch.
FirewallApiKey [Zeichenfolge]	Der API-Zugriffsschlüssel der Firewall. Diese Eingabevariable ist obligatorisch.
FirewallLogType [Zeichenfolge]	Der Typ der abzurufenden Protokolldaten (auf Bedrohung festgelegt). Diese Eingabevariable ist obligatorisch.
FirewallLogFilterQuery [Zeichenfolge]	Die Abfrage, die ausgeführt werden soll, um in der Firewall nach Protokollen zu suchen. Diese Eingabevariable ist obligatorisch.
LogDirection [Zeichenfolge]	Gibt an, ob Protokolle in der Reihenfolge zuerst (rückwärts) oder in der Reihenfolge zuerst (vorwärts) angezeigt werden.
LogNumber [Zeichenfolge]	Gibt die Anzahl der abzurufenden Protokolle an.
ProtokollÜberspringenAnzahl [Zeichenfolge]	Gibt die Anzahl der Protokolle an, die bei einem Protokollabruf übersprungen werden sollen.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
QueuedJobID [Zeichenfolge]	Die von der Firewall zurückgegebene Auftrags-ID.
JobGeplant [Zeichenfolge]	Gibt an (Erfolg oder Fehler), ob der Auftrag an die Firewall gesendet wurde.
Fehler [Zeichenfolge]	Alle zurückgegebenen Fehler.

Palo Alto-Firewall: Auftragsdatenaktion

Nachdem die Aktion **Palo Alto Firewall: Protokoll abrufen** die Suchabfrage in die Firewall stellt und der Auftrag ausgeführt wird, ruft die Aktion **Palo Alto Firewall: Auftragsdatenaktion** die Bedrohungsprotokolldaten von der Firewall ab.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion. Alle Eingabefelder sind Pflichtfelder.

Eingabevariablen

Variable	Beschreibung
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall.
FirewallApiKey [Zeichenfolge]	Der API-Zugriffsschlüssel der Firewall.
Auftrags-ID [Zeichenfolge]	Die ID des Auftrags in der Warteschlange.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
kommandoStatus [Zeichenfolge]	Gibt an (Erfolg oder Fehler), ob Daten von der Firewall abgerufen wurden.
Auftragsdaten [Zeichenfolge]	Die von der Firewall gesammelten Daten.
Fehler [Zeichenfolge]	Alle zurückgegebenen Fehler.

Palo Alto Networks – WildFire Integration

Palo Alto Networks – WildFire ist eine cloudbasierte Anwendung, die mit Ihrer Systemfirewall interagiert.

Erkunden

Security Incident Response-Integrationen

Einrichten

Aktivieren Sie Security Operations Palo Alto Networks – WildFire

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Verwenden	Entwickeln
Rufen Sie den WildFire-Datenanreicherungs-Flow ab	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Aktivieren Sie Security Operations Palo Alto Networks – WildFire

Bevor Sie die Integration „Security Operations Palo Alto Networks - WildFire“ verwenden können, müssen Sie die Integration aus dem ServiceNow Storeherunterladen.

Vorbereitungen

Erforderliche Rolle: Administrator

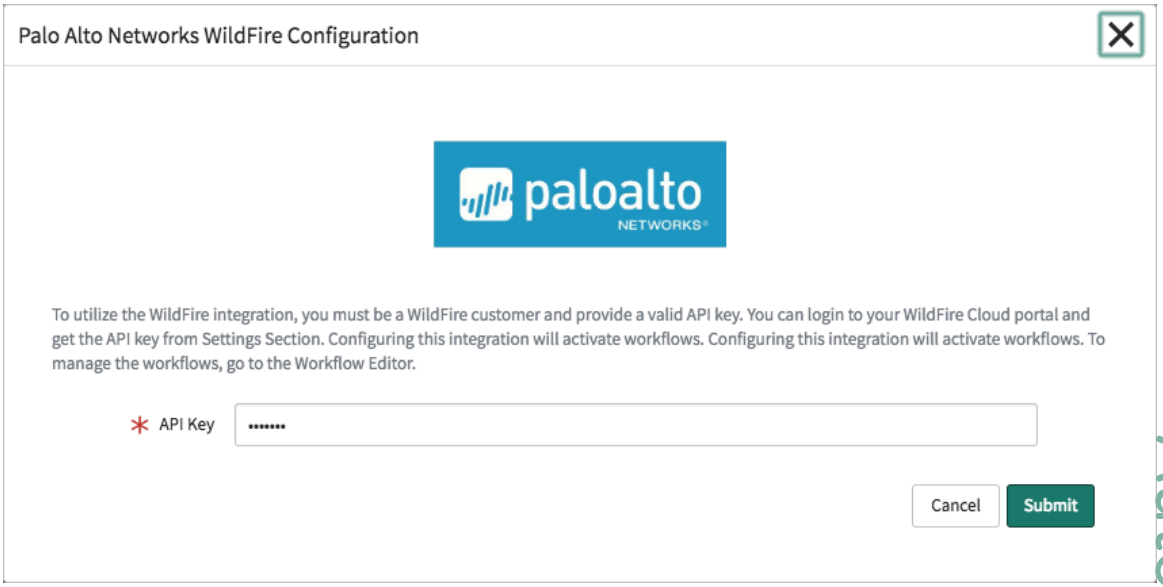
Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf der Karte Carbon Black auf **Konfigurieren**.



4. Geben Sie den API-Schlüssel ein, und klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
5. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

Rufen Sie den WildFire-Datenanreicherungs-Flow ab

Wenn der Flow „ **Security Operations Palo Alto Networks – WildFire-Datenanreicherung abrufen“** ausgeführt wird, wird eine Hash-Datei in WildFire hochgeladen. Die Daten werden angereichert, und Berichte werden in die Instanz heruntergeladen, um die Verarbeitung potenzieller Malware-Angriffe zu unterstützen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

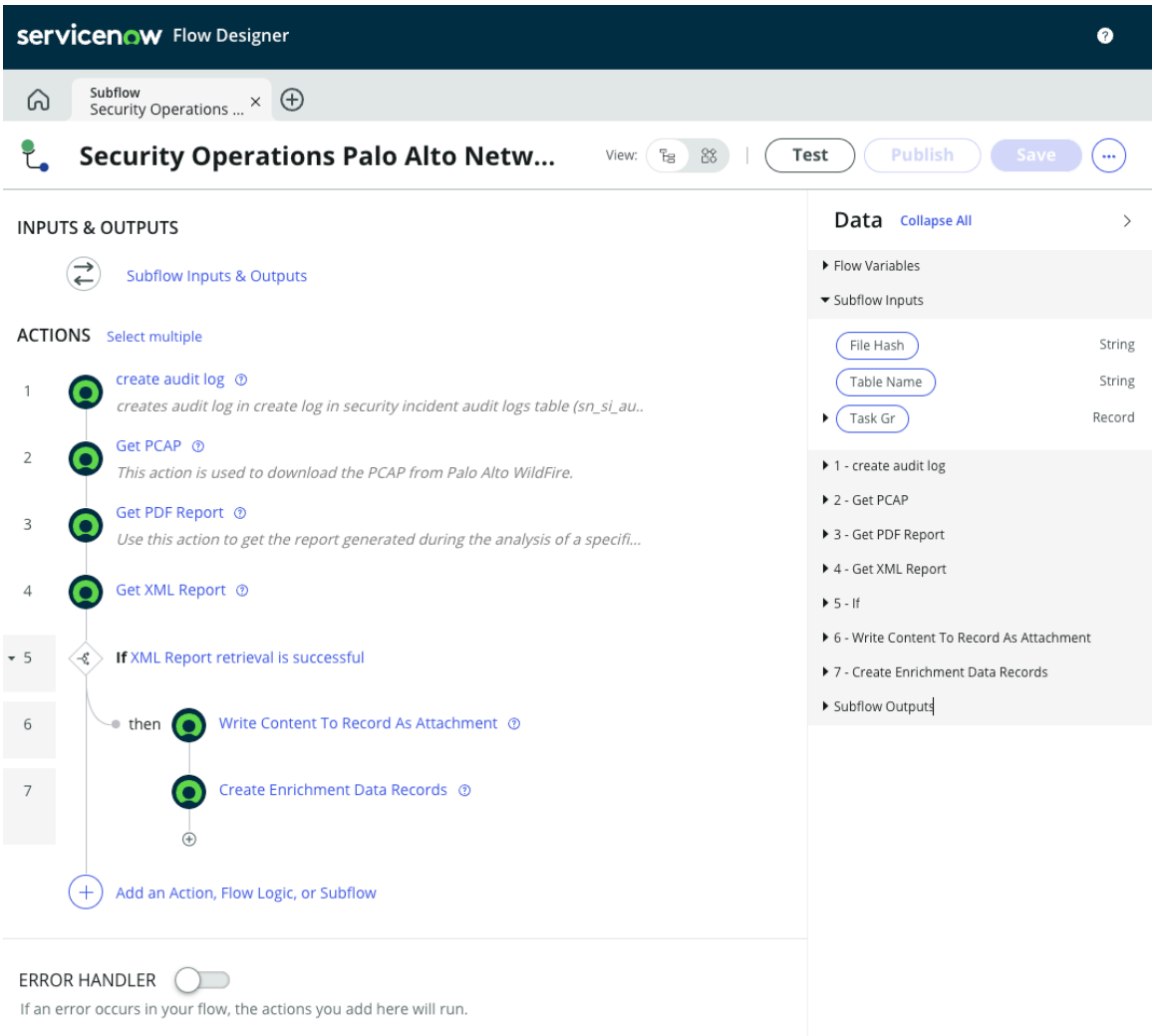
Warum und wann dieser Vorgang ausgeführt wird

Der Flow **„Security Operations Palo Alto Networks – WildFire-Datenanreicherung abrufen“** wird ausgeführt, wenn ein Security Incident aus einer Warnung erstellt wird, die von der Anwendung Palo Alto Network Firewall empfangen wurde. Auf der Registerkarte **„IoC“** des Security Incident wird ein Malware-Hash aus der E-Mail-Benachrichtigung eingegeben, die von der Firewall empfangen wurde, und der Datensatz wird aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations Palo Alto Networks – WildFire-Datenanreicherungs-Flow abrufen



Prozedur

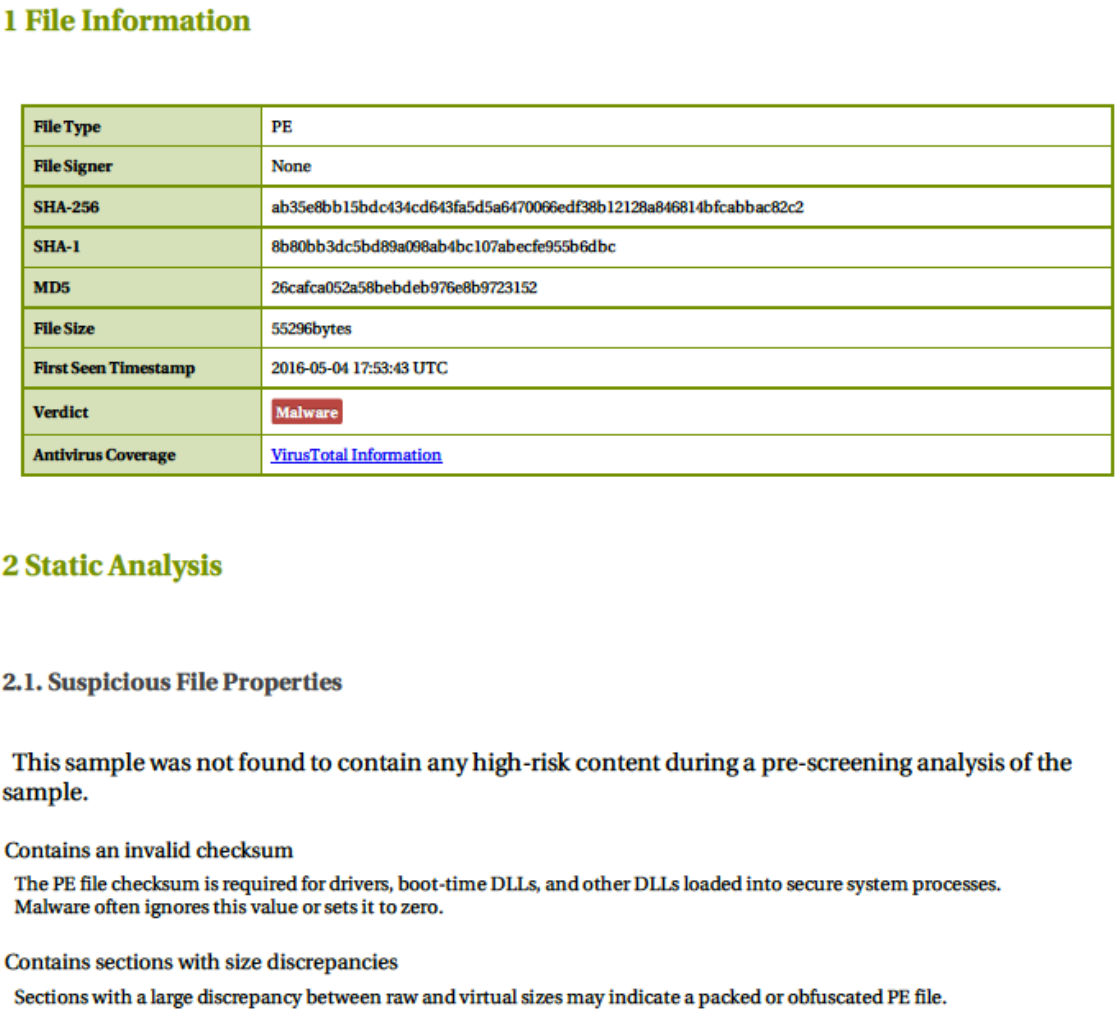
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Suchen und öffnen Sie den erstellten Security Incident anhand der E-Mail-Benachrichtigung, die Sie von der Firewall erhalten haben.
3. Klicken Sie auf die Registerkarte **Kompromittierungsindikatoren**, und füllen Sie den **Malware-Hash** mit dem Hash aus, den Sie in der Warnung erhalten haben.
4. Klicken Sie auf **Aktualisieren**.
   Der Flow bewirkt, dass die Hash-Datei in WildFire hochgeladen wird, wo die Daten angereichert werden. Berichte im PDF- und XML-Format werden an den Datensatz (Security Incident oder IoC) in Ihrer -Instanz angehängt, um die Verarbeitung potenzieller Malware-Angriffe zu unterstützen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn die angereicherten Daten Paketerfassungsinformationen enthalten, werden auch PCAP-Informationen heruntergeladen. PCAP-Daten erfassen, welche Aktionen die Datei ausgeführt hat. Beispielsweise kann gemeldet werden, welche Server die Datei kontaktiert hat. Zum Anzeigen von PCAP-Dateien benötigen Sie einen Paketanalysierer, z. B. Wireshark .

Beispiel für eine von WildFire generierte PDF-Datei



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

WildFire: PCAP-Aktion abrufen

Die Flow-Aktion **WildFire: Get PCAP** ruft die Paketerfassungsinformationen (PCAP) ab, die während der Analyse eines angegebenen Datei-Hashs in WildFire generiert wurden. Das Ergebnis dieser Aktion wird an einen bestimmten Datensatz angehängt, der durch **TableName** und **RecordId**identifiziert wird.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
DateiSHA256Hash [Zeichenfolge]	Der Hash der Datei, der von der Palo Alto Network Firewall-Anwendung empfangen wurde.
Tabellenname [Zeichenfolge]	Die betroffene Tabelle.
RecordId [Zeichenfolge]	Der Security Incident oder IoC, der aktualisiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
kommandierenStatus [Boolesch]	„Wahr“, wenn ein Ergebnis abgerufen und erfolgreich angehängt wurde.
errorMessage	Der Fehler, der in der Aktion aufgetreten ist, falls vorhanden.

WildFire: Aktion zum Abrufen des PDF-Berichts

Mit der Flow-Aktion **WildFire: Get PDF Report (WildFire: PDF-Bericht abrufen)** wird der Bericht, der während der Analyse eines angegebenen Datei-Hashs in WildFire generiert wurde, im PDF-Format abgerufen. Das Ergebnis dieser Aktion wird an einen bestimmten Datensatz angehängt, der durch **TableName** und **RecordId**identifiziert wird.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
Tabellenname [Zeichenfolge]	Die betroffene Tabelle.
DateiSHA256Hash [Zeichenfolge]	Der Hash der Datei, der von der Palo Alto Network Firewall-Anwendung empfangen wurde.
RecordId [Zeichenfolge]	Der Security Incident oder IoC, der aktualisiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
kommandierenStatus [Boolesch]	„Wahr“, wenn ein Ergebnis abgerufen und erfolgreich angehängt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
errorMessage	Der Fehler, der in der Aktion aufgetreten ist, falls vorhanden.

WildFire: Aktion zum Abrufen des XML-Berichts

Mit der Flow-Aktion **„WildFire: XML-Bericht abrufen“** wird der Bericht, der während der Analyse eines angegebenen Datei-Hashs in WildFire generiert wurde, im XML-Format abgerufen. Das Ergebnis dieser Aktion wird an einen bestimmten Datensatz angehängt, der durch **TableName** und **RecordId**identifiziert wird.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
Tabellenname [Zeichenfolge]	Die betroffene Tabelle.
DateiSHA256Hash [Zeichenfolge]	Der Hash der Datei, der von der Palo Alto Network Firewall-Anwendung empfangen wurde.
RecordId [Zeichenfolge]	Der Security Incident oder IoC, der aktualisiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
kommandierenStatus [Boolesch]	„Wahr“, wenn ein Ergebnis abgerufen und erfolgreich angehängt wurde.
errorMessage	Der Fehler, der in der Aktion aufgetreten ist, falls vorhanden.

Palo Alto Networks Next-Generation Firewall Integration

Nach der Installation und Konfiguration verwendet der Security Incident-Analyst diese Integration, um schädliche IP-Adressen, URLs und Domänen mithilfe von EDL-Funktionen (External Dynamic List) mit den -Produkten ServiceNow Security Incident Response (SIR) zu blockieren. Der Security Incident-Analyst erstellt Einträge für eine EDL aus erkennbaren Elementen, die bei Security Incidents ServiceNow SIR als schädlich eingestuft wurden.

Eine EDL ist eine Textdatei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihre Instanz Now Platform, die es der Instanz Palo Alto Networks Next-Generation Firewall ermöglicht, Objekte zu importieren, die in der Liste, IP-Adressen, URLs und Domänen enthalten sind, und Richtlinien zu erzwingen.

Um eine Richtlinie für die EDL-Einträge zu erzwingen, wird in einer Richtlinienregel oder einem Profil auf die Liste verwiesen. Wenn die EDL-Einträge geändert werden, importiert die Firewall die Liste dynamisch im konfigurierten Intervall und erzwingt die Richtlinie ohne Konfigurationsänderung oder Commit auf der Firewall. Für diese Integration hat Now Platform

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Tabelle mit EDL-Einträgen erstellt, die vom autorisierten Palo Alto Networks Next-Generation Firewall in den konfigurierten Abrufintervallen abgerufen werden.

Die Integration umfasst die folgenden Funktionen:

- Flexibilität zum Erstellen mehrerer EDLs, die für verschiedene Firewall-Richtlinien zum Verweigern oder Zulassen gelten.
- Detaillierte Berichte zu den Arten von blockierten Websites (Phishing, Malware und auf der Zulassungsliste aufgeführte Websites).
- Tagging von Now Platform Security Incidents mit EDL-Einträgen nach erkennbarem Elementtyp (URL, Domäne, IP-Adresse).
- EDL-Ablaufzeiträume konfigurieren, um die EDL-Listengröße durch automatisches Ablaufen oder Entfernen älterer Einträge beizubehalten.
- Suchen, Löschen oder Migrieren von EDL-Einträgen zwischen EDL-Listen.
- Verknüpfen von EDL-Einträgen mit erkennbaren Datensätzen und Security Incidents, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert wurde.

Zur Integration müssen die Plugins (com.snc.security_incident) und (com.snc.secops.orchestration) aus dem Produkt Security Incident Response aktiviert sein.

Diese Integration unterstützt nur Palo Alto Networks (PAN-OS 8.x). Frühere Versionen werden nicht unterstützt.

Diese Integration ist kompatibel mit den Releases Kingston, London, Madrid und New York von Now Platform®.

Hinweis:
Die folgenden Themen sind nummeriert. Um eine reibungslose Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse zu gewährleisten, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.

Erstellen Sie ein Zertifikatprofil für Palo Alto Networks Next-Generation Firewall

Die Integration erfordert ein Zertifikatprofil zum Validieren und Authentifizieren der sicheren Verbindung zwischen den Servern Now Platform® und dem Server Palo Alto Networks Next-Generation Firewall.

Erforderliche Rolle: Palo Alto Networks Next-Generation Firewall Administrator.

Ein Palo Alto Networks Next-Generation Firewall authentifiziert sich bei einer Now Platform® -Instanz, ruft EDL-Einträge aus der Datenbanktabelle ab und integriert die Einträge in die entsprechenden Firewall-Richtlinienregeln. Dieser Abruf erfordert die Rolle „API-Anwenderkonto“ in der Instanz Now Platform®, die vom PAN-Firewall-Administrator für den Zugriff auf die API Now Platform® verwendet wird.

Führen Sie die folgenden Schritte aus, um DigiCertificates herunterzuladen und das Zertifikatprofil zu konfigurieren.

1. Laden Sie das DigiCert- oder Entrust CA-Gateway-Zertifikat je nach Anwendungsfall herunter. Weitere Informationen finden Sie im Artikel KB1702083 in der Now Support Knowledge Base.
2. Konfigurieren Sie das Zertifikatprofil. Weitere Informationen finden Sie in der Dokumentation zu Palo Alto Networks .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

„Ein Zertifikatprofil konfigurieren“ im PAN-OS 10.0-Administratorhandbuch

Richten Sie ein, und installieren Sie Palo Alto Networks Next-Generation Firewall

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation erforderlich.

Vorbereitungen

Erforderliche Rolle: (admin)

Setupaufgabe	Beschreibung
Vergewissern Sie sich, dass Ihnen die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen sind.	Die folgenden Rollen sind erforderlich: • Der Systemadministrator (admin) installiert die App und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und erstellt, aktiviert und entfernt EDLs. Mit dieser Rolle wird auch die Rolle sn_si.analyst zugewiesen. • Der -Administrator weist die API-Kontorolle Now Platform® (sn_sec_panfw.api_account_access) zu, die ausschließlich für die Eingabe der Anmeldeinformationen verwendet wird, die für die Authentifizierung bei Palo Alto Networks erforderlich sind, damit die Firewalls EDLs von Now Platform®abrufen können. • (sn_si.analyst) oder Security Operations Center-Analyst (SOC), erstellt EDL-Einträge und arbeitet mit Security Incidents.
Stellen Sie sicher, dass Sie Palo Alto Networks Next-Generation Firewall Version-BS 9.x und 10.x verwenden.	Diese Integration unterstützt nur Palo Alto Networks Next-Generation Firewall OS 9.0 und höher.
Richten Sie alle EDL-Profile, Sicherheitsrichtlinienregeln und Zertifikatprofile in Palo Alto Networks ein, wie in der Dokumentation zu Palo Alto Networks empfohlen.	Weitere Informationen finden Sie in der allgemeinen Dokumentation und den Anforderungen für Palo Alto Networks auf der Website der Paloalto Networks-Dokumentation .
Vergewissern Sie sich, dass Sie das DigiCert-Root Authority-Zertifikat heruntergeladen und konfiguriert haben.	Die Integration erfordert dieses Zertifikat, um die sichere Verbindung zwischen dem Server Now Platform und dem Server Palo Alto Networks Next-Generation Firewall zu validieren und zu authentifizieren. Weitere Informationen zum Einrichten des Zertifikats finden Sie unter „Configure a Certificate Profile“ (Ein Zertifikatprofil konfigurieren) im PAN-OS 10.0-Administratorhandbuch . Informationen zum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	Herunterladen finden Sie unter Erstellen Sie ein Zertifikatprofil für Palo Alto Networks Next-Generation Firewall und DigiCert Trusted Root Authority Certificates (DIG-Zertifikate) .
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Madrid- und höher-Release-Anforderungen Für das Madrid-Release und spätere Familienreleases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.
Wenn Ihre Organisation über Now Platform® Change-Management- und Genehmigungsprozesse für das Löschen von E-Mails verfügt, vergewissern Sie sich, dass die Funktion zum Senden/Empfangen von E-Mails aktiviert ist.	Um sicherzustellen, dass die Funktion zum Senden/Empfangen von E-Mails in Ihrer Instanz Now Platform® aktiviert ist, navigieren Sie zu **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**. Überprüfen Sie unter „Konfiguration ausgehender E-Mails“, ob **E-Mail-Versand** und **-Empfang** ausgewählt sind.

Prozedur

Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie die API-Kontorolle für Palo Alto Networks Next-Generation Firewall

Für diese Integration ist in Ihrer Instanz Now Platform® eine API-Kontorolle erforderlich. Der diesem Account zugeordnete Anwendername und das Passwort werden in Now Platform® erstellt und in Palo Alto Networks eingegeben, damit sich Palo Alto Networks Next-Generation Firewall beim Abrufen von EDL-Einträgen mit Now Platform® authentifiziert.

Vorbereitungen

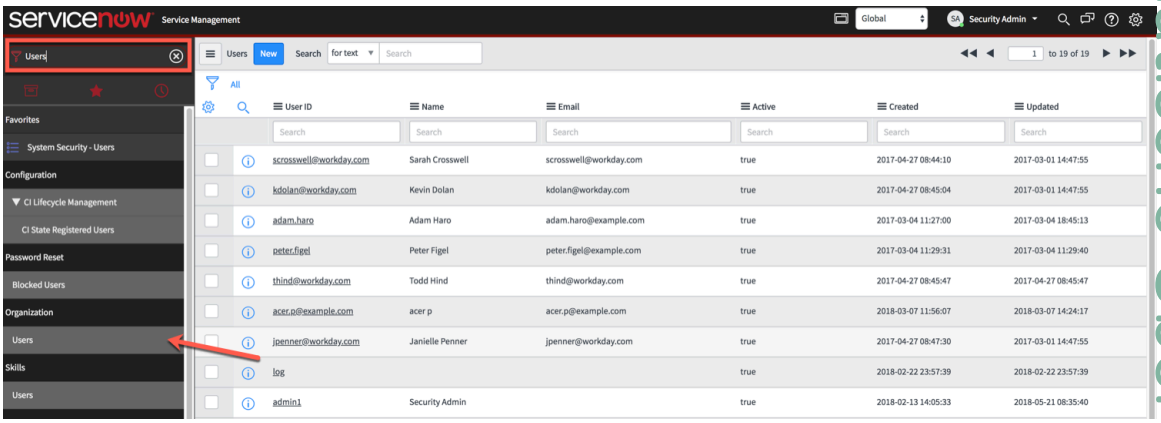
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

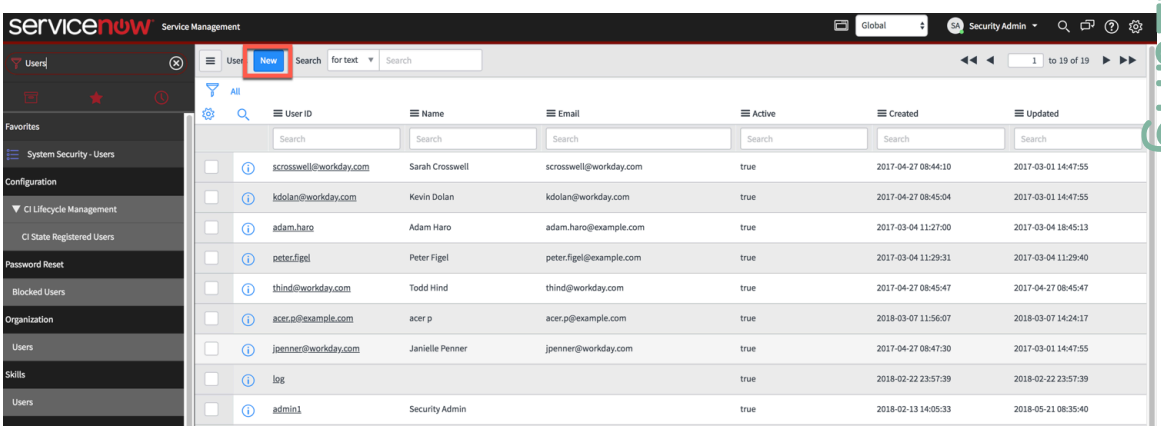
Der Administrator Now Platform® erstellt eine API-Kontorolle (sn_sec_panfw.api_account_access). Dieser Account wird ausschließlich für die Eingabe von Anmeldeinformationen verwendet, die für die Authentifizierung bei Palo Alto Networks erforderlich sind, damit die Firewalls EDLs von Now Platform®abrufen können. Dieser Account ist ein separater, eindeutiger API-Anwenderaccount in der Instanz Now Platform® und wird dem Administrator Palo Alto Networks Next-Generation Firewall zugewiesen.

Prozedur

1. Navigieren zu **Alle** > **Organisation** > **Anwender**.
2. Klicken Sie auf das Modul **Benutzer**.



3. Klicken Sie in der angezeigten Benutzerliste auf **Neu**.



Ein neues Anwenderformular wird angezeigt.

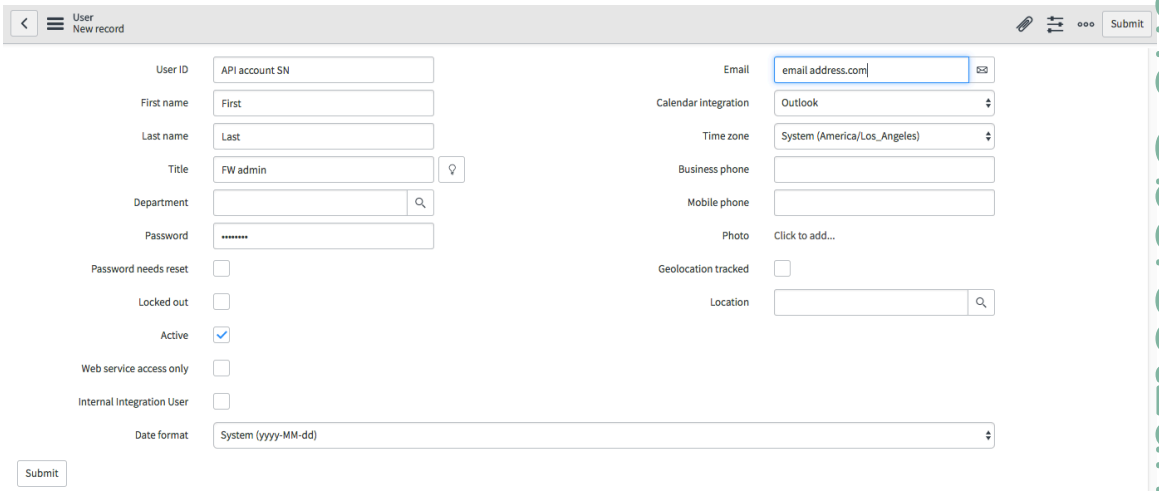
4. Füllen Sie das Formular aus.

Automatische Übersetzung

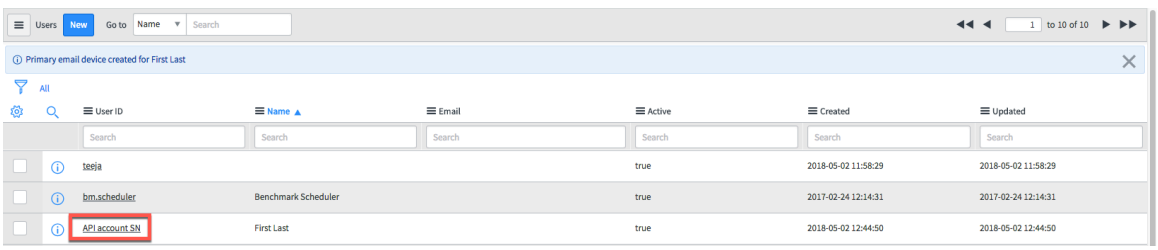
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die in der folgenden Tabelle und Abbildung gezeigten Werte für Anwender-ID-Titel und E-Mail-Adresse sind Beispielwerte.

Feld	Beschreibung
Anwender-ID	Eindeutige Anwender-ID für die Rolle in Ihrer Instanz Now Platform®. Diese Anwender-ID wird im Feld **Anwendername** im Abschnitt **„Client-Authentifizierung“** des Dialogfelds „Externe dynamische Listen“ auf der Site Palo Alto Networks eingegeben. Ein Beispiel ist API-Account SN.
Vorname	Person, die Sie zuweisen
Nachname	Person, die Sie zuweisen
Titel	Stellenbezeichnung, z. B. FW-Administrator.
Passwort	Eindeutiges Passwort, das für diese Rolle erstellt wurde. Dieses Passwort wird im Feld **Passwort** im Abschnitt **„Client-Authentifizierung** “ des Dialogfelds „Externe dynamische Listen“ auf der Website Palo Alto Networks eingegeben.
E-Mail	Eindeutige E-Mail-Adresse.



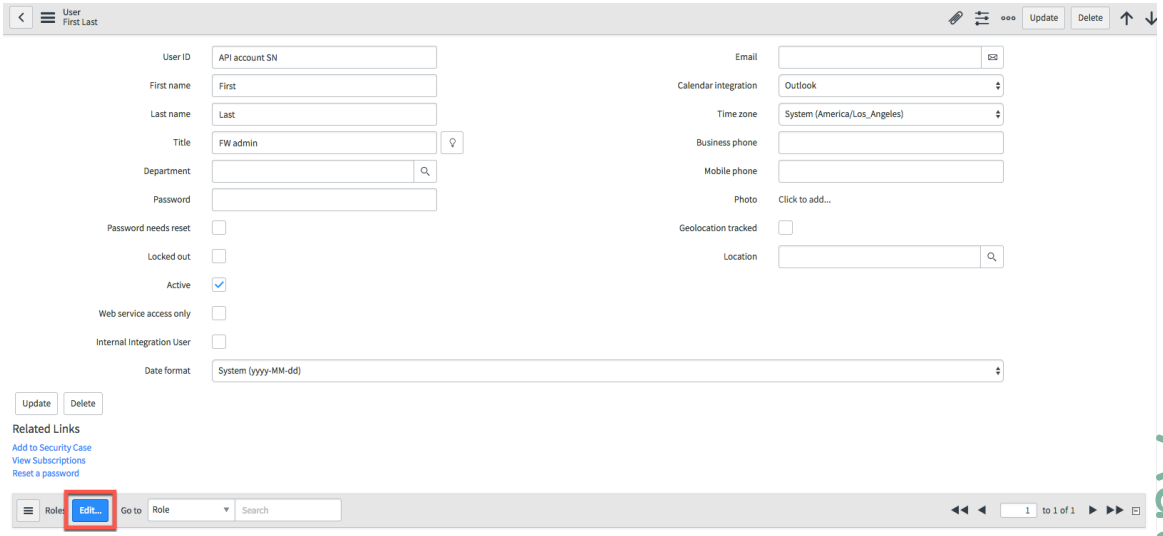
5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung können Sie die Rolle zuweisen.
6. Klicken Sie in der Liste Benutzer in der Spalte **Benutzer-ID** auf den Namen der eingegebenen Benutzer-ID, z. B. API-Konto SN.



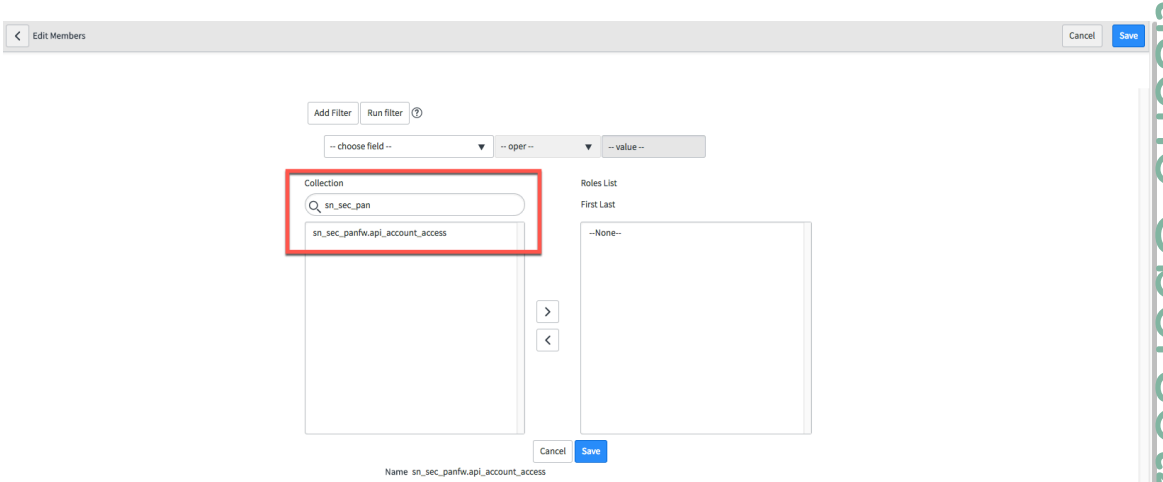
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

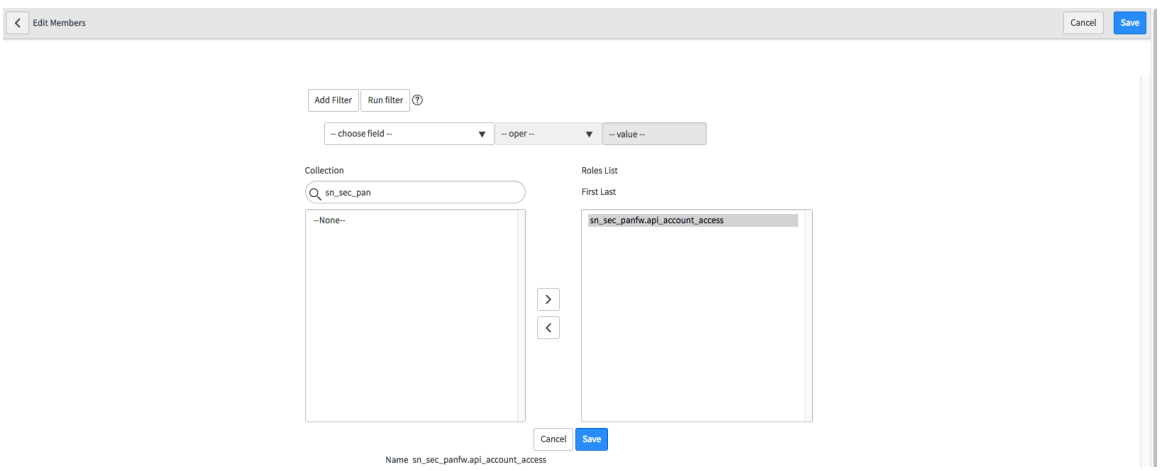
7. Klicken Sie im geöffneten Datensatz im Abschnitt „Rollen“ auf **Bearbeiten**.



8. Geben Sie im angezeigten Formular **„Mitglieder bearbeiten“** im Feld **Sammlung**den Wert sn_sec_panfw.api_account_access ein.
Unter dem Feld **Sammlung** wird die Rolle in der Spalte angezeigt.



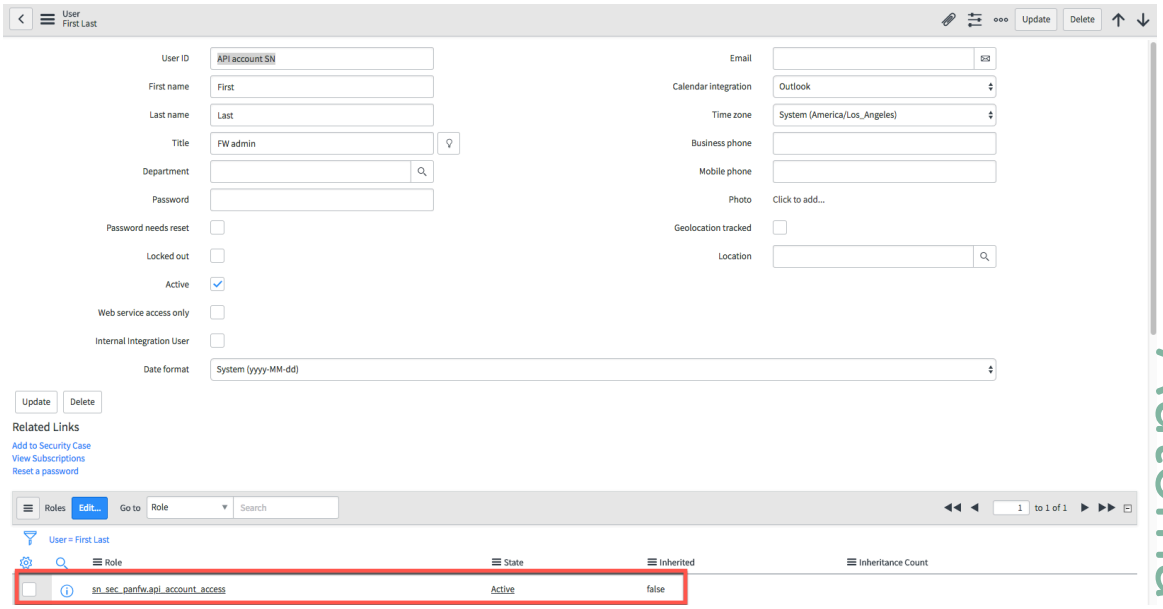
9. Wählen Sie in der Spalte **Sammlung** die Option aus, und verschieben Sie sn_sec_panfw.api_account_access in die **Rollenliste**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf **Speichern**.
11. Navigieren Sie zu **Benutzer**, und klicken Sie in der **Benutzerspalte** der Liste auf den ID-Namen, den Sie für die Rolle (API-Konto-SN) erstellt haben.



Der Benutzerdatensatz wird angezeigt. Dieser Datensatz verifiziert, ob der Anwenderaccount zugewiesen wurde. Der **Status** ist „Aktiv“, und die Rolle wird nicht geerbt.

Unterstützte externe dynamische Listen für Palo Alto Networks Next-Generation Firewall

Die ServiceNow Palo Alto Networks Next-Generation Firewall -Integration unterstützt externe dynamische Listen (External Dynamic Lists, EDLs), die erkennbare IP-, URL- und Domänenelemente akzeptieren.

Unterstützte EDLs und erkennbare Elemente

Eine *externe dynamische Liste* ist eine Textdatei, die auf einem externen *Webserver*gehostet wird, der für diese Integration die Instanz Now Platform ist. Palo Alto Networks Next-Generation Firewall kann dann Objekte importieren – IP-Adressen, URLs, Domänen –, die in der Liste enthalten sind, und die Richtlinie erzwingen. Um eine Richtlinie für die EDL-Einträge zu erzwingen, wird in einer Richtlinienregel oder einem Profil auf die Liste verwiesen.

Diese Integration unterstützt drei Arten von EDLs:

- IP (Dies umfasst eine einzelne IP-Adresse sowie CIDR-Blöcke (Bereiche) von Adressen).
- URL
- Domäne

Die folgende Tabelle enthält Beschreibungen der von dieser Integration unterstützten erkennbaren Elemente und Beispielformate für jeden Typ.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte erkennbare Elemente und Beispielformate

Erkennbares Element	Beispielformate	Beschreibung
IP-Adresse	• 95.153.103.54 (IPv4) • (IPv6): 2001:00B8:130F:FE03:0000:0900:980F:130B	Stellt eine einzelne, eindeutige Schnittstellenadresse dar. Die Integration unterstützt die Formate IPv4, IPv6 und CIDR. Die Unterstützung für erkennbare IP-Adressen umfasst CIDR-Bereiche (Classless Inter-Domain Routing), z. B. 95.153.100.0/22. Hinweis: Eine Fehlermeldung wird angezeigt, wenn Sie versuchen, eine einzelne IP-Adresse an eine EDL anzuhängen, die Sie bereits als Teil eines CIDR-Bereichs blockiert haben. Zum Beispiel ist die einzelne Adresse 95.153.103.54 Teil des CIDR-Bereichs 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	Platzhalter werden unterstützt. Now Platform formatiert URL-Einträge neu, um die EDL-Formatanforderungen für Palo Alto Networks zu erfüllen.
Domäne	• www.example.com • example.com • mail.example.com	Platzhalter werden nicht unterstützt.

Weitere Informationen zu Formatierungsrichtlinien und EDLs finden Sie unter „Formatierungsrichtlinien für eine externe dynamische Liste“ im PAN-OS 10.0-Administratorhandbuch auf der Website Palo Alto Networks.

Erstellen Sie eine EDL für Palo Alto Networks Next-Generation Firewall

Erstellen Sie eine externe dynamische Liste (External Dynamic List, EDL) in Ihrer Instanz Now Platform. Nach der Genehmigung und Aktivierung können Sie Einträge für EDLs aus erkennbaren Elementen erstellen, die in Incidents Now Platform Security Incident Response (SIR) als schädlich eingestuft wurden, und eine Genehmigung zu deren Blockierung anfordern.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie die EDL in Ihrer Instanz Now Platform, damit die Firewall in der Liste enthaltene Objekte (IP-Adressen, URLs, Domänen) importieren und die Richtlinie erzwingen kann. Um eine Richtlinie für die EDL-Einträge zu erzwingen, wird in einer Richtlinienregel oder einem Profil auf die Liste verwiesen.

Die Abbildungen im folgenden Abschnitt werden mit in den Systemeinstellungen gelöschten **Formularen mit Registerkarten** angezeigt. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt „Formulare mit Registerkarten anzeigen“ in Configuring the form layout .

Prozedur

1. Navigieren Sie nach Abschluss der Anwendungsinstallation zu **Integrationen** > **Integrationskonfigurationen**.
2. Suchen Sie die Kachel Palo Alto Networks Next-Generation Firewall, und klicken Sie auf **Konfigurieren**.

3. Klicken Sie **auf Neue EDL-Liste erstellen**.

4. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Palo Alto Networks Formular „Externe dynamische Firewall-Liste“.

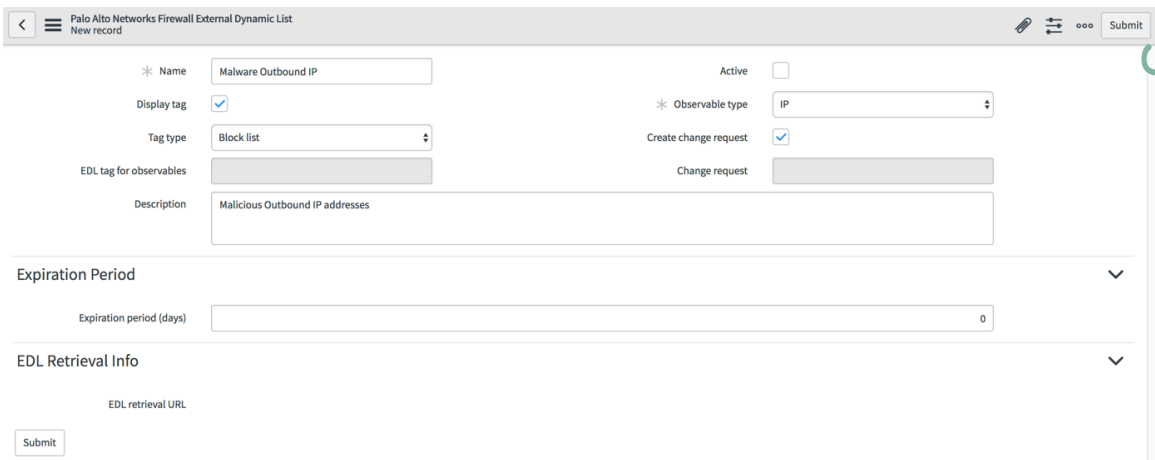
Feld	Beschreibung
Name	Palo Alto Networks Name der dynamischen Firewall-Liste. Fügen Sie den Typ des erkennbaren Elements (URL, IP, Domäne) in dieses Feld ein, damit der Sicherheitsanalyst die Absicht der EDL anhand des Namens leicht erkennen kann. Der Name sollte auch eindeutig angeben, welcher Firewall-Richtlinie diese EDL-Objekte zugeordnet sind. Einige Beispiele für EDL-Namen sind „Ausgehende Malware-IP“ oder „Ausgehende Phishing-URL“.
Aktiv	Dieses Kontrollkästchen ist standardmäßig deaktiviert, um anzugeben, dass die EDL inaktiv ist. Wenn sie inaktiv ist, kann die EDL keine zusätzlichen Einträge empfangen. Wenn das Kontrollkästchen aktiviert ist, ist die EDL aktiviert und für EDL-Einträge verfügbar.
Tag anzeigen	Das Kontrollkästchen ist standardmäßig aktiviert, um das erkennbare Element und den zugehörigen Security Incident-Datensatz automatisch zu kennzeichnen, wenn das erkennbare Element auf einer EDL blockiert ist. Wenn diese Option ausgewählt ist, sind die Felder Tag-Typ und EDL-Tag für erkennbare Elemente im Formular verfügbar. **Hinweis:** Ein Tag-Name wird standardmäßig aus dem Wert erstellt, den Sie im Feld **Name** mit einem *EDL*-Präfix eingeben, z. B. EDL-Malware OutBound IP. Sie können den Tag-Namen und die Farbe ändern. Siehe: (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall. Der Tag-Name wird im Feld EDL-Tag für erkennbare Elemente angezeigt, sobald die EDL gespeichert wird. Wenn das Kontrollkästchen deaktiviert ist, wird kein Tag erstellt, und die Felder Tag-Typ und EDL-Tag für erkennbare Elemente sind im Formular nicht verfügbar.
Erkennbarer Typ	Wählen Sie in der Auswahlliste einen erkennbaren Elementtyp aus, den diese EDL akzeptiert: IP (einschließlich CIDR), URL oder Domäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tag-Typ	Tags, die in der Auswahlliste verfügbar sind. Eine Sperrliste ist eine Liste der erkennbaren Elemente, die Palo Alto Networks Next-Generation Firewall blockieren soll. Eine Allow-Liste ist eine Liste von erkennbaren Elementen, die Palo Alto Networks Next-Generation Firewall zulassen soll. Standardmäßig ist die Tag-Farbe der Sperrliste schwarz und die Tag-Farbe der Allow-Liste grau. Sie können die Farbe ändern. Siehe: (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall.
Erstellen Sie eine Change-Anforderung	Dieses Kontrollkästchen ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in Ihrer Instanz Now Platform zu erstellen, die an den EDL-Datensatz angehängt sind. Die Change-Anforderung wird verwendet, um die Abruf-URL für die EDL-Liste auf dem Server Palo Alto Networks Next-Generation Firewall zu konfigurieren. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch Now Platform für Änderungen an Firewall-Richtlinien oder -Regeln verwendet. Wenn Sie eine Anforderung erstellen, wird die EDL-Liste nach dem Schließen automatisch aktiviert. Deaktivieren Sie das Kontrollkästchen, um die EDL manuell zu aktivieren, nachdem Sie per E-Mail vom Firewall-Administrator benachrichtigt wurden, dass die Konfiguration auf Palo Alto Networks abgeschlossen ist. Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, ist das Feld Change-Anforderung nicht verfügbar.
EDL-Tag für erkennbare Elemente	Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen Tags anzeigen aktiviert ist. Das Feld wird automatisch ausgefüllt, nachdem die EDL mit einem Standardwert aus dem Feld Name gespeichert wurde. Weitere Informationen zum Ändern des Standard-Tag-Namens und der Farbe finden Sie unter (Optional) Bearbeiten Sie den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall
Change-Anforderung	Wenn das Kontrollkästchen Change-Anforderungen erstellen aktiviert ist, wird die Nummer der Change-Anforderung in der Instanz Now Platform angezeigt, sobald die EDL gespeichert wurde. Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, wird dieses Feld nicht angezeigt.
Beschreibung	Beschreibung der dynamischen Liste der Palo Alto Networks-Firewalls. Der Name enthält im Allgemeinen die Typen von Websites und erkennbaren Elementen, die erwartet werden, dass sie sich in dieser EDL befinden. Sie können dieses Feld für weitere Details verwenden.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der EDL. 0 (Standardeinstellung) gibt an, dass der EDL-Eintrag nie abläuft. Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Es gibt keinen Höchstwert. Wenn Sie beispielsweise am 1. Mai um 14:01 Uhr 30 Tage eingeben, läuft die EDL am 31. Mai um 14:01 Uhr ab. Alle Einträge in dieser EDL erben dann diesen Wert standardmäßig, es sei denn, Sie überschreiben den Wert auf Basis einzelner Einträge.

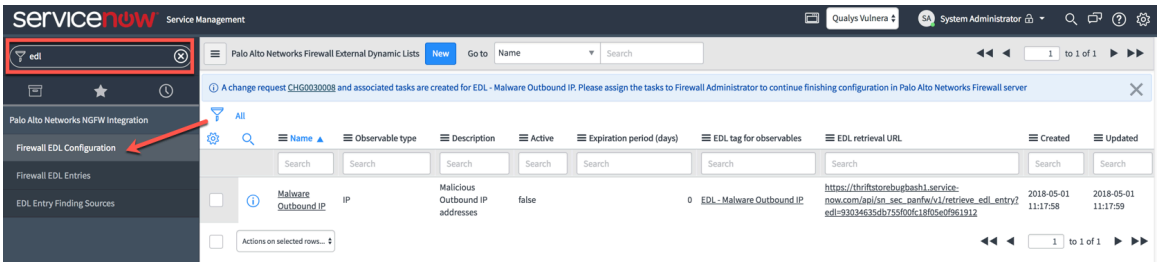


5. Klicken Sie auf **Absenden**.

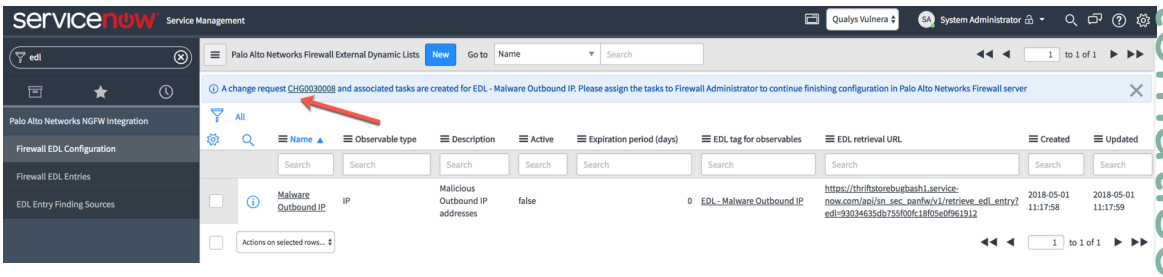
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

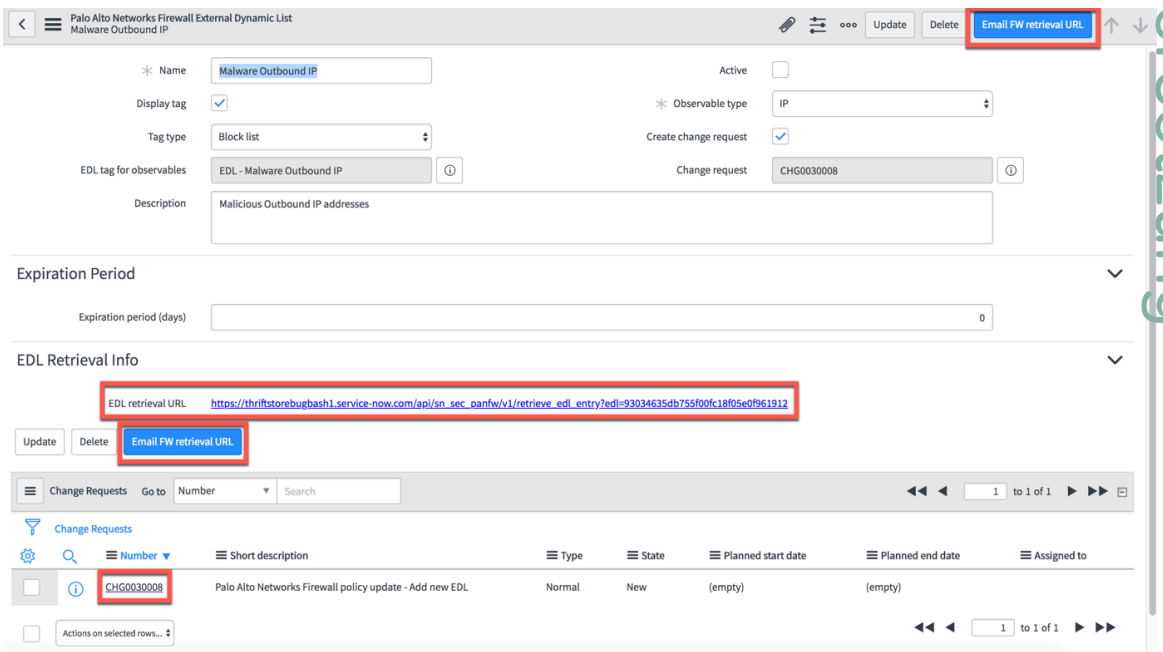
6. Wenn die Liste der externen dynamischen Listen der Palo Alto Networks-Firewalls nicht angezeigt wird, navigieren Sie zu **Palo Alto Networks NGFW-Integration** > **EDL-Konfiguration der Firewall** und klicken Sie auf **Firewall-EDL-Konfiguration**.



Die neue EDL wird angezeigt. Der EDL-Status ist weiterhin inaktiv (false), was bedeutet, dass die EDL nicht für die Annahme von Einträgen verfügbar ist. Wenn **Change-Anforderung erstellen** konfiguriert wurde, wird eine Nachricht angezeigt, die angibt, dass in Ihrer Instanz Now Platform ein Change-Anforderung und Aufgaben erstellt wurden.



7. Klicken Sie in der Spalte **Name** auf ein Element, um den Datensatz zu öffnen.
Der EDL-Datensatz wird angezeigt. Dieses Beispiel zeigt eine ausgehende IP-EDL für Malware. Die folgenden Felder, Optionen und Links werden nach der Übermittlung im neuen Datensatz angezeigt und in der folgenden Tabelle beschrieben.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abruf-URL und Change-Anforderungs-Links im EDL-Datensatz

Option	Beschreibung
FW-Abruf-URL mailen	Sendet eine Benachrichtigung per E-Mail, dass der EDL-Link für die Konfiguration verfügbar ist, an den Firewall-Administrator Palo Alto Networks.
EDL-Abruf-URL	Diese URL wird im Authentifizierungsdialogfeld „Externe dynamische Listen“ auf der Registerkarte **„Liste erstellen“** auf der Website Palo Alto Networks im Feld **„Quelle“** platziert. Der URL-Link, den der Firewall-Administrator für Palo Alto Networks für die Konfiguration in der Firewall Palo Alto Networks von verwendet, wird automatisch generiert und angezeigt. **Hinweis:** Wenn Ihre Systemeinstellungen auf **Formulare mit Registerkarten**festgelegt sind, wird dieser Link auf der Registerkarte **EDL-Abrufinformationen** unten im Datensatz angezeigt.
Now Platform Change-Anforderung	Ein Link zum Datensatz der Change-Anforderung wird im Abschnitt „Change-Anforderungen“ angezeigt, sofern konfiguriert, und die Nummer der Anforderung wird im Feld Change-Anforderung angezeigt.
Aktualisieren	Ändern Sie Daten, und aktualisieren Sie die bearbeitbaren Felder.
Löschen	Löschen Sie den Datensatz.

8. Erstellen und fügen Sie nach Bedarf weitere EDLs hinzu.
   Die EDLs werden in der Liste Palo Alto Networks Externe dynamische Listen angezeigt.

Nächste Maßnahme

Aktivieren Sie eine EDL manuell oder mit einer Change-Anforderung Now Platform.

Aktivieren Sie eine EDL für Palo Alto Networks Next-Generation Firewall

Nachdem die externe dynamische Liste (External Dynamic List, EDL) in Ihrem Now Platform® erstellt wurde und die URL verfügbar ist, konfiguriert der Firewall-Administrator Palo Alto Networks die EDL im Palo Alto Networks Next-Generation Firewall. Die Abruf-URL wird vom Firewall-Administrator Palo Alto Networks zum Konfigurieren der EDL auf dem Server Palo Alto Networks Next-Generation Firewall verwendet. Bevor EDL-Einträge akzeptiert werden können, muss die EDL in Palo Alto Networks konfiguriert und in Now Platform®aktiviert werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

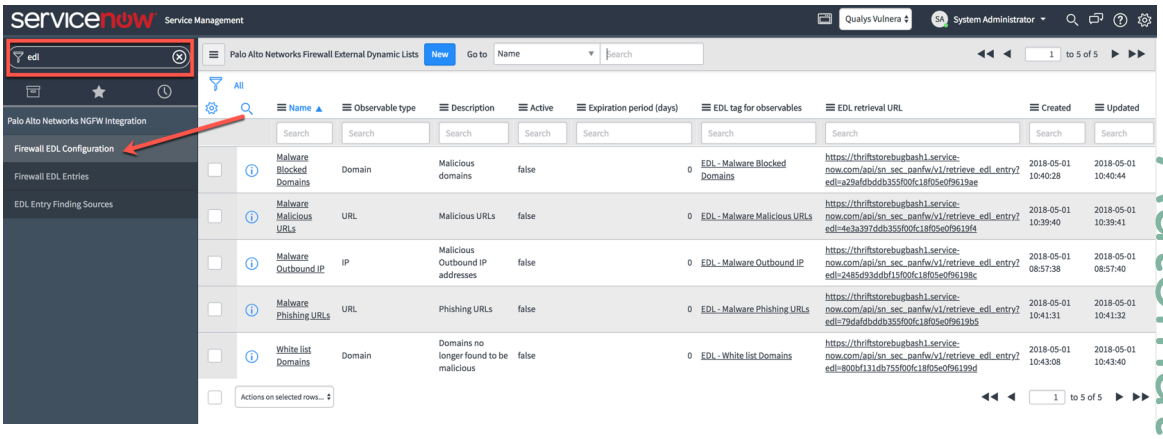
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Nachdem die EDL konfiguriert wurde, können Sie sie als Security Incident-Administrator manuell aktivieren. Alternativ wird sie automatisch nach Abschluss einer Now Platform® Change-Anforderung aktiviert. Die EDL muss genehmigt und vom Status „Inaktiv“ in den Status „Aktiv“ versetzt werden, bevor sie EDL-Einträge akzeptieren kann.

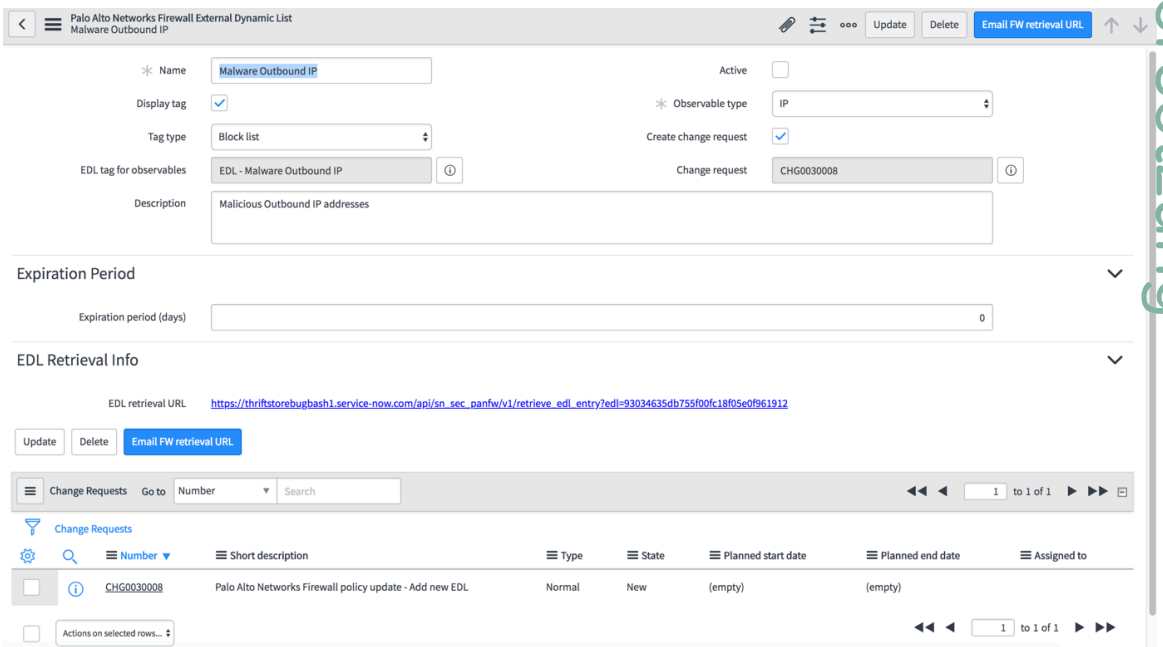
Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks NGFW-Integration** > **EDL-Konfiguration der Firewall** und wählen Sie das Modul **Firewall-EDL-Konfiguration** aus.



2. Wählen Sie in der Liste „Dynamische Listen der Palo Alto Networks-Firewall“, die angezeigt wird, in der Spalte Name Ihre neue EDL aus.

3. Beachten Sie im angezeigten Datensatz die Schaltflächen **Abruf-URL für E-Mail-Weiterleitung**, den aktiven Link EDL-Abruf-URL und, falls konfiguriert, die Change-Anforderung Now Platform® im Abschnitt Change-Anforderungen.
   Stellen Sie sicher, dass das Kontrollkästchen **Aktiv** deaktiviert ist.



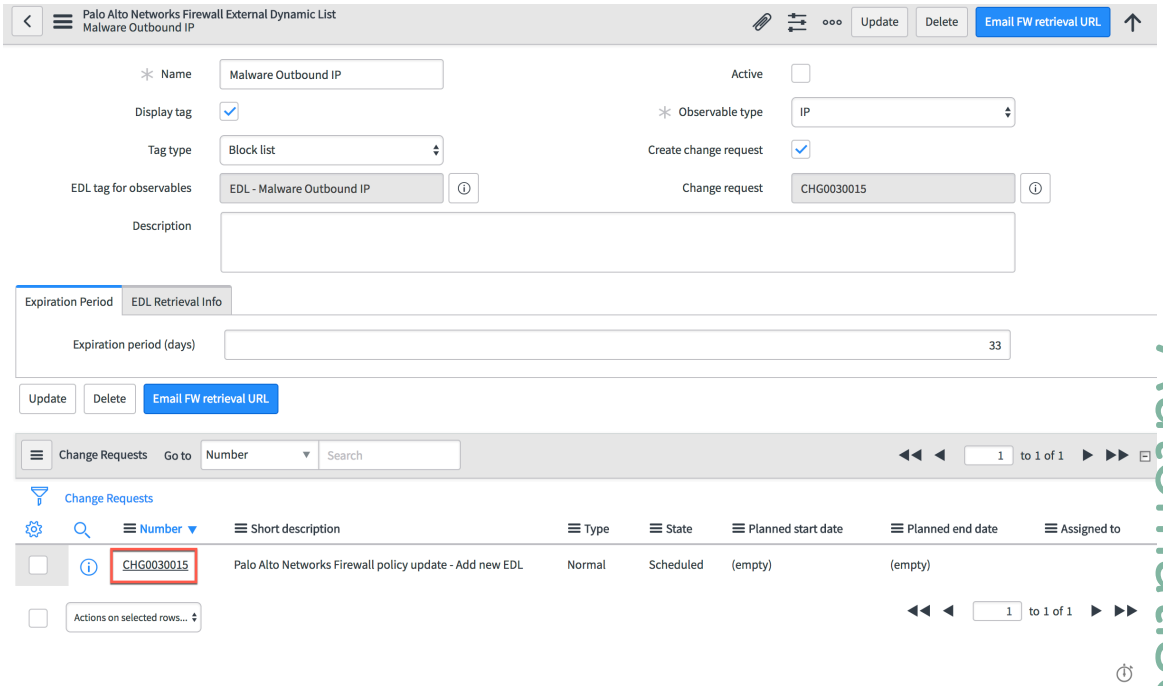
Hinweis:

Wenn Sie in Ihren Systemeinstellungen **Formulare mit Registerkarten** deaktiviert haben, wird die EDL-Abruf-URL im Abschnitt **„EDL-Abrufinformationen“** angezeigt (siehe vorherige Abbildung).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt die **EDL-Abrufinformationen,** die als Registerkarte mit **Formularen mit Registerkarten** angezeigt werden, die in Ihren Systemeinstellungen ausgewählt sind. Klicken Sie auf die Registerkarte **EDL-Abrufinformationen,** um die Abruf-URL anzuzeigen. Der Link zum Change Request (**CH0030015**) wird ebenfalls angezeigt.



4. Um die Konfiguration abzuschließen und die EDL von „inaktiv“ in „aktiv“ zu verschieben, müssen Sie eine der folgenden Optionen auswählen, um den Firewall-Administrator zu benachrichtigen, dass die Abruf-URL verfügbar ist.
   Nachdem Sie den Firewall-Administrator über die Verfügbarkeit der Abruf-URL informiert und bestätigt haben, dass die EDL in Palo Alto Networkskonfiguriert wurde, besteht Ihr nächster Schritt als Security Incident-Administrator in der Aktivierung der EDL. Sie aktivieren die EDL entweder manuell oder verwenden, falls konfiguriert, das Change-Anforderungsformular Now Platform, um die EDL zu aktivieren.

Zugehörige Informationen

Konfigurieren Sie eine EDL in Palo Alto Networks Next-Generation Firewall

Aktivieren Sie manuell eine EDL für Palo Alto Networks Next-Generation Firewall

Wenn der Palo Alto Networks-Firewalladministrator Now Platformnicht verwendet und Sie direkt benachrichtigt werden, dass Palo Alto Networks Next-Generation Firewall konfiguriert ist, können Sie die externe dynamische Liste (External Dynamic List, EDL) manuell aktivieren.

Vorbereitungen

Weisen Sie in Palo Alto Networksder von Ihnen erstellten EDL ein EDL-Objekt, eine Richtlinie und die Quell-URL zu. Weitere Informationen zum Konfigurieren der EDL für Palo Alto Networks Next-Generation Firewall in Palo Alto Networksfinden Sie unter Konfigurieren Sie eine EDL in Palo Alto Networks Next-Generation Firewall.

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

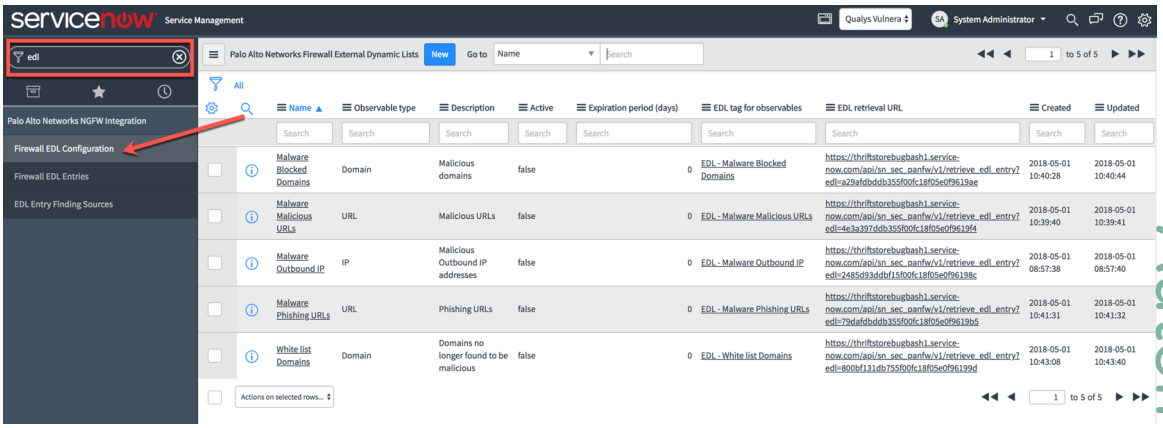
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

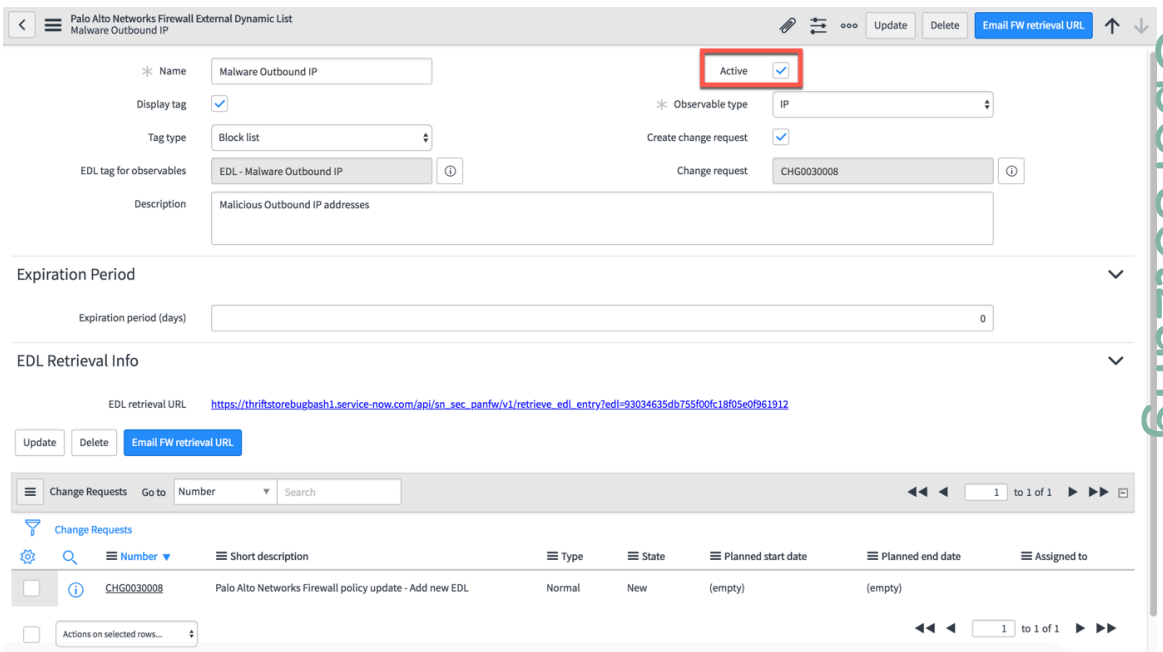
Als Security Incident-Administrator für Now Platform werden Sie vom Firewall-Administrator Palo Alto Networks benachrichtigt, wenn die EDL-Konfiguration in Palo Alto Networks Next-Generation Firewallabgeschlossen ist.

Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks NGFW-Integration** > **EDL-Konfiguration der Firewall**.



2. Wählen Sie das Modul **EDL-Firewallkonfiguration** aus.
3. Klicken Sie in der Liste „Palo Alto Networks-Firewall der externen dynamischen Listen“ in der Spalte **Name** auf ein Element, um es zu öffnen.
4. Aktivieren Sie im Datensatz, der geöffnet wird, das Kontrollkästchen **Aktiv**.

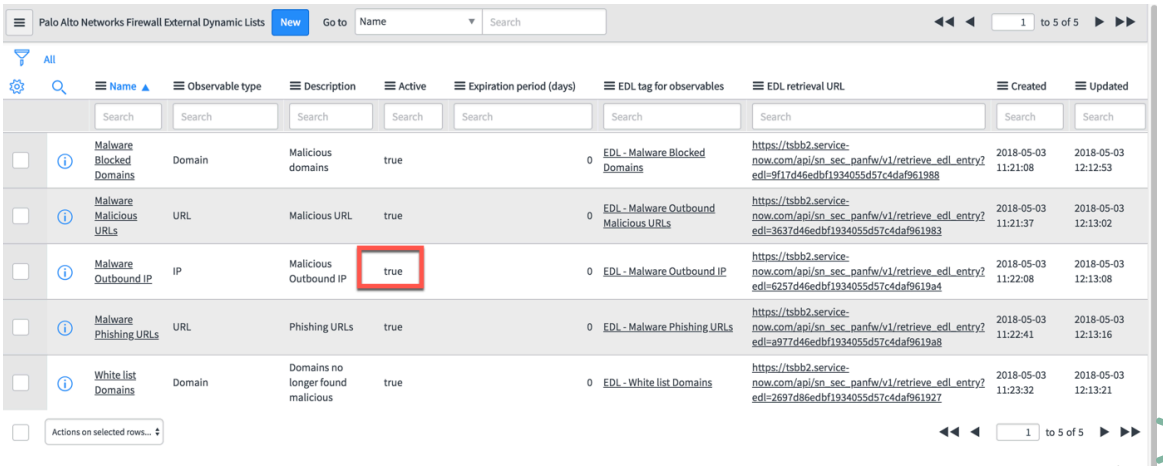


5. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Spalte **Aktiv** der Liste „Externe dynamische Palo Alto Networks-Firewall-Listen“ wird „true“ für den Status der EDL angezeigt.



Ergebnisse

Die EDL ist aktiviert und bereit zum Empfangen von EDL-Einträgen

Nächste Maßnahme

Senden Sie EDL-Einträge aus einem Security Incident oder aus der Sperrliste.

Konfigurieren Sie eine EDL in Palo Alto Networks Next-Generation Firewall

Der Firewall-Administrator Palo Alto Networks konfiguriert eine EDL für den Palo Alto Networks Next-Generation Firewall, sobald er benachrichtigt wurde, dass die Abruf-URL im Now Platformverfügbar ist. Bevor die EDL EDL-Einträge akzeptieren kann, muss sie in Palo Alto Networkskonfiguriert und in Now Platform®aktiviert werden.

Vorbereitungen

Erforderliche Rolle: Palo Alto Networks Firewall-Administrator

Warum und wann dieser Vorgang ausgeführt wird

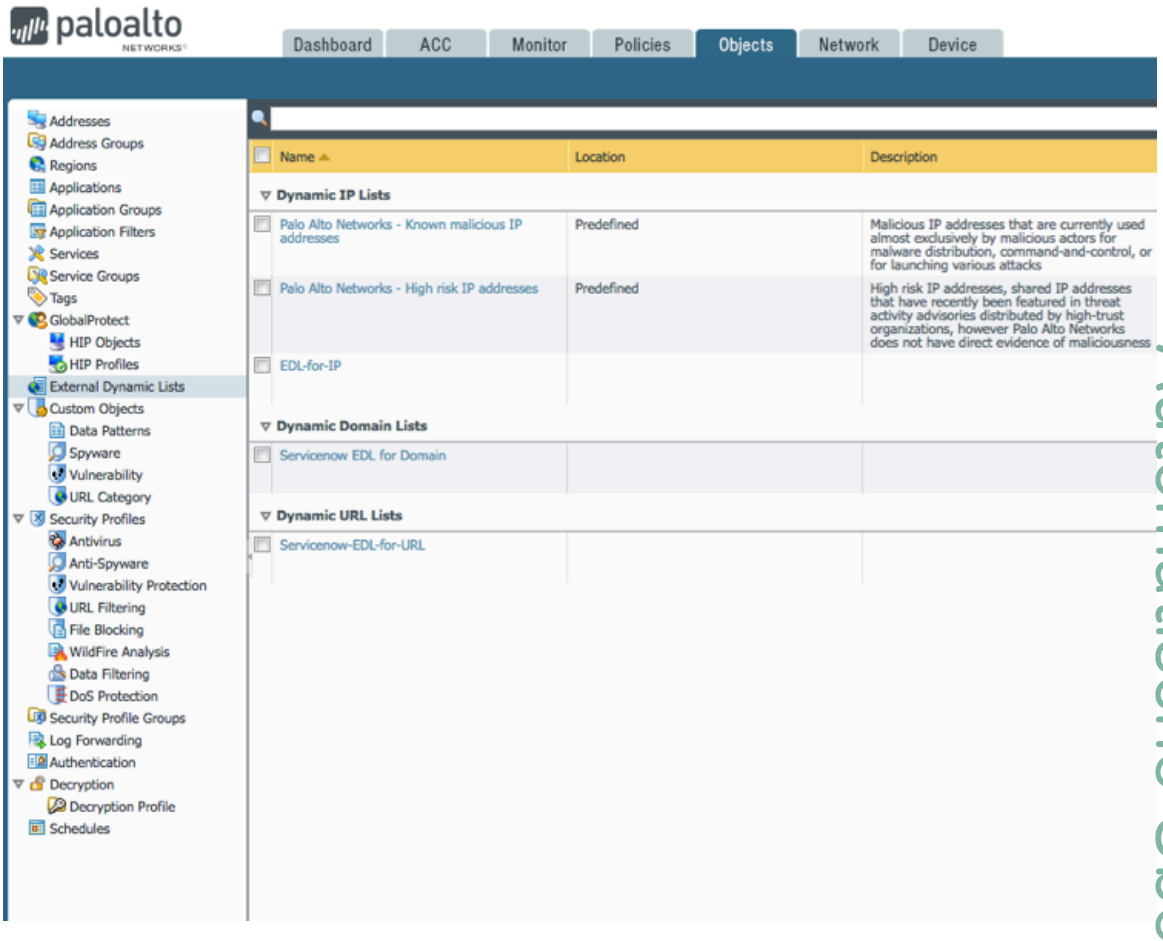
Der Palo Alto Networks Next-Generation Firewall -Administrator erstellt ein EDL-Objekt und weist der EDL die Quell-URL (Abruf-URL) und die Richtlinie zu. Diese Aufgaben werden in Palo Alto Networks ausgeführt, bevor die EDL in Now Platformaktiviert wird.

Die Bilder im folgenden Abschnitt werden mit Genehmigung verwendet und sind PRIVILEGED und PROPRITÄR.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

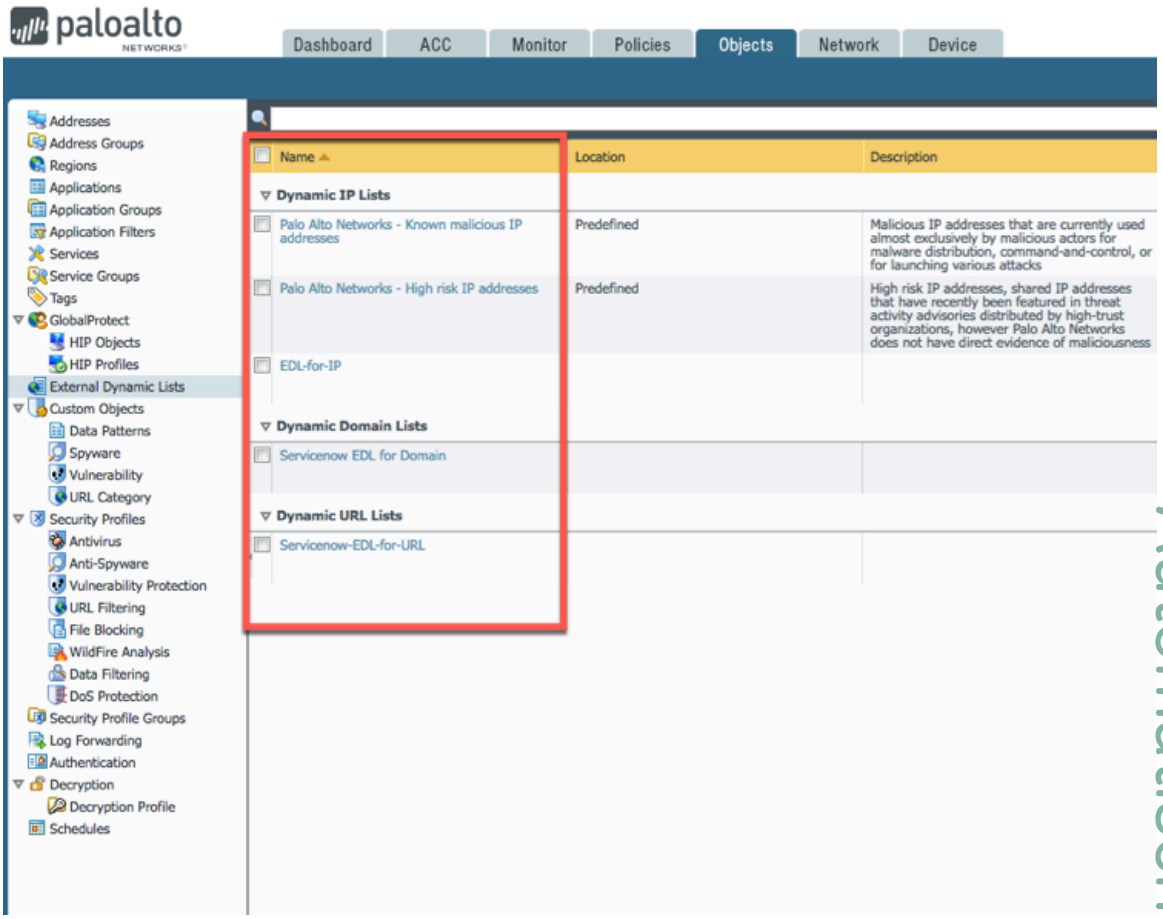
1. Wenn Sie die EDL nicht für die Firewall konfiguriert haben, navigieren Sie zu **Externe dynamische Listen** > **Objekte** in Palo Alto Networks.



2. Wählen Sie in der Spalte **Name** die ServiceNow EDL aus, die Sie konfigurieren möchten, z. B. **ServiceNow EDL für URL**.

Automatische Übersetzung

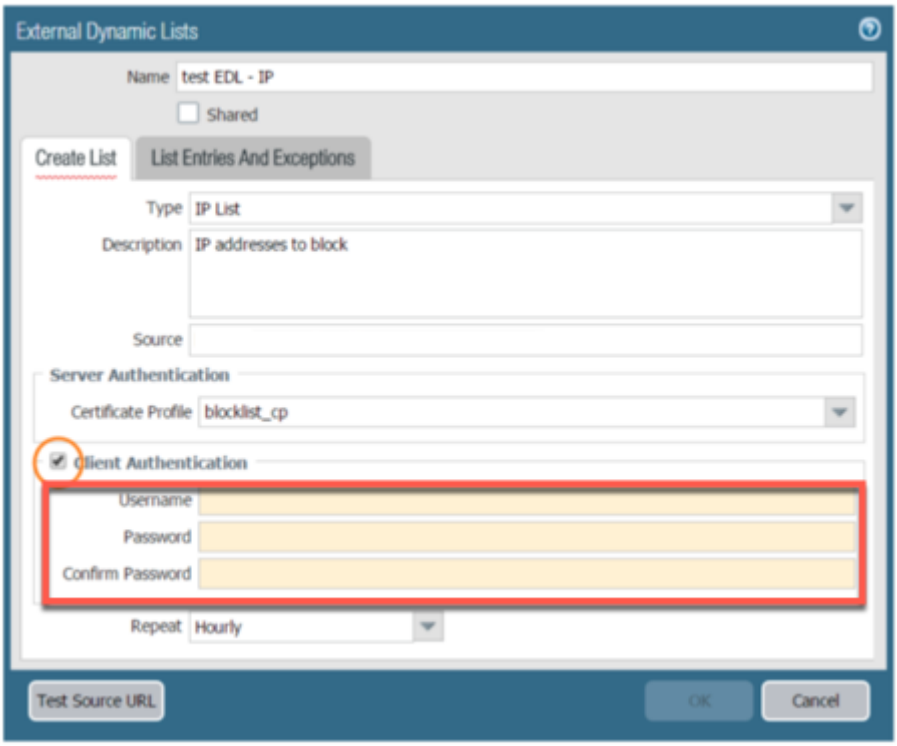
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



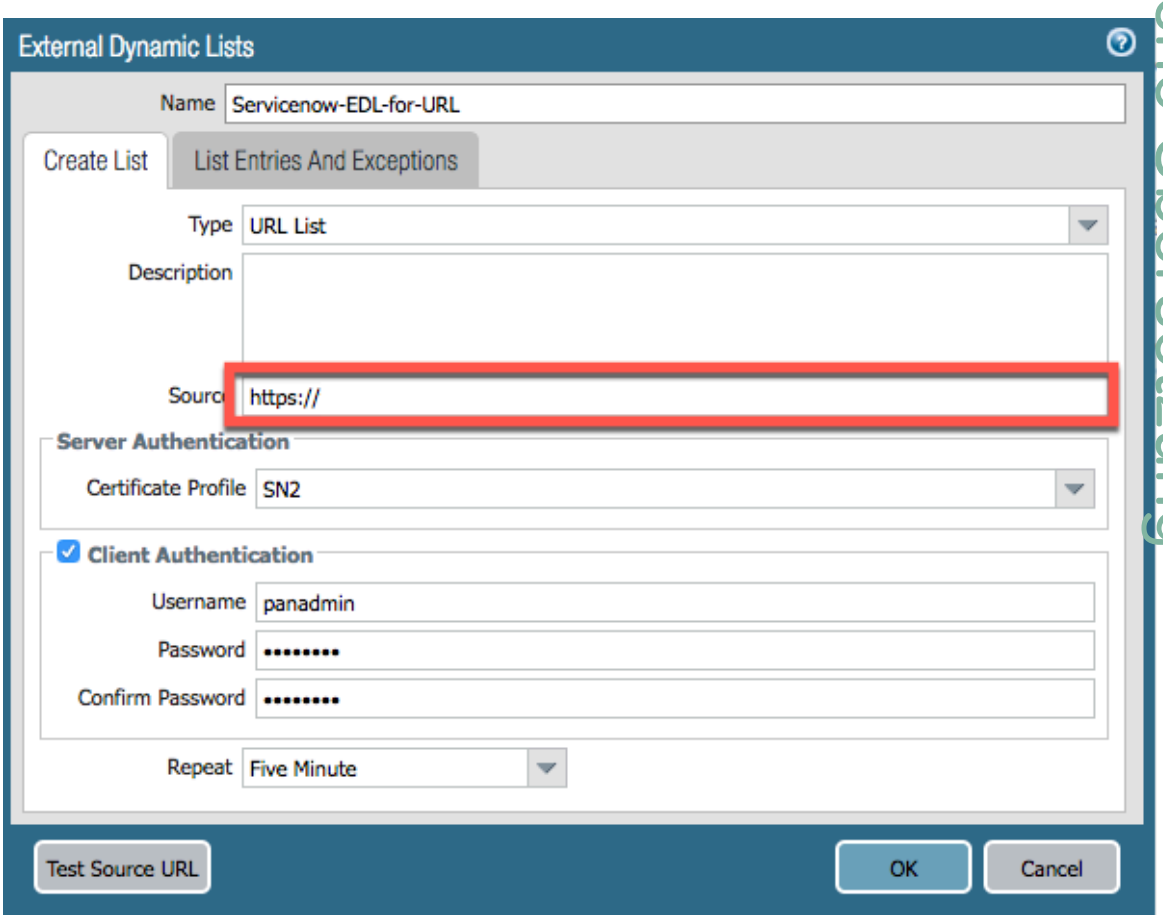
3. Geben Sie im Dialogfeld „Externe dynamische Listen“ den Anwendernamen und das Passwort ein, um sich mit Now Platform®zu authentifizieren.
Bei diesen Anmeldeinformationen handelt es sich um den Anwendernamen und das Passwort, die Sie für die API-Kontorolle (sn_sec_panfw.api_account_access) in Ihrer Instanz ServiceNow erstellt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie im Feld Quelle die URL ein, die in der EDL-Liste in Ihrer Instanz ServiceNow generiert wurde.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie in der Auswahlliste ein Zertifikatprofil aus, z. B. SN2.

6. Klicken Sie auf OK.

Aktivieren Sie eine EDL für Palo Alto Networks Next-Generation Firewall mit einer Change-Anforderung

Falls konfiguriert, wird das Change-Anforderungsformular ServiceNow zum Aktivieren der externen dynamischen Liste (External Dynamic List, EDL) verwendet. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch Now Platform für Änderungen an Firewall-Richtlinien oder -Regeln verwendet. Die EDL wird automatisch aktiviert und ist nach Abschluss der Change-Anforderung Now Platform für den Empfang von EDL-Einträgen bereit.

Vorbereitungen

Hinweis:
Die Abbildungen im folgenden Abschnitt werden mit in den Systemeinstellungen ausgewählten **Formularen mit Registerkarten** angezeigt. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt mit der Bezeichnung Formulare mit Registerkarten anzeigen in Formularlayout konfigurieren auf der Website der Produktdokumentation von ServiceNow .

Erforderliche Rolle: sn_si.admin zum Genehmigen der Change-Anforderung und der Change-Aufgaben

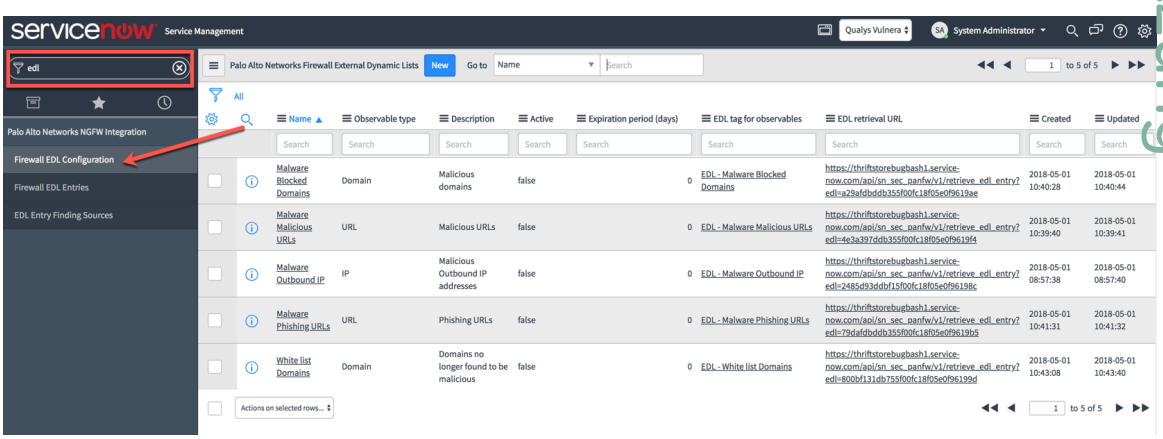
Palo Alto Networks -Firewall-Administrator für das Durchführen von Konfigurationsaufgaben in Palo Alto Networks

Warum und wann dieser Vorgang ausgeführt wird

Wenn konfiguriert, überwachen Sie Ihre Change-Anforderung Now Platform und weisen Sie alle Aufgaben zu, die zur Konfiguration von Palo Alto Networks Next-Generation Firewallerforderlich sind. Schließen Sie nach Abschluss dieser Aufgaben die Change-Anforderung Now Platform, um die EDL automatisch zu aktivieren.

Prozedur

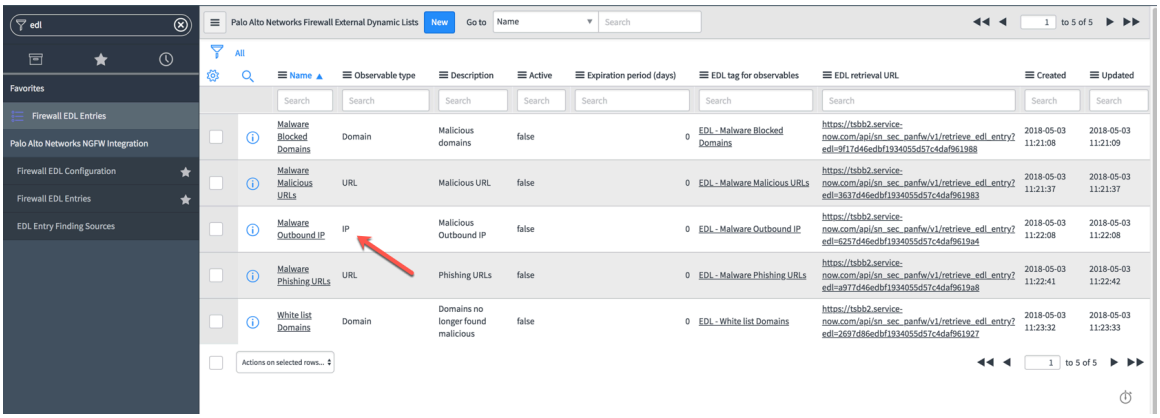
1. Navigieren zu **Alle** > **Palo Alto Networks NGFW-Integration** > **EDL-Konfiguration der Firewall**.



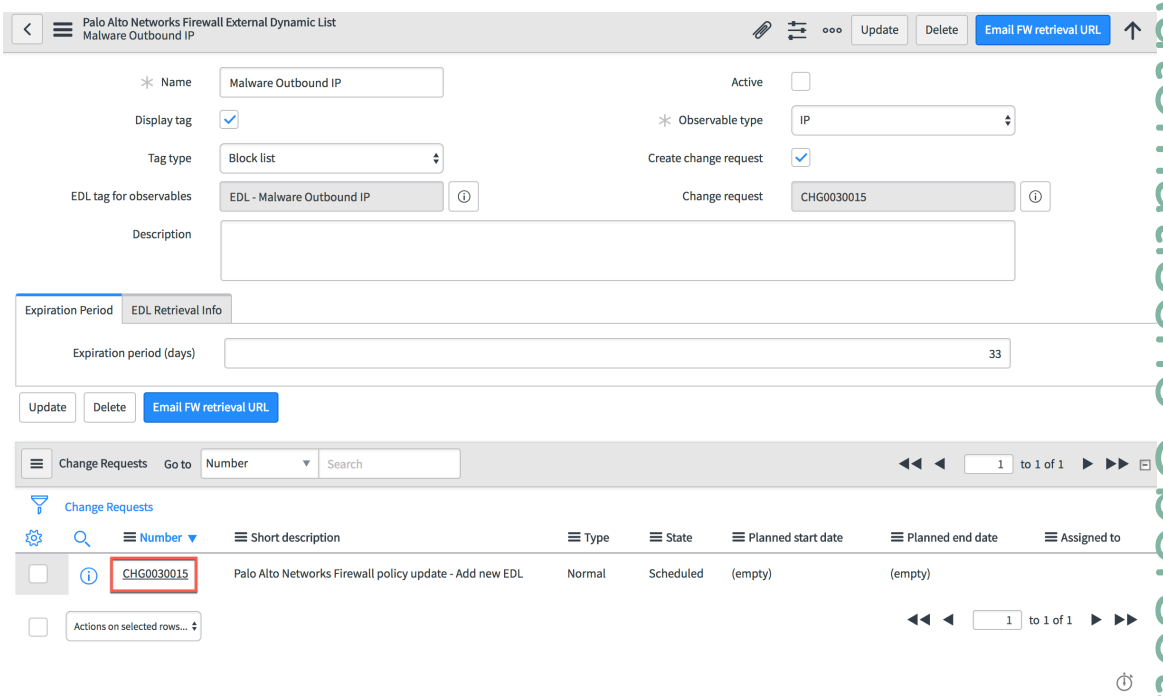
2. Wählen Sie das EDL-Modul aus, und klicken Sie in der Spalte **Name** auf eine EDL.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



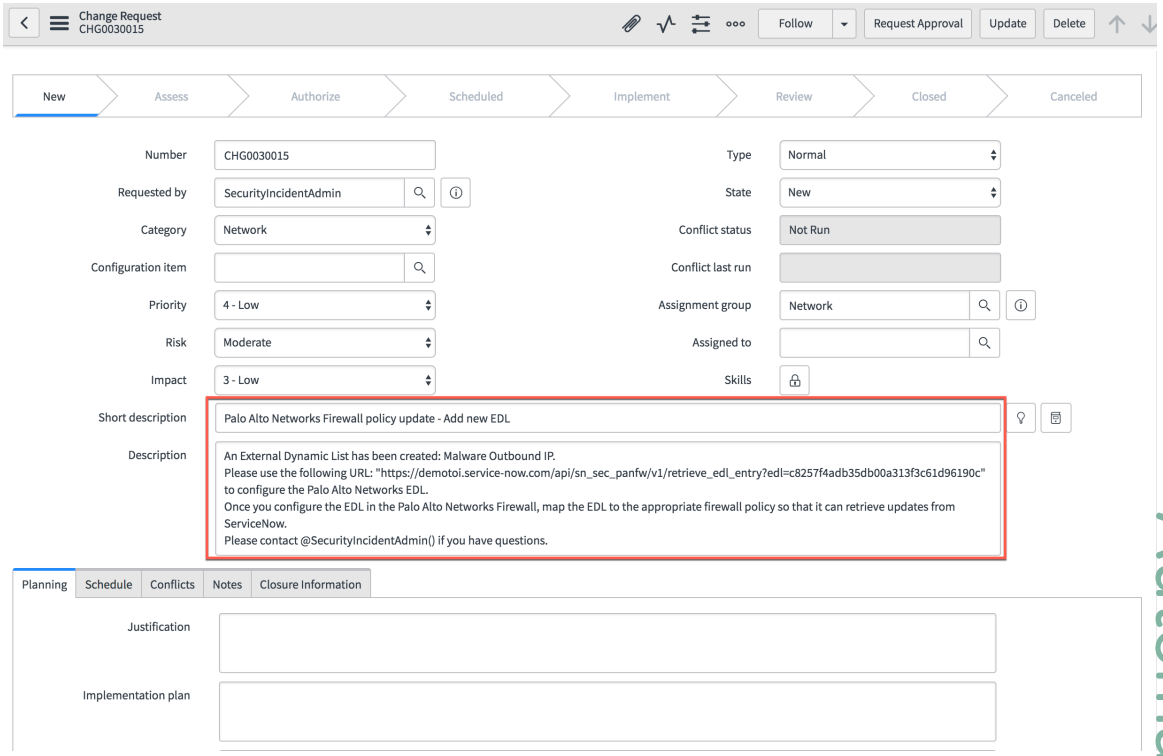
3. Klicken Sie im geöffneten EDL-Datensatz in der zugehörigen Liste Change-Anforderungen auf die Nummer der Change-Anforderung.



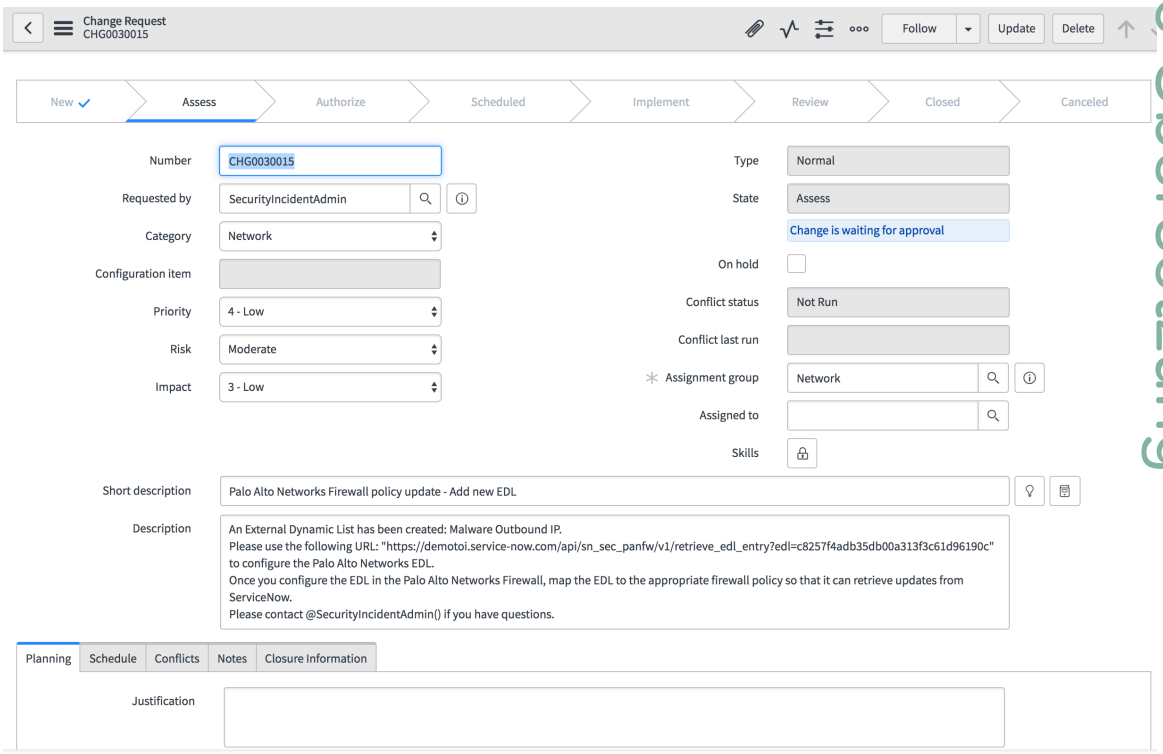
Der Datensatz für die Change-Anforderung wird angezeigt. Im Feld **Beschreibung** wird die Abruf-URL angegeben, die zum Konfigurieren der Palo Alto Networks EDL verwendet wird. Details zur Zuordnung der EDL zur entsprechenden Palo Alto Networks Next-Generation Firewall -Richtlinie sind ebenfalls enthalten. Im Feld **Kurzbeschreibung**zeigt ein Kommentar an, dass eine Anforderung zum Hinzufügen einer neuen EDL vorliegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie in der oberen rechten Ecke des Datensatzes **auf Genehmigung anfordern**.
Der Status ändert sich in Bewerten, und es wird eine Nachricht angezeigt, dass der Change Request auf Genehmigung wartet.

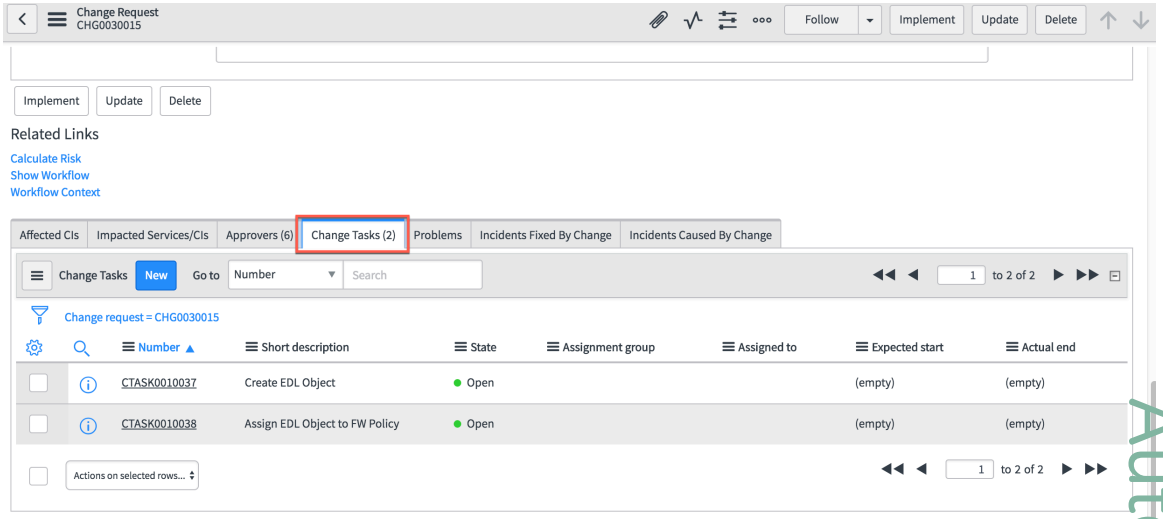


5. Um die Change-Anforderung abzuschließen und die EDL zu aktivieren, befolgen Sie die Schritte zum Zuweisen der Aufgaben und zum Schließen der Change-Anforderung.

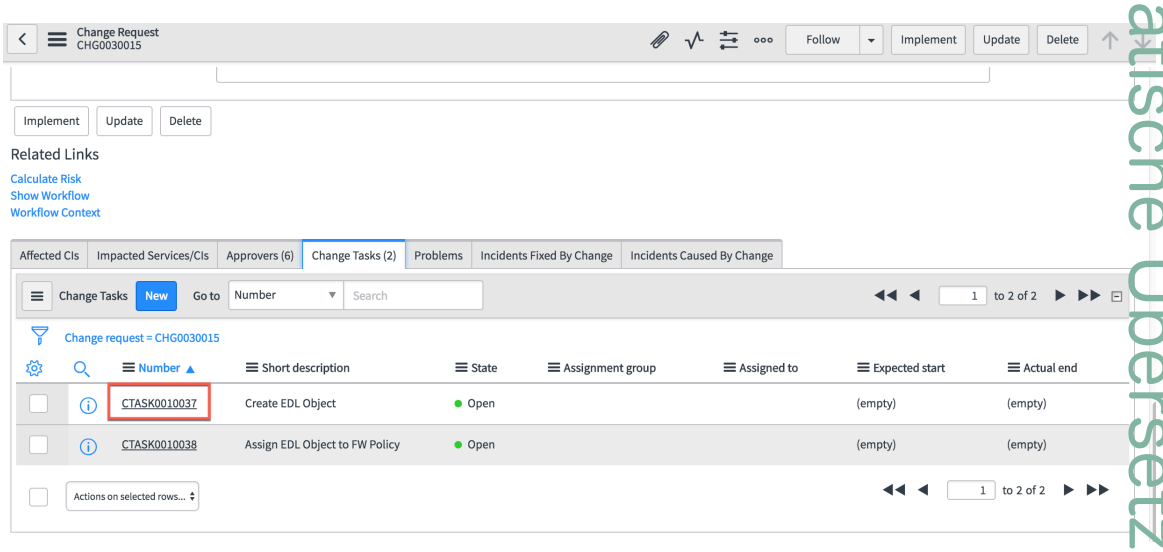
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn dies nicht angezeigt wird, öffnen Sie den Change Request, und wählen Sie die Registerkarte **Change-Aufgaben**.



b. Klicken Sie auf die Aufgabe, die der Erstellung des EDL-Objekts zugeordnet ist, um es zu öffnen.

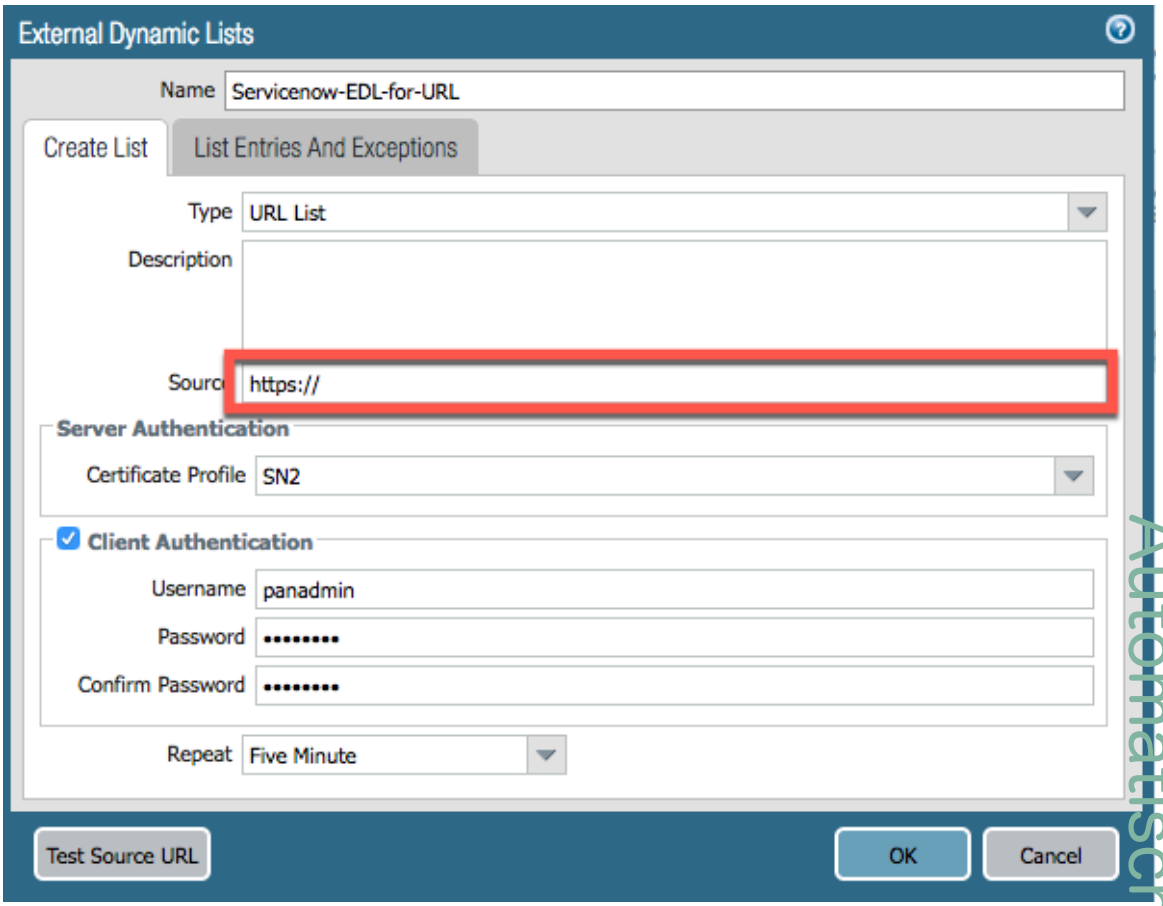


c. Weisen Sie im angezeigten Datensatz die Aufgabe dem Firewall-Administrator Palo Alto Networks zu, und klicken Sie auf **Aktualisieren**.
Der Firewall-Administrator wird benachrichtigt und erstellt das EDL-Objekt in Palo Alto Networks Next-Generation Firewall.

Um das EDL-Objekt zu erstellen, wird die Abruf-URL Now Platform in Palo Alto Networks unter kopiert **Externe dynamische Listen** > **Erstellen Sie Listen** > **Quelle**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Bild wird mit Erlaubnis verwendet und ist PRIVILEGED und PROPRITÄR.

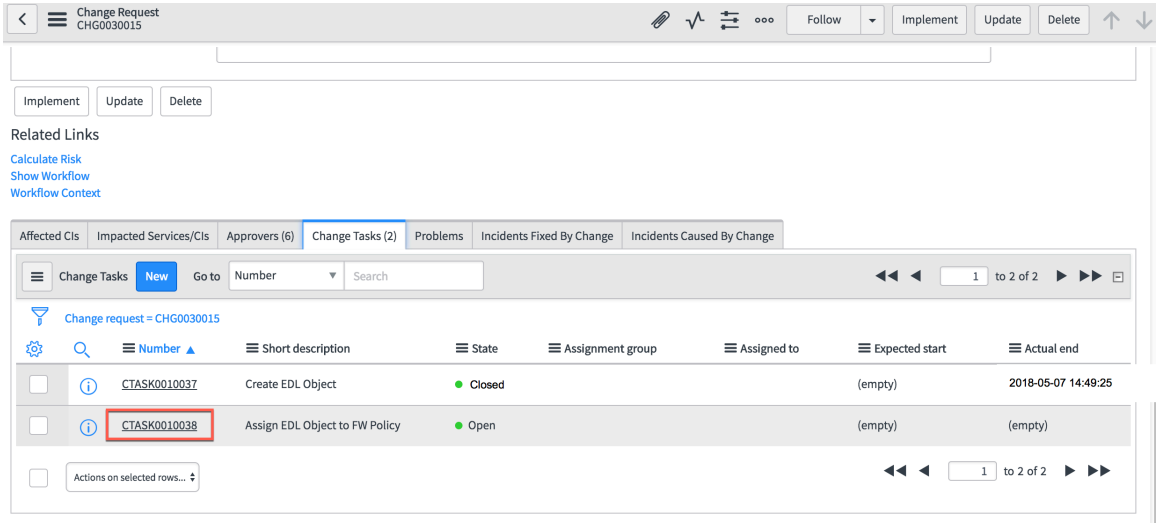
d. Nachdem Sie verifiziert haben, dass das EDL-Objekt in Palo Alto Networkserstellt wurde, navigieren Sie im Now Platformzu dem Change Request, der der Erstellung des EDL-Objekts zugeordnet ist, und klicken Sie auf **Abschlussaufgabe**.

Im Aufgabendatensatz für dieses Beispiel wurde CTASK0010037 für diese Aufgabe geschlossen.

e. Navigieren Sie zur Registerkarte Change-Aufgaben, und klicken Sie auf die Aufgabe, um dem EDL-Objekt eine Firewall-Richtlinie zuzuweisen.

Automatische Übersetzung

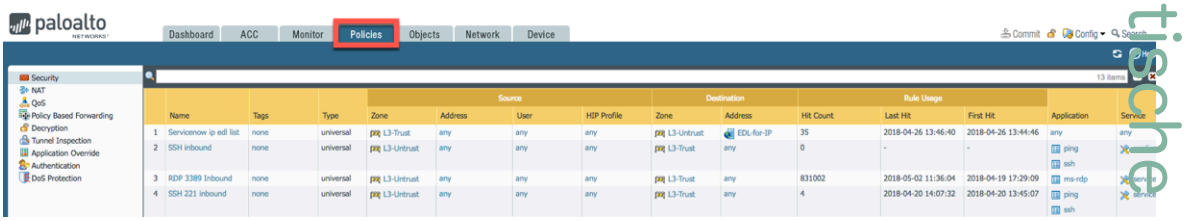
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Status für CTASK0010037 lautet „Geschlossen“.

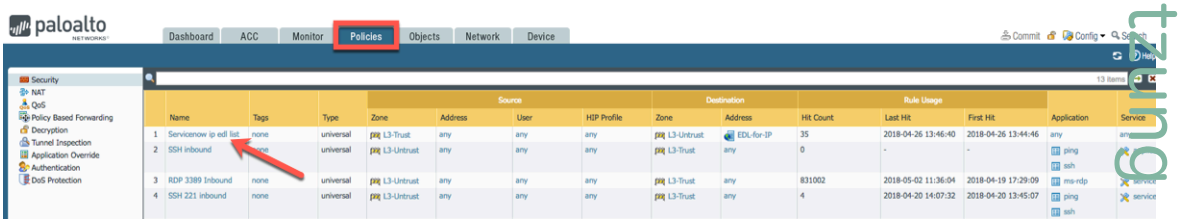
f. Öffnen Sie den Datensatz, und weisen Sie die nächste Aufgabe zu.

Nachdem die Aufgabe zugewiesen wurde, navigiert der Firewall-Administrator in Palo Alto Networkszur Registerkarte **Richtlinien**, um die Richtlinie zuzuweisen.



Das Bild wird mit Erlaubnis verwendet und ist PRIVILEGED und PROPRITÄR.

g. Suchen Sie in der Spalte **Name** nach der Sicherheitsrichtlinienregel, der Sie die EDL hinzufügen möchten, z. B. **ServiceNow IP-EDL-Liste**.



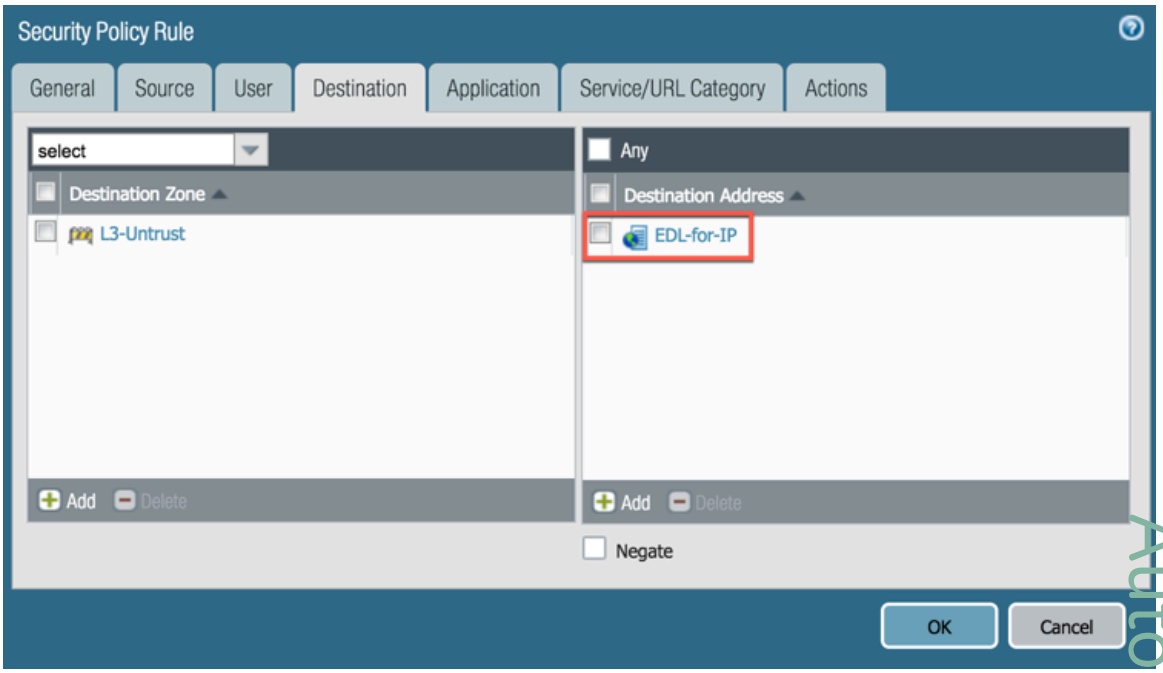
Das Bild wird mit Erlaubnis verwendet und ist PRIVILEGED und PROPRITÄR.

h. Wählen Sie im Dialogfeld „Sicherheitsrichtlinienregel“ die Registerkarte **Ziel** aus, um im Feld **Zieladresse** eine EDL hinzuzufügen.

i. Um alle verfügbaren EDLs anzuzeigen, klicken Sie auf das Symbol **Hinzufügen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Bild wird mit Erlaubnis verwendet und ist PRIVILEGED und PROPRITÄR.

j. Klicken Sie auf **OK**.

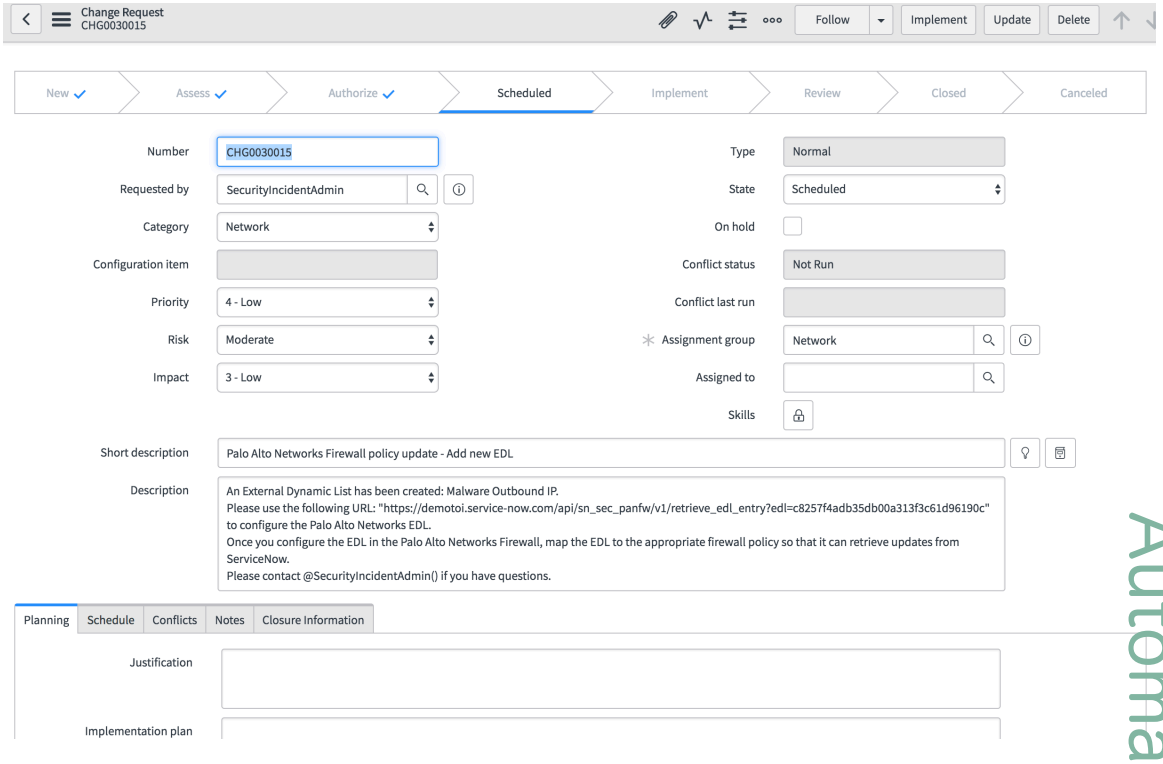
k. Nachdem Sie verifiziert haben, dass das EDL-Objekt einer Sicherheitsrichtlinie zugewiesen wurde, navigieren Sie im Now Platformzu der Change-Anforderung, öffnen Sie die Aufgabe, die der Zuweisung des EDL-Objekts zugeordnet ist, und klicken Sie auf **Abschlussaufgabe**.
Nachdem beide Aufgaben geschlossen wurden, ist die Change-Anforderung zur Genehmigung bereit.

l. Klicken Sie im Datensatz „Change-Anforderung“ auf die zugehörige Liste **Genehmiger**, und wählen Sie ein Element in der Spalte **Status** aus, um die Anforderung zu öffnen, die zum Erstellen der EDL verwendet wird.

m. Klicken Sie im Formular zum Öffnen der Genehmigungsanforderung **auf Genehmigen**.
Der Status des Change Request wird in Geplant geändert.

Automatische Übersetzung

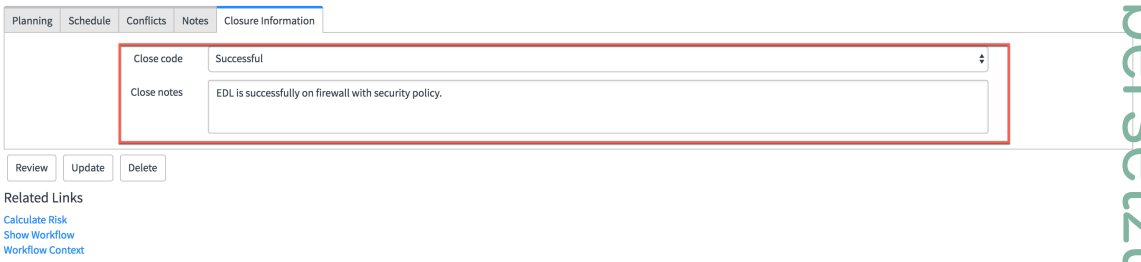
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



n. Klicken Sie auf **Implementieren**.

o. Klicken Sie auf die zugehörige Registerkarte **Abschlussinformationen**, und geben Sie Notizen ein, um die Anforderung zu schließen.

Ein Eintrag in diesem Feld ist erforderlich, um die Change-Anforderung zu schließen.

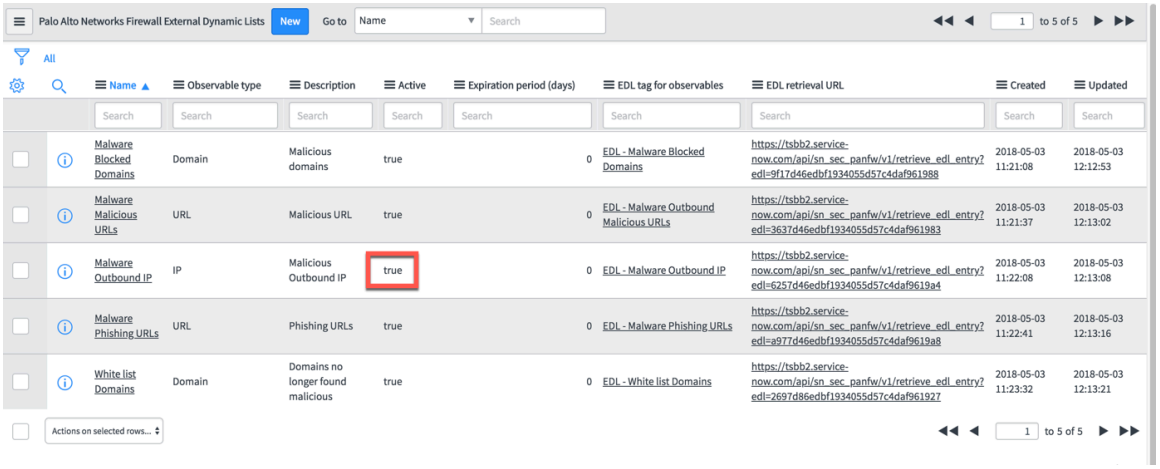


Nachdem die Change-Anforderung geschlossen wurde, wird die EDL automatisch aktiviert. Wenn Sie nicht verifiziert haben, dass die EDL aktiviert ist, navigieren Sie zu **Palo Alto Networks NGFW-Integration** > **EDL-Konfiguration der Firewall**.

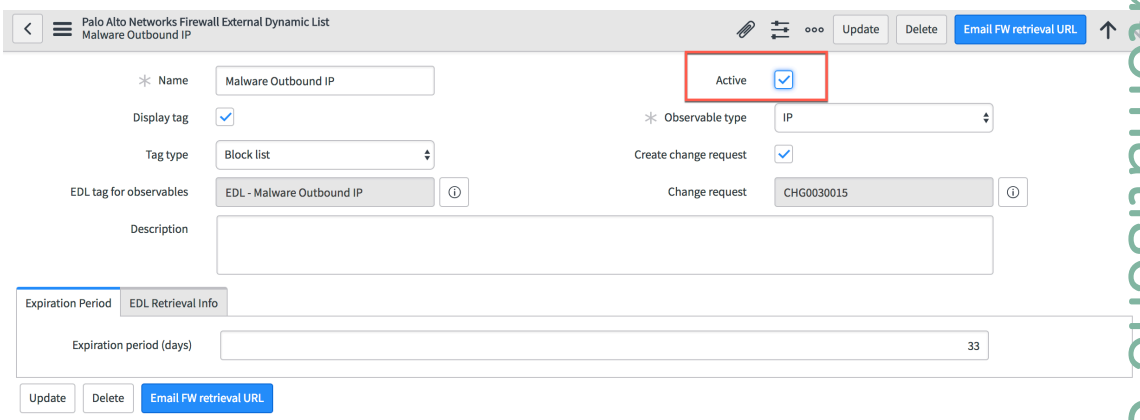
Beachten Sie, dass in der Spalte „Aktiv“ der Liste der Status für die EDL (true) lautet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie in der Spalte Name auf den EDL-Namen, und beachten Sie, dass im geöffneten Datensatz auch das Kontrollkästchen **Aktiv** aktiviert ist.



Die EDL ist jetzt bereit, EDL-Einträge zu akzeptieren.

Nächste Maßnahme

Senden Sie EDL-Einträge aus einem Security Incident oder aus der Sperrliste.

Senden Sie EDL-Einträge aus einem Security Incident-Datensatz für Palo Alto Networks Next-Generation Firewall

Erkennbare Elemente, die an einen Security Incident-Datensatz angehängt sind, werden als EDL-Einträge (External Dynamic List) zur Genehmigung an EDLs übermittelt. Ein Genehmigungsprozess für EDL-Einträge ist Teil des vorkonfigurierten Workflows. Die Firewall importiert EDL-Einträge (IP-Adressen, URLs, Domänen), die in EDL-Listen enthalten sind, und erzwingt Richtlinien.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst zum Senden von EDL-Einträgen. So genehmigen Sie EDL-Einträge: Die Genehmigung ist standardmäßig „sn_si.admin“ zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation zugewiesen werden.

Warum und wann dieser Vorgang ausgeführt wird

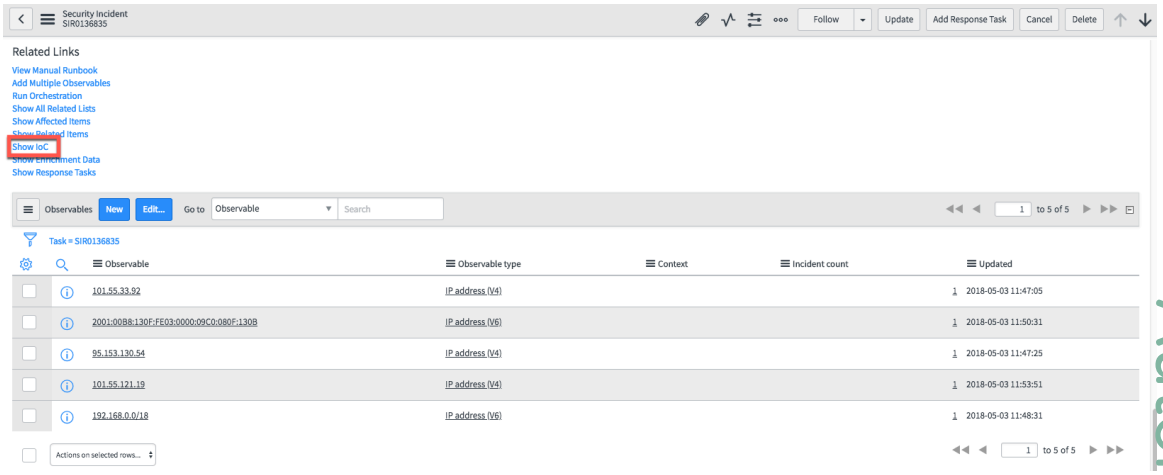
Benutzer mit der Rolle sn_si.analyst übermitteln EDL-Einträge, indem sie einen Block für erkennbare Elemente anfordern, die an einen Security Incident-Datensatz angehängt sind. Nach der Übermittlung wird ein EDL-Eintrag mit dem Status Ausstehend generiert und zur Genehmigung gesendet. Das folgende Beispiel zeigt eine Blockierungsanforderung für ein erkennbares URL-Element.

Automatische Übersetzung

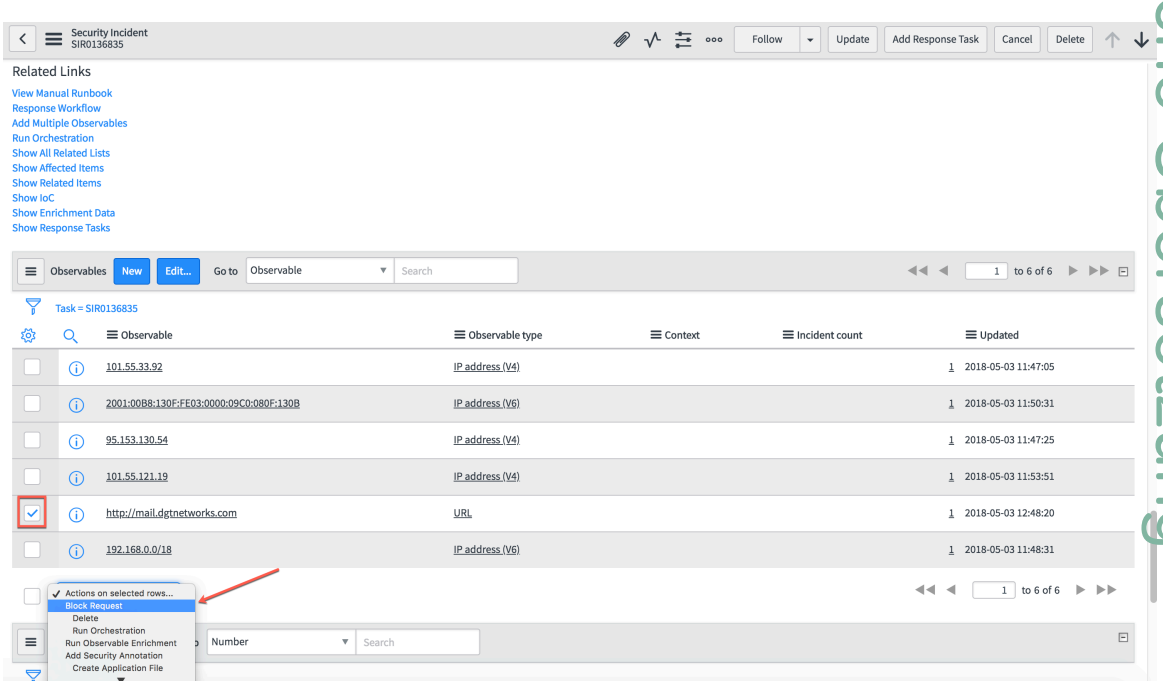
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**, und klicken Sie auf einen Security Incident-Datensatz, um ihn zu öffnen.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.



3. Wählen Sie in der zugehörigen Liste „Erkennbare Elemente“ die erkennbaren Elemente aus, die Sie blockieren möchten, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die **Option Anforderung blockieren**aus.

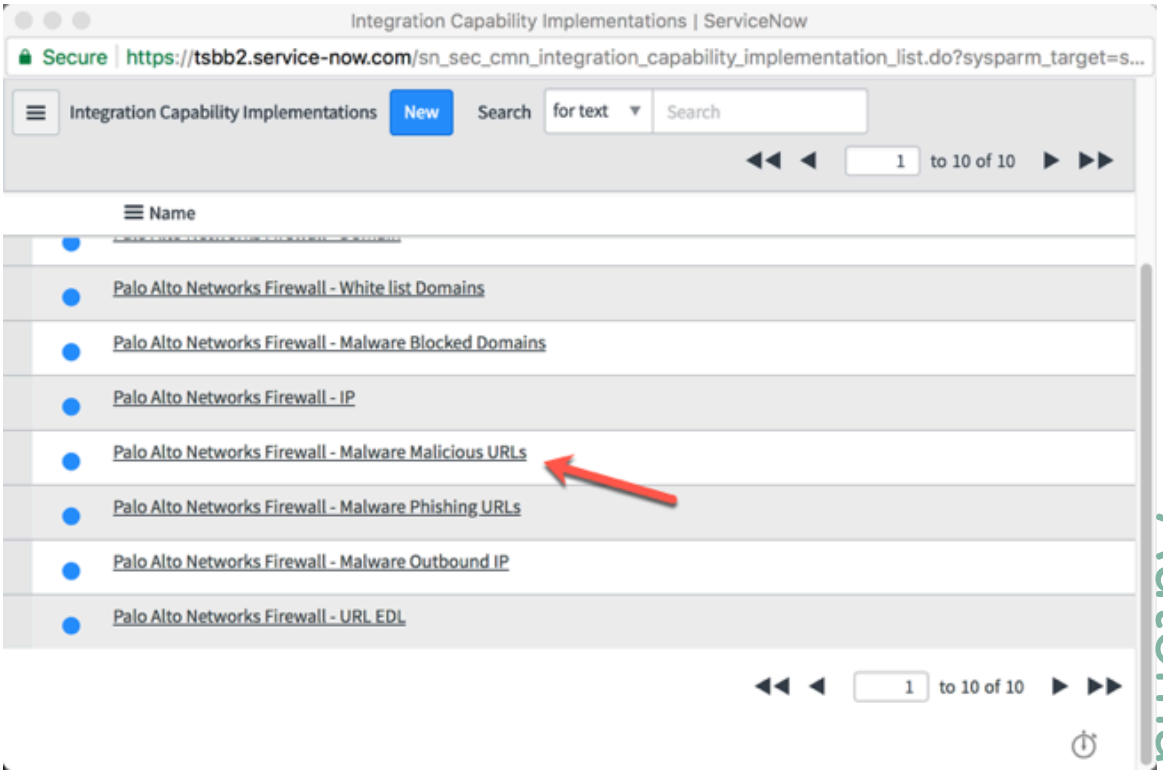


4. Klicken Sie im angezeigten Dialogfeld auf das Suchsymbol ( ).
5. Wählen Sie in der angezeigten Liste die EDL aus, an die Sie diesen Eintrag anhängen möchten.

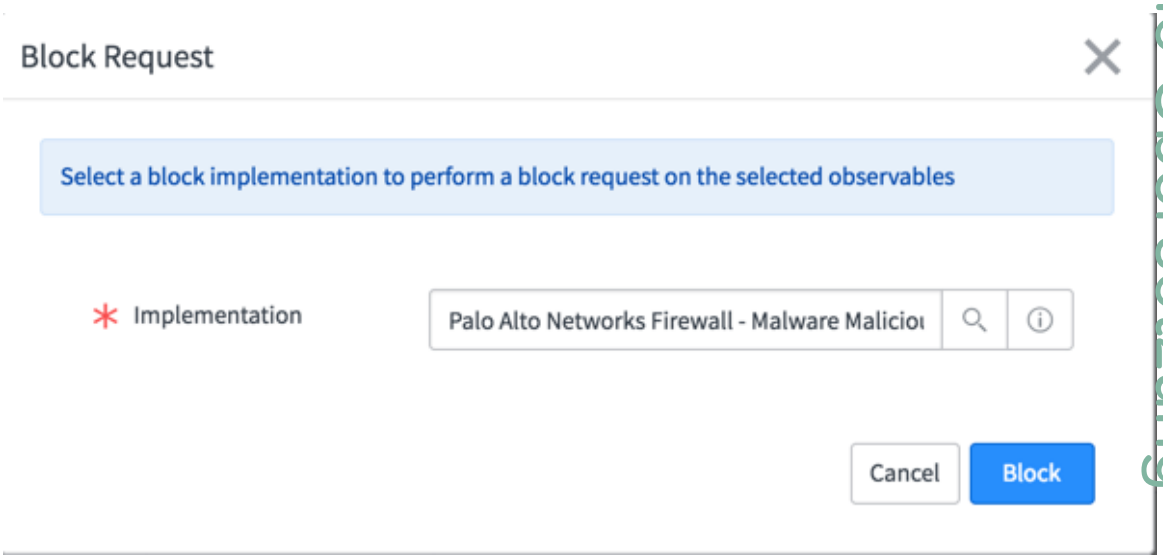
Hinweis:
In diesem Beispiel muss der erkennbare Elementtyp (URL) des Eintrags mit dem erkennbaren Elementtyp (URL) der EDL übereinstimmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



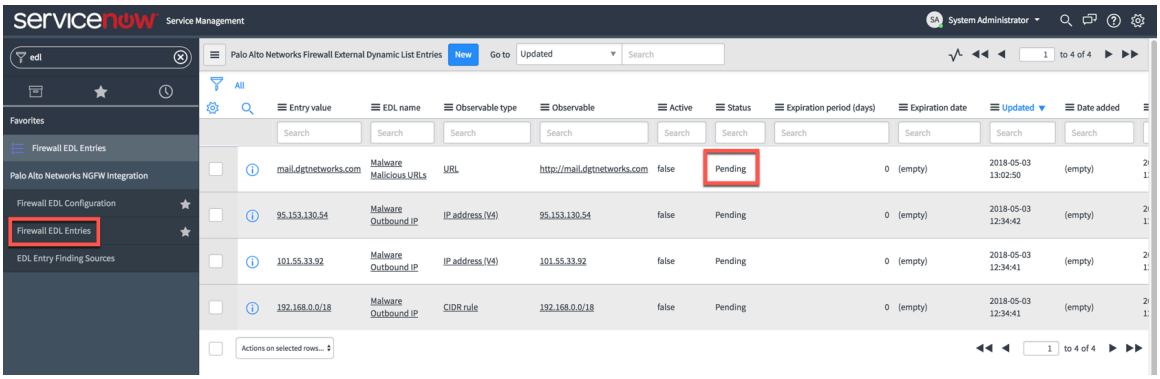
6. Klicken Sie im Dialogfeld „Sperranforderung“ mit dem EDL-Namen im Feld **Implementierung** auf **Sperren**.



7. Navigieren zu **Palo Alto Networks NGFW-Integration** > **Firewall-EDL-Einträge** und klicken Sie auf **Firewall-EDL-Einträge**.

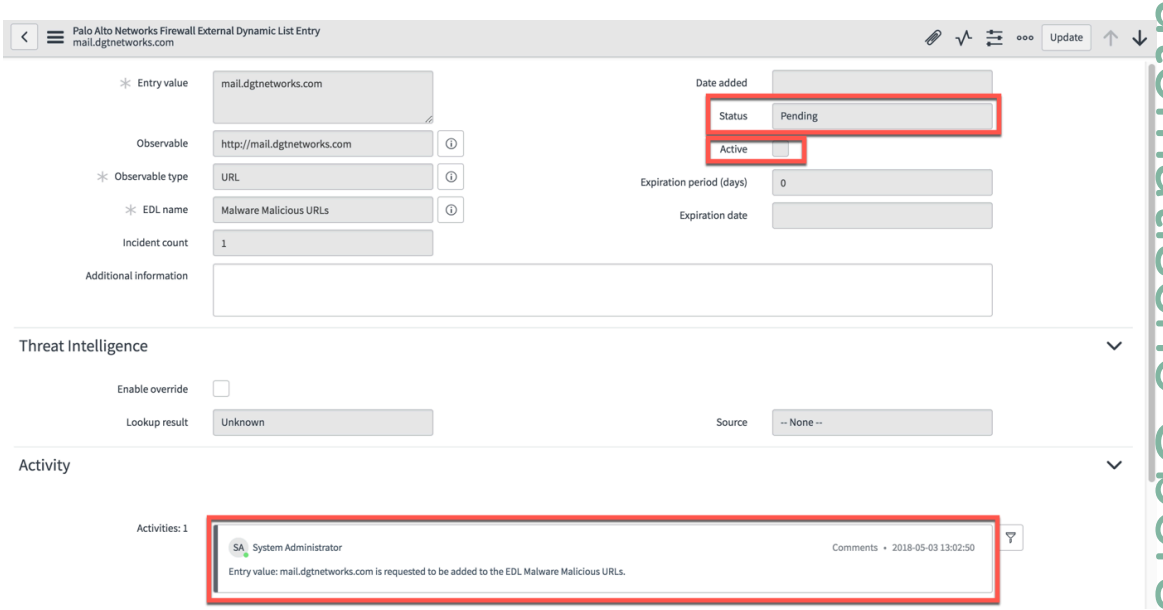
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Klicken Sie in der Liste „Palo Alto Networks-Firewall der externen dynamischen Listeneinträge“ in der Spalte **„Eintragswert“** auf das erkennbare Element, um den Datensatz zu öffnen.

In diesem Beispiel wird der Datensatz für **„mail.dgtnetworks.com“** angezeigt.

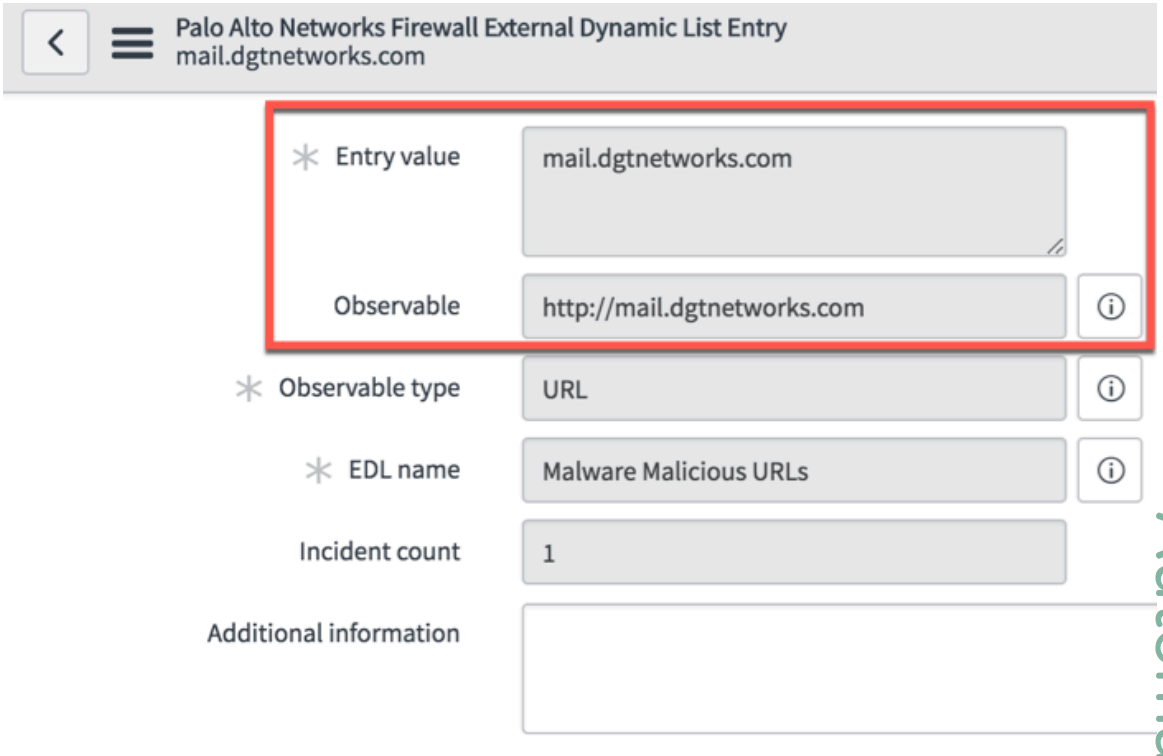


Der Status lautet Ausstehend, das Kontrollkästchen Aktiv ist deaktiviert, und in den Arbeitsnotizen wird angezeigt, dass eine Anforderung zum Hinzufügen des erkennbaren Elements vorhanden ist. Diese EDL-Eintragsanforderung ist zur Genehmigung bereit.

Die Felder Eintragswert und Erkennbares Element zeigen verschiedene Formate für das erkennbare URL-Element an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Symbol neben dem Feld Erkennbares Element ist ein Link zur Tabelle Now Platform® Erkennbares Element.

Der Wert im Feld „Erkennbares Element “ (http://mail.dgtnetworks.com) ist mit der Tabelle „Erkennbares Element“ verknüpft und stimmt mit dem Format überein, das aus dem Incident-auslösenden Ereignis Security Incident Response übernommen wurde.

Now Platform® kann EDL-Einträge automatisch so ändern, dass sie mit dem EDL-URL-Format von Palo Alto Networks kompatibel sind.

In diesem Beispiel wurde das erkennbare Element mit dem Protokoll http:// (http://mail.dgtnetworks.com) erstellt, und dieses Format wird im Feld Erkennbares Element angezeigt. Das Protokoll „http://“ wird von Now Platform® automatisch aus dem erkennbaren Element entfernt, sodass es mit Palo Alto Networks kompatibel ist und abgerufen werden kann. Daher wird „mail.dgtnetworks.com“ im Feld Eintragswert angezeigt.

Nächste Maßnahme
Genehmigen Sie EDL-Einträge.

Zugehörige Informationen

EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

Senden Sie EDL-Einträge aus der Sperrliste für Palo Alto Networks Next-Generation Firewall

Für erkennbare Elemente, die als schädlich eingestuft wurden und keinem bestimmten Security Incident Now Platform zugeordnet sind, übermitteln Sie EDL-Einträge (External Dynamic List) aus der Sperrliste.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

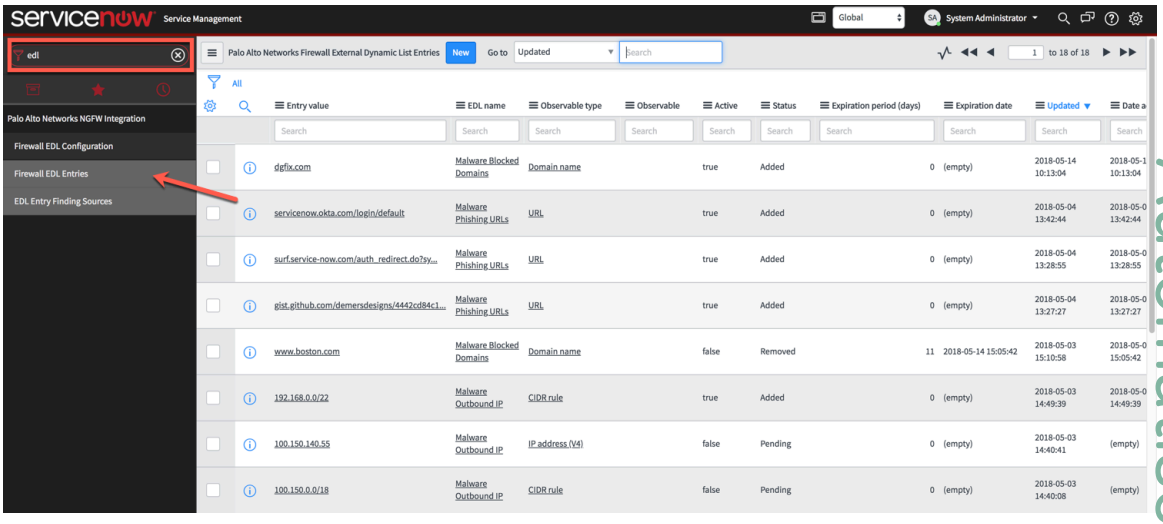
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein erkennbares Element blockieren möchten, von dem Sie festgestellt haben, dass es schädlich ist, oder zulassen möchten, dass ein erkennbares Element von Ihrer Meinung nach nicht schädlich ist und keinem bestimmten Now Platform Security Incident-Datensatz zugeordnet ist, übermitteln Sie EDL-Einträge direkt aus der Sperrliste. Beispiele für diese Art von EDL-Einträgen können URLs oder Domänen für bestimmte Sites sein.

Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks NGFW-Integration** > **Firewall-EDL-Einträge**.



2. Klicken Sie auf das Modul **Firewall-EDL-Einträge**.
3. Klicken Sie in der Liste Palo Alto Networks-Firewall der externen dynamischen Listeneinträge auf **Neu**.
4. Geben Sie im neuen Datensatz, der angezeigt wird, im Feld **Eingabewert** einen Wert für Ihr erkennbares Element ein.
   Die zwei möglichen Ergebnisse dieses Eintrags:

   Die übrigen Felder des Formulars werden automatisch ausgefüllt.

   Es wird ein übereinstimmendes erkennbares Element gefunden, und es wird eine Meldung angezeigt, dass ein übereinstimmendes erkennbares Element vorhanden ist. Wählen Sie die EDL aus, an die Sie diesen Eintrag anhängen möchten, und klicken Sie auf **Absenden**. Wählen Sie die EDL aus, an die Sie diesen Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.

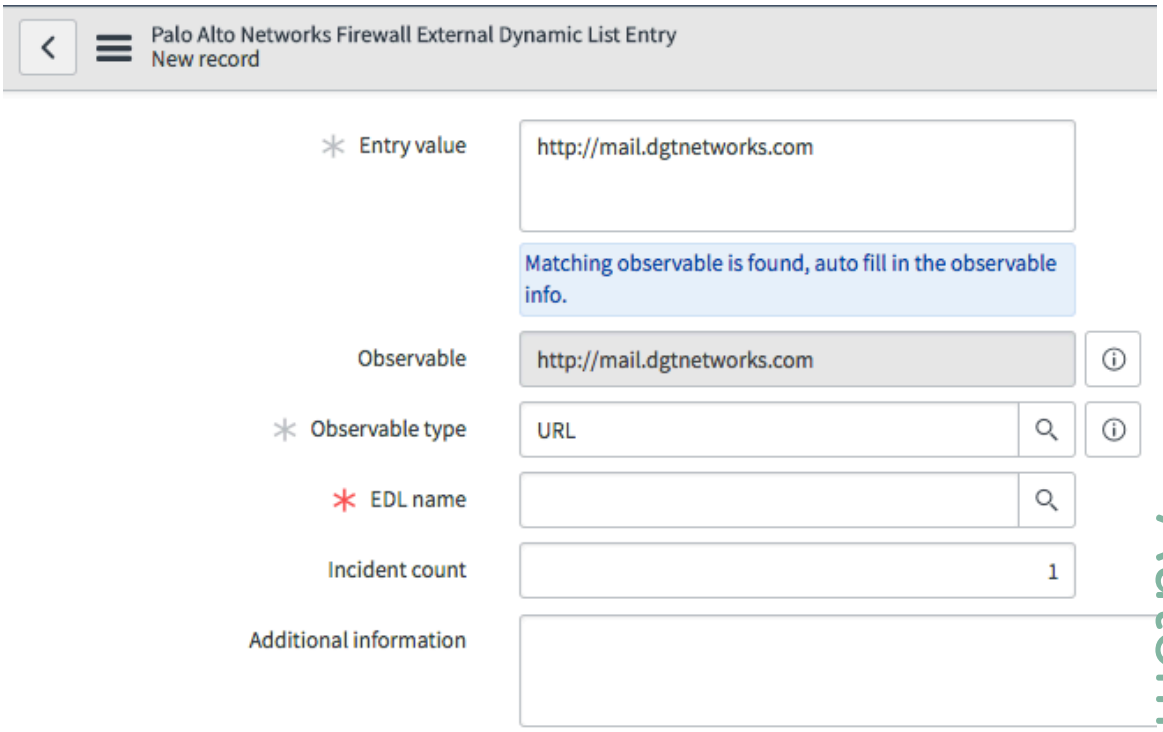
   Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, das Formular auszufüllen.

   Es wurde kein passendes erkennbares Element gefunden, und Sie müssen das Formular ausfüllen. Nachdem Sie den Vorgang abgeschlossen haben, wählen Sie die EDL aus, an die Sie das erkennbare Element anhängen möchten, und klicken Sie auf **Absenden**. Ein Datensatz eines erkennbaren Elements wird erstellt.

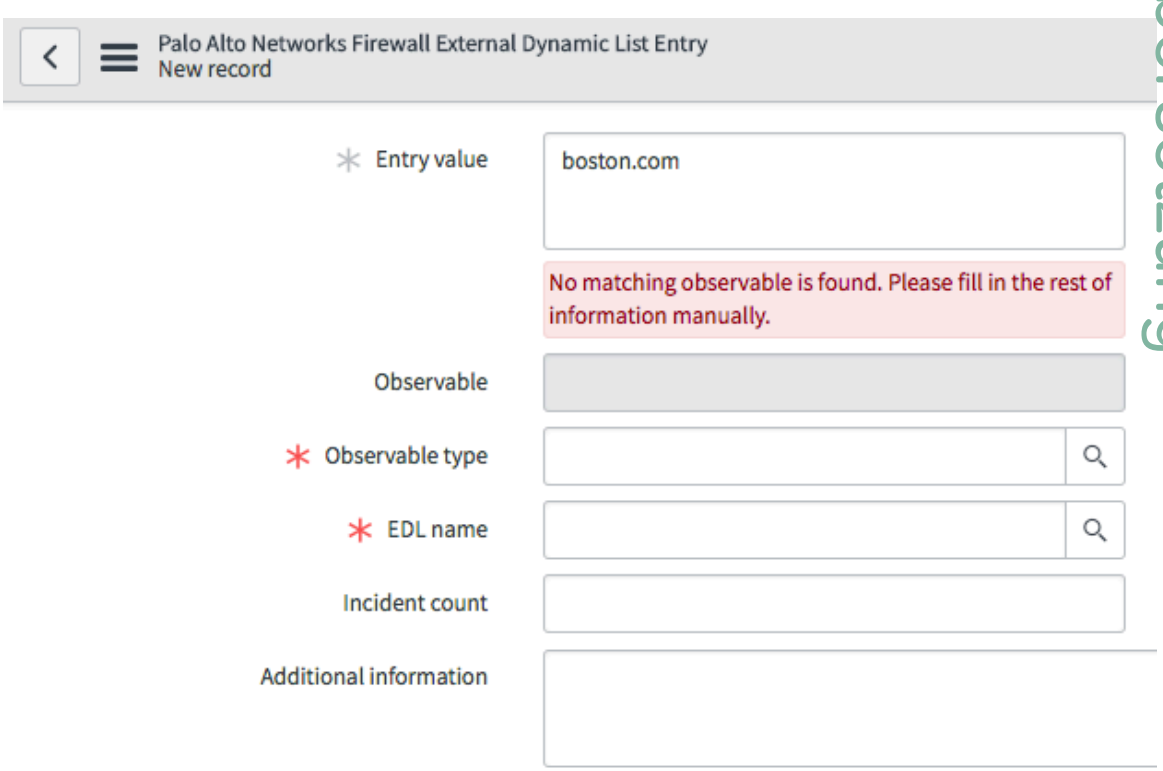
Die folgende Abbildung zeigt ein Beispiel für ein vorhandenes erkennbares Domänenelement und wie die Felder automatisch ausgefüllt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



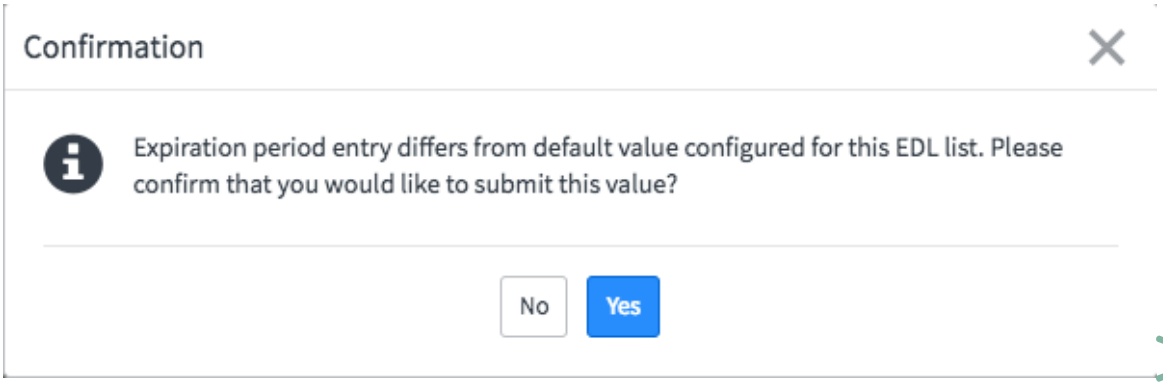
5. Klicken Sie auf das Suchsymbol, um die EDL auszuwählen, an die Sie den Eintrag anhängen möchten.
6. Klicken Sie auf **Absenden**.
   Wenn Sie die E-Mail-Genehmigung in Ihrem Workflow konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
7. Wenn eine Meldung angezeigt wird, in der Sie aufgefordert werden, die restlichen Informationen manuell einzugeben, füllen Sie die Felder aus.



Automatische Übersetzung

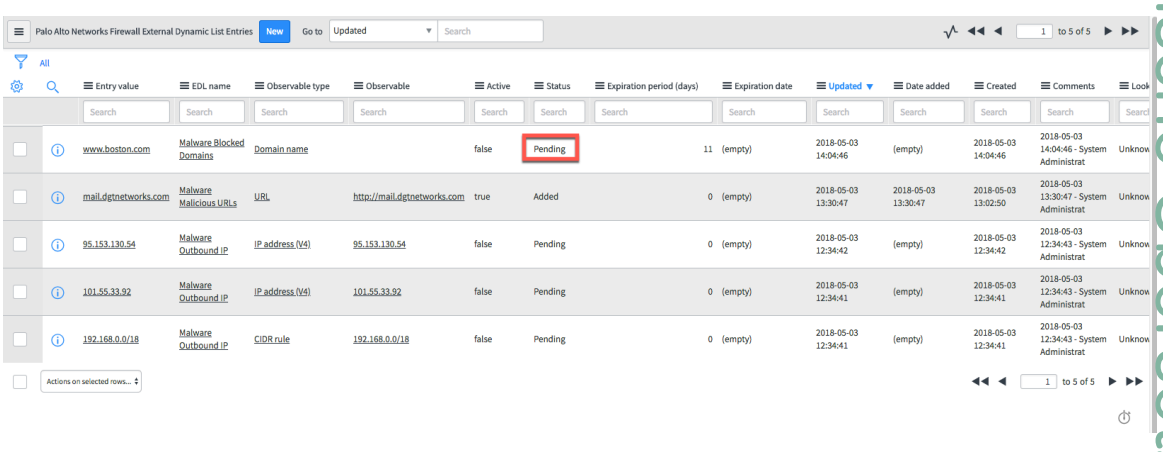
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Absenden**.
   Wenn Sie den standardmäßigen Ablaufzeitraum des EDL-Eintrags geändert haben, wird ein Bestätigungsdialogfeld mit einer Warnung angezeigt, das Sie darauf hinweist, dass sich der Zeitraum von der ausgewählten EDL unterscheidet.



9. Wählen Sie eine Option aus, um den Ablaufzeitraum zu konfigurieren.

10. Falls nicht angezeigt, navigieren Sie zur Liste **der externen dynamischen Listeneinträge für Palo Alto Networks-Firewall,** und beachten Sie, dass der Status für den Eintrag Ausstehend lautet.



Der Eintrag ist jetzt zur Genehmigung bereit.

Nächste Maßnahme
Genehmigen Sie EDL-Einträge.

Zugehörige Informationen

EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

Genehmigen Sie EDL-Einträge für Palo Alto Networks Next-Generation Firewall

Ein Genehmigungsprozess für EDL-Einträge (External Dynamic List) ist Teil des vorkonfigurierten Workflows. Sie genehmigen EDL-Einträge, bevor die Einträge auf EDLs aktiviert werden. Sobald Sie den EDL-Eintrag genehmigen, ruft die Firewall den Eintrag ab, und Ihr erkennbares Element wird ab diesem Zeitpunkt blockiert.

Vorbereitungen
Erforderliche Rolle: Die Genehmigung für EDL-Einträge ist standardmäßig „sn_si.admin“ zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugewiesen werden. Im folgenden Beispiel verfügt der -Administrator Now Platform über die Genehmigungsberechtigung.

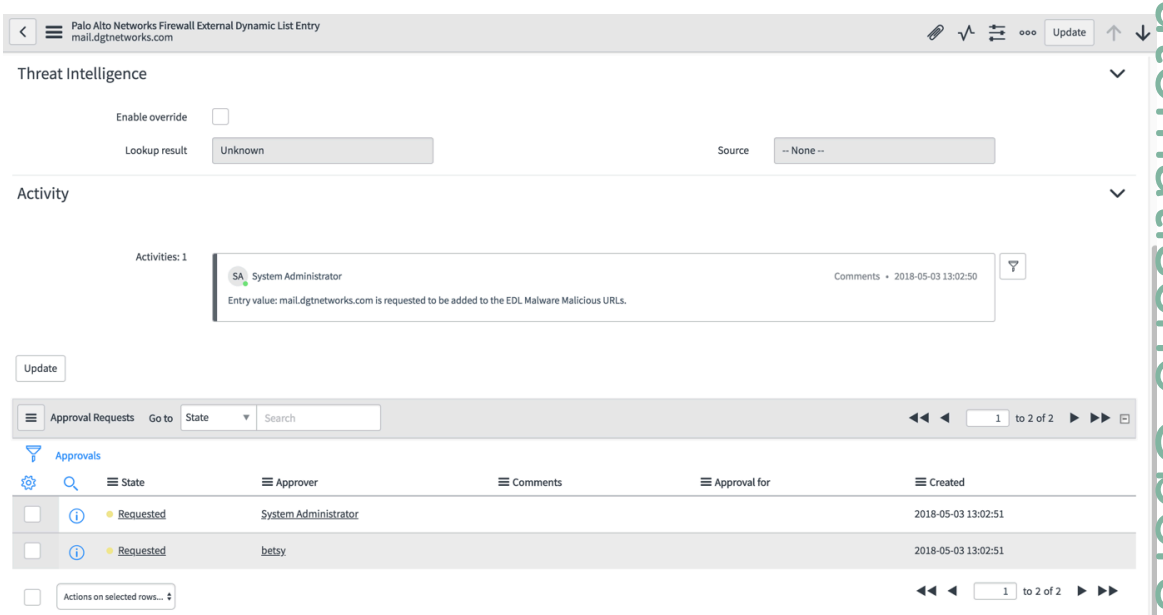
Warum und wann dieser Vorgang ausgeführt wird

Wenn der Genehmigungsprozess aktiviert ist, wird ein EDL-Eintrag in der EDL erst aktiviert oder deaktiviert, wenn er genehmigt wurde.

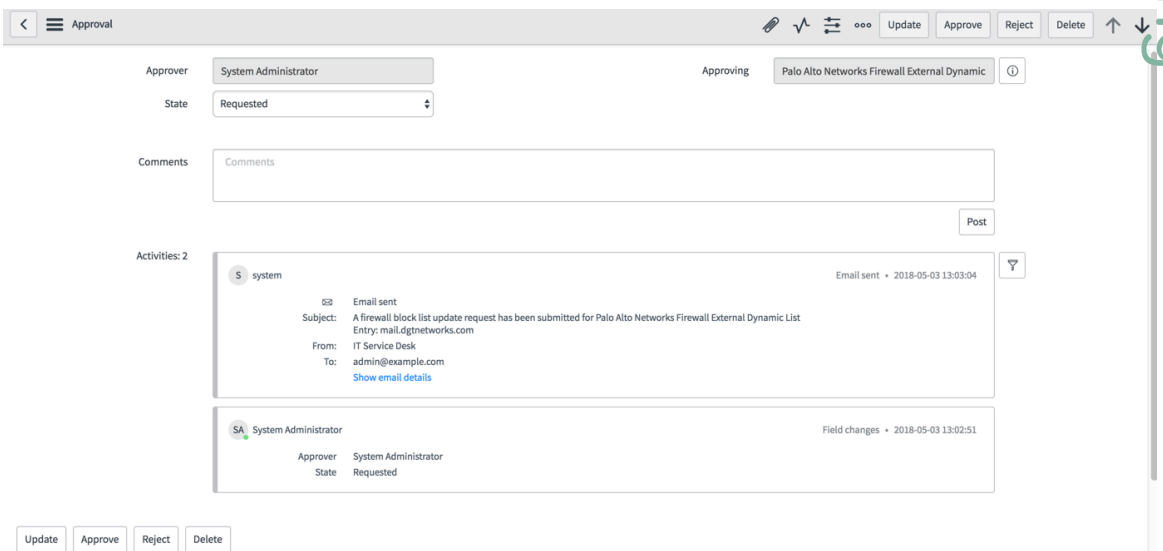
Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks NGFW-Integration** > **Firewall-EDL-Einträge** und öffnen Sie den EDL-Datensatz.
2. Scrollen Sie im EDL-Datensatz zum Abschnitt „Genehmigungsanforderungen“.

Hinweis:
Wenn Sie in den Systemeinstellungen Formulare mit Registerkarten ausgewählt haben, wird der Abschnitt als Registerkarte im Datensatz angezeigt.



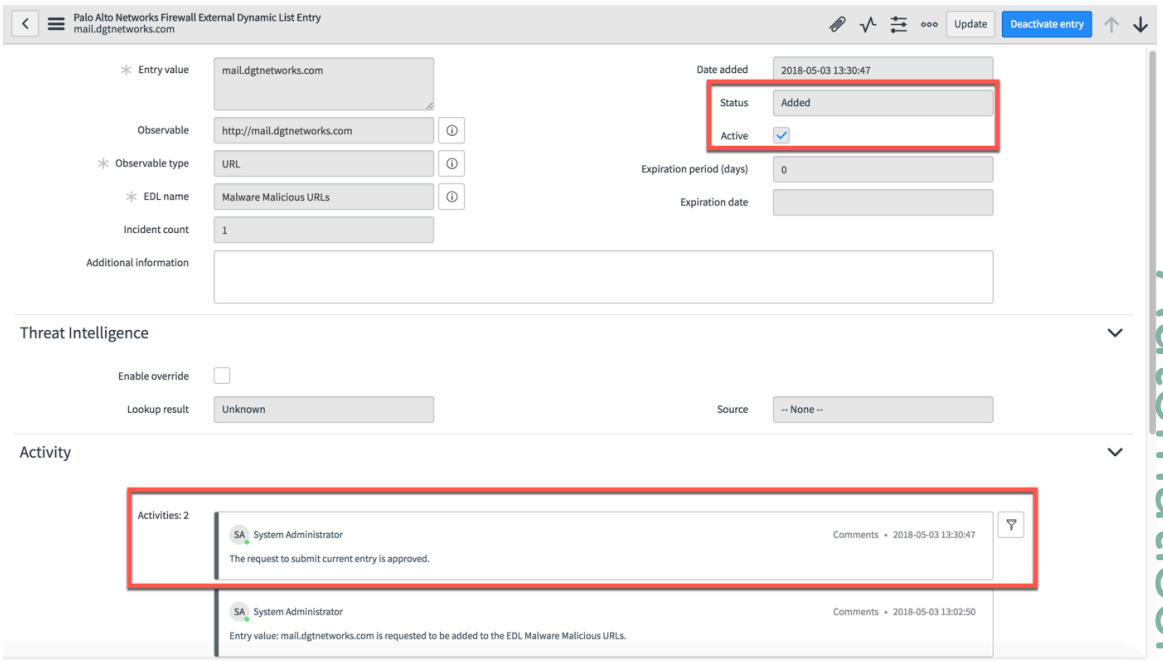
3. Klicken Sie unter Genehmigungsanforderungen auf ein Element in der Spalte **Status**, um es zu öffnen. Der Genehmigungsdatensatz wird angezeigt.



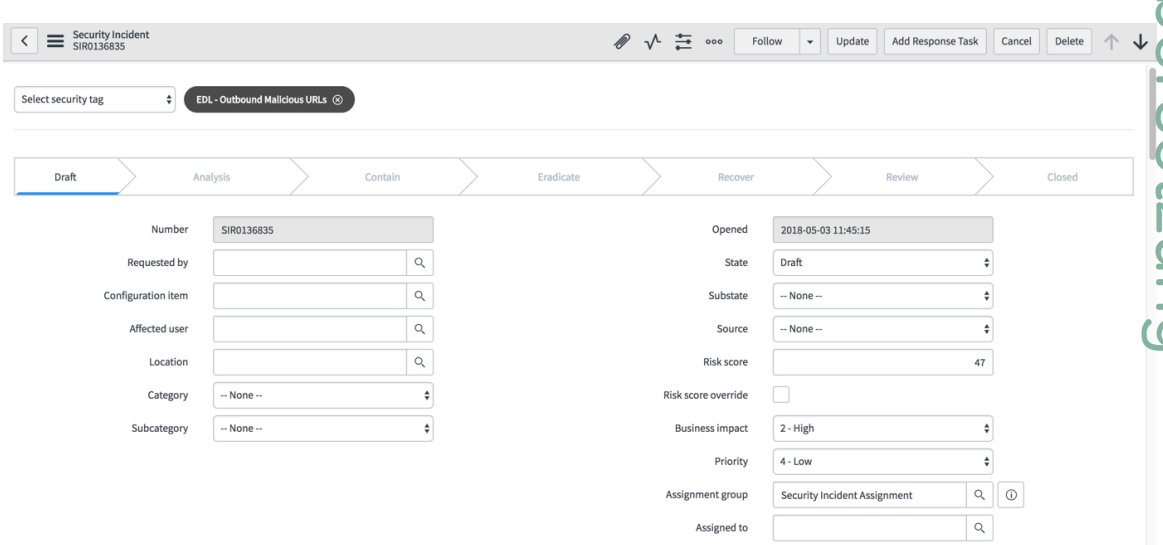
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie eine Option zum Genehmigen des EDL-Eintrags aus.
   Nachdem Sie den EDL-Eintrag genehmigt haben und er aktiviert ist, ruft Palo Alto Networks Next-Generation Firewall den EDL-Eintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, ist das erkennbare Element ab diesem Punkt blockiert. Beachten Sie, dass in der folgenden Abbildung das Kontrollkästchen Aktiv aktiviert ist, der Status Hinzugefügt lautet und in den Arbeitsnotizen angegeben ist, dass die Anforderung genehmigt wurde.



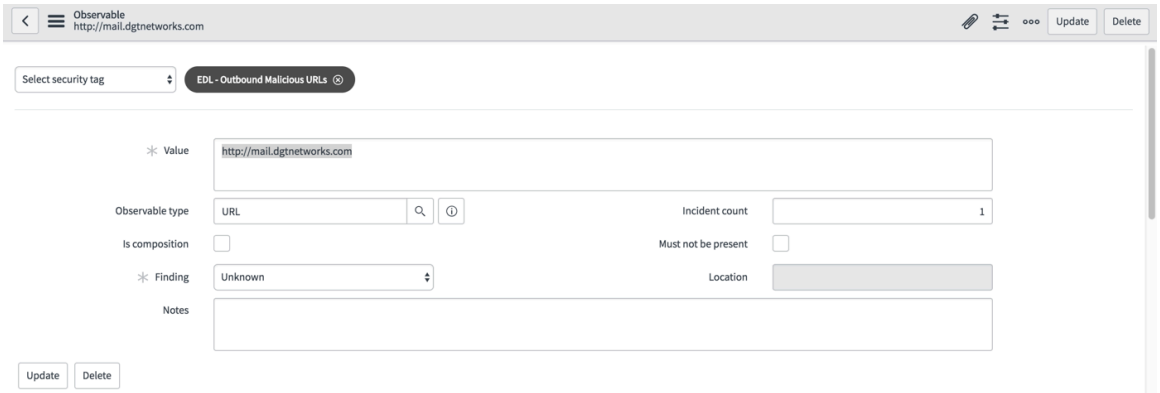
Nachdem der EDL-Eintrag genehmigt und aktiviert wurde, wird der Security Incident-Datensatz mit einem Sicherheits-Tag versehen. Das Tag wird oben im Datensatz angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Sicherheits-Tag wird auch im Datensatz des erkennbaren Elements angezeigt.



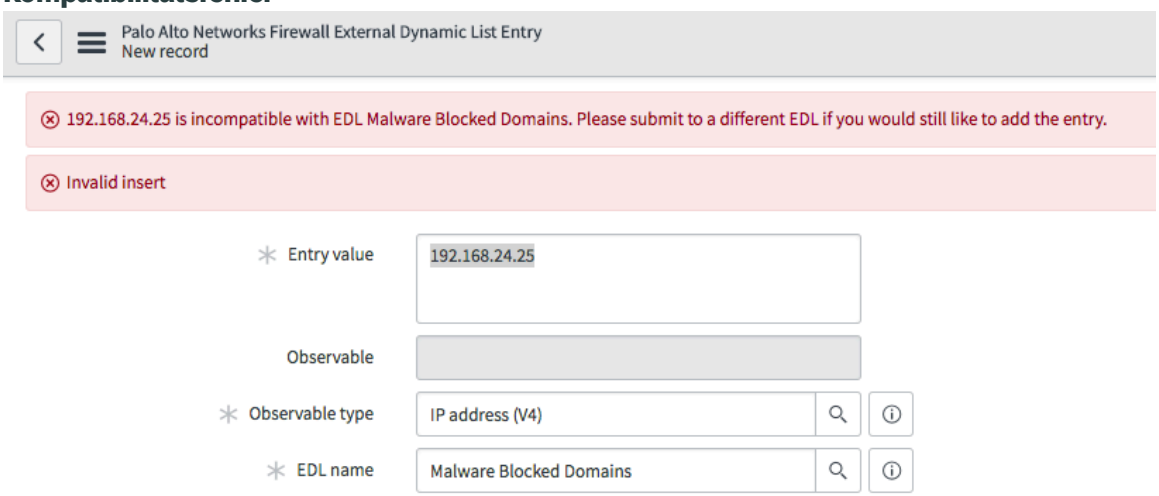
EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

Es gibt Einschränkungen für das Hinzufügen von EDL-Einträgen (External Dynamic List) zu EDLs. Wenn beim Versuch, EDL-Einträge zu EDLs hinzuzufügen, Duplikat-, Kompatibilitäts- oder CIDR-Konflikte (Classless Inter-Domain Routing) bestehen, werden Fehlermeldungen angezeigt, die Ihnen helfen, diese Fehler zu beheben.

Kompatibilitätsausnahme

Jede EDL akzeptiert nur Einträge, die mit ihrem erkennbaren Elementtyp kompatibel sind. Wenn Sie eine Domänen-EDL erstellen und versuchen, ihr ein erkennbares IP-Adressen-Element anzuhängen, wird eine inkompatible Fehlermeldung angezeigt. Beispielsweise kann eine Domänen-EDL nur erkennbare Domänenelemente akzeptieren, wie in der folgenden Abbildung dargestellt.

Kompatibilitätsfehler

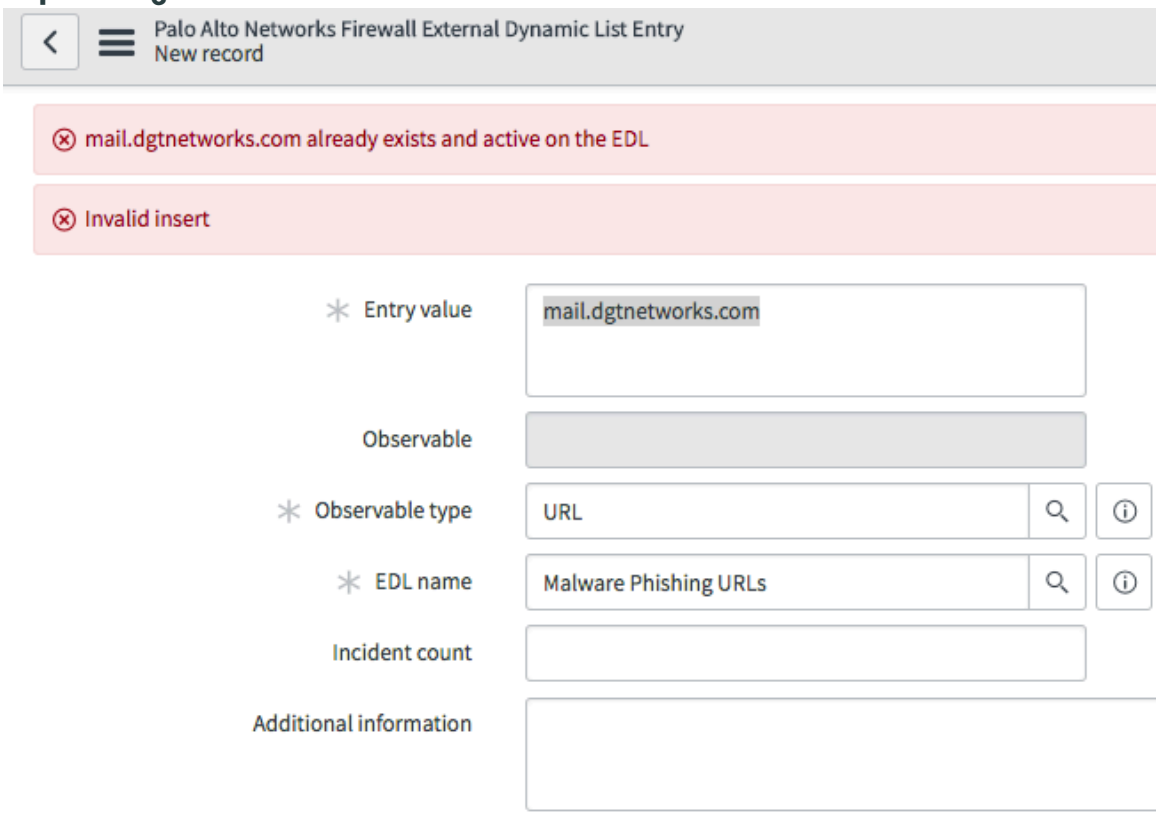


Duplizierungsausnahme

Ein erkennbares Element kann nicht auf mehreren EDLs des gleichen erkennbaren Elementtyps aktiviert werden. Wenn ein erkennbares URL-Element bereits auf einer URL-EDL aktiviert ist und Sie versuchen, dasselbe erkennbare Element auf einer Phishing-URL-EDL zu aktivieren, wird eine Duplizierungsfehlermeldung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Duplizierungsfehler

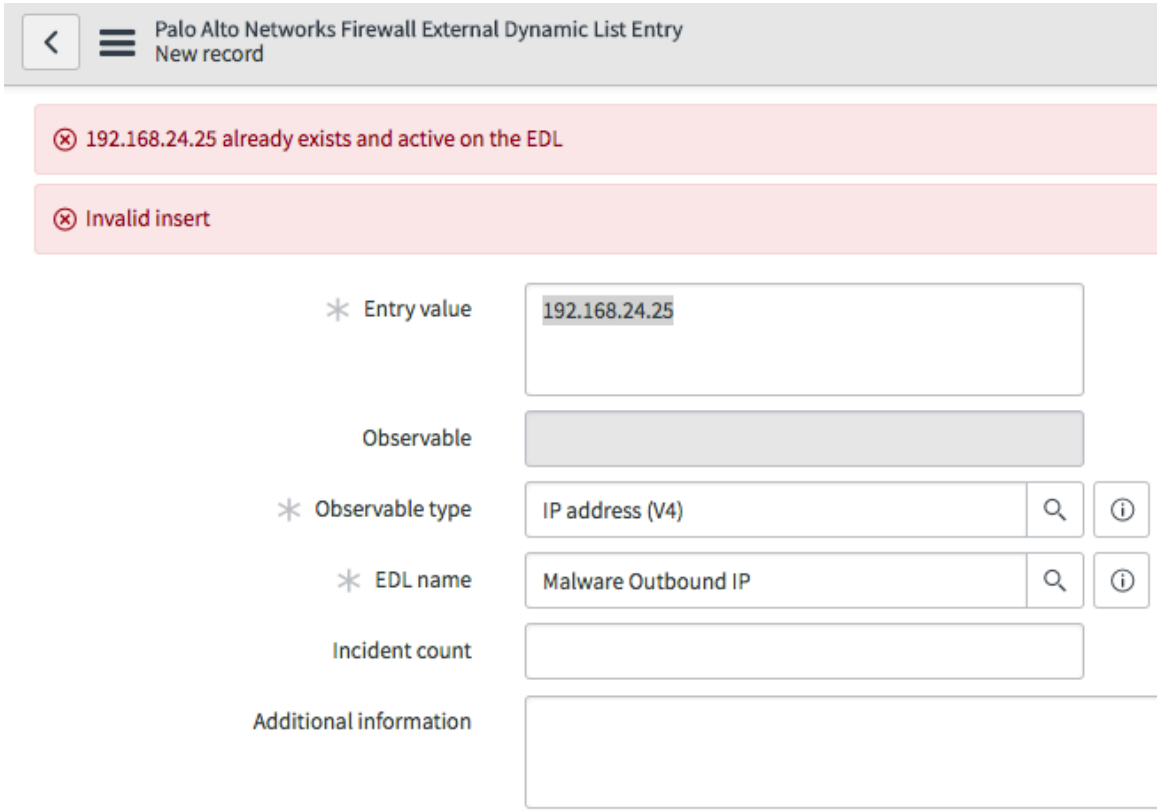


CIDR-Ausnahme (Classless Inter-Domain Routing).

Wenn Sie versuchen, eine einzelne IP-Adresse an eine EDL anzuhängen, und diese IP-Adresse Teil eines erkennbaren CIDR-Elements ist, das sich bereits auf einer EDL befindet, wird ein CIDR-Konfliktfehler angezeigt. Dieser Fehler weist darauf hin, dass die einzelne IP-Adresse bereits in der EDL als Teil des erkennbaren CIDR-Elements enthalten ist. Zum Beispiel ist 192.168.24.25 Teil des CIDR-Blocks 192.168.0.0/22.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIDR-Konflikt



(Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall

Wenn beim Erstellen des EDL-Datensatzes (External Dynamic List) das Kontrollkästchen **Tag anzeigen** aktiviert ist, können Sie die Tag-Namen und die Farben der Sicherheits-Tags bearbeiten. Mit Sicherheits-Tags können Sie bereits blockierte erkennbare Elemente nachverfolgen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

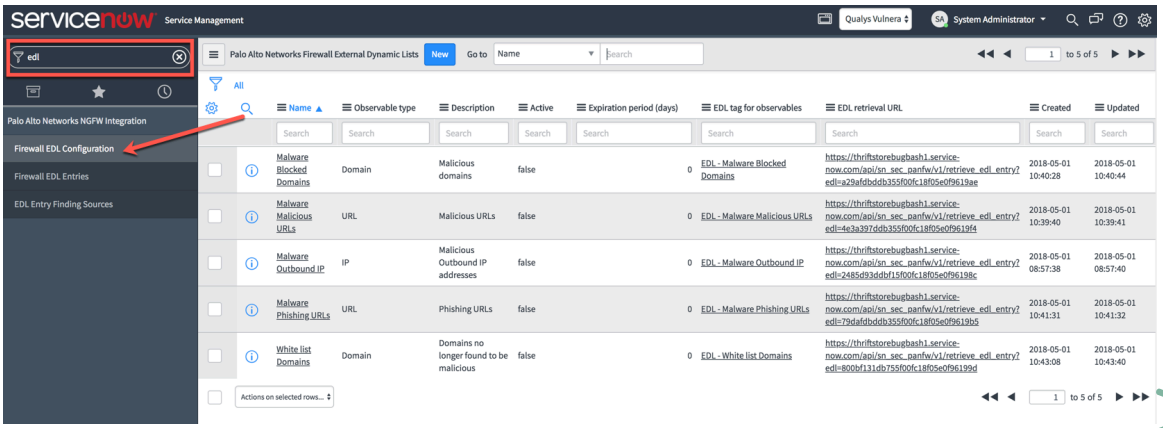
Warum und wann dieser Vorgang ausgeführt wird

Mit Sicherheits-Tags können Sie schnell identifizieren, welche Security Incidents erkennbare Elemente auf einer Sperrliste haben. Mithilfe von Tags können Sie auch identifizieren, ob ein erkennbares Element bereits blockiert ist oder aus einer EDL entfernt wurde. Standardmäßig ist die Farbe des Sicherheits-Tags für Sperrlisteneinträge schwarz und für Allow-Listeneinträge grau. Sie können die Namen und Farben der Tags ändern, um bestimmte Tags leichter zu erkennen.

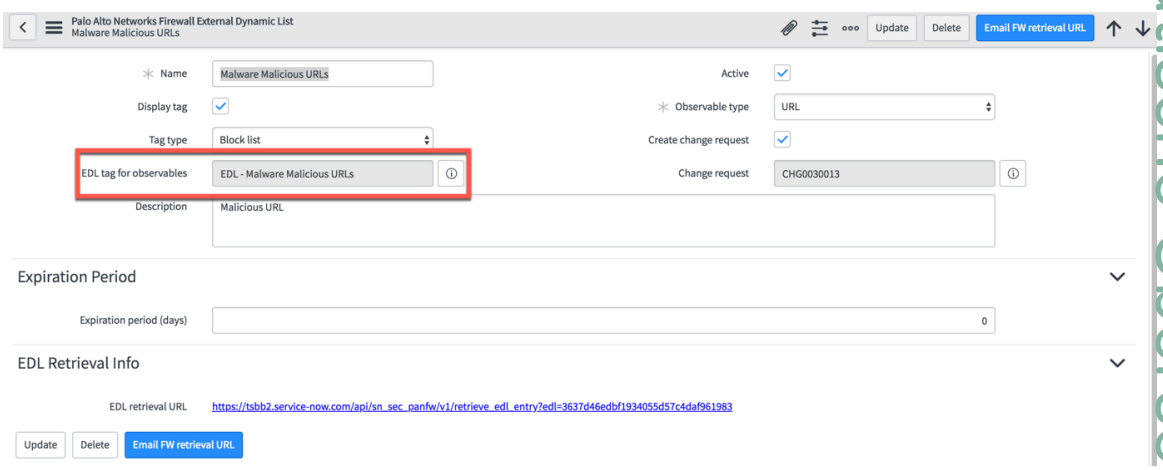
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

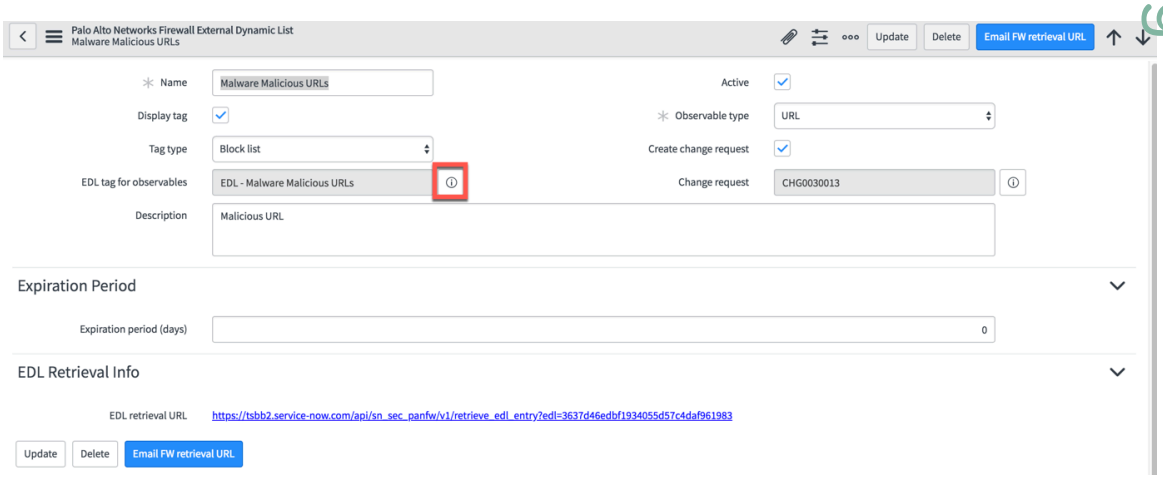
1. Navigieren zu **Alle** > **Palo Alto Networks NGFW-Integration** > **EDL-Konfiguration der Firewall**.



2. Klicken Sie auf ein Element in der Spalte **Name**, um es zu öffnen
   Der EDL-Datensatz wird angezeigt. Standardmäßig ist der Sicherheits-Tag-Name derselbe Wert, den Sie im Feld **Name** der EDL eingegeben haben, als Sie sie erstellt haben. Standardmäßig enthält der Name auch ein *EDL*- Präfix, z. B. EDL – Malware Malicius-URLs.



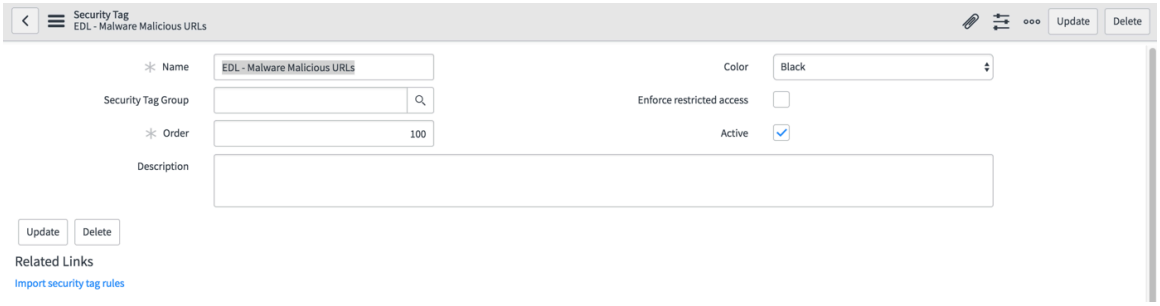
3. Klicken Sie auf das Informationssymbol ( ) neben **EDL-Tag für erkennbare Elemente** und dann **auf Datensatz öffnen**.



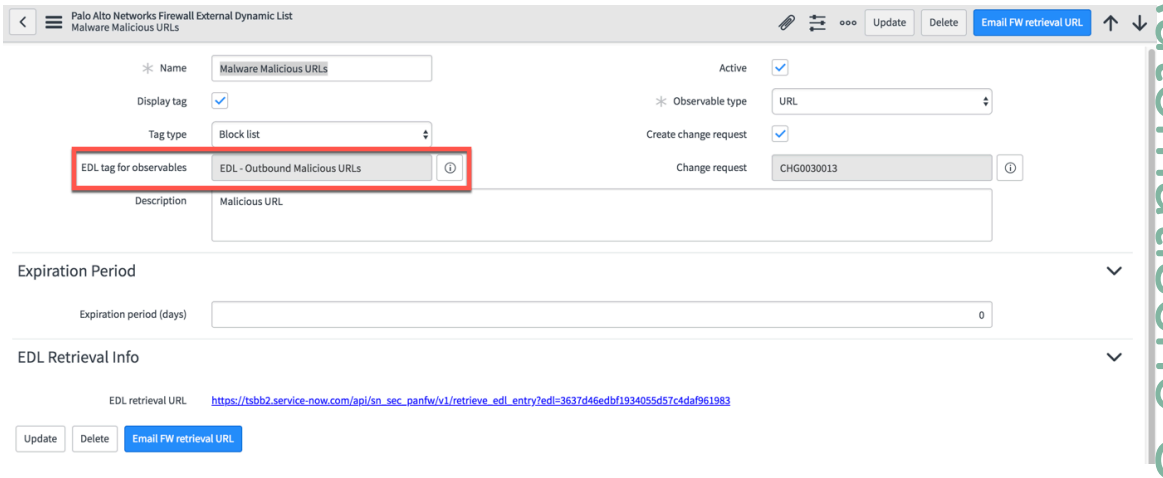
   Das Sicherheits-Tag-Formular wird angezeigt.

Automatische Übersetzung

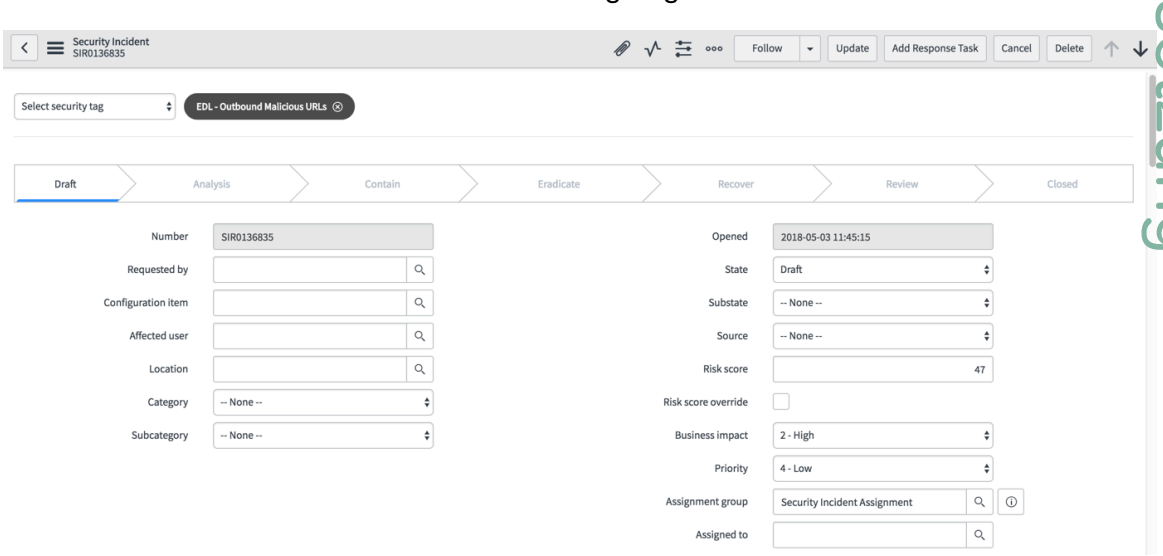
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Ändern Sie im Feld **Name** den Sicherheits-Tag-Namen, und klicken Sie auf **Aktualisieren**.
   Der aktualisierte EDL-Datensatz wird mit dem geänderten Tag-Namen angezeigt. Im folgenden Beispiel wurde dem Tag-Namen „ Ausgehend“ hinzugefügt. Behalten Sie das EDL- Präfix in Ihrem neuen Tag-Namen bei, damit Sie leichter erkennen können, ob das Tag mit der Palo Alto Networks Next-Generation Firewall -Integration verknüpft ist.



Die Sicherheits-Tags werden für jeden erkennbaren Typ (IP, URL, Domäne) im Security Incident-Datensatz und im Datensatz des erkennbaren Elements jedes Mal angezeigt, wenn dieses erkennbare Element zu einer EDL hinzugefügt wird.



Wenn ein erkennbares Element bereits einer EDL hinzugefügt wurde und ein Sicherheits-Tag für einen Security Incident für dieses erkennbare Element angezeigt wird, wird das EDL-Sicherheits-Tag automatisch auch für alle nachfolgenden Security Incident-Datensätze angezeigt, die erstellt werden. Diese Duplizierung weist darauf hin, dass

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sich das erkennbare Element bereits in einer Sperrliste befindet. Sie müssen dieses erkennbare Element nicht hinzufügen und erneut blockieren.

Wenn ein erkennbares Element nicht mehr blockiert ist, wird im Security Incident-Datensatz oder im Datensatz des erkennbaren Elements kein Sicherheits-Tag angezeigt. In dieser Instanz zeigt kein Sicherheits-Tag an, dass das Ablaufdatum des erkennbaren Elements möglicherweise verstrichen ist oder das erkennbare Element in einer EDL deaktiviert wurde.

Palo Alto Networks Next-Generation Firewall deinstallieren

Wenn Sie Palo Alto Networks Next-Generation Firewall aus Ihrer Instanz Now Platform deinstallieren und alle Reste aus der Integration entfernen möchten, finden Sie auf der Dokumentationswebsite ServiceNow Anweisungen zur Deinstallation von Anwendungen.

Vorbereitungen

Erforderliche Rolle: Systemadministrator (admin)

Siehe Anwendungen deinstallieren auf der Website der ServiceNow-Produktdokumentation .

PhishTank Integration

PhishTank ist ein Community-basiertes Phishing-Verifizierungssystem, bei dem Anwender vermutete Bedrohungen einreichen und andere Anwender im System abstimmen, um zu bestimmen, ob die Phishing-Bedrohungen berechtigt sind. Bei Integration mit dem -Produkt Now Platform Security Operations bieten die -Ergebnisse Analysten zusätzliche Einblicke in Security Incidents oder Untersuchungen im Zusammenhang mit Phishing.

Die PhishTank -Integration führt Suchen nach potenziellen Phishing-Website-URLs durch.

Der Workflow sucht nach neuen erkennbaren Elementen, sobald sie in Security Incidents eingehen. Wenn die erkennbaren Elemente von einem Typ sind, der von der API-Integration erkannt wird, werden die erkennbaren Elemente ausgewertet. Als schädlich erkannte erkennbare Elemente werden getaggt.

PhishTank installieren und konfigurieren

Bevor Sie die Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit die Anwendung PhishTank ordnungsgemäß in Now Platform Security Operationsintegriert werden kann.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform für Ihre Instanz zugewiesen haben.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (admin) installiert die App und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf das Modul Security Operations.
Rufen Sie einen API-Schlüssel ab.	Besuchen Sie die Website PhishTank, um Informationen zu API-Schlüsseln zu erhalten und ein Konto zu erstellen: PhishTank-Website .
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Madrid- und höher-Release-Anforderungen Für das Madrid-Release und spätere Familienreleases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

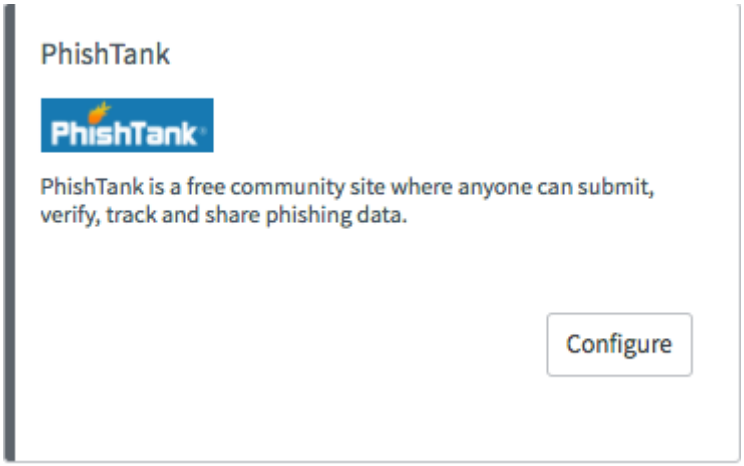
Erforderliche Rolle: Administrator

Prozedur

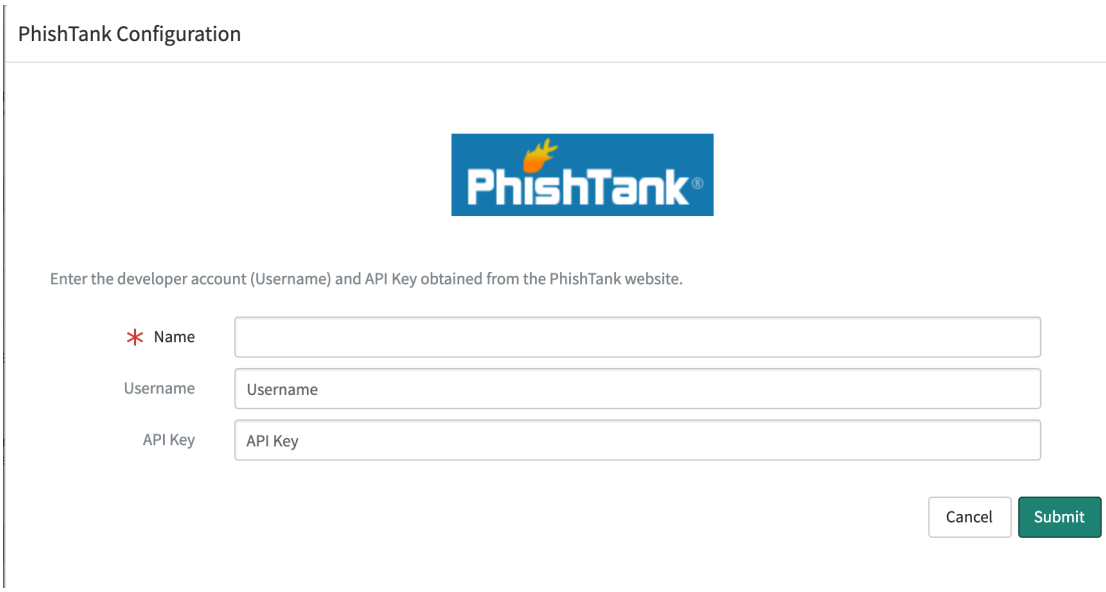
1. Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel PhishTank.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Konfigurieren**.



4. Geben Sie im Dialogfeld **„PhishTank-Konfiguration** “ den Namen der Konfiguration, den Anwendernamen (in PhishTank erstellter Entwickleraccount) und den API-Schlüssel ein, den Sie von der Website PhishTank erhalten haben, und klicken Sie auf **Absenden**.



5. Überprüfen Sie die erfolgreiche Konfiguration.
Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, es wird eine Fehlermeldung angezeigt.

Trouble?

Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, ist der API-Schlüssel PhishTank möglicherweise ungültig.

Überprüfen Sie die erwarteten Ergebnisse für PhishTank

Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Suchergebnisse werden auf der Registerkarte Ergebnisse der Bedrohungssuche unten im Security Incident-Datensatz angezeigt.

Vorbereitungen

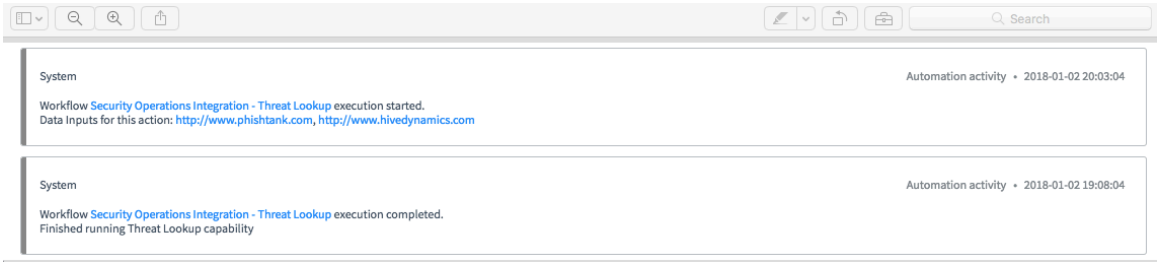
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie das Security Incident-Formular, mit dem Sie arbeiten, und vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.



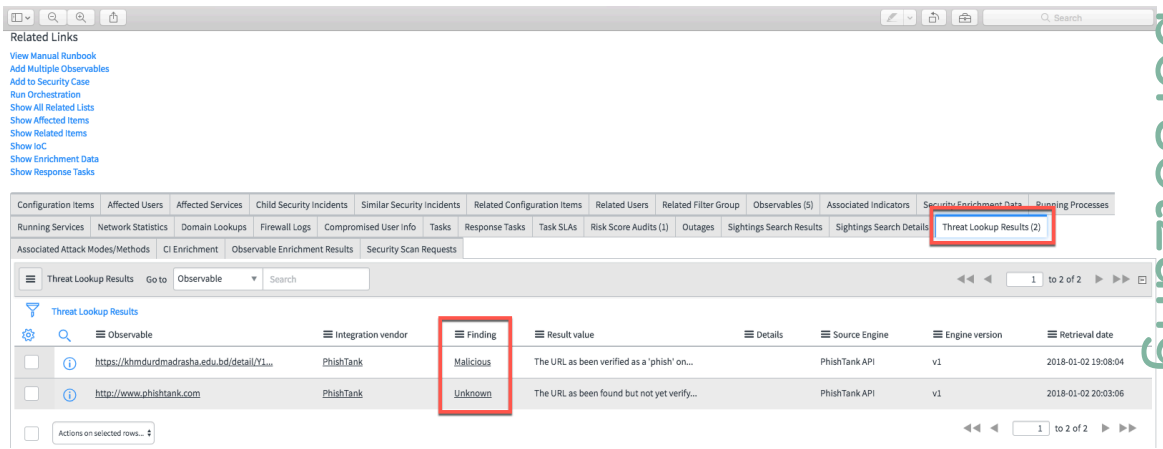
Nachdem die Anwendung konfiguriert wurde, wird der Flow bei der Erstellung des incident automatisch gestartet. Der Ausführungs- und Abschlussstatus der Suche wird dann in den Arbeitsnotizen im Security Incident-Datensatz angezeigt.

2. Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweise, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incidents, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**.

Hinweis:

Die Abbildungen in den folgenden Schritten werden mit aktivierter Einstellung **für Formulare mit Registerkarten** in den Systemeinstellungen angezeigt. Wenn Formulare mit Registerkarten nicht angezeigt werden, klicken Sie in der oberen rechten Ecke des Bannerframes auf das Zahnradsymbol Einstellungen. Klicken Sie im angezeigten Dialogfeld **„Systemeinstellungen“** auf **Formulare**, und vergewissern Sie sich, dass **Formulare mit Registerkarten** und **Mit Formular** ausgewählt sind.



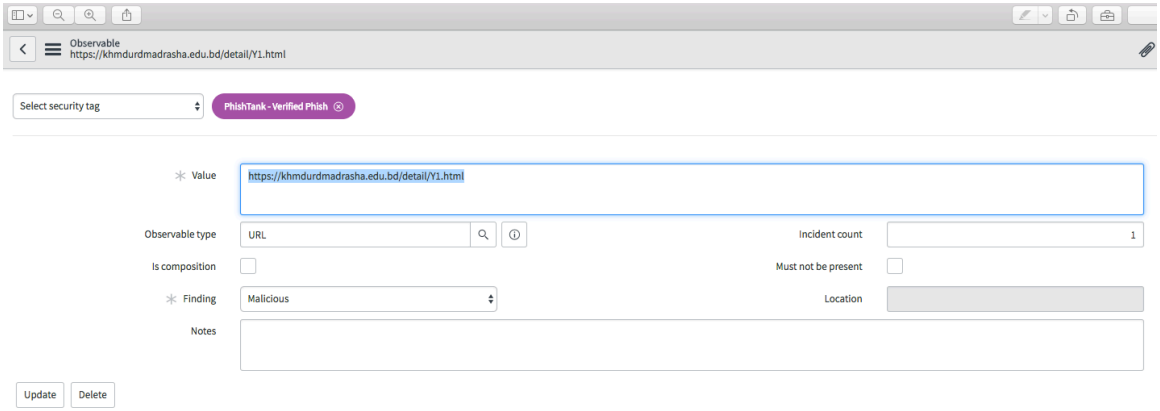
Auf der Registerkarte **Ergebnisse der Bedrohungssuche** im unteren Bereich des Security Incident-Datensatzes werden die Suchergebnisse angezeigt.

In der Spalte **„Ergebnis** “ wird für Datensätze, die nicht als schädlich eingestuft wurden, Unbekannt angezeigt. Bei Ergebnissen, die mit schädlichen übereinstimmen, wird Böswillig in der Spalte **Ergebnis** angezeigt.

4. Klicken Sie in der Spalte **Erkennbares** Element auf ein erkennbares Element, um einen Datensatz zu öffnen und weitere Informationen anzuzeigen.

Automatische Übersetzung

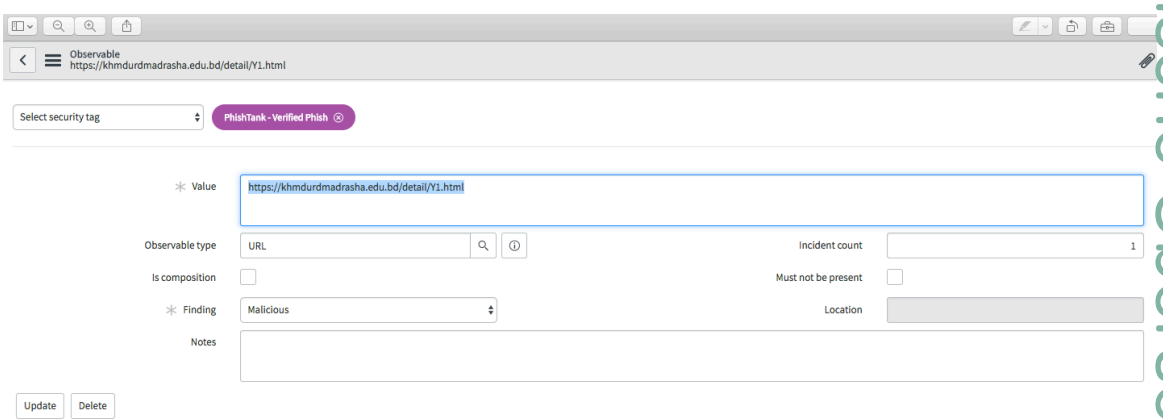
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Datensatz des erkennbaren **Elements wird für Suchen, die mit böswilligen Elementen übereinstimmen, das Feld Ergebnis**angezeigt. Das erkennbare Element ist mit der Quelle Threat Intelligence getaggt, die es als schädlich eingestuft hat, in diesem Fall die Anwendung PhishTank.

5. Um Rohdaten anzuzeigen, navigieren Sie zurück zum Security Incident, und klicken Sie auf das blaue Informationssymbol neben einem erkennbaren Element.

6. Klicken Sie im angezeigten Fenster **auf Datensatz öffnen**.



Der von der API erstellte Link und das Feld **„Ergebnis“**, das mit den Ergebnissen angezeigt wird.

Trouble?

Wenn auf der Registerkarte **Ergebnisse der Bedrohungssuche** keine Ergebnisse angezeigt werden, vergewissern Sie sich, dass das erkennbare Element ein Typ ist, der von der Integration für die Suche unterstützt wird.

(Optional) Fügen Sie manuell ein erkennbares Element für hinzu PhishTank

Sie können erkennbare Elemente manuell an einen Security Incident anhängen. Sie können erkennbare Elemente manuell anhängen, wenn Sie Bedrohungssuchen für erkennbare Elemente durchführen möchten, die beim ersten Ereignisauslöser nicht an einen Security Incident angehängt sind. Außerdem können Sie diese Aufgabe ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

Vorbereitungen

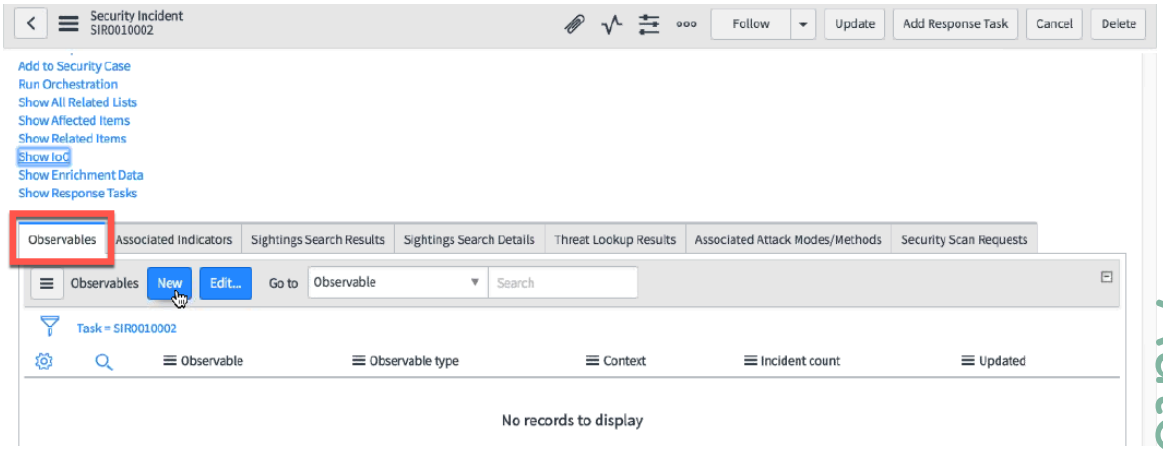
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

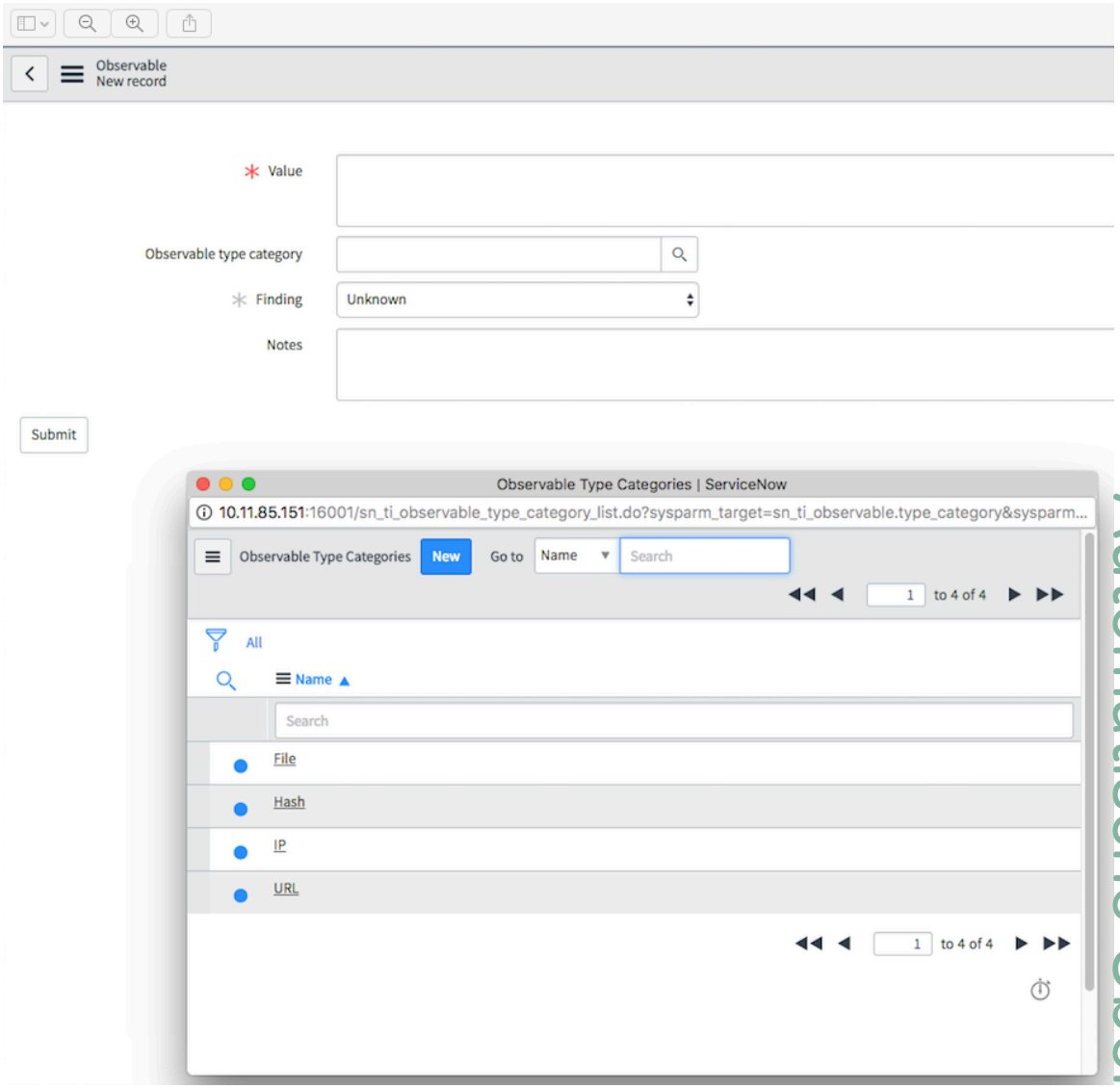
1. Navigieren Sie zu Ihrem offenen Security Incident.
2. Klicken Sie im geöffneten Security Incident-Datensatz auf den Link **IoC anzeigen**unter **Zugehörige Links,** um die Registerkarte **Erkennbare Elemente** anzuzeigen.



3. Klicken Sie auf **Neu**.
   Das Formular „Erkennbares Element“ wird angezeigt.
4. Geben Sie im Feld **Wert** eine URL ein.
5. Klicken Sie auf das Suchsymbol, und klicken Sie im Dialogfeld **„Kategorien erkennbarer Elemente“** in der Liste auf **URL**, um das Feld auszufüllen.

Automatische Übersetzung

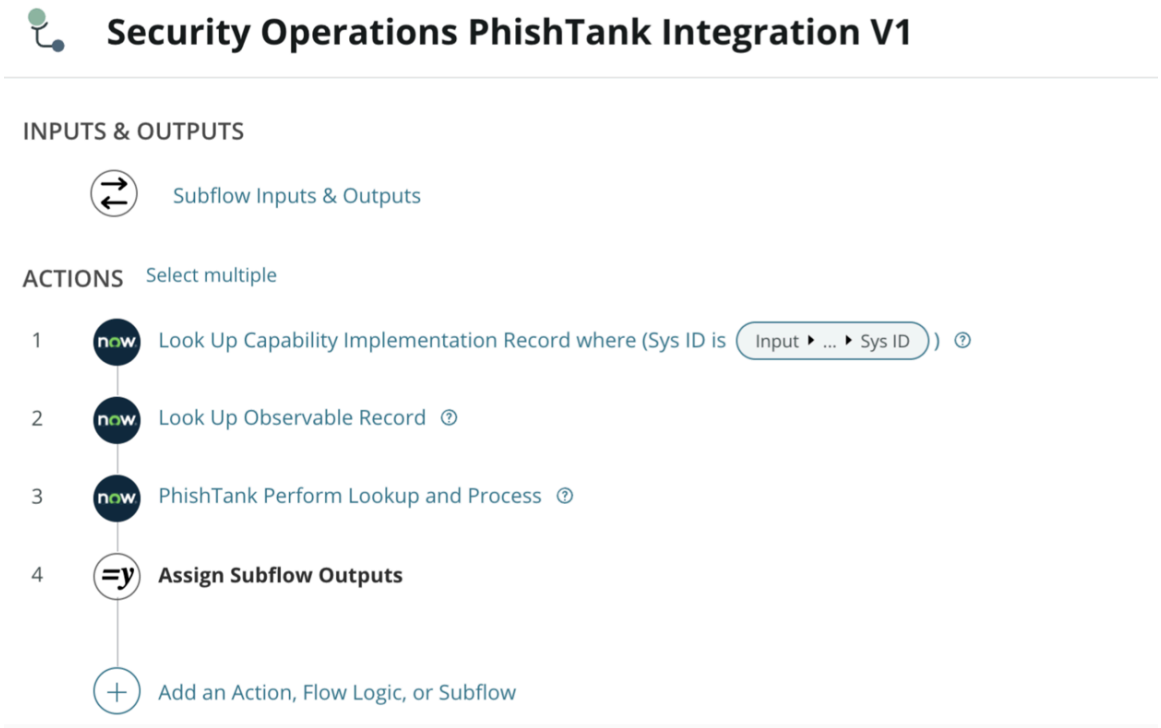
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



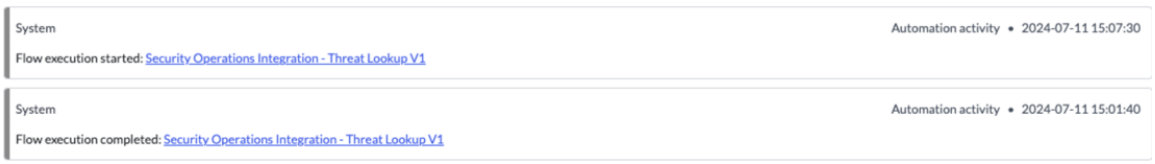
6. Klicken Sie auf **Absenden**.
Der Flow wird gestartet und sucht nach dem neuen erkennbaren Element. Der Ausführungs- und Abschlussstatus werden im Abschnitt „Arbeitsnotizen“ im Datensatz „Security Incident“ angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

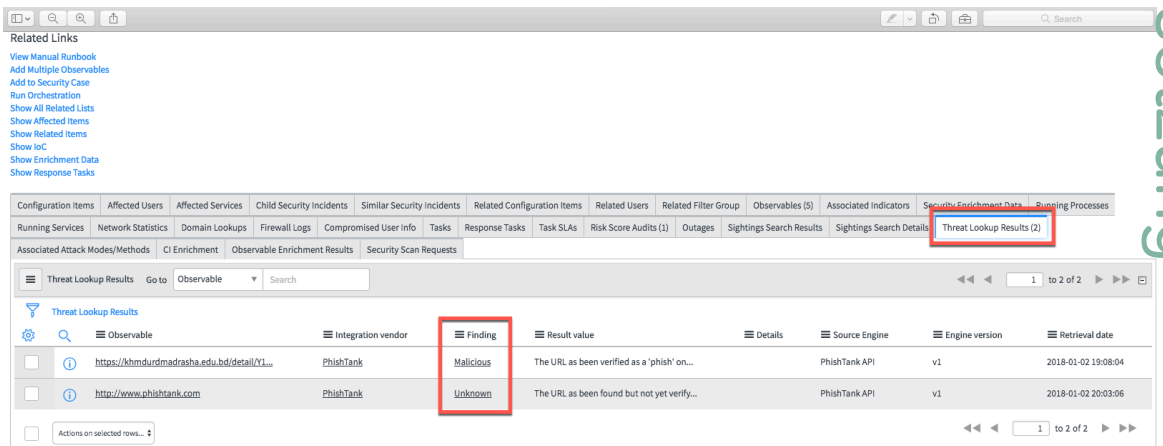


7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.



8. Klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen anzeigen** am unteren Rand des Security Incidents.

9. Klicken Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche,** um die Ergebnisse anzuzeigen.



10. Klicken Sie in der Spalte „ **Erkennbares** Element“ auf das blaue Informationssymbol neben einem bestimmten erkennbaren Element, um weitere Informationen und Rohdaten zu erhalten.

11. Klicken Sie im angezeigten Dialogfeld **auf Datensatz öffnen**.

Automatische Übersetzung

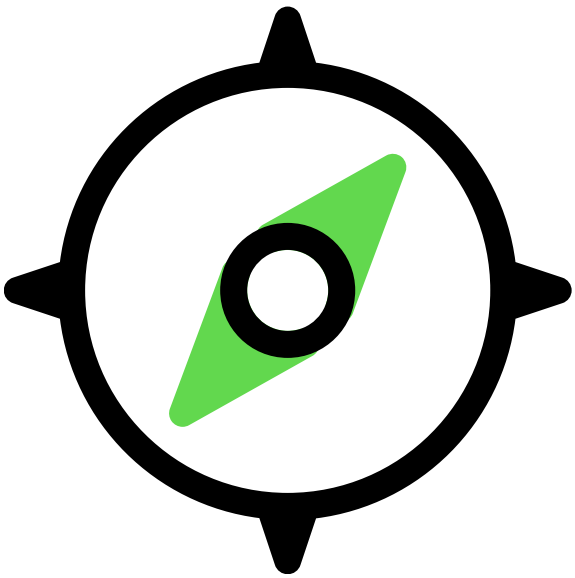
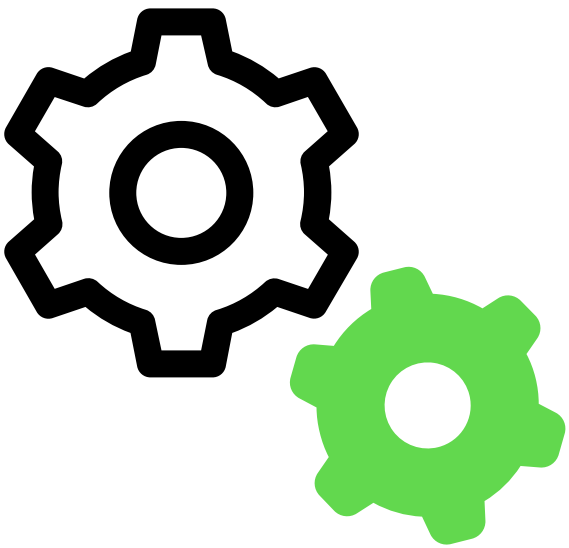
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?
Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweise, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

Proofpoint -Integration für Security Operations

DieProofpointSecurity Operations -Integration unterstützt die Erfassung von Ereignissen von Proofpoint. Security Incident Response (SIR) erstellt einen Incident für jedes erfasste Ereignis, das Analysten überprüfen oder bearbeiten können.

Erste Schritte

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über Proofpoint die -Integration	Konfigurieren Sie Proofpoint für SIR-Arbeitsbereich

Proofpoint -Integration für Security Operationserkunden

Sie können Ereignisprofile in Security Incident Response (SIR) konfigurieren, um Ereignisse von Proofpointzu erfassen. SIR erstellt einen Incident für jedes erfasste Ereignis, das Analysten überprüfen oder bearbeiten können.

Proofpoint Integration für Security Operations Benutzer

Anwender

Anwender	Beschreibung
Sicherheitsadministrator	Erstellen Sie Ereignisprofile zum Filtern der erfassten Ereignisse. SIR erstellt Incidents für diese erfassten Ereignisse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proofpoint Integration für Security Operations Leistungen

Proofpoint Integration für Security Operations Leistungen

Leistung	Funktion	Anwender
Rufen Sie Event-Daten in Ihre -Instanz ab, und erstellen Sie Security Incidents. Überprüfen Sie Security Incidents von einem zentralen Ort aus auf Ereignisse, die als verdächtig oder böswillig eingestuft werden.	Wenn zugestellte E-Mail-Nachrichten und zulässige Klicks später als schädlich eingestuft werden, wurden diese Nachrichten wahrscheinlich von Ihren Mitarbeitern geöffnet und interagiert. Um diese Nachrichten zur Überprüfung nachzuverfolgen, erstellen Sie automatisch Security Incidents basierend auf den Ereignisprofilen, die Sie für den Nachrichtenverkehr für die Integration erstellen und konfigurieren. Sie können auch die Erstellung von Security Incidents für die blockierten Nachrichten und Klicks zu Audit-Zwecken aktivieren.	Manager

Automatische Übersetzung

Empfehlungen für weitere Themen

Weitere Informationen zum Konfigurieren und Verwenden von Proofpointfinden Sie in den folgenden Themen:

- Proofpoint -Integration für Security Operationskonfigurieren
- Überprüfen Sie die Integrationseinstellungen für Proofpoint .
- Zeigen Sie das Analytics-Dashboard Proofpoint an

Proofpoint -Integration für Security Operationskonfigurieren

Konfigurieren Sie Ihre Implementierung der Proofpoint -Integration für Security Operations.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration – Übersicht

1. Proofpoint Integration für Security Operationsinstallieren und konfigurieren.

   Laden Sie die Integrationsanwendung herunter, installieren und aktivieren Sie sie.

2. Erstellen Sie ein Ereignisprofil für die Proofpoint -Integration für Security Operations.

   Erstellen Sie ein Ereignisprofil, um die Ereignisse zu identifizieren, die Sie aus dem Produkt Proofpoint importieren möchten, und die Bedingungen, die Sie zum Erstellen von Security Incidents aus den importierten Daten verwenden möchten.

3. Überprüfen Sie die Integrationseinstellungen für Proofpoint .

   Überprüfen Sie die Integrationseinstellungen zum Erstellen der Ereignisprofile.

Proofpoint Integration für Security Operationsinstallieren und konfigurieren

Installieren und konfigurieren Sie die Anwendung Proofpoint Integration for Security Operations (Integration von []) für ServiceNow® Store in der Instanz ServiceNow.

Vorbereitungen
Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Anwendung Proofpoint Integration for Security Operations (Integration für []) von ServiceNow® Store herunter, und installieren Sie sie.
   Weitere Informationen finden Sie unter Eine ServiceNow Store-Anwendung installieren .
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie die Kachel Proofpoint Integration für Security Operations, und wählen Sie **Konfigurieren**aus.
4. Füllen Sie die Felder des Formulars aus.

Proofpoint Formular „Integrationskonfiguration“.

Feld	Beschreibung
Name	Name der Konfiguration von Proofpoint Integration for Security Operations.
Service-Prinzipal	Anwendername des Mandanten Proofpoint
Geheimer Schlüssel	Die ID des Proofpoint -Mandanten.

5. Wählen Sie **Absenden**.

Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Ereignisprofil für die Proofpoint -Integration für Security Operations

Erstellen Sie ein Ereignisprofil, um die Ereignisse zu identifizieren, die Sie aus dem Produkt Proofpoint importieren möchten, und erstellen Sie in der Anwendung Security Incident Response einen Security Incident.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können ein Ereignisprofil erstellen, indem Sie Ereignistypen, Zuordnungen und Importzeitpläne konfigurieren. Ein Fortschrittsbalken auf der Seite zeigt alle Schritte an und ist für die derzeit aktive Konfiguration hervorgehoben. Mit der Schaltfläche **„Fortsetzen“** bzw. **„Zurück“** können Sie vorwärts oder rückwärts navigieren.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Navigieren zu **Alle** > **SIR-Integration mit Proofpoint** > **Proofpoint-Ereignisprofil**.
   Auf der Seite Proofpoint Ereignisprofile werden die vorhandenen Ereignisprofile aufgelistet.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

   Der Fortschrittsbalken wird beginnend mit Name angezeigt.

Formular „Proofpoint-Ereignisprofil

Feld	Beschreibung
Name	Name für das Ereignisprofil. Erwägen Sie die Verwendung eines Namens, der den zugehörigen Ereignistyp enthält: ○ Klicks blockiert ○ Klicks zugelassen ○ Nachrichten blockiert ○ Nachrichten zugestellt
Quelle	Die für die Integration auf der Seite Integrationskonfigurationen konfigurierte Quelle.
Bestellung	Der Auftrag, in dem dieses Profil ausgeführt wird. Der Standardwert ist 100.
Aktiv	Option zum Aktivieren des Profils.
Beschreibung	Optionale dBeschreibung für dieses Ereignisprofil.

4. Wählen Sie **Fortsetzen**.
5. Wählen Sie einen oder mehrere Ereignistypen aus, indem Sie sie aus der Spalte **Verfügbar** in die Spalte **Ausgewählt** verschieben.
   Die verfügbaren Ereignistypen sind:
   - Klicks blockiert
   - Klicks zugelassen
   - Nachrichten blockiert
   - Nachrichten zugestellt
6. Wählen Sie **Fortsetzen**.

   Die Konfigurationsschritte, die sich auf den/die ausgewählten Ereignistyp(en) beziehen, werden in der Fortschrittsleiste angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Werte für die Quellfelder werden aus den Daten des gezielten Angriffsschutzes (TAP) in Ihrer Umgebung als Referenz bereitgestellt.

Die Standardzuordnung der Quellfelddaten an die Zielfelder wird auf der Seite angezeigt. Basisdaten sind als Leitfaden enthalten, Sie können diese Zuordnung jedoch ändern.

7. **Wahlweise:** Wählen Sie das Symbol **f(x),** um die in der Anwendung enthaltenen Standardübersetzungen anzuzeigen.

   (Optional) Diese Übersetzungen berücksichtigen mehrere Werte für ein Feld, indem Kommas zwischen den Werten eingefügt werden.

8. Wählen Sie **Fortsetzen**.
9. Konfigurieren Sie auf der Seite „Filtern und Zusammenfassungen“ die Eigenschaften in der folgenden Tabelle.

Filter- und Zusammenfassungseigenschaften

Option	Beschreibung
Basierend auf Bedingungen für Nachrichtenereignisse filtern	Option zum Aktivieren der Filterung basierend auf Nachrichtenereignissen.
Filterbedingungen für Nachrichtenereignisse	Filterbedingungen für Nachrichten-Ereignisse.
Basierend auf Bedingungen für Klickereignisse filtern	Option zum Aktivieren der Filterung basierend auf Klickereignissen.
Filterbedingungen für Klickereignisse	Klicken Sie auf Ereignisfilterbedingungen.
Zusammenfassungsbedingungen	Option, um zuzulassen, dass ein eingehender Incident an einen offenen Security Incident angehängt wird, anstatt einen neuen zu erstellen.
Incident-Felder mit übereinstimmenden Werten	Fügen Sie die Felder Security Incident Response hinzu, deren Werte übereinstimmen müssen, damit ein Incident in eine Zusammenfassung aufgenommen wird.
Protokoll-Arbeitsnotiz für neuen Incident	Mit dieser Option wird die Protokollierung von Arbeitsnotizen im übergeordneten Element Security Incident Responseaktiviert.
Aktivieren Sie die ThreatID-Beziehung	Option zum Aktivieren der Zusammenfassung aller Incidents mit übereinstimmenden ThreatIDs.

10. Wählen Sie **Fortsetzen**.
11. Wählen Sie einen der Importtypen aus und geben Sie an, wie oft Sie Ereignisdaten importieren möchten.
12. Wählen Sie **Fertigstellen** aus.

Ergebnisse

DDas neu erstellte Ereignisprofil wird zusammen mit den vorhandenen Ereignisprofilen[] aufgelistet .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die Integrationseinstellungen für Proofpoint .

Überprüfen Sie die IntegrationseinstellungenProofpointfür [], damit Sie die Systemeigenschaften für Ihre Umgebung ändern können.

Proofpoint Formular „Integrationseinstellungen“

Eigenschaftsname	Beschreibung
Zeitüberschreitung für die restAPI-Aufrufe. sn_sec_ Proofpoint.http_timeout	Die Zeitüberschreitung (in Sekunden) für das Abrufen von Daten aus den API-Aufrufen. Typ: Ganzzahl Standardwert: 3000
Protokollierungsebene – Debugging, Information, Warnung, Fehler sn_sec_probepunkt.protokollierung_verbosity	Die Protokoll-Ausführlichkeitsstufe der Anwendung, die den Namen des Informationstyps angibt. Verfügbare Werte: • Fehler • warnen • Info • debuggen Standardwert: info
Erzwingt einen Grenzwert für die Anzahl von Proofpoint-Ereignissen, die zu einem einzelnen Incident aggregiert werden können. sn_sec_ Proofpoint.max_aggregations_per_si	Die maximale Anzahl von Proofpoint Ereignissen, die zu einem Incident zusammengefasst werden können. Typ: Ganzzahl Standardwert: 100
Grenzwert für die Anzahl von Security Incidents erzwingen, die innerhalb von 24 Stunden erstellt werden können. sn_sec_ Proofpoint.max_si_per_day	Die maximale Anzahl von Incidents, die innerhalb von 24 Stunden erstellt werden können Typ: Ganzzahl Standardwert: 1000
Anzahl der Tage, die wir im API-Aufruf für Top-Klicker verwenden müssen, vap. sn_sec_proofpoint.default_days	Die Anzahl der Tage, an denen Daten für Top-Klicker und VAP abgerufen werden sollen. Verfügbare Werte: • 14 • 30 • 90.0 Typ: Ganzzahl Standardwert: 90
Boolesche Kennzeichnung. Wenn diese Option aktiviert ist, wird ein API-Aufruf durchgeführt und die Topclicker-Details ausgefüllt.	Option zum Aktivieren und Abrufen von Top-Clicker-Daten. Typ: Boolesch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proofpoint Formular „Integrationseinstellungen“ (Fortsetzung)

Eigenschaftsname	Beschreibung
sn_sec_ Proofpoint.call_topclickers_api	Standardwert: True
Boolesche Kennzeichnung. Wenn diese Option aktiviert ist, wird ein API-Aufruf durchgeführt und VAP-Details ausgefüllt. sn_sec_ Proofpoint.call_vap_api	Option zum Aktivieren und Abrufen von VAP-Daten. Typ: Boolesch Standardwert: False
Dient zum Einschränken der maximalen Anzahl von Anwendern, die für topClickers, VAP-Anwender, angezeigt werden sollen. sn_sec_proofpoint.maxresults	Die maximale Anzahl von Anwendern, die für Top-Klicker und VAP-Anwender angezeigt werden sollen Typ: Ganzzahl Standardwert: 100
Aktiviert/deaktiviert die Verwendung des sich überschneidenden Zeitraums während der geplanten Abfrage von Proofpoint-Ereignissen. sn_sec_ Proofpoint.allow_overlap	Option zum Aktivieren des sich überschneidenden Zeitraums, wenn die geplante Abfrage konfiguriert wird. Typ: Boolesch Standardwert: False
Überlappungszeit in Minuten für die geplante Abfrage von ProofpointEvents, wenn Überlappung aktiviert ist. sn_sec_prüfpunkt.überlappung_zeit	Die Überlappungszeit in Minuten, wenn eine geplante Abfrage konfiguriert ist. Typ: Ganzzahl Standardwert: 5

Zeigen Sie das Analytics-Dashboard Proofpoint an

Das Analytics-Dashboard Proofpoint enthält Details zu VAP-Anwendern und Top-Klickern.

Warum und wann dieser Vorgang ausgeführt wird

UServer , die hauptsächlich Ziel von Sicherheitsangriffen sind, gelten als [VAP-Benutzer. EMitarbeiter, die häufig auf auf verdächtige Links und Phishing-Links klicken, gelten als Top-Klicker.

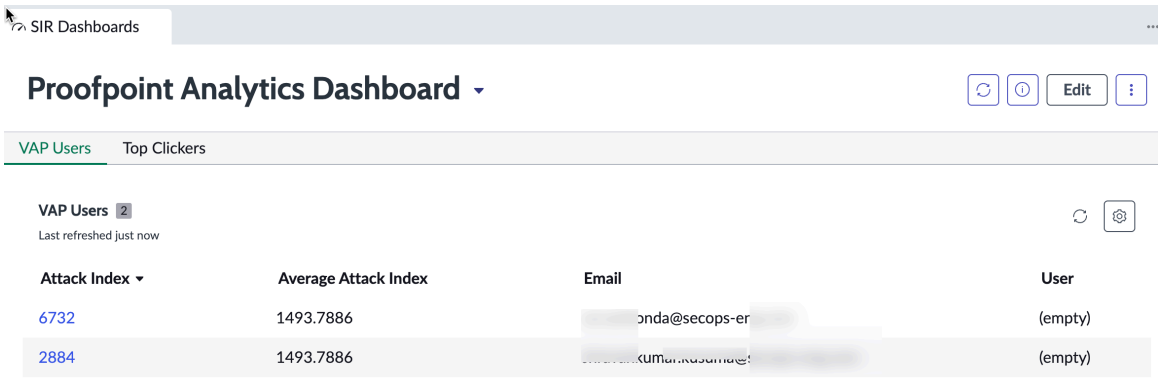
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen Sie **SIR-Dashboards**aus.
3. Wählen Sie **Proofpoint Analytics-Dashboard** in der Dropdown-Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie Informationen zu VAP-Benutzern an.
   a. Zeigen Sie die Liste der VAP-Benutzer an, indem Sie die Registerkarte **VAP-Benutzer** auswählen.
   b. Zeigen Sie die Details eines VAP-Anwenders an, indem Sie den Anwendernamen auswählen.
5. Zeigen Sie Informationen zu den Top-Klickern an.
   a. Zeigen Sie die Liste der Top-Klicker an, indem Sie die Registerkarte **Top-Klicker** auswählen.
   b. Zeigen Sie die Details eines Top-Clickers an, indem Sie den Anwendernamenauswählen.

Reverse Whois Integration

Reverse Whois ist ein Service, der Suchen nach Domänennamen durchführt, die von Einzelpersonen oder Organisationen registriert sind.

Führen Sie Domänensuchen mit Suchbegriffen in erkennbaren Elementen durch, die Sie an einen Security Incident anhängen. Die Reverse Whois API durchsucht Domänendatensätze basierend auf den von Ihnen eingegebenen Suchbegriffen und gibt alle Datensätze zurück, die diesen Begriffen entsprechen.

Analysten verwenden diese Integration manchmal zusammen mit der -Integration Whois für die Untersuchung von Security Incidents. Die Whois -Integration bietet zusätzliche Ergänzungsinformationen basierend auf den Domänensuchen aus der Reverse Whois -Integration.

Reverse Whois installieren und konfigurieren

Bevor Sie die -Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit die Anwendung Reverse Whois ordnungsgemäß in das Produkt Security Operations integriert wird.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen ServiceNow Rollen zugewiesen haben.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (admin) installiert die App und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

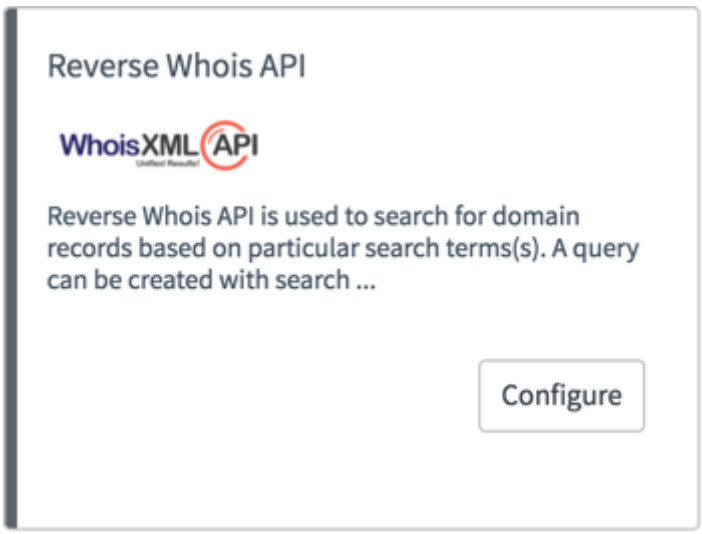
Setupaufgabe	Beschreibung
	• Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration. Der Security Incident-Administrator weist auch die Rolle „Security Incident Analyst“ (sn_si.analyst) zu. • Der Security Incident-Analyst (sn_si.analyst) führt Domänensuchen mit Reverse Whois durch und analysiert und arbeitet mit Security Incidents.
Rufen Sie einen API-Schlüssel ab.	Besuchen Sie die WhoisXML-API-Website, um Informationen zu API-Schlüsseln zu erhalten und ein Konto zu erstellen: WhoisXML-API-Website . Die Konfiguration erfordert die Eingabe der API-Schlüssel.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Madrid- und höher-Release-Anforderungen Für das Madrid-Release und spätere Familienreleases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

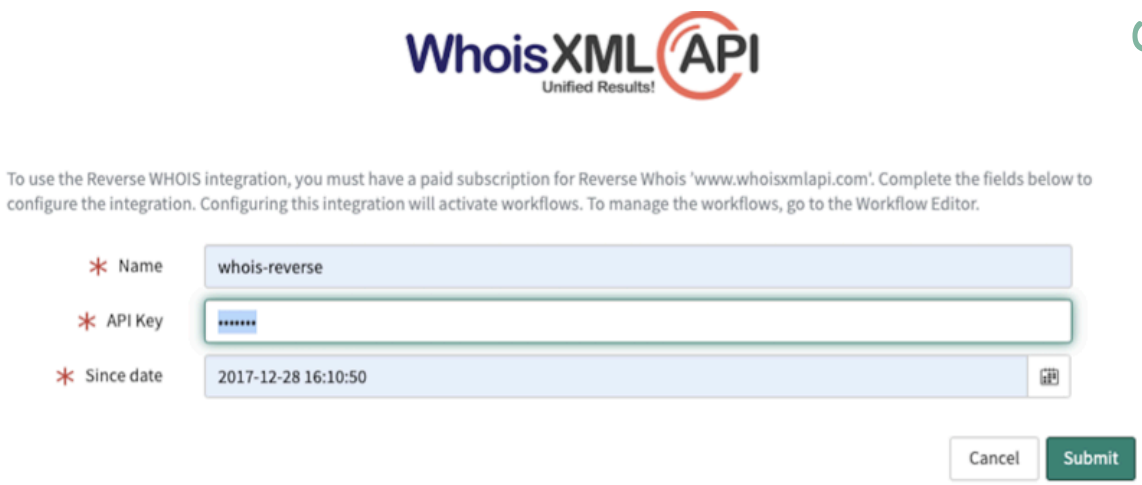
Erforderliche Rolle: Administrator

Prozedur

1. Wenn Sie die Anwendung Reverse Whois bereits installiert und konfiguriert haben, gehen Sie wie folgt vor:
   a. Löschen Sie die vorhandene Konfiguration.
   b. Installieren Sie, und erstellen Sie eine neue Konfiguration mit dem erhaltenen API-Schlüssel.
2. Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
3. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die API-Kachel Reverse Whois.
4. Klicken Sie auf **Konfigurieren**.



5. Geben Sie im Dialogfeld **Reverse Whois API-Konfiguration** den API-Schlüssel ein, den Sie von der XML-API-Website Whois erhalten haben.
6. Wählen Sie eine Option in der folgenden Tabelle aus, um Domänensuchen nach Ihren Suchbegriffen zu filtern.
   Diese Konfigurationseinstellungen bleiben gespeichert, bis Sie sie ändern, und gelten für alle Reverse Whois API-Suchen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Absenden**.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, es wird eine Fehlermeldung angezeigt.

Trouble?
Wenn eine Fehlermeldung angezeigt wird, ist der API-Schlüssel möglicherweise ungültig.

Fehlermeldung

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

(Optional) Installieren und konfigurieren Sie Whois

Installieren Sie das Plugin Whois, um zusätzliche Ergänzungsinformationen für Ihre Domänensuchen in der Reverse Whois API bereitzustellen. Diese Suche liefert zusätzliche Ergänzungsdaten zur Domäne, z. B. das Registrierungsdatum, den Namen der Registrierungsstelle und das Ursprungsland.

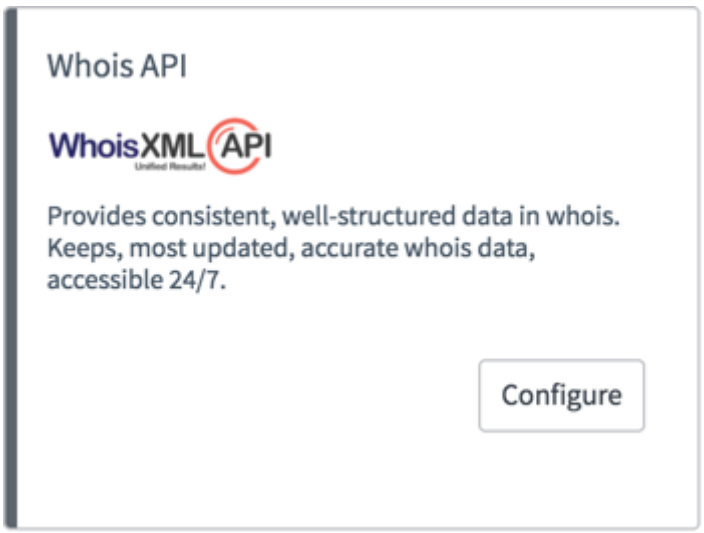
Vorbereitungen

1. Wenn Sie keine Berechtigung für die Anwendung angefordert haben, finden Sie weitere Informationen zur Anwendung WhoisRufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab im ServiceNow Store unter [].
2. Rufen Sie die Anmeldeinformationen für den API-Schlüssel Whois von der Produktwebsite ab: WHOIS-API-Website .

Erforderliche Rolle: Administrator

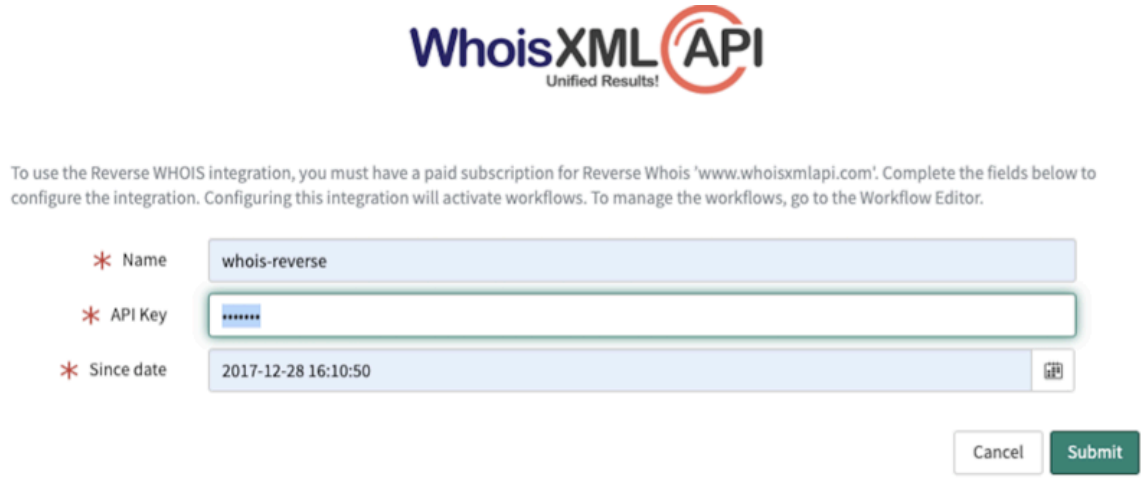
Prozedur

1. Wenn Sie die Anwendung nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration und befolgen Sie die Schritte zur Installation.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die API-Kachel Whois.
3. Klicken Sie auf **Konfigurieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

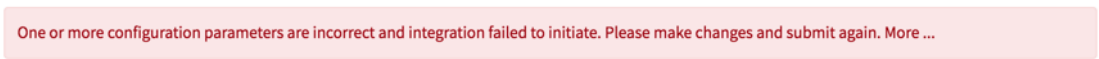
4. Geben Sie im Dialogfeld **Whois-API-Konfiguration** den API-Schlüssel ein, den Sie von der Produktwebsite erhalten haben.



5. Klicken Sie auf **Absenden**.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, es wird eine Fehlermeldung angezeigt. Sie können jetzt Ergänzungssuchen für die von der Reverse Whois -Integration zurückgegebenen Domänen ausführen.

Trouble?
Wenn eine Fehlermeldung angezeigt wird, ist der API-Schlüssel möglicherweise ungültig.

Problembehandlung



Starten Sie die Suche nach Reverse Whois

Initiieren Sie Domänensuchen mithilfe von Suchbegriffen in erkennbaren Elementen, die Sie manuell an einen Security Incident-Datensatz anhängen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

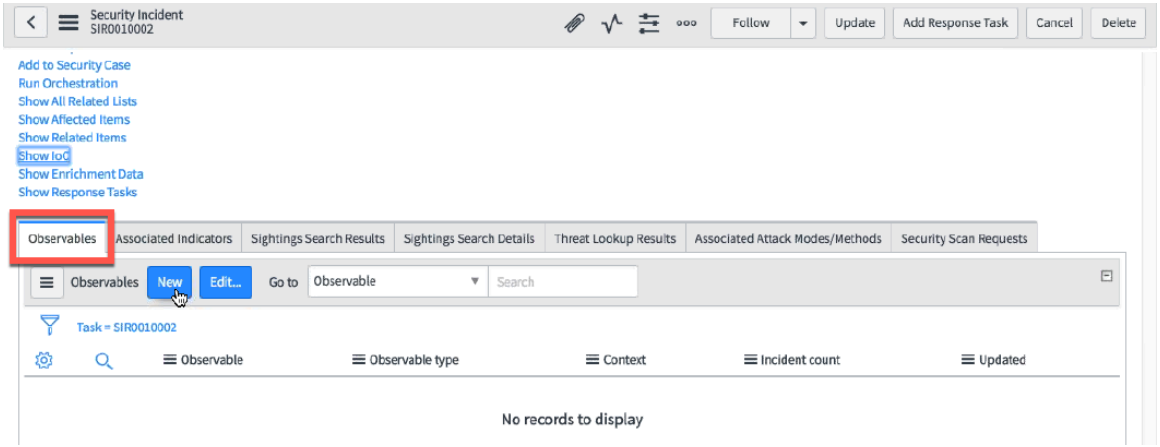
Prozedur

1. Wenn nicht geöffnet, navigieren Sie zu **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie den Security Incident, mit dem Sie arbeiten.
2. Klicken Sie unten im Datensatz auf den zugehörigen Link **IoC anzeigen**, um die Registerkarte Erkennbare Elemente anzuzeigen.

Hinweis:
Die Abbildungen in den folgenden Schritten werden mit aktivierter Einstellung **für Formulare mit Registerkarten** in den Systemeinstellungen angezeigt. Wenn für den Security Incident keine Registerkarten angezeigt werden, klicken Sie in der oberen rechten Ecke des Bannerframes auf das Zahnradsymbol **Einstellungen**. Klicken Sie im angezeigten Dialogfeld **„Systemeinstellungen“** auf **Formulare**, und vergewissern Sie sich, dass **Formulare mit Registerkarten** und **Mit Formular** ausgewählt sind.

Automatische Übersetzung

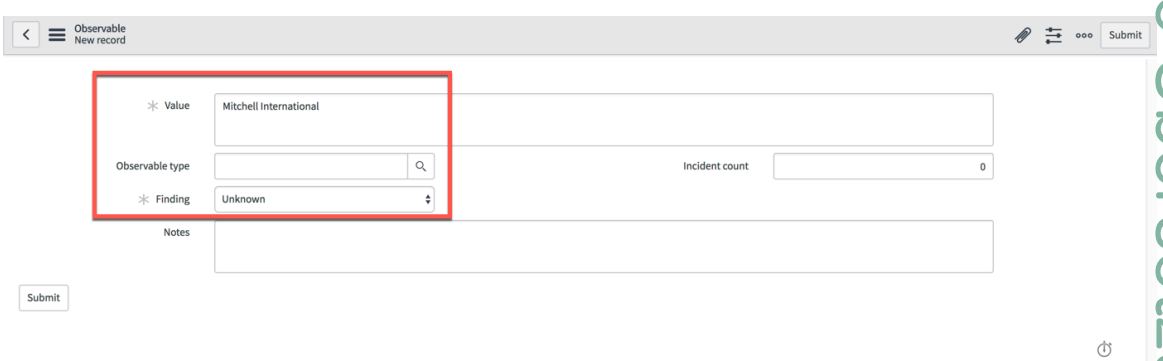
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf der Registerkarte Erkennbare Elemente **auf Neu**.
4. Füllen Sie die Felder aus.

Pflichtfelder im neuen Datensatz

Feld	Beschreibung
Wert	Eindeutiger Suchbegriff für eine Domäne.
Erkennbarer Typ	Dieses Feld wird automatisch gelöscht.
Ergebnis	Dieses Feld wird automatisch auf **Unbekannt**festgelegt.



5. Klicken Sie auf **Absenden**.
   Sie kehren zum Security Incident-Datensatz zurück, und der Flow initiiert die Suche.

Nächste Maßnahme

Überprüfen Sie die Suchergebnisse für den Security Incident. Weitere Informationen finden Sie unter Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois.

Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois

Datenanreicherungs-Ergebnisse werden auf der Registerkarte **ReverseWhais-Domänen** unten im Security Incident-Datensatz angezeigt. Suchen Sie die Suchergebnisse, um zu überprüfen, ob die Suche erfolgreich ausgeführt wurde.

Vorbereitungen

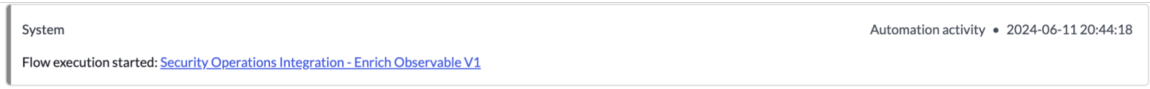
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

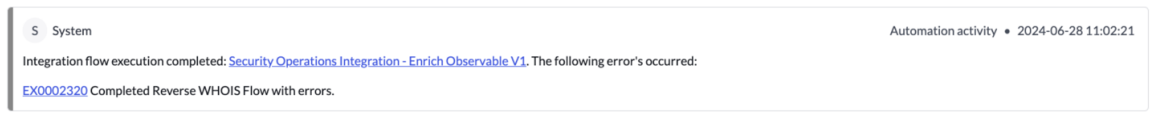
Prozedur

1. Wenn er noch nicht geöffnet ist, navigieren Sie zu **Security Incidents** > **Incidents** > **Alle Incidents anzeigen** und suchen Sie den Security Incident, mit dem Sie arbeiten.



Nachdem die Anwendung konfiguriert ist und Sie ein erkennbares Element angehängt haben, wird der Flow automatisch gestartet. Die Arbeitsnotizen im Security Incident-Datensatz zeigen den Ausführungs- und Abschlussstatus der Suche an.

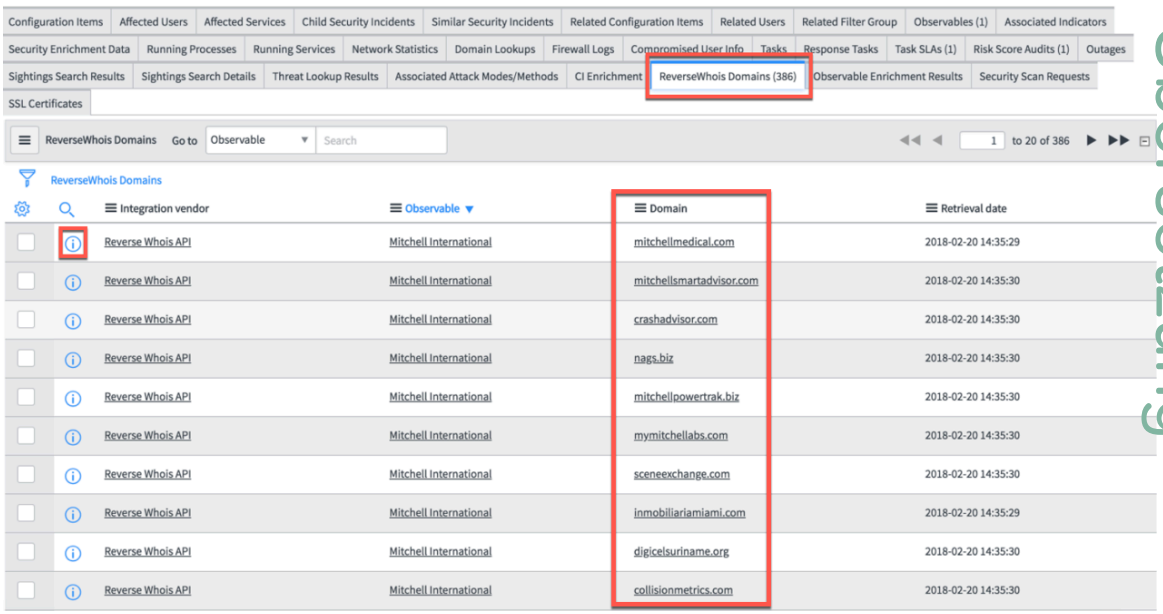
2. Wenn Sie nicht verifizieren können, dass die Suche erfolgreich ausgeführt wurde, lesen Sie die Arbeitsnotizen, um weitere Informationen zum weiteren Vorgehen zu erhalten.



3. Navigieren Sie zum Ende des Security Incidents, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**.

Hinweis:

Für die in der folgenden Abbildung gezeigten gefilterten Suchergebnisse wurden die Konfigurationseinstellungen auf der API-Konfigurationskachel Reverse Whois gespeichert, wobei im Feld **Seit Datum** das Datum **1991-06-01** eingegeben wurde.

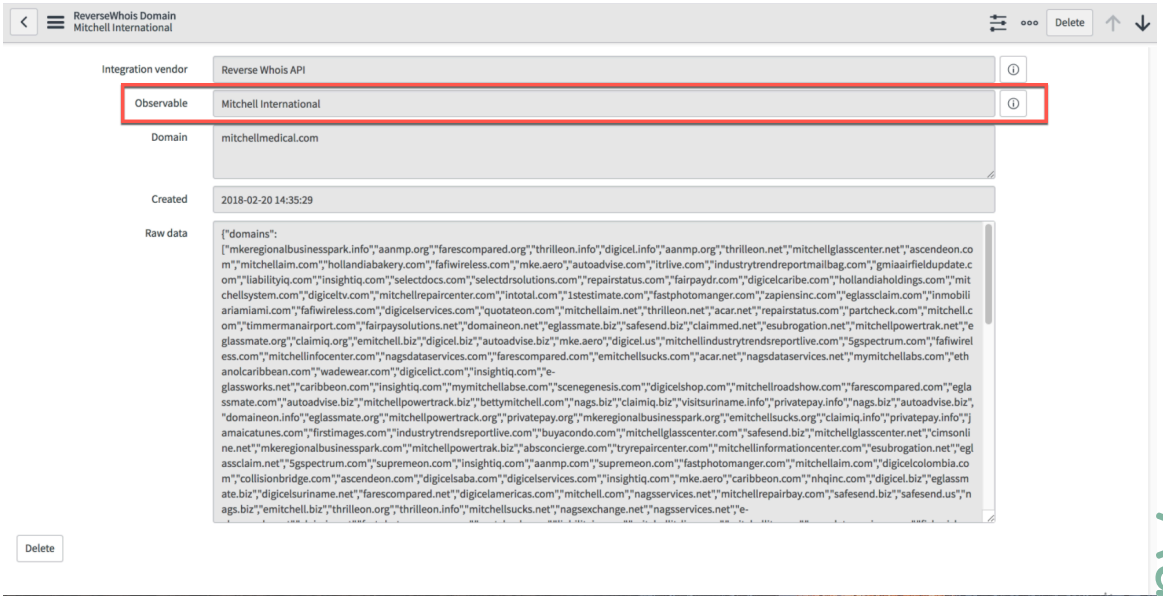


Datenanreicherungs-Ergebnisse werden auf der Registerkarte **ReverseWhais-Domänen** angezeigt. Die aktiven Domänen für dieses erkennbare Element werden in der Spalte **„Domäne“** angezeigt.

4. Klicken Sie auf das blaue Informationssymbol neben einem Element, und klicken Sie dann im angezeigten Dialogfeld **auf Datensatz öffnen**.

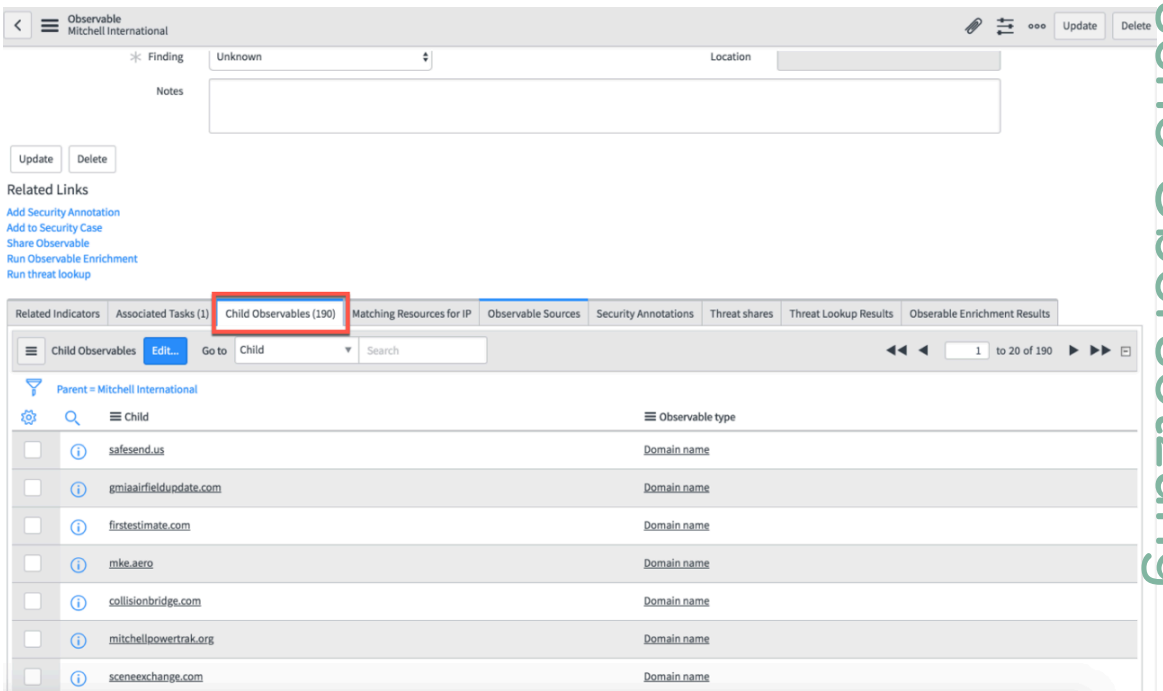
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Datensatz wird mit Ergänzungsdetails angezeigt, einschließlich der Rohdaten.

5. Navigieren Sie zurück zum Security Incident, und klicken Sie bei ausgewählter Registerkarte **ReverseWhais-Domänen** auf ein erkennbares Element in der Spalte **Erkennbares** Element, um einen Datensatz zu öffnen.



Die untergeordneten erkennbaren Elemente werden auf der Registerkarte **Untergeordnete erkennbare Elemente im Datensatz des erkennbaren Elements** angezeigt. Die untergeordneten erkennbaren Elemente werden nur generiert, wenn die Anwendung Reverse Whois Domänen zurückgegeben hat.

Trouble?

Wenn die Suche nicht erfolgreich abgeschlossen wird, überprüfen Sie, ob die von Ihnen eingegebenen Suchbegriffe von der Integration unterstützt werden. Weitere Informationen finden Sie in den Arbeitsnotizen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Um weitere Ergänzungsdaten zu den Ergebnissen der Domänensuche zu erhalten, können Sie die Integration Whois ausführen, um Ergänzungssuchen für die von der Integration Reverse Whois zurückgegebenen untergeordneten erkennbaren Elemente durchzuführen. Diese Ergänzungsdaten zu den untergeordneten erkennbaren Elementen enthalten Informationen zum Registrierungsdatum, zum Namen der Registrierungsstelle und zum Herkunftsland.

(Optional) Führen Sie eine Ergänzungssuche durch, und überprüfen Sie die erwarteten Ergebnisse für Whois

Führen Sie die Whois -Integration aus, um Ergänzungssuchen für die von der Reverse Whois -Integration zurückgegebenen Domänen durchzuführen.

Vorbereitungen

Stellen Sie sicher, dass Sie die Plugins Reverse Whois und Whois installiert und konfiguriert haben. Führen Sie diese Schritte erst aus, nachdem Sie die Domänensuche mit dem Plugin Reverse Whois erfolgreich ausgeführt haben.

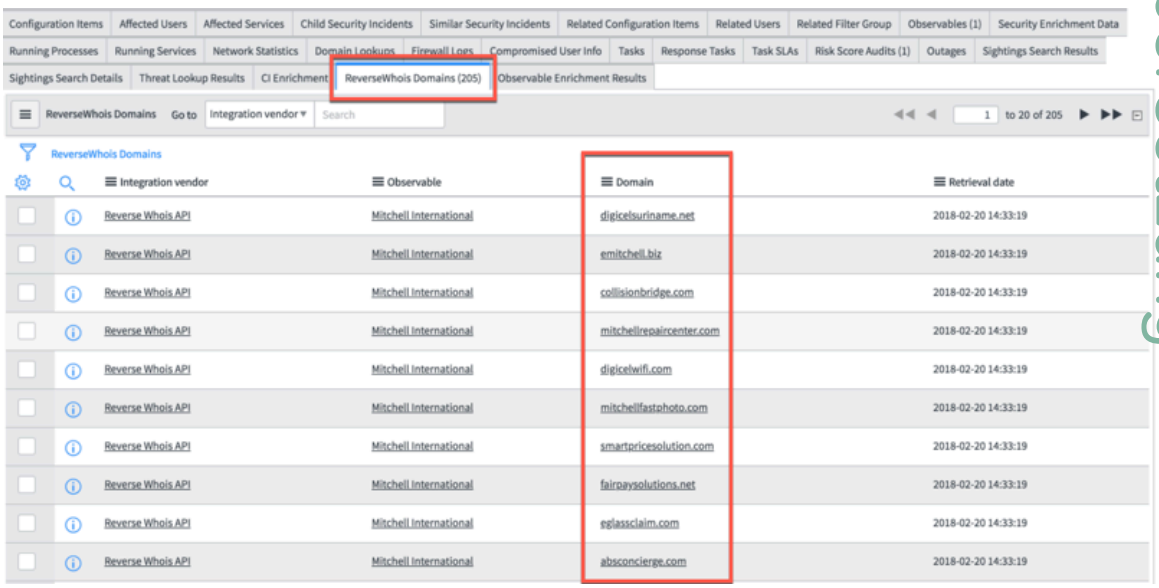
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Ergebnisse werden auf der Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente** im Datensatz erkennbarer Elemente angezeigt.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Incidents** > **Alle Incidents anzeigen** und suchen Sie den Security Incident, mit dem Sie arbeiten und der die Domänensuche erfolgreich ausgeführt hat.
2. Öffnen Sie den Datensatz, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**.
3. Wählen Sie die Registerkarte **Reverse Whois Domains (Whois-Domänen umkehren)** am unteren Rand des Datensatzes.

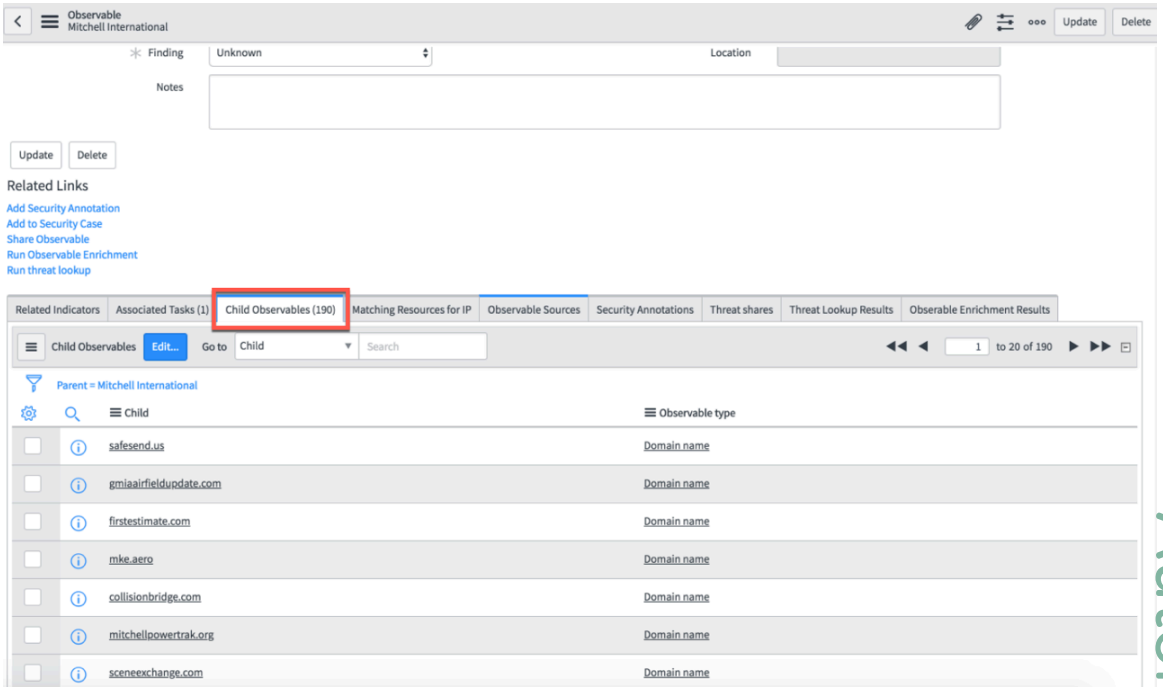


In der Spalte **Domänen** wird die Liste der zurückgegebenen Domänen angezeigt.

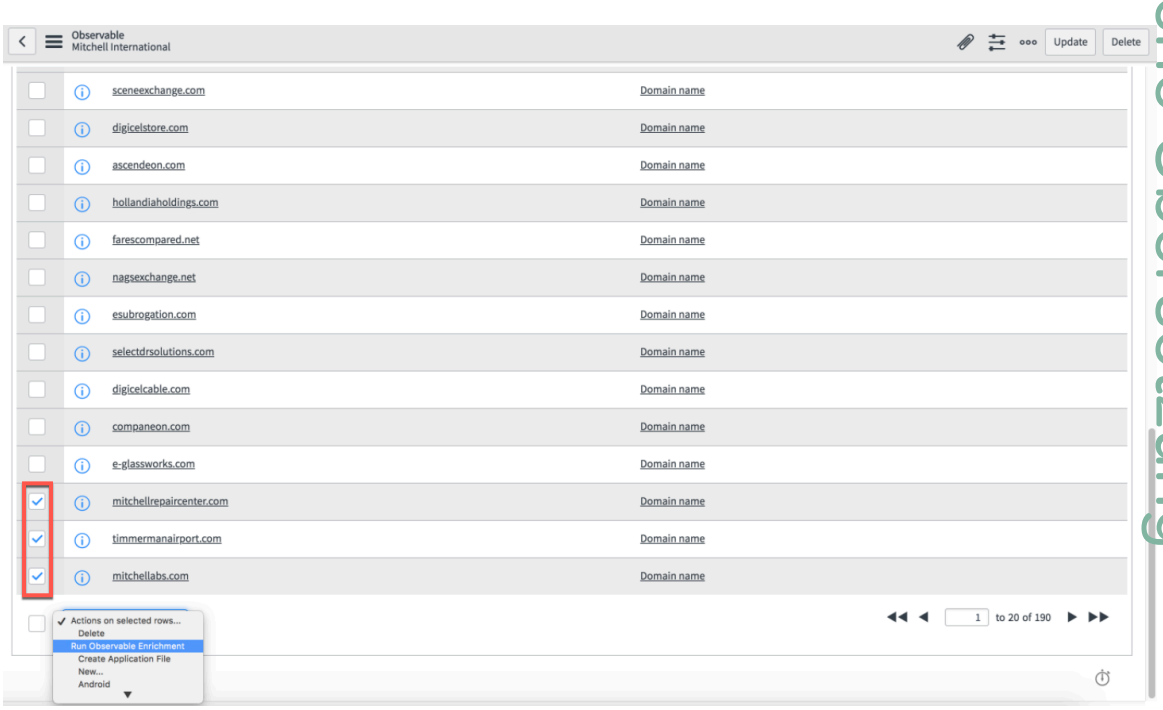
4. Klicken Sie in der Spalte **Erkennbares** Element auf ein erkennbares Element.
   Auf der Registerkarte **Untergeordnete erkennbare Elemente** werden die untergeordneten erkennbaren Elemente angezeigt. Die untergeordneten erkennbaren Elemente werden nur generiert, wenn der erste Scan des erkennbaren Elements durch die Anwendung Reverse Whois Domänen zurückgegeben hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie die untergeordneten erkennbaren Elemente aus, für die Sie die Ergänzung erkennbarer Elemente ausführen möchten, und wählen Sie in der Auswahlliste **Aktion für ausgewählte Zeilendie Option Ergänzung erkennbarer Elemente ausführen aus**.

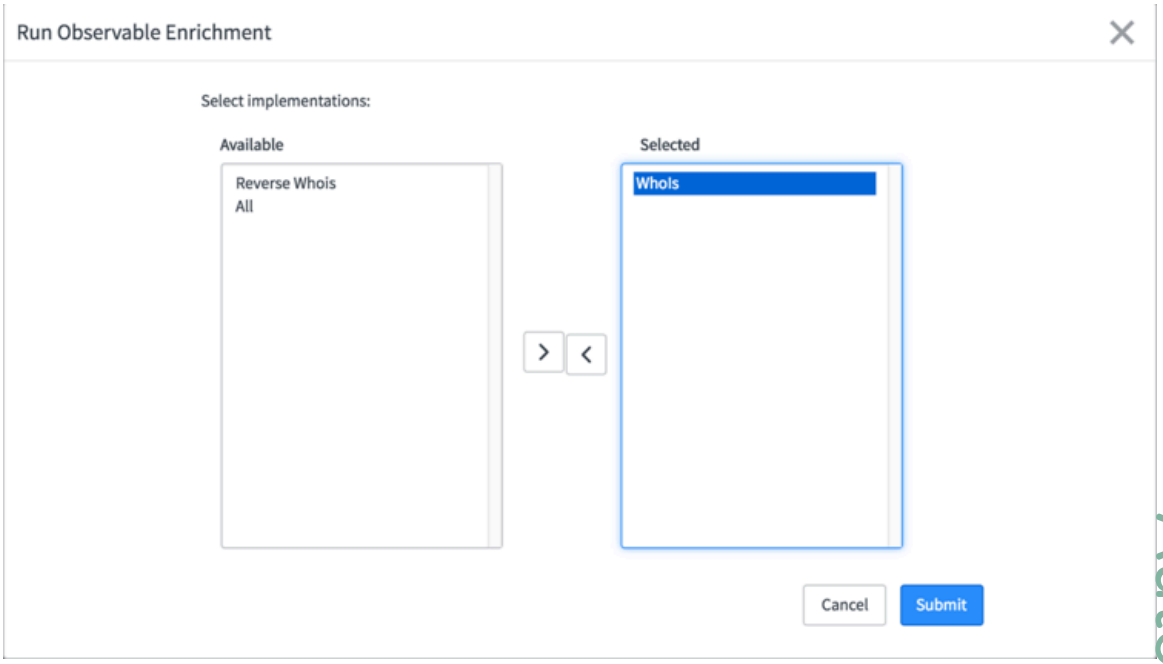


Das Dialogfeld **„Anreicherung erkennbarer Elemente durchführen“** wird angezeigt.

6. Verschieben Sie die Integration Whois von **Verfügbar** zu **Ausgewählt**, und klicken Sie auf **Absenden**.

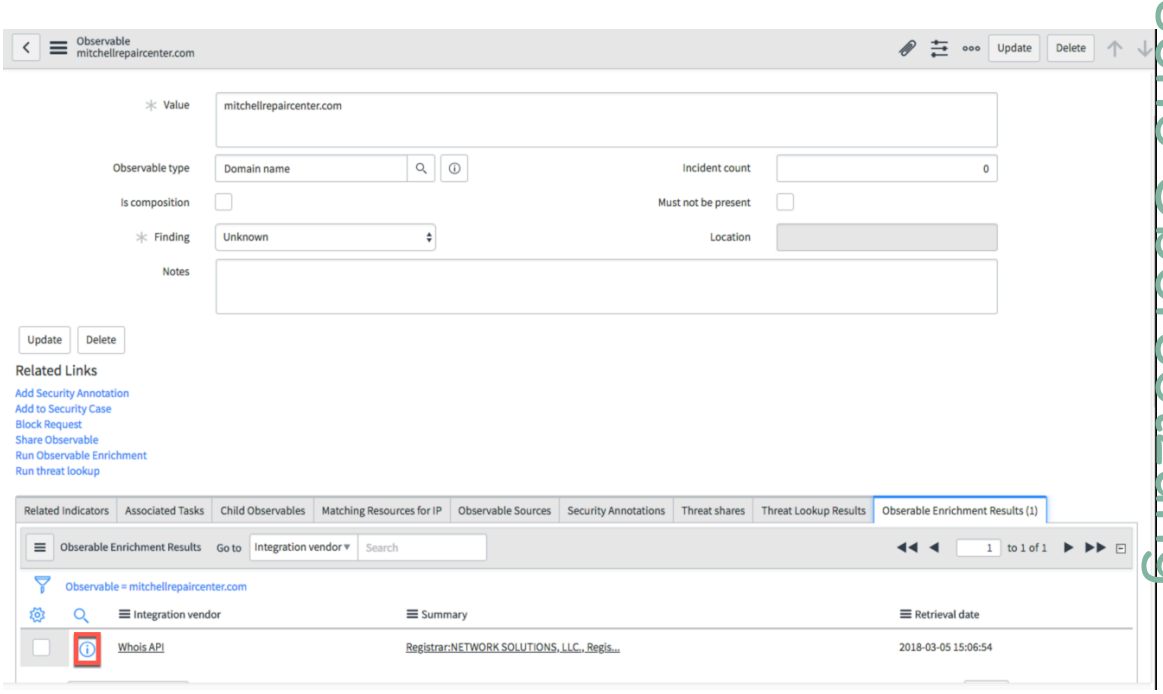
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ergebnisse werden auf der Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente** des Datensatzes erkennbarer Elemente angezeigt.

7. Klicken Sie auf das blaue Informationssymbol und dann im angezeigten Dialogfeld **auf Datensatz öffnen**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen und Rohdaten im Zusammenhang mit der ursprünglichen Domänensuche werden angezeigt, z. B. Registrierungsdatum, Name des Registrators und Ursprungsland.

Trouble?
Wenn Sie keine untergeordneten erkennbaren Elemente oder Ergänzungsergebnisse finden können, überprüfen Sie, ob die Reverse Whois -Integration erfolgreich ausgeführt wurde und Domänen zurückgegeben hat. Weitere Informationen finden Sie auch in den Arbeitsnotizen im Datensatz.

Zugehörige Informationen

Reverse Whois installieren und konfigurieren

Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois

Integration von RISKIQ und WHOISIQ

Durch die Integration der APIs RISKIQ und WHOISIQ mit dem Produkt Now Platform® Security Operations erhalten Sicherheitsanalysten zusätzliche Ergänzungsdaten und Einblicke in die Gültigkeit von Websites.

Die RISKIQ SSL Certificates API führt Suchvorgänge für SSL-Zertifikate durch, die Details zur ausstellenden Zertifizierungsstelle, zu den Organisationen, die Zertifikate anfordern, zu den Entitäten, für die Zertifikate ausgestellt werden, und zur Domäne enthalten. SSL-Zertifikatsuchen werden automatisch durchgeführt, wenn Security Incidents erstellt werden.

Die RISKIQ WHOISIQ -API führt Suchen nach anderen erkennbaren Elementen wie Domäne, E-Mail, Nameserver, Organisation, Adresse und Telefonnummer durch. Erkennbare URL- und Domänenelemente werden automatisch angereichert, wenn Security Incidents erstellt werden.

Für die -Integration sind die Produkte Security Incident Response und Threat Intelligence erforderlich.

Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

Die RISKIQ -API unterstützt die automatische SSL-Zertifikatsuche für erkennbare Elemente wie IP-Adresse, Datei-Hash, Zertifikat-Seriennummer, Domäne und URL. Erkennbare URL- und Domänenelemente werden automatisch mit der WHOISIQ -API angereichert. Zur Ergänzung erkennbarer Elemente für andere Arten von erkennbaren Elementen mit der API WHOISIQ erstellen Sie erkennbare Elemente, und führen Sie Suchvorgänge manuell in der Tabelle „Erkennbare Elemente“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte erkennbare Elemente

In der folgenden Tabelle sind der Typ der in dieser Integration verwendeten APIs und die erkennbaren Elemente aufgeführt, die jede API unterstützt. Die Tabelle gibt auch an, ob eine Suche automatisch erfolgt, wenn Security Incidents erstellt werden, oder ob die Suche manuell über die Tabelle „Erkennbare Elemente“ ausgeführt wird.

Unterstützte erkennbare Elemente und Suche

API	Unterstützte erkennbare Elemente	Suche (automatisiert oder manuell)
RISKIQ SSL-Zertifikat-API	• IP-Adresse • Datei-Hash (Fingerabdruck des Zertifikats). In der folgenden Abbildung finden Sie ein Beispiel für einen Datei-Hash. • Seriennummer des Zertifikats oder Seriennummer. Diese Zeichenfolge ist eine eindeutige ID für die Entität. In der folgenden Abbildung finden Sie ein Beispiel für eine Zertifikat-Seriennummer. • Domäne (www.site.comoder Site.com) • URL **Hinweis:** Für das URL-Format werden automatische Scans mit dem Protokoll https:// ausgeführt, z. B. https://example.com/index.html	Automatisierte Suche beim Erstellen von Incidents Die Ergebnisse werden auf der Registerkarte **SSL-Zertifikate** des Security Incident-Datensatzes angezeigt.
RISKIQ WHOISIQ API	• Domäne • URL	Automatisierte Suche beim Erstellen von Incidents Die Ergebnisse werden auf der Registerkarte **„Datenanreicherungs-Ergebnisse erkennbarer Elemente“** im Security Incident-Datensatz angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte erkennbare Elemente und Suche (Fortsetzung)

API	Unterstützte erkennbare Elemente	Suche (automatisiert oder manuell)
RISKIQ WHOISIQ API	• E-Mail-Adresse • Organisationsname • Telefonnummer • Postanschrift	Die manuelle Suche wird in der Tabelle „Erkennbare Elemente“ ausgeführt. Ergebnisse werden auf der Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente** im Datensatz erkennbarer Elemente angezeigt.

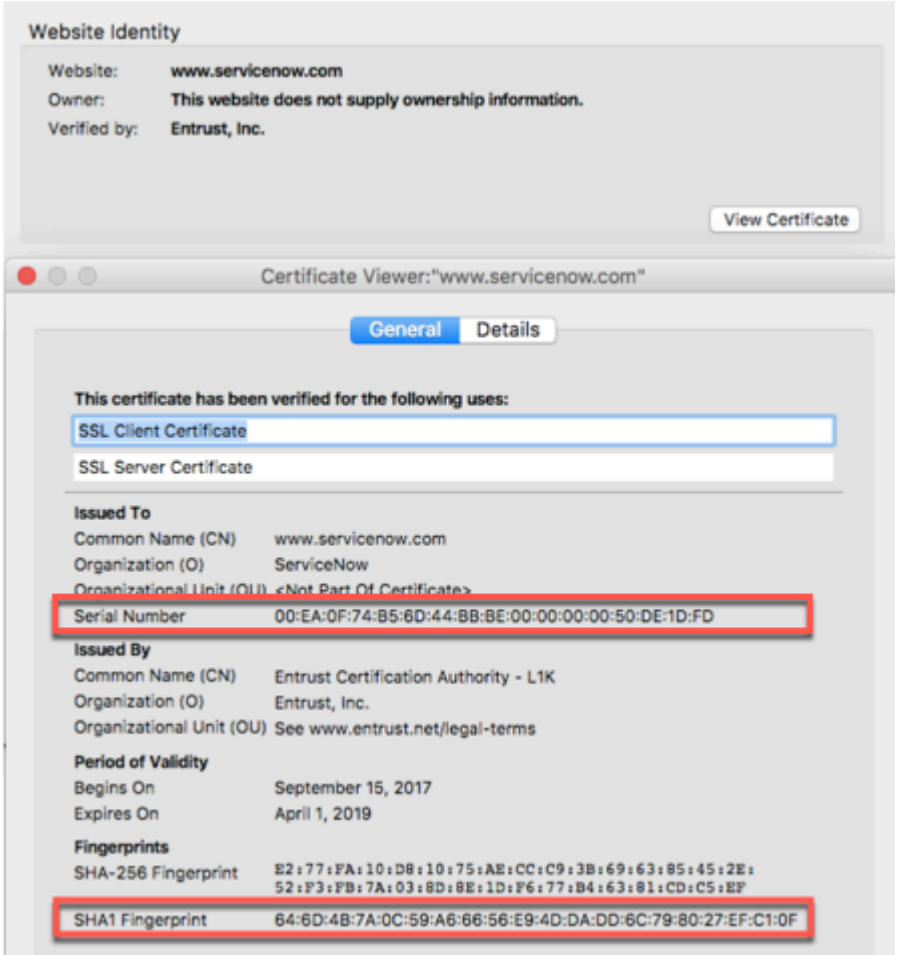
Beispiel für einen Datei-Hash und die Seriennummer des Zertifikats

Diese Abbildung zeigt ein Beispiel für die erkennbaren Elemente Datei-Hash und Zertifikat-Seriennummer, die für die SSL-Zertifikatsuchen für diese Integration verwendet werden. Der Datei-Hash bezieht sich auf einen SHA-1-Fingerabdruck. Dieser Wert wird in Ihrer Instanz Now Platform ohne Doppelpunkttrennzeichen angezeigt. Beispiel: 646D4B7A0C59A66656E94DDADD6C798027EFC10F.

Das erkennbare Element der Zertifikatseriennummer bezieht sich auf die eindeutige ID oder Seriennummer für die Entität. Dieser Wert wird auch ohne Doppelpunkttrennzeichen angezeigt. Beispiel: 00EA0F74B56D44BBBE0000000050DE1DFD.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datei-Hash und Seriennummer des Zertifikats



RISKIQ und WHOISIQinstallieren und konfigurieren

Bevor Sie die Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit die Anwendungen RISKIQ und WHOISIQ ordnungsgemäß in Now Platform Security Operationsintegriert werden können.

Vorbereitungen

Erforderliche Rolle: admin, RISKIQ und WHOISIQ admin.

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen zugewiesen haben.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (admin) installiert die App und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf

Automatische Übersetzung

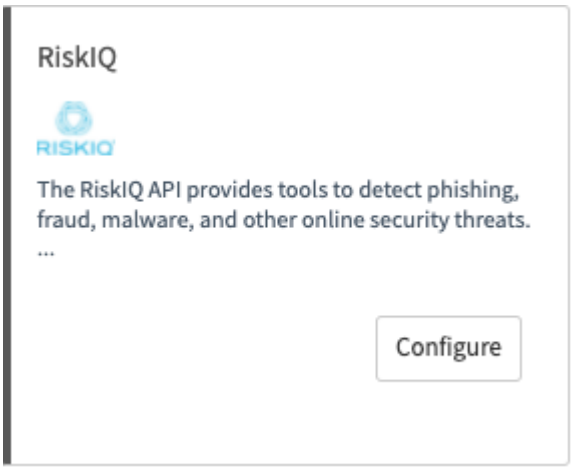
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	das Modul Security Operations und weist die Rolle „Security Incident Analyst“ (sn_si.analyst) zu. • Der Security Incident-Analyst (sn_si.analyst) arbeitet mit Security Incident-Datensätzen.
Rufen Sie einen Anwendernamen und einen API-Schlüssel ab.	Informationen zum API-Schlüssel und zur Erstellung eines Kontos finden Sie auf der Website RISKIQ-Website. Die Konfiguration erfordert die Eingabe des API-Schlüssels.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Madrid- und höher-Release-Anforderungen Für das Madrid-Release und spätere Familienreleases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

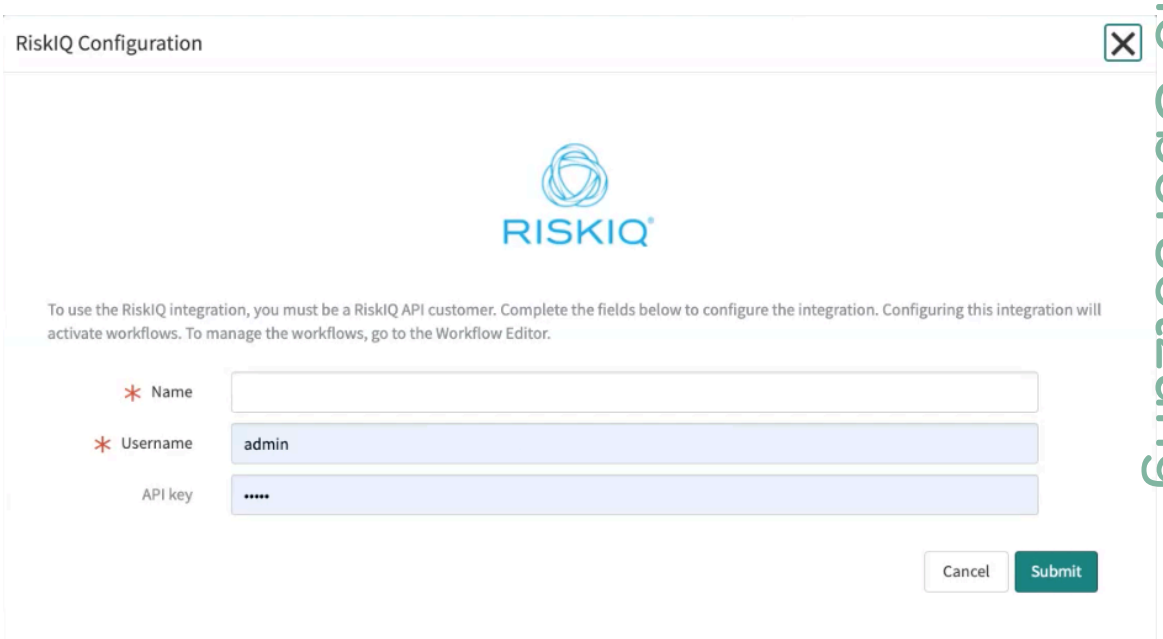
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen** und suchen Sie die API-Kachel.
3. Klicken Sie auf **Konfigurieren**.



4. Geben Sie im angezeigten Dialogfeld RiskIQ Configuration (RisikoIQ-Konfiguration) den **Anwendernamen** und **den API-Schlüssel**ein.



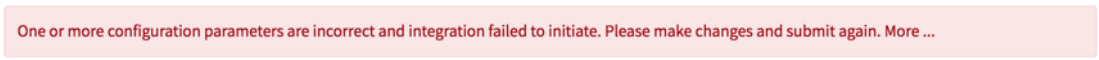
5. Klicken Sie auf **Absenden**.
6. Überprüfen Sie die erfolgreiche Konfiguration.
   Wenn die Konfiguration erfolgreich abgeschlossen wurde, wird die Seite „Security Integrations“ (Sicherheitsintegrationen) mit den Integrationskacheln angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?
Wenn eine Fehlermeldung angezeigt wird, ist der Anwendername oder API-Schlüssel möglicherweise ungültig. Stellen Sie sicher, dass Ihr Anwendername und API-Schlüssel korrekt sind:

Problembehandlung



Überprüfen Sie die erwarteten Ergebnisse für RISKIQ SSL-Zertifikatsuchen

Wenn ein Security Incident erkennbare Elemente für URLs, Domänen, IP-Adressen, Hashes der Zertifikatdatei (SHA-1-Fingerabdruck) und Seriennummern des Zertifikats generiert, verwenden Security Incident-Analysten die Ergebnisse der SSL-Zertifikatsuche, um zu überprüfen, ob Sites über Zertifikate verfügen, die von einer vertrauenswürdigen Person ausgestellt wurden Zertifizierungsstelle (Certificate Authority, CA).

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Bei unterstützten erkennbaren Elementen sucht Now Platform nach dem neuesten Vorkommen von URLs, Domänen, IP-Adressen, Zertifikatdatei-Hashes (SHA-1-Fingerabdruck) und Zertifikatseriennummern. Dies sind mögliche Ergebnisse der Prüfung:

Es wurde eine exakte Übereinstimmung gefunden

Ein gültiger Aussteller eines SSL-Zertifikats wird im Security Incident-Datensatz aufgeführt.

Es wurden keine Zertifikatergebnisse gefunden

Im Security Incident-Datensatz sind keine Ergebnisse aufgeführt.

Es wurde eine exakte Übereinstimmung für ein selbstsigniertes oder intern generiertes Zertifikat gefunden

Ergebnisse für ein intern generiertes SSL-Zertifikat werden im Security Incident-Datensatz angezeigt.

Für ein primäres SSL-Zertifikat wurde keine exakte Übereinstimmung gefunden

Ein Suchwert gibt mehrere Einträge zurück, und ein primäres Zertifikat kann nicht identifiziert werden. Im Security Incident-Datensatz wird eine Zusammenfassungsmeldung angezeigt.

Prozedur

1. Um die erkennbaren Elemente anzuzeigen und Suchergebnisse zu überprüfen, öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und suchen Sie die Arbeitsnotizen.

   Example
   Um Beispiele für die möglichen Suchergebnisse für diese Integration zu veranschaulichen, nehmen wir an, dass ein Security Incident mit den folgenden erkennbaren Elementen generiert wurde:

   - community.servicenow.com
   - invalidsubdomain.servicenow.com
   - mail.dgnetworks.com
   - servicenow.com

Automatische Übersetzung

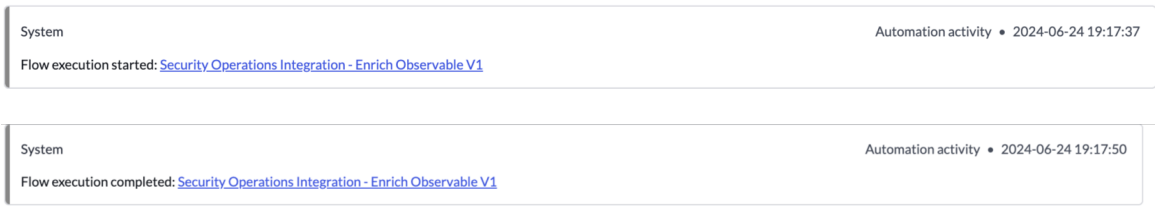
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennbare Elemente und Ort der Suchergebnisse

Erkennbares Element (Beispiel)	Scan-Ergebnisse	Beschreibung und Speicherort
Community.serviceNow.com	Zertifikat mit einem SHA1-Hash gefunden.	Es wird eine exakte Übereinstimmung gefunden, und ein gültiger Aussteller eines SSL-Zertifikats wird aufgelistet. Die Ergebnisse für die genaue Übereinstimmung werden auf der Registerkarte **SSL-Zertifikate** im Datensatz „Security Incident“ angezeigt.
ungültigesubdomäne.servicenow.com	Keine Zertifikate gefunden.	Auf der Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente** im Datensatz des Security Incidents wird eine Zusammenfassung angezeigt, die angibt, dass keine Zertifikatergebnisse gefunden wurden.
Mail.dnetworks.com	Zertifikat mit SHA1-Hash gefunden.	Eine genaue Übereinstimmung wird für ein selbstsigniertes oder intern generiertes Zertifikat aufgelistet. Die Ergebnisse werden auf der Registerkarte **„SSL-Zertifikate“** im Security Incident-Datensatz angezeigt.
servicenow.com	Die Suche ergab 138 Zertifikate, und ein einzelnes primäres Zertifikat konnte nicht identifiziert werden.	Für ein primäres SSL-Zertifikat wurde keine exakte Übereinstimmung gefunden, da ein Suchwert mehrere Zertifikate zurückgibt. Auf der Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer** Elemente im Datensatz des Security Incidents wird eine Zusammenfassung angezeigt, die angibt, dass kein primäres Zertifikat gefunden wurde.

Nachdem die Anwendung konfiguriert wurde, wird der Flow automatisch gestartet. Der Suchstatus und die erkennbaren Elemente werden in den Arbeitsnotizen angezeigt.

2. Vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?
Wenn Sie die erwarteten Ergebnisse nicht anzeigen können, überprüfen Sie, ob das erkennbare Element von der SSL-Zertifikatsuche für die Integration unterstützt wird.

Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

RISKIQ SSL-Zertifikatsuchen, die eine genaue Übereinstimmung zurückgeben

RISKIQ Die Ergebnisse der SSL-Zertifikatsuche für eine genaue Übereinstimmung werden auf der Registerkarte **SSL-Zertifikate** im Datensatz des Security Incidents angezeigt. Eine genaue Übereinstimmung liefert einen gültigen Zertifizierungsstellennamen, anhand dessen ein Security Incident-Analyst die Gültigkeit einer Website bestimmen kann.

Example: Genaue Übereinstimmung mit einem gültigen SSL-Zertifikat

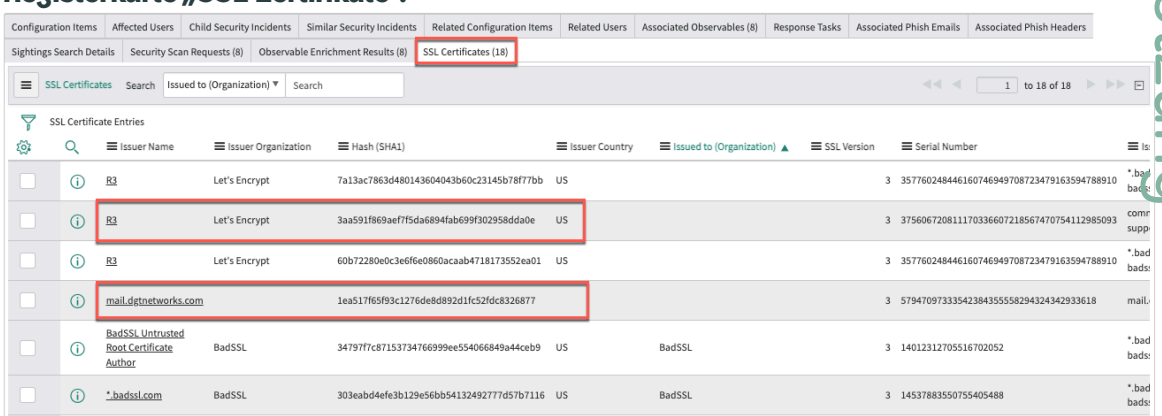
Das folgende Beispiel zeigt einen gültigen Aussteller eines SSL-Zertifikats aus einer genauen Übereinstimmung in den Suchergebnissen. Führen Sie die Schritte aus, um die Ergebnisse und Rohdaten anzuzeigen.

Hinweis:
Die Abbildungen in den folgenden Beispielen werden mit aktivierter Einstellung **für Formulare mit Registerkarten** in den Systemeinstellungen angezeigt. Wenn Ihr Bildschirm nicht mit der unten gezeigten Ansicht übereinstimmt, befolgen Sie die Schritte zum Festlegen von Formularen mit Registerkarten.

1. Klicken Sie in der oberen rechten Ecke des Bannerframes auf das Symbol Einstellungen.
2. Klicken Sie im angezeigten Dialogfeld **„Systemeinstellungen“** auf **Formulare**, und vergewissern Sie sich, dass **Formulare mit Registerkarten** und **Mit Formular** ausgewählt sind.

1. Klicken Sie im Datensatz des Security Incident auf die Registerkarte **SSL-Zertifikate**.

Registerkarte „SSL-Zertifikate“.



Informationen über den Namen des Zertifikatausstellers, die Organisation des Ausstellers und den Besitzer des Zertifikats (Organisation) werden zusammen mit anderen Daten angezeigt.

In der Spalte **Ausstellername** werden 18 Elemente angezeigt. Das zweite Element (R3) gibt einen gültigen Zertifizierungsstellennamen (Let's Encrypt) in der Spalte **Ausstellerorganisation** an.

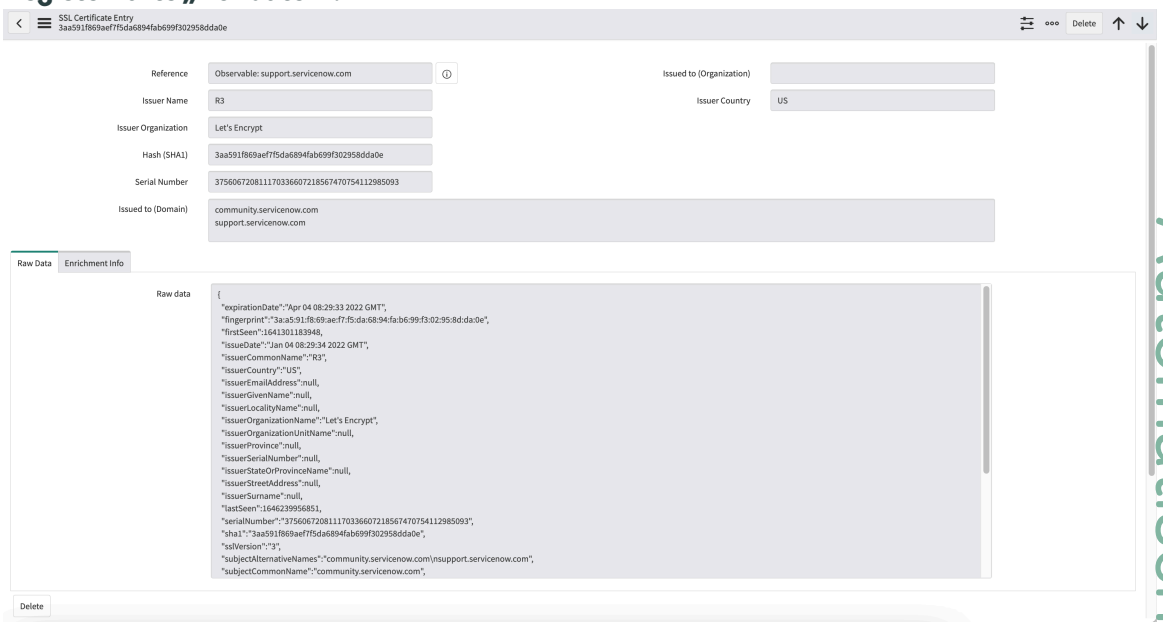
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für das zweite Element (mail.dgtnetworks.com) werden in den Spalten **Ausstellerorganisation** und **Ausgestellt an**keine Informationen angezeigt.

2. Klicken Sie auf das zweite Element in der Spalte **Ausstellername**(**R3**), um den Eintragsdatensatz zu öffnen. Alternativ klicken Sie auf das Informationssymbol neben dem Element und anschließend auf **Datensatz öffnen**.
3. Wählen Sie die Registerkarte **Rohdaten**.

Registerkarte „Rohdaten“.



Der Datensatz „SSL-Zertifikateintrag“ enthält das erkennbare Element auf der Registerkarte **Rohdaten** unter der Spalte **Entitätsname** sowie andere Daten.

Beachten Sie, dass in der Spalte **Kategorie**, Betreffund Aussteller erkennbaren Entitäten in der Spalte **Entitätsname** entsprechen. Der Aussteller dieses Zertifikats ist höchstwahrscheinlich gültig und stammt von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle. Beachten Sie auch, dass der Betreffund der Aussteller unterschiedliche Entitäten sind. Diese separaten Entitäten zeigen an, dass das Zertifikat kein intern signiertes Zertifikat einer unbekannten Zertifizierungsstelle ist.

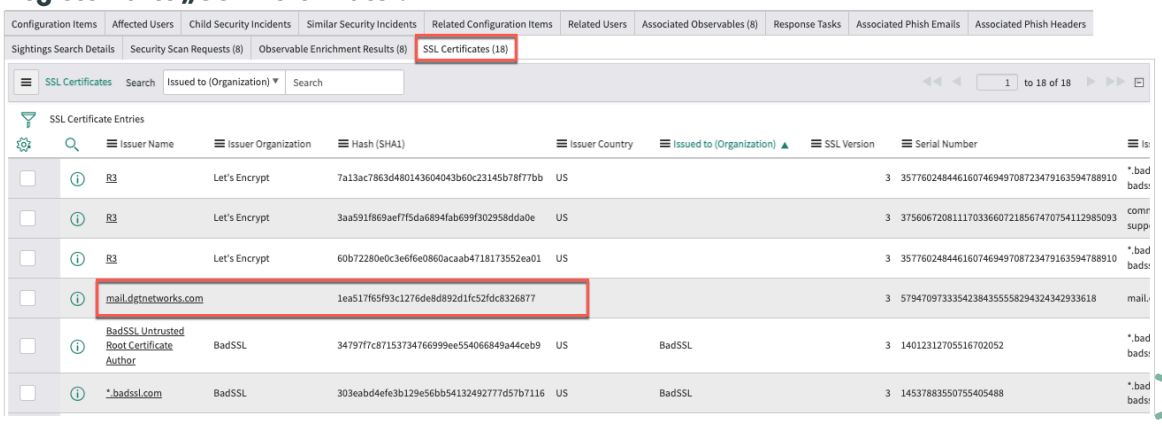
Example: Genaue Übereinstimmung für ein selbstsigniertes SSL-Zertifikat

Das folgende Beispiel zeigt Ergebnisse für ein selbstsigniertes SSL-Zertifikat aus der -Suche. Führen Sie die Schritte aus, um die Ergebnisse und Rohdaten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

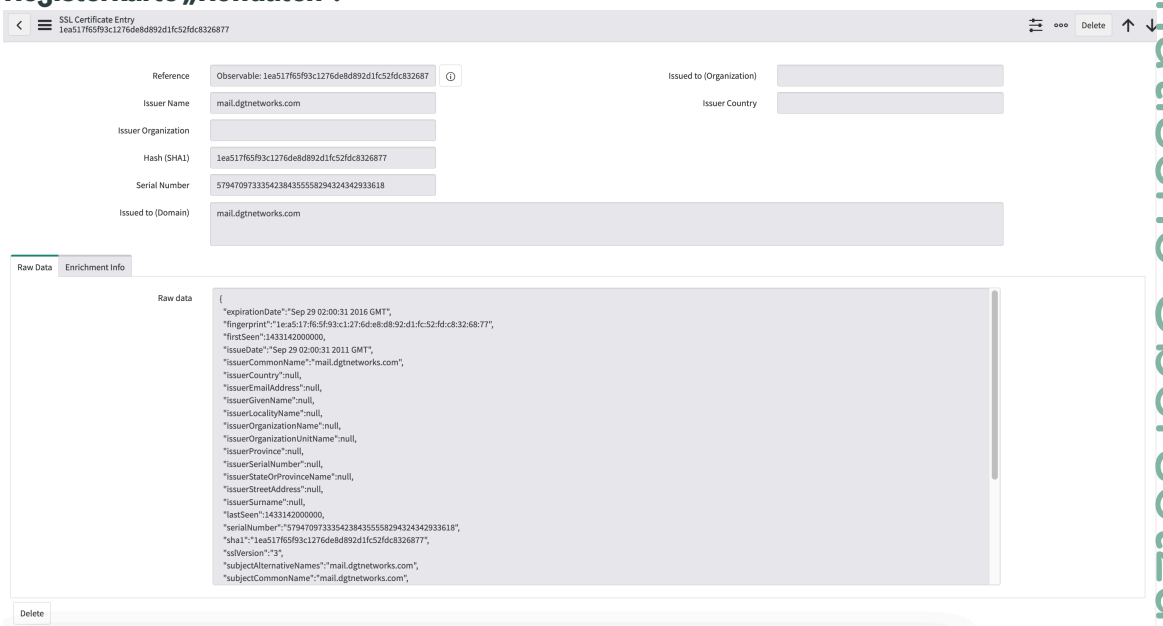
1. Navigieren Sie zurück zum Security Incident-Datensatz. Klicken Sie in der Spalte **Ausstellername** auf das andere Element (**mail.dgtnetworks.com**).

Registerkarte „SSL-Zertifikate“.



2. Wählen Sie im geöffneten Datensatz die Registerkarte **Rohdaten**.

Registerkarte „Rohdaten“.



Die Spalte **„Kategorie“** gibt an, dass der Aussteller (mail.dgtnetworks.com und dgtsbs.DgtNetworks.local) keine vertrauenswürdigen öffentlichen Zertifizierungsstellen sind. Beachten Sie auch, dass Aussteller und Betreff dieselbe Entität sind (dgtsbs.DgtNetworks.local) und jeweils den Namen des erkennbaren Elements (dgtsbs) enthalten. Dieses Zertifikat ist möglicherweise ein selbstsigniertes Zertifikat. Selbstsignierte Zertifikate können weitere Untersuchungen rechtfertigen, da diese Zertifikate nicht von einer bekannten Zertifizierungsstelle ausgestellt werden.

RISKIQ SSL-Zertifikatsuchen, die mehrere Zertifikate oder keine Zertifikate zurückgeben

Ein Security Incident-Analyst kann die Ergebnisse mehrerer SSL-Zertifikate verwenden, um zu bestimmen, ob ein Standort Teil einer gemeinsamen, erkennbaren Entität ist. Wenn kein SSL-Zertifikatergebnis angezeigt wird, kann dies darauf hinweisen, dass Sites mit obskuren oder verdächtigen Namen keine vertrauenswürdigen Zertifikate besitzen. Suchergebnisse für erkennbare Elemente, die keine SSL-Zertifikate oder mehrere SSL-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

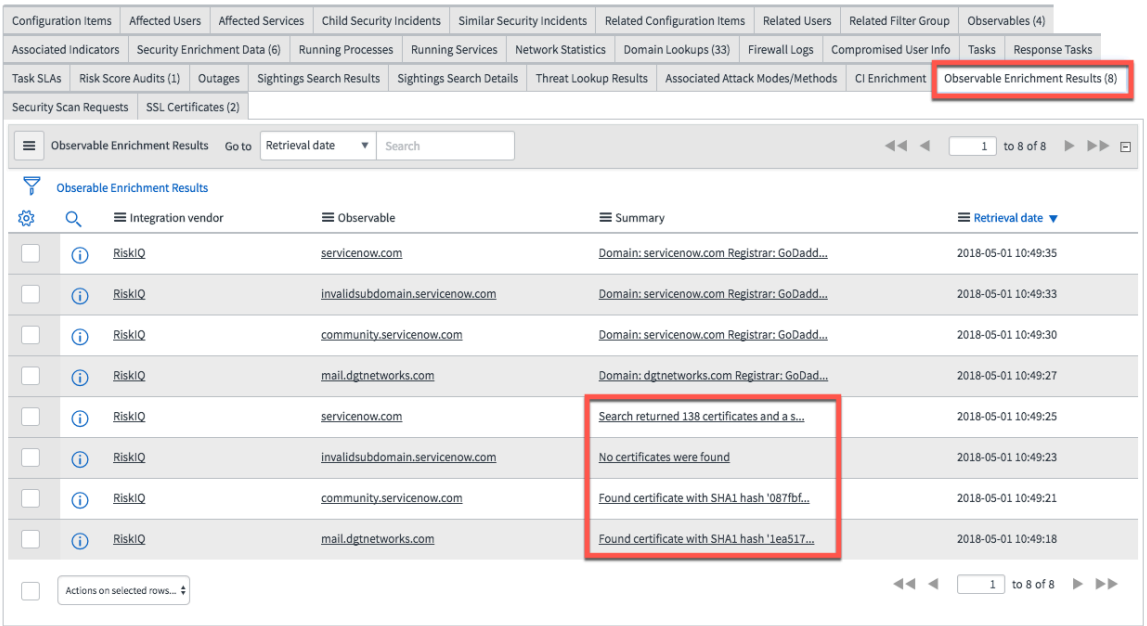
Zertifikate zurückgeben, werden auf der Registerkarte Datenanreicherungs-Ergebnisse erkennbarer Elemente im Security Incident-Datensatz angezeigt.

Example: Keine SSL-Zertifikatergebnisse oder mehrere SSL-Zertifikatergebnisse

Führen Sie die Schritte aus, um die Ergebnisse für erkennbare Elemente anzuzeigen, die keine SSL-Zertifikate oder mehrere Zertifikate zurückgeben.

1. Klicken Sie im Datensatz des Security Incident auf die Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente**.

Registerkarte „Datenanreicherungs-Ergebnisse erkennbarer Elemente“.

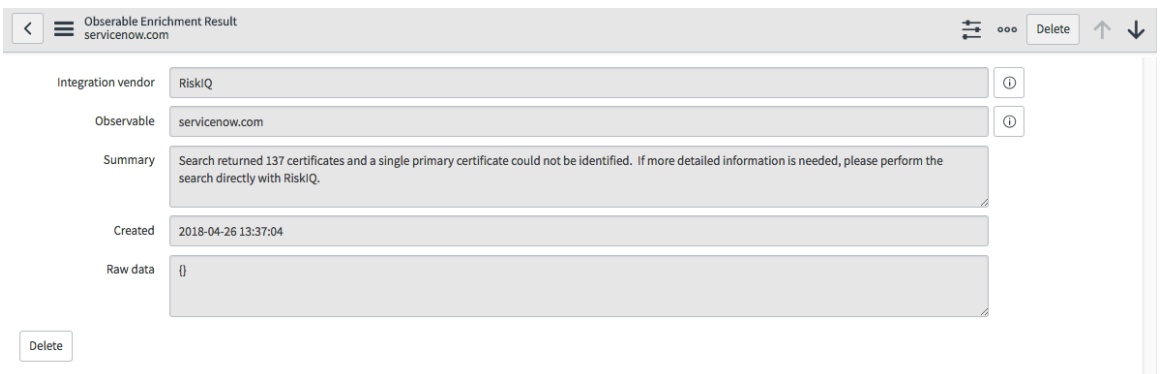


Die Datenanreicherungs-Ergebnisse für erkennbare Elemente für die Suche RISKIQ und WHOISIQ werden angezeigt.

In der Spalte **„Erkennbares** Element“ entspricht servicenow.com der Meldung „Suche hat 138 Zertifikate zurückgegeben“ in der Spalte **Zusammenfassung**. In ähnlicher Weise entspricht „invalidsubdomain.servicenow.com“ dem Wert In der Spalte **„Zusammenfassung**“ wurden keine Zertifikate gefunden. Diese Zusammenfassungen geben an, dass mehrere SSL-Zertifikate gefunden wurden und dass keine genauen Übereinstimmungen für SSL-Zertifikate gefunden wurden.

2. Klicken Sie in der Spalte **„Erkennbares Element** “ auf **servicenow.com**.

Mehrere SSL-Zertifikate



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die im Datensatz angezeigte Zusammenfassungsmeldung gibt an, dass für servicenow.commehrere Ergebnisse für SSL-Zertifikate zurückgegeben wurden und kein primäres SSL-Zertifikat abgeglichen werden konnte. Diese Nachricht wird häufig bei Suchen zurückgegeben, die allgemeine Domänennamen enthalten, z. B. servicenow.com.

Wenn Sie weitere Informationen zu einer gemeinsamen Domäne benötigen, können Sie die Suche direkt mit der RISKIQ -API durchführen.

3. Navigieren Sie zurück zur Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente**, und klicken Sie in der Spalte **Erkennbares** Element auf **ungültigsubdomain.servicenow.com**.

Keine SSL-Zertifikate

Hinweis:

- Wenn für das aktuell erkennbare Element keine SSL-Zertifikate gefunden werden, zeigt das Feld Zusammenfassung die Meldung Es wurden keine Zertifikate gefunden an.
- Wenn für das aktuell erkennbare Element keine aktiven SSL-Zertifikate gefunden werden, zeigt das Feld Zusammenfassung die Meldung Es wurden keine aktiven Zertifikate gefunden an.

Überprüfen Sie die erwarteten Ergebnisse für WHOISIQ -URL-Suchen

Wenn ein Security Incident erkennbare Elemente für URLs oder Domänen generiert, führt die WHOISIQ API die Anreicherung erkennbarer Elemente automatisch bei der Erstellung des Security Incidents durch. Die Suchergebnisse werden auf den Registerkarten **Datenanreicherungs-Ergebnisse erkennbarer Elemente** und **SSL-Zertifikate** im Security Incident-Datensatz angezeigt.

Vorbereitungen

Hinweis:

Die Abbildungen in den folgenden Schritten werden mit aktivierter Einstellung **für Formulare mit Registerkarten** in den Systemeinstellungen angezeigt.

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

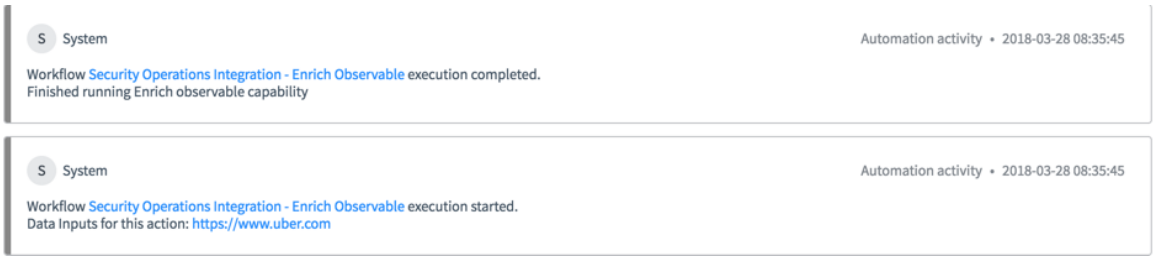
Die Datenanreicherungs-Ergebnisse erkennbarer Elemente werden auf der Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente** unten im Security Incident-Datensatz angezeigt. Für unterstützte erkennbare Elemente wird auch eine SSL-Zertifikatsuche ausgeführt, und die Ergebnisse werden auf der **Registerkarte SSL-Zertifikate**angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

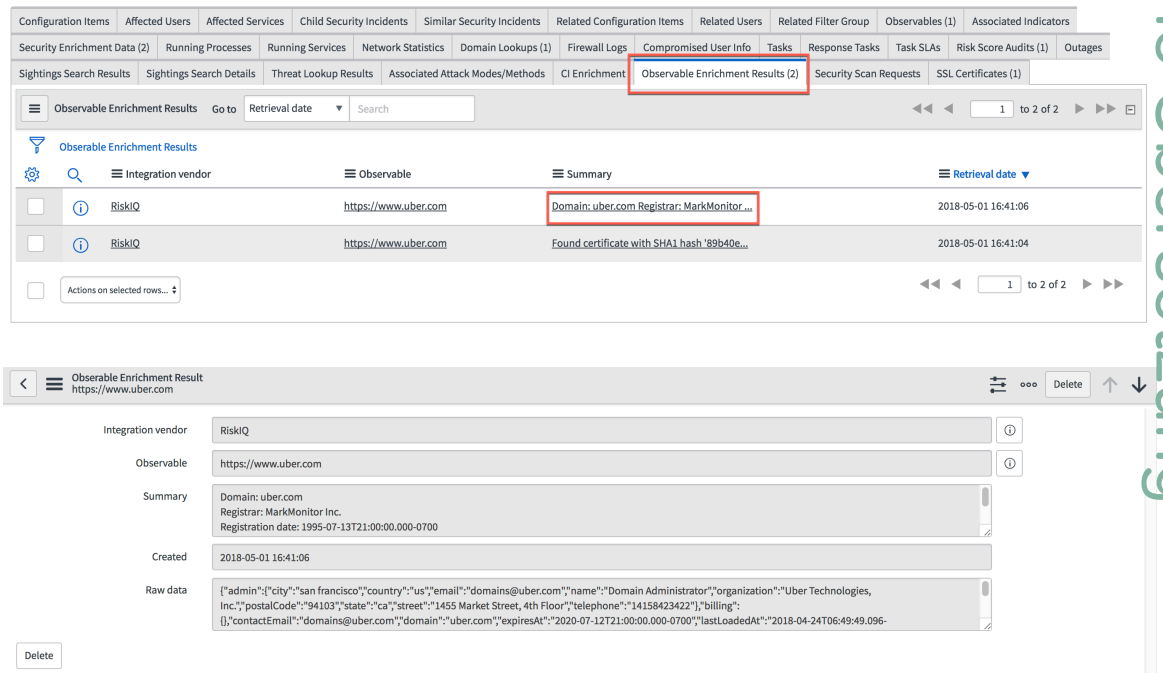
Prozedur

1. Öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und vergewissern Sie sich, dass die Suche in den Arbeitsnotizen erfolgreich ausgeführt wurde.



   Sobald die Anwendung konfiguriert ist, wird der Flow bei der Erstellung des incident automatisch gestartet. Der Ausführungs- und Abschlussstatus der Suche wird in den Arbeitsnotizen im Security Incident-Datensatz angezeigt.

2. Wenn Sie nicht verifizieren können, dass die Suche erfolgreich ausgeführt wurde, lesen Sie die Arbeitsnotizen, um weitere Informationen zum weiteren Vorgehen zu erhalten.
3. Klicken Sie im offenen Security Incident auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**.
4. Klicken Sie auf die Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente**, um sie auszuwählen.
5. Klicken Sie in der **Spalte** Zusammenfassung auf das erste Element **Domain: uber.com Registrierungsstelle: Markmonitor...**.

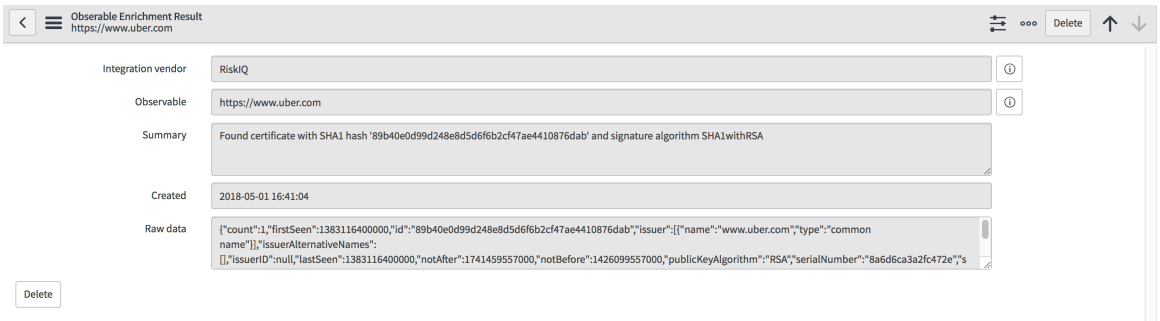


   Der angezeigte Datensatz enthält Informationen zur Domäne.

6. Navigieren Sie zurück zur Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente**, und klicken Sie in der **Spalte** Zusammenfassung auf das zweite Element **Zertifikat mit SHA1-Hash gefunden...**.

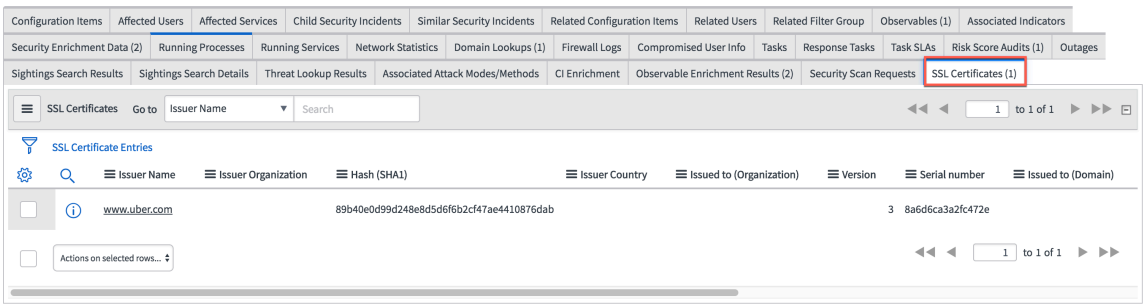
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieser Datensatz gibt an, dass ein SSL-Zertifikat mit einem Datei-Hash gefunden wurde.

7. Navigieren Sie zurück zum Security Incident-Datensatz, und klicken Sie auf die Registerkarte **SSL-Zertifikate**.



Die SSL-Zertifikatergebnisse für den Datei-Hash werden auch hier angezeigt.

Trouble?

Wenn Sie die erwarteten Ergebnisse nicht anzeigen können, überprüfen Sie die Arbeitsnotizen. Stellen Sie außerdem sicher, dass das erkennbare Element für die Suche von der Integration unterstützt wird.

Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

Erstellen Sie ein erkennbares Element für manuelle WHOISIQ Suchen

Security Incident-Analysten verwenden Informationen aus der Ergänzung erkennbarer Elemente mit der WHOISIQ -API, um mehr über die E-Mail-Adressen, Namen und Telefonnummern von Organisationen zu erfahren.

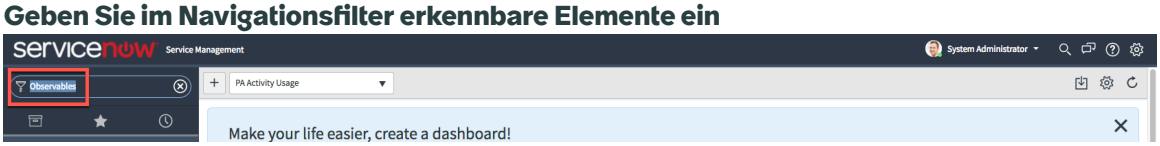
Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Alle** > **IoC-Repository** > **Erkennbare Elemente**.

Geben Sie im Navigationsfilter erkennbare Elemente ein

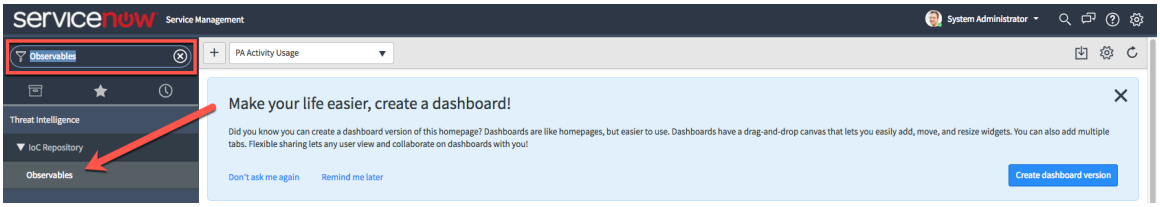


Unter dem Navigationsbereich wird das Modul Observables (Erkennbare Elemente) angezeigt.

Automatische Übersetzung

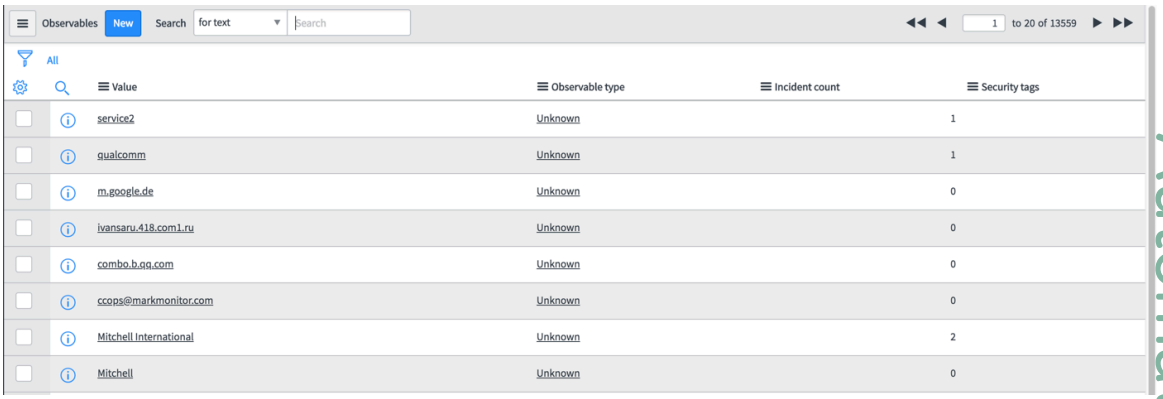
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul „Erkennbare Elemente“.



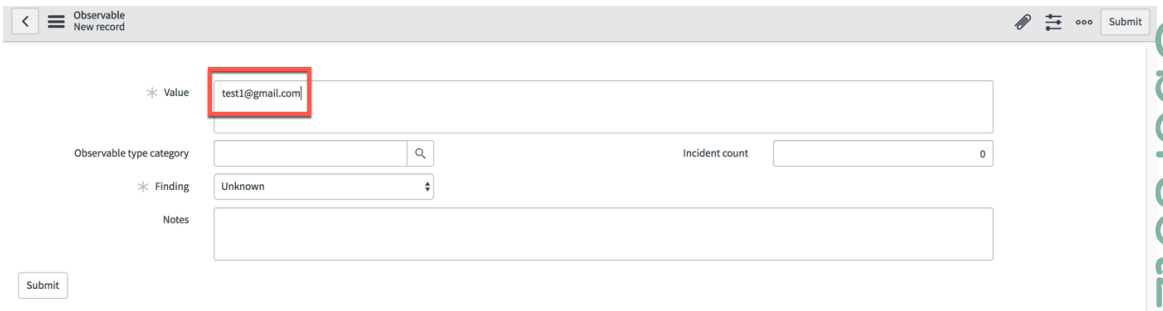
2. Klicken Sie auf das Modul **„Erkennbare Elemente“**, um die Liste der erkennbaren Elemente anzuzeigen.

Liste der erkennbaren Elemente



3. Klicken Sie auf **Neu**, um ein neues erkennbares Element zu erstellen.
4. Füllen Sie die Felder im Formular „Erkennbares Element“ aus.

Erstellen Sie ein neues erkennbares Element



5. Klicken Sie auf **Absenden**.
   Sie kehren zur Liste der erkennbaren Elemente zurück. In der Spalte **„Wert“** wird Ihr neues erkennbares Element angezeigt.

> **Hinweis:**
> Wenn Sie Ihr erkennbares Element im angezeigten Teil der Liste nicht finden können, verwenden Sie die Suchfunktion, um es zu finden.

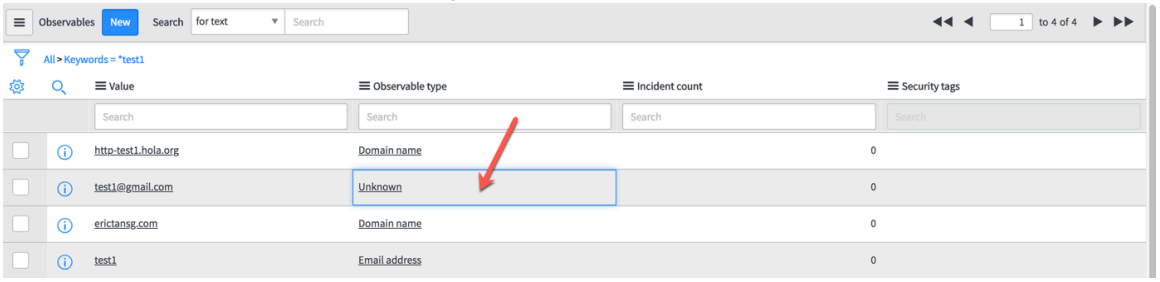
6. Bearbeiten Sie das Feld **Erkennbarer Typ**, um den Typ entsprechend Ihrem erkennbaren Element von **Unbekannt** in **E-Mail-Adresse** zu ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Spalte **Erkennbarer Typ** rechts neben dem Text **Unbekannt**, um ihn auszuwählen.

Wählen Sie das Feld Erkennbarer Typ aus

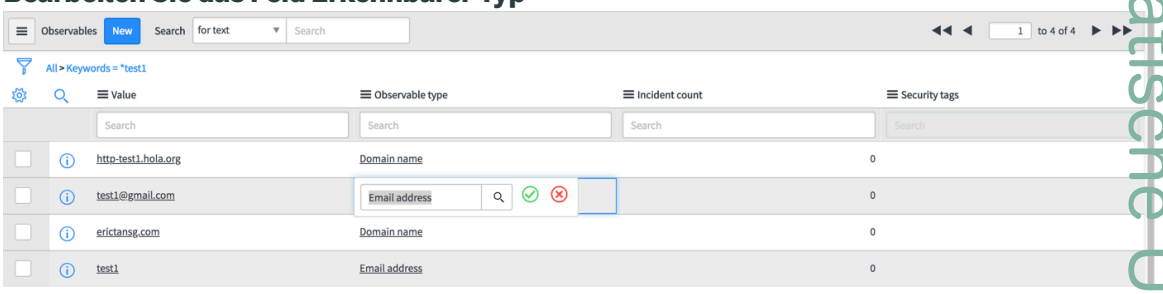


Das ausgewählte Feld ist blau umrandet.

b. Doppelklicken Sie bei blau umrandetem Feld auf eine beliebige Stelle innerhalb des hervorgehobenen Felds, um den Editor zu öffnen.

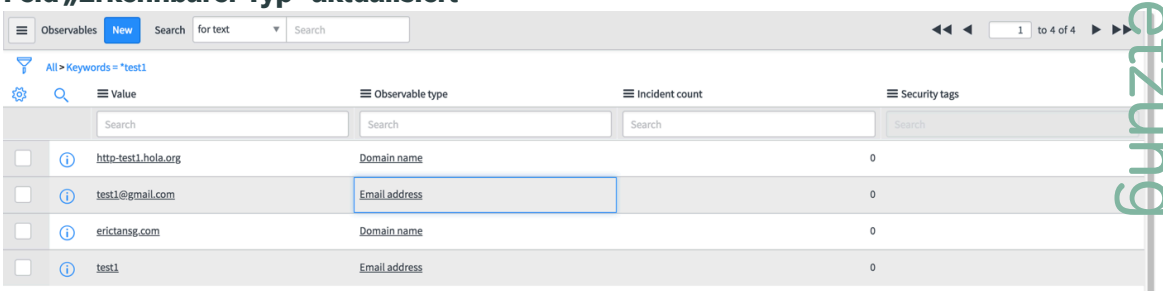
c. Geben Sie im angezeigten Feld den Typ des erkennbaren Elements (E-Mail-Adresse) ein, und klicken Sie auf das grüne Häkchen, um den Wert zu speichern.

Bearbeiten Sie das Feld Erkennbarer Typ



In der Spalte **„Erkennbarer Typ“** in der Liste wird die E-Mail-Adresse für das neue erkennbare Element angezeigt.

Feld „Erkennbarer Typ“ aktualisiert



Nächste Maßnahme

Wenn Sie ein erkennbares Element für die Suche erstellt und bearbeitet haben, führen Sie die Ergänzungssuche des erkennbaren Elements im Datensatz des erkennbaren Elements mit der API WHOISIQ aus.

Überprüft die erwarteten Ergebnisse für manuelle WHOISIQ Suchvorgänge

Führen Sie eine manuelle Suche für ein erkennbares Element durch, wenn nicht automatisch ein Security Incident generiert wird. Initiieren Sie Anreicherungssuchen erkennbarer Elemente mithilfe der API WHOISIQ für E-Mail-Adressen, Organisationsnamen, Telefonnummern oder Postanschriften manuell über die Tabelle „Erkennbare Elemente“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

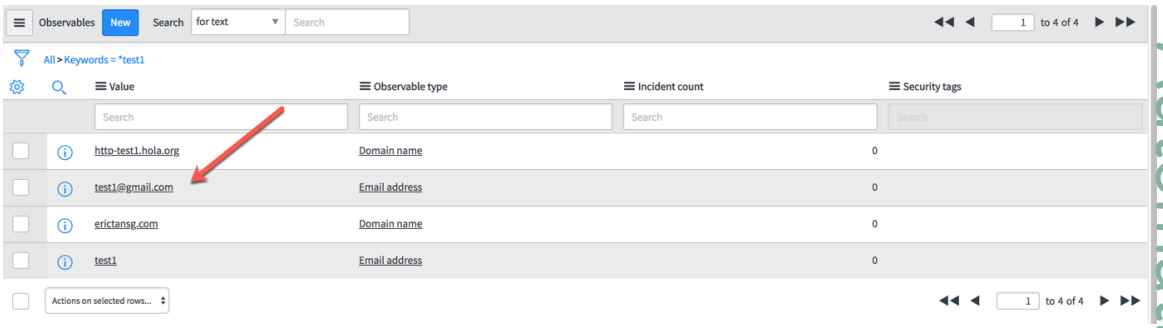
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

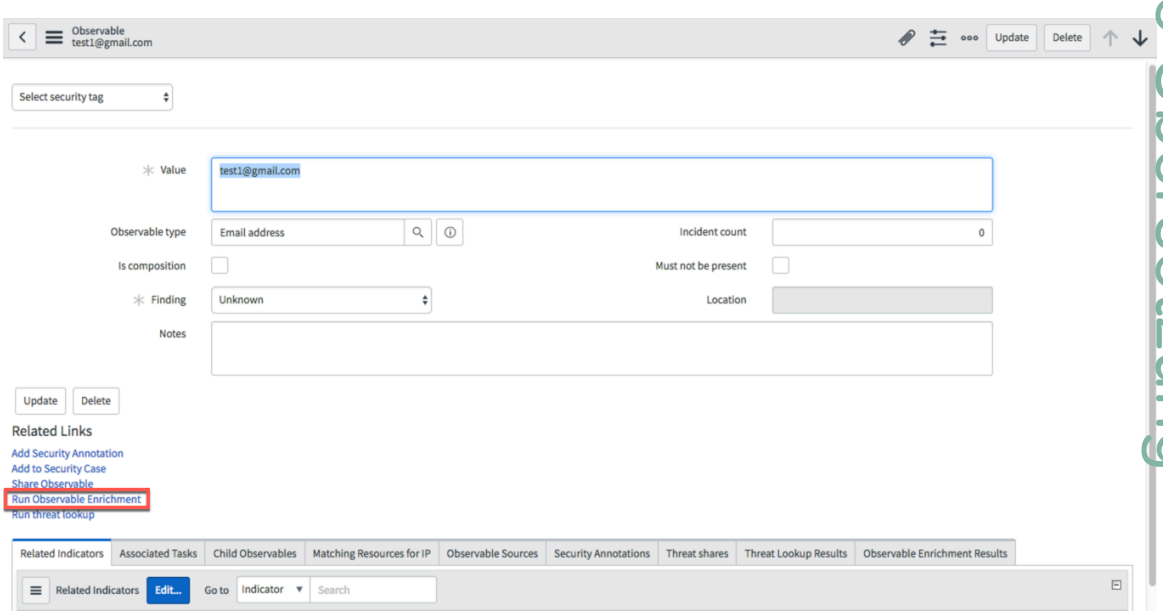
Erstellen Sie mit der WHOISIQ -API ein erkennbares Element für eine manuelle Suche. Weitere Informationen zum Erstellen und Bearbeiten eines erkennbaren Elements finden Sie unter Erstellen Sie ein erkennbares Element für manuelle WHOISIQ Suchen.

Prozedur

1. Navigieren zu **Alle** > **IoC-Repository** > **Erkennbare Elemente** und suchen Sie das erkennbare Element in der Liste, mit der Sie arbeiten.
2. Klicken Sie in der Spalte **„Wert“** auf das erkennbare Element, um den Datensatz zu öffnen.



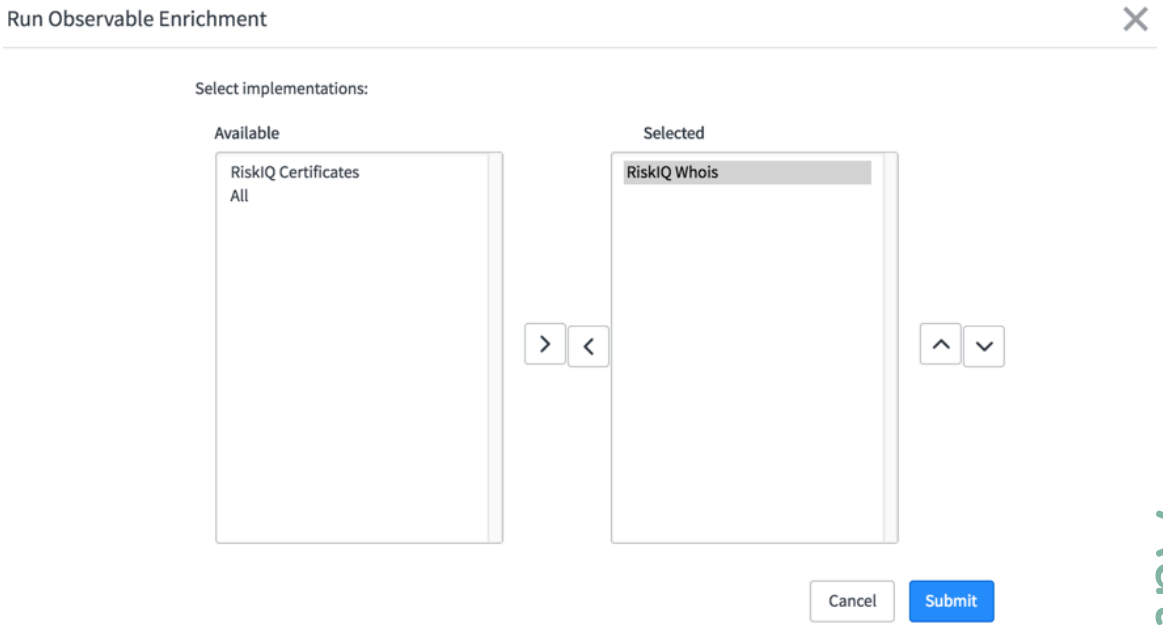
3. Klicken Sie auf den zugehörigen Link **Anreicherung von erkennbaren Elementen ausführen**, um die Suche auszuführen.



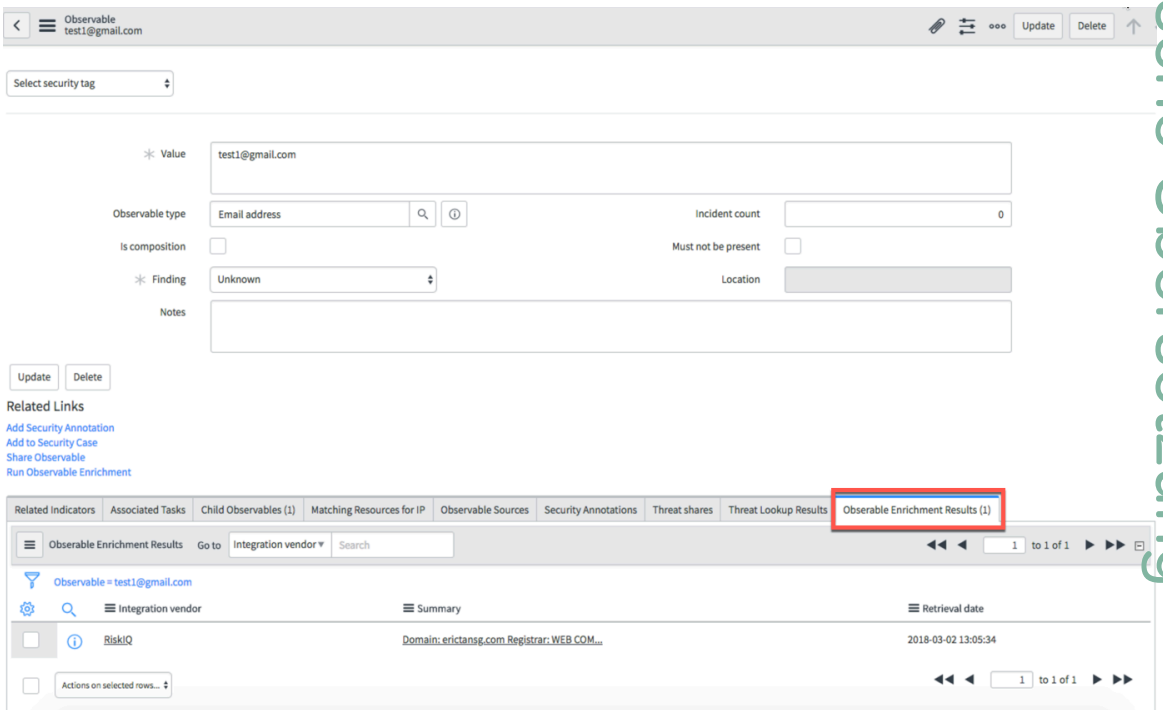
4. Verschieben Sie im Fenster **„Anreicherung erkennbarer Elemente** ausführen“ **RiskIQ Whois** in die Liste Ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.
   Suchergebnisse werden auf der Registerkarte **Datenanreicherungs-Ergebnisse erkennbarer Elemente** im Datensatz des erkennbaren Elements angezeigt.



Trouble?

Wenn für das erkennbare Element keine Ergebnisse zurückgegeben werden, wird in der **Spalte** Zusammenfassung eine Meldung angezeigt. Wenn keine Ergebnisse angezeigt werden, überprüfen Sie, ob das erkennbare Element von der API unterstützt wird.

Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Shodan Integration

Shodan ist eine Suchmaschine, die Servicebannerinformationen von verbundenen Geräten auf der ganzen Welt analysiert. Servicebanner enthalten Informationen über ein Computersystem, z. B. Hostname, Gerätetyp, Betriebssystem, geografischer Standort und verbundener ISP. Bei Integration mit dem Produkt Now Platform Security Operations bieten diese Servicebannerinformationen Analysten zusätzliche Ergänzungsdaten und Einblicke für Security Incidents oder Untersuchungen.

Zur Integration sind die Plugins Security Incident Response und Threat Intelligence erforderlich.

Die Shodan -Integration führt eine Ergänzung der folgenden erkennbaren Elemente durch:

- IP-Adressen
- URLs

Die Anwendung sucht alle fünf Minuten nach neuen erkennbaren Elementen. Wenn die erkennbaren Elemente von einem Typ sind, der von der Shodan -Integration erkannt wird, werden die erkennbaren Elemente angereichert.

Shodan installieren und konfigurieren

Bevor Sie die Integration in Ihrer -Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit die Anwendung Shodan ordnungsgemäß in Now Platform Security Operationsintegriert werden kann.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform für Ihre Instanz zugewiesen haben.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (admin) installiert die App und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf das Modul Security Operations.
Rufen Sie den API-Schlüssel Shodan ab.	Erstellen Sie ein Konto, und rufen Sie den API-Schlüssel von der Website Shodan ab: Shodan-Website .
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren.	Für das Madrid-Release und spätere Familienreleases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts

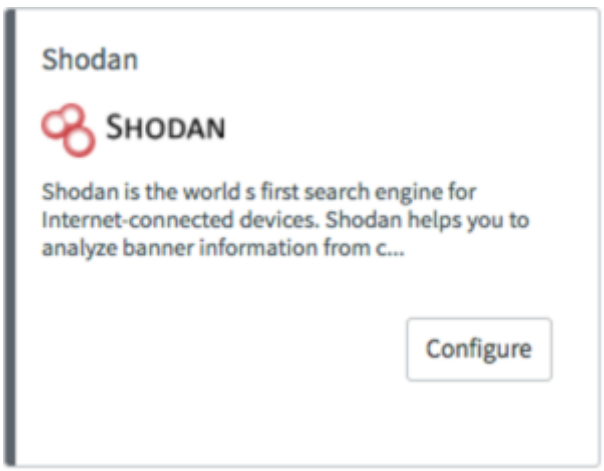
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Erforderliche Rolle: Administrator

Prozedur

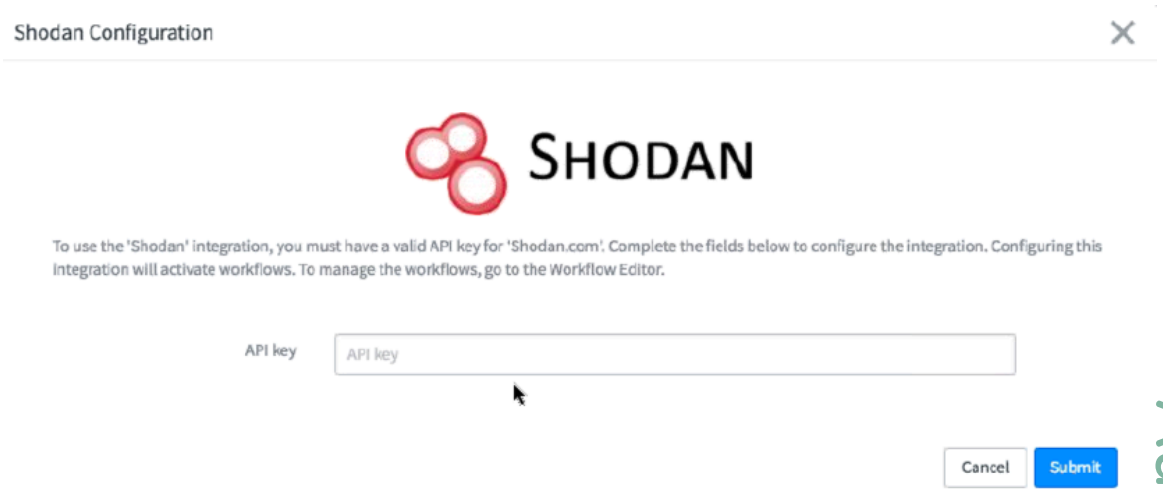
1. Wenn Sie die Anwendung für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Shodan.



3. Klicken Sie auf **Konfigurieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie im Dialogfeld **„Shodan-Konfiguration** “ den API-Schlüssel ein, den Sie von der Website Shodan erhalten haben, und klicken Sie auf **Absenden**.



5. Überprüfen Sie die erfolgreiche Konfiguration.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, es wird eine Fehlermeldung angezeigt.

   Trouble?

   Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, ist der API-Schlüssel Shodan möglicherweise ungültig.

Überprüfen Sie die erwarteten Ergebnisse für Shodan

Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Datenanreicherungs-Ergebnisse werden auf den Registerkarten **Datenanreicherungs-Ergebnisse für erkennbare Elemente** und **Netzwerkbanner** angezeigt.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst.

Prozedur

1. Öffnen Sie den Security Incident, mit dem Sie arbeiten, und vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.

   Sobald die Anwendung konfiguriert ist, wird der Workflow automatisch bei der Incident-Erstellung gestartet. Der Ausführungs- und Abschlussstatus der Suche wird in den Arbeitsnotizen im Security Incident angezeigt.

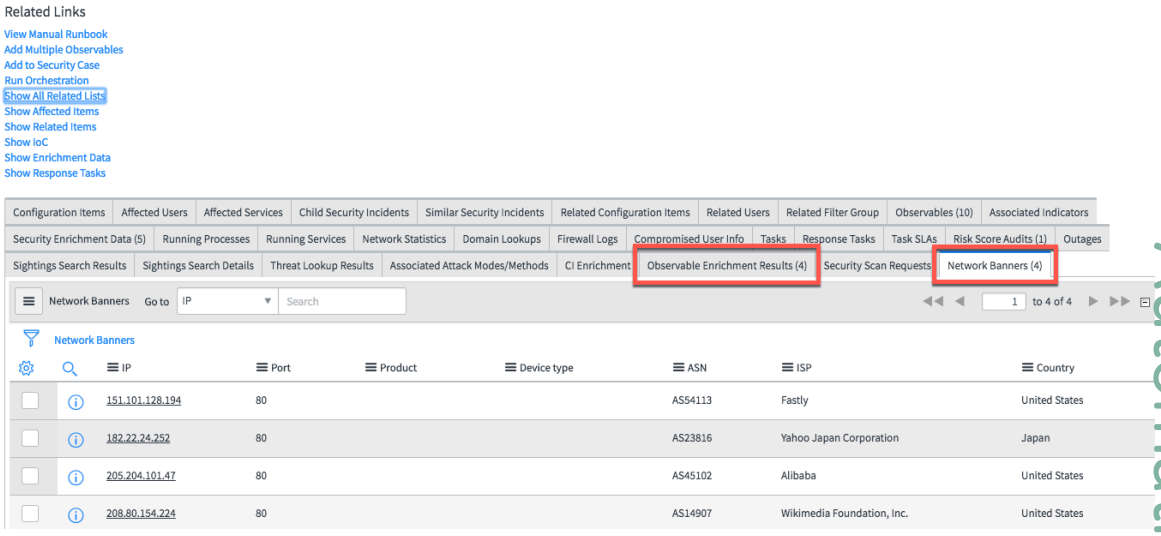
2. Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweise, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incidents, und klicken Sie unter **Zugehörige** Links auf den Link **Alle zugehörigen Listen anzeigen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Abbildungen in den folgenden Schritten werden mit aktivierter Einstellung **für Formulare mit Registerkarten** in den Systemeinstellungen angezeigt. Wenn Formulare mit Registerkarten nicht angezeigt werden, klicken Sie in der oberen rechten Ecke des Bannerframes auf das Zahnradsymbol Einstellungen. Klicken Sie im angezeigten Dialogfeld **„Systemeinstellungen"** auf **Formulare**, und vergewissern Sie sich, dass **Formulare mit Registerkarten** und **Mit Formular** ausgewählt sind.



Die Ergebnisse werden auf den Registerkarten **Datenanreicherungs-Ergebnisse erkennbarer Elemente** und **Netzwerkbanner** unten im Security Incident angezeigt.

4. Klicken Sie bei ausgewählter Registerkarte **Netzwerkbanner** auf das blaue Informationssymbol neben einem erkennbaren Element.

5. Klicken Sie im angezeigten Dialogfeld **auf Datensatz öffnen**, um Rohdaten und weitere Details anzuzeigen.

Trouble?
Wenn auf den Registerkarten **Datenanreicherungs-Ergebnisse erkennbarer Elemente** und **Netzwerkbanner** keine Ergebnisse angezeigt werden, vergewissern Sie sich, dass das erkennbare Element ein Typ ist, der von der Integration für die Suche unterstützt wird.

(Optional) Fügen Sie manuell ein erkennbares Element für hinzu Shodan

Sie können erkennbare Elemente manuell an einen Security Incident anhängen. Sie können erkennbare Elemente manuell anhängen, wenn Sie Bedrohungssuchen für erkennbare Elemente durchführen möchten, die beim ersten Ereignisauslöser nicht an einen Security Incident angehängt sind. Außerdem können Sie diese Aufgabe ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

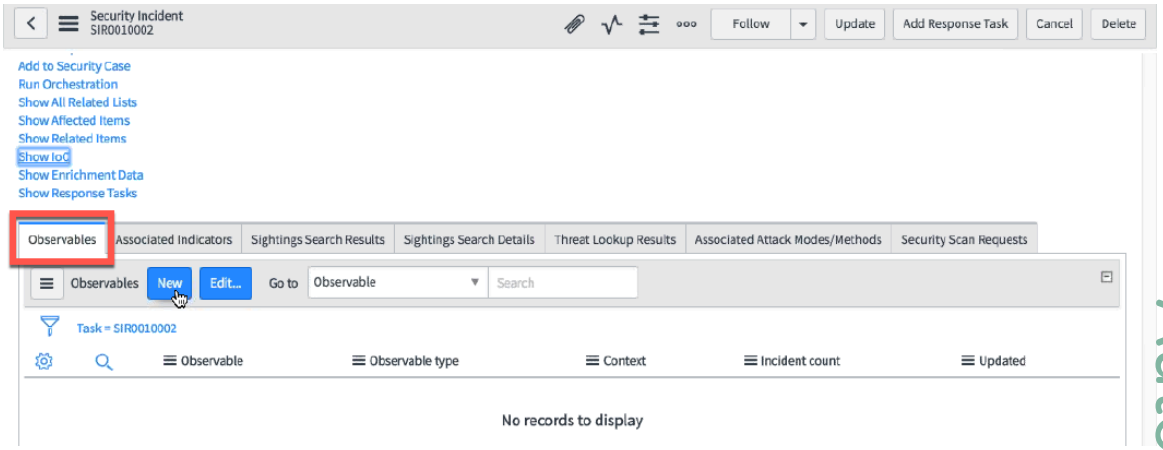
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

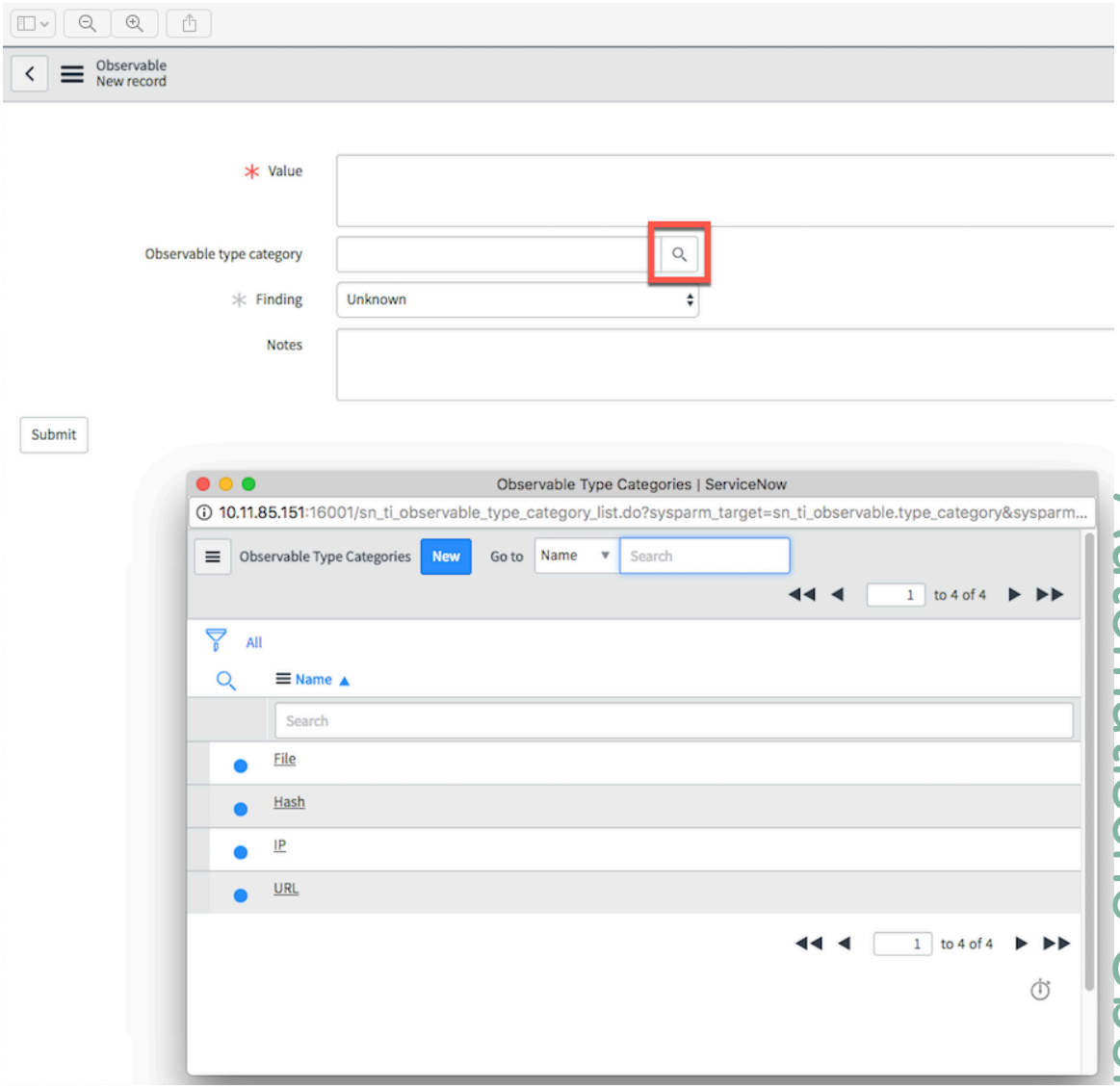
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie einen Security Incident, an den Sie das erkennbare Element anhängen möchten.
2. Klicken Sie unten im Datensatz auf den Link **IoC anzeigen**unter **Zugehörige Links**.



3. Klicken Sie auf der Registerkarte **Erkennbare Elementeauf Neu**.
   Das Formular „Erkennbares Element“ wird angezeigt.
4. Geben Sie im Feld **Wert** ein erkennbares Element ein (IP-Adresse oder URL).
5. Klicken Sie auf das Suchsymbol, und klicken Sie im Dialogfeld **„Kategorien erkennbarer Elemente“** in der Liste auf den Typ des gewünschten erkennbaren Elements, um das Feld auszufüllen.

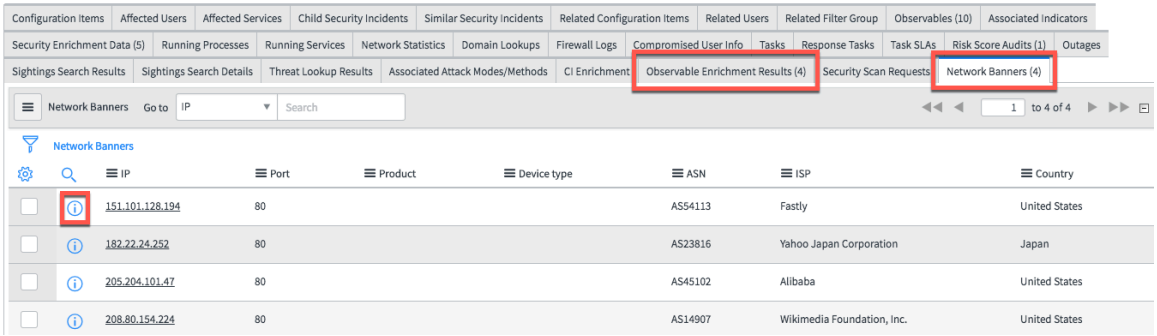
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie auf **Absenden**.
   Der Workflow wird gestartet und sucht nach dem neuen erkennbaren Element. Der Ausführungs- und Abschlussstatus werden im Abschnitt „Arbeitsnotizen“ des Security Incident-Datensatzes angezeigt.
7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.

8. Klicken Sie unten im Datensatz auf den zugehörigen Link **Alle zugehörigen Listen anzeigen**.
9. Klicken Sie auf die Registerkarten **Datenanreicherungs-Ergebnisse erkennbarer Elemente** oder **Netzwerkbanner**, um Ergebnisse anzuzeigen, und klicken Sie auf das blaue Informationssymbol neben einem erkennbaren Element, um weitere Informationen zu einem bestimmten Element zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Klicken Sie im angezeigten Dialogfeld **auf Datensatz öffnen**, um Rohdaten und weitere Details anzuzeigen.
11. **Wahlweise:** Klicken Sie auf das blaue Einstellungssymbol neben dem Suchsymbol, um die Spaltenausgabe und -reihenfolge zu personalisieren.
12. Wählen Sie unter „ **Listenspalten personalisieren“**die verfügbaren Einstellungen aus, verschieben Sie sie in die Spalte **Ausgewählt**, und klicken Sie auf **OK**.

Trouble?
Überprüfen Sie die **Arbeitsnotizen** auf weitere Informationen und Vorgehensweise, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

Secureworks CTP Integration zur Ticketerfassung

Mit der Integration zur Erfassung von Secureworks Counter Threat Platform -Tickets können Sie Tickets Secureworks CTP automatisch abrufen, in Security Incidents konvertieren und automatisierte Antwortaktionen durchführen.

Die wichtigsten Funktionen dieser Integration sind:

- Automatische Erfassung ausgewählter Tickets (einschließlich Anhängen) basierend auf einem vordefinierten Zeitplan.
- Zuordnung von Ticket- und Ereignisfeldern zu Feldern Security Incident Response.
- Vorschau der Security Incidents, die den Ticketfeldern zugeordnet sind.
- Filtern und Zusammenfassung von Tickets.
- Abruf von Ereignissen, die einem Ticket zugeordnet sind, bei Bedarf.
- Regelmäßige Nachverfolgung wichtiger Aktualisierungen von Tickets.
- Automatisierung von Ticketaktualisierungen und -schließungen basierend auf dem SIR-Incident-Status
- Aktualisierung des Master-Tickets.
- Synchronisierung von Secureworks-Arbeitsprotokollen mit Security Incident Response -Arbeitsnotizen.

Richten Sie Ihre Instanz Now Platform für die Integration der Secureworks CTP -Ticketerfassung ein

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in der Instanz Now Platform ausführen müssen, bevor Sie die Anwendung von ServiceNow Storeinstallieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sehen Sie sich die folgende Tabelle an, und vergewissern Sie sich, dass Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen haben.	Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Instanz Now Platform von erforderlich. • Ein Benutzer mit der Administratorrolle Now Platform (admin) installiert die Anwendung über ServiceNow Store und weist die Rolle SIR -Administrator (sn_si.admin) zu. • Ein Benutzer mit der Rolle sn_si.admin überwacht die folgenden Aufgaben in Now Platform: ◦ Benennt, erstellt und bearbeitet Profile. ◦ Wählt die Ticketfelder Secureworks CTP aus und ordnet sie den Feldern für Security Incidents zu. ◦ Zeigt eine Vorschau der Details von Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird. ◦ Plant die laufende Ticket-Erfassung. ◦ Ermöglicht Ticket-Aktualisierungen, wenn ein SIR-Incident SIR erstellt und geschlossen wird. ◦ Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu. ◦ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Managing roles
Stellen Sie sicher, dass Sie die folgenden Versionen verwenden: • Secureworks Ticket-API 4.0 • Secureworks Event API 1.0 • Secureworks Ergänzung API 1.0	Wenn Sie Zugriff auf das -Portal Secureworks CTP haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich.
Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor	Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Sie die Anwendung für die Integration installieren.	Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. 1. Security Incident Response 2. Ereignis- und Warnungserfassung für Security Operations (Erforderlich für SIEM-Integrationen): Diese Anwendung erfordert: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST **Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Ereignis- und Warnungserfassung“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport. Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration der Secureworks CTP-Ticketerfassung

Bevor Sie die -Integration in Ihrer Instanz Now Platform ausführen, führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in die -Produkte Security Incident Response und Security Operations in Ihrer Instanz Now Platform integriert werden kann.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn Sie die Anwendung Secureworks CTP für die -Integration nicht aus ServiceNow Store installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Secureworks CTP Integration der Ticketerfassung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie zum Konfigurieren der Anwendung auf **Neu**.
4. Alternativ: Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, können Sie darauf klicken, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie im angezeigten Dialogfeld die Felder aus.
6. Klicken Sie auf **Absenden**.
   Nach erfolgreicher Validierung und Übermittlung wird jede Konfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Ergebnisse

Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden. Klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste **Konfigurationen anzeigen** auf **Ja**.

Erstellen Sie ein Profil für die Integration der Secureworks CTP-Ticketerfassung

Erstellen Sie ein Profil in Ihrer Instanz Now Platform, und bestimmen Sie, welche Tickets erfasst werden müssen und welche Tickets zum Erstellen von Security Incidents verwendet werden. Bevor Security Incidents aus erfassten Tickets erstellt werden, werden die Feldwerte aus Tickets in einem Layout eines Now Platform -Security Incidents angezeigt, sodass Sie eine Vorschau auf die Darstellung des tatsächlichen Security Incidents anzeigen können.

Die Integration ermöglicht Ihnen das Erfassen von Tickets basierend auf den Profilen, die Sie in der Umgebung Security Operations Ihrer -Instanz konfigurieren. Alle Tickets werden zunächst für einen konfigurierten Tickettyp in einem Profil erfasst. Erfasste Tickets können dann weiter gefiltert werden, um anzugeben, welche Tickets Security Incidents erstellen.

Beispielsweise können Sie Filter bevorzugen, die Security Incidents nur für Tickets erstellen, die als hoch riskant eingestuft werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Tickets erstellt, werden einzelne Feldwerte in den Tickets für eine Vorschau den entsprechenden Feldern in einem Layout von Security Incidents zugeordnet.

Geben Sie die Quelle des Profils an

Geben Sie den Namen und die Quelle des Profils an.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

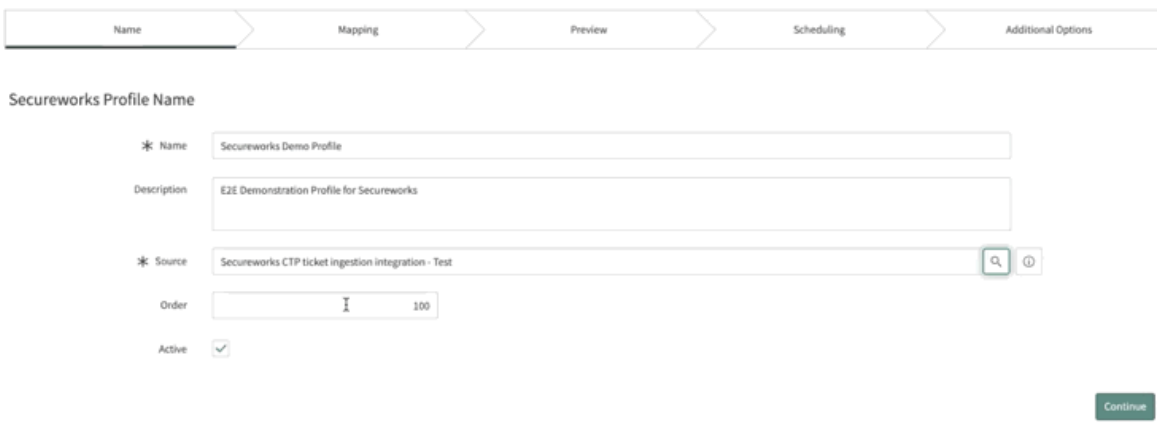
Prozedur

1. Um ein Profil für ein Ticket in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **Integration zur Secureworks-Ticketerfassung** > **Secureworks-Profile**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn die Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert. Profilnamen in Ihrer Instanz Now Platform müssen eindeutig sein.
Quelle	Wählen Sie die Quelle aus, aus der Sie die Daten erfassen möchten.
Bestellung	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile dieselben Auslösebedingungen verwenden. Je niedriger der Reihenfolgenwert, desto höher die Priorität.
Aktiv	Diese Option ist standardmäßig deaktiviert. Wenn diese Option deaktiviert ist, ist das Profil nicht aktiv. **Hinweis:** Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Ordnen Sie die Ticketfelder zu.

Zuordnung von Ticketfeldern für die SecureWorks CTP-Integration

Ordnen Sie die Felder „Ticket“ und „Ereignis“ den Feldern im Formular „Security Incident“ zu.

Für den Zuordnungsschritt müssen Sie zuerst Beispieltickets erfassen, dann sicherstellen, dass alle relevanten Ticketfelder an der entsprechenden Stelle im Formular Security Incident Response zugeordnet sind, und dann den Security Incident im Vorschaubereich visualisieren.

Die Zuordnung der Beispielticketfelder umfasst Folgendes:

- Beispieldaten werden abgerufen und ausgefüllt: Siehe Erfassung der Secureworks-Beispieltickets
- Ticketfelder dem Security Incident zuordnen: Siehe Secureworks-Ticketfelder werden Security Incident Response-Feldern zugeordnet

Erfassung der Secureworks-Beispieltickets

Wählen Sie die Beispieltickets aus, die erfasst werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
2. Sie können entweder die fünf neuesten Beispieltickets abrufen oder die eindeutigen Ticket-IDs für die spezifischen Tickets angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   Wählen Sie in der Auswahlliste **Erfassungseinstellung** eine der folgenden Optionen aus:
   - Neueste Tickets abrufen: Die 5 neuesten Tickets werden abgerufen.
   - Tickets basierend auf der Ticket-ID auswählen: Geben Sie die Ticket-ID für das abzurufende Ticket an. Sie können maximal 5 durch Kommas getrennte Ticket-IDs angeben.
3. Klicken Sie **auf Beispieldaten abrufen**, um die aktuellen Beispielticketdaten vom Server Secureworks CTP abzurufen.
   Das Abrufen von Beispieltickets kann einige Minuten dauern. Oben auf dem Bildschirm wird eine Meldung angezeigt, dass die Transaktion funktioniert. Die abgerufenen Tickets werden als einzelne Registerkarten angezeigt. Klicken Sie auf eine Registerkarte, um die Ticketdaten anzuzeigen. Für jedes Ticket sehen Sie die Ticketfelder und ihre Werte sowie Details zum beitragenden Ereignis, das das Ticket ausgelöst hat.

Hinweis:
Sie sehen nur dann Details zu beitragenden Ereignissen, wenn sie in den letzten 7 Tagen stattgefunden haben. Ereignisse, die älter als 7 Tage sind, werden nicht angezeigt.

Nächste Maßnahme
Nachdem Sie die Beispieldaten abgerufen haben, besteht der nächste Schritt darin, die Ticketfelder dem Security Incident zuzuordnen.

Secureworks-Ticketfelder werden Security Incident Response-Feldern zugeordnet

Ordnen Sie einzelne Ticket- oder Ereignisfelder Feldern in einem Security Incident Now Platform SIR zu.

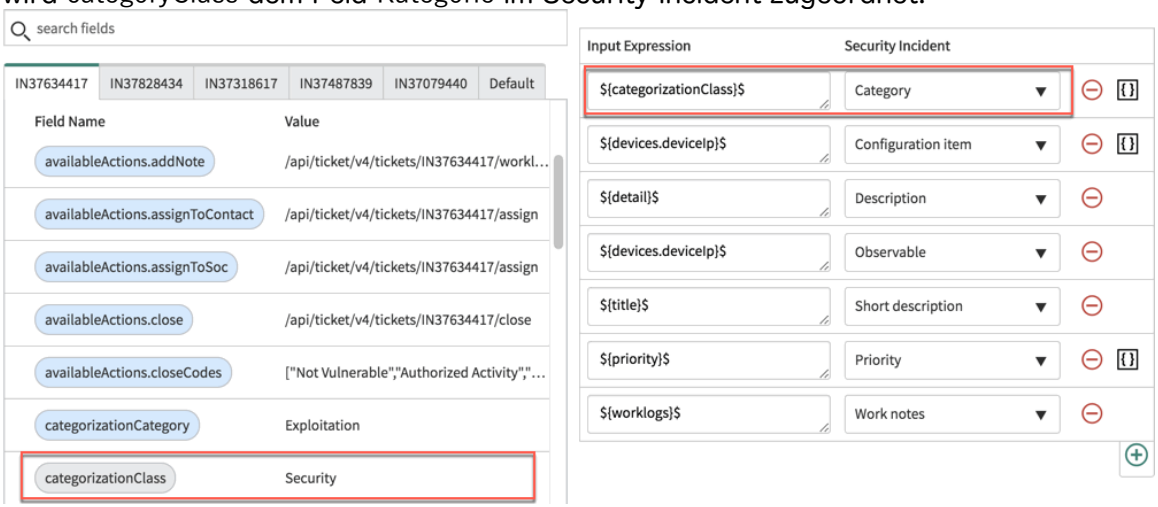
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldzuordnung für Ticket

Als Benutzer mit der Rolle sn_si.admin verwenden Sie die Felder aus dem Abschnitt Beispieltickets auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in der Spalte **„SIR-Incident-Feldzuordnung“** zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Ticket- oder Ereignisfelder aus der linken Seite ziehen und im Abschnitt „SIR-Incident-Feldzuordnung“ auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das eingehende Ticketfeld einem ausgehenden Security Incident-Feld zu.

1. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf einen blauen Feldnamen auf der linken Seite des Formulars.
2. Sie können den Feldnamen manuell in die Spalte „Eingabeausdruck“ eingeben oder den Feldnamen per Drag-and-Drop verschieben. Beispiel: Beschreibungund legen Sie es auf einem Feld in der Spalte **Eingabeausdruck** neben einem Feldnamen in der Spalte **Security Incident** fest.

   Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird categoryClass dem Feld Kategorie im Security Incident zugeordnet.



> **Hinweis:**
> Wenn Sie den Namen des Ereignisfelds manuell im Abschnitt **„Eingabeausdruck“** eingeben, müssen Sie vor dem Namen des zuzuordnenden Felds das Präfix `${Event:eventfield}$` hinzufügen.

Um sicherzustellen, dass bei der Zuordnung keine Ticket- oder Event-Felder übersehen oder dupliziert werden, sind die Felder farbcodiert. Die Farbcodierung der Ticketfelder hilft Ihnen, die bereits zugeordneten Ticketwerte nachzuverfolgen, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. So können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob noch wichtige Ticketinformationen zugeordnet werden.

Hellblaue Felder auf der linken Seite zeigen an, dass im Security Incident noch kein Ticketfeld ausgewählt und zugeordnet wurde. Unter Umständen möchten Sie ein Feld für eingehende Tickets oder Ereignisse mit mehr als einem Feld in einem Security Incident verknüpfen. Ein graus Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

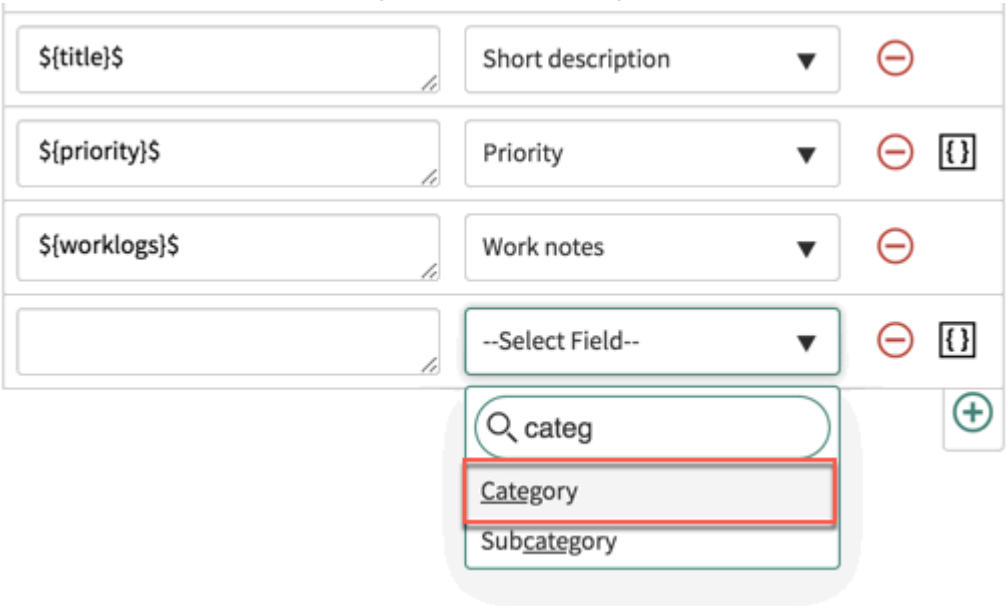
3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie rechts im Formular im Abschnitt SIR Incident-Feldzuordnung unten im Raster auf das Pluszeichen (+). Ein neues Feld wird angezeigt.

b. Erweitern Sie in der Spalte „Security Incident“ die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung ist die Kategorie grau hinterlegt, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Ticketfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Security Incident-Felder auf der rechten Seite beim Verfolgen der bereits zugeordneten Incident-Felder SIR.



Hinweis:
Da für denselben Security Incident mehrere erkennbare Elemente angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der mehrere Optionen ausgewählt werden können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident ebenfalls nicht ausgefüllt.

c. Geben Sie alternativ einen Wert in das Feld Suchen für die neue Zeile ein.

d. Wählen Sie auf der linken Seite des Formulars das Ticketfeld aus, und ziehen Sie es per Drag-and-Drop in ein entsprechendes Feld für Security Incidents auf der rechten Seite.

4. Entfernen Sie Felder, indem Sie das Symbol – neben dem Feldnamen im Abschnitt „SIR-Incident-Feldzuordnung“ verwenden.

5. Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.

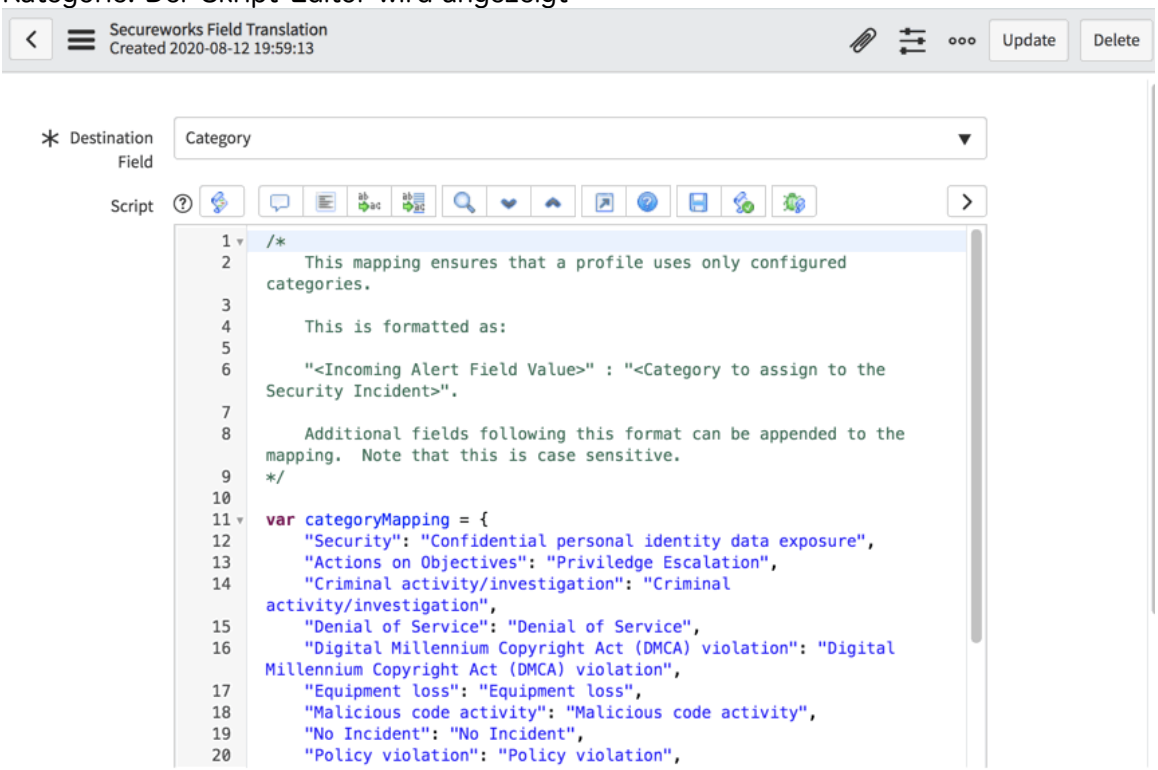
Formatfeldübersetzung

In bestimmten Fällen werden Ticketfelder möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten. Beispielsweise können mit dem Skript-Editor die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategoriewerte „Malware-Warnung“ und „Virusinfizierung“ unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mithilfe von in eine gemeinsame böswillige Code-Aktivität im Feld „Kategorie“ des Security Incident SIR übersetzt werden Formatfeldübersetzungsfunktion.

Um den Skript-Editor zu verwenden, klicken Sie auf das Symbol {} neben dem Feld Kategorie. Der Skript-Editor wird angezeigt



.

Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.

Bedingungen für Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um festzulegen, welche Tickets Security Incidents erstellen und welche Tickets herausgefiltert werden sollen (z. B. Tickets mit niedriger Priorität). Dieselben Feldwerte können Sie im Builder für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ticket erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

1. Scrollen Sie im Formular zum Abschnitt **„Bedingungen für Incident-Generierung“,** und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen filtern,** um die Option zu aktivieren.

   Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt **„Beispiel für eine Ticketerfassung“** für die erfassten Tickets angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach den von Ihnen erfassten Tickets. Bei den von Ihnen eingegebenen Kriterien wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des Tickets Secureworks CTP übereinstimmen. Wenn Sie sich bei den Werten, die Sie in die Filterfelder eingeben sollen, nicht sicher sind, kehren Sie möglicherweise zu Ihrer Secureworks CTP -Konsole zurück und überprüfen Ihre Tickets für die Stichwörter.

Hinweis:
Die Ticketfelder *„Arbeitsprotokolle“*, *„Geräte“*, *„Anhänge“*, *„Beobachter“*, *„Verfügbare Aktionen“*und *„CloseCodes“* können mehrere Werte aufweisen (da die Werte in Arrays gespeichert werden). Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie für diese Felder die Filterbedingung „ *Enthält* “ verwenden, um sicherzustellen, dass die Daten ordnungsgemäß gefiltert werden.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **AND** oder **OR**.
   - Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.
4. (Optional) Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

   Diese Art der Filterung von Bedingungen für die Incident-Generierung hilft Ihnen, die Tickets einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Regel oder Filter zu ändern. Wenn zusätzliche Filterkriterien festgelegt sind, werden Security Incidents nur Tickets zugeordnet, die allen Kriterien entsprechen.

Kriterien für die Zusammenfassung von Tickets, um ähnliche Tickets zu verarbeiten und doppelte Incidents zu verhindern

Definieren Sie zusätzliche Kriterien für die Ticket-Zusammenfassung, die ein eingehendes Ticket zu einem vorhandenen Security Incident SIR zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Ticketdaten in einem einzigen Security Incident platziert werden. Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:

1. Scrollen Sie im Formular zum Abschnitt **„Ticket-Zusammenfassungskriterien“,** und aktivieren Sie das Kontrollkästchen **Zusammenfassungsbedingungen,** um diese Option zu aktivieren.

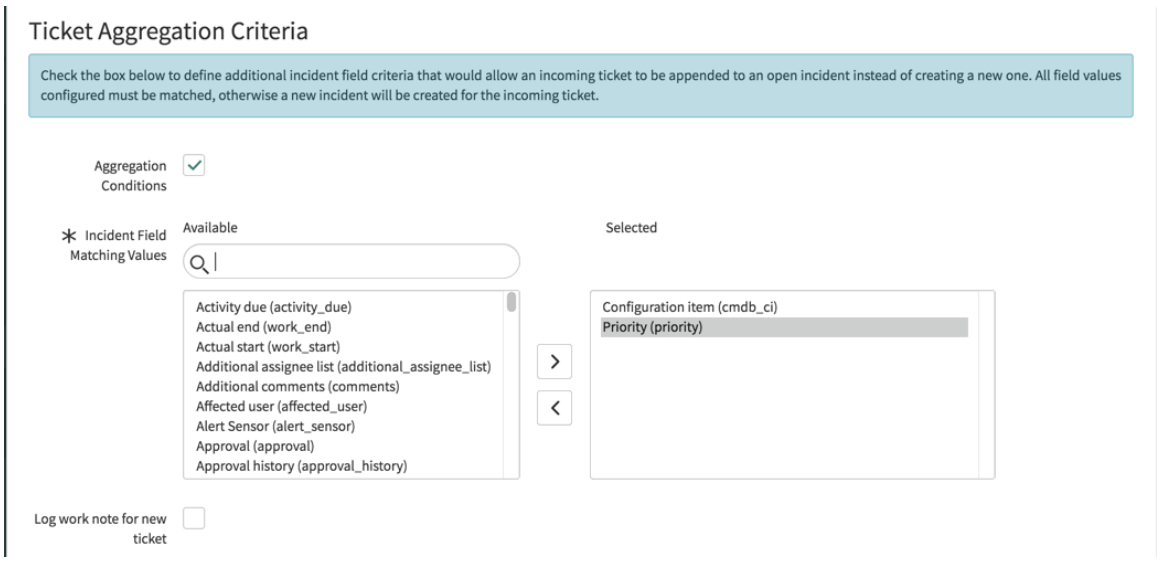
   Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die im Security Incident SIR konfiguriert sind.

2. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Ihrer NOW Platform abgleichen möchten, und verschieben Sie sie in die Liste Ausgewählt.

   Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, damit dieses eingehende Ticket an einen vorhandenen Security Incident angehängt wird. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Ticketfeldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Ticket-Zusammenfassung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nicht erfüllt, und es wird ein neuer Security Incident erstellt. Screenshot unten für Feldzuordnung mit mehreren Werten.



Wenn ein neues Ticket allen Werten entspricht, die in den Bedingungen des Zusammenfassungsfelds im Zuordnungsschritt ausgewählt sind, wird das neue Ticket automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, die mit Security Incidents arbeiten, können Sie alle hinzugefügten aggregierten Tickets in einer zugehörigen Liste für einen Security Incident anzeigen. Diese Liste enthält Details zu zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese Tickets zu vorhandenen Security Incidents zusammengefasst werden. Wenn diese Registerkarte in einem Security Incident nicht angezeigt wird, scrollen Sie unter **„Zugehörige Links“** im Datensatz zur linken Seite, und klicken Sie auf den Link **Alle zugehörigen Listen anzeigen**.

Hinweis:
Die zugehörige Liste „Aggregierte Secureworks-Tickets“ ist mit dem Basissystem nicht verfügbar. Sie müssen das Layout der zugehörigen Liste konfigurieren und explizit in die anderen zugehörigen Listen aufnehmen.

3. (Optional) Um eine Arbeitsnotiz für ein neues Ticket zu protokollieren, das kürzlich für den Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen zum Aktivieren dieser Option. Die Arbeitsnotiz protokolliert, dass ein neues Ticket hinzugefügt wurde, zusammen mit einem Link zu den Ticketdetails und allen anderen Details, die dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben erfolgreich Werte aus einem Ticket Secureworks CTP Feldern in einem Security Incident zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben Tickets auch an vorhandene Security Incidents angehängt, wenn Ticketfeldwerte den konfigurierten Zusammenfassungskriterien entsprechen.

4. Klicken Sie auf **„Fortsetzen** “, um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht in der Vorschau der Felder, die Sie im Security Incident SIR zugeordnet haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie eine Vorschau der zugeordneten Werte im Security Incident an

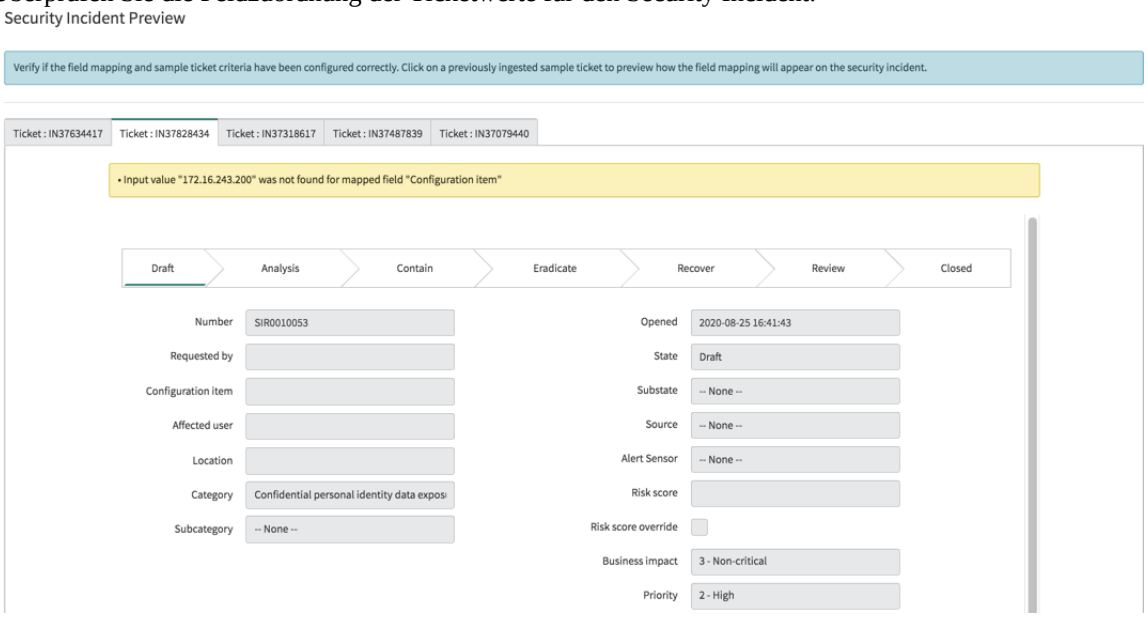
Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Security Incident SIR zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Ticketfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie die Vorschau eines Security Incidents an, und bearbeiten Sie die Zuordnung bei Bedarf erneut, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wird, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen auf Security Incidents SIR werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

Prozedur

1. Wenn die Vorschau des Security Incidents nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Vorschau**.
   Die Tickets werden als Registerkarten angezeigt.
2. Klicken Sie auf eine Registerkarte, um eine Vorschau des Security Incident anzuzeigen.
   Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Ticketwerte für den Security Incident.



Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in den -Fehlermeldungen beschrieben werden.

Nächste Maßnahme
Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung im Security Incident zufrieden sind. Definieren Sie den Zeitplan.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie einen Zeitplan für die Secureworks CTP-Ticketerfassung

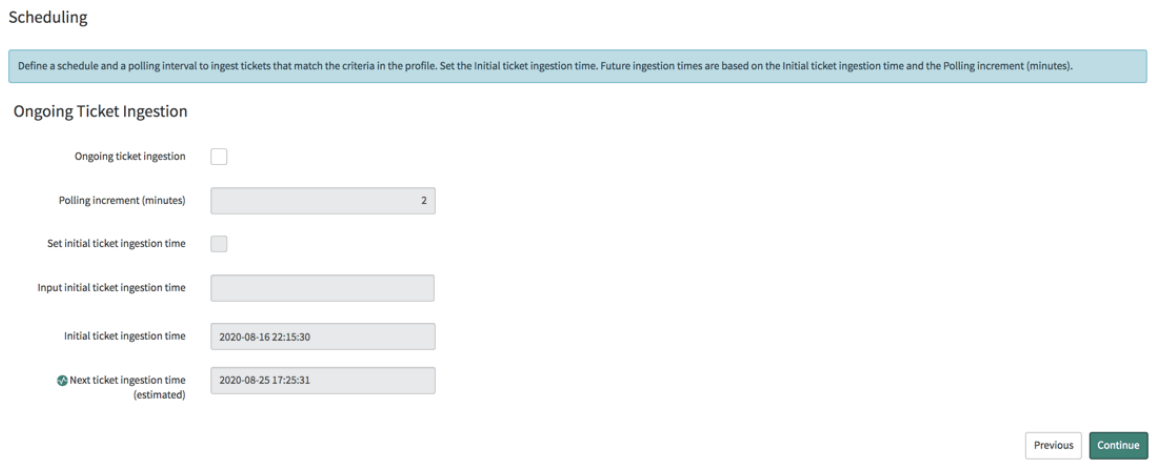
Überprüfen Sie die Standardeinstellungen für den Ticketabruf, oder ändern Sie die Zeitplanung nach Bedarf. Mit diesem Schritt können Sie Ihren Ticketabruf basierend auf einem Datumsbereich und einem Abfrageintervall filtern.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch auswählen, wie oft Sie zukünftige Tickets abfragen, die der Ticketprofilkonfiguration entsprechen. Konfigurieren Sie diese Abfrageintervalle für einzelne Profile. Bei der Planung möchten Sie möglicherweise die Systemlast gegen die Dringlichkeit des incident abwägen. Für jedes Profil ist ein Standardwert von einer Minute festgelegt. Sie können diese Einstellung jedoch je nach Dringlichkeit des incident und der erwarteten Auslastung Ihres Systems ändern.

Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **„Zeitplanung“**aus.
2. Wählen Sie eine aus, um zu planen, wie und wann Tickets aus dem Secureworks CTP -Portal abgerufen werden.



3. Klicken Sie auf **„Fortsetzen** “, um zur Seite „Zusätzliche Optionen“ zu navigieren.

Automatisieren Sie Ticketaktualisierungen und -schließungen basierend auf dem SIR-Incident-Status

Die Integration zur Erfassung von Tickets Secureworks CTP verfügt über eine bidirektionale Schnittstelle, die sowohl Tickets zum Erstellen von Security Incidents ermöglicht, als auch die Möglichkeit, die Tickets zu aktualisieren, sobald der Security Incident mit relevanten Incident-Details wie der Security Incident-Nummer erstellt und/oder geschlossen wird , Zuweisungsgruppe, Security Incident-URL usw.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Schließen Sie die Konfiguration für die Aktualisierung von Tickets ab, wenn der Security Incident erstellt wird.
3. Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen und das Profil in den Status **Warten** zu versetzen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Profil erfolgreich eingerichtet. Aktivieren Sie dieses Profil, um Tickets basierend auf Ihrer Zeitplanung aus dem -Portal Secureworks CTP abzurufen.

Optional: Kopieren Sie ein Secureworks CTP-Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich möglicherweise, Profile zu kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname zunächst geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es nicht versehentlich aktiviert wird, bevor die Konfiguration abgeschlossen wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

Prozedur

1. Navigieren zu **Alle** > **Integration zur Secureworks-Ticketerfassung** > **Secureworks-Profil**.
2. Wählen Sie in der Liste der Secureworks-Profile, die angezeigt wird, ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste **Aktionen für ausgewählte Zeilen aufKopieren**.
   Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Zeitplankonfiguration. Der Name des Profils enthält (Kopie). Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie an dieser Stelle deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.

   Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **„Aktiv“** auf „falsch“ festgelegt ist, da das Profil aktiviert werden muss.

Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren, nachdem Sie die Konfigurationsschritte abgeschlossen haben.

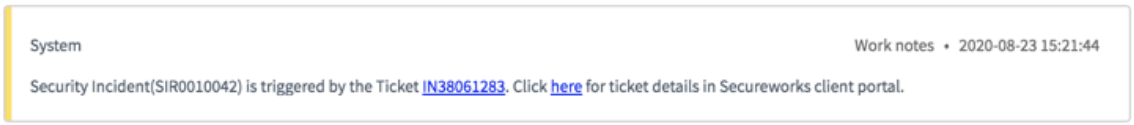
Das Security Incident Response-Formular ändert sich nach der Ticket-Erfassung

Nachdem ein Ticket Secureworks CTP erfasst wurde, wird ein Security Incident erstellt und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

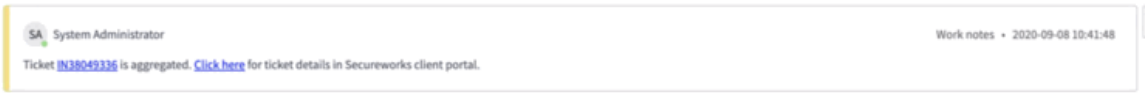
Arbeitsnotiz

Es wird eine Arbeitsnotiz mit Details zu dem Ticket veröffentlicht, das den Security Incident ausgelöst hat.



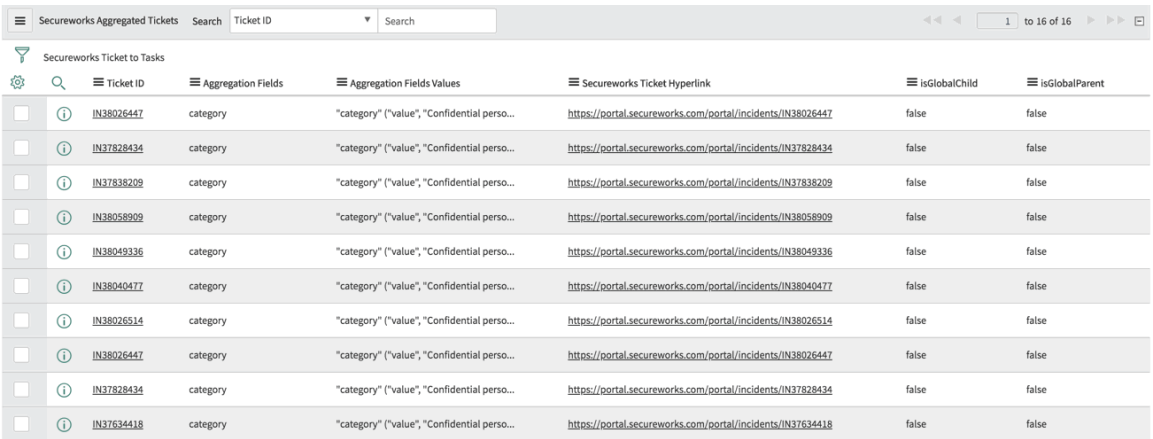
Klicken Sie auf den Ticket-Link, um zum internen Secureworks-Datensatz „Ticket zu Aufgabe“ zu navigieren. Über den Hyperlink **Hier klicken** gelangen Sie zum Dashboard Secureworks CTP, in dem Sie die Ticketdetails anzeigen können.

Wenn Sie die Option **Arbeitsnotiz für neues Ticket protokollieren** in den Ticket-Zusammenfassungskriterien ausgewählt haben, wie auf der Seite Profil erstellen: Zuordnung beschrieben, wird beim Aggregieren des Tickets eine Arbeitsnotiz veröffentlicht.



Aggregierte Tickets

Klicken **Zugehörige Listen** > **Aggregierte Secureworks-Tickets** um das mit dem Security Incident aggregierte Ticket anzuzeigen. Klicken Sie auf den Ticket-Hyperlink, um das Ticket im Dashboard Secureworks CTP anzuzeigen.



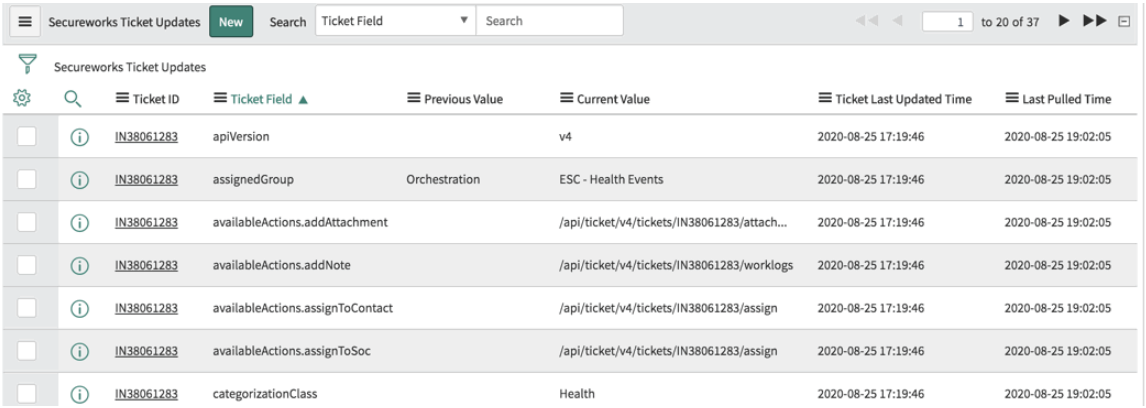
Security Incident erstellen: Wählen Sie ein Ticket aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie dann auf **Security Incident erstellen**. Mit dieser Option wird ein neuer Security Incident für das Ticket erstellt, und dieses Ticket wird aus dem übergeordneten Security Incident deaggregatiert.

Ticketdatensatz löschen: Wählen Sie ein Ticket aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie auf **Löschen**. Mit dieser Option wird der Ticketdatensatz gelöscht.

Secureworks-Ticketaktualisierungen

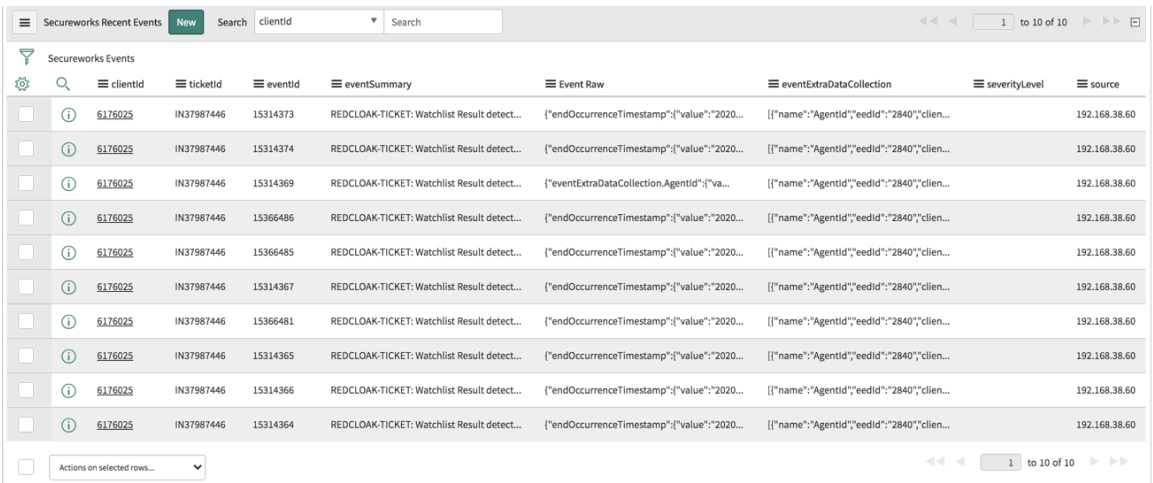
Dies zeigt die Standardticketfelder und verfolgt Änderungen an den Tickets während jedes Abfrageintervalls nach. Dies ist hilfreich, da Sie alle Ticket-Updates direkt anzeigen können, ohne zum Dashboard Secureworks CTP navigieren zu müssen. Alle Änderungen an den Werten werden in den Feldern Vorheriger Wert und Aktueller Wert angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aktuelle Secureworks-Ereignisse

Klicken Sie unter „ **Zugehörige Links“** auf die Option **Aktuelle Secureworks-Ereignisse abrufen,** um die neuesten Secureworks-Ereignisse anzuzeigen.



Standardmäßig werden maximal 50 Ereignisse angezeigt. Sie können diese Standardeinstellung in den Secureworks-Integrationseinstellungen ändern.

Zeigen Sie die Secureworks-Tickets und die entsprechenden Security Incidents an

Die importierten Secureworks CTP Tickets werden zunächst in der Tabelle „Ticketimport“ gespeichert. Zeigen Sie alle Secureworks CTP Tickets an, die importiert wurden, bevor Filterbedingungen angewendet wurden.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Integration zur Secureworks-Ticketerfassung** > **Sicherer Ticketimport**.
2. Sie können alle Secureworks CTP Tickets anzeigen, die importiert wurden, bevor sie zusammengefasst oder Filterbedingungen angewendet werden.
3. Klicken Sie auf eine Ticket-ID, um die Ticket-Rohdaten anzuzeigen.
4. Navigieren zu **Secureworks-Ticketerfassung** > **Secureworks-Ticket zu Aufgabe**.
   Die Tickets Secureworks CTP mit den entsprechenden Security Incidents werden angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Secureworks CTP Master – Hinweis zum Schließen von Tickets

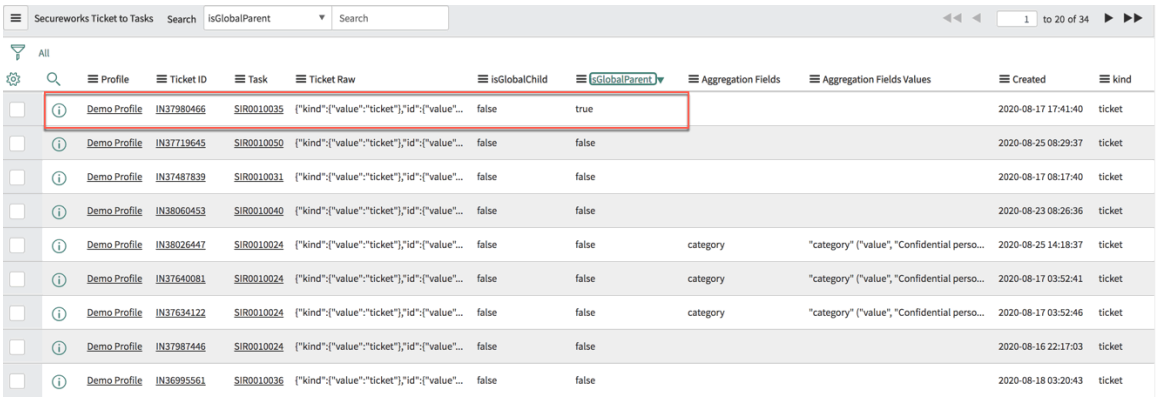
Bevor Sie einen Security Incident schließen, der von einem Secureworks CTP -Master-Ticket erstellt wurde, müssen Sie überprüfen, ob alle dem Master-Ticket zugeordneten untergeordneten Tickets geschlossen sind.

Vorbereitungen

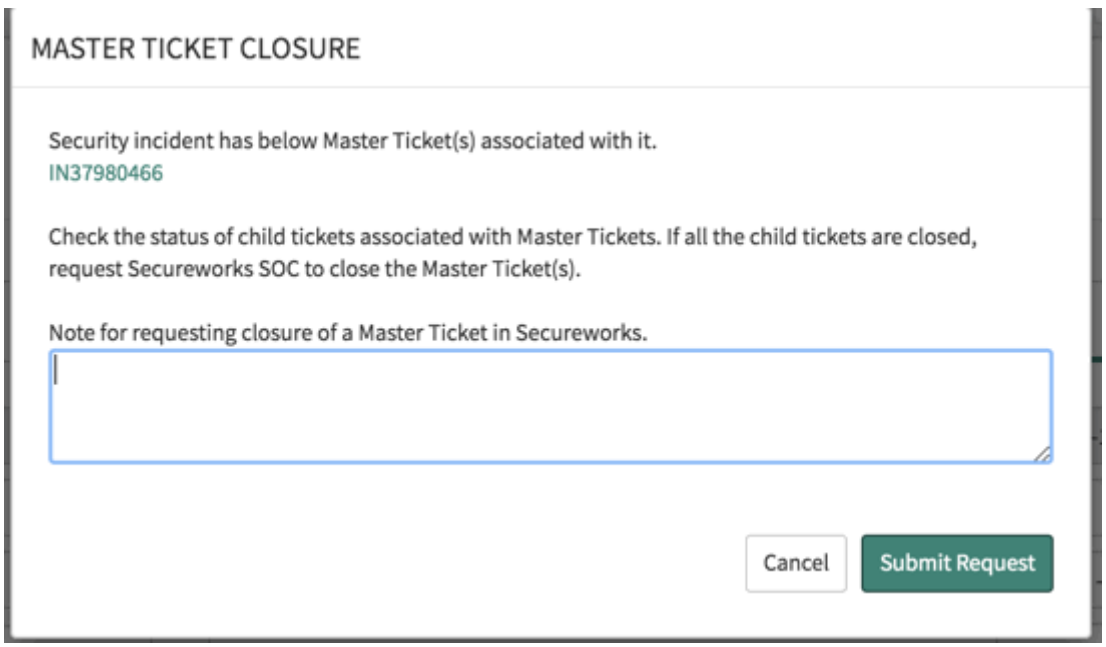
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Secureworks-Ticketerfassung** > **Secureworks-Ticket zu Aufgabe**.
   Die Tickets Secureworks CTP mit den entsprechenden Security Incidents werden angezeigt.



2. Klicken Sie auf den Security Incident, bei dem das Feld **isGlobalParent** auf **„true“ festgelegt ist.**
3. Ändern Sie den Status des Security Incidents in **Geschlossen**, geben Sie die Abschlusscodes an, und klicken Sie auf **Speichern**.
   Das folgende Dialogfeld wird angezeigt.



Dieser Security Incident ist einem Secureworks Master-Ticket zugeordnet. Einem Master-Ticket können mindestens ein untergeordnetes Ticket zugeordnet sein. Bevor das Master-Ticket geschlossen werden kann, müssen Sie zuerst überprüfen, ob alle untergeordneten Tickets, die diesem Master-Ticket zugeordnet sind, geschlossen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

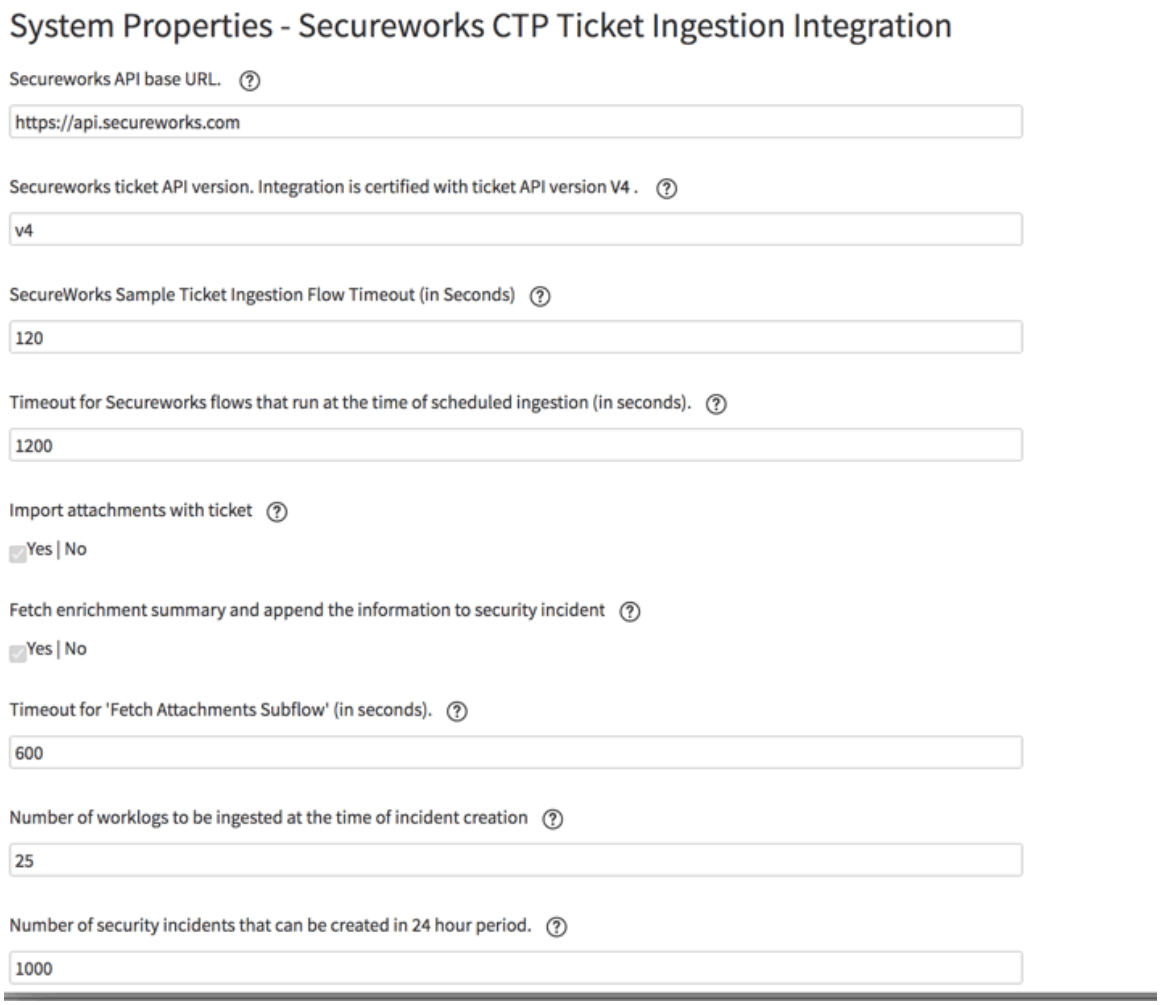
4. Fügen Sie eine Notiz hinzu, in der das Schließen des Master-Tickets in Secureworks angefordert wird, und klicken Sie auf **Anforderung senden**.
   Das Master-Ticket ist jetzt dem Secureworks SOC-Team zugewiesen.
5. Sobald die Anforderung übermittelt wurde, können Sie den Security Incident schließen.
6. Navigieren zu **Anwendung** > **Modul**.

Konfigurationseinstellungen für die Secureworks CTP-Integration

Verwenden Sie diese Option, um die Standardsystemeigenschaften der Integration der Secureworks CTP Ticketerfassung zu ändern.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **Integration zur Secureworks-Ticketerfassung** > **Secureworks-Integrationseinstellungen**.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.



Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

Integration von Security Incident Response mit zScaler

Sie können das Produkt Integration von Security Incident Response mit zScaler verwenden, um Ihre Zscaler Internet Access -Serverprotokolle (ZIA) mit Now Platformzu verbinden. Mit dieser

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration können Sie Dashboards anzeigen, anwenderdefinierte Warnungen erstellen und Security Incidents untersuchen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht

Das Internet- und Web-Gateway-Produkt Zscaler wird aus der -Cloud bereitgestellt. Bietet Ihnen die wichtigsten Datenpunkte und Einblicke in die Sicherheitsumgebung Ihres Unternehmens. Integration von Security Incident Response mit zScaler verbindet das Produkt Zscaler Internet Access mit Ihrer Instanz Now Platform. Durch die Verwendung des Produkts Zscaler auf dem Now Platformerhalten Sie mehr Einblicke in die Internetnutzung Ihrer Organisation.

Schlüsselfunktionen der Integration

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Reputationssuche von erkennbaren Elementen in der globalen Bedrohungsbibliothek, die vom Produkt Zscaler verwaltet wird.

  Hinweis:
  In der globalen Bedrohungsbibliothek Zscaler werden Bedrohungen nach Trends, Ursprungsland, Ziel, Volume und verschiedenen Bedrohungskategorien aufgelistet. Mit dieser globalen Bedrohungsbibliothek können Sie Ihre erkennbaren Elemente anhand der globalen Bedrohungslandschaft untersuchen.

- Wartung von erkennbaren Elementen in einer Sperrliste oder Allow-Liste für das Produkt Zscaler.
- Möglichkeit zum Abrufen und Überprüfen von Sandbox-Berichten aus dem Produkt Zscaler für einen MD5-Hash. Die Cloud-Sandbox-Funktion im Produkt Zscaler wird in einer virtuellen Umgebung ausgeführt und analysiert Dateien, um böswilliges Verhalten zu erkennen.
- Sicherheitswarnungen von „Patient 0“-Ereignissen, die im Produkt Zscaler generiert werden, wenn ein Benutzer eine unbekannte schädliche Datei herunterlädt.
- Mehrere URL-Kategorielisten, die als Sperrlisten oder Allow-Listen fungieren, wie im Produkt Zscaler definiert.
- Now Platform Security Incidents, die mit Tags versehen werden können, um die URL-Kategorie zu identifizieren, der die erkennbaren Elemente hinzugefügt werden.
- Ablaufzeiträume, die die Größe der URL-Kategorielisteneinträge beibehalten, indem die älteren Einträge automatisch ablaufen oder entfernt werden.
- Genehmigungsworkflow zum Hinzufügen und Entfernen von erkennbaren Elementen zu den URL-Kategorielisten.
- URL-Kategorieeinträge, die mit erkennbaren Datensätzen und Security Incidents verknüpft werden können, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
Zscaler Website mit Produktdokumentation	Website mit der Produktdokumentation für ZScaler
ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

Erste Schritte mit Integration von Security Incident Response mit zScaler

Aktivieren Sie das Produkt Zscaler Internet Access, und richten Sie es als Schnittstelle mit Ihrer Instanz Now Platform und dem Produkt Security Incident Response ein.

Prüfliste

Setupaufgabe	Beschreibung

Weisen Sie die erforderlichen Rollen Now Platform und Security Incident Response zu, und überprüfen Sie sie.	Diese Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich:
	• Die Rolle admin installiert die Integration aus ServiceNow Store und weist die Rolle sn_si.admin zu.
	• Die Rolle sn_si.admin führt die folgenden Aufgaben aus:
	  ○ Konfiguriert die Integration.
	  ○ Erstellt, aktiviert und entfernt die URL-Kategorielisten.
	  ○ Weist die Rolle sn_si.analyst zu.
	• Die Rolle sn_si.analyst erstellt Einträge und arbeitet mit Security Incidents.

Stellen Sie sicher, dass die Kernanwendungen ServiceNow installiert und aktiviert sind, bevor Sie diese Integration konfigurieren.	Das Plugin ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] ist erforderlich. Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten für das Produkt Security Incident Response. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen für die Integration installieren und aktivieren. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Wenn diese Anwendungen noch nicht installiert sind, installieren und aktivieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	Sie sie nacheinander in der folgenden Reihenfolge: **1.** Security Incident Response Abhängigkeit (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration **5.** Threat Intelligence Support Common **6.** Trusted Security Circles **7.** Security Operations Setup-Assistent **8.** Security Incident Response
Überprüfen Sie die Versionen Zscaler.	• Diese Integration wird ab Zscaler Internet Access Version 1.0 oder höher unterstützt. • Diese Integration wird mit den folgenden Zscaler -Versionen getestet: ○ Zscaler Client Connector für Windows – 3.0 ○ Zscaler Client Connector für macOS – 3.0 ○ Zscaler Client Connector für Linux – Beta ○ Zscaler Cloud Connector – 6.1
Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen Zscaler verfügen und konfiguriert haben Zugriff auf Zscaler Internet Access APIs.	• Sie müssen über die Administratoranmeldeinformationen für Zscaler Internet Accessverfügen. • Sie müssen über ein gültiges Abonnement für die Cloud-Service-API verfügen. Zscaler Der Support muss Ihren Schlüssel bereitstellen. • Sie benötigen Zscaler Internet Access Administrator-Anmeldeinformationen (Anwendername und Passwort). Die API-Authentifizierung basiert auf einer Kombination aus dem API-Schlüssel und Zscaler Internet Access den Administratoranmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	Hinweis: Weitere Informationen zum Verwalten der Zscaler Internet Access -API-Schlüssel finden Sie in der Zscaler-Dokumentation .

Konfigurieren Sie den Zugriff auf Zscaler Internet Access APIs

Konfigurieren Sie den Zugriff auf den Server Zscaler Internet Access, um die sichere Verbindung zwischen der Instanz Now Platform und dem Server Zscaler zu authentifizieren.

Vorbereitungen

Erforderliche Rolle: Zscaler Internet Access admin

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Zscaler Ihr API-Abonnement für den Cloudservice Ihrer Organisation aktiviert hat, ist es auf der Seite für die Verwaltung von API-Schlüsseln Zscaler Internet Access mit der Basis-URL verfügbar. Ihre Organisation kann nur einen API-Schlüssel oder ein Token haben. Löschen Sie den vorhandenen Schlüssel oder das Token, bevor Sie einen neuen hinzufügen.

Die Basis-URL für die API lautet `${Cloud_Name}/api/v1`. Überprüfen Sie den Cloud-Namen Zscaler, der für Ihre Organisation bereitgestellt wurde, und verwenden Sie ihn, um `{Cloud_Name}` im Basis-URI zu ersetzen. Einige Beispiele für die Basis-URL sind:

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

Hinweis:
Weitere Informationen zum -Administrationsportal Zscaler Internet Access finden Sie in der Dokumentation zur Zscaler-API-Schlüsselverwaltung und in der Dokumentation zum Zscaler-Portal .

Prozedur

1. Melden Sie sich als Administrator beim -Administrationsportal Zscaler Internet Access an.
2. Navigieren zu **Administration** > **API-Schlüsselverwaltung**.
3. Klicken Sie auf **API-Schlüssel hinzufügen**.
   Wenn die Option **API-Schlüssel hinzufügen** nicht angezeigt wird, löschen Sie den vorhandenen Schlüssel.
   Der neue API-Schlüssel ist sofort gültig und wird auf der Registerkarte angezeigt.

Ergebnisse

Sie haben die Basis-URL und den API-Schlüssel abgerufen, um den Zugriff auf Zscaler aus der Instanz Now Platform zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration von Security Incident Response mit zScaler installieren und konfigurieren

Installieren und konfigurieren Sie das Produkt „Internetzugriff“ von ServiceNow StoreIntegration von Security Incident Response mit zScaler, um die Integration in Ihrer Instanz Now Platform von zu verwenden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie das Produkt Integration von Security Incident Response mit zScaler von ServiceNow Store herunter, und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel Integration von Security Incident Response mit zScaler, und klicken Sie darauf **Konfigurieren** > **Neue Konfiguration erstellen**.
4. Füllen Sie die Felder des Formulars aus.

Zscaler Konfigurationsformular

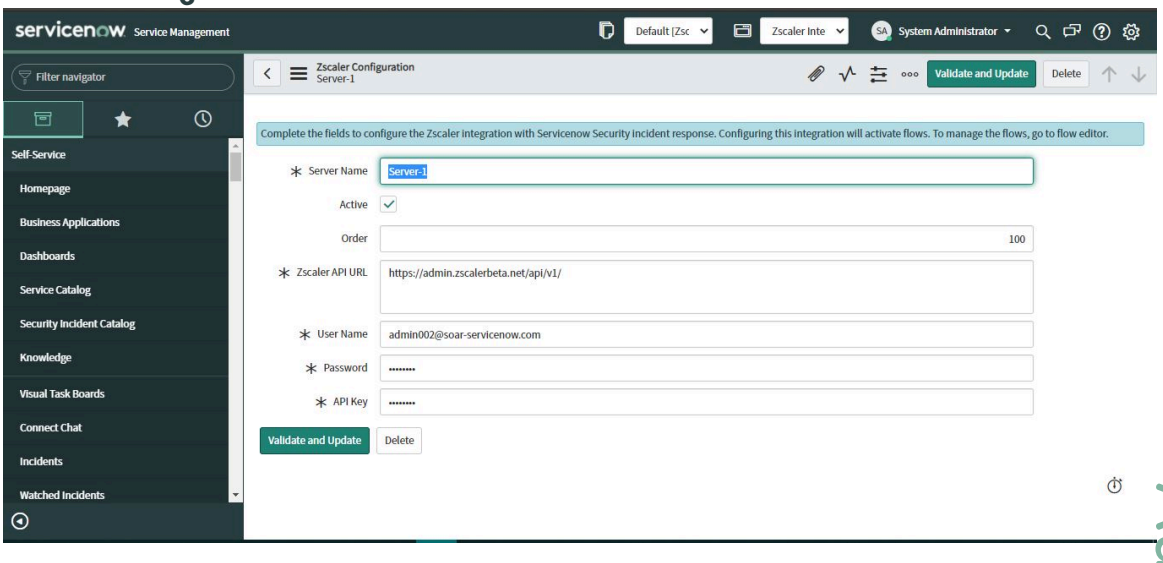
Feld	Beschreibung
Servername	Zscaler Servername. Beispiel: ZSserver.
Aktiv	Indikator, der angibt, dass das Profil aktiv ist.
Bestellung	Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge der Workflows an, wenn zwei oder mehr Profile auslösende Bedingungen gemeinsam nutzen. Der Flow mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Beispiel: 100, 200, 300, 400. Der Standardwert ist 100.
Zscaler API-URL	Basis-URL, die die Zscaler -API hostet. Beispiel: https://example.zscalerbeta.net
Anwendername	Anwendername für das Administratorkonto Zscaler Internet Access
Passwort	Passwort für den Administrator-Account Zscaler Internet Access.
API-Schlüssel	API-Schlüssel, den Sie vom -Administrationsportal Zscaler Internet Access abgerufen haben.

Das folgende Beispiel zeigt die Zscaler-Konfigurationsseite.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ZScaler-Konfigurationsseite



5. Klicken Sie auf **Validieren und aktualisieren**.

Ergebnisse

Nachdem Sie diese Konfiguration validiert und gespeichert haben, kehren Sie zur Seite Zscaler Konfigurationen zurück.

Fügen Sie URL-Kategorielisten Zscaler Internet Access hinzu

Fügen Sie die URL-Kategorien, die im Internetzugriffsprodukt Zscaler verfügbar sind, der Instanz Now Platform hinzu, um für jede URL eine Aktion anzugeben und die granulare Filterung und Richtlinienerstellung zu erleichtern.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Integration von Security Incident Response mit zScaler bietet eine URL-Kategorielisten mit standardmäßiger Allow-Liste und Deny-Liste zum Filtern von Inhalten.

Die URL-Kategorien, die Sie in der Instanz Now Platform hinzufügen, sollten sich bereits in Ihrer Umgebung Zscaler Internet Access befinden. Sie können Integration von Security Incident Response mit zScaler nicht verwenden, um URL-Kategorien in Zscalerzu erstellen.

Hinweis:
Weitere Informationen zu URL-Kategorielisten im Produkt Zscaler finden Sie in der Zscaler-Dokumentation zu URL-Kategorien .

Prozedur

1. Navigieren zu **Alle** > **zScaler-Integration** > **ZScaler URL-Kategorielisten**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zscaler Formular „URL-Kategorielisten“.

Feld	Beschreibung
Quelle	Name des Servers. Sie können nur die zuvor konfigurierten Zscaler Internet Access -Server aus der URL-Kategorieliste anzeigen.
Aktiv	Indikator, der angibt, dass die URL-Kategorieliste aktiv ist.
URL-Kategorie	Feld, das aktiviert wird, nachdem Sie die Quelle ausgewählt haben. Sie können die Liste der URL-Kategorien anzeigen, die in Zscalererstellt werden.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der URL-Kategorieliste. 0 (standardmäßig) gibt an, dass der URL-Kategorielisteneintrag nie abläuft. Durch Ändern dieses Werts ist jedes erkennbare Element, das dieser URL-Kategorie hinzugefügt wurde, für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Wenn Sie beispielsweise einen Ablaufzeitraum von 30 Tagen festlegen, werden die Einträge nach 30 Tagen aus der Kategorieliste entfernt.
Tag anzeigen	Sicherheits-Tag, das im Security Incident SIR angezeigt wird. Wenn Sie die Option **Tag anzeigen** aktivieren, ist das Feld Zscaler Tag für erkennbare Elemente im Formular verfügbar.
Change-Anforderung erstellen	Change-Anforderung und Change-Aufgaben in Ihrer Instanz Now Platform für die Datensätze, die an die URL-Kategorieliste angehängt sind. Wenn Sie die Option **Change-Anforderung erstellen** aktivieren, ist das Feld **Change-Anforderung** im Formular verfügbar.
Genehmigung erforderlich	Liste der Genehmigergruppen. Nachdem Sie eine Anforderung gesendet haben, ist eine Genehmigung durch die Gruppe erforderlich, um die Anforderung abzuschließen. Wenn Sie die Option **Genehmigung erforderlich** aktivieren, sind die Felder **Genehmiger zum Hinzufügen erkennbarer Elemente** und **Genehmiger zum Entfernen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erkennbarer Elemente im Formular verfügbar. ○ **Genehmiger für das Hinzufügen erkennbarer Elemente**: Wählen Sie die Genehmiger mithilfe der Suche aus, um die erkennbaren Elemente auf der Seite mit der **Zscaler-URL-Kategorieliste** hinzuzufügen. Mit dieser Option können Sie die Anwendergruppe(n) für Genehmigungen hinzufügen. ○ **Genehmiger für das Entfernen erkennbarer Elemente**: Wählen Sie die Genehmiger zum Entfernen der erkennbaren Elemente mithilfe der Suche auf der Seite mit der **Zscaler-URL-Kategorieliste** aus. Mit dieser Option können Sie die Anwendergruppe(n) aus der Genehmigungsliste entfernen.
Beschreibung	Beschreibung der URL-Kategorieliste Zscaler Verwenden Sie dieses Feld, um weitere Details zum URL-Kategoriedatensatz hinzuzufügen.

4. Klicken Sie auf **Absenden**.
   Eine erfolgreiche Übermittlung löst eine E-Mail-Benachrichtigung an die Genehmigungsgruppe aus.

Senden Sie erkennbare Elemente aus einem Security Incident-Datensatz an eine URL-Kategorieliste

Senden Sie erkennbare Elemente, die an einen Security Incident-Datensatz angehängt sind, mithilfe der Zulassungs- oder Blockierungsanforderung an eine konfigurierte URL-Kategorieliste. Durch Hinzufügen erkennbarer Elemente zur Zulassungs- oder Sperrliste für Sicherheitsscans können Anwender Inhalte von diesen URLs überprüfen und Zugriff auf vertrauenswürdige Inhalte erhalten.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

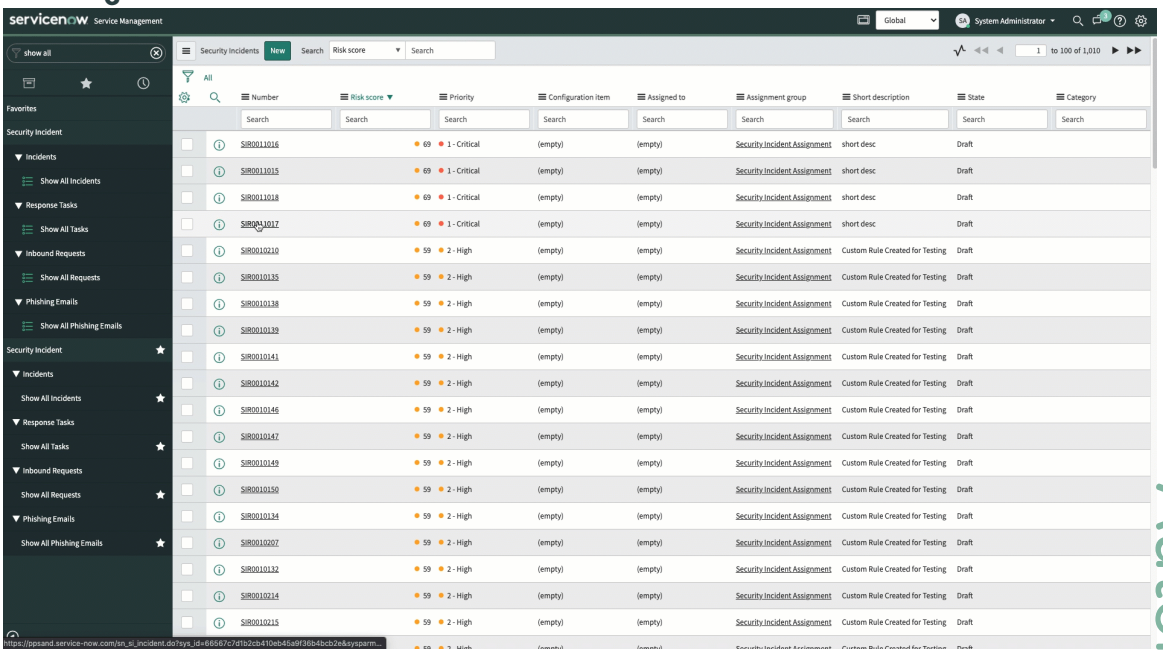
Warum und wann dieser Vorgang ausgeführt wird
Sie übermitteln Einträge erkennbarer Elemente, indem Sie die Anforderungsaktion „Zulassen“ oder „Blockieren“ in der zugehörigen Liste „Zugeordnete erkennbare Elemente“ verwenden. Erkennbare Elemente sind Artefakte, die in einem Netzwerk oder Betriebssystem gefunden werden und wahrscheinlich auf einen Angriff hindeuten. Verwenden Sie die Liste der zuvor konfigurierten URL-Kategorien, um das erkennbare Element auszuwählen, das Sie übermitteln möchten. Nachdem Sie die Anforderung übermittelt haben, wird eine Genehmigungsanforderung an Ihre Genehmigungsgruppe gesendet.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
   In diesem Beispiel erfahren Sie, wie Sie einen Security Incident und ein erkennbares Element auswählen und eine Allow-Liste hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinzufügen einer Allow-Liste



2. Wählen Sie den Security Incident aus, den Sie der Zulassungs- oder Blockierungsanforderung Zscaler zuordnen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete erkennbare Elemente**.
   Wenn Sie keine erkennbaren Elemente finden, klicken Sie auf **Neu**.
4. Wählen Sie ein erkennbares Element aus, und klicken Sie dann im Aktionsmenü auf **Allow/Block Request (Anforderung zulassen/blockieren)**.
5. Wählen Sie im Dialogfeld „Anforderung zulassen/blockieren“ aus, ob die Anforderung „Zulassen“ oder „Blockieren“ für das erkennbare Element ausgeführt werden soll.
6. Klicken Sie auf **Absenden**.
7. Zeigen Sie in den Arbeitsnotizen den Status Ihrer Übermittlung und die Sicherheits-Tags an.
   Klicken Sie auf die Links in den Arbeitsnotizen, um weitere Informationen zum Status zu erhalten oder die Details zu Workflow-Studiozu analysieren. Sicherheits-Tags sind Metadaten im antwortenden Datensatz und definieren, wer Zugriff auf bestimmte Arten von Sicherheitsinhalten haben soll.
8. Um den Status des von Ihnen ausgewählten erkennbaren Elements anzuzeigen, navigieren Sie zu **Zscaler-Integration** > **Zscaler-URL – Kategorielisteneinträge**.
9. Klicken Sie auf der Seite Zscaler-URL-Kategorielisteneinträge auf das erkennbare Element, um den Datensatz anzuzeigen.

Genehmigen Sie erkennbare Elemente für URL-Kategorielisten

Genehmigen Sie erkennbare Elemente, die einer URL-Kategorieliste hinzugefügt werden, sodass sich erkennbare Elementeinträge in den entsprechenden Zulassungs- oder Deny-Listen befinden.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zscaler-Integration** > **Zscaler-Genehmigungen**.
2. Wählen Sie den zu genehmigenden Datensatz aus.
3. Klicken Sie auf **Genehmigen**.
   Die Genehmigergruppe erhält eine E-Mail-Benachrichtigung über die Genehmigungsanforderung. Nachdem die Genehmiger in der E-Mail auf den Link **Genehmigen/Ablehnen** geklickt haben, ändert sich der Status in Genehmigt.

Übermitteln Sie den Security Incident an die URL-Kategorieliste Zscaler.

Übermitteln Sie Einträge direkt für erkennbare Elemente, die keinem bestimmten Now Platform -Security Incident-Datensatz zugeordnet sind, damit erkennbare Einträge in den entsprechenden Zulassungs- oder Deny-Listen enthalten sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können der URL-Kategorieliste auch direkt aus dem Datensatz „Erkennbares Element“ erkennbare Elemente hinzufügen.

Prozedur

1. Navigieren zu **Alle** > **Zscaler-Integration** > **Zscaler-URL – Kategorielisteneinträge**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Zscaler Formular „URL-Kategorielisten-Einträge“.

Feld	Beschreibung
Eingabewert	Name des erkennbaren Elements. Wenn ein übereinstimmendes erkennbares Element gefunden wird, wird der Rest des Formulars automatisch ausgefüllt. Wenn kein übereinstimmendes erkennbares Element gefunden wird, müssen Sie die restlichen Informationen manuell eingeben.
Erkennbares Element	Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.
Erkennbarer Typ	Klassifizierung erkennbarer Elemente, z. B. IP-Adresse oder Datei-Hash.
URL-Kategorieliste	URL-Kategorie. Wenn eine Organisation beispielsweise „example.com“ für Office 365-Services verwendet, kategorisiert Zscaler „example.com“ als Professional Services und Office 365.
Quelle	Name des Servers. Sie können nur die zuvor konfigurierten Zscaler -Server aus der URL-Kategorieliste anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Incident-Anzahl	Anzahl der Incidents, in denen dieses erkennbare Element angezeigt wird. Dieser Wert wird automatisch aktualisiert, wenn das erkennbare Element manuell oder über einen Workflow zu einem anderen Incident hinzugefügt wird.
Aktiv	Indikator, der angibt, dass die URL-Kategorieliste aktiv ist.
Status	Status, wenn das erkennbare Element genehmigt oder abgelehnt wird.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der URL-Kategorieliste. 0 (standardmäßig) gibt an, dass der URL-Kategorielisteneintrag nie abläuft. Durch Ändern dieses Werts ist jedes erkennbare Element, das Sie dieser URL-Kategorie hinzufügen, für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Wenn Sie beispielsweise einen Ablaufzeitraum von 30 Tagen festlegen, werden die Einträge nach 30 Tagen aus der Kategorieliste entfernt. **Hinweis:** Wenn Sie den standardmäßigen Ablaufzeitraum des URL-Kategorielisteneintrags ändern, wird eine Warnung angezeigt, dass der Zeitraum von dem Zeitraum abweicht, der in der ausgewählten URL-Kategorieliste konfiguriert ist.
Zusätzliche Informationen	Feld, in dem Sie weitere Details zum erkennbaren Element hinzufügen können.

4. Klicken Sie auf **Absenden**.

Führen Sie eine Bedrohungssuche mithilfe der globalen Bedrohungsbibliothek Zscaler durch

Führen Sie mithilfe der globalen Bedrohungsbibliothek des Produkts Zscaler Internet Access eine Bedrohungssuche für ein erkennbares Element aus. Zscaler unterstützt Suchen nach erkennbaren Elementen vom Typ IPs, URLs und Domänen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Threat Intelligence-Suchen für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Wenn ein erkennbares Element zum ersten Mal einem Security Incident zugeordnet wird, führen alle aktiven Implementierungen der Bedrohungssuche in Now Platform eine

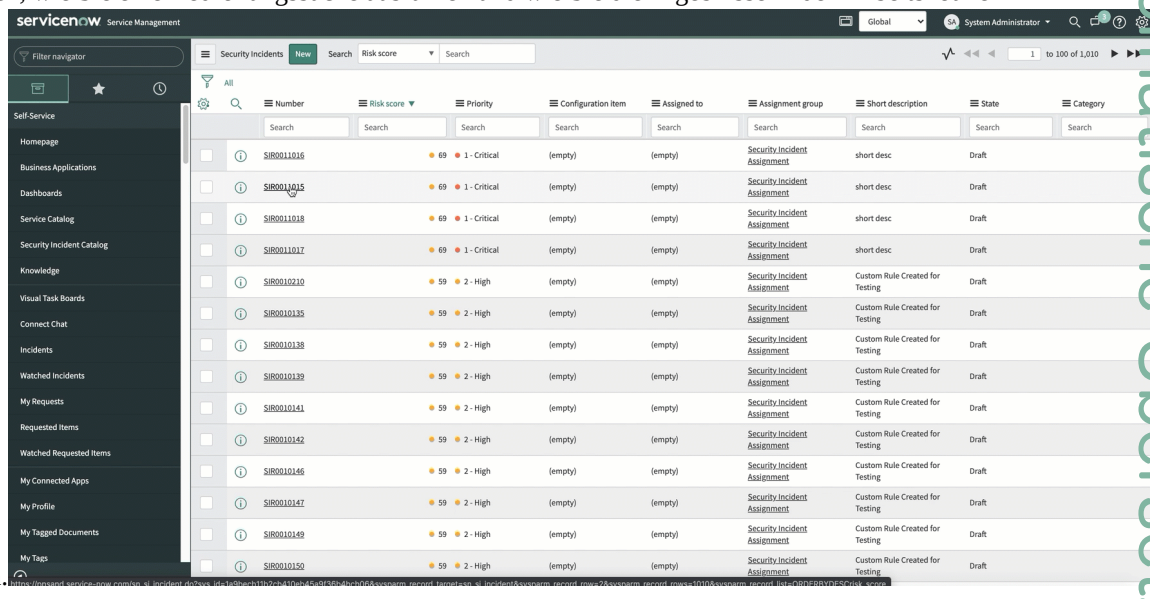
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

automatische Bedrohungssuche durch. Sie können die Ergebnisse in der zugehörigen Liste „Ergebnisse der Bedrohungssuche“ anzeigen.

Standardmäßig wird die Konfiguration mit dem niedrigsten Ordnungszahlwert für die Durchführung der Bedrohungssuche in der globalen Bedrohungsbibliothek des Produkts Zscaler Internet Access ausgewählt. Sie können die Bedrohungssuche auch manuell durchführen.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, für den Sie die Bedrohungssuche ausführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete erkennbare Elemente**.
4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü „Aktionen **“ auf Bedrohungssuche ausführen**.
   In diesem Beispiel erfahren Sie, wie Sie einen Security Incident und ein erkennbares Element auswählen, wie Sie eine Bedrohungssuche ausführen und wie Sie die Ergebnisse in den Arbeitsnotizen anzeigen.



Ergebnisse

Nachdem Sie die Bedrohungssuche initiiert haben, können Sie in den Arbeitsnotizen den Status Ihrer Übermittlung einsehen.

Übermitteln Sie an die Sandbox-Analyse Zscaler .

Verwenden Sie den Sandbox-Service für Zscaler Internet Access -Produkte, um Dateien in einer virtuellen Umgebung zu analysieren und böswilliges Verhalten zu erkennen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine Zscaler -Konfiguration erstellen, wird im Modul Zscaler-Sandbox-Konfiguration standardmäßig eine Sandbox-Übermittlung Zscaler erstellt.

Die Felder „Name“ und „Quelle“ werden automatisch gefüllt, und die Konfiguration ist standardmäßig aktiviert. Sie können nur das Anzeige-Tag und die aktiven Optionen

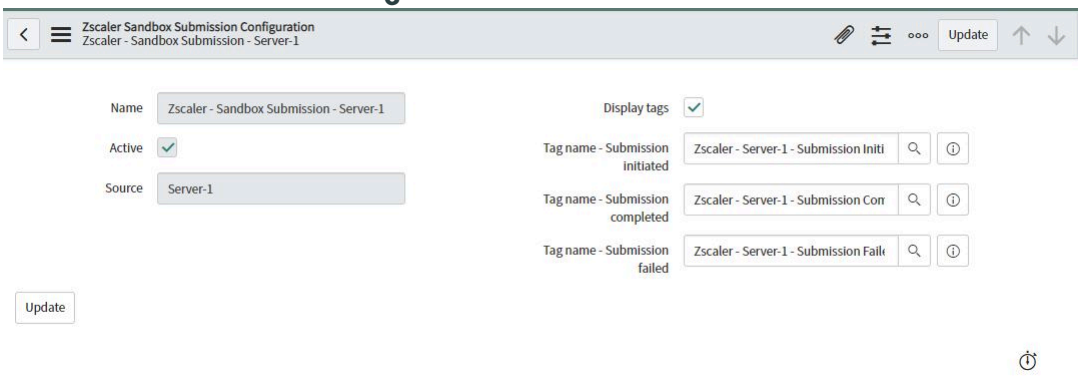
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bearbeiten. Mit dem Produkt Zscaler Internet Access können Sie nur den Sandbox-Bericht für erkennbare Elemente vom Typ MD5-Hash abrufen.

Die Analyse für die Datei, die dem MD5-Hash zugeordnet ist, sollte abgeschlossen sein, und der entsprechende Bericht sollte sich in der Sandbox Zscaler befinden. Wenn der von Ihnen gesendete MD5-Hash keinen Bericht in Zscalerenthält, erhalten Sie eine Fehlermeldung.

Zscaler-Sandbox-Übermittlung



Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, für den Sie die Sandbox-Analyse ausführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete erkennbare Elemente**.
4. Wählen Sie ein erkennbares Element vom Typ MD5-Hash aus, und wählen Sie dann im Menü Aktionen **die Option An die Sandbox übermitteln**aus.
   Erstellen Sie ein erkennbares Element vom Typ MD5-Hash, wenn Sie kein vorhandenes erkennbares Element vom Typ MD5-Hash finden.
5. Wählen Sie im Dialogfeld „Dateiübermittlung“ in der Übermittlungskonfiguration die Option **Zscaler - Sandbox-Übermittlung - Server** aus, und klicken Sie auf **An Sandbox übermitteln**.
   Nachdem Sie die Sandbox-Übermittlung initiiert haben, können Sie in den Arbeitsnotizen den Status Ihrer Übermittlung einsehen. Dem Security Incident wird auch ein -Tag angehängt.
6. Klicken Sie in den Arbeitsnotizen auf den Link im Beitrag Sandbox-Übermittlungsergebnis.

Ergebnisse

Sie können die Ergebnisse auch auf der Registerkarte Alle zugehörigen Listen und Sandbox-Übermittlungsergebnisse anzeigen anzeigen.

Richten Sie E-Mail-Warnungen für „Patient 0“-Ereignisse ein

Konfigurieren Sie das Produkt Zscaler Internet Access so, dass unbekannte, potenziell schädliche Dateien (z. B. Patient 0-Ereignisse) erkannt und danach gesucht werden, damit Sie Ihr Netzwerk vor schädlichen Dateien schützen können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, Zscaler Internet Access admin

Warum und wann dieser Vorgang ausgeführt wird

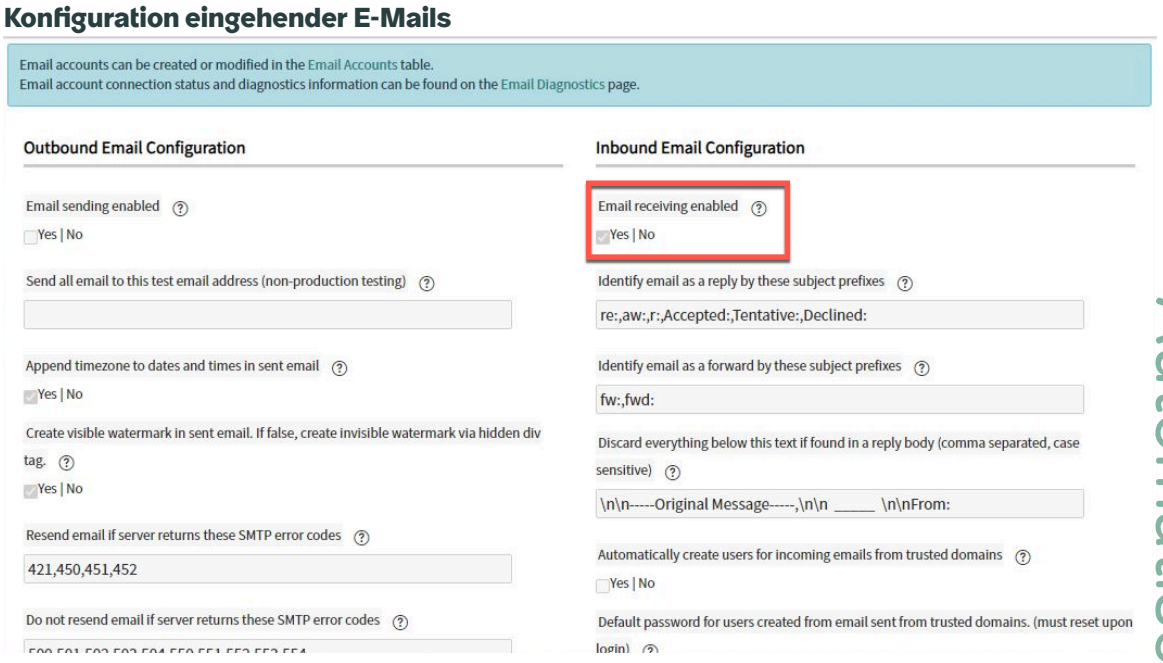
Patient O ist eine Warnungsklasse, die eine unbekannte Datei enthält, deren Download genehmigt wurde, die jedoch als schädlich befunden wurde. Das Ereignis „Patient 0“ wird als kritisch eingestuft. Sie können den Now Platform so einrichten, dass er in regelmäßigen Abständen E-Mail-Benachrichtigungen für Patient 0-Ereignisse erhält.

Automatische Übersetzung

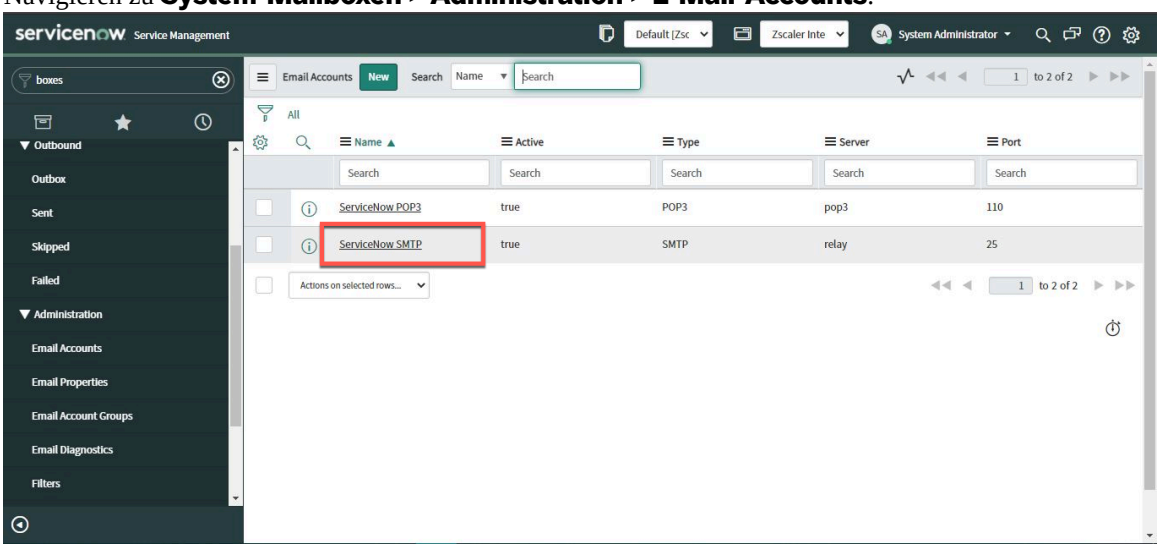
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Mailboxen** > **Administration** > **E-Mail-Eigenschaften**.
2. Wählen Sie im Abschnitt „Konfiguration eingehender E-Mails“ die Option **E-Mail-Empfang aktiviert aus**.



3. Klicken Sie auf **Speichern**.
4. Navigieren zu **System-Mailboxen** > **Administration** > **E-Mail-Accounts**.

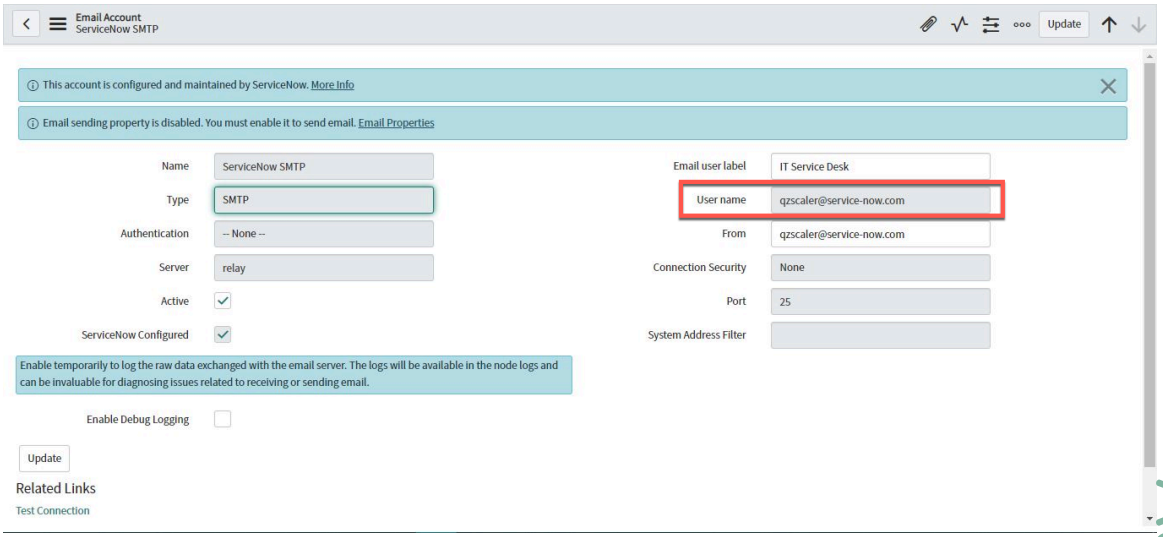


5. Wählen Sie den E-Mail-Account **ServiceNow SMTP** aus.
   Notieren Sie sich den Anwendernamen. Der hier identifizierte Anwendername ist die E-Mail-Adresse Now Platform, die Sie in Zscaler für die Konfiguration von Patienten-0-Warnungen verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendername für das Now Platform SMTP-Konto



6. Melden Sie sich beim -Administrationsportal Zscaler Internet Access an.

> **Hinweis:**
> Weitere Informationen zum -Administrationsportal Zscaler Internet Access finden Sie in der Zscaler-Dokumentation .

7. Navigieren zu **Administration** > **Warnungen** > **Warnungen veröffentlichen**.
8. Klicken Sie **auf Warnungsabonnement hinzufügen**.
9. Füllen Sie die Felder des Formulars aus.

Formular „Warnungsabonnement hinzufügen“.

Feld	Beschreibung
E-Mail	Now Platform E-Mail-Adresse des SMTP-Accounts.
Beschreibung	Feld zum Hinzufügen weiterer Details zu den Patienten-0-Warnungen

10. Klicken Sie auf **Speichern**.

ServiceNow Security Operations -Add-on für die Splunk-Übersicht

Mit dem Add-on ServiceNow Security Operations für Splunk kann ein Splunk -Softwareadministrator in Now PlatformDaten sammeln und Incidents und Ereignisse erstellen.

Das Add-on wird über Splunkbase installiert.

> **Wichtig:**
> Splunk wird auch für die MSP-Umgebung (Managed Service Provider) unterstützt.

Setup der Splunk-Integration

Die Setup-Verfahren für das Add-on ServiceNow Security Operations für Splunk umfassen das Herunterladen der Add-on-Datei in Splunk, die Installation des Add-ons und das Einrichten der Instanz ServiceNow, in der Security Incidents und Ereignisse erstellt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle

Bevor Sie Setupverfahren für die Splunk-Integration durchführen, müssen Sie in Ihrer ServiceNow-Instanz einen Integrationsbenutzer mit den Rollen „sn_si.integration_user“ und „sn_si.analyst“ definieren. Darüber hinaus benötigen Sie zum Durchführen von Importen die Rolle import_transformer, um Lese- und Schreibberechtigungen für die Sicherheitstabellen zu erhalten. Die Rolle „sn_si.integration_user“ muss mit dem Abschnitt „import_transformer“ der Rolle definiert werden.

Laden Sie die Anwendung ServiceNow Security Operations herunter

Der erste Schritt beim Einrichten der ServiceNow-to-Splunk-Integration besteht darin, die Anwendung ServiceNow Security Operations von Splunkbase herunterzuladen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie Splunkbase.
2. Suchen Sie nach ServiceNow Security Operations Integration .
3. Laden Sie die Anwendung herunter.

Installieren Sie das Add-on „ServiceNow Security Operations“ für Splunk

Installieren Sie das **Add-on „ServiceNow Security Operations“ für Splunk,** um Splunk mit ServiceNowzu verknüpfen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie Splunk.
2. Klicken Sie entweder auf das **Apps** -Zahnradsymbol oder auf das Kontextmenüelement **Apps verwalten**.
3. Klicken Sie auf **App aus Datei installieren**.
4. Klicken Sie **auf Datei auswählen**, wählen Sie sn_sec_ops.spl aus, und klicken Sie auf **Hochladen**.
5. Starten Sie Splunkneu, wenn Sie dazu aufgefordert werden.
   Das Add-on ServiceNow Security Operations für Splunk ist installiert und kann eingerichtet werden.

Richten Sie die Instanz ein, in der Incidents oder Ereignisse erstellt werden, oder ändern Sie sie

Um die Instanz ServiceNow, in der neue Security Incidents und Sicherheits-Ereignisse erstellt werden, einzurichten oder zu ändern, verwenden Sie die Aktion Setup in der Anwendungsliste.

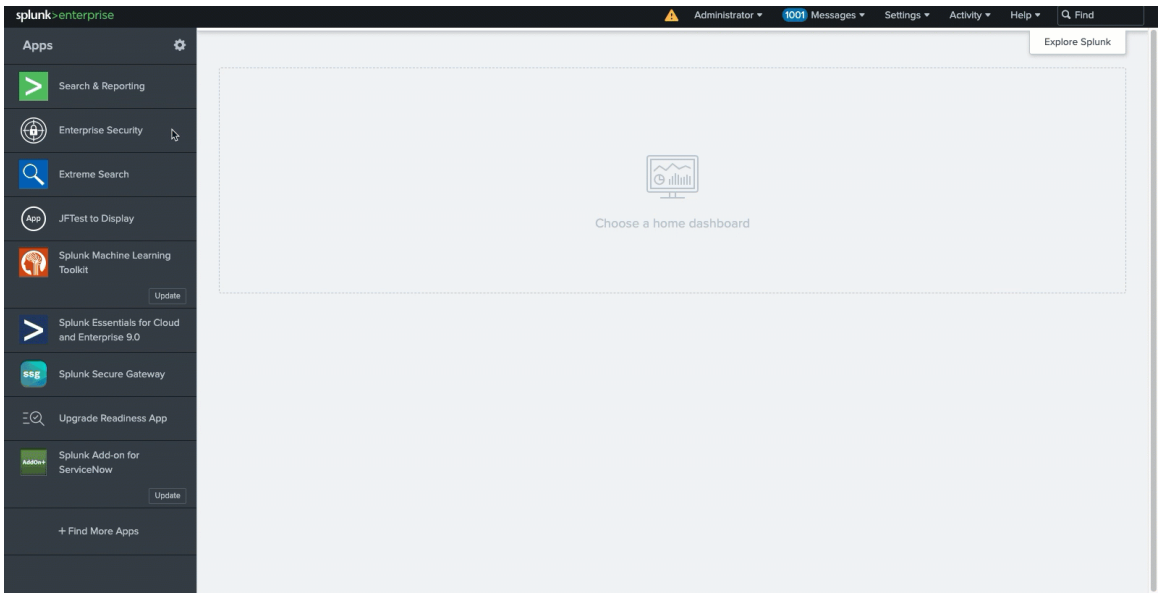
Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Öffnen Sie **Splunk**.
2. Klicken Sie entweder auf das **Apps** -Zahnradsymbol oder auf das Kontextmenüelement **Apps verwalten**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Suchen Sie in der Liste der Anwendungen mit dem Filter nach **ServiceNow** -Apps.
4. Suchen Sie nach **ServiceNow Security Operations Integration**, und klicken Sie auf die entsprechende Aktion **Einrichten**.
5. Füllen Sie die Felder des Formulars aus.

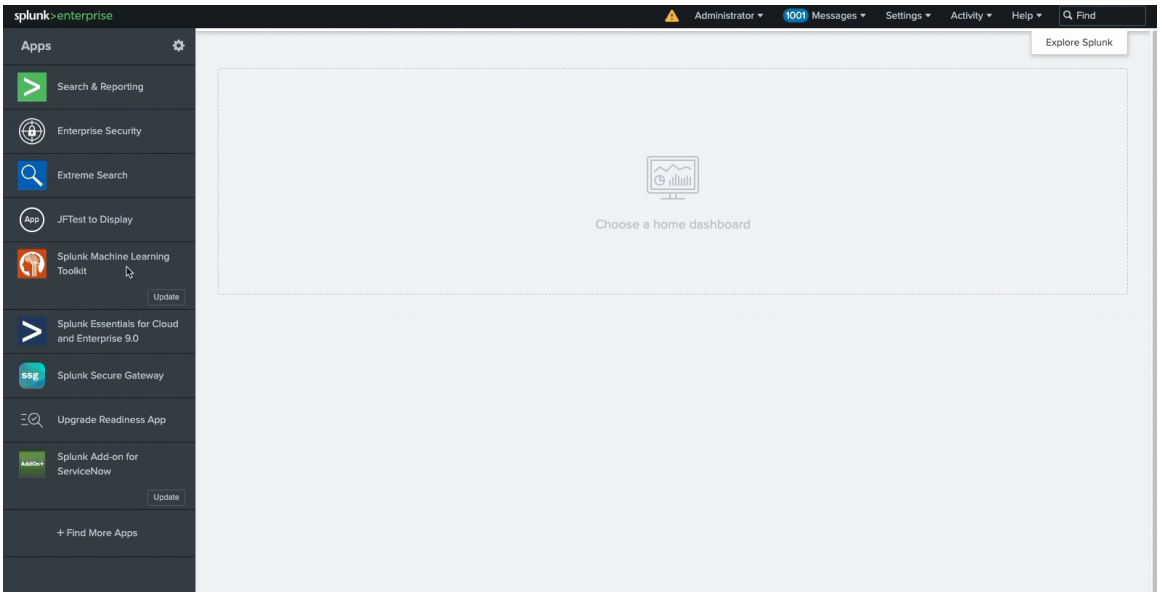


6. Klicken Sie auf **Speichern**.
7. Alternativ können Sie nach **ServiceNow Event Ingestion Integration**suchen und auf die entsprechende Aktion **Einrichten** klicken.

   Die ServiceNow Event Ingestion Integration ist auf drei verschiedene Registerkarten aufgeteilt.

   - **Splunk Primary**: Die standardmäßige oder primäre Splunk-Konfiguration.
   - **Splunk sekundär**: (Optional) Die Sicherungs- oder zweite Splunk-Konfiguration.
   - **Protokollierungsebene**: Die Ebene der von der Integration generierten Berichtsprotokolle, d. h. den Namen des Informationstyps.
8. Wählen Sie die Registerkarte **Splunk Primary** aus.
9. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. **Wahlweise:** Wählen Sie die Registerkarte **Splunk Sekundär** aus.
11. **Wahlweise:** Füllen Sie die Felder des Formulars aus.
12. Wählen Sie die Registerkarte **Protokollierungsebene** aus.
13. Füllen Sie die Felder des Formulars aus.
14. Klicken Sie auf **Speichern**.
    Nach erfolgreich abgeschlossener Validierung wird die Seite „Security Integrations“ (Sicherheitsintegrationen) mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel werden die Schaltflächen **Aktualisieren** und **Löschen** angezeigt (siehe folgende Abbildung).

Hinweis:
Sie müssen entweder nur die Standardauthentifizierung oder die OAuth 2.0-Authentifizierung verwenden. Aktivieren Sie eine der Authentifizierungen, und geben Sie die entsprechenden Authentifizierungsdetails ein. Wenn Sie beide aktivieren, wird ein Fehler angezeigt.

Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration für Ereigniserfassungen Splunk auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Liste Konfigurationen anzeigen auf **Ja**.

Konfigurieren Sie die Anwendungsregistrierung in der ServiceNow-Instanz

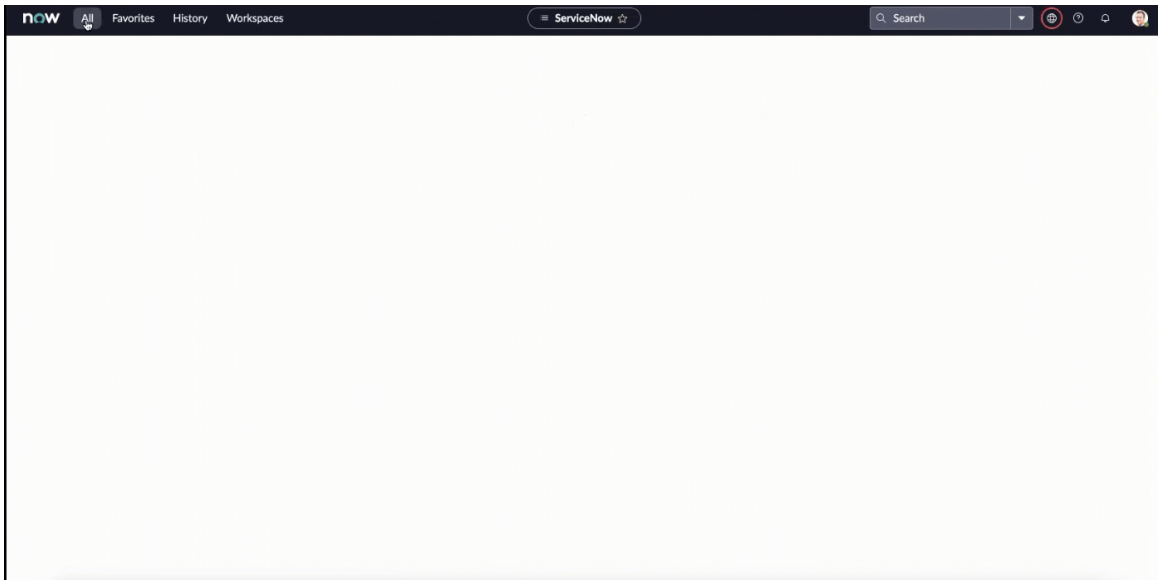
Registrieren Sie die Anwendung bei der -Instanz, um die OAuth-Autorisierung zu verwenden.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **OAuth-API-Endpunkt für externe Clients erstellen**.
4. Füllen Sie die Felder des Formulars aus.



5. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
6. Klicken Sie auf **Absenden**.

Befehle für die manuelle Suche

Manuelle Suchbefehle werden in jedem Suchfenster eingegeben. Sie können einen Security Incident oder ein Security Event erstellen. Nach dem Befehl stehen Feldwert-Paare, die zum Erstellen des gewünschten Datensatzes verwendet werden.

Sicherheitsereignis

Der Sicherheitsereignisbefehl **snsecevent**erstellt in ServiceNow ein Ereignis mit der -Sicherheitsklassifizierung.

Diese Ereignisse können einzeln überprüft werden, oder Warnungsregeln in ServiceNow oder manuelle Aktionen können ein Ereignis oder eine Sammlung von Ereignissen in einen Security Incident umwandeln.

Wenn das Ereignis zu einem Security Incident wird und jeder Parameter in das Ereignis gesendet wird, werden diese Daten wie folgt für den Security Incident verwendet:

Sicherheitsereignis

Parametername	Erforderlich	Verwenden	Verwenden Sie in Security Incident
node	Ja	Der Knoten stellt den Server oder das Configuration Item für das Ereignis dar. Im Idealfall	Verwenden Sie in Security Incident

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsereignis (Fortsetzung)

Parametername	Erforderlich	Verwenden	Verwenden Sie in Security Incident
		wird dieser Knoten einem vorhandenen CI innerhalb von ServiceNowzugeordnet.	
Typ	Ja	Die Kategorie des Ereignisses.	Kurzbeschreibung
Ressource	Ja	Das Configuration Item.	Kurzbeschreibung
Quelle	Nein	Der Ursprung dieser Daten. Standardmäßig generiert der Splunk-Server die Daten.	Aktivitätsprotokoll
external_url	Nein	Die in ServiceNow zu verwendende Drilldown-URL, um zu den Splunk-Daten zu diesem Ereignis zurückzukehren. Standardmäßig enthält diese URL den Ergebnislink für jede Warnung oder einen Link zur standardmäßigen Splunk-Suchseite.	Externe URL, auf die über die Schaltfläche **„Drilldown“** im Formular „Security Incident“ zugegriffen wird
time_of_event	Nein	Die Zeit, zu der das Ereignis in Splunk protokolliert wurde.	N/V
Alle anderen Werte (Kategorie, Unterkategorie im Beispiel)	Nein	Beliebiges Feld, das nicht Teil des Informationsfelds im Ereignis ist. Wenn ein Security Incident erstellt wird, wird er verwendet.	Wenn das Feld vorhanden und nicht ausgefüllt ist, verwendet der Security Incident diesen Wert. Beispielsweise wird die Kategorie, die das Ereignis übergeben hat, zur Kategorie des neuen Security Incident. Wenn ein Feld mit diesem Namen nicht vorhanden ist, wird der Wert in das Aktivitätsprotokoll aufgenommen.

Security Incident

Der Befehl Security Incident **snsecincident**erstellt einen Security Incident in Ihrer Instanz ServiceNow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident

Parameter	Erforderlich	Verwenden
short_description	Ja	Eine kurze, einzeilige Beschreibung des incident.
Kategorie	Nein	Die Kategorie des Security Incidents. Wenn diese Kategorie nicht vorhanden ist, wird sie erstellt.
Unterkategorie	Nein	Die Unterkategorie. Wenn diese Unterkategorie nicht vorhanden ist, wird sie erstellt.
cmdb_ci	Nein	Das Configuration Item für den Security Incident. Idealerweise wird dieses Element einem vorhandenen CI innerhalb von ServiceNowzugeordnet.
description	Nein	Längere, detaillierte Beschreibung des incident.

Es gibt viele nützliche Spalten – alles in der Transformationszuordnung für Security Incidents kann verwendet werden. Wenn dem Security Incident neue Spalten hinzugefügt werden, werden sie ebenfalls verwendet, sofern sie sich in der Transformationszuordnung befinden. Einige nützliche Spalten: „location“, „priority“, „assignment_group“, „assigned_to“, „affected_user“, „attach_vector“ und „watch_list“.

Splunk-Ereignisaktionen

Bei der Überprüfung von Splunk-Protokollen können Sie mithilfe der Ereignisaktionen schnell Sicherheitsereignisse und Security Incidents aus jedem Element im Protokoll erstellen.

Durch Klicken auf eine dieser Aktionen wird ein manueller Suchbefehl erstellt, der mit den Daten im Protokolleintrag gefüllt wird, und wird ausgeführt, um den neuen Datensatz zu generieren.

Diese Aktionen können einfach konfiguriert werden, um Felder in Ihren normalisierten Daten hinzuzufügen. In Splunk verwenden Sie **Einstellungen** > **Felder** > **Workflow-Aktionen**können Sie eine dieser Aktionen mithilfe der manuellen Suchfelder auswählen und bearbeiten.

Sie können auswählen, wo die Aktion für welche Felder angezeigt wird, und die Suchzeichenfolge ändern, die einen Suchbefehl enthält, um Ihren Datensatz zu erstellen.

Splunk-Warnungen für Einzeldatensatz

In jeder Warnung können Sie Sicherheitsereignisse oder Security Incidents angeben, die erstellt werden sollen, wenn die Warnung ausgelöst wird.

Öffnen oder erstellen Sie Ihre Warnung. Wählen Sie beim Bearbeiten von Aktionen den gewünschten Datensatztyp aus, und füllen Sie das Warnungsdialogfeld aus.

Anwenderdefiniertes Feld für Splunk-Warnungen mit mehreren Datensätzen

Warnungen für mehrere Datensätze (definiert mit den Auslöseraktionen **Mehrere ServiceNow-Security-Incidents erstellen** und **Mehrere ServiceNow-Security-Ereignisse**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellen) können automatisch Datensätze mit einem beliebigen Satz von unterstützten Feldern erstellen.

Diese funktionieren anders als die anderen Warnungsaktionen, für die Standardwerte angegeben sind. Die meisten Daten stammen jedoch aus dem Suchergebnis für diese Warnung.

Hinweis:
In früheren Versionen des Add-ons und dieser Dokumentation wurden geskriptete Warnungen unterstützt. Diese Funktion ist veraltet und wurde durch diese Anweisungen ersetzt.

Erstellen Sie ein anwenderdefiniertes Feld mit mehreren Datensätzen Splunk-Warnung

Um eine Splunk-Warnung mit mehreren Datensätzen und anwenderdefinierten Feldern zu erstellen, müssen Sie eine Suche erstellen, die den ServiceNow-Spalten entspricht, die Sie ausfüllen möchten.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren Sie zu **Suche**.
2. Erstellen Sie im Feld **Suchen** eine Suche, die Ihre Datensatzdaten generiert.
   Empfohlene Suchkriterien finden Sie in den Beispielen.
3. Klicken Sie auf **Speichern unter,** und wählen Sie **Warnung**aus.
4. Legen Sie den Namen, die Berechtigungen und den Zeitplan nach Bedarf fest.
5. Klicken Sie auf **Aktionen hinzufügen**.
6. Treffen Sie eine der folgenden Auswahlmöglichkeiten.
   - Um ein Ereignis pro Ergebnis aus Ihrer Suche zu erstellen, wählen Sie **Mehrere ServiceNow-Sicherheitsereignisse erstellen aus**.
   - Um einen Incident pro Ergebnis aus Ihrer Suche zu erstellen, wählen Sie **Mehrere ServiceNow Security Incidents erstellen aus**.
7. Legen Sie nach Bedarf Standardwerte fest.
   Wenn das Feld im Suchergebnis leer oder nicht vorhanden ist, werden die Standardwerte verwendet. Wenn das Ergebnis einen Wert enthält, werden die Standardwerte überschrieben.

Anwenderdefiniertes Feld mit mehreren Datensätzen – Beispiele für Splunk-Warnungen

Wenn Sie Splunk-Warnungen mit mehreren Datensätzen und anwenderdefinierten Feldern erstellen, müssen Sie Suchkriterien für die Generierung von Warnungsdaten definieren. Beispiele für Suchkriterien für Security Incidents und Security Events werden angezeigt.

Suche nach Security Incidents

Für einen Security Incident erstellen diese Kriterien eine Suche, um Spalten in der Security Incident-Tabelle auszufüllen.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suche nach Sicherheitsereignis

Für ein Sicherheitsereignis ist dies dieselbe Suche, es werden jedoch stattdessen Ereignisfelder ausgefüllt. Wenn dieses Ereignis in einen Security Incident umgewandelt wird und Felder ausgefüllt werden, die im Ereignis nicht vorhanden sind, werden sie in den Security Incident übertragen. Andernfalls bleiben sie im Feld „Zusätzliche Informationen“ des Ereignisses und der Warnung.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Hinweis:
Die von Ihnen verwendeten Suchkriterien fügen so viele Datensätze hinzu, wie in der Suche gefunden wurden. Es können 5 oder 10.000.000.000 Datensätze hinzugefügt werden. Daher ist dies KEINE empfohlene Methode für die Massenübertragung von Daten. Der Zweck dieser Methode besteht darin, einen Datensatz pro REST-Aufruf in der ServiceNow-Instanz hinzuzufügen.

Splunk-Fehler-Reporting

Immer wenn ein Konnektivitätsproblem mit Ihrer ServiceNow-Instanz auftritt, wird in Splunk ein Fehler mit entsprechenden Informationen protokolliert.

Fehlermeldungen werden in einem neuen Index namens **servicenow** mit dem Quelltyp **servicenow**gespeichert.

Achten Sie bei der Suche nach Fehlerprotokollen darauf, dass Sie den **ServiceNow** -Index in Ihrer Suche angeben. Alternativ erfahren Sie in der aktuellen Splunk-Dokumentation, wie Sie den neuen **ServiceNow** -Index zu den Standardsuchindizes hinzufügen.

Splunk Enterprise Event Ingestion integration for Security Operations by ServiceNow

Die Integration von Splunk Enterprise Ereignis- und Warnungsdaten mit dem Produkt Security Incident Response (SIR) ermöglicht Security Incident-Analysten das Erfassen und Verarbeiten von Sicherheitsprotokollen und zugehörigen Ereignisdaten.

Übersicht

Daten werden in Echtzeit gesammelt und von Analysten verwendet, um potenzielle Cyberbedrohungen zu identifizieren und entsprechende Berichte zu erstellen. Die gesammelten Sicherheitsereignisse können in ausgelösten Warnungen verarbeitet werden, die mit dieser Integration automatisch erfasst werden. Außerdem können einzelne Sicherheitsereignisse bei Bedarf manuell von der Such- und Berichterstellungsschnittstelle Splunk Enterprise an das Produkt Security Incident Response von Now Platform weitergeleitet werden, um Security Incidents zu erstellen. Sie können wichtige Ereignisse aus der Suche Splunk Enterprise mit der Suchkopf-Clusterkonfiguration abrufen. Sie können dies erreichen, indem Sie die URL und den API-Port eines beliebigen Suchkopfs verwenden, der Teil des Clusters ist.

Diese Integration bietet einem SOC-Analysten (Security Operations Center) Einblick in Ereignisse und zugehörige Warnungsdaten. Diese Daten können zur weiteren Untersuchung und Behebung in Security Incidents Now Platform Security Incident Response (SIR) integriert werden. In Ihrer Instanz Now Platform von werden Profile für Splunk laufende erfasste Warnungen und weitergeleitete Ereignisse erstellt. Diese Profile passen an,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wie verschiedene Splunk -Warnungs- und Ereignis-Felder in SIR -Security Incidents angezeigt werden. Es wird eine Standardzuordnung von Warnungsfeldern bereitgestellt, die bearbeitet und erweitert werden kann, um kundenspezifische Anforderungen zu erfüllen.

Schlüsselfunktionen

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Erstellen Sie mehrere Warnungserfassungsprofile, um SIR-Security Incidents für bestimmte Arten von Bedrohungen wie Phishing und Malware zu erstellen.
- Erstellen Sie mehrere Ereignisprofile für die bedarfsgesteuerte Ereignisweiterleitung über Ihre -Konsole Splunk, um SIR -Security Incidents zu erstellen.
- Drag-and-Drop-Zuordnung von Splunk Warnungs- und Ereignisfeldwerten zu zugehörigen SIR-Security Incident-Feldern.
- Eine Vorschau des Security Incident-Layouts SIR basierend auf Beispielwarnungen oder -ereignissen zur Validierung der Profilkonfiguration.
- Erfassung historischer Warnungen sowie laufender, zukünftiger Warnungen in konfigurierbaren Intervallen.
- Fassen Sie Ereignisse oder Warnungen zu vorhandenen SIR Security Incidents basierend auf übereinstimmenden Feldwerten zusammen, um doppelte Security Incidents zu vermeiden.

Unterstützte Versionen Now Platform.

Das Plugin com.snc.si_dep ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations -Anwendungen müssen über ServiceNow Storeinstalliert und aktiviert werden. Installieren Sie eine Anwendung nach der anderen in der unten aufgeführten Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

ServiceNow Add-ons

Das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise ist nur erforderlich, wenn Sie Ereignisse manuell von Ihrer Splunk Enterprise -Konsole an Ihre Now Platform -Instanz weiterleiten möchten. Das Add-on ServiceNow ist in splunkbase verfügbar.

Dieses ServiceNow Security Operations Event Ingestion Add-on für die Anwendung Splunk Enterprise in Splunkbase ist für die automatisierte Warnungserfassung, die von der Integration unterstützt wird, nicht erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Splunk unterstützte Versionen

Diese Integration unterstützt Version 6.0 oder höher von Splunk Enterprise. Die -Integration unterstützt auch den Enterprise Cloud-Service Splunk.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrer Instanz Now Platform®, um eine Verbindung zum Service Splunk herzustellen, wenn der Server Splunk innerhalb Ihres Unternehmensnetzwerks bereitgestellt wird. Wenn Sie den Service Splunk Cloud verwenden, ist kein MID-Server erforderlich. Weitere Informationen zu MID-Servern finden Sie unter MID-Server .

Integrationsarchitektur und Systemverbindung

Weitere Informationen zur Architektur der Integration, einschließlich wichtiger Begriffe und Details zu Verbindungen externer Systeme, finden Sie unter Integrationsarchitektur und externe Systemverbindung für die Splunk Enterprise Event Ingestion -Integration.

Prüfliste

Eine Druckliste dieser Themen finden Sie unter Prüfliste für die Splunk Enterprise Security Integration „Notable Event Ingestion“.. Sie können diese Liste verwenden, um Ihren Fortschritt bei der Bearbeitung der Aufgaben der Integration zu überwachen.

Die in den folgenden Themen verwendeten Bilder wurden für das Kingston-Release von Now Platformgeneriert. Informationen zur San Diego-Anwenderoberfläche finden Sie unter Sicherheitsbedrohungen mit dem Security Analyst Workspace verwalten.

Die folgenden Themen sind nummeriert. Befolgen Sie die unten in der Reihenfolge aufgeführten Themen, um eine reibungslose Installation und Konfiguration der Anwendung zu gewährleisten.

Richten Sie Ihre Instanz Now Platform® für die Integration Splunk Enterprise Event Ingestion ein

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in der Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung von ServiceNow Storeinstallieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Sehen Sie sich die folgende Tabelle an, und vergewissern Sie sich, dass Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Prozedur

1. Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben.

   Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Instanz Now Platform® von erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.
- Wenn Sie Ereignisse für diese Integration manuell von Splunk Enterprise weiterleiten möchten, weist ein Benutzer mit der Administratorrolle Now Platform® einem Benutzer mit der Rolle (sn_sec_splunk_v2.api_account_access) in Now Platform®zu. Diese Rolle ermöglicht einem Anwender mit der Administratorrolle Splunk Enterprise den Zugriff auf die API in Now Platform®, die für die manuelle Ereignisweiterleitung für diese Integration erforderlich ist.

  Die Rolle (sn_sec_splunk_v2.api_account_access) ist für die Integration nicht erforderlich, wenn Sie Warnungen automatisch aus Splunk Enterprise in Ihrer Instanz Now Platform® erfassen.

- Ein Benutzer mit der Rolle sn_si.admin überwacht die folgenden Aufgaben in Now Platform®:
  - Benennt, erstellt und bearbeitet Warnungs- und Ereignisprofile.
  - Wählt Werte aus Warnungen und Ereignissen aus und ordnet sie den Security Incidents Now Platform® zu.
  - Zeigt eine Vorschau der Details von Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.
  - Plant die laufende Warnungserfassung.
  - Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu.
  - Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.

Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Managing roles .

2. Vergewissern Sie sich, dass Sie Version 6.0 oder höher der Splunk -API verwenden.

   Wenn Sie Zugriff auf die -Konsole Splunk Enterprise haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich.

3. Stellen Sie sicher, dass Sie einen MID-Server installiert und konfiguriert haben.

   Ein MID-Server in Ihrer Instanz Now Platform® ist erforderlich, um eine Verbindung zum Service Splunk herzustellen, wenn der Server Splunk innerhalb Ihres Unternehmensnetzwerks bereitgestellt wird. Weitere Informationen zu MID-Servern finden Sie unter MID-Server

   Wenn Sie den Service Splunk Cloud verwenden, ist kein MID-Server erforderlich.

4. Stellen Sie sicher, dass die ServiceNow Core-Anwendungen, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind.

   Das Plugin Security Incident Response Dependency (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.

a. Security Incident Response

b. Security Integration Framework

c. Security Support Common

d. Security Support Orchestration

Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Nächste Maßnahme

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht in der Installation der Anwendung Splunk Enterprise Event Ingestion aus ServiceNow Store für die Integration. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration Splunk Enterprise Event Ingestion ..

Wenn Sie keine Suchen in Ihrer Splunk Enterprise -Konsole zur Erfassung gespeichert haben oder wenn Sie das Erstsetup für diese Integration gleichzeitig in Ihrer Splunk Enterprise -Konsole und im Security Operations -Produkt Ihrer Now Platform® -Instanz durchführen, finden Sie weitere Informationen unter Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration.

Wenn Sie Ereignisse für die -Integration manuell und bei Bedarf von Ihrer Splunk Enterprise -Konsole exportieren möchten, finden Sie weitere Informationen unter Richten Sie Ihre Splunk -Umgebung für die manuelle Ereigniserfassung für die Splunk Enterprise -Ereigniserfassungsintegration ein.

Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration Splunk Enterprise Event Ingestion .

Bevor Sie die -Integration in Ihrer Instanz Now Platform® ausführen, führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in die -Produkte Security Incident Response und Security Operations in Ihrer Instanz Now Platform® integriert werden kann.

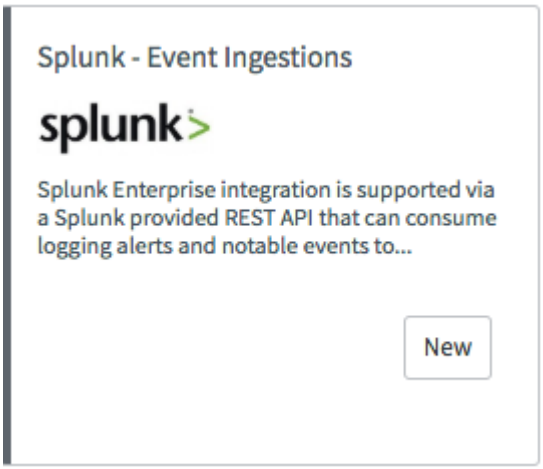
Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

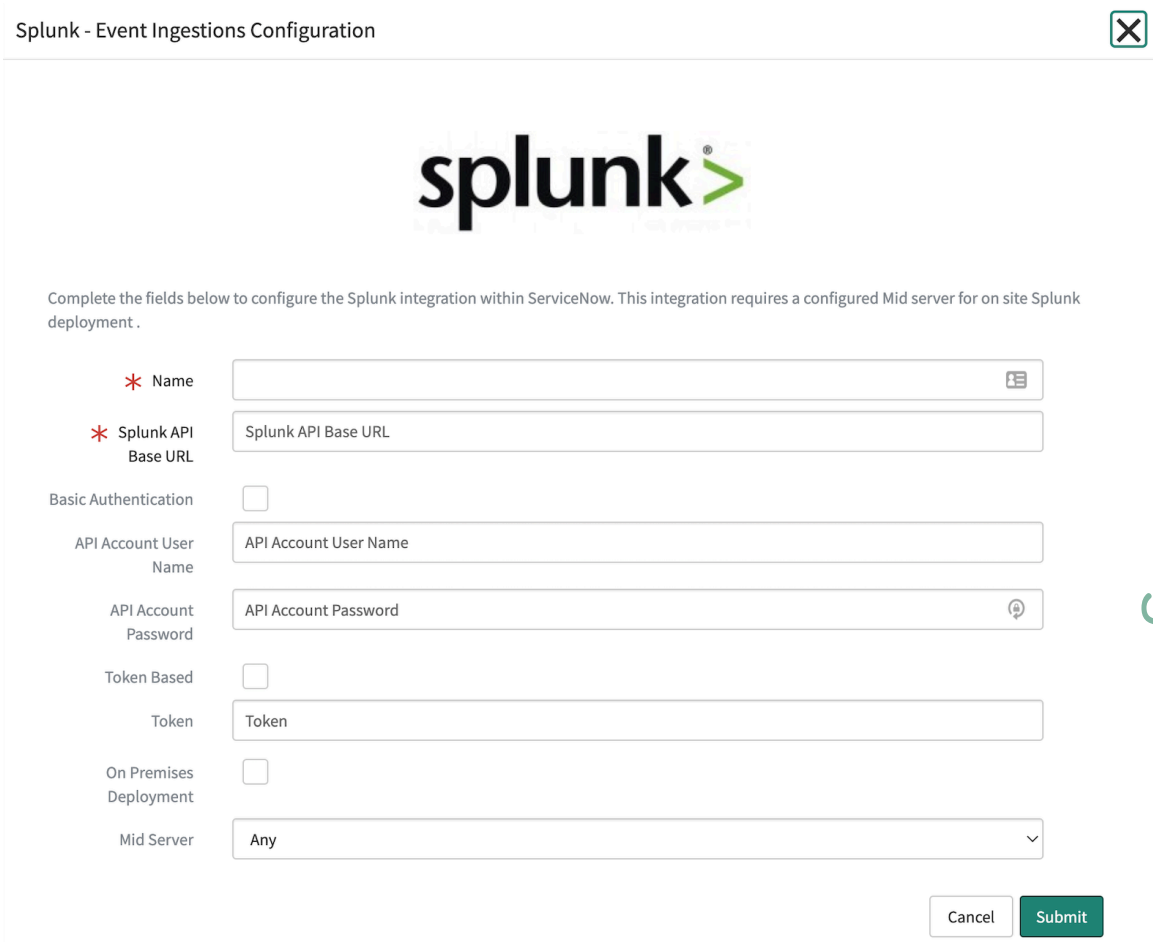
1. Wenn Sie die Anwendung Splunk Enterprise Event Ingestion für die Integration nicht aus ServiceNow Store installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Splunk Ereigniserfassungen.
3. Klicken Sie zum Konfigurieren der Anwendung auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Alternativ: Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, können Sie darauf klicken, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie die Felder im angezeigten Dialogfeld „Konfiguration der Ereigniserfassung“ aus.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für die Konfiguration einer lokalen Version von Splunk Enterprise mit einem MID Server.



Jede Splunk Enterprise -Warnung, die Sie von der Splunk Enterprise -Konsole erfassen, erfordert ein eindeutiges Ereignisprofil in Ihrer Now Platform® -Instanz. Die Quelle, die

Automatische Übersetzung

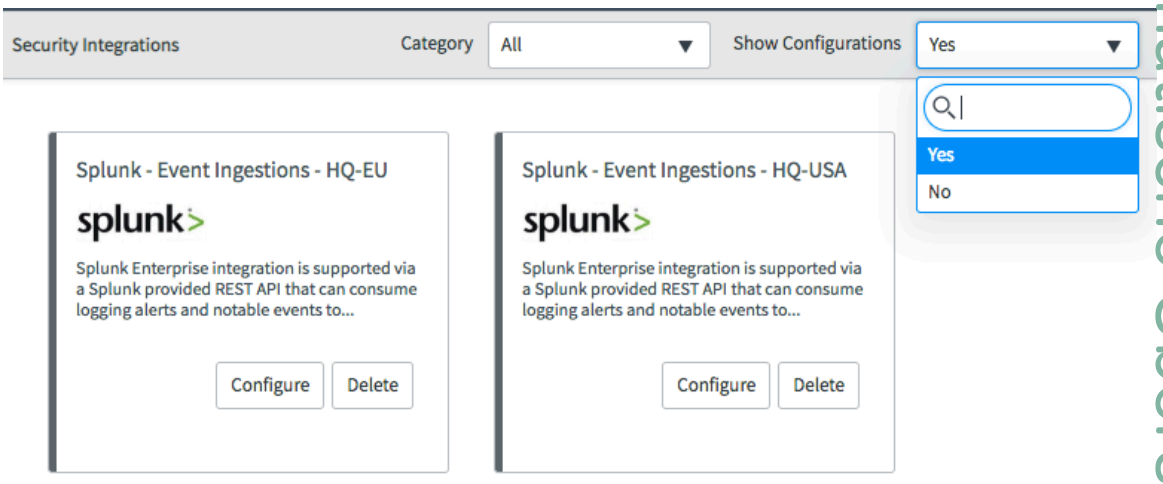
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie im Formular „Konfiguration der Ereigniserfassungen“ konfigurieren, kann jedoch für mehrere Now Platform® Profile wiederverwendet werden, solange jedes Profil eindeutige, durch Splunk ausgelöste Warnungen erfasst.

6. Klicken Sie auf **Absenden**.
   Nach erfolgreich abgeschlossener Validierung wird die Seite „Security Integrations“ (Sicherheitsintegrationen) mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel werden die Schaltflächen **Konfigurieren** und **Löschen** angezeigt (siehe folgende Abbildung).

   Hinweis:
   Sie müssen entweder nur die Standardauthentifizierung oder die tokenbasierte Authentifizierung verwenden. Aktivieren Sie eine der Authentifizierungen, und geben Sie die entsprechenden Authentifizierungsdetails ein. Wenn Sie beide aktivieren, wird ein Fehler angezeigt.

   Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration für Ereigniserfassungen Splunk auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite mit den Sicherheitsintegrationen angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.



Trouble?

Wenn eine Fehlermeldung angezeigt wird, nachdem Sie auf **Absenden**geklickt haben, geben Sie Ihre Informationen erneut ein, und klicken Sie auf **Absenden**.

Nächste Maßnahme
Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht im Erstellen eines Ereignisprofils.

Konfigurieren Sie die Einstellungen für Splunk Enterprise Event Ingestion

Verwenden Sie die Splunk Enterprise Event Ingestion-Einstellungen, um die voreingestellten Konfigurationen und ihre Werte entsprechend Ihren Anforderungen zu ändern.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Integrationseinstellungen**.
2. Füllen Sie die Felder im Formular aus.

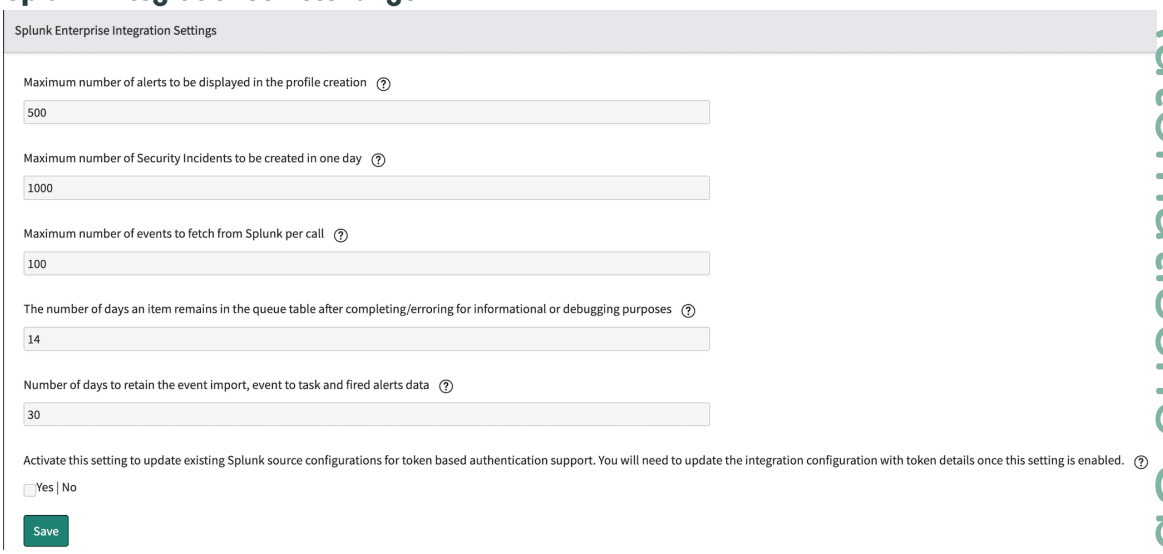
Splunk-Integrationseinstellungen

Feld	Beschreibung
Maximale Anzahl von Warnungen, die bei der Profilerstellung angezeigt werden sollen	Option zum Definieren der maximalen Anzahl von Warnungen, die beim Erstellen eines Ereignisprofils angezeigt werden sollen. Standardmäßig ist der Wert auf 500 festgelegt.
Maximale Anzahl von Security Incidents, die an einem Tag erstellt werden sollen	Option zum Definieren der maximalen Anzahl von Security Incidents, die an einem Tag erstellt werden können. Standardmäßig ist der Wert auf 1000 festgelegt.
Maximale Anzahl von Ereignissen, die pro Anruf aus Splunk abgerufen werden sollen	Option zum Definieren der maximalen Anzahl von Ereignissen, die für jeden Anruf von Splunk abgerufen werden sollen. Standardmäßig ist der Wert auf 100 festgelegt.
Die Anzahl der Tage, die ein Element in der Warteschlangentabelle verbleibt, nachdem es zu Informations- oder Debugging-Zwecken abgeschlossen wurde oder ein Fehler aufgetreten ist	Option zum Definieren der Anzahl der Tage, für die ein Element nach Abschluss oder Auftreten eines Fehlers aufgrund von Informations- oder Debugging-Zwecken in der Warteschlangentabelle verbleiben soll. Standardmäßig ist der Wert auf 14 festgelegt.
Anzahl der Tage, für die Daten zu Ereignisimporten, Ereignissen zu Aufgaben und ausgelösten Warnungen aufbewahrt werden	Mit dieser Option können Sie die Anzahl der Tage festlegen, die Daten für Ereignisimport, Ereignis-zu-Aufgaben und ausgelöste Warnungen aufbewahrt werden sollen. Standardmäßig ist der Wert auf 30 festgelegt.
Aktivieren Sie diese Einstellung, um vorhandene Splunk-Quellkonfigurationen für die Unterstützung der tokenbasierten Authentifizierung zu aktualisieren. Sie müssen	Option zum Aktualisieren der vorhandenen Splunk-Quellkonfiguration auf Unterstützung der tokenbasierten Authentifizierung von einer vorhandenen Version auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
die Integrationskonfiguration mit Tokendetails aktualisieren, sobald diese Einstellung aktiviert ist.	**Hinweis:** Nach dem Upgrade auf die neue Version ist das Tokenfeld nicht mehr verfügbar. Sie müssen diese Einstellung aktivieren, um die tokenbasierte Authentifizierung zu erhalten. Anschließend müssen Sie die Integrationskonfiguration mit den Tokendetails aktualisieren. Standardmäßig ist der Wert auf Nein festgelegt.

Splunk-Integrationseinstellungen



3. Klicken Sie auf **Speichern**.

Erstellen und benennen Sie ein Ereignisprofil für die Splunk Enterprise Event Ingestion -Integration

Erstellen Sie ein Ereignisprofil in Ihrer Instanz Now Platform, und bestimmen Sie, welche Splunk -Warnungen Security Incidents erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Bevor -Security Incidents vom Now Platform Security Incident Response Typ (SIR) aus erfassten Warnungen erstellt werden, werden die Feldwerte aus Warnungen in einem Layout eines Now Platform -Security Incidents angezeigt, sodass Sie eine Vorschau auf die Darstellung des tatsächlichen Security Incidents anzeigen können.

Aus Sicht der Integration mit verfügbaren APIs werden Splunk -Ereignisse einzeln und manuell als diskrete Ereignisse weitergeleitet, oder sie werden zu ausgelösten Warnungen kombiniert, die automatisch in der Security Operations -Umgebung Ihrer Instanz von Now Platform erfasst werden. Die Integrations-Workflows erfassen verschiedene Arten von Warnungen, z. B. solche zu nicht autorisierten Zugriffsversuchen und zu Malware.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Warnungen werden basierend auf den Profilen erfasst, die Sie in der Umgebung Security Operations Ihrer -Instanz konfigurieren. Alle Warnungen werden anfänglich für einen konfigurierten Warnungstyp in einem Profil erfasst. Erfasste Warnungen können dann weiter gefiltert werden, um anzugeben, welche Warnungen Security Incidents erstellen. Beispielsweise können Sie Filter bevorzugen, die Security Incidents nur für Warnungen erstellen, die als hoch riskant eingestuft werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Warnungen erstellt, werden einzelne Feldwerte in den gefilterten Warnungen für eine Vorschau den entsprechenden Feldern in einem Layout von Security Incidents zugeordnet.

Warnungsnamen für Ereignisprofile in Ihrer Instanz Now Platform müssen eindeutig sein und können jeweils nur einem aktiven Ereignisprofil zugeordnet werden. Dies sind die Namen der ausgelösten Warnungen, die Sie in Ihrem Splunk -Service als Teil des Setups für die Integration konfiguriert haben. Weitere Informationen zum Konfigurieren von Warnungen in Ihrer Splunk Enterprise -Umgebung finden Sie unter Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration.

Now Platform erfasst bestimmte Warnungen mithilfe der Workflows der -Integration. Alle Warnungen, die die Auswahlkriterien in Ihrer -Unternehmenskonsole Splunk erfüllen, werden zunächst in Ihrer -Instanz Now Platform erfasst.

Ein Profil in Ihrem Now Platform ist eine Kapselung einer Splunk -Warnung in Ihrer Splunk -Enterprise-Konsole. Es besteht eine 1:1-Beziehung zwischen Warnungen, die mit einem Profil erfasst werden, und Verbindungen mit Ihrer Splunk -Enterprise-Konsole: eine Warnung für eine Verbindung. In Ihrer Splunk Enterprise -Konsole besteht eine einzelne HTTPS-Verbindung zu einem Suchheader. Mehrere Warnungen können von einem einzigen Suchkopf stammen. Wenn Sie in der Konsole Splunk Enterprise eine Verbindung zu mehreren Suchköpfen herstellen, müssen Sie in der Instanz Now Platform mehrere Profile erstellen, um diese Warnungen zu erfassen.

Schritte zum Erstellen von Profilen für die geplante Warnungserfassung

Prozedur

1. Um ein Ereignisprofil für eine Warnung zu erstellen, navigieren Sie in Ihrer Instanz Now Platform zu **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wenn das Formular Splunk Ereignisprofil nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Name**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

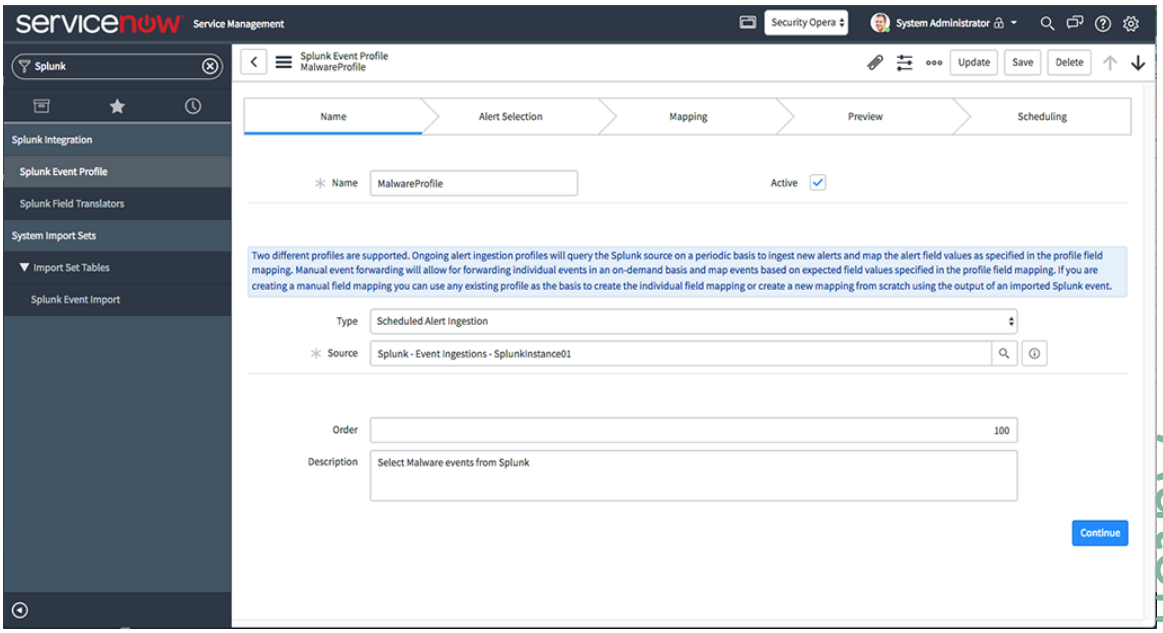
Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn die Namen nicht eindeutig sind, werden keine doppelten Profilnamen gespeichert. Profilnamen in Ihrer Instanz Now Platform müssen eindeutig sein.
Aktiv	Checkbox ist standardmäßig deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die Option „Aktiv“ ist deaktiviert und erst verfügbar, wenn Sie alle Profilkonfigurationsschritte abgeschlossen haben und auf **„Fertigstellen“**klicken.
Typ	Wählen Sie den Profiltyp aus der Auswahlliste aus. ○ Geplante Warnungserfassung: Dieser Profiltyp unterstützt ausgelöste Warnungen, die nach einem von Ihnen konfigurierten Zeitplan erfasst werden. Füllen Sie die Felder aus, und klicken Sie auf „ **Fortsetzen“**, um mit dem Schritt „Warnungsauswahl“ des Profils fortzufahren. ○ Manuelle Ereignisweiterleitung: Dieser Profiltyp unterstützt einzelne Ereignisse, die bei Bedarf manuell von Ihrer Splunk Enterprise -Konsole weitergeleitet werden. Führen Sie die folgenden Schritte aus, um das Formular für diese Profiltypen auszufüllen.
Quelltyp	Splunk Server oder Suche, die Sie für die Erfassung von Warnungen konfiguriert haben. Wenn Sie mehrere Splunk -Server konfiguriert haben, wählen Sie den entsprechenden Server für die Warnungstypen aus, die Sie für das Profil erfassen möchten. Sie müssen einen Wert eingeben.
Bestellung	Der Standardwert ist 100. Belassen Sie diese Einstellung auf dem Standard. Wenn Sie mehrere Profile erstellt haben, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile dieselben Auslösebedingungen verwenden. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität.
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für eine geplante Warnung.



5. Wählen Sie für ein Profil mit einer geplanten Warnung eine Option aus, um mit der Profilkonfiguration fortzufahren.
   Schritte zum Erstellen von Profilen für die manuelle Ereignisweiterleitung
6. Führen Sie die folgenden Schritte aus, um ein Profil zu erstellen, das die manuelle Ereignisweiterleitung unterstützt.

   Für Ereignisse, die Sie bei Bedarf von Ihrer Unternehmenskonsole Splunk aus weiterleiten, können Sie die einzelnen Feldzuordnungen auf einem vorhandenen Profil basieren. Alternativ können Sie ein neues Zuordnungsraster für exportierte Anhangsdaten erstellen. Ereignisse, die Sie manuell weiterleiten, sind im Ereignisprofil nicht geplant.

   a. Wenn dies noch nicht ausgewählt ist, wählen Sie in der Auswahlliste für das Feld Typ die Option **Manuelle Ereignisweiterleitung**aus.

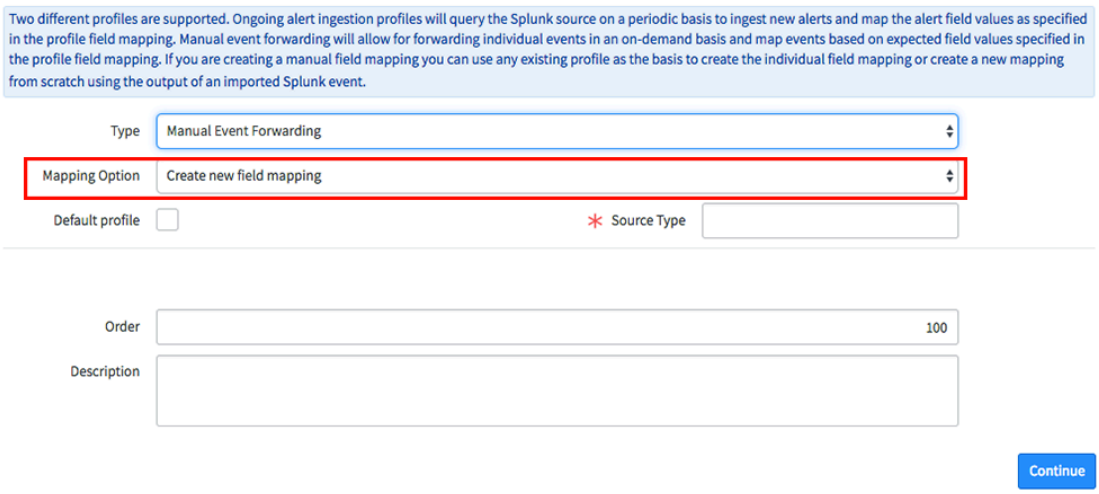
   b. Wählen Sie im angezeigten Feld Zuordnungsoption aus der Auswahlliste eine Zuordnungsoption aus, um fortzufahren.

      Weitere Informationen zu den verfügbaren Zuordnungsoptionen in der Auswahlliste Zuordnungsoptionen finden Sie in den folgenden Abbildungen und Tabellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine neue Feldzuordnungsoption



Erstellen Sie eine neue Feldzuordnungsoption

Option oder Feld	Beschreibung
Erstellen Sie eine neue Feldzuordnungsoption	Neue Feldzuordnung für Ihr Ereignis. Wenn Sie keine ähnliche Feldzuordnung wie das von Ihnen erstellte Profil haben, wählen Sie diese Option, um eine neue Zuordnung zu erstellen.
Standardprofil	Standardprofil für die Ereignisweiterleitung für alle Splunk -Ereignisse. Standard ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Ereignisweiterleitung. Dieses Profil ist das einzige Profil, das aktiv ist und für jede Splunk -Ereignisfeldzuordnung zu einem SIR -Security Incident verwendet wird. Ein Profil für alle weitergeleiteten Ereignisse. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelltyp	Splunk Server. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. Wenn verfügbar, ermöglicht die Option Quelltyp die eindeutige Zuordnung von Ereignisfeldern zu Security Incident-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	Feldern auf Grundlage des Quelltyps Splunk. Wenn Sie Firewall-Protokollereignisse anders als Endpunkterkennungsereignisse verwalten möchten und diese unterschiedliche Splunk Quelltypen haben, können Sie unterschiedliche Ereignisprofile basierend auf den Quelltypen erstellen, um diese Anforderung zu erfüllen.
Bestellung	Der Standardwert ist 100. Belassen Sie diese Einstellung auf dem Standard. Wenn Sie eine große Anzahl von Profilen erstellt haben, gibt dieser Wert eine Laufzeit-Ausführungspriorität an, wenn zwei oder mehr Profile auslösende Bedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität.
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Vergewissern Sie sich bei einem Profil mit einer neuen Feldzuordnung, dass Sie einen Wert in das Feld Quelltyp eingegeben haben, und klicken Sie auf **Fortfahren**, um mit dem Zuordnungsschritt der Konfiguration fortzufahren.

Weitere Informationen zu einem Profil mit einer vorhandenen Feldzuordnung finden Sie in der folgenden Abbildung und Tabelle.

Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

Option oder Feld	Beschreibung
Wählen Sie ein vorhandenes Profil für die Feldzuordnung aus	Eine vorhandene Feldzuordnung für Ihr Ereignis Das Feld Aus Profil kopieren wird angezeigt. Führen Sie diese Schritte aus, um eine vorhandene Feldzuordnung für dieses Profil zu kopieren. i. Klicken Sie links neben dem angezeigten Feld Kopieren aus Profil auf das Suchsymbol. ii. Klicken Sie in der angezeigten Liste Ereignisprofile Splunk auf den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	Profilnamen, der die zu kopierende Karte enthält. Der Profilname wird im Feld Von Profil kopieren angezeigt.
Standardprofil	Standardprofil für die Ereignisweiterleitung für alle Splunk -Ereignisse. Standard ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Ereignisweiterleitung. Dieses Profil ist das einzige aktive Profil. Es wird für jedes Splunk -Ereignisfeld verwendet, das einem SIR -Security Incident zugeordnet ist. Ein Profil für alle weitergeleiteten Ereignisse. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelltyp	Splunk Server. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption ausgewählt ist. Wenn verfügbar, ermöglicht die Option Quelltyp die eindeutige Zuordnung von Ereignisfeldern zu Security Incident-Feldern auf Grundlage des Quelltyps Splunk. Wenn Sie Firewall-Protokollereignisse anders als Endpunkterkennungsereignisse verwalten möchten und diese unterschiedliche Splunk Quelltypen haben, können Sie unterschiedliche Ereignisprofile basierend auf den Quelltypen erstellen, um diese Anforderung zu erfüllen.
Bestellung	Der Standardwert ist 100. Belassen Sie diese Einstellung auf dem Standard. Wenn Sie mehrere Profile erstellt haben, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile auslösende Bedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Klicken Sie unten im Formular zur Auswahl einer vorhandenen Zuordnung für Ihr Profil **auf Fertigstellen**, um die Profilkonfiguration abzuschließen.

Nächste Maßnahme

Sie haben die Schritte zum Erstellen von Profilen sowohl für geplante Warnungen als auch für die manuelle Ereignisweiterleitung erfolgreich abgeschlossen. Sie haben die Profilkonfiguration für Profile für die manuelle Ereignisweiterleitung abgeschlossen. Der nächste Schritt besteht im Laden der Anhangdaten im Zuordnungsschritt.

Bei Profilen für geplante Warnungen besteht der nächste Schritt in der Auswahl von Warnungen für die automatische Erfassung.

Wählen Sie geplante Warnungen für die Integration Splunk Enterprise Event Ingestion aus

Nachdem Sie ein Profil für eine geplante Warnung erstellt haben, wählen Sie für dieses Profil eine Splunk -Warnung aus, die Sie einem Now Platform Security Incident Response -Security Incident zuordnen möchten.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Warnungen in Ihrer Instanz Now Platform an, damit Sie wissen, welche Feldwerte für die Zuordnung verfügbar sind. Wählen Sie eine Warnung aus, um zu überprüfen, ob Sie im grundlegenden Formularlayout die erwarteten Ergebnisse erhalten, bevor Sie die Werte Feldern in Security Incidents SIR zuordnen. Sie können in diesem Formular nur eine Warnung aus der Liste auswählen.

Prozedur

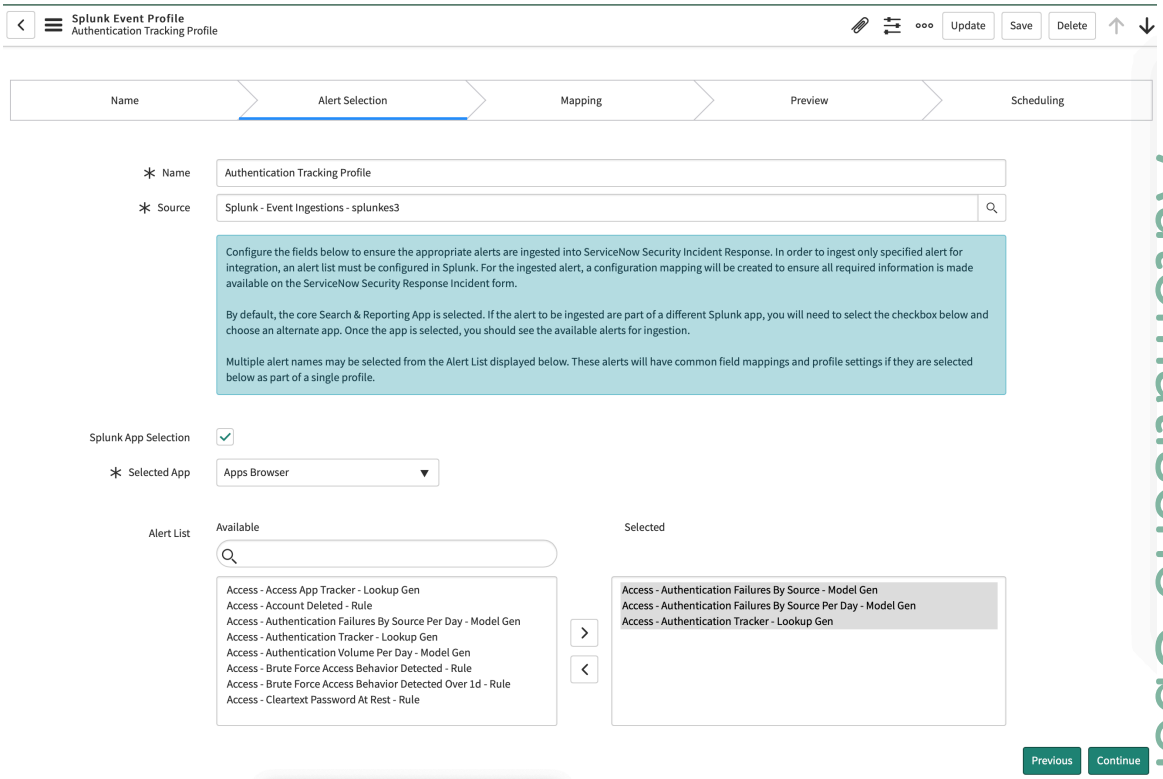
1. Wenn die Seite „Warnungsauswahl“ nicht angezeigt wird, wählen Sie sie in der Fortschrittsleiste aus, um sie anzuzeigen.
   Standardmäßig ist die Core-Such- und Berichterstellungs-App ausgewählt.
2. Wenn die zu erfassende Warnung Teil einer anderen App Splunk ist, wählen Sie **Splunk-App-Auswahl**, und wählen Sie Ihre Splunk -App aus der Liste **Ausgewählte App** aus.
3. Wählen Sie in der **Warnungsliste**eine Warnung aus, und verschieben Sie sie aus der Spalte **Verfügbar** in die Spalte **Ausgewählt**.
   Sie können auch mehrere Warnungen auswählen. Wenn die Warnungen als Teil eines einzelnen Profils ausgewählt werden, weisen die Warnungen allgemeine Feldzuordnungen und Profileinstellungen auf.

   Die Liste der Warnungen in diesem Formular entspricht der Liste der Warnungen in Ihrer Splunk -Konsole. In diesem Formular werden bis zu 500 Warnungen angezeigt. Wenn in Ihrer Splunk-Konsole auf der Seite „Warnungen“ mehr als 500 Warnungen aufgeführt sind, werden in diesem Formular in Ihrer Instanz Now Platform nur die ersten 500 Warnungen angezeigt.

Option	Beschreibung
Geben Sie im Suchfeld Warnungsliste Text ein.	Die Spalte unter dem Suchfeld wird anhand der verfügbaren Optionen basierend auf dem von Ihnen eingegebenen Text gefiltert. Wählen Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	eine Warnung aus und verschieben Sie sie mit den Pfeiltasten von **Verfügbar** in **Ausgewählt**.
Doppelklicken Sie in der Warnungsliste auf eine Warnung.	Die Spalte **Ausgewählt** wird mit Ihrer Auswahl gefüllt.
Klicken Sie in der Warnungsliste einmal auf eine Alarmregel.	Der Alarm ist ausgewählt. Verschieben Sie die ausgewählte Warnung mit den Pfeiltasten von **Verfügbar** in **Ausgewählt**.



4. Wählen Sie eine Option aus, um fortzufahren.

Nächste Maßnahme

Sie haben erfolgreich eine Warnung für ein geplantes Warnungsprofil ausgewählt. Der nächste Schritt besteht darin, Feldern in einem Security Incident Warnungswerte zuzuordnen.

Zuordnung von Warnungen und Ereignissen für die Splunk Enterprise Event Ingestion -Integration

Nachdem Sie die Quellen für die geplante Warnungserfassung oder die manuelle Ereignisweiterleitung identifiziert haben, besteht der nächste Schritt in der Zuordnung einzelner Ereignisfelder zu den Feldern in einem Security Incident Now Platform Security Incident Response (SIR).

Übersicht

Für den Zuordnungsschritt erfassen Sie als Benutzer mit der Rolle sn_si.admin Beispielwarnungen aus Ihrer Splunk Enterprise -Konsole, oder exportieren Sie Ereignisdaten für ein Splunk Enterprise -Ereignis.

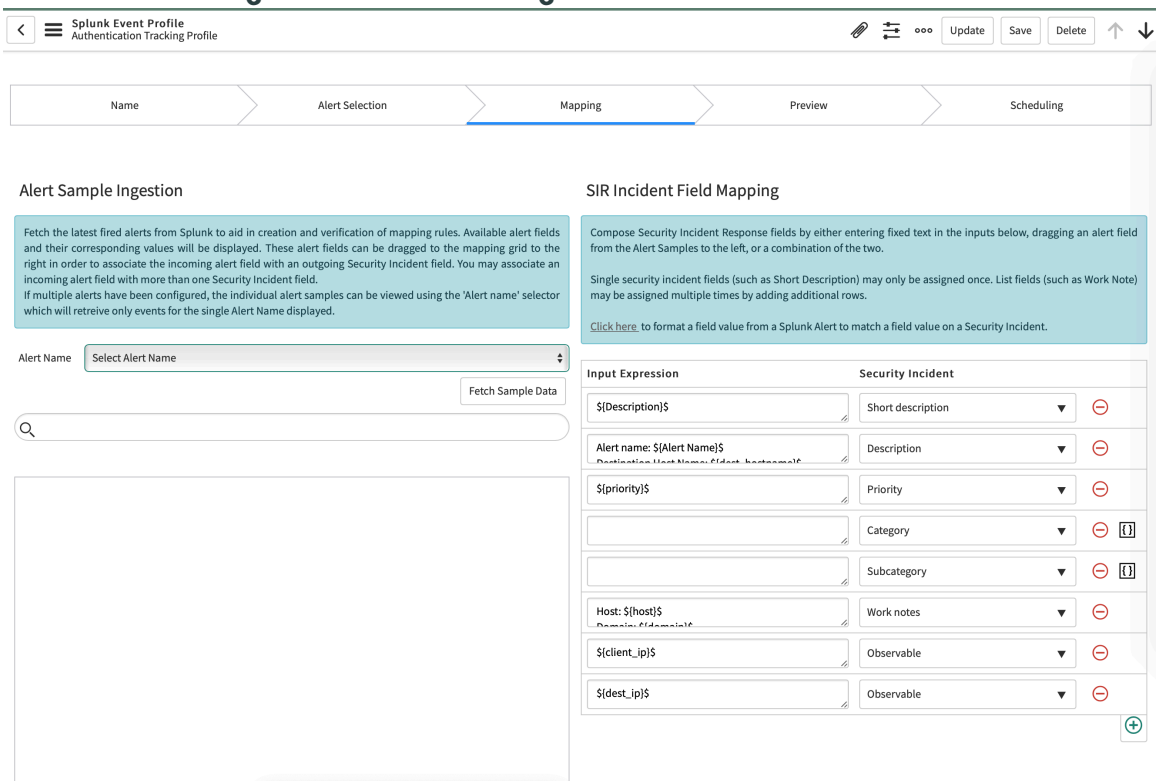
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Abbildungen sind Beispiele für die standardmäßigen Zuordnungsraster, die für jeden Typ von Ereignisprofil bereitgestellt werden. Diese Standardzuordnung kann bearbeitet werden. Mit dieser Änderung können Sie die Felder anpassen, die den Security Incident ausfüllen. Mit dem Zuordnungsschritt können Sie visualisieren, wie sich das Hinzufügen oder Entfernen von Ereignisfeldern auf die Werte des Felds SIR Security Incident auswirkt.

Wählen Sie den **Warnungsnamen**aus. Nachdem Sie auf **Beispieldaten abrufen**geklickt haben, werden die Werte des Warnungsfelds Splunk auf der linken Seite des Formulars ausgefüllt, wenn Beispielwarnungen vom Profil erfasst werden. Dies sind die Warnungsfelder Splunk, die Sie den Security Incident-Feldern SIR zuordnen.

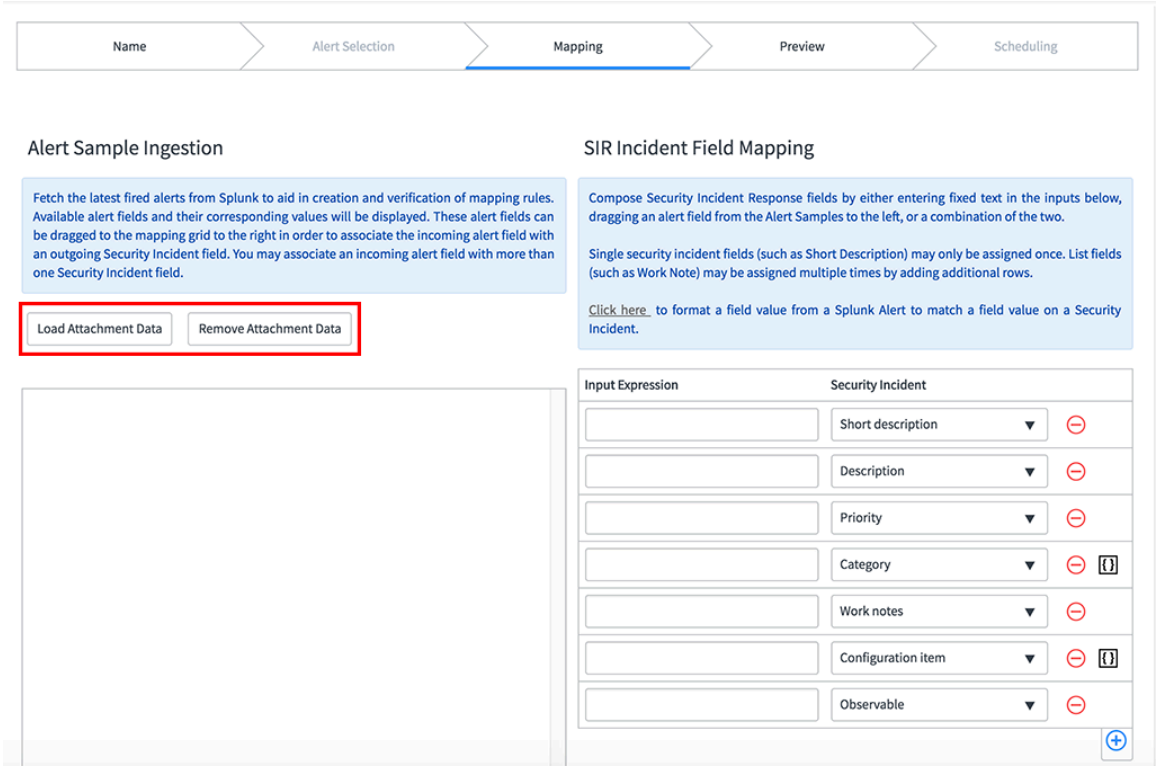
Standardzuordnungsformular für Warnungen



Nachdem Sie auf geklickt haben, um Anhangdaten für weitergeleitete Ereignisse zu laden, werden die Ereignisfelder Splunk auf der linken Seite des Formulars ausgefüllt. Dies sind die Datenfelder Splunk, die den Security Incident-Feldern SIR zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardzuordnungsformular für weitergeleitete Ereignisse



Möglicherweise möchten Sie einige Beispielwarnungen in Ihrer Splunk -Konsole überprüfen, um sie für den Konfigurationsschritt der Feldzuordnung zu erfassen. Dieser Schritt wird auf dem Fortschrittsbalken **mit Zuordnung** gekennzeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.

Das Zuordnen von Warnungen und Exportieren von Ereignissen bei Bedarf über die Enterprise-Konsole Splunk umfasst die folgenden Konzepte und Aufgaben:

- Rufen Sie Beispieldaten für automatisch erfasste Warnungsprofile ab. Nachdem in der Konsole Splunk Enterprise Daten aus einer ausgelösten Warnung abgerufen (abgerufen) wurden, werden verfügbare Warnungsfelder und die entsprechenden Werte in einem Standardzuordnungslayout auf der linken Seite des Zuordnungsformulars angezeigt. Registerkarten werden angezeigt, auf denen Sie die Werte für eine von Ihnen abgerufene Warnungs-ID anzeigen können. Stellen Sie sicher, dass alle kritischen Felder aus dem Abschnitt „Erfassung des Warnungsbeispiels“ auf der linken Seite des Formulars dem Raster auf der rechten Seite des Formulars zugeordnet sind.
- Laden Sie bei Bedarf Ereignisbeispieldaten für manuell weitergeleitete Ereignisprofile. Beispieldaten für diese Ereignisse werden in einer XML- Datei aus der Konsole Splunk Enterprise exportiert und in Ihre Instanz Now Platform® geladen. Die importierten Daten werden im Abschnitt „Erfassung des Warnungsbeispiels“ auf der linken Seite des Formulars angezeigt.
- Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Warnungen von der linken Seite in das Zuordnungsraster auf der rechten Seite ziehen. Das Zuordnungsraster auf der rechten Seite ordnet das Feld für eingehende Warnungen einem Feld für ausgehende Security Incidents zu.
- Passen Sie das Zuordnungsraster durch Hinzufügen oder Entfernen von Feldern an. Verfolgen Sie übersehene oder duplizierte Felder anhand der angegebenen Farbcodierung.
- Legen Sie Filterbedingungen fest, um festzulegen, welche Warnungen in der Anwendung SIR erfasst und welche Warnungen herausgefiltert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Definieren Sie zusätzliche Incident-Feldkriterien, die eine eingehende Warnung zu einem vorhandenen Security Incident SIR zusammenfassen, um doppelte Incidents zu verhindern. Diese zusätzliche Filterung kann die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Sicherheitsereignisdaten in einem einzigen Security Incident platziert werden.
- In bestimmten Fällen werden Ereignisfeldwerte in der Enterprise-Konsole Splunk möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten. Beispiel: Mit dem Skript-Editor werden die Feldwerte Malware-Warnung und Viruserkrankung in der Konsole Splunk beide in böswillige Codeaktivität im Feld Kategorie des Security Incident SIR übersetzt.

Profile für geplante Warnungen

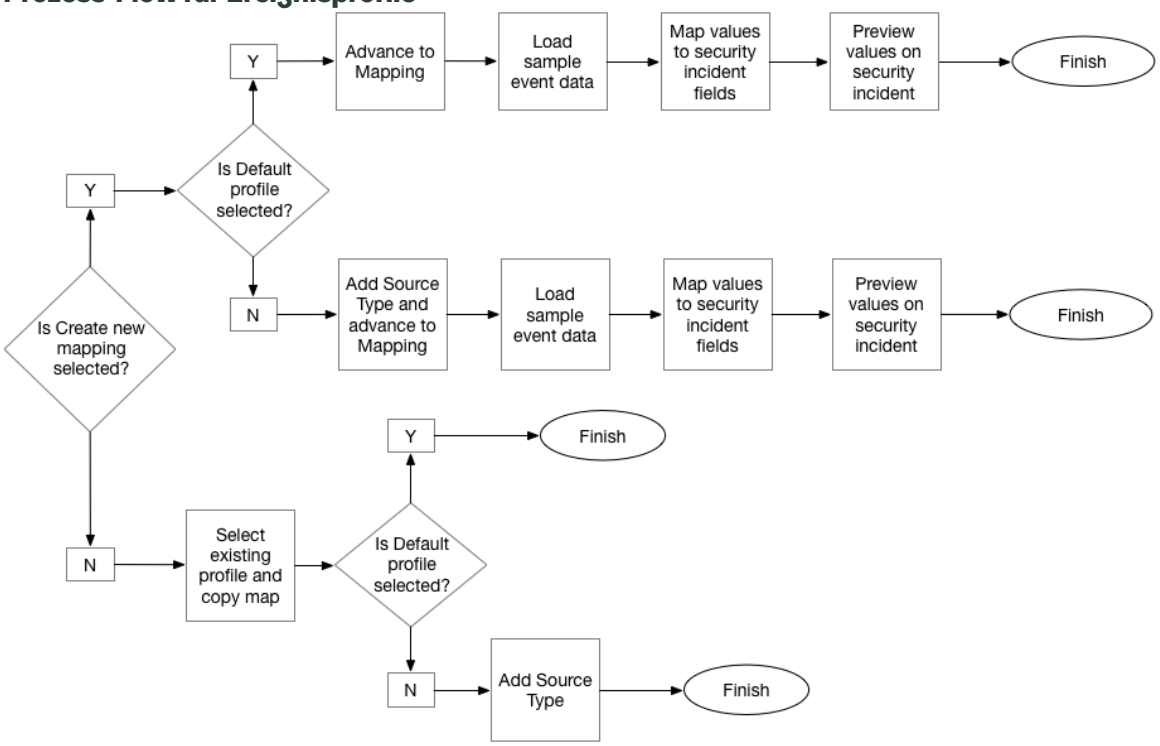
Nach dem Erstellen eines geplanten Warnungsprofils wird der Prozessablauf für die Konfiguration in der folgenden Abbildung dargestellt.

Prozess-Flow für geplante Warnungsprofile

Profile für die manuelle Ereignisweiterleitung

Nach dem Erstellen eines Profils für ein Ereignis wird der Prozessablauf für die Konfiguration in der folgenden Abbildung dargestellt.

Prozess-Flow für Ereignisprofile



Der nächste Schritt besteht darin, ausgelöste Warnungen zu erfassen oder Daten zu exportieren und Werte den Security Incident-Feldern SIR zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungswarnungen für die Splunk Enterprise Event Ingestion -Integration

Während des Schritts der Ereignisfeldzuordnung ordnen Sie einzelne Ereignisfelder aus ausgelösten Warnungen oder importierten Ereignisdaten Feldern in einem Security Incident Now Platform Security Incident Response (SIR) zu.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Das vorkonfigurierte Zuordnungsraster der Standardfelder für Security Incidents kann bearbeitet werden. Anhand der Farbcodierung der Ereignisfelder können Sie die Feldwerte überwachen, die Sie bereits zugeordnet haben. Mit diesem Schritt können Sie visualisieren, wie sich Ihre Änderungen auf die Felder im Security Incident auswirken.

Ordnen Sie bis zu fünf Warnungen aus der Spalte „Erfassung des Warnungsbeispiels“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu.

Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie im Zuordnungsraster auf der rechten Seite des Formulars Felder hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie Splunk -Felder zuordnen, die nicht im Standardzuordnungsraster im Security Incident SIR angezeigt werden.

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
2. Wählen Sie für ein Profil mit einer geplanten Warnung unter Erfassung des Alarmbeispiels die Warnung unter **Warnungsname** aus, und klicken Sie **auf Beispieldaten abrufen,** um die aktuelle Instanz einer ausgelösten Warnung aus der Konsole Splunk Enterprise abzurufen.

   Die Warnungen werden als Registerkarten angezeigt. Sie können bis zu fünf der neuesten Warnungen erfassen.

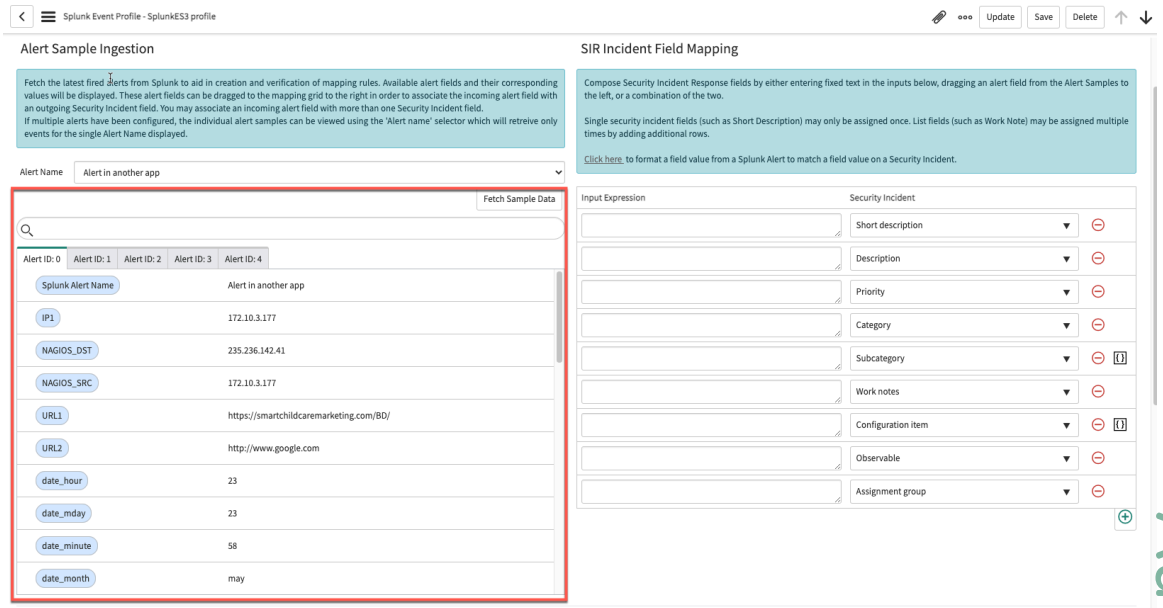
   Das Abrufen von Beispielereignissen kann einige Minuten dauern. Oben auf dem Bildschirm wird eine Meldung angezeigt, dass die Transaktion funktioniert.

   Hinweis:
   Die Integration fügt ein zusätzliches Zuordnungsfeld, **Splunk-Warnungsname**, hinzu, um die Nachverfolgung eines Ereignisses zur Quellwarnungsregel in Splunkzu ermöglichen. Dies kann in Szenarien hilfreich sein, in denen mehrere Warnungen Splunk in einem einzigen Profil kombiniert werden.

   Wenn ein einzelnes Feld mehrere Werte enthält, werden diese Werte analysiert und einzelnen Feldeinträgen im Abschnitt „SIR-Incident-Feldzuordnung“ zugeordnet. Beispielsweise können die Quell-IP-Adressen, Asset-Namen oder URLs mehrere Feldeinträge für erkennbare Elemente oder mehrere CIs aufweisen, die analysiert und einzelnen Feldeinträgen im Abschnitt „SIR-Incident-Feldzuordnung“ zugeordnet werden.

   In der folgenden Abbildung werden auf der linken Seite dieses Formulars die Feld-Name-Wert-Paare für die erfasste Warnung oder das importierte Beispielereignis angezeigt, nachdem der Abruf abgeschlossen wurde. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Fahren Sie für geplante Warnungsprofile mit Schritt 5 fort, um die Werte zuzuordnen.
4. Alternativ können Sie für ein Profil für einen Ereignistyp, das Sie aus Ihrer Splunk Enterprise -Konsole exportieren möchten, die folgenden Schritte ausführen, um Anhangdaten in Ihre Now Platform® -Instanz hochzuladen.

   a. Wenn Sie noch nicht angemeldet sind, melden Sie sich bei Ihrer Splunk Enterprise -Konsole an.

   b. Navigieren Sie zur Registerkarte Suchen, und geben Sie einen Namen für eine Suche ein, die die zu exportierenden Ereignisdaten enthält.

      Beispielsweise ist „Malware“ ein Suchbegriff, der für alle Malware-Ereignisse verwendet wird, die Sie mit dem Workflow dieser Integration weiterleiten können.

   c. Erweitern Sie das Ereignis, und wählen Sie in der Spalte Feld die Felder aus, die Sie importieren möchten.

      Diese Felder sind die Feld-Wert-Paare, die exportiert und auf der Seite „Zuordnung“ in Ihrer Instanz Now Platform® angezeigt werden.

   d. Klicken Sie in Ihrer Splunk Enterprise -Konsole oben rechts auf der Suchseite auf das **Exportieren** -Symbol.

   e. Klicken Sie in der Liste für das Feld Format im angezeigten Dialogfeld auf **XML-Format**.

   f. **Wahlweise:** Geben Sie einen neuen Dateinamen ein.

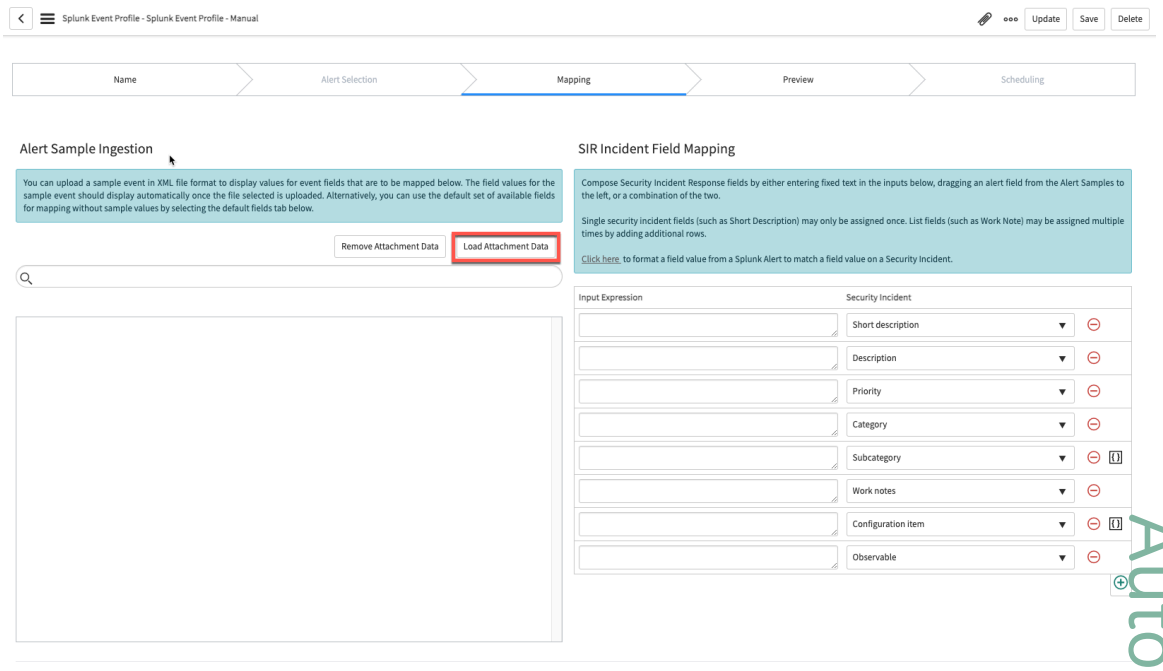
   g. Klicken Sie auf **Exportieren**.
   Die Datei wird in Ihre Instanz Now Platform® heruntergeladen.

   h. Wenn die Seite „Zuordnung“ in Ihrer Instanz Now Platform® noch nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.

   i. Klicken Sie in der Spalte Erfassung des Warnungsbeispiels **auf Anhangdaten laden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



j. Klicken Sie im angezeigten Dialogfeld **auf Dateien auswählen**, navigieren Sie zu der exportierten XML- Datei, und klicken Sie auf **Öffnen**.
Die Wertepaare für die Felder, die Sie für das Ereignis exportiert haben, werden auf der linken Seite des Zuordnungsformulars angezeigt.

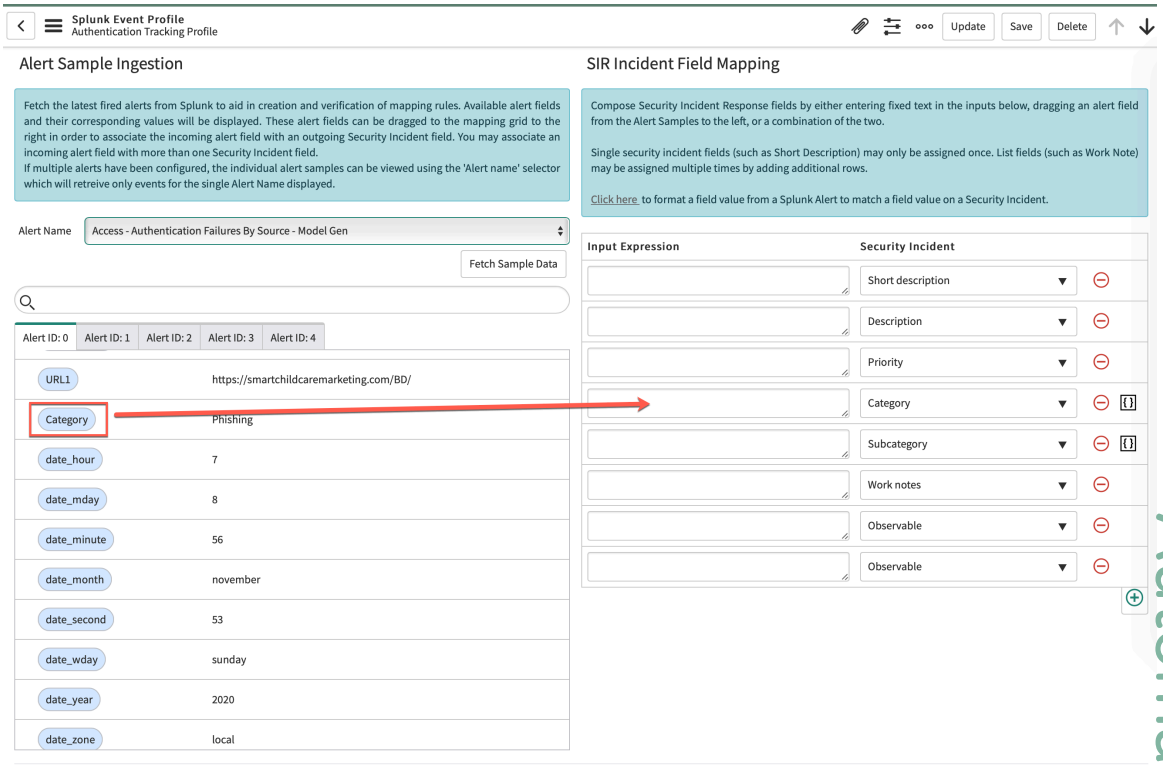
In der folgenden Abbildung werden auf der linken Seite des Formulars die Datenpaare für eine erfasste geplante Warnung angezeigt. Wertepaare für importierte Ereignisse werden auch auf dieser Seite des Formulars angezeigt. Diese Werte sind die Feldwerte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

5. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf einen blauen Feldnamen auf der linken Seite des Formulars.

6. Ziehen Sie den Feldnamen, z. B. Kategorie, in ein Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“.

Automatische Übersetzung

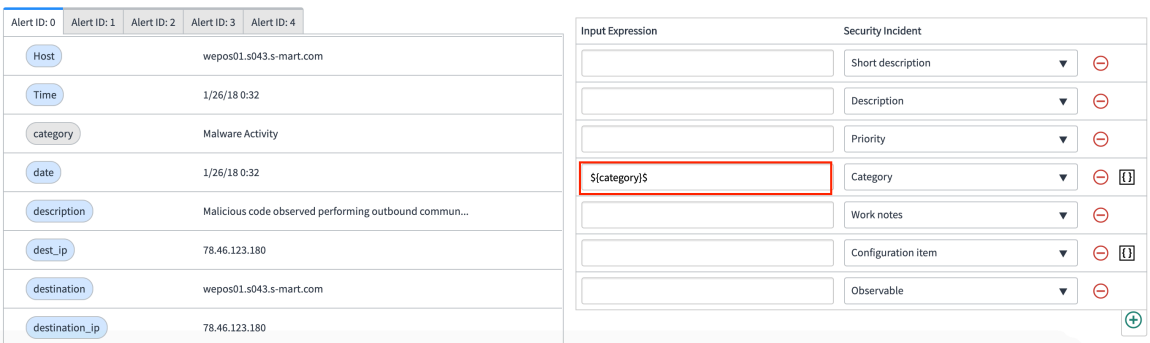
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird die Kategorie dem Feld „Kategorie“ im Security Incident zugeordnet. Sie können jedoch jeden Wert auf der linken Seite mit einem Feld auf der rechten Seite abgleichen. Vergewissern Sie sich, dass der Wert dem Security Incident während des Vorschauschritts korrekt zugeordnet wurde.

Um sicherzustellen, dass im Zuordnungsprozess keine Ereignisse übersehen oder dupliziert werden, sind Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass im Security Incident noch kein Feld ausgewählt und zugeordnet wurde. Unter Umständen möchten Sie ein Feld für eingehende Warnungen mehreren Feldern in einem Security Incident zuordnen.

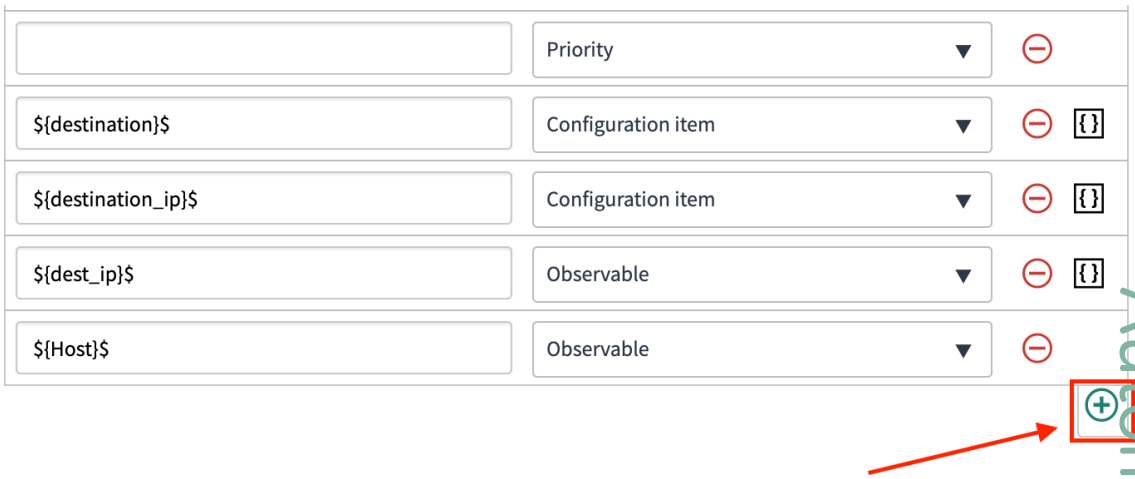
Ein graus Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen, da Warnungsereignisfelder in bestimmten Fällen möglicherweise nur einmal zugewiesen werden. Beispielsweise können Sie Feldern wie „Kurzbeschreibung“ nur einmal Werte zuweisen. Sie können Listenfelder wie Arbeitsnotiz jedoch mehrmals zuweisen, indem Sie dem Zuordnungsraster zusätzliche Zeilen hinzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Führen Sie die folgenden Schritte aus, um der Standardzuordnung des Security Incident auf der rechten Seite des Formulars Felder hinzuzufügen.

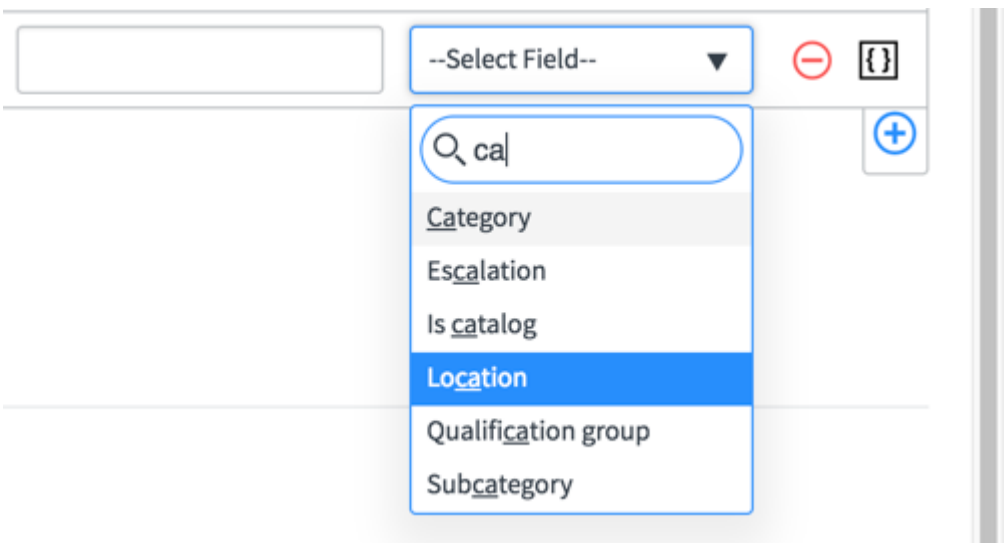
   a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol.



   Ein neues Feld wird angezeigt.

   b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie ein Feld aus.

   In der erweiterten Liste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung ist die Kategorie grau hinterlegt, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für Warnungsfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Felder für Security Incidents auf der rechten Seite beim Nachverfolgen der Zuordnung.



Automatische Übersetzung

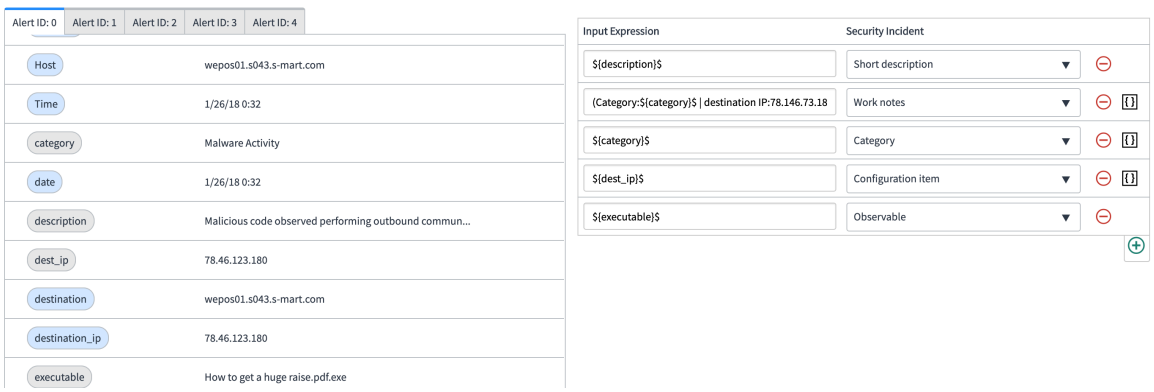
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident ebenfalls nicht ausgefüllt.

c. Geben Sie alternativ einen Wert in das Feld Suchen für die neue Zeile ein.

d. Wählen Sie auf der linken Seite des Formulars mit der linken Maustaste die **Warnungs-ID** aus, die Sie im Feld Eingabeausdruck verwenden möchten.
Ordnen Sie es mit der Ziehfunktion neben Ihrem neuen Feld zu.

8. Setzen Sie die Zuordnung fort, indem Sie Felder hinzufügen oder entfernen und Werte zur Zuordnung hinzufügen.
Die folgende Abbildung zeigt ein Beispiel für ein bearbeitetes Zuordnungsraster. Im unteren Feld rechts wird das Feld Arbeitsnotizen hinzugefügt, das mehr als einen Wert hat. Die Werte sind durch Leerzeichen und Satzzeichen getrennt (Kategorie:${category} | Ziel-IP:78.146.73.180).



In der Vorschau werden diese Werte in den Arbeitsnotizen zum Security Incident angezeigt. Da der Wert für ein Feld gilt, das Sie dem Raster hinzugefügt haben, und dem Feld Arbeitsnotizen mehrere Werte zugeordnet sind, werden die Werte wie eingegeben angezeigt. In diesem Beispiel werden die von Ihnen in das Feld eingegebenen Leerzeichen und Interpunktionszeichen im Abschnitt „Zugehörige Elemente“ als Arbeitsnotiz in der Vorschau des Security Incident angezeigt.

Die folgende Abbildung zeigt ein Beispiel dafür, wie die Werte in der vorherigen Abbildung für den Security Incident angezeigt werden.

Filterbedingungen für die Incident-Generierung

9. Wahlweise: Nachdem Sie die vorhergehenden Zuordnungsschritte auf Feldebene abgeschlossen haben, können Sie dieselben Feldwerte im Filterbedingungsgenerator verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen SIR Security Incident zu erstellen.

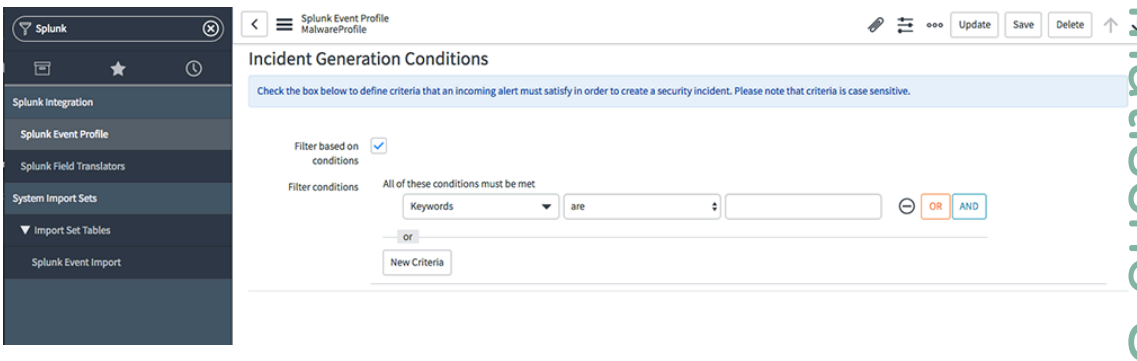
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie die folgenden Schritte aus, um Filterbedingungen festzulegen.

a. Scrollen Sie im Formular zum Abschnitt „Bedingungen für Incident-Generierung“, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen filtern,** um die Option zu aktivieren.

(Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

Die Optionen in den Listen für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt „Erfassung des Warnungsbeispiels“ für die von Ihnen erfasste Warnung angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach der Warnung Splunk, die Sie erfassen, oder je nach Ereignis, das Sie manuell weiterleiten. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau den Werten der Warnung oder des Ereignisses Splunk Enterprise entsprechen. Wenn Sie sich bei den Werten, die Sie in die Filterfelder eingeben sollen, nicht sicher sind, kehren Sie möglicherweise zu Ihrer Splunk Enterprise -Konsole zurück und überprüfen Ihre Warnungen und Ereignisse auf die Stichwörter.

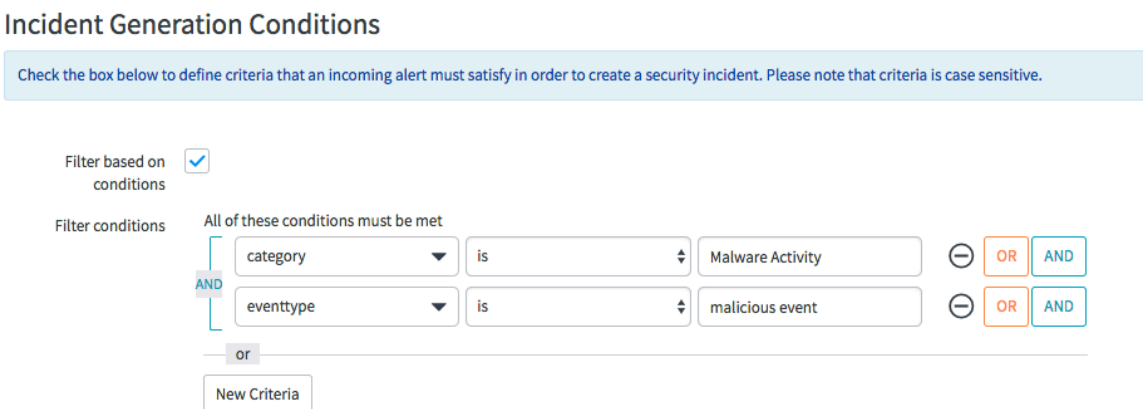


b. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

c. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **AND** oder **OR**. Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.

d. **Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Sie haben die Auslösebedingungen so festgelegt, dass Security Incidents nur erstellt werden, wenn die beiden von Ihnen eingegebenen Filterbedingungen erfüllt sind.

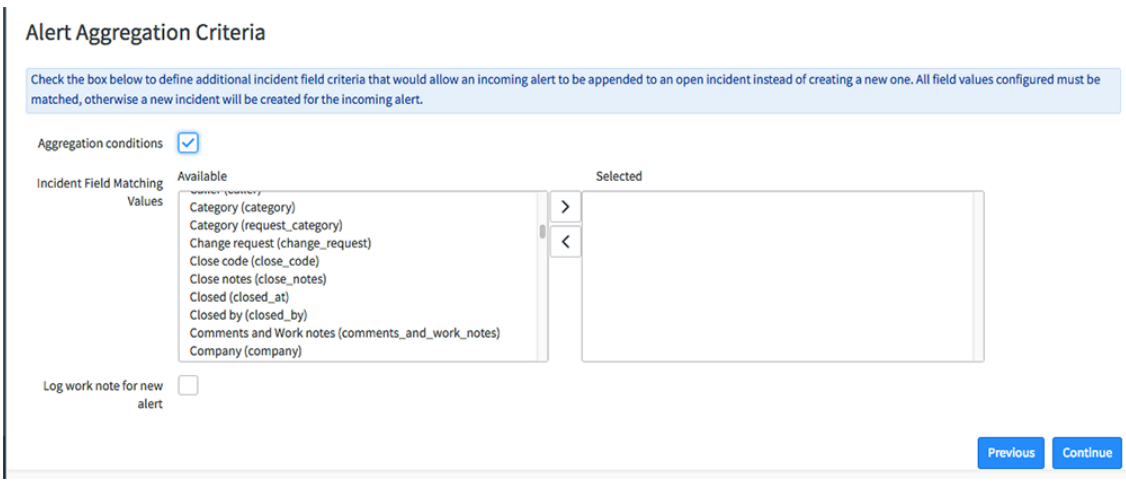
Diese Art der Filterung hilft Ihnen, Sicherheitsereignisse zu isolieren, und begrenzt die Anzahl der von Ihnen erstellten Security Incidents. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur erforderliche Warnungen erfasst, ohne dass die Abfrage Splunk oder die Konfiguration der ausgelösten Warnung geändert werden muss.

Zusammenfassung von Warnungen zur Verhinderung doppelter Incidents

10. **Wahlweise:** Um zu vermeiden, dass doppelte Security Incidents erstellt werden, definieren Sie zusätzliche Incident-Feldkriterien, damit eingehende Warnungen zu einem offenen Security Incident zusammengefasst werden.
Führen Sie die folgenden Schritte aus, um diese Kriterien festzulegen.

   a. Scrollen Sie im Formular zum Abschnitt Kriterien für Warnungszusammenfassung, und aktivieren Sie das Kontrollkästchen Bedingungen zusammenfassen, um diese Option zu aktivieren.

   (Optional) Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die im Security Incident SIR konfiguriert sind.



   b. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die mit vorhandenen Security Incidents in Now Platform abgeglichen werden sollen, und verschieben Sie sie in die Liste Ausgewählt.

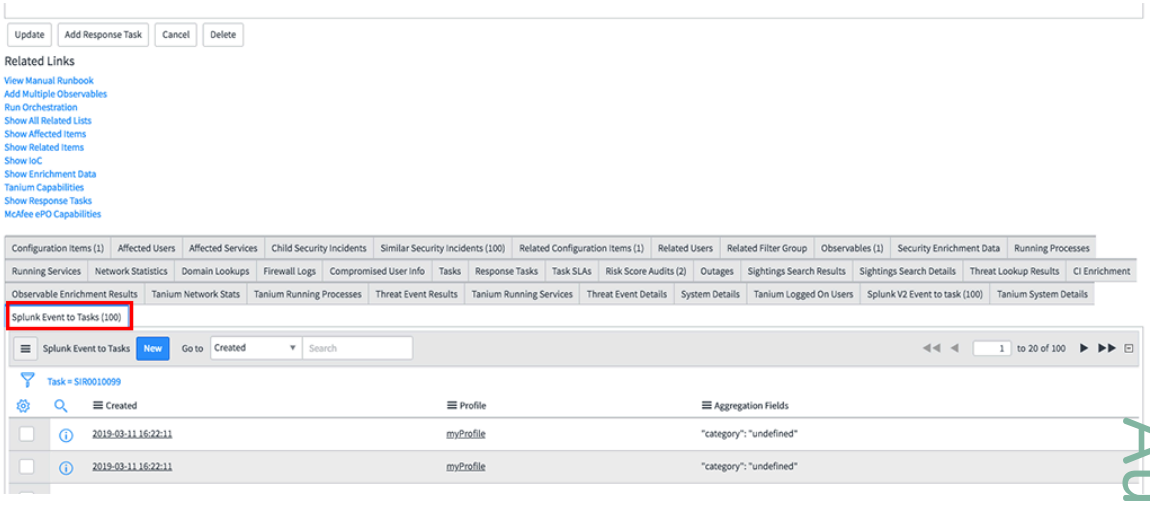
   (Optional) Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, damit diese eingehende Warnung an einen vorhandenen Security Incident angehängt wird. Wenn Sie Feldwerte zu Security Incidents überprüfen möchten, die für diese Kriterien verwendet werden sollen, navigieren Sie zu **Incidents** > **Alle Incidents anzeigen**.

   Wenn eine neue Warnung allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird die Warnung automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, die mit Security Incidents arbeiten, können Sie alle hinzugefügten aggregierten Warnungen in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle aggregierten Warnungen zu einem Security Incident werden in der zugehörigen Liste Splunk Ereignis für Aufgaben angezeigt. Diese Liste enthält Details zu zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum Warnungen zu vorhandenen Security Incidents hinzugefügt werden. Wenn diese Registerkarte nicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angezeigt wird, scrollen Sie unter „Zugehörige Links“ zur linken Seite des Datensatzes, und klicken Sie auf den Link **Alle zugehörigen Listen anzeigen**.



c. **Wahlweise:** Um eine Arbeitsnotiz für eine neue Warnung zu protokollieren, die dem Security Incident kürzlich hinzugefügt wurde, aktivieren Sie das Kontrollkästchen zur Aktivierung dieser Option.
Die Arbeitsnotiz protokolliert, dass eine neue Warnung hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails.

Sie haben erfolgreich Werte aus einer Warnung oder einem Ereignis Splunk Feldern in einem Security Incident SIR zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents anhand von Filterkriterien einzuschränken. Sie haben Warnungen oder Ereignisse auch an vorhandene SIR Security Incidents angehängt.

11. **Wahlweise:** Öffnen Sie den Skript-Editor und setzen Sie die Bearbeitung fort.

(Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor zum Formatieren von Warnungswerten für die Integration Splunk Enterprise Event Ingestion ..

12. Wählen Sie eine aus, um mit der Profilkonfiguration fortzufahren.

Nächste Maßnahme

Der nächste Schritt besteht in der Vorschau der Werte, die Sie dem Security Incident zugeordnet haben.

Zeigen Sie eine Vorschau des Security Incident für die -Integration Splunk Enterprise Event Ingestion an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie im Security Incident Now Platform® Security Incident Response (SIR) zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Warnungsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

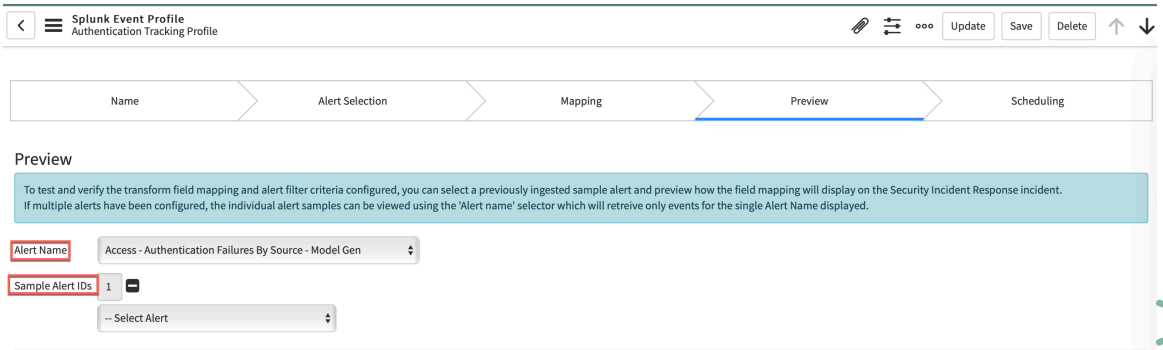
Zeigen Sie die Vorschau eines Security Incidents an, und bearbeiten Sie die Zuordnung bei Bedarf erneut, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wird, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen auf Security Incidents SIR werden nicht als tatsächliche Incidents im Produkt SIR gespeichert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

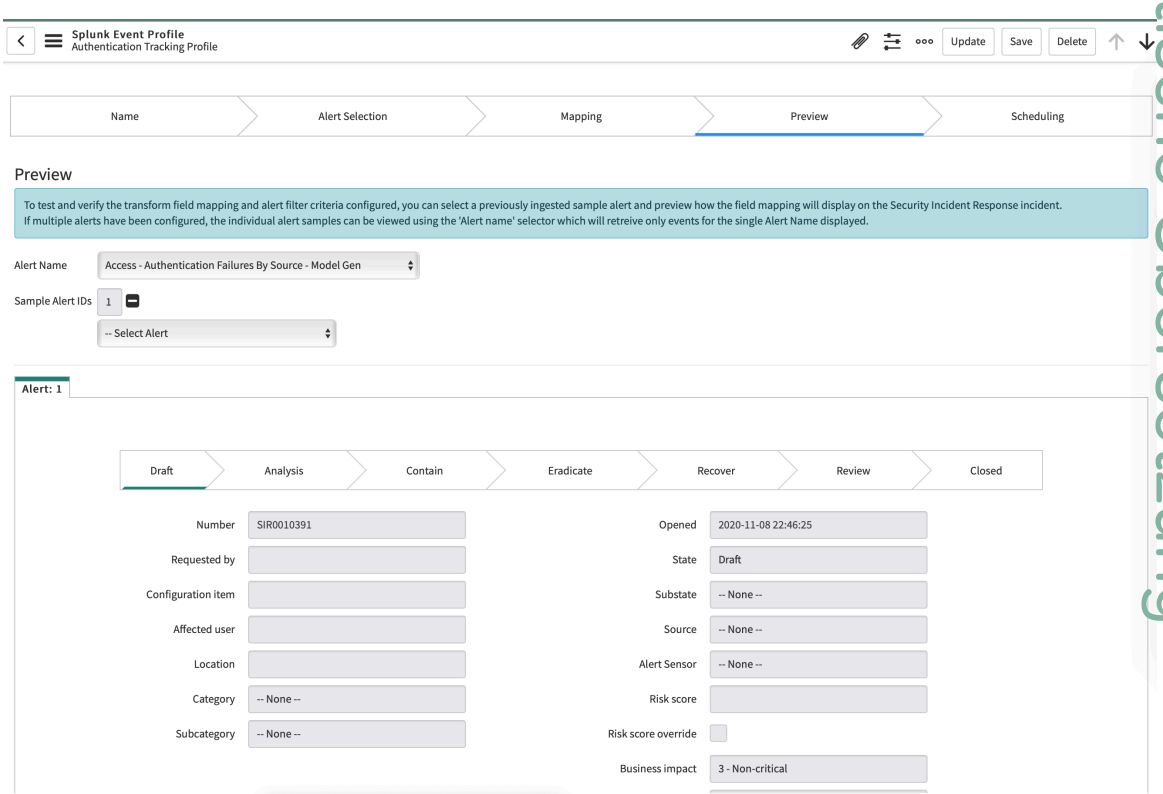
Prozedur

1. Wenn die Vorschau des Security Incidents nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Vorschau**.
2. Wählen Sie den **Warnungsnamen** und dann ein Element in der Liste **Beispielwarnungs-IDs** aus.



Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.

3. Überprüfen Sie die Feldzuordnung der Warnungswerte für den Security Incident.



Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel ist ein Feld im Security Incident für einen Wert nicht vorhanden, oder das Feld unterstützt den von Ihnen zugeordneten Wert nicht. Es wird eine Fehlermeldung angezeigt, die darauf hinweist, dass für das Feld Konfigurationselement kein Eingabewert gefunden wurde.

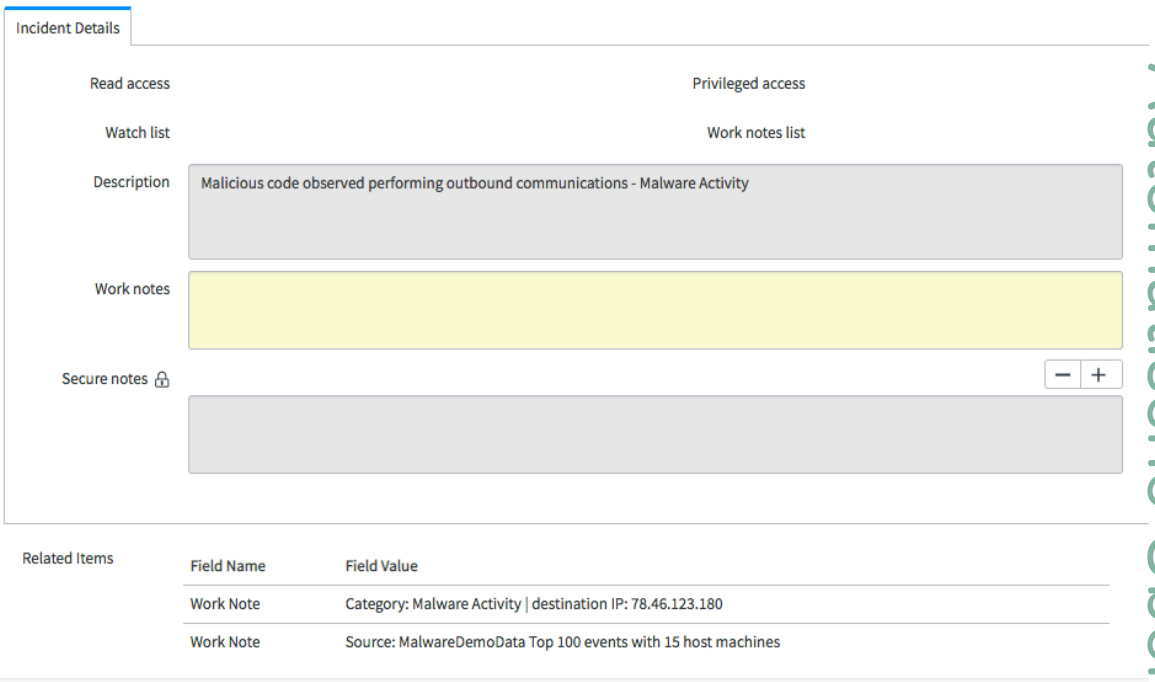
4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in den -Fehlermeldungen beschrieben werden.

   Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Incident-Details in der unteren Hälfte eines SIR -Security Incidents, nachdem alle Fehlermeldungen gelöst wurden. Für dieses Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und diese Felder werden mit den Werten aus den Wertepaaren gefüllt, die aus der Konsole Splunk Enterprise abgerufen wurden. Das erste Feld „Arbeitsnotizen“ enthält keinen Wert. Dieses Feld wurde im Zuordnungsraster während des Zuordnungsschritts leer gelassen. Die zusätzlichen Arbeitsnotizfelder, die Werte enthalten, die dem Zuordnungsraster während des Zuordnungsschritts hinzugefügt wurden.



7. Nachdem Sie alle Fehler behoben und verifiziert haben, dass die Felder Ihren Vorstellungen entsprechen, wählen Sie eine Option aus, um fortzufahren.

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung im Security Incident zufrieden sind, fahren Sie als Nächstes mit Planen Sie Warnungen für die Integration Splunk Enterprise Event Ingestion, und rufen Sie sie abfort.

Planen Sie Warnungen für die Integration Splunk Enterprise Event Ingestion, und rufen Sie sie ab

Für Profile zur automatisierten Warnungserfassung ist dieser Schritt der letzte Schritt der Ereignisprofilkonfiguration. Während dieses Schritts können Sie die Standardeinstellungen für den Warnungsabruf überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie den Abruf Ihrer Warnung basierend auf einem Datumsbereich filtern.

Vorbereitungen

Erforderliche Rolle: Rolle sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie alle Schritte im Fortschrittsbalken für die Profilkonfiguration abgeschlossen haben (siehe folgende Abbildung), haben Sie die Konfiguration für Profile für die manuelle Ereignisweiterleitung abgeschlossen. Für Ereignisse, die manuell von Ihrer Splunk Enterprise -Konsole weitergeleitet werden, ist keine Planung verfügbar. Bei Profilen für die automatisierte Warnungserfassung wählen Sie aus, ob Sie während des Schritts „Zeitplanung“ historische Warnungen erfassen möchten. Sie können auch auswählen, wie häufig zukünftige Warnungen abgefragt werden, die der Konfiguration des Warnungsprofils entsprechen.

Fortschrittsbalken

Bei Profilen zur automatisierten Warnungserfassung überprüfen und ändern Sie vor der Aktivierung des Profils die Zeitplanung und den Warnungsabruf. Dieser Schritt ist der letzte Schritt im Ereignisprofil-Konfigurationsprozess für geplante Warnungsprofile.

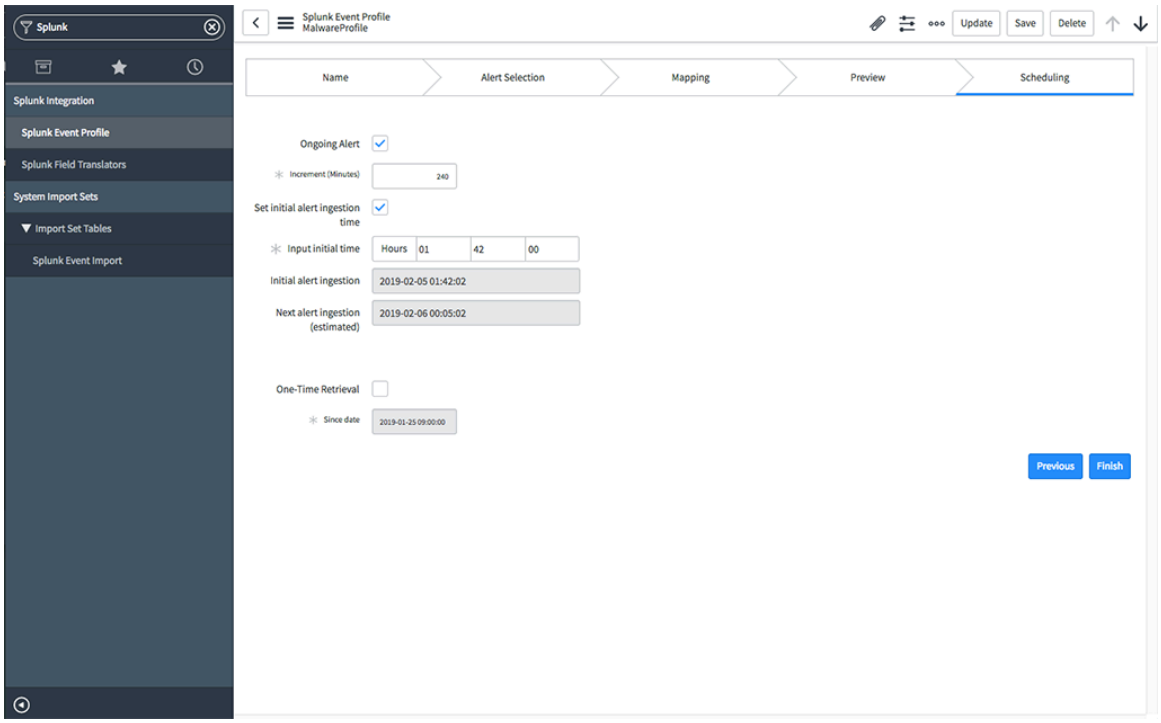
Konfigurieren Sie diese Abfrageintervalle für einzelne Profile. Die Leistung der Splunk Integration zur Erfassung von Ereignissen wird durch die unterschiedlichen Abfrageintervalle beeinflusst. Bei der Planung möchten Sie möglicherweise die Systemlast gegen die Dringlichkeit des incident abwägen. Für jedes Profil ist ein Standardwert von fünf Minuten festgelegt. Sie können diese Einstellung jedoch je nach Dringlichkeit des incident und der erwarteten Auslastung Ihres Systems ändern.

In der Konsole Splunk Enterprise legen Sie eine -Warnung fest, die basierend auf Inkrementen oder einer bestimmten Zeit ausgelöst wird. Verwenden Sie diese Einstellung, um die Zeitplanung in Ihrer Instanz Now Platform zu konfigurieren, damit die Zeitschritte in der Konsole Splunk Enterprise mit der Zeitplanung in Ihrer Instanz Now Platform synchronisiert werden.

Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **„Zeitplanung“**aus.
2. Wählen Sie eine aus, um zu planen, wie und wann Warnungen von der Konsole Splunk Enterprise abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Als Beispiel für die Planung können Sie, wenn Sie eine tägliche Warnung Splunk haben, die einmal täglich um 4:00 Uhr Ortszeit ausgeführt wird, das entsprechende Warnungsprofil in Ihrer Instanz Now Platform so einrichten, dass es um 4:05 Uhr Ortszeit ausgeführt wird, um zu erfassen sofort melden und einen Security Incident erstellen. Geben Sie `04 05 00` in das Feld **Erfassung von ersten Warnungen** ein. Geben Sie im Feld **Inkrement (Minuten)** den `Wert 1440` (24 Stunden) ein, um die nächste Warnungserfassung für 24 Stunden ab der ersten Warnungserfassung zu planen. In den Feldern wird sowohl die Zeit der ersten Warnungserfassung als auch die Zeit der nächsten Warnungserfassung angezeigt.

3. Führen Sie die folgenden Schritte aus, um die Einstellungen für dieses Beispiel zu konfigurieren.

   a. Aktivieren Sie auf der Seite „Zeitplanung“ das Kontrollkästchen **Laufende Warnung**, um diese Option zu aktivieren.

   b. Geben Sie im Feld **Schritt (Minuten) den**`Wert 1440` (24 Stunden) ein.

   c. Klicken Sie auf das Kontrollkästchen **Anfängliche Warnungserfassung auswählen,** um die Bearbeitung der Felder Anfängliche Warnungserfassung und Nächste Warnungserfassung zu aktivieren.

   d. Geben Sie im Feld Anfängliche Warnungserfassung `04 05 00`ein.
   Im Feld **Nächste Warnungserfassung (geschätzt)** wird die Zeit der nächsten Warnungserfassung angezeigt.

4. Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Dieses Profil ist aktiviert und ruft basierend auf Ihrer Planung Warnungen aus der Konsole Splunk Enterprise ab. Innerhalb von 24 Stunden können maximal 1.000 Security Incidents erstellt werden. Bis zu 100 Ereignisse pro ausgelöste Warnung. Nachfolgende Ereignisse werden ignoriert, nachdem die Grenzwerte erreicht sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsarchitektur und externe Systemverbindung für die Splunk Enterprise Event Ingestion -Integration

Das folgende Thema beschreibt die Integrationsarchitektur, die zur Unterstützung der Erfassung von ausgelösten Warnungen über die -Konsole Splunk Enterprise entwickelt wurde. Diese Informationen erläutern allgemein den konzeptionellen Betrieb der Integration. Außerdem wird erläutert, warum vor der Installation der Anwendung von ServiceNow StoreSetupschritte erforderlich sind.

Für diese Integration verwendete Schlüsselbegriffe

Die folgenden Schlüsselbegriffe werden während der Installation und Konfiguration von verwendet. Weitere Informationen zu diesen Begriffen finden Sie auf der Website mit der Produktdokumentation von ServiceNow sowie auf der Splunk-Website und auf der Seite „Splunk-Ressourcen“ .

Now Platform

Ein Produkt des Unternehmens ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management (ITSM) und andere -Produkte aufbauen.

ServiceNow Splunkbase-Add-on

Eine ServiceNow -Anwendung, die auf Ihrer Splunk Enterprise -Konsole installiert ist und die manuelle Ereignisweiterleitungsoption der Integration unterstützt. Die manuelle Ereignisweiterleitung ist eine optionale Funktion der Integration. Dieses ServiceNow Splunkbase-Add-on ist für die von der -Integration bereitgestellte automatisierte Warnungserfassung nicht erforderlich.

Security Incident Response (SIR)

Eine Anwendung Now Platform, die den Fortschritt von Security Incidents von der Discovery und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur abschließenden Überprüfung und Schließung nach Incident verfolgt.

Splunk Enterprise

Ein automatisiertes SIEM-Produkt (Security Incident Event Management) oder ein Cloud-Service, das Daten sammelt, die für die Analyse und Verwaltung von Incidents verwendet werden. Dieser Service befindet sich auf einem Host, der in diesem Handbuch manchmal auch als Splunk -Konsole bezeichnet wird.

Splunk Warnung

Eine Suche, die Sie konfigurieren und in Splunk speichern, um anhand der von Ihnen im Service Splunk Enterprise eingerichteten Parameter nach bestimmten Daten zu suchen. Wenn Sie Warnungen aus Splunkabrufen, rufen Sie auch alle Ereignisse ab, die dieser Warnung zugeordnet sind.

Splunk hat Warnung ausgelöst

Eine konfigurierte Suche in der Konsole Splunk Enterprise, die Ergebnisse zurückgibt und diese Ergebnisse als ausgelöste Warnungen kennzeichnet. Die ausgelösten Warnungen werden für diese Integration von der Konsole Splunk in Ihrer Instanz Now Platform erfasst. Ausgelöste Warnungen haben mindestens ein Ereignis Splunk.

Splunk Termin

Mindestens ein Datenelement, das zu den ausgelösten Warnungen des Service Splunk führt. In Ihrer Instanz Now Platform können Sie nachschlagen, welche Splunk Ereignisse die Security Incidents Now Platform vom Typ ausgelöst haben.

MID-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Anwendung erleichtert die Kommunikation und das Verschieben von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services. Diese Anwendung ist normalerweise für die Integration mit lokalen Technologien erforderlich, und für diese Splunk Enterprise Event Ingestion -Integration vereinfacht der MID-Server die Kommunikation zwischen Now Platform und der lokalen Instanz von Splunk Enterprise. Ein MID-Server ist nicht erforderlich, wenn Sie Ihre Now Platform -Instanz mit einer Splunk Cloud -Instanz integrieren.

Security Incident-Administrator (sn_si.admin)

Der Benutzer mit dieser Rolle überwacht die Konfiguration der Integration mit dem Produkt SIR in Ihrer Instanz Now Platform.

Security Incident-Analyst (sn_si.analyst)

Der Benutzer mit dieser Rolle interagiert mit Security Incidents im Produkt ServiceNow Security Incident Response und analysiert sie.

Verbindung mit externen Systemen

Ein Ereignisprofil ist ein Container, den Sie für eine einzelne Verbindung erstellen, benennen und konfigurieren. Anschließend rufen Sie den Service Splunk auf, um die neuesten ausgelösten Warnungen abzurufen, die bestimmten Kriterien entsprechen. Nachdem ausgelöste Warnungen, die Ihrem Profil entsprechen, aus Splunkabgerufen wurden, wählen Sie aus, welche dieser Warnungen als Now Platform Security Incident Response SIR Security Incident angezeigt werden sollen. Eine Standardansicht der Warnungsfelder Splunk Enterprise ist verfügbar, und Sie bearbeiten diese Zuordnung von Warnungsfeldern zu den Feldern in einem SIR -Security Incident entsprechend Ihren Anforderungen. Zeigen Sie eine Vorschau Ihrer Zuordnung an, um zu überprüfen, ob alle erforderlichen Warnungsfeldwerte im Security Incident SIR ausgefüllt sind. Um die Konfiguration des Warnungsprofils abzuschließen, planen Sie den Abruf von Warnungen und aktivieren dann das Profil. Nachdem Sie das Profil in Now Platformaktiviert haben, können Sie historische und laufende Warnungen Splunk automatisch erfassen.

Wenn Sie als Benutzer mit der Rolle sn_si.admin feststellen, dass eine neue ausgelöste Warnung zuvor erfassten Warnungen ähnelt, können Sie neu ausgelöste Warnungen zu vorhandenen Security Incidents SIR zusammenfassen. Sie legen Kriterien fest, um übereinstimmende Zielfeldwerte im Warnungsprofil Splunk Enterprise anzugeben, die definieren, wann ein vorhandener Security Incident aktualisiert wird und wann ein neuer Security Incident erstellt wird. Wenn in Ihrem Ereignisprofil die Zusammenfassungsfunktion aktiviert ist, sucht Ihre Instanz Now Platform bei der Transformation des Importsatzes nach einem vorhandenen Datensatz in der Zieltabelle, der denselben Wert in den Feldern „Ziel“ und „Quelle“ aufweist. Wenn ein vorhandener Datensatz mit einem übereinstimmenden Wert in der Zieltabelle gefunden wird, wird dieser Datensatz aktualisiert. Wenn kein übereinstimmender Datensatz gefunden wird, wird ein neuer Datensatz in der Zieltabelle erstellt. Wenn diese Option aktiviert ist, aktualisiert die Zusammenfassungsoption vorhandene Security Incidents mit neuen ausgelösten Warnungen, und Sie vermeiden die Erstellung mehrerer Security Incidents. Weitere Informationen zum Aktualisieren von Datensätzen mithilfe von Zusammenfassungsoptionen finden Sie unter Datensätze durch Zusammenfügung aktualisieren .

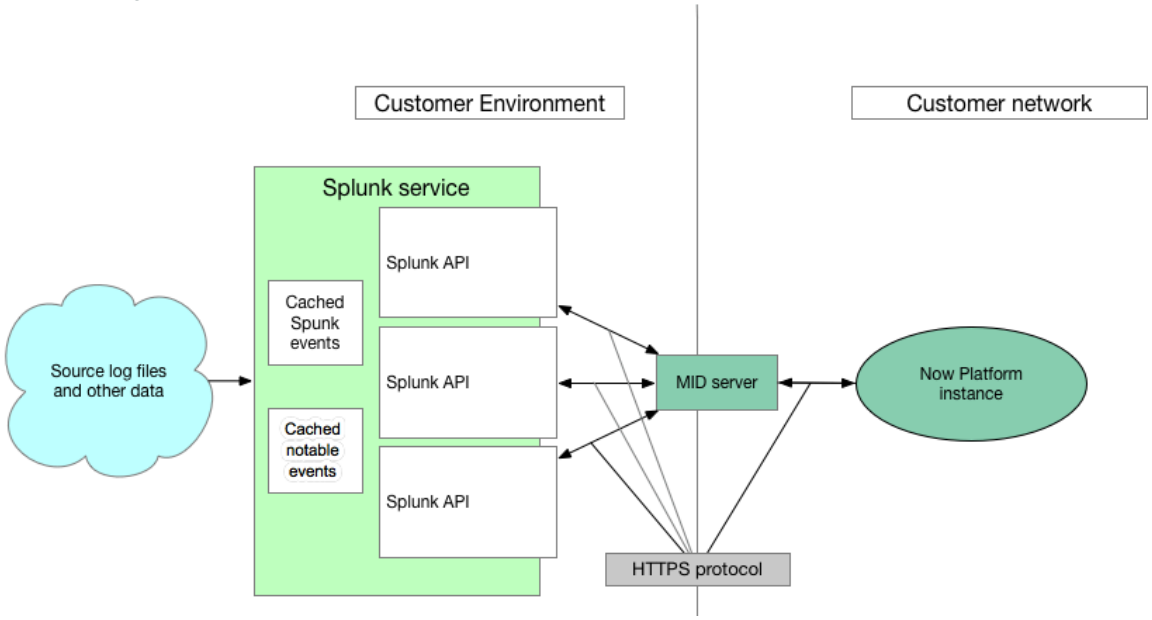
Diese Anwendung verwendet den API-Service Splunk, um Informationen vom Service Splunk abzurufen. Eine ausgehende HTTPS-Verbindung vom MID-Server zu dieser Umgebung ist erforderlich, damit die Integration ordnungsgemäß funktioniert.

Nach der Verbindung mit dem Service Splunk unterstützt die Integration das Abrufen und Erfassen von ausgelösten Warnungen und Ereignissen, die Security Incidents auslösen.

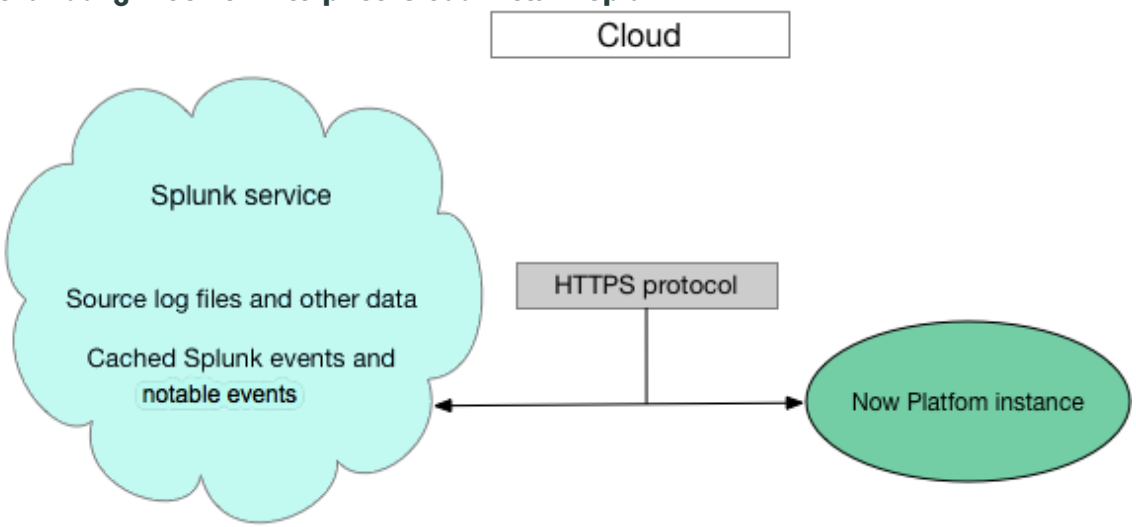
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der grundlegende Daten-Flow ist in den folgenden Abbildungen dargestellt. In jeder Abbildung ruft Ihr Now Platform Daten ab (erfasst sie). Splunk sendet keine Daten für geplante Warnungen.

Verbindung mit lokalem Splunk Enterprise-Service mit einzelnenMID -Servern



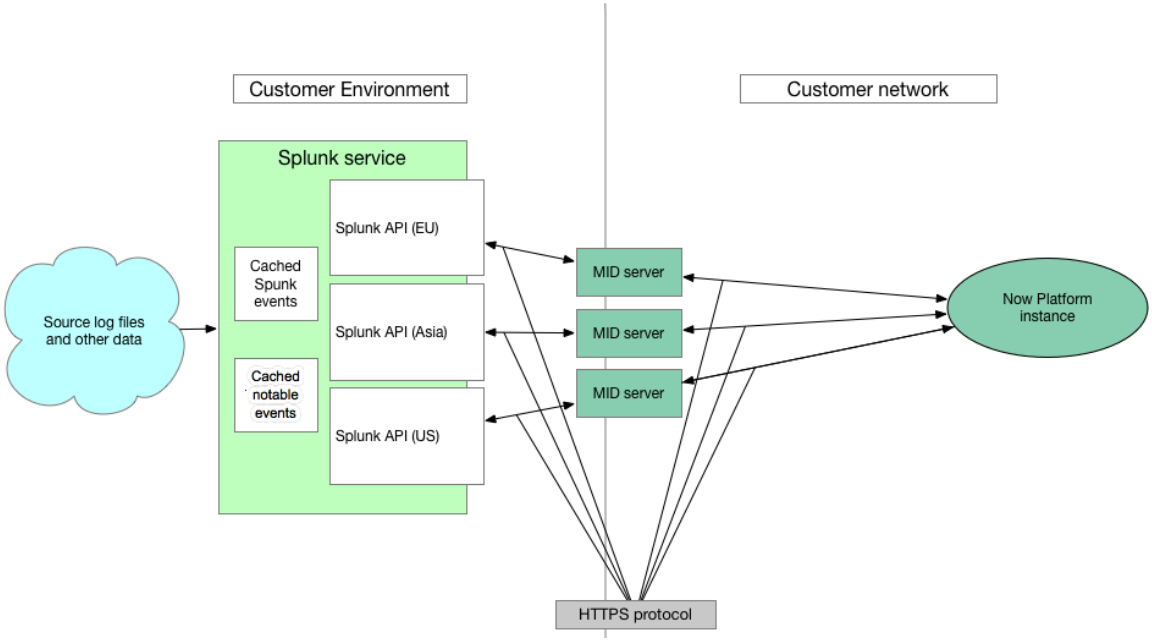
Verbindung mit einer Enterprise-Cloud-Instanz Splunk



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrere Verbindungen zum Enterprise-Service Splunk über mehrere MID-Server



Kopieren Sie Splunk Enterprise Event Ingestion Profile mithilfe der Export-/Importfunktion von einer Instanz in eine andere

Sie können Splunk Enterprise Event Ingestion -Profileinstellungen aus einer Now Platform -Instanz in eine andere Now Platform -Instanz exportieren und importieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Funktionalität ermöglicht es dem Sicherheitsadministrator, Profile, die in einer Instanz Now Platform, z. B. außerhalb der Produktion, getestet und verifiziert wurden, in eine andere Now Platform -Instanz, z. B. die Produktion, zu kopieren, ohne alle Konfigurationseinstellungen wiederholen zu müssen. Zu den Einstellungen, die exportiert und importiert werden, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel.

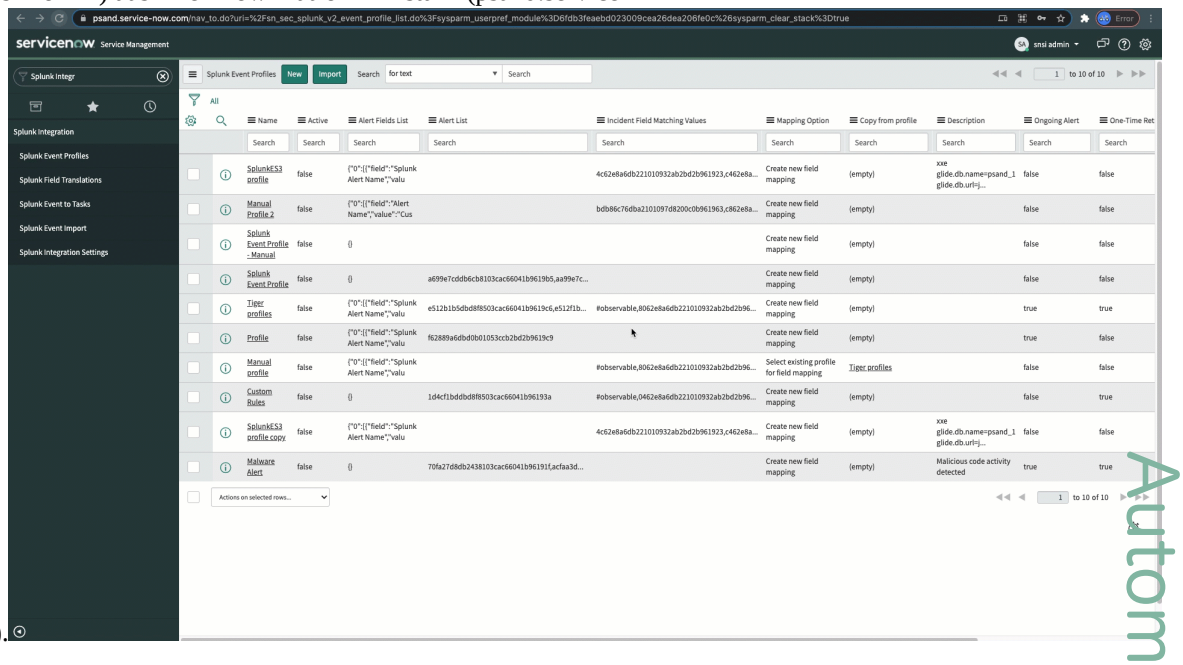
Hinweis:
Wenn Sie einen Profiltyp für die manuelle Ereignisweiterleitung exportieren, werden die für die Beispielfeldzuordnung verwendeten Anhangdaten kopiert. Die Anhangdatei selbst wird jedoch nicht exportiert.

Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Ereignisprofile**.
2. Wählen Sie ein Profil aus, das Sie in eine andere Now Platform -Instanz exportieren möchten. Sie können mehrere Profile für den Export auswählen.
3. Klicken Sie im Menü Aktionen auf **Exportieren**.
4. Wenn die Meldung angezeigt wird, dass der Export abgeschlossen ist, klicken Sie auf **Herunterladen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt den Export eines Splunk -Profils (manuelles Profil 2) aus Ihrer Now Platform -Instanz (psand.service-now.com).



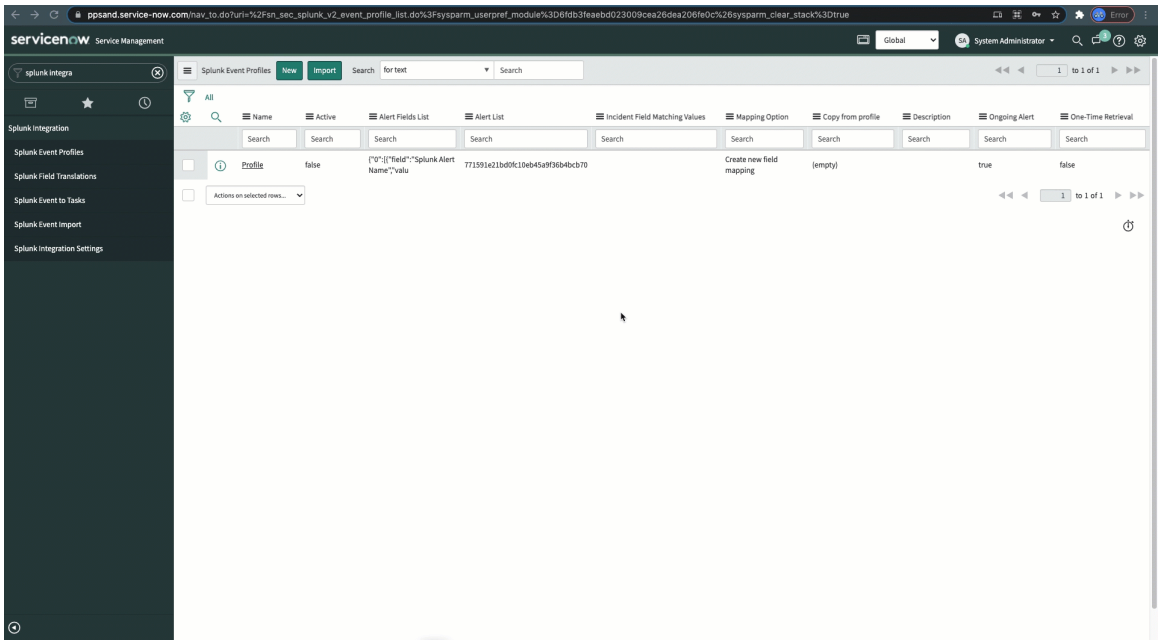
Die exportierte Datei payload.xml wird auf Ihren Computer heruntergeladen. Die Datei enthält den Profilnamen, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel. Wenn Sie mehrere Profile auswählen und herunterladen, werden sie in derselben Datei „payload.xml“ angezeigt.

Sie können jetzt das Profil in einer anderen Now Platform -Instanz importieren.

5. Navigieren zu **Splunk-Integration** > **Splunk-Ereignisprofile**.
6. Klicken Sie auf **Importieren**.
7. Klicken Sie **auf Datei auswählen**, und wählen Sie die XML-Datei auf Ihrem Computer aus.
8. Klicken Sie auf **Hochladen**.
9. Klicken Sie **auf Profile schließen und neu laden**.
   Die folgende Abbildung zeigt den Import eines Splunk -Profils (Manuelles Profil 2) aus der Instanz Now Platform (psand.service-now.com) in eine andere Instanz Now Platform (ppsand.service-now.com).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie haben das Profil erfolgreich aus einer anderen Instanz von Now Platform importiert.

Stellen Sie sicher, dass die exportierte Quelle (API-AccountSplunk und URL des Servers Splunk) und die Konfigurationseinstellungen für den MID-Server gültig und in der importierten Instanz Now Platform verfügbar sind. Aktualisieren Sie bei Bedarf Ihre Splunk Enterprise Event Ingestion -Konfiguration.

10. **Wahlweise:** Überprüfen Sie die MID-Server-Einstellungen, nachdem Sie ein Profil importiert haben.
11. **Wahlweise:** Navigieren zu **Security Operations** > **Integrationskonfigurationen**.
12. **Wahlweise:** Wählen Sie die Konfigurationskachel Splunk Enterprise Event Ingestion aus, und klicken Sie auf **Aktualisieren**.
13. **Wahlweise:** Überprüfen und aktualisieren Sie die Details zur Quelle und zum MID-Server nach Bedarf.

Kopieren Sie ein Ereignisprofil für die Integration Splunk Enterprise Event Ingestion .

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich möglicherweise, Alarmprofile zu kopieren, um Zeit zu sparen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Das Kopieren eines vorhandenen Profils und der zugehörigen Einstellungen ist optional.

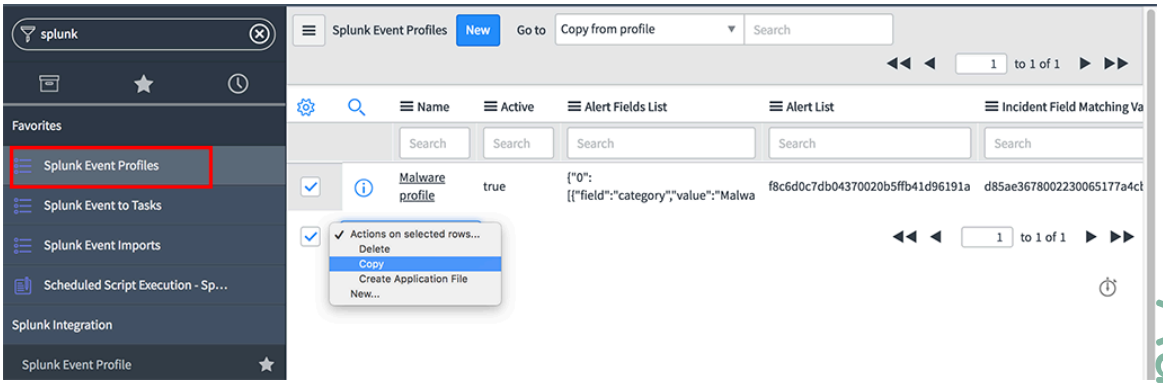
Wenn Sie ein Profil kopieren, wird der Profilname zunächst geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es nicht versehentlich aktiviert wird, bevor die Konfiguration abgeschlossen wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

Automatische Übersetzung

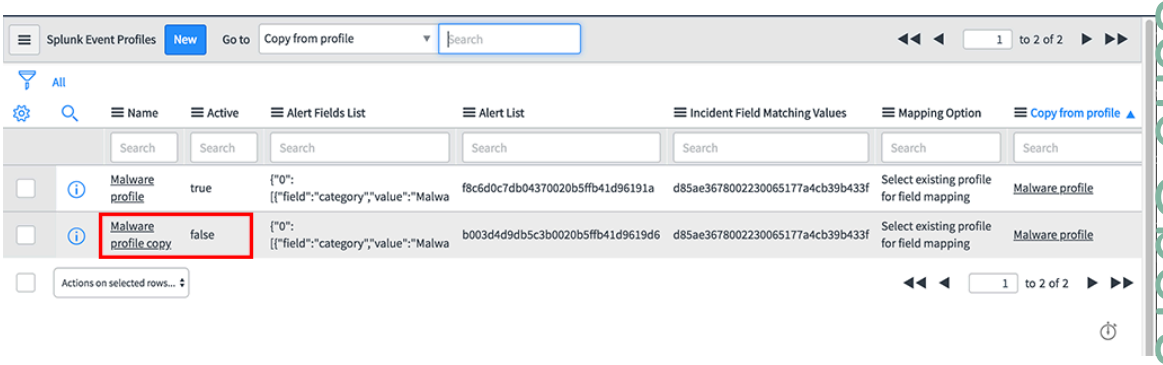
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wählen Sie in der angezeigten Liste Splunk Ereignisprofile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Zeitplankonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie an dieser Stelle deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert.

Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren, nachdem Sie die Konfigurationsschritte abgeschlossen haben.

Richten Sie Ihre Splunk -Umgebung für die manuelle Ereigniserfassung für die Splunk Enterprise -Ereigniserfassungsintegration ein

Wenn Sie Ereignisse für diese Integration manuell und bei Bedarf von Ihrer Splunk Enterprise -Konsole exportieren möchten, installieren und richten Sie die Anwendung ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise in Ihrer Splunk -Unternehmenskonsole oder in der Splunk-Cloud-Instanz ein.

Vorbereitungen

Stellen Sie sicher, dass Sie die Anwendung für diese Integration von ServiceNow Store installiert haben, bevor Sie das Add-on-Plugin von splunkbase installieren, das für die manuelle Ereigniserfassung erforderlich ist. Wenn Sie die Anwendung für die -Integration aus ServiceNow Storenicht installiert haben, rufen Sie Installieren und konfigurieren Sie die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung ServiceNow für die Integration Splunk Enterprise Event Ingestion . auf und befolgen Sie die Anweisungen zur Installation.

Erforderliche Rolle: Now Platform Administrator (admin)

Warum und wann dieser Vorgang ausgeführt wird

Die Installation und Einrichtung des ServiceNow Security Operations Event Ingestion Add-ons ist optional.

Wenn Sie Ereignisse für die Integration manuell und bei Bedarf von Ihrer Konsole Splunk Enterprise exportieren möchten, laden Sie das Add-on „Security Operations Event Ingestion“ für ServiceNowSplunk Enterprise aus splunkbase in Ihrer Konsole Splunk Enterprise herunter, installieren und richten Sie es ein.

Dieses Erweiterungs-Add-on ServiceNow ist erforderlich, damit Security Incidents aus manuell exportierten Ereignissen in Ihrer Instanz Now Platform erstellt werden können. Dieses ServiceNow Security Operations Event Ingestion Add-on für die Anwendung Splunk Enterprise ist auf splunkbase verfügbar.

Für die manuelle Ereignisweiterleitung können Sie bis zu zwei verschiedene Now Platform -Endpunkte (Instanzen) in Ihrer Splunk Enterprise -Konsole identifizieren. Sie leiten die Ereignisse manuell an den Endpunkt oder die Endpunkte weiter, um Security Incidents zu erstellen. Sie können beispielsweise eine Staging-Instanz (Entwicklungsinstanz) und eine Produktionsinstanz angeben. Durch Angabe separater Instanzen und Benennung primärer und sekundärer Workflows für jede Instanz können Sie auswählen, wohin Sie verschiedene Ereignisse weiterleiten möchten.

Prozedur

1. Wenn Sie das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprisenoch nicht installiert haben, führen Sie die folgenden Schritte aus, um es zu installieren und zu konfigurieren.

   a. Navigieren Sie zu splunkbase .

   b. Suchen Sie nach dem ServiceNow Security Operations Security Operations Event Ingestion Add-on für Splunk Enterprise.

   Hinweis:
   Stellen Sie sicher, dass Sie ServiceNow Security Operations Add-on zur Ereigniserfassung für Splunk Enterpriseausgewählt haben. Es gibt zusätzliche ServiceNow Add-ons, die in dieser Liste angezeigt werden. Diese Add-ons gelten für verschiedene ServiceNow Splunk -Integrationen und sind für diese Integration nicht erforderlich.

   c. Laden Sie die Anwendung herunter.

   d. Öffnen Sie Ihr Splunk Enterprise -Konto.

   e. Klicken Sie auf der Seite „Apps“ auf das Zahnradsymbol oder auf die Verknüpfung **Apps verwalten** in der Dropdown-Liste des Menüs.

   f. Klicken Sie oben links auf der angezeigten Seite „Apps“ **auf App aus Datei installieren**.

   g. Klicken Sie **auf Datei auswählen**, wählen Sie ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterpriseaus, und klicken Sie auf **Hochladen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Starten Sie Splunk Enterpriseneu, wenn Sie dazu aufgefordert werden.
Das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise wird in Ihrer Splunk Enterprise Enterprise-Konsole installiert. Der nächste Schritt zum Einrichten des Add-ons.

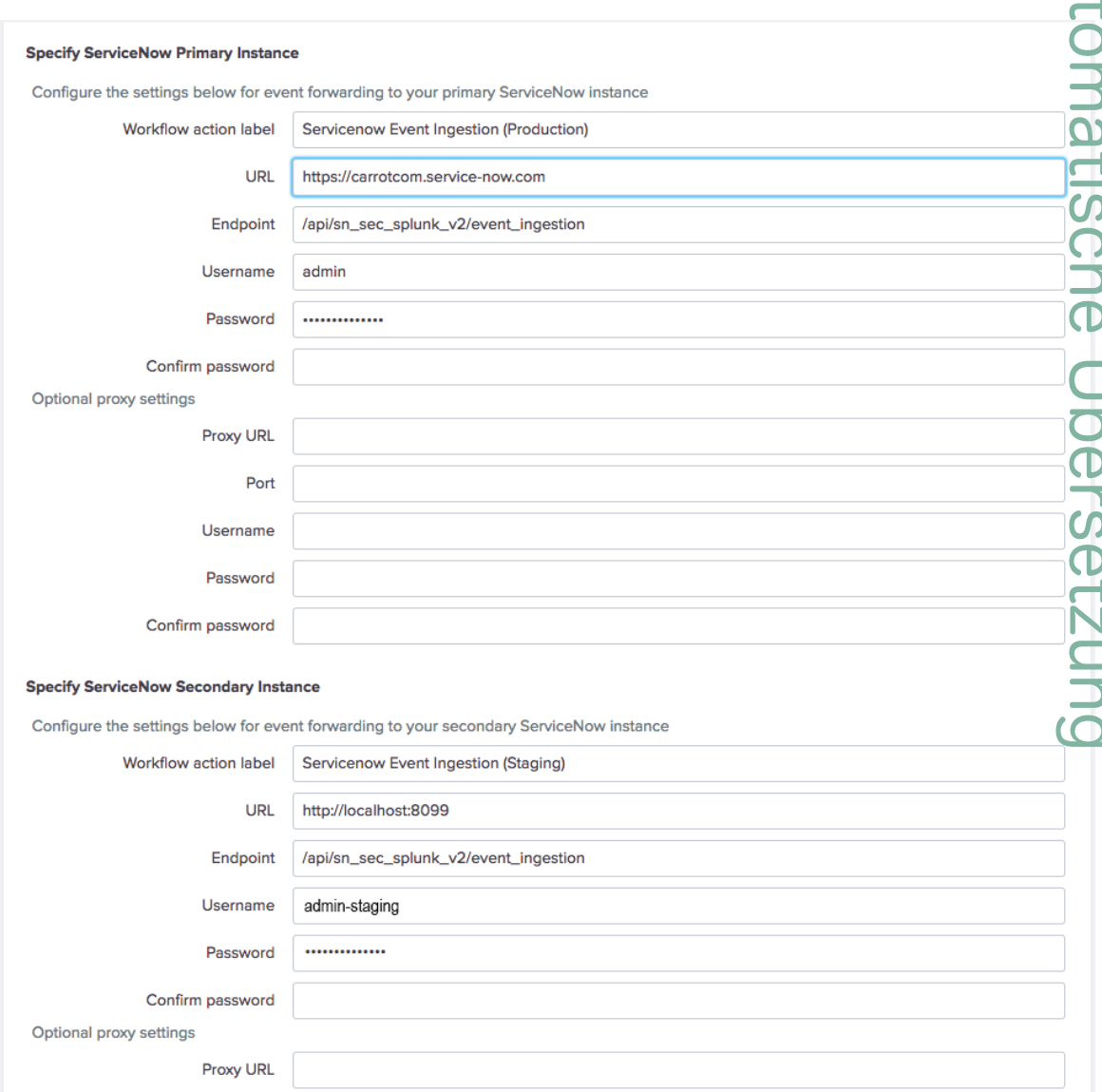
2. Führen Sie die folgenden Schritte aus, um das -Add-on einzurichten.

a. Klicken Sie in Splunk Enterpriseauf das Zahnradsymbol **Apps**, oder klicken Sie in der Dropdown-Liste des Menüs **auf Apps verwalten**.

b. Klicken Sie in der Liste der Anwendungen, die angezeigt wird, in der Spalte **Aktionen** auf Für ServiceNow Security Operations Add-on zur Ereigniserfassung für Splunk Enterprise**einrichten**.

c. Füllen Sie das Formular aus.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes -Formular in Ihrer -Konsole Splunk Enterprise.

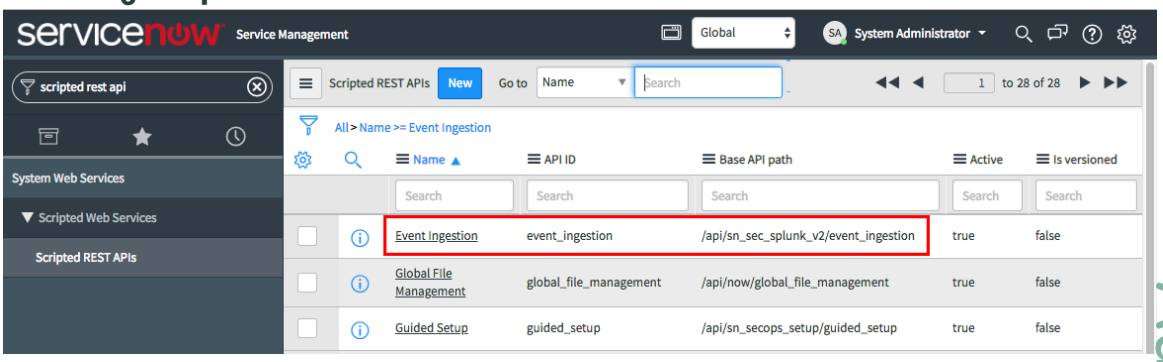


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt ein Beispiel für die Liste der geskripteten REST APIs in Ihrem Now Platform. In der Liste wird die Position des Endpunktwerts einer Now Platform -Instanz angezeigt, die Sie im Rahmen der Einrichtung des ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise in Ihrer Splunk Enterprise -Konsole in das Formular eingeben.

Liste der geskripteten REST APIs in Now Platform



3. Klicken Sie im Setup-Formular in der Konsole Splunk Enterprise auf **Speichern**, um Ihre Änderungen zu speichern.

   Nach einigen Minuten wird oben links im Formular in der Splunk Enterprise -Konsole eine Meldung angezeigt, dass der Datensatz erfolgreich aktualisiert wurde.

   Nachdem Sie das Formular gespeichert haben, sind die Namen (Workflow-Aktionsbezeichnungen) für die von Ihnen im Formular erstellten Instanzen Now Platform in der Auswahlliste Ereignisaktionen für ein ausgewähltes Ereignis einer Suche in Ihrer Konsole Splunk Enterprise verfügbar.

Nächste Maßnahme

Wenn Sie Suchen noch nicht in der Konsole Splunk Enterprise gespeichert haben, besteht der nächste Schritt darin, Suchen als Warnungen in der Konsole Splunk Enterprise zu speichern.

Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration

Die folgenden Schritte zum Speichern von Suchen in der Konsole Splunk Enterprise werden für Benutzer mit der Administratorrolle Splunk Enterprise bereitgestellt.

Vorbereitungen

Wenn Sie bereits gespeicherte Suchen und ausgelöste Warnungen in Ihrer Splunk Enterprise -Konsole haben, müssen Sie diese Suchen für diese Integration nicht ändern.

Durch die Integration des Produkts Now Platform® Security Operations mit dem Ereignisbenachrichtigungsservice Splunk werden Ereignis- und Warnungsinformationen aus Splunkabgerufen.

Bevor Sie Warnungen in Ihrer Security Operations -Umgebung erfassen, konfigurieren Sie Suchvorgänge in Ihrer Splunk Enterprise -Konsole, um automatisch die relevanten Sicherheitsereignisse in Splunk Enterprise abzurufen, die Sie als Warnungen speichern möchten.

Wenn Sie keine gespeicherten Suchen und keine ausgelösten Warnungen für Benachrichtigungen bei wichtigen Sicherheits-Ereignisse in der Splunk Enterprise -Konsole eingerichtet haben, führen Sie die folgenden Schritte aus, um Suchen zu speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Splunk Enterprise Administrator

Prozedur

1. Melden Sie sich bei Ihrem Splunk Enterprise-Konto an.
2. Klicken Sie auf die Registerkarte **Suchen**.
3. Geben Sie im angezeigten Feld Neue Suche einen Wert für die Warnung ein, z. B. Malware.
4. Um die Ereignisse im Zusammenhang mit Ihrer Suche anzuzeigen, klicken Sie rechts neben dem Feld Neue Suche auf das Suchsymbol, oder drücken Sie die Eingabetaste.
   Die Suchergebnisse mit Ereignissen werden angezeigt.
5. Um die Suche als Warnung zu speichern, erweitern Sie oben rechts auf der Seite die Auswahlliste Speichern unter, und wählen Sie **Warnung**aus.
6. Füllen Sie die Felder im angezeigten Formular aus.
7. Klicken Sie auf **Speichern**.
   Ihre Warnung wird gespeichert und auf der Suchseite auf der Registerkarte Warnungen angezeigt.
   Der Service Splunk ruft die Ereignisse ab, indem er die Kriterien erfüllt, die Sie in der Warnung konfiguriert haben. Die Ereignisse werden zwischengespeichert, und Sie fordern diese Ereignisse dann von Ihren Profilen an, die Sie in Ihrer Instanz Now Platform eingerichtet haben. Da der Erfassungsabruf von Ereignissen aus einem Cache im Service Splunk erfolgt, wirkt sich diese Erfassung von Ihrem Now Platform nicht auf die Leistung Ihrer Plattform Splunk aus.

Nächste Maßnahme

Sie haben das erforderliche Setup für die Integration in Ihrer Splunk Enterprise -Konsole erfolgreich abgeschlossen. Wenn Sie die Anwendung für die Integration noch nicht aus ServiceNow Storeinstalliert haben, besteht der nächste Schritt darin, die Anwendung für die Integration zu installieren und zu konfigurieren.

Verwenden Sie den Skript-Editor zum Formatieren von Warnungswerten für die Integration Splunk Enterprise Event Ingestion .

Verwenden Sie den Skript-Editor zum Formatieren von Feldwerten im Security Incident während des Zuordnungsschritts.

Vorbereitungen

Zusätzlich zu den direkt zugeordneten Feldern aus den abgerufenen Warnungswerten und den manuell eingegebenen Warnungswerten können Sie optional den Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Der Skript-Editor ändert die Werte einer Splunk -Warnung so, dass Werte, die vom Security Incident Now Platform® Security Incident Response unterstützt werden, den Feldern „Kategorie“, „Configuration Item“ (CI) und „Erkennbares Element“ zugeordnet werden.

Erforderliche Rolle: sn_si.admin

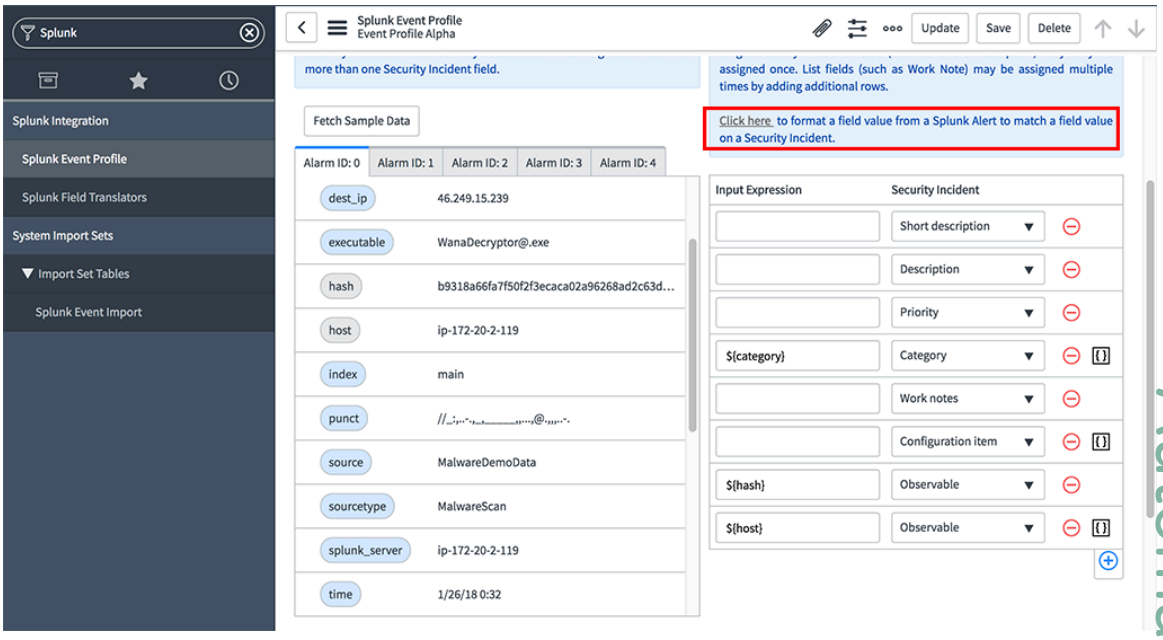
Warum und wann dieser Vorgang ausgeführt wird

In bestimmten Fällen werden die Warnungswerte Splunk Enterprise den Feldern Kategorie, Configuration Item (CI) und Erkennbares Element im Incident SIR zugeordnet und nicht unterstützt. Möglicherweise möchten Sie die zugeordneten Werte bearbeiten. Wenn Sie den Wert einer Splunk Enterprise -Warnung in einen Wert übersetzen möchten, der von diesen Feldern im Security Incident SIR unterstützt wird, verwenden Sie den Skript-Editor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.

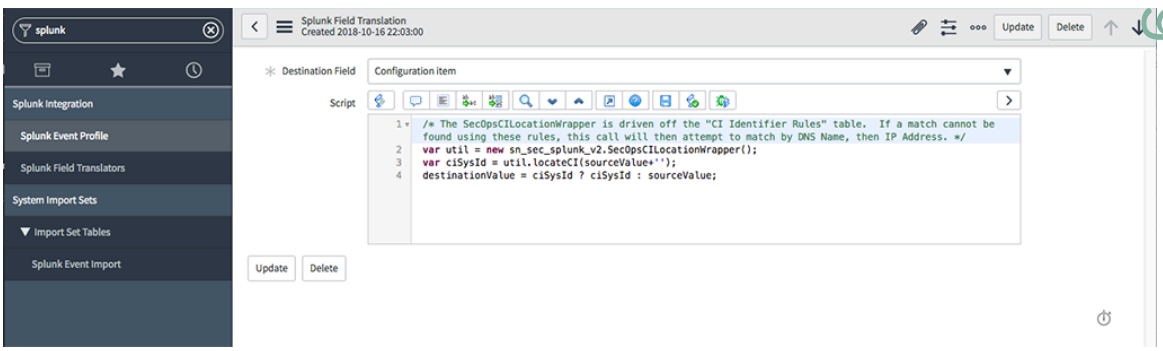


2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt „SIR-Incident-Feldzuordnung“ auf das Klammersymbol [{}] neben einem Feld klicken, um den Skript-Editor für dieses Feld zu öffnen.

   In bestimmten Fällen ist möglicherweise eine Skripteinbindung für das Feld Konfigurationselement geeignet. Bei einer Warnung stimmt möglicherweise kein Wert für das Configuration Item mit überein.

   Wie in der folgenden Abbildung gezeigt, können Sie, wenn im CMBD Now Platform® für das Feld Konfigurationselement keine Übereinstimmung für einen Hostnamen gefunden wird, die Regel so bearbeiten, dass das Feld Konfigurationselement ausgefüllt wird, sobald eine IP-Adresse gefunden wird. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf NULL gesetzt.

   Der Editor wird mit dem Feld unter Zielfeld geöffnet. Die folgende Abbildung zeigt den Editor mit dem Feld Konfigurationselement als Zielfeld.



4. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
   Die Tabelle „Feldübersetzungen Splunk “ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für die Splunk Enterprise Event Ingestion -Integration

Verwenden Sie diese Prüfliste, um sich durch alle Aufgaben der Integration zu führen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle mit den erwarteten Ergebnissen für die Integration.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration anhand der folgenden Tabelle. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jede Zeile der Tabelle listet Aufgaben auf und gibt die Rollen an, die zum Ausführen der Aufgaben erforderlich sind. Außerdem wird auf nummerierte Themen im Installations- und Konfigurationsleitfaden verwiesen.

Erforderliche Rollen: Nachfolgend werden für jeden Schritt Rollen aufgeführt.

Prozedur

1. Richten Sie als Benutzer mit der Administratorrolle Now Platform Ihre Instanz Now Platform ein.
   - Weisen Sie nach Bedarf Benutzer mit den Rollen sn_si.admin und sn_si.analyst zu.
   - Installieren und konfigurieren Sie einen MID-Server, wenn der -Server Splunk in Ihrem Unternehmensnetzwerk bereitgestellt wird.
   - Vergewissern Sie sich, dass die Plugins ServiceNow Security Incident Response für Ihr Release von Now Platformaktiviert sind.
   - Wenn Sie Ereignisse manuell von Ihrer Splunk Enterprise -Konsole an Ihre Now Platform -Instanz weiterleiten möchten, vergewissern Sie sich, dass Sie die Rolle (sn_sec_splunk_v2.api_account_access) einem Benutzer mit der Enterprise-Administratorberechtigung Splunk Enterprise zugewiesen haben.

   Weitere Informationen finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration Splunk Enterprise Event Ingestion ein.

   Sie haben die Einrichtungsschritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration verifiziert.
2. Installieren und konfigurieren Sie als Benutzer mit der Administratorrolle Now Platform die Anwendung Splunk Enterprise Event Ingestion über ServiceNow Store.
   a. Laden Sie die Anwendung herunter, und installieren Sie sie in Ihrer Instanz Now Platform.
   b. Konfigurieren Sie die Anwendung, und stellen Sie eine Verbindung zu Ihrer Splunk Enterprise -Konsole her.

   Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration Splunk Enterprise Event Ingestion ..
3. **Wahlweise:** Wenn Sie Ereignisse manuell von der Konsole Splunk Enterprise in die Instanz Now Platform exportieren möchten, gehen Sie wie folgt vor:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Als Splunk Enterprise -Administrator müssen Sie das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise über splunkbase in Ihrer Splunk Enterprise -Konsole installieren, einrichten und aktivieren.

b. Wenn Sie als Splunk Enterprise -Administrator dies noch nicht konfiguriert haben, können Sie Suchvorgänge als Warnungen in Ihrer Splunk Enterprise -Konsole speichern.

(Optional) Weitere Informationen finden Sie unter Richten Sie Ihre Splunk -Umgebung für die manuelle Ereigniserfassung für die Splunk Enterprise -Ereigniserfassungsintegration ein und Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration.

4. Als Benutzer mit der Rolle Now Platform sn_si.admin müssen Sie ein Ereignisprofil erstellen und benennen.

Wählen Sie den Profiltyp aus der Auswahlliste aus. Optionen sind ein geplantes Warnungsprofil, das Sie zum Erfassen von Beispieldaten verwenden, oder ein Ereignisprofil, das Sie zum manuellen Exportieren von Anhangsdaten aus Ihrer Splunk Enterprise -Konsole verwenden.

- Wählen Sie für eine geplante Warnung eine verfügbare Warnung aus.
- Erstellen Sie für ein Profil für manuell exportierte Daten eine neue Karte, oder kopieren Sie eine vorhandene Karte.

Weitere Informationen finden Sie unter Erstellen und benennen Sie ein Ereignisprofil für die Splunk Enterprise Event Ingestion -Integration.

5. Ordnen Sie als Benutzer mit der Rolle Now Platform sn_si.admin erfasste Werte oder Anhangsdaten, die aus Security Incidents Splunk Enterprise exportiert werden, nach Now Platform zu.

a. Rufen Sie Beispieldaten für eine geplante Warnung ab.

b. Exportieren Sie Anhangdaten für ein Ereignis manuell aus Splunk Enterprise.

c. Bearbeiten Sie die Standardzuordnungskonfiguration.

d. Fügen Sie optional Filterkriterien hinzu, hängen Sie eine Warnung an einen vorhandenen Security Incident an, und verwenden Sie den Skript-Editor.

Weitere Informationen finden Sie unterZuordnung von Warnungen und Ereignissen für die Splunk Enterprise Event Ingestion -Integration und Zuordnungswarnungen für die Splunk Enterprise Event Ingestion -Integration.

6. Zeigen Sie als Benutzer mit der Rolle Now Platform sn_si.admin eine Vorschau der Daten von Splunk Enterprise an, die zu einem Security Incident Now Platform angezeigt werden.

Beheben Sie Fehler, oder fügen Sie fehlende Daten hinzu, damit keine Fehlermeldungen angezeigt werden.

Weitere Informationen finden Sie unter Zeigen Sie eine Vorschau des Security Incident für die -Integration Splunk Enterprise Event Ingestion an.

7. Planen Sie als Benutzer mit der Rolle „sn_si.admin“ Now Platform den Warnungsabruf für ein Profil mit einer geplanten Warnung.

Weitere Informationen finden Sie unter Planen Sie Warnungen für die Integration Splunk Enterprise Event Ingestion, und rufen Sie sie ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunk Enterprise Security Event Ingestion Integration für Security Operations von ServiceNow

Die Integration der Splunk Enterprise Security Erfassung beachtenswerter Ereignisse mit dem Produkt Security Incident Response (SIR) ermöglicht Security Incident-Analysten das Sammeln und Verarbeiten von Daten zu beachtenswerten Ereignissen (sog. „notables“).

Übersicht

Daten werden kontinuierlich basierend auf einem konfigurierten Abfragezeitplan erfasst und von Analysten verwendet, um potenzielle Cyberbedrohungen zu identifizieren und darauf zu reagieren. Gesammelte Sicherheitsereignisse können zu wichtigen Ereignissen in Splunk Enterprise Security korreliert und dann mit dieser Integration automatisch erfasst werden. Außerdem können einzelne wichtige Ereignisse bei Bedarf manuell von der Incident-Überprüfungskonsole und der Berichterstellungsschnittstelle Splunk Enterprise Security an das Produkt Security Incident Response von [Now Platform weitergeleitet werden, um Security Incidents zu erstellen.

Diese Integration bietet einem SOC-Analysten (Security Operations Center) Einblick in wichtige Ereignisse und zugehörige beitragende Ereignisdaten. Diese Daten können zur weiteren Untersuchung und Behebung in Security Incidents Now Platform Security Incident Response (SIR) integriert werden. In Ihrer Instanz Now Platform werden Profile erstellt, um verschiedene Typen von beachtenswerten Ereignissen zu verarbeiten, die über Korrelationssuchen in Splunk Enterprise Securityerstellt werden. Diese Profile passen an, wie verschiedene Splunk -Ereignisfelder in SIR -Security-Incidents angezeigt werden.

Schlüsselfunktionen

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Erstellen Sie mehrere Profile zur Erfassung wichtiger Ereignisse, um SIR-Security Incidents für bestimmte Arten von Bedrohungen wie Phishing, Malware und nicht autorisierte Zugriffsversuche zu erstellen.
- Erstellen Sie mehrere Ereignisprofile für die bedarfsgesteuerte Ereignisweiterleitung über Ihre Incident-Überprüfungskonsole Splunk ES, um SIR-Security-Incidents zu erstellen.
- Drag-and-Drop-Zuordnung von Splunk Feldwerten für wichtige Ereignisse zu zugehörigen SIR-Security Incident-Feldern.
- Eine Vorschau des SIR Security Incident-Layouts basierend auf wichtigen Beispielereignissen zur Validierung der Ereigniszuordnungsdetails.
- Erfassen Sie historische beachtenswerte Ereignisse sowie laufende, neue und aktualisierte beachtenswerte Ereignisse in konfigurierbaren Intervallen.
- Filtern Sie wichtige Ereignisse heraus, die die SIR-Kriterien für die Incident-Generierung nicht erfüllen, z. B. Ereignisse mit niedriger Priorität, Ereignisse, die einen bestimmten Status noch nicht erreicht haben, usw.
- Fassen Sie Ereignisse oder Warnungen zu vorhandenen SIR Security Incidents basierend auf übereinstimmenden Feldwerten zusammen, um doppelte Security Incidents zu vermeiden.
- Aktualisieren Sie wichtige Ereignisse basierend auf den Bedingungen für die Erstellung und/oder den Abschluss von SIR-Incidents über eine bidirektionale Schnittstelle, um die Aktualisierung von wichtigen Ereignissen Splunk ES mit dem SIR-Incident-Status ServiceNow synchron zu halten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Versionen Now Platform.

Das Plugin „com.snc.si_dep“ ist für diese Integration erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations -Anwendungen müssen über ServiceNow Storeinstalliert und aktiviert werden. Installieren Sie eine Anwendung nach der anderen in der unten aufgeführten Reihenfolge, und aktivieren Sie sie dann, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response

Weitere Informationen zur Installation der Security Operations -Core-Anwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

ServiceNow Add-ons

Das ServiceNow Security Operations Event Ingestion Add-on für Splunk ES ist nur erforderlich, wenn Sie Ereignisse manuell von Ihrer Splunk Enterprise Security Incident Review-Konsole an Ihre Now Platform Instanz weiterleiten möchten. Das Add-on ServiceNow ist in splunkbase verfügbar.

Dieses ServiceNow Security Operations Event Ingestion Add-on für die Anwendung Splunk Enterprise in Splunkbase ist für die automatisierte Warnungserfassung, die von der Integration unterstützt wird, nicht erforderlich.

Von Splunk unterstützte Versionen

Diese Integration wurde mit Splunk Enterprise Version 8.0.1 und mit Splunk Enterprise Security Anwendungsversion 6.2.1 getestet.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrer Instanz Now Platform®, um eine Verbindung zum Service Splunk herzustellen, wenn der Server Splunk innerhalb Ihres Unternehmensnetzwerks bereitgestellt wird. Wenn Sie den Service Splunk Cloud verwenden, ist kein MID-Server erforderlich. Weitere Informationen zu MID-Servern finden Sie unter MID-Server.

Referenzen

Referenz	Dokumentbezeichner	Dokumententitel
1	Splunk Produktwebsite	Produktwebsite von Splunk Enterprise Security

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Eine Druckliste dieser Themen finden Sie unter Prüfliste für die Splunk Enterprise Security Integration „Notable Event Ingestion“.. Sie können diese Liste verwenden, um Ihren Fortschritt bei der Bearbeitung der Aufgaben der Integration zu überwachen.

In dieser Integration verwendete Schlüsselbegriffe

In diesem Abschnitt werden einige der wichtigsten in dieser Integration verwendeten Begriffe beschrieben.

Die folgenden Schlüsselbegriffe werden während der Installation und Konfiguration von verwendet. Weitere Informationen zu diesen Begriffen finden Sie auf der Website mit der Produktdokumentation von ServiceNow sowie auf der Splunk-Website und auf der Seite „Splunk-Ressourcen“ .

Now Platform

Ein Produkt des Unternehmens ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management (ITSM) und andere -Produkte aufbauen.

ServiceNow Splunkbase-Add-on

Eine ServiceNow -Anwendung, die auf Ihrer Splunk Enterprise Security -Konsole installiert ist und die manuelle Ereignisweiterleitungsoption der Integration unterstützt. Die manuelle Ereignisweiterleitung ist eine optionale Funktion der Integration. Das Splunkbase-Add-on ServiceNow ist nicht für die automatisierte Erfassung wichtiger Ereignisse erforderlich, die von der Integration bereitgestellt wird, die Ereignisse aus Splunkabruft.

Security Incident Response (SIR)

Eine Anwendung Now Platform, die den Fortschritt von Security Incidents von der Discovery und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur abschließenden Überprüfung und Schließung nach Incident verfolgt.

Splunk Enterprise Security

Splunk Enterprise Security hilft Teams, unternehmensweite Transparenz und Sicherheitsinformationen für die kontinuierliche Überwachung, die Reaktion auf Incidents und den SOC-Vorgang zu gewinnen, und bietet Führungskräften Einblicke in Geschäftsrisiken. Splunk Enterprise Security ist eine Premium-Sicherheitslösung, die eine kostenpflichtige Lizenz erfordert. Dieser Service befindet sich auf einem Host oder einem Splunk-Cloud-Angebot, das in diesem Handbuch als Splunk -Konsole bezeichnet wird.

Splunk Enterprise Security Bemerkenswertes Ereignis

Wenn eine Korrelationssuche ein Ereignis oder ein Ereignismuster identifiziert, erstellt sie ein beachtenswertes Ereignis. Korrelationssuchen filtern die Sicherheitsdaten und korrelieren ereignisübergreifend, um einen bestimmten Typ von Incident (oder ein bestimmtes Muster von Ereignissen) zu identifizieren. Anschließend werden nennenswerte Ereignisse erstellt.

Splunk Termin

Mindestens ein Datenelement, das zu den beachtenswerten Ereignissen des Service Splunk führt. In Ihrer Instanz Now Platform können Sie nachschlagen, welche Splunk Ereignisse die Security Incidents Now Platform vom Typ ausgelöst haben.

MID-Server

Diese Anwendung erleichtert die Kommunikation und das Verschieben von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services. Diese Anwendung ist in der Regel für die Integration mit lokalen Technologien erforderlich, und für diese Splunk Enterprise Security Integration der Ereigniserfassung erleichtert der MID-Server die Kommunikation zwischen Now Platform und der lokalen Instanz von Splunk Enterprise Security.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein MID-Server ist nicht erforderlich, wenn Sie Ihre Now Platform -Instanz mit einer Splunk Cloud -Instanz integrieren.

Security Incident-Administrator (sn_si.admin)

Der Benutzer mit dieser Rolle überwacht die Konfiguration der Integration mit dem Produkt SIR in Ihrer Instanz Now Platform.

Security Incident-Analyst (sn_si.analyst)

Der Benutzer mit dieser Rolle interagiert mit Security Incidents im Produkt ServiceNow Security Incident Response und analysiert sie.

Richten Sie Ihre Instanz Now Platform® für die Integration Splunk Enterprise Security ein

Im folgenden Abschnitt werden die Setupaufgaben aufgeführt, die Sie in der Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung von ServiceNow Storeinstallieren.

Erforderliche Rolle: admin.

Sehen Sie sich die folgende Tabelle an, und vergewissern Sie sich, dass Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

1. Vergewissern Sie sich, dass die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen wurden.

   Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Instanz Now Platform® von erforderlich.

   - Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.
   - Wenn Sie wichtige Ereignisse für diese Integration manuell von Splunk Enterprise Security weiterleiten möchten, weist ein Benutzer mit der Administratorrolle Now Platform® einen Benutzer mit der Rolle (sn_sec_splunkes.api_account_access) in Now Platform®zu. Diese Rolle ermöglicht einem Anwender mit der Administratorrolle Splunk Enterprise Security den Zugriff auf die API in Now Platform®, die für die manuelle Ereignisweiterleitung für diese Integration erforderlich ist.

     Die Rolle (sn_sec_splunkes.api_account_access) ist für die -Integration nicht erforderlich, wenn Sie wichtige Ereignisse automatisch aus Splunk Enterprise Security in Ihrer -Instanz Now Platform® erfassen.

   - Ein Benutzer mit der Rolle sn_si.admin überwacht die folgenden Aufgaben in Now Platform®:
     - Er benennt Ereignisprofile und erstellt sie.
     - Wählt Werte aus Splunk Enterprise Security bis Now Platform® Security Incidents aus und ordnet sie zu.
     - Zeigt eine Vorschau der Details von Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.
     - Plant die laufende Erfassung wichtiger Ereignisse.
     - Aktiviert die Aktualisierung wichtiger Ereignisse, wenn ein SIR-Incident erstellt und geschlossen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weist die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu.
- Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.

Weitere Informationen finden Sie unter Managing roles .

2. Weisen Sie die Anwenderrolle Splunk zu.

   Weisen Sie in Splunk ES eine Sicherheitsanalysten-Anwenderrolle (ess_analyst) zu, um alle integrationsbezogenen Aktivitäten auf dem Server Splunk auszuführen.

3. Stellen Sie sicher, dass Sie Version 7.2.6 oder höher der Splunk API verwenden. Frühere Versionen werden nicht unterstützt.

   Wenn Sie Zugriff auf die -Konsole Splunk Enterprise Security haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich.

4. Stellen Sie sicher, dass Sie einen MID-Server installiert und konfiguriert haben.

   Ein MID-Server in Ihrer Instanz Now Platform® ist erforderlich, um eine Verbindung zum Service Splunk herzustellen, wenn der Server Splunk innerhalb Ihres Unternehmensnetzwerks bereitgestellt wird. Weitere Informationen finden Sie unter MID-Server .

   Wenn Sie den Cloud-Service Splunk Enterprise Security verwenden, ist ein MID-Server nicht erforderlich.

5. Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind.

   Das Dependency-Plugin Security Incident Response (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.

   Stellen Sie sicher, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.

   a. Security Incident Response
   b. – Framework für Sicherheitsintegration
   c. Sicherheitssupport Allgemein

   Weitere Informationen zur Installation der Security Operations -Kernanwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab und Aktivieren Sie eine ServiceNow Store -Anwendung.

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht in der Installation der Anwendung Splunk Enterprise Security Notable Event Ingestion aus ServiceNow Store für die -Integration. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration Splunk Enterprise Security „ Notable Event Ingestion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie wichtige Ereignisse manuell und bei Bedarf von Ihrer Splunk Enterprise Security -Konsole für die Integration exportieren möchten, finden Sie weitere Informationen unter Richten Sie Ihre Umgebung Splunk für die manuelle Ereigniserfassung für die Integration Splunk Enterprise Security „ Notable Event Ingestion ein.

Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration Splunk Enterprise Security „ Notable Event Ingestion

Bevor Sie die -Integration in Ihrer Instanz Now Platform® ausführen, führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in die -Produkte Security Incident Response und Security Operations in Ihrer Instanz Now Platform® integriert werden kann.

Vorbereitungen

Erforderliche Rolle: ess_analyst

Weisen Sie in Splunk ES die Anwenderrolle „Sicherheitsanalyst“ (ess_analyst) zu, um alle integrationsbezogenen Aktivitäten auf dem Splunk-Server auszuführen.

Prozedur

1. Wenn Sie die Anwendung Splunk Enterprise Security Event Ingestion (Ereigniserfassung) aus ServiceNow Store für die Integration nicht installiert haben, rufen Sie Installieren Sie eine Security Operations -Integration auf und befolgen Sie die Schritte zur Installation.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Splunk Ereigniserfassungen.
3. Klicken Sie zum Konfigurieren der Anwendung auf **Neu**.

4. Alternativ: Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, können Sie darauf klicken, um eine vorhandene Konfiguration zu bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie die Felder im angezeigten Dialogfeld „Konfiguration der Ereigniserfassung“ aus.

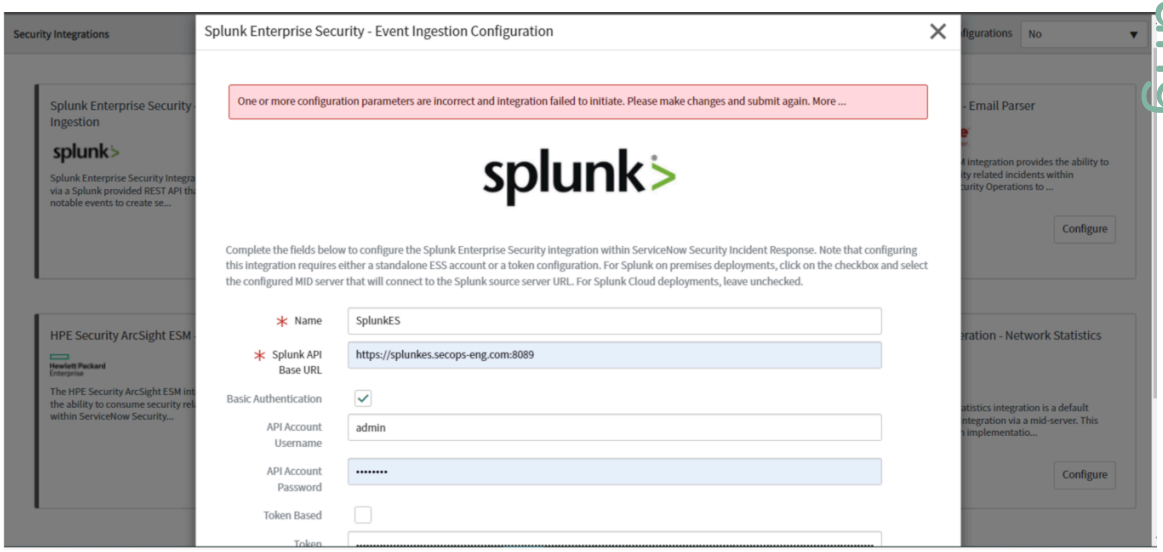
Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für die Konfiguration einer lokalen Version von Splunk Enterprise Security mit einem MID Server.

Jeder Splunk Enterprise Security wichtige Ereignistyp, den Sie über die Incident-Überprüfungskonsole Splunk Enterprise Security erfassen, erfordert ein eindeutiges Ereignisprofil in Ihrer Instanz Now Platform®. Die Quelle, die Sie im Formular „Konfigurationen für Ereigniserfassungen“ konfigurieren, kann jedoch für mehrere Now Platform® Profile wiederverwendet werden, solange jedes Profil eindeutige Typen von wichtigen Ereignissen erfasst.

6. Klicken Sie auf **Absenden**.
Nach erfolgreich abgeschlossener Validierung wird die Seite „Security Integrations“ (Sicherheitsintegrationen) mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel werden die Schaltflächen **Aktualisieren** und **Löschen** angezeigt (siehe folgende Abbildung).

Hinweis:

Benutzer müssen entweder die Standardauthentifizierung oder die tokenbasierte Authentifizierung verwenden. Wenn Sie beide aktivieren, wird der folgende Fehler ausgegeben.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Benutzer es vorziehen, die vorhandenen Konfigurationskacheln auf tokenbasiert zu aktualisieren, müssen sie Aktivieren Sie diese Einstellung, um vorhandene Splunk Quellkonfigurationen für die Einstellung zur Unterstützung der tokenbasierten Authentifizierung im Modul Splunk Unternehmenseinstellungen zu aktualisieren.

Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration für Ereigniserfassungen Splunk auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, wählen Sie in der oberen rechten Ecke der Seite in der Liste Konfigurationen anzeigen die Option **Ja**aus.

Nächste Maßnahme
Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht im Erstellen eines Ereignisprofils.

Konfigurieren Sie Splunk Enterprise Security-Einstellungen

Verwenden Sie die Einstellungen für Splunk Enterprise Security (ES), um die voreingestellten Konfigurationen und ihre Werte gemäß Ihren Anforderungen zu ändern.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Splunk ES Integration** > **Splunk ES-Einstellungen**.
2. Füllen Sie die Felder im Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunk ES-Einstellungen

Feld	Beschreibung
Erzwingt einen Grenzwert für die Anzahl der wichtigen Ereignisse, die zu einem einzelnen Incident zusammengefasst werden können.	Option zum Erzwingen eines Grenzwerts für die Anzahl Ihrer wichtigen Ereignisse, die Sie zu einem einzelnen Incident zusammenfassen möchten. Standardmäßig ist der Wert auf 100 festgelegt.
Erzwingt einen Grenzwert für die Anzahl von Security Incidents, die innerhalb von 24 Stunden erstellt werden können.	Option zum Erzwingen eines Grenzwerts für die Anzahl von Security Incidents, die innerhalb von 24 Stunden erstellt werden können. Standardmäßig ist der Wert auf 1000 festgelegt.
Erzwingt einen Grenzwert für die Anzahl der Werte, die in jedem von Splunkempfangenen Feld analysiert werden sollen.	Option zum Erzwingen eines Grenzwerts für die Anzahl der Werte, die Sie für jedes von Splunkempfangene Feld analysieren möchten. Standardmäßig ist der Wert auf 1000 festgelegt.
Anzahl der Korrelationsregeln, die aus Splunkabgerufen werden sollen.	Option zum Definieren der Anzahl der Korrelationsregeln, die aus Splunkabgerufen werden sollen. Standardmäßig ist der Wert auf 500 festgelegt.
Der Lebensdauerparameter für den Suchauftrag Splunk in Sekunden.	Option zum Definieren des Parameters „Lebensdauer“ für die Suche Splunk in Sekundenform. Standardmäßig ist der Wert auf 600 festgelegt.
Anzahl der beachtenswerten Typen, die in einer Suche gebündelt werden sollen.	Option zum Definieren der Gesamtzahl der beachtenswerten Typen, die Sie in einer einzigen Suche stapeln möchten. Standardmäßig ist der Wert auf 20 festgelegt.
Anzahl der Tage für die Aufbewahrung der Metadaten des Suchauftrags Splunk in ServiceNow	Mit dieser Option können Sie die Anzahl der Tage definieren, für die die Metadaten des Splunk-Suchauftrags in ServiceNowaufbewahrt werden sollen. Standardmäßig ist der Wert auf 30 festgelegt.
Das Trennzeichen zum Teilen der Werte in Feldzuordnungen.	Option zum Definieren des Trennzeichens zum Teilen der Werte in Feldzuordnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standardmäßig ist der Wert auf (,) festgelegt.
Anzahl der Überlappungsminuten, die beim Abrufen der Ereignisse von Splunk hinzugefügt werden sollen (zur Überwindung der Indizierungsverzögerung von Splunk)	Option zum Definieren der Anzahl der Überlappungsminuten, die beim Abrufen der Ereignisse von Splunk hinzugefügt werden sollen, um die Indizierungsverzögerung von Splunkzu umgehen. Standardmäßig ist der Wert auf 30 festgelegt.
Aktualisierte wichtige Ereignisse abrufen	Option zum Abrufen aktualisierter wichtiger Ereignisse. Standardmäßig ist der Wert auf Nein festgelegt.
Aktivieren Sie diese Einstellung, um vorhandene Splunk -Quellkonfigurationen für die Unterstützung der tokenbasierten Authentifizierung zu aktualisieren. Sie müssen die Integrationskonfiguration mit Tokendetails aktualisieren, nachdem diese Einstellung aktiviert wurde.	Option zum Aktualisieren der vorhandenen Splunk -Quellkonfiguration auf Unterstützung der tokenbasierten Authentifizierung von einer vorhandenen Version. **Hinweis:** Nach dem Upgrade auf die neue Version ist das Tokenfeld nicht mehr verfügbar. Sie müssen diese Einstellung aktivieren, um die tokenbasierte Authentifizierung zu erhalten. Anschließend müssen Sie die Integrationskonfiguration mit den Tokendetails aktualisieren. Standardmäßig ist der Wert auf Nein festgelegt.

3. Klicken Sie auf **Speichern**.

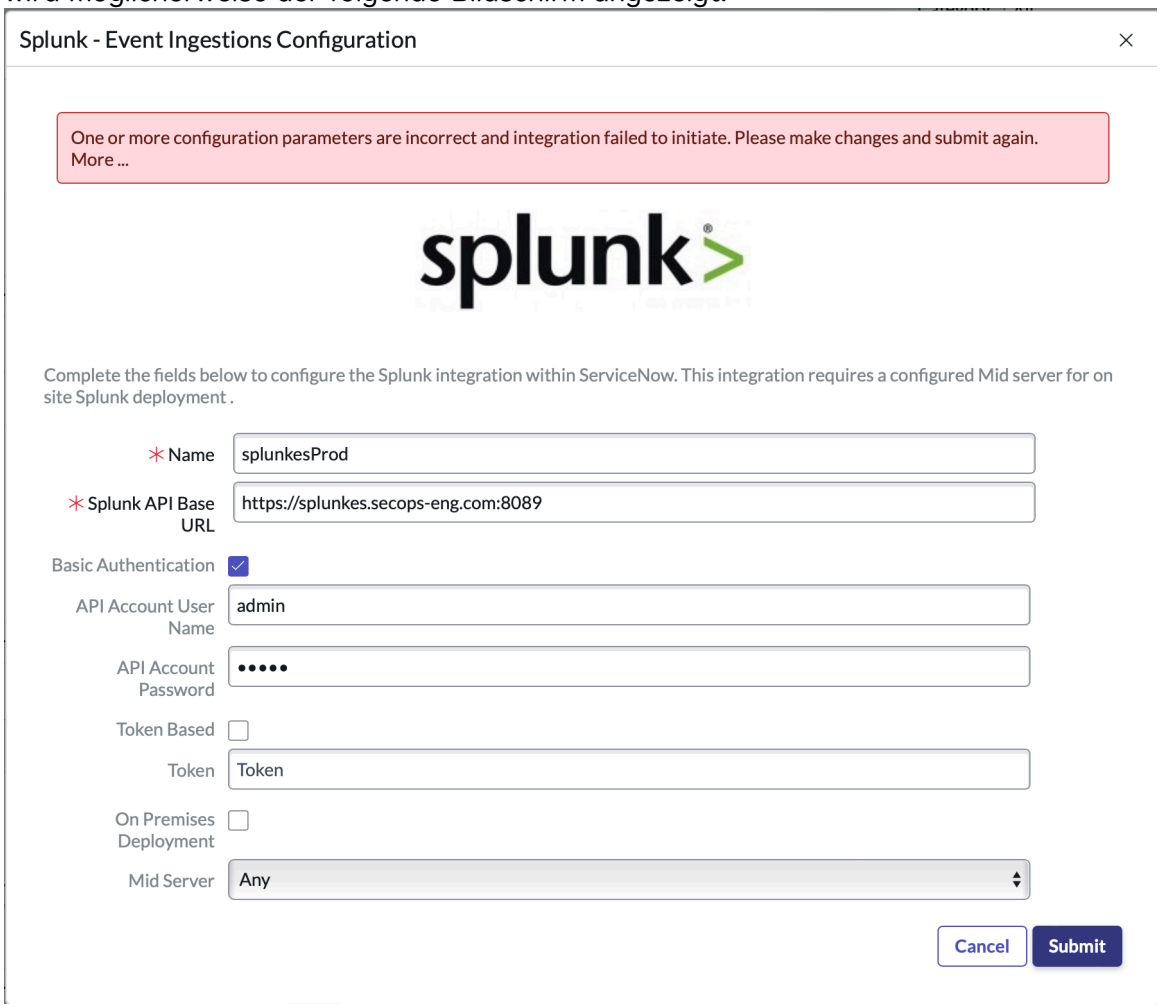
Authentifizierungsfehler

In diesem Abschnitt werden einige häufige Authentifizierungsfehler und ihre Lösung beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem bei der Zertifikatvalidierung

Wenn während der Authentifizierung ein Fehler auftritt, wird möglicherweise der folgende Bildschirm angezeigt:



Wenn Sie verifiziert haben, dass Ihre API-Kontoanmeldeinformationen und die Splunk-Basis-URL korrekt sind, kann dieser Fehler auf ein Problem mit dem Splunk-Zertifikat für die Kommunikation über Port 8089 zurückzuführen sein. Die Instanz ServiceNow® erfordert ein gültiges Zertifikat mit einem allgemeinen Namen, der mit dem Hostnamen des Servers übereinstimmt, um sichere Verbindungen herzustellen. Weitere Informationen finden Sie unter Zertifikate. Wenn dieser Fehler angezeigt wird, können Sie anhand der Systemprotokolle überprüfen, ob das Problem auf ein Zertifikatproblem zurückzuführen ist.

Wahrscheinlich wird eine ähnliche Fehlerbedingung wie die folgende angezeigt:

Um mit der Authentifizierung fortzufahren, müssen Sie das Splunk-Standardzertifikat ersetzen, das für den API-Zugriff an Port 8089 bereitgestellt wird. Ausführliche Anweisungen zum Ersetzen des SSL-Zertifikats finden Sie unter KB0778285.

Erstellen und benennen Sie ein Ereignisprofil für die Splunk Enterprise Security Ereigniserfassungsintegration

Sie erstellen ein Ereignisprofil in Ihrer Instanz Now Platform und bestimmen, welche wichtigen Splunk -Ereignisse Security Incidents erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Bevor -Security Incidents vom Now Platform Security Incident Response Typ (SIR) aus erfassten wichtigen Ereignissen erstellt werden, werden die Feldwerte aus Warnungen in einem Layout eines Now Platform -Security Incidents angezeigt, sodass Sie eine Vorschau auf die Erstellung des tatsächlichen Security Incidents anzeigen können.

Aus der Perspektive der Integration mit den verfügbaren APIs werden Splunk ES wichtige Ereignisse einzeln und manuell als diskrete wichtige Ereignisse weitergeleitet oder je nach definiertem Profiltyp automatisch in der Umgebung Security Operations Ihrer Instanz Now Platform erfasst.

Die Integrations-Workflows erfassen verschiedene Arten von wichtigen Ereignissen, wie z. B. nicht autorisierte Zugriffsversuche und Malware. Diese wichtigen Ereignisse werden basierend auf den Profilen erfasst, die Sie in der Umgebung Security Operations Ihrer -Instanz konfigurieren.

Alle wichtigen Elemente werden anfänglich für einen konfigurierten Korrelationssuchtyp in einem Profil erfasst. Erfasste wichtige Elemente können dann weiter gefiltert werden, um anzugeben, welche wichtigen Elemente Security Incidents erstellen. Beispielsweise können Sie Filter bevorzugen, die Security Incidents nur für wichtige Ereignisse erstellen, die als hoch riskant eingestuft werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten wichtigen Ereignissen erstellt werden, werden einzelne Feldwerte in den wichtigen Ereignissen den entsprechenden Feldern in einem Layout des Security Incident zugeordnet, um eine Vorschau anzuzeigen.

Prozedur
1. Namen für die Ereignisprofile in Ihrer Instanz Now Platform müssen eindeutig sein und können jeweils nur einem aktiven Ereignisprofil zugeordnet werden.
2. Now Platform erfasst bestimmte Notizen mithilfe der Workflows der -Integration.
   Alle wichtigen Ereignisse, die die Auswahlkriterien in Ihrer Splunk ES -Konsole erfüllen, werden zunächst in Ihrer Now Platform -Instanz erfasst.
3. Ein Profil in Ihrem Now Platform ist eine Kapselung eines wichtigen Ereignisses in Ihrer Splunk ES -Konsole.
   Es besteht eine Eins-zu-eins-Beziehung zwischen beachtenswerten Ereignissen, die mit einem Profil und Verbindungen zu Ihrer Splunk ES -Konsole erfasst werden: einem beachtenswerten Ereignistyp für eine Verbindung.
4. Informationen zum Erstellen von Profilen für geplante wichtige Ereignisse finden Sie unter Richten Sie ein Profil für die geplante Erfassung wichtiger Ereignisse ein.
5. Informationen zum Erstellen von Profilen für die manuelle Ereignisweiterleitung finden Sie unter Richten Sie ein Profil für die manuelle Ereignisweiterleitung ein.

Richten Sie ein Profil für die geplante Erfassung wichtiger Ereignisse ein
Je nach definiertem Profil werden Splunk ES wichtige Ereignisse automatisch in die Umgebung Security Operations Ihrer Instanz von Now Platform aufgenommen.

Die folgende Tabelle zeigt die Liste der Aufgaben, die Sie ausführen müssen, um ein Profil für die geplante Erfassung wichtiger Ereignisse einzurichten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritte zum Einrichten eines Profils für die geplante Erfassung wichtiger Ereignisse

Aufgabe	Abschnitt
Erstellen Sie ein Ereignisprofil	Siehe Erstellen Sie Profile für die geplante Erfassung wichtiger Ereignisse
Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationssuche aus	Siehe Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationsregel für das Profil für die Integration der Splunk ES Ereigniserfassung aus
Felder für wichtige Ereignisse zuordnen	Siehe Zuordnung wichtiger Ereignisfelder für die Splunk Enterprise Security -Integration
Erstellen Sie anwenderdefinierte Zuordnungen	Siehe Zuordnungen für Splunk ES – Überprüfung von Incidents für wichtige Ereignisse und Details zu beitragenden Ereignissen (geplante Erfassung) erstellen
Zeigen Sie eine Vorschau des Security Incident an	Siehe Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an
Planen und rufen Sie neue und aktualisierte wichtige Ereignisse ab	Siehe Planen und rufen Sie neue und aktualisierte wichtige Ereignisse für die Splunk Enterprise Security Event Ingestion-Integration ab
Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status	Siehe Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status

Erstellen Sie Profile für die geplante Erfassung wichtiger Ereignisse

Sie können ein Profil einrichten, um wichtige Ereignisse automatisch zu erfassen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Um ein Ereignisprofil für ein wichtiges Ereignis oder einen Korrelationsregeltyp in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wenn das Formular Splunk Ereignisprofil nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Name**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

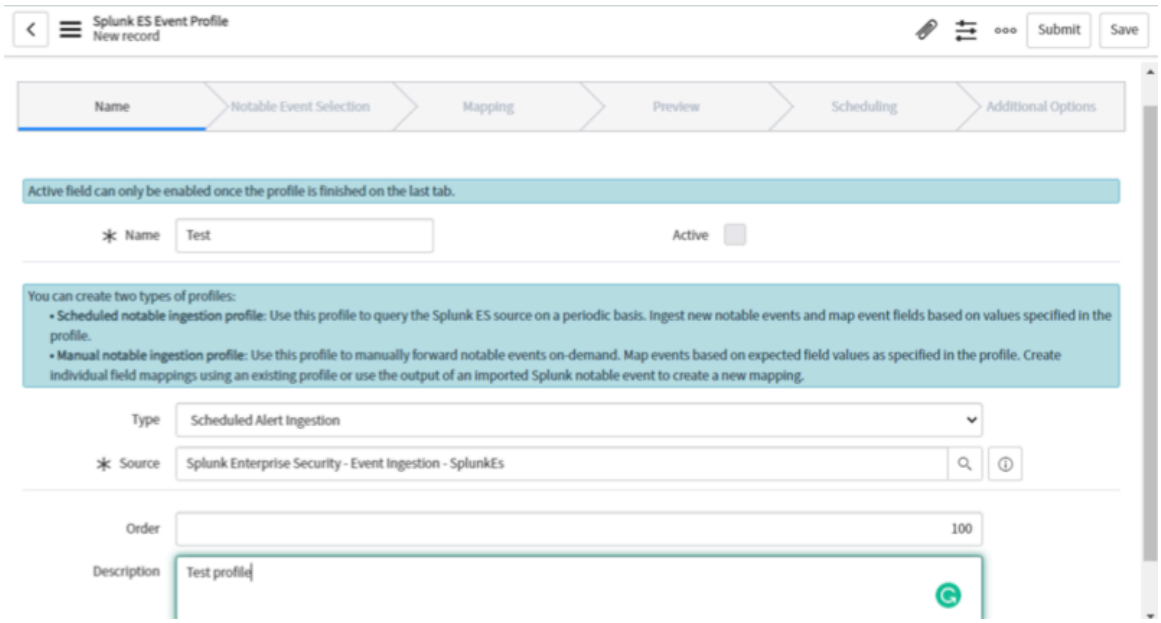
Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn die Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Profilnamen in Ihrer Instanz Now Platform müssen eindeutig sein.
Aktiv	Das Kontrollkästchen ist standardmäßig deaktiviert. Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.
Typ	Wählen Sie den Profiltyp aus der Auswahlliste aus. ○ Geplante Ereigniserfassung: Dieser Profiltyp unterstützt wichtige Ereignisse, die nach einem konfigurierten Zeitplan erfasst werden. Füllen Sie die Felder aus. ○ Manuelle Ereignisweiterleitung: Dieser Profiltyp unterstützt wichtige Ereignisse, die bei Bedarf manuell von Ihrer Splunk Enterprise Security Incident Review-Konsole weitergeleitet werden. Führen Sie die folgenden Schritte aus, um das Formular für diese Profiltypen auszufüllen.
Quelle	Splunk Server oder Suche, die Sie für die Erfassung wichtiger Ereignisse konfiguriert haben. Wenn mehrere Splunk -Server konfiguriert sind, wählen Sie den entsprechenden Server für die wichtigen Ereignistypen aus, die für das Profil erfasst werden. Sie müssen einen Wert eingeben.
Bestellung	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile dieselben Auslösebedingungen verwenden. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität.
(Optional) Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für den Typ eines geplanten wichtigen Ereignis.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie für ein Profil mit einem geplanten wichtigen Ereignis eine Option aus, um mit der Profilkonfiguration fortzufahren.

Nächste Maßnahme

Der nächste Schritt besteht in der Auswahl wichtiger Ereignisse für die automatische Erfassung.

Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationsregel für das Profil für die Integration der Splunk ES Ereigniserfassung aus

Nachdem Sie ein Profil für die geplante Erfassung eines erkennbaren Ereignistyps erstellt haben, wählen Sie den Namen einer Korrelationsregel Splunk Enterprise Security für dieses Profil aus, für das Sie einem Security Incident Now Platform Security Incident Response entsprechende beachtenswerte Ereignisse zuordnen möchten.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Korrelationsregeln in Ihrer Instanz Now Platform an, damit Sie wissen, für welche wichtigen Ereignistypen Sie Security Incidents erfassen und erstellen möchten. Wählen Sie eine Korrelationsregel aus. Sie können ein oder mehrere wichtige Ereignisse aus der Liste in diesem Formular auswählen.

Prozedur

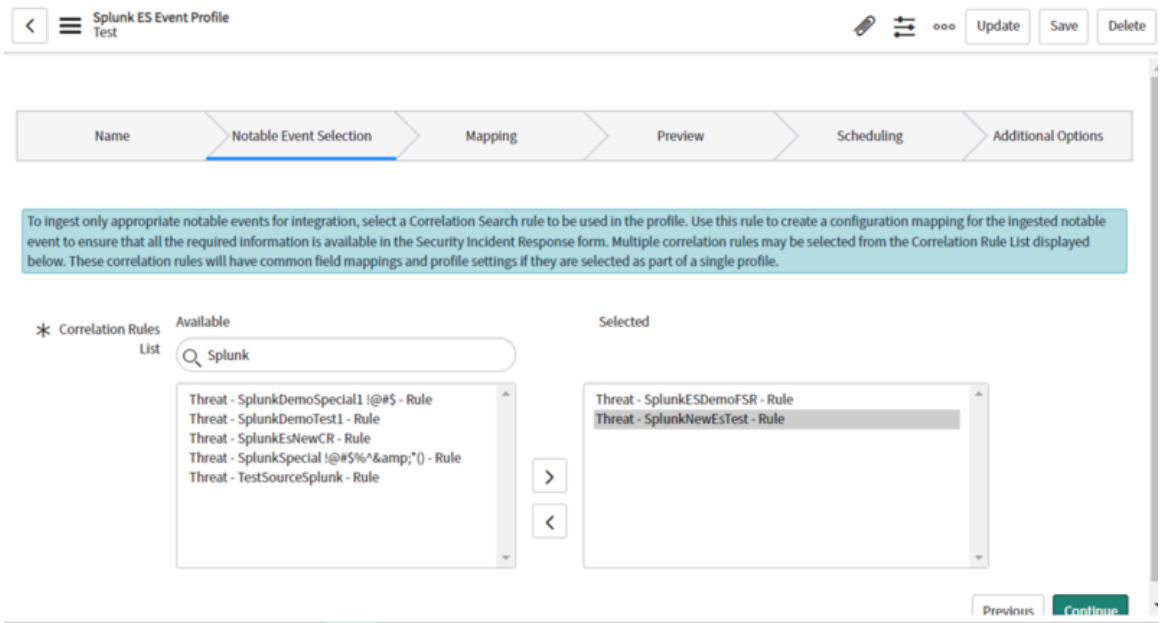
1. Wenn die Seite „Auswahl wichtiger Ereignisse“ nicht angezeigt wird, wählen Sie sie in der Fortschrittsleiste aus, um sie anzuzeigen.
2. Wählen Sie in der Liste der Korrelationsregeln eine der folgenden Optionen aus, um eine einzelne Korrelationsregel oder mehrere Korrelationsregeln auszuwählen und sie zu verschieben und sie aus der Spalte Verfügbar in die Spalte Ausgewählt zu verschieben.

   Die Liste der Korrelationsregeln in diesem Formular entspricht der Liste der Korrelationsregeln in Ihrer Incident-Review-Konsole Splunk ES. Bis zu 500 Korrelationsregeln werden in diesem Formular angezeigt. Wenn in Splunk ESmehr als

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

500 Korrelationsregeln aufgeführt sind, werden in diesem Formular nur die ersten 500 relevanten Ereignisse in Ihrer Instanz Now Platform angezeigt.

Option	Beschreibung
Geben Sie im Suchfeld „Korrelationsregelliste“ Text ein.	Die Spalte unter dem Suchfeld wird anhand der verfügbaren Optionen basierend auf dem von Ihnen eingegebenen Text gefiltert. Wählen Sie eine Korrelationsregel aus, und verschieben Sie den ausgewählten Alarm mit den Pfeiltasten von **Verfügbar** in **Ausgewählt**.
Doppelklicken Sie in der Liste der Korrelationsregeln auf eine Korrelationsregel.	Die Spalte **Ausgewählt** wird mit Ihrer Auswahl gefüllt.
Klicken Sie in der Liste der Korrelationsregeln einmal auf eine Korrelationsregel.	Die Korrelationsregel ist ausgewählt. Verschieben Sie die ausgewählte Korrelationsregel mit den Pfeiltasten von **Verfügbar** in **Ausgewählt**.



3. Wählen Sie eine Option aus, um fortzufahren.

Nächste Maßnahme

Sie haben erfolgreich eine Korrelationsregel für ein geplantes Splunk Enterprise Security Profil ausgewählt. Der nächste Schritt besteht darin, Feldern in einem Security Incident wichtige Ereigniswerte zuzuordnen.

Zuordnung wichtiger Ereignisfelder für die Splunk Enterprise Security -Integration

Nachdem Sie die spezifische Korrelationsregel und den Typ des beachtenswerten Ereignisses für das Profil identifiziert haben, besteht der nächste Schritt in der Zuordnung einzelner Felder für beachtenswerte Ereignisse zu den Feldern in einem Security Incident Now Platform Security Incident Response (SIR).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

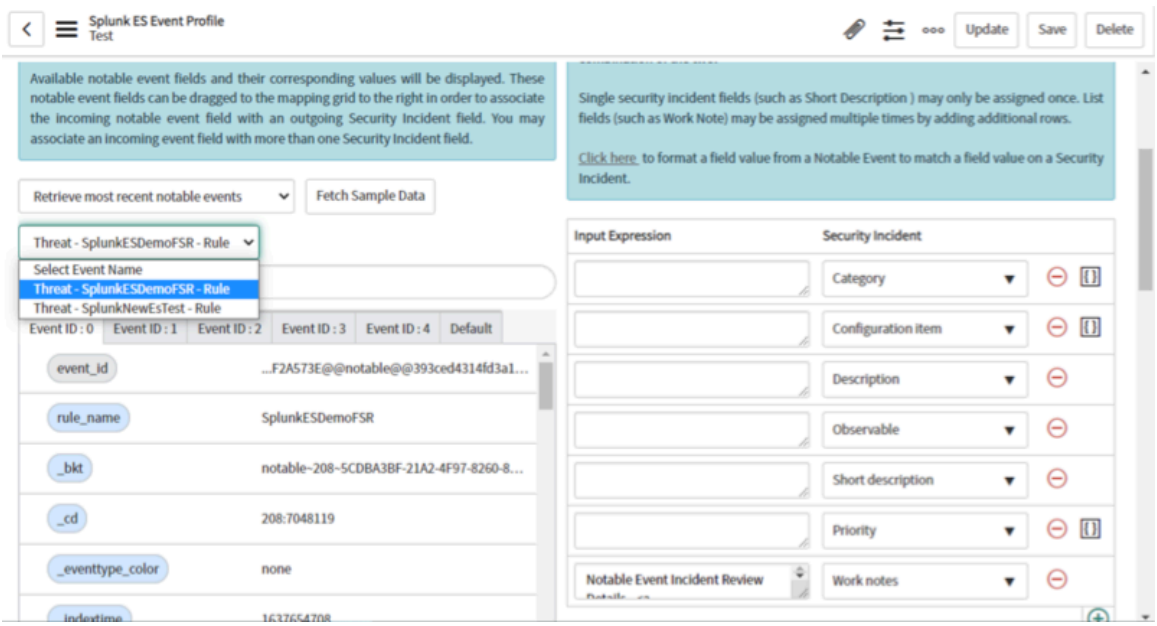
Übersicht

Für den Zuordnungsschritt können Sie wichtige Beispiele für wichtige Ereignisse für die ausgewählte Korrelationsregel erfassen oder Daten zu wichtigen Ereignissen für manuell weitergeleitete wichtige Ereignisse exportieren. Der Ereigniszuordnungsprozess ist unabhängig vom Profiltyp, den Sie erstellen, identisch.

Die folgenden Abbildungen zeigen Beispiele für die standardmäßigen Zuordnungskonfigurationen, die für jeden Typ von Ereignisprofil bereitgestellt werden. Sie können die Felder anpassen, in denen der Security Incident ausgefüllt wird. Während dieser Zuordnungsphase können Sie sicherstellen, dass alle relevanten Felddaten für wichtige Ereignisse der entsprechenden Stelle im SIR-Incident-Formular zugeordnet sind, und anschließend den SIR-Incident im Vorschaubereich visualisieren.

Wenn mehrere Korrelationen verwendet werden, können wichtige Ereignisse durch Auswahl des erforderlichen Ereignisses abgerufen werden. Verwenden Sie **den Warnungsnamen**, um Ihre Warnung auszuwählen, wenn Sie mehrere Warnungen für die Erfassung konfiguriert haben.

Nachdem Sie auf geklickt haben, um Daten abzurufen, werden die Feldnamen des wichtigen Ereignisses Splunk und die entsprechenden Werte auf der linken Seite des Formulars ausgefüllt. Dies sind die Felder für wichtige Ereignisse Splunk, die für die Zuordnung zu den Feldern SIR für Security Incidents verfügbar sind. Einige Felder können den SIR-Security Incident-Feldern mehrmals zugeordnet werden.



Möglicherweise möchten Sie einige wichtige Beispielereignisse in Ihrer Splunk -Konsole überprüfen, um sie für den Konfigurationsschritt der Feldzuordnung zu erfassen. Dieser Schritt wird auf dem Fortschrittsbalken als Zuordnung bezeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**. Sie können bis zu fünf erkennbare Beispielereignisse aus Splunk Enterprise Security erfassen, um den Feldzuordnungsprozess für beachtenswerte Ereignisse zu unterstützen. Es gibt Optionen, um entweder die fünf neuesten beachtenswerten Ereignisse für die ausgewählte Korrelationsregel oder bis zu fünf spezifische beachtenswerte Ereignisse basierend auf den IDs der beachtenswerten Ereignisse zu erfassen.

Nachfolgend finden Sie eine Zusammenfassung der Schritte, die zum Zuordnen wichtiger Ereignisse erforderlich sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erfassung von Beispieldaten für geplante wichtige Ereignisse: Für Beispieldaten, die für automatisch erfasste Profile bedeutender Ereignisse verwendet werden, werden verfügbare Felder für wichtige Ereignisse und ihre entsprechenden Werte in einem Standardzuordnungslayout auf der linken Seite des Zuordnungsformulars angezeigt, sobald die Beispieldaten abgerufen wurden. Registerkarten werden angezeigt, auf denen Sie die Werte für eine bestimmte, von Ihnen abgerufene ID eines beachtenswerten Ereignisses anzeigen können. Stellen Sie sicher, dass alle kritischen Felder aus dem Abschnitt „Beispielerfassung für wichtige Ereignisse“ auf der linken Seite des Formulars den Feldern „Security Incident“ ServiceNow auf der rechten Seite des Formulars zugeordnet sind.
- Feldzuordnung: Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Felder für wichtige Ereignisse aus der linken Seite ziehen und im Abschnitt ServiceNow SIR-Incident-Zuordnung auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das Feld für eingehende beachtenswerte Ereignisse einem Feld für ausgehende Security Incidents zu.
- Zuordnungs-Experience: Passen Sie das Zuordnungsraster an, indem Sie Felder über das Symbol + unten im Abschnitt „SIR-Incident-Feldzuordnung“ hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder anhand der angegebenen Farbcodierung (zugeordnete Felder sind ausgegraut, blaue Felder sind nicht zugeordnet).
- Bedingungen für Incident-Generierung: Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um festzulegen, welche wichtigen Ereignisse Security Incidents erstellen und welche wichtigen Ereignisse herausgefiltert werden sollen, z. B. wichtige Ereignisse mit niedriger Priorität. Dies geschieht im Abschnitt „Bedingungen für Incident-Generierung“, der sich unter dem Abschnitt „Zuordnung wichtiger Ereignisse“ befindet.
- Kriterien für Ereigniszusammenfassung: Definieren Sie zusätzliche Kriterien für Ereigniszusammenfassung, die ein eingehendes wichtiges Ereignis zu einem vorhandenen SIR -Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Daten zu wichtigen Sicherheitsereignissen in einem einzigen Security Incident zusammengefasst werden.
- Formatfeldübersetzung: In bestimmten Fällen werden Ereignisfeldwerte in den wichtigen Splunk Enterprise -Ereignissen möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie ähnliche, aber nicht identische Werte formatieren möchten. Beispielsweise können mit dem Skript-Editor die Kategoriewerte „Malware-Warnung“ und „Virusinfizierung“ unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mithilfe von in eine gemeinsame böswillige Code-Aktivität im Feld „Kategorie“ des Security Incident SIR übersetzt werden Formatfeldübersetzungsfunktion.

Der nächste Schritt besteht darin, wichtige Ereignisse zu erfassen und den Security Incident-Feldern SIR Werte zuzuordnen.

Zuordnungen für Splunk ES – Überprüfung von Incidents für wichtige Ereignisse und Details zu beitragenden Ereignissen (geplante Erfassung) erstellen

Während des Schritts der Zuordnung des Felds „Bemerkbares Ereignis“ ordnen Sie einzelne Ereignisfelder aus beachtenswerten Ereignissen Feldern in einem Now Platform Security Incident Response (SIR)-Security Incident zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Das Zuordnungsraster kann für den beachtenswerten Ereignistyp angepasst werden, der in der Auswahl der Korrelationsregel ausgewählt wurde. Die Farbcodierung der Ereignisfelder hilft Ihnen, die bereits zugeordneten Ereigniswerte nachzuverfolgen, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob wichtige Ereignisinformationen verbleiben.

Ordnen Sie bis zu fünf wichtige Ereignisse aus der Spalte „Beispielerfassung für wichtige Ereignisse“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „Feldzuordnung für SIR-Incident“ auf der rechten Seite zu.

Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie im Zuordnungsraster auf der rechten Seite des Formulars Felder hinzufügen oder entfernen. Es werden Standardfelder angezeigt, die normalerweise als wichtige Felder im Security Incident Response-Formular ausgefüllt werden. Diese Felder können jedoch entfernt und zusätzliche Felder mit den Schaltflächen „+“ und „-“ angezeigt werden. Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie im Zuordnungsraster auf der rechten Seite des Formulars Felder hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie Splunk -Felder zuordnen, die nicht im Standardzuordnungsraster im Security Incident SIR angezeigt werden.

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
2. Klicken Sie bei einem Profil mit einer geplanten Erfassung unter „Beispielerfassung für wichtiges Ereignis “ **auf Beispieldaten abrufen**, um die neuesten erkennbaren Ereignisse aus der Konsole Splunk Enterprise für die ausgewählte Korrelationsregel abzurufen.

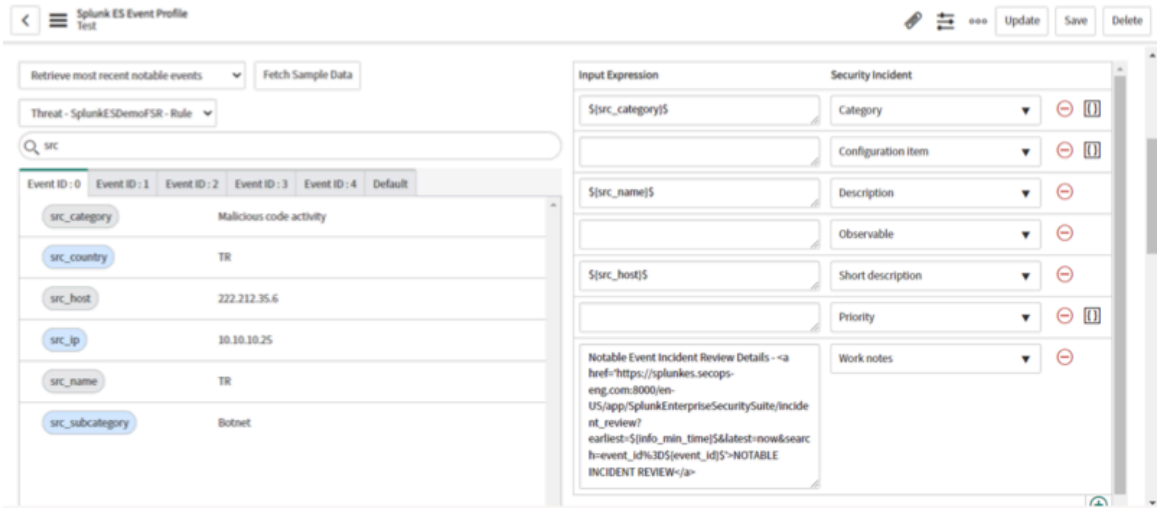
   Hinweis:
   Sie können entweder die neuesten Beispiele für beachtenswerte Ereignisse abrufen oder die eindeutigen beachtenswerten Ereignis-IDs für die spezifischen beachtenswerten Ereignisse angeben, die Sie für die Zuordnung Ihrer beachtenswerten Ereignisse verwenden möchten.

   Die wichtigsten Ereignisfelder und -wertergebnisse werden als einzelne Registerkarten angezeigt. Sie können bis zu fünf wichtige Ereignisse erfassen.

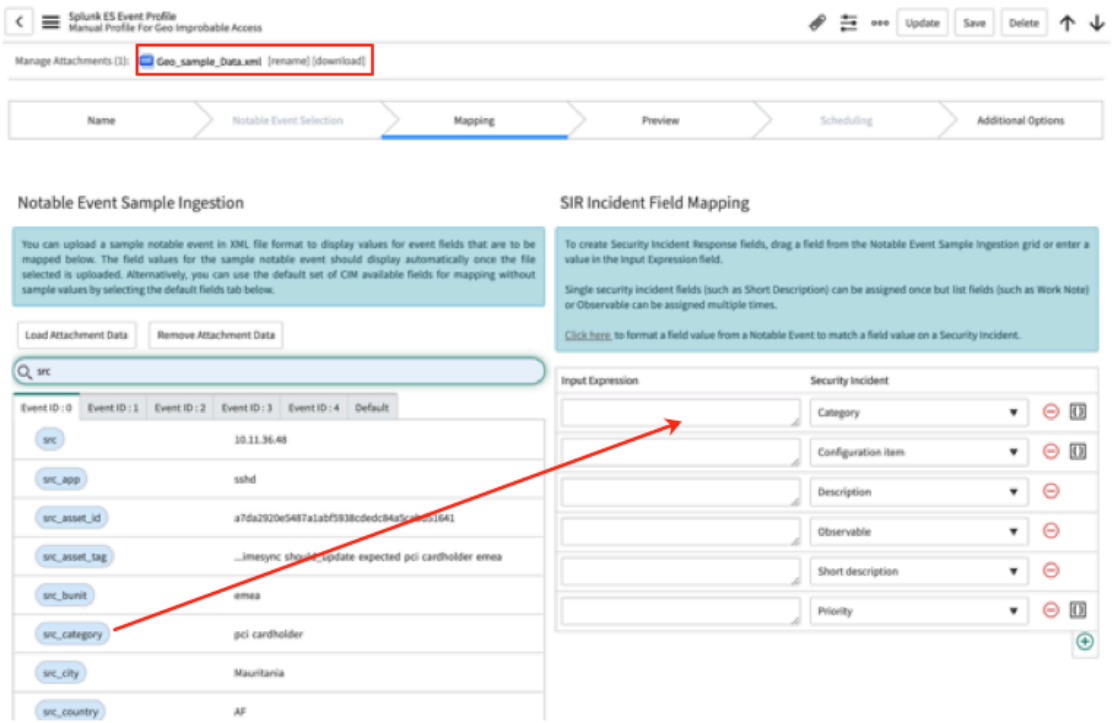
   Das Abrufen von Beispielereignissen für wichtige Ereignisse kann einige Minuten dauern. Oben auf dem Bildschirm wird eine Meldung angezeigt, dass die Transaktion funktioniert.

   In der folgenden Abbildung werden auf der linken Seite dieses Formulars die Feld-Name-Wert-Paare für das erfasste wichtige Ereignis oder die importierten Beispielereignisse angezeigt, nachdem der Erfassungsabruf abgeschlossen wurde. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf einen blauen Feldnamen auf der linken Seite des Formulars.
4. Ziehen Sie den Feldnamen, z. B. src_category, in ein Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“.

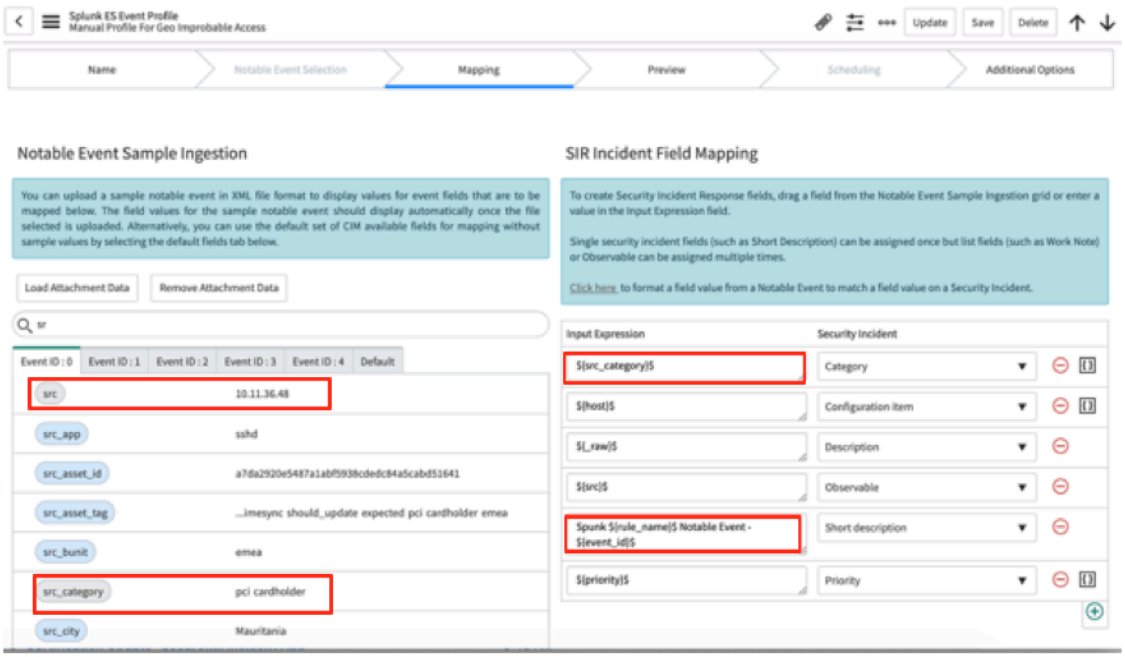


Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird src_category dem Feld „Kategorie“ im Security Incident zugeordnet. Sie können jedoch jeden Wert auf der linken Seite mit einem Feld auf der rechten Seite abgleichen. Vergewissern Sie sich, dass der Wert dem Security Incident während des Vorschauschritts korrekt zugeordnet wurde.

Um sicherzustellen, dass im Zuordnungsprozess keine Ereignisfelder übersehen oder dupliziert werden, sind Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass das Feld für ein wichtiges Ereignis noch nicht ausgewählt und dem Security Incident zugeordnet wurde. Unter Umständen möchten Sie ein eingehendes wichtiges Feld mehreren Feldern in einem Security Incident zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein graus Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.



5. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

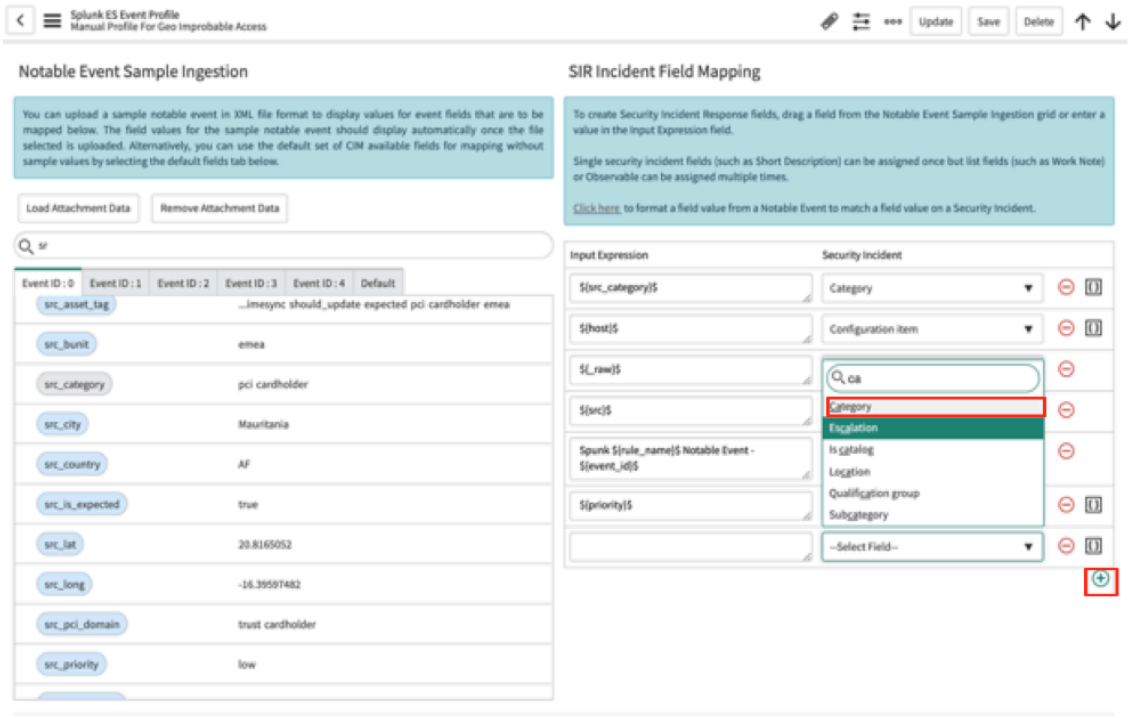
a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol.
Ein neues Feld wird angezeigt.

b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie ein Feld aus.

In der erweiterten Liste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung ist die Kategorie grau hinterlegt, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Felder für wichtige Ereignisse auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Felder für Security Incidents auf der rechten Seite, die bereits zugeordneten Felder für SIR-Incidents nachzuverfolgen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



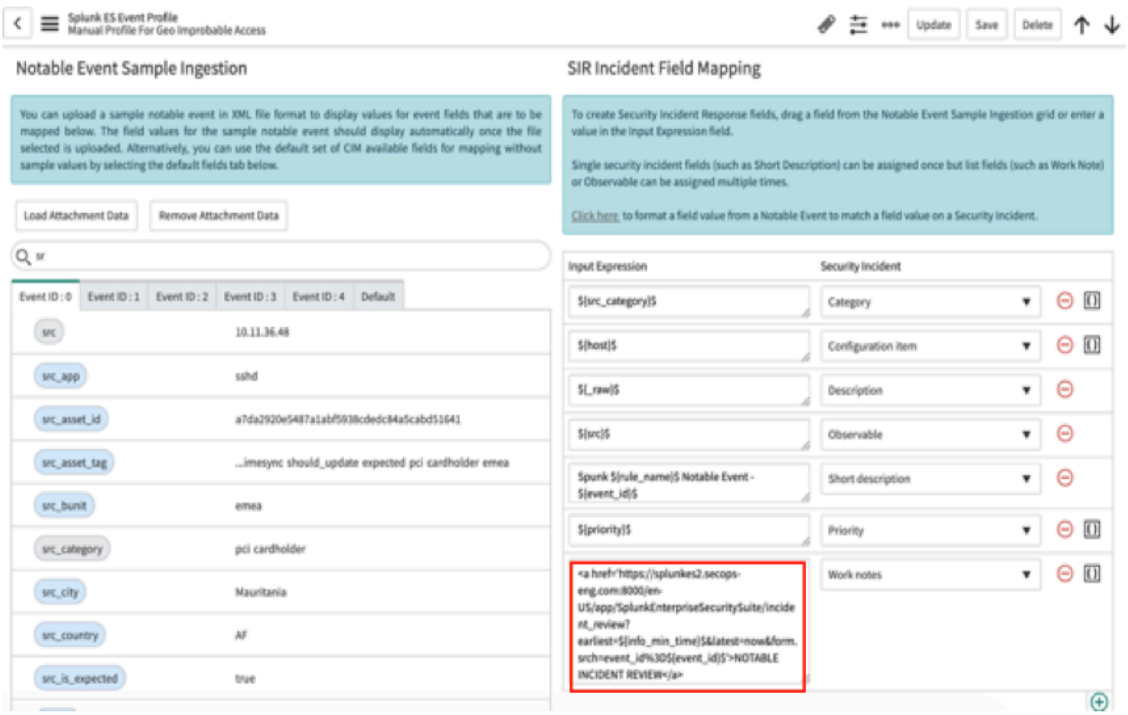
Hinweis:
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident ebenfalls nicht ausgefüllt.

c. Geben Sie alternativ einen Wert in das Feld Suchen für die neue Zeile ein.

d. Klicken Sie auf der linken Seite des Formulars, um die **Ereignis-ID** auszuwählen, die Sie im Feld Eingabeausdruck verwenden möchten.

6. Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.
Die folgende Abbildung zeigt ein Beispiel für eine bearbeitete Zuordnung. Im unteren Feld rechts wird das Feld Arbeitsnotizen hinzugefügt, das mehr als einen Wert hat. Beachten Sie, dass Sie für ein langes Textzeichenfolgenfeld das Zuordnungsfeld erweitern können, um die vollständige Zeichenfolge anzuzeigen und die Größe nach Bedarf zu ändern, indem Sie an der rechten unteren Ecke des Felds ziehen (siehe Screenshot unten mit dem hinzugefügten Feld für Arbeitsnotizen):

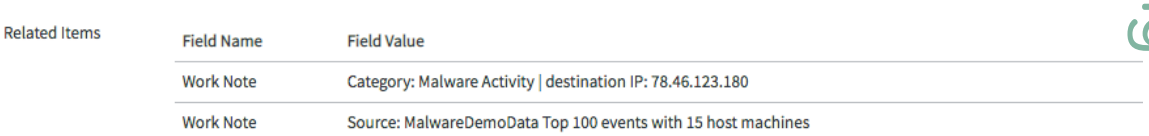
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Warnung:
Beachten Sie, dass die im Abschnitt **„SIR-Incident-Feldzuordnung“** im Feld **„Eingabeausdruck“** angegebene URL und Portnummer nur ein Beispiel ist und nicht die sofort einsatzbereite URL oder Portnummer.

In der Vorschau werden diese Werte in den Arbeitsnotizen zum Security Incident angezeigt. Da der Wert für ein Feld gilt, das Sie dem Zuordnungsabschnitt hinzugefügt haben, und dem Feld Arbeitsnotizen mehrere Werte zugeordnet sind, werden die Werte wie eingegeben angezeigt. In diesem Beispiel werden die von Ihnen in das Feld eingegebenen Leerzeichen und Interpunktionszeichen im Abschnitt „Zugehörige Elemente“ als Arbeitsnotiz in der Vorschau des Security Incident angezeigt.

Die folgende Abbildung zeigt ein Beispiel dafür, wie die Werte in der vorherigen Abbildung für den Security Incident angezeigt werden.



7. **Wahlweise:** Öffnen Sie den Skript-Editor und setzen Sie die Bearbeitung fort.

   (Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor zum Formatieren von Warnungswerten für die Integration Splunk Enterprise Event Ingestion ..

   Einschließlich Hyperlinks zur Überprüfung wichtiger Ereignis-Incidents und beitragender Ereignisse

   Zusätzlich zur Zuordnung von Feldern kann `sn_si.admin` einen Zeichenfolgenwert zuordnen, der es dem Sicherheitsanalysten, der an einem Incident arbeitet, ermöglicht, einen Hyperlink zurück zu Incident-Überprüfung für wichtige Ereignisse in der Konsole

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunk Enterprise Security und zu den zugrunde liegenden beitragenden Ereignissen zu erstellen, die Teil sind der Drilldown-Suche.

Die folgenden Zeichenfolgenwerte enthalten den Servernamen Splunk Enterprise Security und entsprechende Variablen, die für die Hyperlink-Verknüpfung dieser Details verwendet werden können:

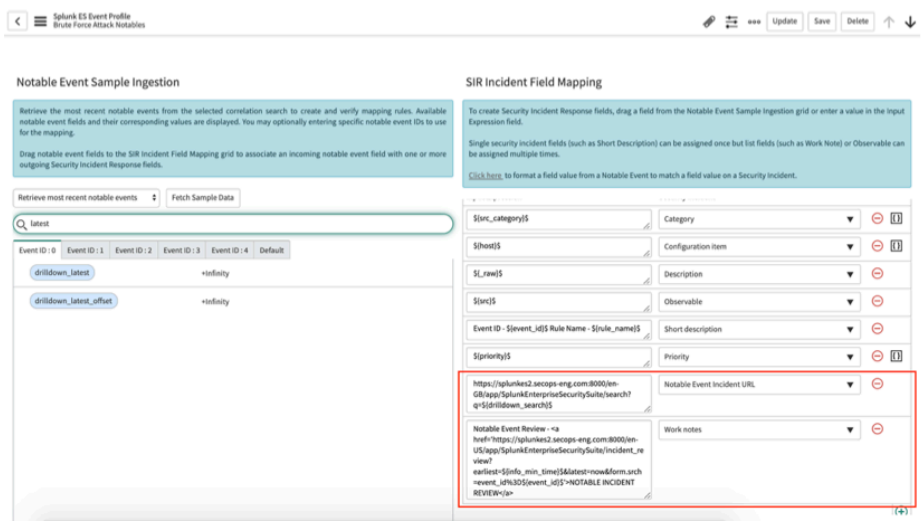
- **Hyperlink zur Überprüfung von Incidents für wichtige Ereignisse**: https://splunkes2.secops-eng.com:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earriest=${info_min_time}$&latest=now&form.srch=event_id%3D${event_id} $

  wobei splunkes2.secops-eng.com:8000 die Splunk-Serverquelle und info_min_time und event_id Ereignisfeldwerte sind, die aus den wichtigen Ereignissen extrahiert wurden.

- **Bemerkbare Ereignisbeiträge (Drilldown-Suche) Hyperlink**: https://splunkes2.secops-eng.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/search?q=${drilldown_search}$

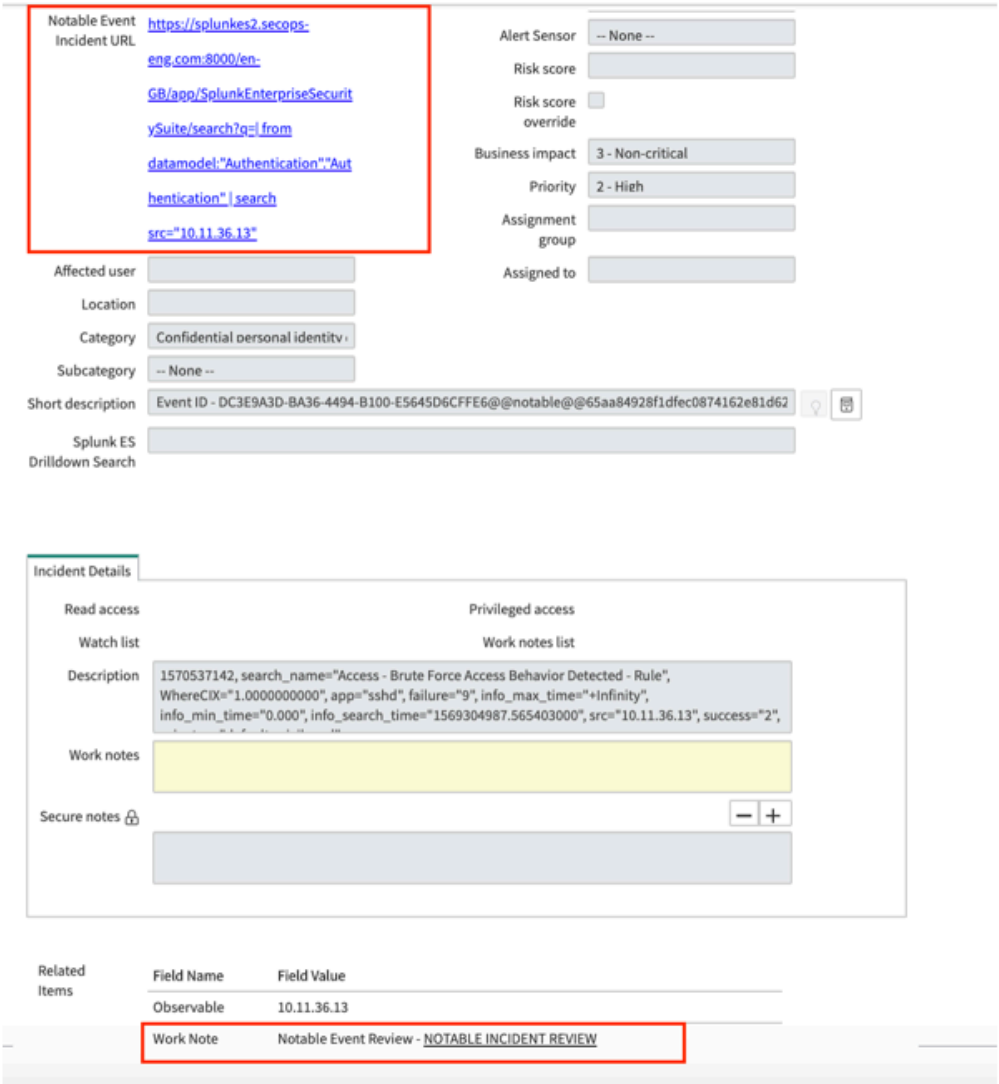
  wobei splunkes2.secops-eng.com:8000 die Splunk-Serverquelle und Drilldown_search der Wert eines Ereignisfelds ist, das aus den beachtenswerten Ereignissen extrahiert wurde.

Die folgende Abbildung zeigt die URL zur Überprüfung von Incidents für wichtige Ereignisse, die dem Feld „Arbeitsnotiz“ zugeordnet sind, und den Hyperlink für beitragende Ereignisse für wichtige Ereignisse (Drilldown-Suche), der einem anwenderdefinierten Feld mit der Bezeichnung „URL für Incidents für wichtige Ereignisse“ zugeordnet ist:



Die folgende Abbildung zeigt die SIR-Incident-Vorschau mit dem Hyperlink zur Überprüfung von Incidents für wichtige Ereignisse und der URL für beitragende Ereignisse:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Filterbedingungen für die Incident-Generierung

8. **Wahlweise:** Nachdem Sie die vorhergehenden Schritte zur Feldzuordnung abgeschlossen haben, können Sie dieselben Feldwerte im Builder für Bedingungen für Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes wichtiges Event erfüllen muss, um einen SIR -Security Incident zu erstellen.
Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

   a. Scrollen Sie im Formular zum Abschnitt „Bedingungen für Incident-Generierung“, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen filtern,** um die Option zu aktivieren.

      (Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

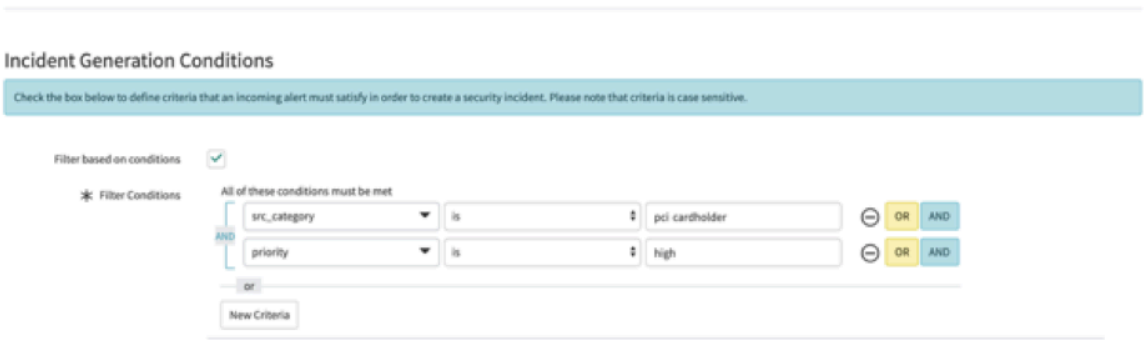
Die Optionen in den Listen für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt „Beispielerfassung für wichtiges Ereignis“ für die von Ihnen erfassten Ereignisse angezeigt werden. Diese Felder sind dynamisch und ändern sich abhängig von den Splunk erkennbaren Ereignissen, die Sie erfassen, oder abhängig von dem Ereignis, das Sie für die manuell weitergeleiteten Beispiele für wichtige Ereignisse auswählen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des wichtigen Ereignisses Splunk Enterprise Security übereinstimmen. Wenn Sie sich bei den Werten, die Sie in die Filterfelder eingeben sollen, nicht sicher sind, kehren Sie möglicherweise zu Ihrer Splunk Enterprise Security -Konsole zurück und überprüfen Ihre wichtigen Ereignisse auf die Stichwörter.

b. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

c. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **AND** oder **OR**. Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.

d. **Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.



(Optional) Sie haben die Bedingungen für die Incident-Generierung so festgelegt, dass Security Incidents nur erstellt werden, wenn die beiden von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Bedingungsfilterung für die Incident-Generierung hilft Ihnen, die Sicherheitsereignisse einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Korrelationssuche oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter in Splunkzu ändern. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur nennenswerte Ereignisse, die allen Kriterien entsprechen, Incidents zugeordnet.

Hinweis:
Wenn einer der Ereignisfeldnamen Sonderzeichen wie Anführungszeichen (“), Bindestriche ('), Unterstriche (-), At-Zeichen (@) oder kaufmännische Und-Zeichen (&) enthält, müssen diese Zeichen möglicherweise zu Zuordnungsübersetzungszwecken und möglicherweise ersetzt werden einen doppelten Ereignisnamen erstellen. Die Zuordnung kann entsprechend erfolgen, es wird jedoch ein numerisches Suffix angehängt, um Felder mit doppelten Ereignisnamen zu unterscheiden. Beispiel: Wenn das erste Ereignisfeld `alerts.alert` und das zweite Ereignisfeld `alerts@alertsist`, können diese Felder nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Ereignisfeld ein Suffix hinzugefügt, und das Feld wird in `alerts@alert(1)`umbenannt.

(Optional) Ereignis-Zusammenfassungskriterien zur Verarbeitung ähnlicher bedeutender Elemente und zur Verhinderung doppelter Incidents

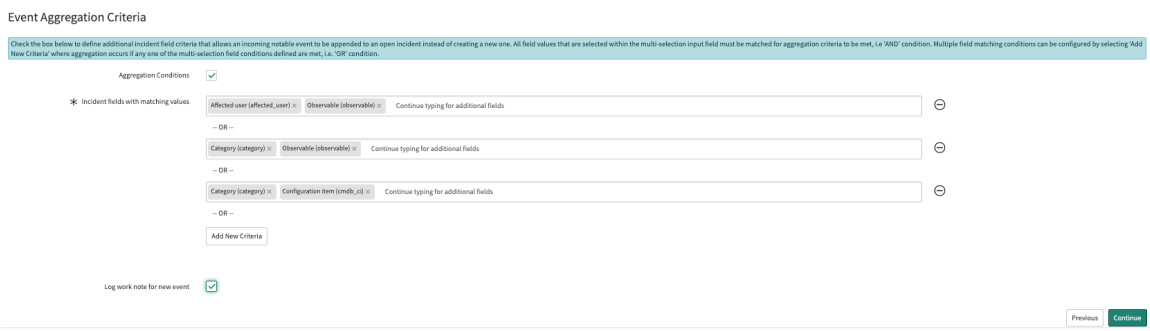
9. **Wahlweise:** Um zu vermeiden, dass doppelte Security Incidents erstellt werden, definieren Sie zusätzliche Kriterien für die Zusammenfassung von Ereignissen, damit eingehende wichtige Ereignisse zu einem offenen Security Incident zusammengefasst werden.
Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen.

   a. Scrollen Sie im Formular zum Abschnitt „Ereignis-Zusammenfassungskriterien“, und aktivieren Sie das Kontrollkästchen **Bedingungen** zusammenfassen, um diese Option zu aktivieren.

   (Optional) Die Incident-Felder mit übereinstimmenden Werten werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die im Security Incident SIR konfiguriert sind.

   b. Wählen Sie im Eingabefeld mit Mehrfachauswahl die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Now Platformabgleichen möchten.

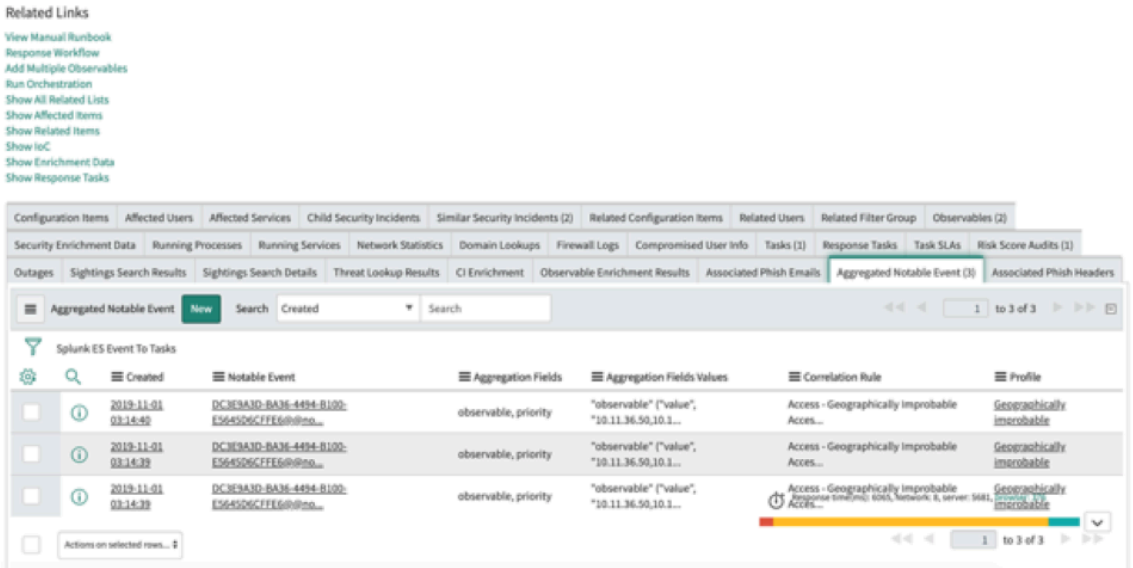
   c. Verwenden Sie **Neues Kriterium hinzufügen,** um mehrere Felder auszuwählen, die den Bedingungen entsprechen.
   Alle Feldwerte, die Sie im Eingabefeld für Mehrfachauswahl auswählen, werden anhand der UND-Bedingung mit Aggregationskriterien abgeglichen. Klicken Sie **auf Neue Kriterien hinzufügen,** um mehrere Feldabgleichsbedingungen auszuwählen, bei denen die Zusammenfassung erfolgt, wenn eine der definierten mehrfach ausgewählten Feldbedingungen mit der ODER-Bedingung erfüllt wird.



Wenn ein neues beachtenswertes Ereignis mit allen Werten übereinstimmt, die in den Bedingungen des Zusammenfassungsfelds im Zuordnungsschritt ausgewählt sind, wird das neue erkennbare Ereignis automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wichtigen Ereignisse in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten wichtigen Ereignisse für einen Security Incident werden in der zugehörigen Liste Splunk Ereignis für Aufgaben angezeigt. Diese Liste enthält Details zu zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese wichtigen Ereignisse zu vorhandenen Security Incidents zusammengefasst werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter „Zugehörige Links“ zur linken Seite des Datensatzes, und klicken Sie auf den Link **Alle zugehörigen Listen anzeigen**.



d. **Wahlweise:** Um eine Arbeitsnotiz für ein neues wichtiges Ereignis zu protokollieren, das dem Security Incident kürzlich hinzugefügt wurde, aktivieren Sie das Kontrollkästchen zur Aktivierung dieser Option. Die Arbeitsnotiz protokolliert, dass ein neuer Notable hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails und allen anderen Details, die dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

Sie haben erfolgreich Werte aus einem wichtigen Ereignis Splunk Feldern in einem Security Incident SIR zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben auch wichtige Ereignisse an vorhandene SIR Security Incidents angehängt, wenn Ereignisfeldwerte den konfigurierten Zusammenfassungskriterien entsprechen.

10. Wählen Sie eine aus, um mit der Profilkonfiguration fortzufahren.

Nächste Maßnahme

Der nächste Schritt besteht in der Vorschau der Werte, die Sie dem Security Incident zugeordnet haben.

Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie im Security Incident Now Platform® Security Incident Response (SIR) zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle wichtigen Felder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

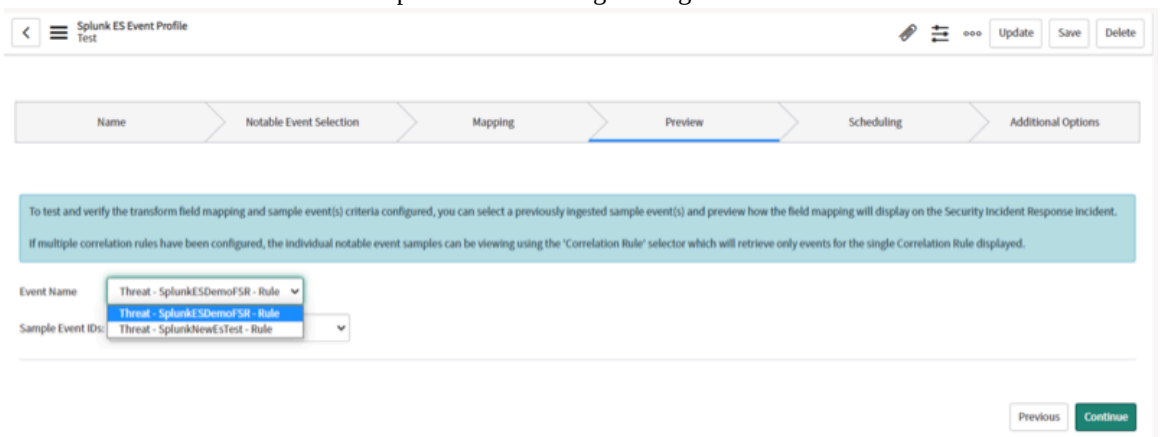
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die Vorschau eines Security Incidents an, und bearbeiten Sie die Zuordnung bei Bedarf erneut, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wird, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen auf Security Incidents SIR werden nicht als tatsächliche Incidents im Produkt SIR gespeichert.

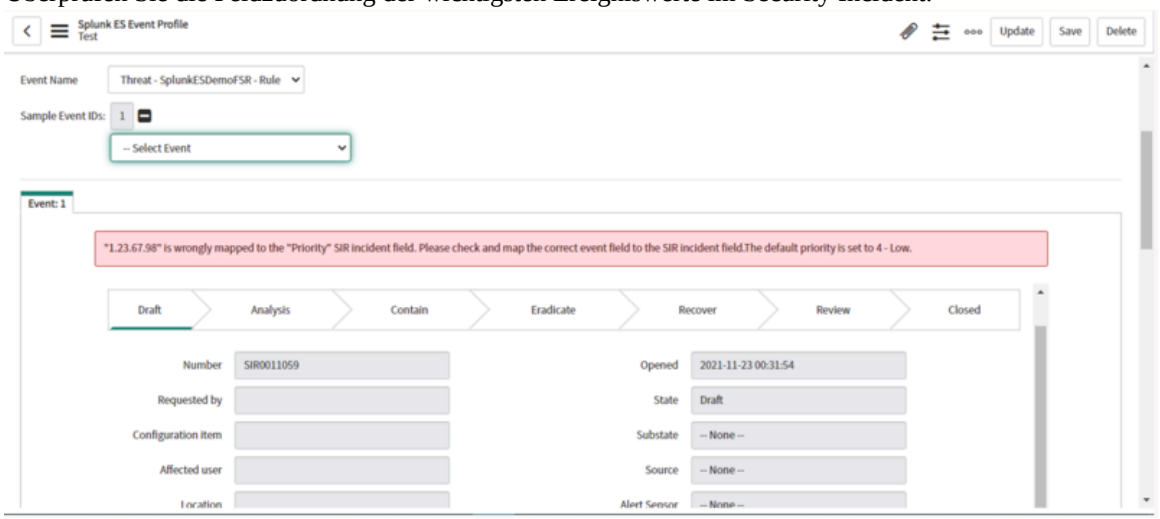
Prozedur

1. Wenn die Vorschau des Security Incidents nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Vorschau**.
2. Wählen Sie in der Auswahlliste Ereignisname ein Element aus, wenn mehrere Ereignisse verwendet wurden.
3. Wählen Sie in der Auswahlliste „Beispiel für IDs wichtiger Ereignisse“ Ereignis-IDs aus.
4. Wählen Sie in der Auswahlliste Beispiel für IDs wichtiger Ereignisse ein Element aus.



Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.

5. Überprüfen Sie die Feldzuordnung der wichtigsten Ereigniswerte im Security Incident.



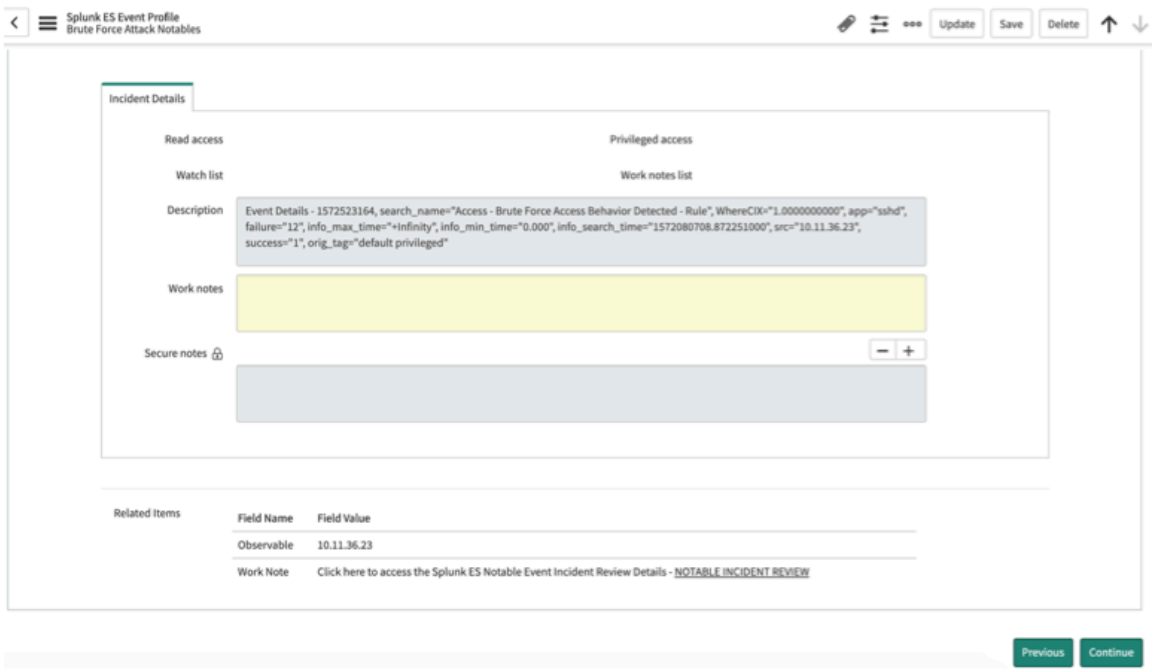
Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel hat ein Feldwert aus dem wichtigen Ereignis keinen akzeptablen Wert für das Referenzfeld im SIR-Incident-Formular. Es wird eine Fehlermeldung angezeigt, die darauf hinweist, dass für das Feld Konfigurationselement in der ServiceNow® Customer Management Database (CMDB) kein Eingabewert gefunden wurde. Daher wird dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugeordnete Feldwert nicht ohne weitere Änderung im Formular „SIR-Security Incident“ angezeigt.

6. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.
7. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
8. Zeigen Sie erneut eine Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in den -Fehlermeldungen beschrieben werden.

   Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Incident-Details in der unteren Hälfte eines SIR -Security Incidents, nachdem alle Fehlermeldungen gelöst wurden. Für dieses Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und diese Felder werden mit den Werten aus den Wertepaaren gefüllt, die aus den Beispielen für wichtige Ereignisse Splunk Enterprise Security abgerufen wurden. Das erste Feld „Arbeitsnotizen“ enthält keinen Wert. Dieses Feld wurde im Zuordnungsraster während des Zuordnungsschritts leer gelassen. Die zusätzlichen Arbeitsnotizfelder, die Werte enthalten, wurden dem Zuordnungsabschnitt hinzugefügt.



9. Nachdem Sie alle Fehler behoben und verifiziert haben, dass die Felder Ihren Vorstellungen entsprechen, wählen Sie eine Option aus, um fortzufahren.

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung im Security Incident zufrieden sind, fahren Sie als Nächstes mit Planen Sie Warnungen für die Integration Splunk Enterprise Event Ingestion, und rufen Sie sie abfort.

Planen und rufen Sie neue und aktualisierte wichtige Ereignisse für die Splunk Enterprise Security Event Ingestion-Integration ab

Bei automatisierten Profilen zur Erfassung wichtiger Ereignisse ist dieser Schritt in der Ereignisprofilkonfiguration erforderlich. Während dieses Schritts können Sie die Standardeinstellungen für den Abruf wichtiger Ereignisse überprüfen oder die Zeitplanung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische beachtenswerte Ereignisse mithilfe eines Datumsbereichs abrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Bei Profilen für die automatisierte Erfassung bedeutender Ereignisse wählen Sie aus, ob Sie historische beachtenswerte Ereignisse während des Schritts „Zeitplanung“ erfassen möchten. Sie können auch auswählen, wie häufig Sie zukünftige neue wichtige Ereignisse und aktualisierte wichtige Ereignisse abfragen möchten, die der Konfiguration des Warnungsprofils entsprechen.

Bei Profilen zur automatisierten Erfassung wichtiger Ereignisse überprüfen und ändern Sie vor der Aktivierung des Profils die Zeitplanung und den Warnungsabruf. Dies ist ein erforderlicher Schritt für den gesamten Konfigurationsprozess für Ereignisprofile für geplante Warnungsprofile.

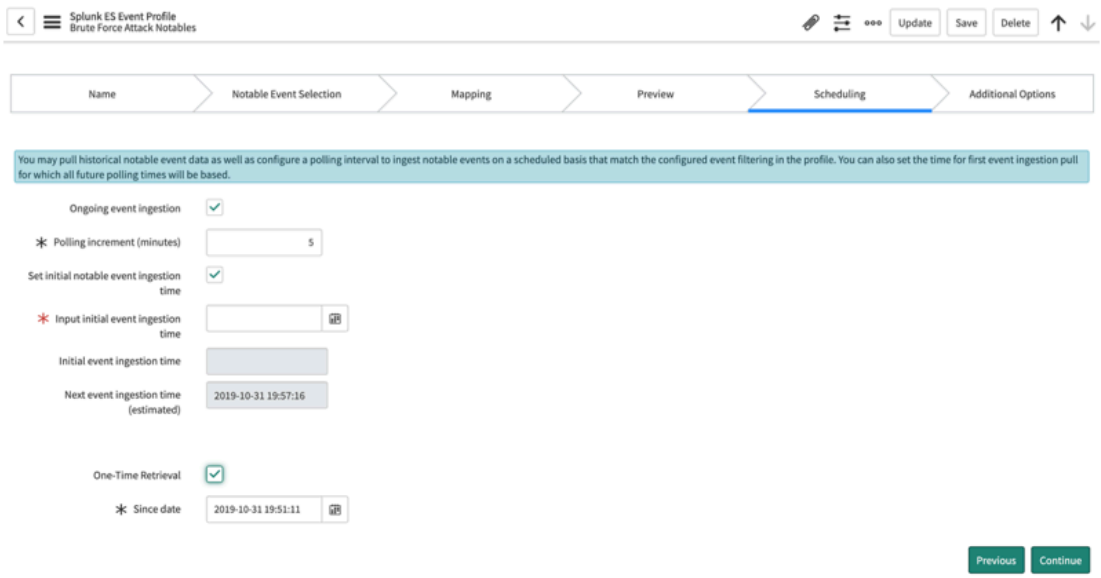
Sie konfigurieren diese Abrufintervalle für einzelne Profile. Die Leistung der Splunk -Ereigniserfassungsintegration kann durch die verschiedenen Abfrageintervalle beeinflusst werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrageaufwands auf dem Server Splunk Enterprise Security mit dem Wunsch in Einklang bringen, so bald wie möglich benachrichtigt zu werden, wenn ein wichtiges Ereignis erstellt oder aktualisiert wird. Für jedes Profil ist ein Standardwert von fünf Minuten festgelegt. Bei Bedarf können Sie diese Einstellung jedoch auch auf einen Wert von nur einer Minute ändern.

Es werden neue und aktualisierte wichtige Ereignisse abgerufen

Wenn der Abfragezeitplan festgelegt ist, ruft die geplante Aufgabe sowohl neue als auch aktualisierte wichtige Ereignisse ab, die zuvor abgerufen wurden, aber die Filterkriterien für Incidents nicht erfüllt haben. Dies gibt Ihnen die Flexibilität, Incidents basierend auf Kriterien zu erstellen, die bei der ersten Erstellung eines wichtigen Ereignisses möglicherweise nicht vorhanden sind, aber nach einem Update verfügbar werden, z. B. während der Untersuchungsphase. Sobald ein Incident für ein bestimmtes wichtiges Ereignis erstellt wurde, werden seine nachfolgenden Aktualisierungen ignoriert, da zu erwarten ist, dass das wichtige Ereignis jetzt als aktiver ServiceNow® Security Incident behandelt wird. Alle anderen beachtenswerten Elemente, die zuvor erfasst wurden, aber die Kriterien für die Incident-Generierung nicht erfüllen, werden weiterhin abgerufen und anhand der Kriterien für die Incident-Generierung überprüft, bis sie Teil eines aktiven Incidents werden.

Prozedur
1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **„Zeitplanung“** aus.
2. Wählen Sie eine aus, um zu planen, wie und wann wichtige Ereignisse aus der Konsole Splunk Enterprise Security abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um ein Beispiel für die Planung der ersten Erfassungszeit eines wichtigen Ereignisse zu geben: Wenn Sie eine tägliche Sicherheitsprüfung Splunk haben, die einmal täglich um 4 Uhr Ortszeit ausgeführt wird, können Sie das entsprechende Profil für ein wichtiges Ereignis in Ihrer Instanz Now Platform so einrichten, dass es um 4 Uhr ausgeführt wird :05 Uhr Ortszeit, um das Sicherheitsfehlerereignis sofort zu erfassen und einen Security Incident zu erstellen. Geben Sie 04 05 00 in das Feld Anfängliche Ereigniserfassung ein. Geben Sie im Feld Inkrement (Minuten) den Wert 1440 (24 Stunden) ein, um die nächste Ereigniserfassung für 24 Stunden ab der ersten Ereigniserfassung zu planen. Sowohl die Zeit der ersten Ereigniserfassung als auch die Zeit der nächsten Ereigniserfassung werden in den Feldern angezeigt.

3. Führen Sie die folgenden Schritte aus, um die Einstellungen für dieses Beispiel zu konfigurieren.

   a. Aktivieren Sie auf der Seite „Zeitplanung“ das Kontrollkästchen **Fortlaufende Ereigniserfassung**, um diese Option zu aktivieren.

   b. Geben Sie im Feld Schritt (Minuten) den Wert 1440 (24 Stunden) ein.

   c. Klicken Sie auf das Kontrollkästchen **Erste Ereigniserfassung auswählen,** um die Bearbeitung der Felder „Erste Ereigniserfassung“ und „Nächste Ereigniserfassung“ zu aktivieren.

   d. Geben Sie im Feld Erste Ereigniserfassung 04 05 00ein.
   Im Feld Nächste Ereigniserfassung (geschätzt) wird die Zeit der nächsten Ereigniserfassung angezeigt.

4. Klicken Sie auf eine der folgenden Optionen, um mit der Profilkonfiguration fortzufahren.

Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status

Security Incidents können erstellt und aktualisiert werden, nachdem sie mit einer bidirektionalen Schnittstelle mit der -Integration Splunk Enterprise Security erstellt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Splunk Enterprise Security -Integration verfügt über eine bidirektionale Schnittstelle, über die wichtige Ereignisse Security Incidents erstellen und wichtige Ereignisse aktualisieren können, nachdem der Security Incident erstellt und/oder geschlossen wurde.

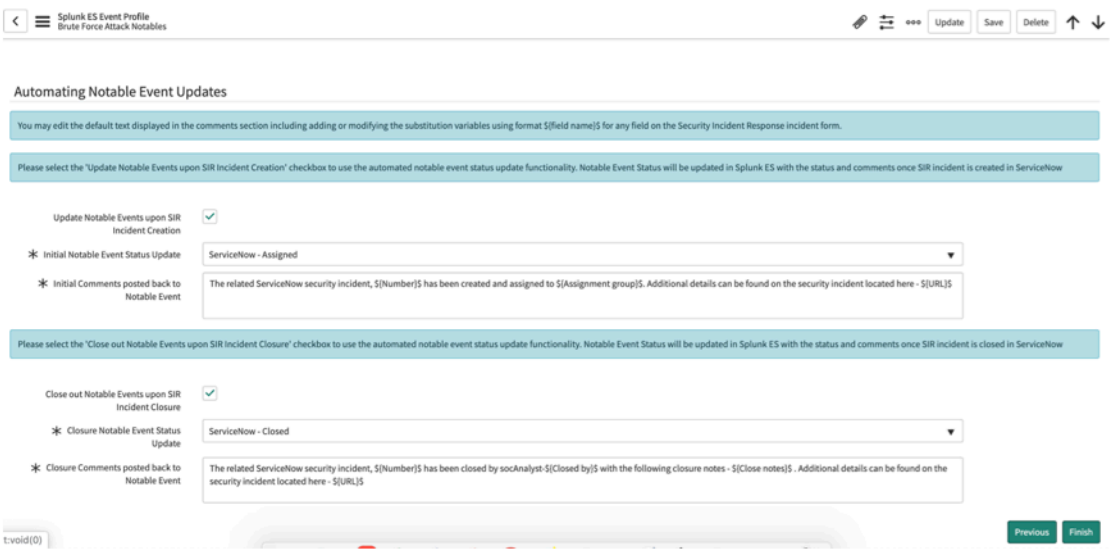
Relevante Incident-Details umfassen SIR Incident-Nummer, Zuweisungsgruppe, SIR Incident-URL. Dieser Abschnitt ist der letzte Teil der Profilkonfigurations-Einrichtung, die optionale Funktionen zum Aktualisieren der wichtigen Splunk Enterprise Security -Ereignisse bereitstellt.

Erforderliche Rolle: sn_si.admin

Prozedur

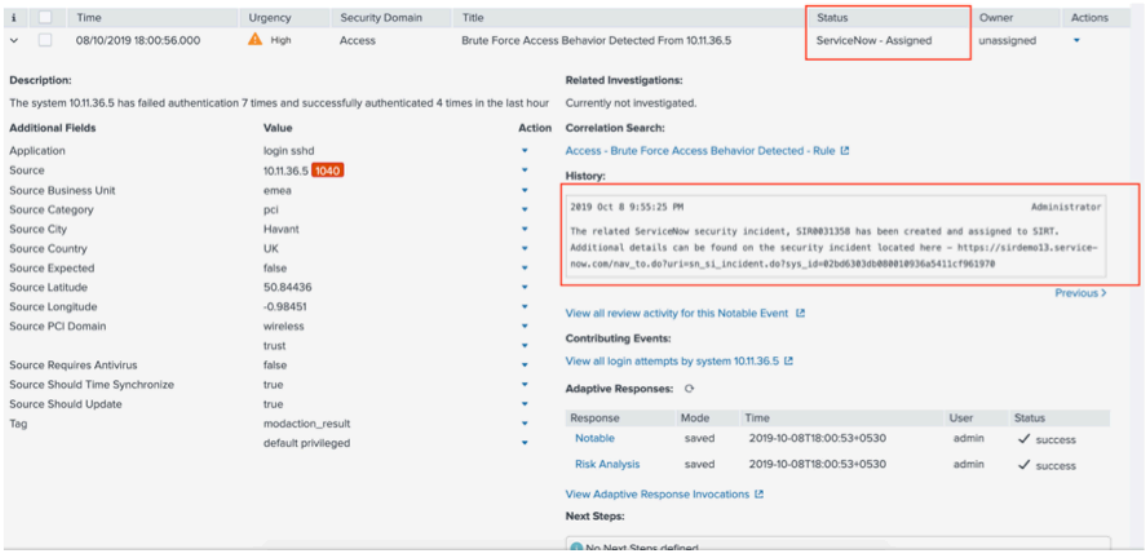
1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration für die Aktualisierung wichtiger Ereignisse auf Grundlage von Updates zu Security Incidents abzuschließen.
3. Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um wichtige Ereignisse basierend auf Ihrer Planung aus der Konsole Splunk Enterprise Security abzurufen. Innerhalb von 24 Stunden können maximal 1.000 Security Incidents erstellt werden. Bis zu 100 wichtige Ereignisse pro ausgelöste Warnung. Nachfolgende wichtige Ereignisse werden ignoriert, nachdem die Grenzwerte erreicht sind.

   Die folgende Abbildung zeigt die Registerkarte Zusätzliche Optionen mit ausgefüllten Standardwerten:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Konfiguration „Zusätzliche Optionen“ aktiviert ist, zeigt die Incident-Überprüfung für ein wichtiges Ereignis die Statusänderung und eine Aktualisierung des Verlaufskommentars an:



Richten Sie ein Profil für die manuelle Ereignisweiterleitung ein

Je nach definiertem Profil werden wichtige Ereignisse Splunk ES manuell als diskrete wichtige Ereignisse in die Umgebung Security Operations Ihrer Instanz von Now Platform weitergeleitet.

So richten Sie ein Profil für die manuelle Weiterleitung wichtiger Ereignisse ein:

Aufgabe	Abschnitt
Erstellen Sie ein Ereignisprofil	Siehe Erstellen Sie Profile für manuell weitergeleitete Ereignisse
Felder für wichtige Ereignisse zuordnen	Siehe Zuordnung wichtiger Ereignisfelder für die Splunk Enterprise Security -Integration
Erstellen Sie anwenderdefinierte Zuordnungen	Siehe Zuordnungen für Splunk ES zur Überprüfung eines wichtigen Ereignis-Incidents und beitragende Ereignisdetails erstellen (manuelle Weiterleitung)
Zeigen Sie eine Vorschau des Security Incident an	Siehe Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an
Richten Sie Ihre Splunk -Umgebung für die manuelle Erfassung ein	Siehe Richten Sie Ihre Umgebung Splunk für die manuelle Ereigniserfassung für die Integration Splunk Enterprise Security „ Notable Event Ingestion ein
Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status	Siehe Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status

Erstellen Sie Profile für manuell weitergeleitete Ereignisse

Sie können ein Profil für manuell weitergeleitete Ereignisse einrichten.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

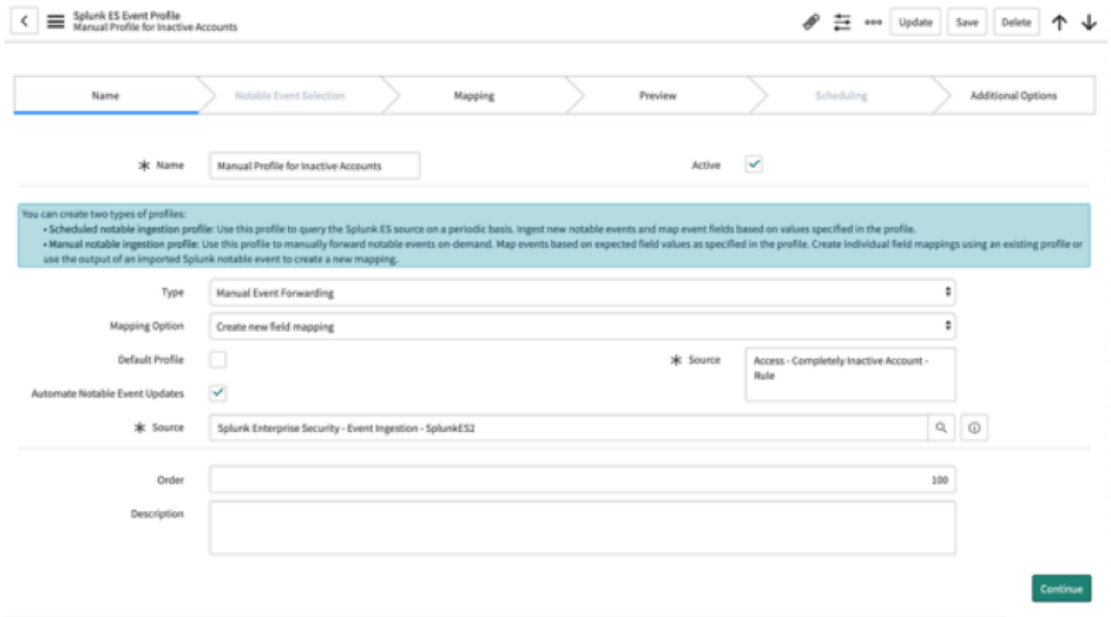
Führen Sie die folgenden Schritte aus, um ein Profil zu erstellen, das die manuelle Ereignisweiterleitung unterstützt.

Für Ereignisse, die Sie bei Bedarf von Ihrer -Konsole Splunk Enterprise Security aus weiterleiten, können Sie die individuelle Feldzuordnung auf einem beliebigen vorhandenen Profil basieren. Alternativ können Sie ein neues Zuordnungsraster für exportierte Anhangsdaten erstellen. Ereignisse, die Sie manuell weiterleiten, sind im Ereignisprofil nicht geplant.

a. Wenn dies noch nicht ausgewählt ist, wählen Sie in der Auswahlliste für das Feld Typ die Option **Manuelle Ereignisweiterleitung**aus.

b. Wählen Sie im angezeigten Feld Zuordnungsoption aus der Auswahlliste eine Zuordnungsoption aus, um fortzufahren.

Weitere Informationen zu den verfügbaren Zuordnungsoptionen in der Auswahlliste Zuordnungsoptionen finden Sie in den folgenden Abbildungen und Tabellen.



Erstellen Sie eine neue Feldzuordnungsoption

Option oder Feld	Beschreibung
Erstellen Sie eine neue Feldzuordnungsoption	Neue Feldzuordnung für Ihr Ereignis. Wenn Sie keine ähnliche Feldzuordnung wie das von Ihnen erstellte Profil haben, wählen Sie diese Option, um eine neue Zuordnung zu erstellen.
Standardprofil	Standardprofil für die Ereignisweiterleitung für alle Splunk -Ereignisse. Standard ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

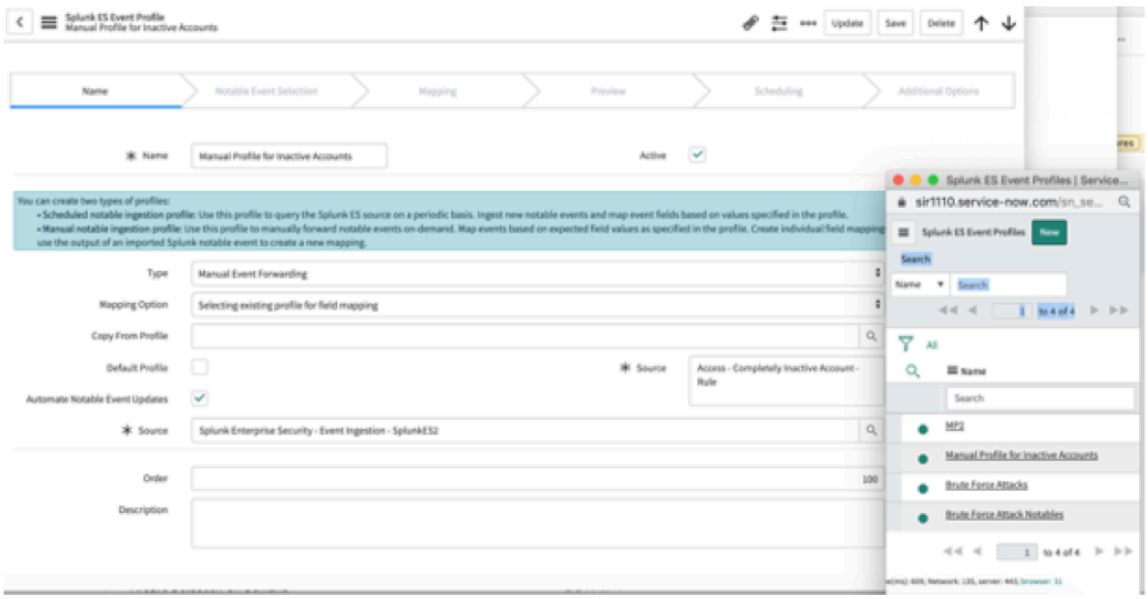
Option oder Feld	Beschreibung
	manuelle Ereignisweiterleitung. Dieses Profil wird verwendet, wenn es keine Übereinstimmung für die Quelle aus dem manuell weitergeleiteten Ereignis gibt. Es wird zum Standardprofil für alle Ereignisse mit unbekannten Quellen. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelle (Feld „Bemerkungswertes Ereignis“)	Dies ist ein Feld, das normalerweise die Korrelationsregel definiert, die die wesentlichen Elemente ausgelöst hat, z. B. Brute-Force-Angriffe. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. Wenn verfügbar, ermöglicht dieses Feld eine eindeutige Zuordnung von Ereignisfeldern zu Security Incident-Feldern basierend auf der Splunk-Korrelationsregel, die normalerweise für verschiedene Ereignistypen unterschiedlich ist. Wenn Sie verschiedene Korrelationsregeln separat verwalten möchten, können Sie basierend auf der Korrelationsregel verschiedene Profilereignisprofile erstellen, um diese Anforderung zu erfüllen.
Automatisieren Sie die Aktualisierung wichtiger Ereignisse	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Status des wichtigen Ereignisses aktualisieren und zusätzliche Kommentare hinzufügen möchten, wenn ein SIR-Incident aus dem wichtigen Ereignis erstellt wird und/oder wenn der SIR-Incident geschlossen wird. Dies gilt sowohl für die ersten auslösenden nennenswerten Ereignisse, die den SIR-Incident erstellen, als auch für aggregierte Ereignisse.
Quelle (Splunk Server)	Der Server Splunk, den Sie als Quelle für wichtige Ereignisse konfiguriert haben. Wenn mehrere Splunk -Server konfiguriert sind, wählen Sie den entsprechenden Server für die wichtigen Ereignistypen aus, die für das Profil aktualisiert werden. Sie müssen einen Wert eingeben.
Bestellung	Der Standardwert ist 100. Belassen Sie diese Einstellung auf dem Standard. Wenn Sie eine große Anzahl von Profilen erstellt haben, gibt dieser Wert eine Laufzeit-Ausführungspriorität an, wenn zwei oder mehr Profile auslösende

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	Bedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität.
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Vergewissern Sie sich bei einem Profil mit einer neuen Feldzuordnung, dass Sie einen Wert in das Feld Quelltyp eingegeben haben, und klicken Sie auf **Fortfahren**, um mit dem Zuordnungsschritt der Konfiguration fortzufahren.

Weitere Informationen zu einem Profil mit einer vorhandenen Feldzuordnung finden Sie in der folgenden Abbildung und Tabelle.



Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

Option oder Feld	Beschreibung
Wählen Sie ein vorhandenes Profil für die Feldzuordnung aus	Verwenden Sie eine vorhandene Feldzuordnung für Ihr neues Profil für wichtige Ereignisse. Das Feld Aus Profil kopieren wird angezeigt. Führen Sie diese Schritte aus, um eine vorhandene Feldzuordnung für dieses Profil zu kopieren. **i.** Klicken Sie links neben dem angezeigten Feld Kopieren aus Profil auf das Suchsymbol. **ii.** Klicken Sie in der angezeigten Liste Splunk ES-Ereignisprofile auf den Profilnamen, der die zu kopierende Zuordnung enthält. Der Profilname wird im Feld Von Profil kopieren angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
Standardprofil	Standard-Ereignisweiterleitungsprofil für alle Splunk wichtigen Ereignisse mit nicht abgeglichener Quelle. Standard ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Ereignisweiterleitung. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelle (Feld „Bemerkungswertes Ereignis“)	Dies ist ein Feld, das normalerweise die Korrelationsregel definiert, die die wesentlichen Elemente ausgelöst hat, z. B. Brute-Force-Angriffe. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. Wenn verfügbar, ermöglicht dieses Feld eine eindeutige Zuordnung von Ereignisfeldern zu Security Incident-Feldern basierend auf der Splunk-Korrelationsregel, die normalerweise für verschiedene Ereignistypen unterschiedlich ist. Wenn Sie verschiedene Korrelationsregeln separat verwalten möchten, können Sie basierend auf der Korrelationsregel verschiedene Profilereignisprofile erstellen, um diese Anforderung zu erfüllen.
Automatisieren Sie wichtige Ereignisse	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Status des wichtigen Ereignisses aktualisieren und zusätzliche Kommentare hinzufügen möchten, wenn aus dem wichtigen Ereignis ein Security Incident erstellt oder wenn der Security Incident geschlossen wird. Dies gilt sowohl für die ersten auslösenden wichtigen Ereignisse, die den Security Incident erstellen, als auch für aggregierte Ereignisse.
Quelle (Splunk Server)	Splunk Server oder Suche, die Sie als Quelle für wichtige Ereignisse konfiguriert haben. Wenn mehrere Splunk -Server konfiguriert sind, wählen Sie den entsprechenden Server für die wichtigen Ereignistypen aus, die für das Profil aktualisiert werden. Sie müssen einen Wert eingeben.
Bestellung	Der Standardwert ist 100. Belassen Sie diese Einstellung auf dem Standard.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	Wenn Sie mehrere Profile erstellt haben, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile auslösende Bedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität.
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Klicken Sie unten im Formular zur Auswahl einer vorhandenen Zuordnung für Ihr Profil **auf Fertigstellen**, um die Profilkonfiguration abzuschließen.

Zuordnungen für Splunk ES zur Überprüfung eines wichtigen Ereignis-Incidents und beitragende Ereignisdetails erstellen (manuelle Weiterleitung)

Während des Schritts der Zuordnung des Felds „Bemerkungswertes Ereignis“ ordnen Sie einzelne Ereignisfelder aus beachtenswerten Ereignissen Feldern in einem Now Platform Security Incident Response (SIR)-Security Incident zu.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Ordnen Sie bis zu fünf wichtige Ereignisse aus der Spalte „Beispielerfassung für wichtige Ereignisse“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „Feldzuordnung für SIR-Incident“ auf der rechten Seite zu.

Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie im Zuordnungsraster auf der rechten Seite des Formulars Felder hinzufügen oder entfernen. Es werden Standardfelder angezeigt, die normalerweise als wichtige Felder im SIR-Incident-Formular ausgefüllt werden müssen. Diese Felder können jedoch entfernt und zusätzliche Felder mit den Schaltflächen „+“ und „-“ angezeigt werden. Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie im Zuordnungsraster auf der rechten Seite des Formulars Felder hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie Splunk -Felder zuordnen, die nicht im Standardzuordnungsraster im Security Incident SIR angezeigt werden.

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
2. Führen Sie diese Schritte aus, um Anhangdaten in Ihre Instanz Now Platform® hochzuladen.

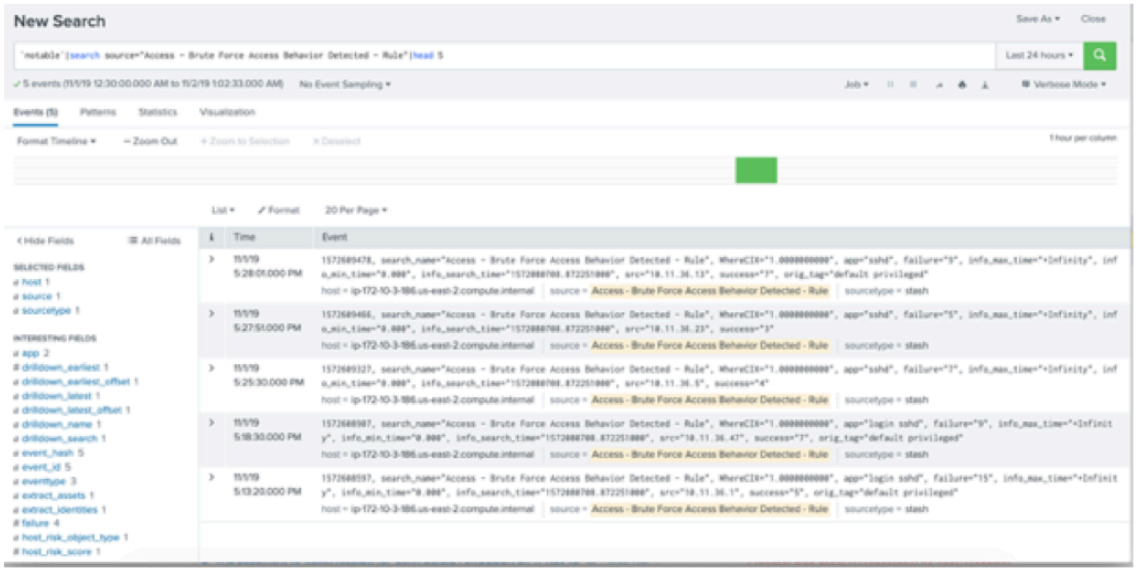
   a. Wenn Sie noch nicht angemeldet sind, melden Sie sich bei Ihrer Splunk Enterprise -Konsole an.

   b. Navigieren Sie zur Registerkarte Suche und geben Sie einen Namen für eine Suche ein, die die wichtigen Ereignisdaten enthält, die Sie exportieren möchten.
   Ein Beispielsuchformat zum Abrufen erkennbarer Ereignisse für die Korrelationsregel für das Brute-Force-Zugriffsverhalten wäre: `notable`|search source="Access - Brute-Force-Zugriffsverhalten erkannt - Regel".

   c. Erweitern Sie das wichtige Ereignis, und wählen Sie in der Spalte Feld die Felder aus, die Sie importieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Felder sind die Feld-Wert-Paare, die exportiert und auf der Seite „Zuordnung“ in Ihrer Instanz Now Platform® angezeigt werden.

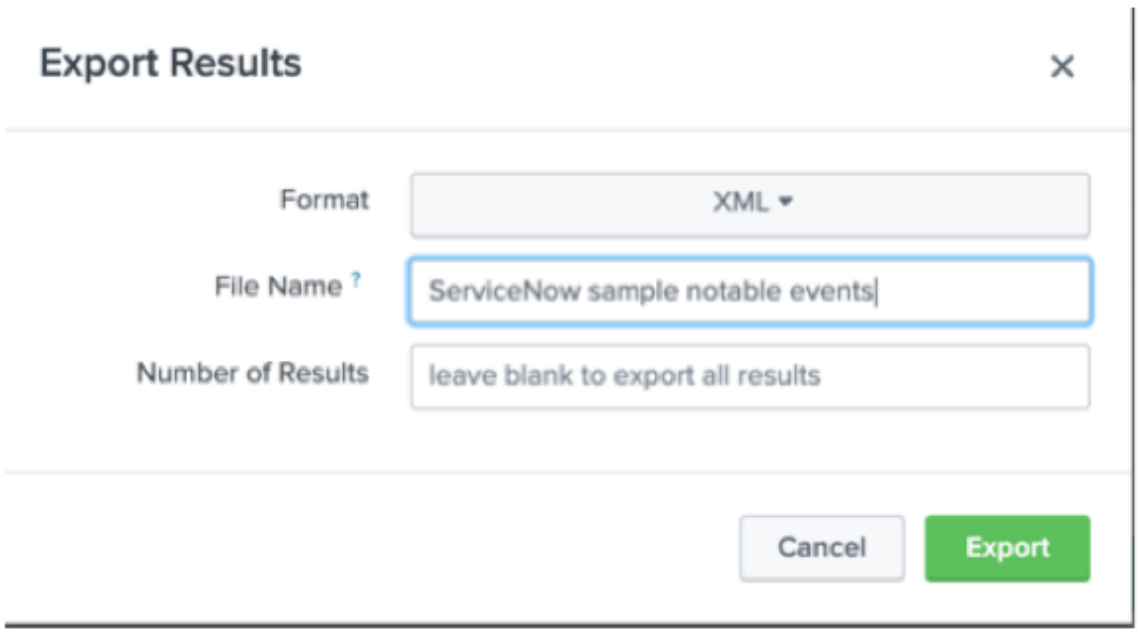


d. Klicken Sie in Ihrer Splunk Enterprise -Konsole oben rechts auf der Suchseite auf das **Exportieren** -Symbol.

e. Klicken Sie in der Auswahlliste für das Feld Format Format im angezeigten Dialogfeld auf **XML-Format**.

f. Wahlweise: Geben Sie einen neuen Dateinamen ein.

g. Klicken Sie auf **Exportieren**.

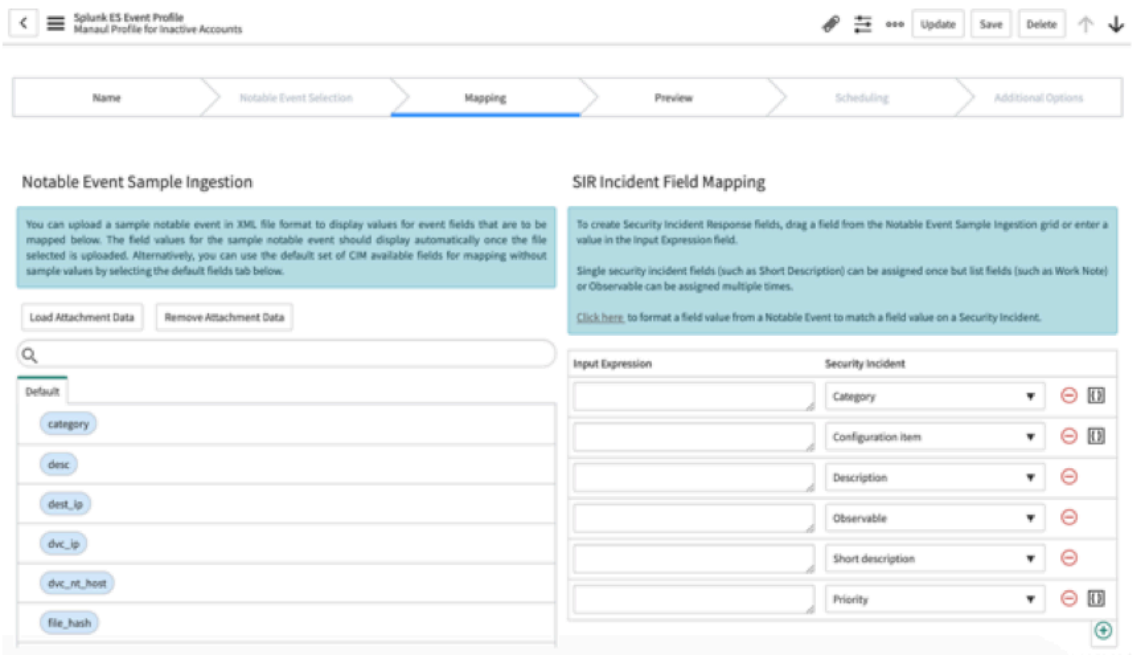


Die exportierte Splunk XML-Datei für das wichtige Ereignis muss jetzt in Ihre Instanz Now Platform® hochgeladen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Wenn die Seite „Zuordnung“ in Ihrer Instanz Now Platform® noch nicht angezeigt wird, klicken Sie in der Fortschrittsleiste **auf Zuordnung**.

i. Klicken Sie in der Spalte „Beispielerfassung für wichtiges Ereignis **“ auf Anhangdaten laden**.



j. Klicken Sie im angezeigten Dialogfeld **auf Dateien auswählen**, navigieren Sie zu der exportierten XML- Datei, und klicken Sie auf **Öffnen**.
Nachdem Sie auf geklickt haben, um Anhangdaten für manuell weitergeleitete Ereignisse zu laden, werden die Felder für wichtige Ereignisse Splunk ES auf der linken Seite des Formulars ausgefüllt. Diese Werte sind die Feldwerte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.
Die Wertepaare für die Felder, die Sie für das Ereignis exportiert haben, werden auf der linken Seite des Zuordnungsformulars angezeigt.

3. Führen Sie die Schritte 5 bis 10 im Abschnitt Zuordnungen für Splunk ES – Überprüfung von Incidents für wichtige Ereignisse und Details zu beitragenden Ereignissen (geplante Erfassung) erstellen aus.

Richten Sie Ihre Umgebung Splunk für die manuelle Ereigniserfassung für die Integration Splunk Enterprise Security „ Notable Event Ingestion ein

Installieren und richten Sie die Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise Security in Ihrer Splunk Enterprise-Konsole oder Splunk-Cloud-Instanz ein, wenn Sie für diese Integration Ereignisse manuell und bei Bedarf von Ihrer Splunk Enterprise Security -Konsole exportieren möchten.

Vorbereitungen

Das Installieren und Einrichten der Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise Security in Ihrer Unternehmenskonsole Splunk oder in der Splunk-Cloud-Instanz ist optional.

Stellen Sie sicher, dass Sie die Anwendung für diese Integration von ServiceNow Store installiert haben, bevor Sie das Add-on-Plugin von splunkbase installieren, das für die manuelle Ereigniserfassung erforderlich ist. Wenn Sie die Anwendung für die -Integration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aus ServiceNow Storenicht installiert haben, rufen Sie Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration Splunk Enterprise Security „ Notable Event Ingestion auf und befolgen Sie die Anweisungen zur Installation.

Erforderliche Rolle: Splunk Enterprise Security Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie Ereignisse für die Integration manuell und bei Bedarf von Ihrer Konsole Splunk Enterprise exportieren möchten, laden Sie das Add-on „Security Operations Event Ingestion“ für ServiceNowSplunk Enterprise Security aus splunkbase in Ihrer Konsole Splunk Enterprise Security herunter, installieren und richten Sie es ein. Dieses Erweiterungs-Add-on ServiceNow ist erforderlich, damit Security Incidents aus manuell exportierten Ereignissen in Ihrer Instanz Now Platform erstellt werden können. Dieses ServiceNow Security Operations Event Ingestion Add-on für die Anwendung Splunk Enterprise Security ist auf splunkbase verfügbar.

Für die manuelle Ereignisweiterleitung können Sie bis zu zwei verschiedene Now Platform -Endpunkte (Instanzen) in Ihrer Splunk Enterprise Security -Konsole identifizieren. Sie leiten die Ereignisse manuell an den Endpunkt oder die Endpunkte weiter, um Security Incidents zu erstellen. Sie können beispielsweise eine Staging-Instanz (Entwicklungsinstanz) und eine Produktionsinstanz angeben. Durch Angabe separater Instanzen und Benennung primärer und sekundärer Workflows für jede Instanz können Sie auswählen, wohin Sie verschiedene Ereignisse weiterleiten möchten.

Prozedur

1. Wenn Sie das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise Securitynoch nicht installiert haben, führen Sie die folgenden Schritte aus, um es zu installieren und zu konfigurieren.

   a. Navigieren Sie zu splunkbase .

   b. Suchen Sie nach dem ServiceNow Security Operations Security Operations Event Ingestion Add-on für Splunk Enterprise Security.

   Hinweis:
   Stellen Sie sicher, dass Sie ServiceNow Security Operations Add-on zur Ereigniserfassung für Splunk Enterprise Securityausgewählt haben. Es gibt zusätzliche ServiceNow Add-ons, die in dieser Liste angezeigt werden. Diese Add-ons gelten für verschiedene ServiceNow Splunk -Integrationen und sind für diese Integration nicht erforderlich.

   c. Laden Sie die Anwendung herunter.

   d. Öffnen Sie Ihr Splunk Enterprise Security -Konto.

   e. Klicken Sie auf der Seite „Apps“ auf das Zahnradsymbol oder auf die Verknüpfung **Apps verwalten** in der Dropdown-Liste des Menüs.

   f. Klicken Sie oben links auf der angezeigten Seite „Apps“ **auf App aus Datei installieren**.

   g. Klicken Sie **auf Datei auswählen**, wählen Sie ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise Securityaus, und klicken Sie auf **Hochladen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Starten Sie Splunk Enterpriseneu, wenn Sie dazu aufgefordert werden.
Das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise Security wird in Ihrer Splunk Enterprise Security -Konsole installiert. Der nächste Schritt zum Einrichten des Add-ons.

2. Führen Sie die folgenden Schritte aus, um das -Add-on einzurichten.

a. Klicken Sie in Splunk Enterprise Securityauf das Zahnradsymbol **Apps**, oder klicken Sie in der Dropdown-Liste des Menüs **auf Apps verwalten**.

b. Klicken Sie in der Liste der Anwendungen, die angezeigt wird, in der Spalte **Aktionen** auf Für ServiceNow Security Operations Add-on zur Ereigniserfassung für Splunk Enterprise Security**einrichten**.

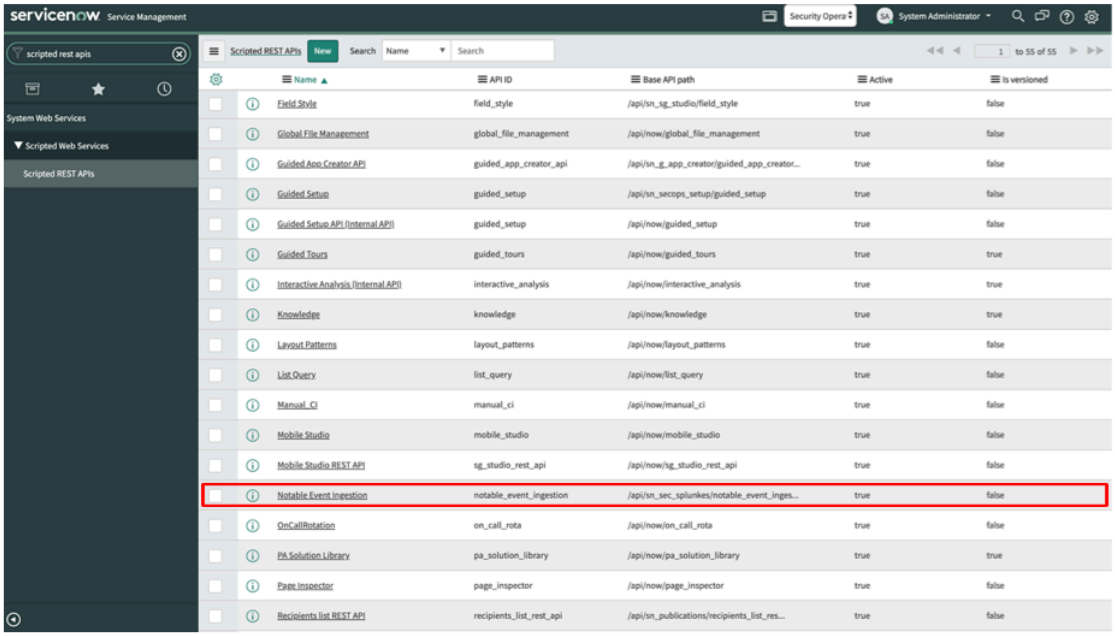
c. Füllen Sie das Formular aus.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes -Formular in Ihrer -Konsole Splunk Enterprise Security.

Die folgende Abbildung zeigt ein Beispiel für die Liste der geskripteten REST APIs in Ihrem Now Platform. In der Liste wird die Position des Endpunktwerts einer Now Platform -Instanz angezeigt, die Sie im Rahmen der Einrichtung des ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise Security in Ihrer Splunk Enterprise Security -Konsole in das Formular eingeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie im Setup-Formular in der Konsole Splunk Enterprise Security auf **Speichern**, um Ihre Änderungen zu speichern.

   Nach einigen Minuten wird oben links im Formular in der Splunk Enterprise Security -Konsole eine Meldung angezeigt, dass der Datensatz erfolgreich aktualisiert wurde.

   Nachdem Sie das Formular gespeichert haben, sind die Namen (Workflow-Aktionsbezeichnungen) für die von Ihnen im Formular erstellten Instanzen Now Platform in der Auswahlliste Ereignisaktionen für ein ausgewähltes Ereignis einer Suche in Ihrer Konsole Splunk Enterprise Security verfügbar.

Nächste Maßnahme

Wenn Sie Suchen noch nicht in der Konsole Splunk Enterprise Security gespeichert haben, besteht der nächste Schritt darin, Suchen als Warnungen in der Konsole Splunk Enterprise Security zu speichern.

Kopieren Sie ein Ereignisprofil für die Integration Splunk Enterprise Security Event Ingestion

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, können Sie Alarmprofile kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

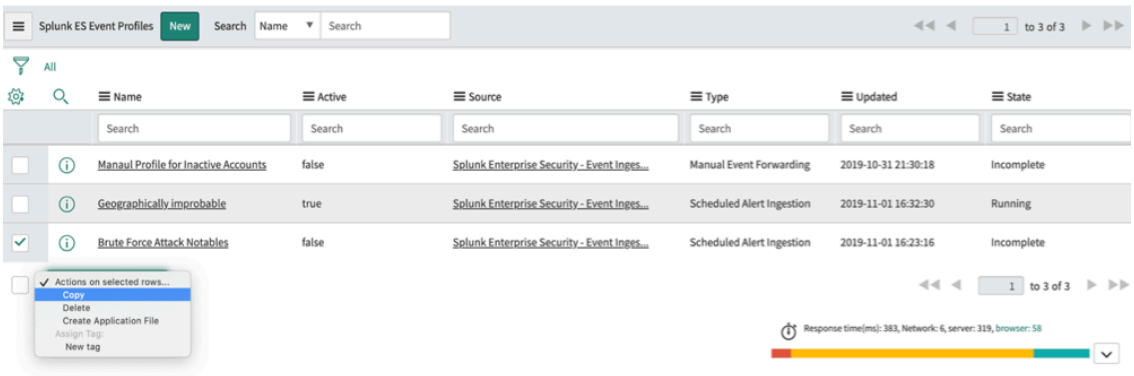
Wenn Sie ein Profil kopieren, wird der Profilname zunächst geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es nicht versehentlich aktiviert wird, bevor die Konfiguration abgeschlossen wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

Automatische Übersetzung

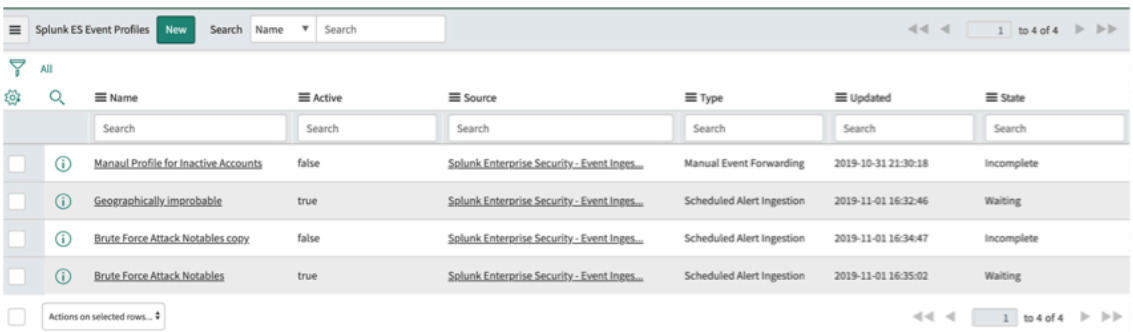
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wählen Sie in der angezeigten Liste Splunk Ereignisprofile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Zeitplankonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie an dieser Stelle deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert.

Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren, nachdem Sie den Konfigurationsschritt abgeschlossen haben.

Verwenden Sie den Skript-Editor zum Formatieren von Warnungswerten für die Splunk Enterprise Security Event Ingestion-Integration

Verwenden Sie zusätzlich zu den direkt zugeordneten Feldern aus den erfassten Werten für wichtige Ereignisse und den Werten, die Sie manuell eingeben, den Skript-Editor, um während des Zuordnungsschritts Feldwerte im Security Incident zu formatieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

In bestimmten Fällen werden Splunk Enterprise Security wichtige Ereigniswerte den Feldern „Kategorie“, „Configuration Item (CI)“ und „Erkennbares Element“ im Incident SIR zugeordnet. Dies wird nicht unterstützt. Möglicherweise möchten Sie die zugeordneten Werte bearbeiten. Wenn Sie den Wert eines wichtigen Ereignisses Splunk Enterprise Security

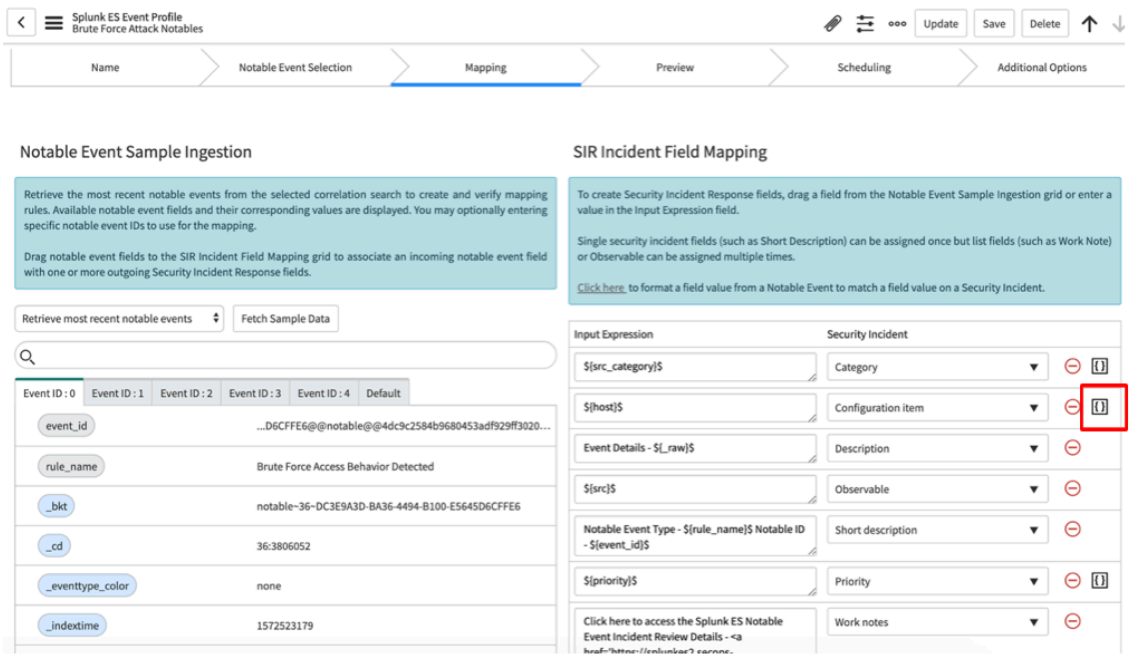
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in einen Wert übersetzen möchten, der von diesen Feldern im Security Incident SIR unterstützt wird, verwenden Sie den Skript-Editor.

Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.



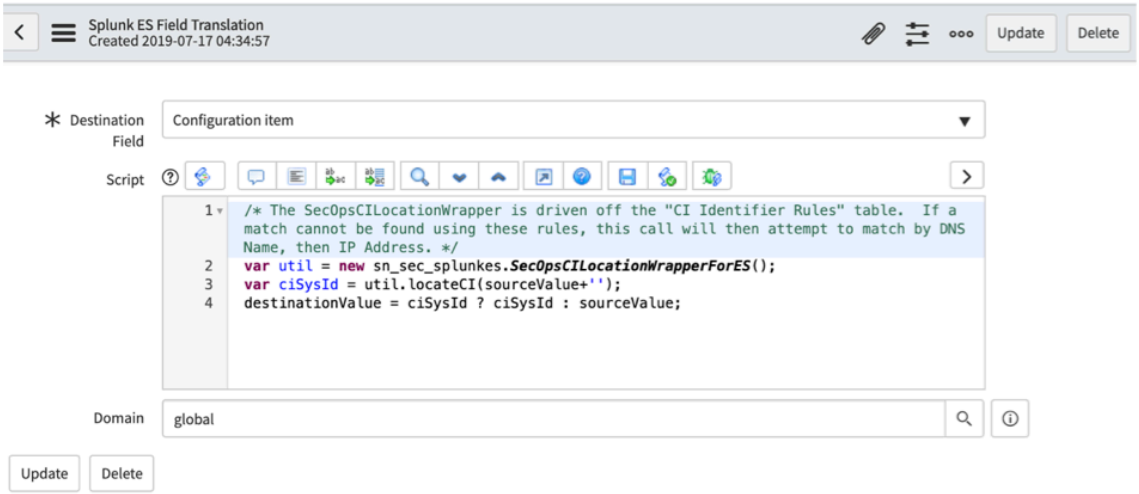
2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt „SIR-Incident-Feldzuordnung“ auf das Klammersymbol [{}] neben einem Feld klicken, um den Skript-Editor für dieses Feld zu öffnen.

   In bestimmten Fällen ist möglicherweise eine Skripteinbindung für das Feld Konfigurationselement geeignet. Bei einem beachtenswerten Ereignis stimmt beispielsweise ein Wert für das Konfigurationselement möglicherweise nicht überein.

   Wie in der folgenden Abbildung gezeigt, können Sie, wenn in der CMDB Now Platform® für das Feld Konfigurationselement keine Übereinstimmung mit einem Hostnamen gefunden wird, die Regel so bearbeiten, dass das Feld Konfigurationselement ausgefüllt wird, sobald eine IP-Adresse gefunden wird. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf NULL gesetzt.

   Der Editor wird mit dem Feld unter Zielfeld geöffnet. Die folgende Abbildung zeigt den Editor mit dem Feld Konfigurationselement als Zielfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
   Die Tabelle „Feldübersetzungen Splunk “ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Kopieren Sie Splunk Enterprise Security Profile mithilfe der Export-/Importfunktion von einer Instanz in eine andere

Sie können Splunk Enterprise Security -Profileinstellungen aus einer Now Platform -Instanz in eine andere Now Platform -Instanz exportieren und importieren.

Vorbereitungen

Zu den Einstellungen, die Sie exportieren und importieren können, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel.

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Funktionalität ermöglicht es dem Sicherheitsadministrator, Profile, die in einer Instanz Now Platform, z. B. außerhalb der Produktion, getestet und verifiziert wurden, in eine andere Now Platform -Instanz, z. B. die Produktion, zu kopieren, ohne alle Konfigurationseinstellungen wiederholen zu müssen. Zu den Einstellungen, die exportiert und importiert werden, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel.

Hinweis:
Wenn Sie einen Profiltyp für die manuelle Ereignisweiterleitung exportieren, werden die für die Beispielfeldzuordnung verwendeten Anhangdaten kopiert. Die Anhangdatei selbst wird jedoch nicht exportiert.

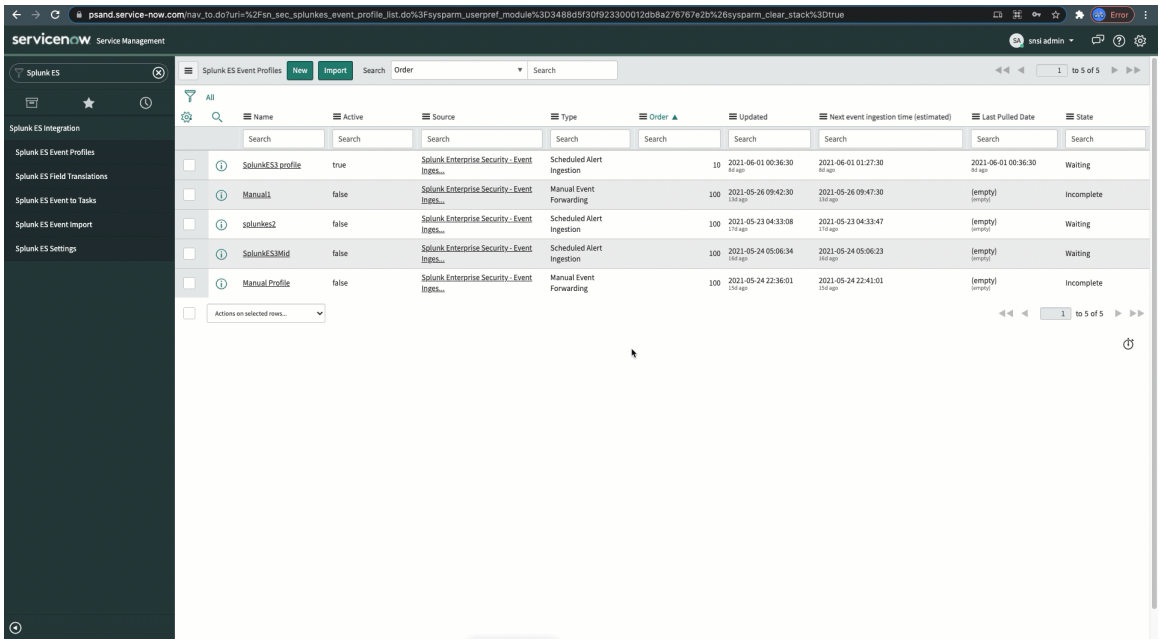
Prozedur

1. Navigieren zu **Alle** > **Splunk ES Integration** > **Splunk ES Ereignisprofile**.
2. Wählen Sie ein Profil aus, das Sie in eine andere Now Platform -Instanz exportieren möchten.
   Sie können mehrere Profile für den Export auswählen.
3. Klicken Sie im Menü Aktionen auf **Exportieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn die Meldung angezeigt wird, dass der Export abgeschlossen ist, klicken Sie auf **Herunterladen**.

   Die folgende Abbildung zeigt den Export eines Profils (SplunkES3profile) aus der Instanz Now Platform (psand.service-now.com).



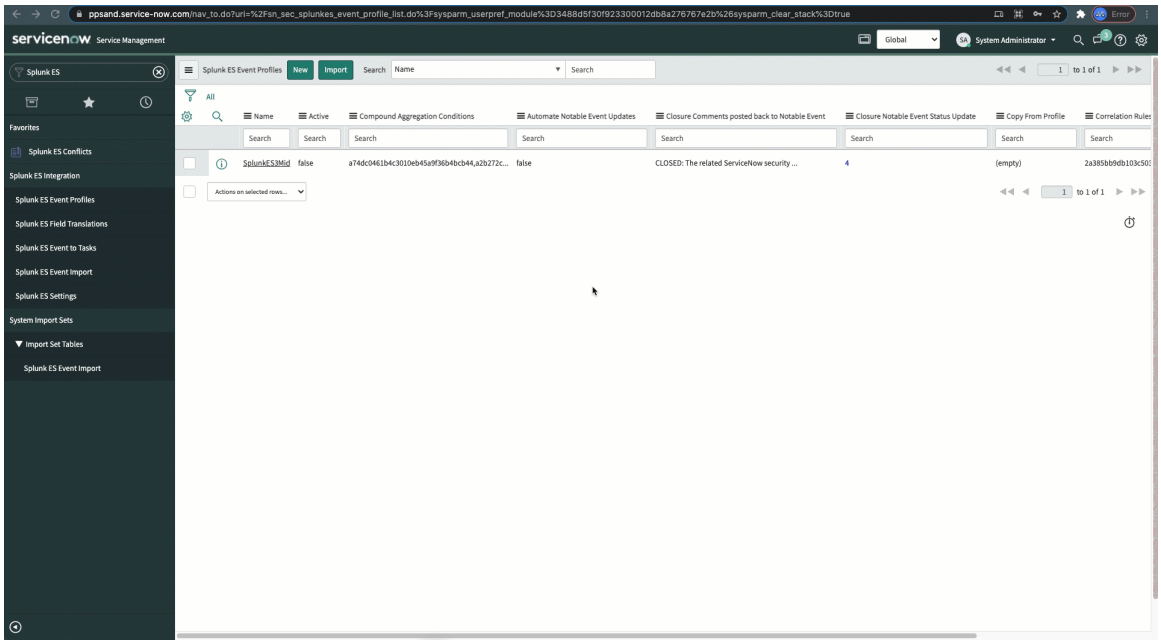
   Die exportierte Datei payload.xml wird auf Ihren Computer heruntergeladen. Die Datei enthält den Profilnamen, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel. Wenn Sie mehrere Profile auswählen und herunterladen, werden sie in derselben Datei „payload.xml“ angezeigt.

   Sie können jetzt das Profil in einer anderen Now Platform -Instanz importieren.

5. Navigieren zu **Splunk ES Integration** > **Splunk ES Ereignisprofile**.
6. Klicken Sie auf **Importieren**.
7. Klicken Sie **auf Datei auswählen**, und wählen Sie die XML-Datei auf Ihrem Computer aus.
8. Klicken Sie auf **Hochladen**.
9. Klicken Sie **auf Profile schließen und neu laden**.

   Die folgende Abbildung zeigt den Import eines Profils (SplunkES3profile) aus der Instanz Now Platform (psand.service-now.com) in die Instanz Now Platform (ppsand.service-now.com).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie haben das Profil erfolgreich aus einer anderen Instanz von Now Platform importiert.

Stellen Sie sicher, dass die exportierte Quelle (API-AccountSplunk und URL des Servers Splunk) und die Konfigurationseinstellungen für den MID-Server gültig und in der importierten Instanz Now Platform verfügbar sind. Aktualisieren Sie bei Bedarf Ihre Splunk Enterprise Security -Konfiguration.

10. **Wahlweise:** Überprüfen Sie die MID-Server-Einstellungen, nachdem Sie ein Profil importiert haben.
11. **Wahlweise:** Navigieren zu **Security Operations** > **Integrationskonfigurationen**.
12. **Wahlweise:** Wählen Sie die Konfigurationskachel Splunk Enterprise Security aus, und klicken Sie auf **Aktualisieren**.
13. **Wahlweise:** Überprüfen und aktualisieren Sie die Details zur Quelle und zum MID-Server nach Bedarf.

Prüfliste für die Splunk Enterprise Security Integration „Notable Event Ingestion“.

Verwenden Sie diese Prüfliste, um sich durch alle Aufgaben der Integration zu führen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle mit den erwarteten Ergebnissen für die Integration.

Vorbereitungen

Erforderliche Rolle: admin, sn_si.admin, sn_si.analyst, Splunk Enterprise Security Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration anhand der folgenden Tabelle. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jede Zeile der Tabelle listet Aufgaben auf und gibt die Rollen an, die zum Ausführen der Aufgaben erforderlich sind. Außerdem wird auf nummerierte Themen im Installations- und Konfigurationsleitfaden verwiesen.

Die für jede Aufgabe erforderlichen Rollen werden mit jedem Schritt in der folgenden Tabelle aufgelistet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren.
2. Befolgen Sie die Schritte in der Tabelle in der Reihenfolge, in der sie angezeigt werden.

Prüfliste

☐	Richten Sie als Benutzer mit der Administratorrolle Now Platform Ihre Instanz Now Platform ein. ○ Weisen Sie nach Bedarf Benutzer mit den Rollen sn_si.admin und sn_si.analyst zu. ○ Installieren und konfigurieren Sie einen MID-Server, wenn der -Server Splunk in Ihrem Unternehmensnetzwerk bereitgestellt wird. ○ Vergewissern Sie sich, dass die Plugins ServiceNow Security Incident Response für Ihr Release von Now Platformaktiviert sind. ○ (Optional) Wenn Sie Ereignisse manuell von Ihrer Splunk Enterprise Security -Konsole an Ihre Now Platform -Instanz weiterleiten möchten, vergewissern Sie sich, dass Sie die Rolle (sn_sec_splunkes.api_account_access) einem Benutzer mit der Administratorberechtigung Splunk Enterprise Security zugewiesen haben. Weitere Informationen finden Sie unter Richten Sie Ihre Instanz Now Platform für die Integration Splunk Enterprise Security ein.
☐	Installieren und konfigurieren Sie als Benutzer mit der Administratorrolle Now Platform die Anwendung Splunk Enterprise Security über ServiceNow Store. **a.** Laden Sie die Anwendung herunter, und installieren Sie sie in Ihrer Instanz Now Platform. **b.** Konfigurieren Sie die Anwendung, und stellen Sie eine Verbindung zu Ihrer Splunk Enterprise Security -Konsole her. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration Splunk Enterprise Security „ Notable Event Ingestion.
☐	(Optional) Wenn Sie Ereignisse manuell von der Konsole Splunk Enterprise Security in die Instanz Now Platform exportieren möchten, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	○ Als Splunk Enterprise Security -Administrator müssen Sie das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise Security über splunkbase in Ihrer Splunk Enterprise Security -Konsole installieren, einrichten und aktivieren. ○ Speichern Sie als Splunk Enterprise Security -Administrator, sofern dies noch nicht konfiguriert ist, Suchen als beachtenswerte Ereignisse in Ihrer Splunk Enterprise Security -Konsole. Weitere Informationen finden Sie unter Richten Sie Ihre Umgebung Splunk für die manuelle Ereigniserfassung für die Integration Splunk Enterprise Security „ Notable Event Ingestion ein.
☐	Als Benutzer mit der Rolle Now Platform sn_si.admin müssen Sie ein Ereignisprofil erstellen und benennen. Wählen Sie den Profiltyp aus der Auswahlliste aus. Optionen sind ein geplantes Warnungsprofil, das Sie zum Erfassen von Beispieldaten verwenden, oder ein Ereignisprofil, das Sie zum manuellen Exportieren von Anhangsdaten aus Ihrer Splunk Enterprise Security -Konsole verwenden. ○ Wählen Sie für eine geplante Warnung eine verfügbare Warnung aus. ○ Erstellen Sie für ein Profil für manuell exportierte Daten eine neue Karte, oder kopieren Sie eine vorhandene Karte. Weitere Informationen finden Sie unter Erstellen und benennen Sie ein Ereignisprofil für die Splunk Enterprise Security Ereigniserfassungsintegration.
☐	Ordnen Sie als Benutzer mit der Rolle Now Platform sn_si.admin erfasste Werte oder Anhangsdaten, die aus Security Incidents Splunk Enterprise Security exportiert werden, nach Now Platform zu. **a.** Rufen Sie Beispieldaten für eine geplante Warnung ab. **b.** (Optional) Exportieren Sie Anhangdaten für ein Ereignis manuell aus Splunk Enterprise Security. **c.** Bearbeiten Sie die Standardzuordnungskonfiguration. **d.** Fügen Sie optional Filterkriterien hinzu, hängen Sie eine Warnung an einen vorhandenen Security Incident an, und verwenden Sie den Skript-Editor. Weitere Informationen finden Sie unter Zuordnung wichtiger Ereignisfelder für die Splunk Enterprise Security -Integration und Zuordnungen für Splunk ES – Überprüfung von Incidents für wichtige Ereignisse und Details zu beitragenden Ereignissen (geplante Erfassung) erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

☐	○ Zeigen Sie als Benutzer mit der Rolle Now Platform sn_si.admin eine Vorschau der Daten von Splunk Enterprise an, die zu einem Security Incident Now Platform angezeigt werden. ○ Beheben Sie Fehler, oder fügen Sie fehlende Daten hinzu, damit keine Fehlermeldungen angezeigt werden. Weitere Informationen finden Sie unter Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an.
☐	Planen Sie als Benutzer mit der Rolle „sn_si.admin“ Now Platform den Warnungsabruf für ein Profil mit einer geplanten Warnung. Weitere Informationen finden Sie unter Planen und rufen Sie neue und aktualisierte wichtige Ereignisse für die Splunk Enterprise Security Event Ingestion-Integration ab.

Sie haben die Einrichtungsschritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration verifiziert.

Integration mit Splunk - Incident Enrichment

Die Integration Splunk – Incident Enrichment durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden	Einrichtung
Integrationen mit Security Incident Response	Erste Schritte mit der Splunk -Suchintegration für Security Operations
Verwenden	**Entwickeln**
• Führen Sie eine Sichtungssuche aus • Security Operations Integration - Sichtungssuche-Flow • Security Operations Integration - Splunk Sightings Search Flow • Zeigen Sie Details der Sichtungssuche an • Sichtungssuchergebnisse anzeigen	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten
Problembehandlung und zusätzliche Informationen	
• Problembehandlung bei Integration • Stellen oder beantworten Sie Fragen in der Security Operations-Community	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der Splunk -Suchintegration für Security Operations

DieSplunk -Software durchsucht, überwacht und analysiert maschinell generierte Big Data und lässt sich problemlos in Security Operationsintegrieren. Bevor Sie die Integration Splunk - Incident Enrichment verwenden können, müssen Sie sie von ServiceNow Store herunterladen und die entsprechende API-Basis-URL sowie Anmeldeinformationen hinzufügen.

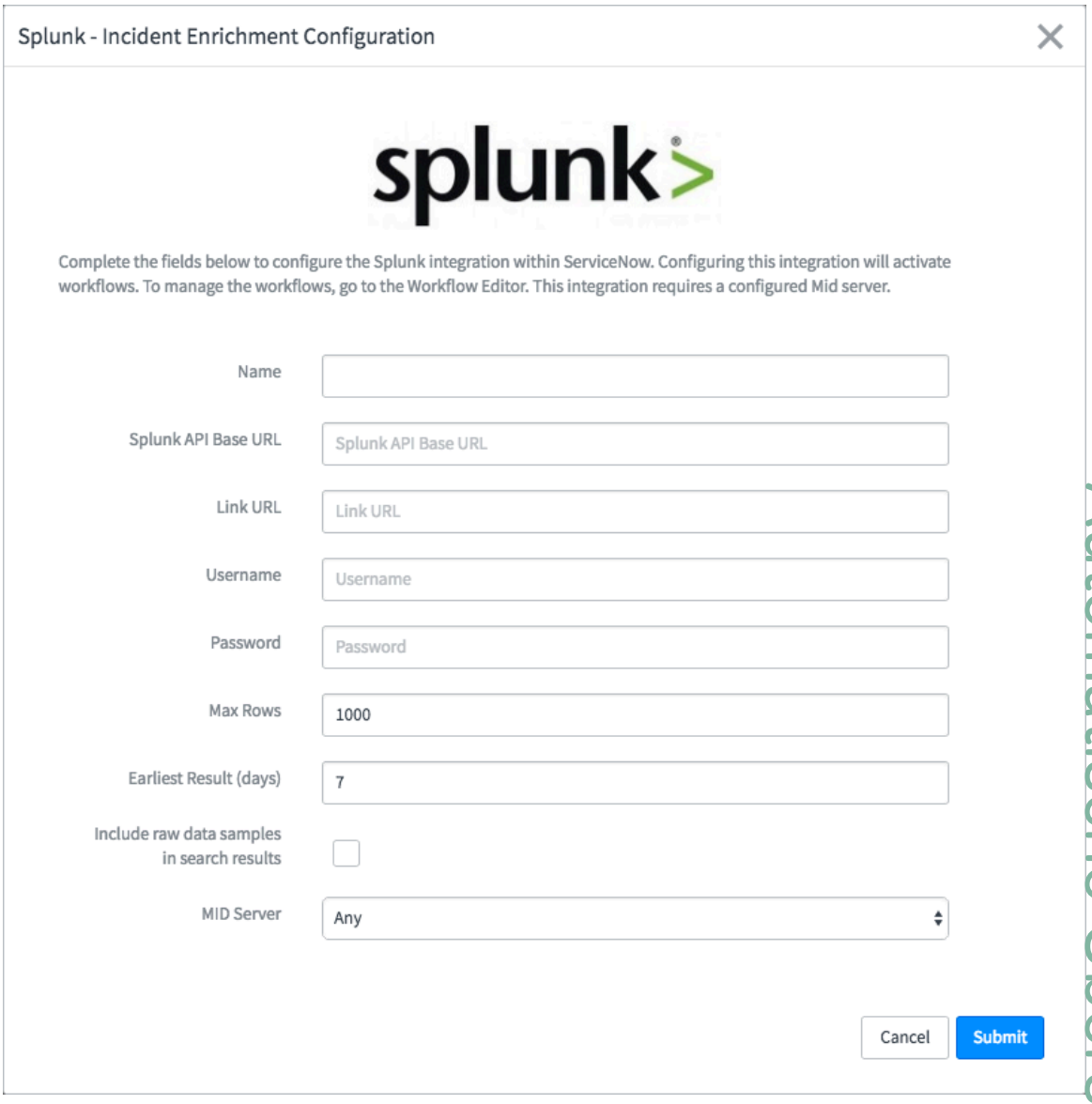
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, greifen Sie in Ihrem Profil auf Splunk zu, und rufen Sie den API-Schlüssel und die API-ID ab.
3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte Splunk – Incident Enrichment auf **New**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der Splunk-API	Die Basis-URL, die Sie von der Website Splunk erhalten haben.
Link-URL	[Optional] Die Link-URL, die auf die Webschnittstelle Splunk verweist, falls verfügbar.
Anwendername	Ihr Splunk-Anwendername.
Passwort	Ihr Splunk-Passwort.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.
Rohdatenmuster in	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchergebnissen berücksichtigen	Einstellung in der **Anzahl der Zeilen der Rohdateneigenschaft** in den Security Incident Response-Eigenschaftenab.
MID-Server	Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern bzw. zu löschen.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie **Nein** in der Dropdown-Liste **Konfigurationen anzeigen aus**.

Mobile Experience für Security Incident Response

Verwenden Sie Ihr Android- oder iOS-Mobilgerät, um Ihre Aufgaben im Security Operations Center (SOC) zu verwalten.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Security Incident Response

Wenn Sie mit den Grundkonzepten des Produkts Security Incident Response (SIR) in Ihrer Instanz Now Platform® von nicht vertraut sind, finden Sie unter Security Incident Response Übersicht weitere Informationen zu Threat Intelligence und dazu, wie dieses Produkt Sie bei der Priorisierung und Lösung von Cyberbedrohungen für Ihre Organisation unterstützen kann.

Übersicht

Als Manager des Security Operations Center (SOC) oder als Benutzer mit der Rolle „Sicherheitsanalyst“ Now Platform (sn_si.analyst) können Sie sich direkt von Ihrem Mobilgerät aus bei einer Instanz Now Platform anmelden. Mit Security Incident Response Mobile-Appkönnen Sie Ihre aktuellen und kritischsten SIR Security Incidents und Antwortaufgaben anzeigen, bearbeiten und zuweisen. Benachrichtigungen informieren Sie, wenn Ihnen zugewiesene kritische Security Incidents eintreffen.

Mit Security Incident Response Mobile-Appkönnen Sie die folgenden SIR -bezogenen Aufgaben auf Ihrem Mobilgerät ausführen:

- Zeigen Sie eine Liste kritischer Security Incidents und Reaktionsaufgaben an.
- Erhalten Sie detaillierte Benachrichtigungen für Security Incidents und Aufgaben, die vordefinierte Benachrichtigungskriterien erfüllen.
- Zeigen Sie Gruppierungen von Security Incidents oder Aufgaben an, die auf einem vordefinierten Satz von Abfragen oder Filtern basieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie die Arbeitsnotizen und zugehörigen Listen von Security Incidents an.
- Aktualisieren Sie Security Incidents, und fügen Sie Arbeitsnotizen oder Anhänge hinzu.
- Bearbeiten Sie die Felder in Security Incidents.
- Weisen Sie sich selbst oder anderen Mitgliedern Ihres Sicherheitsteams Security Incidents zu.

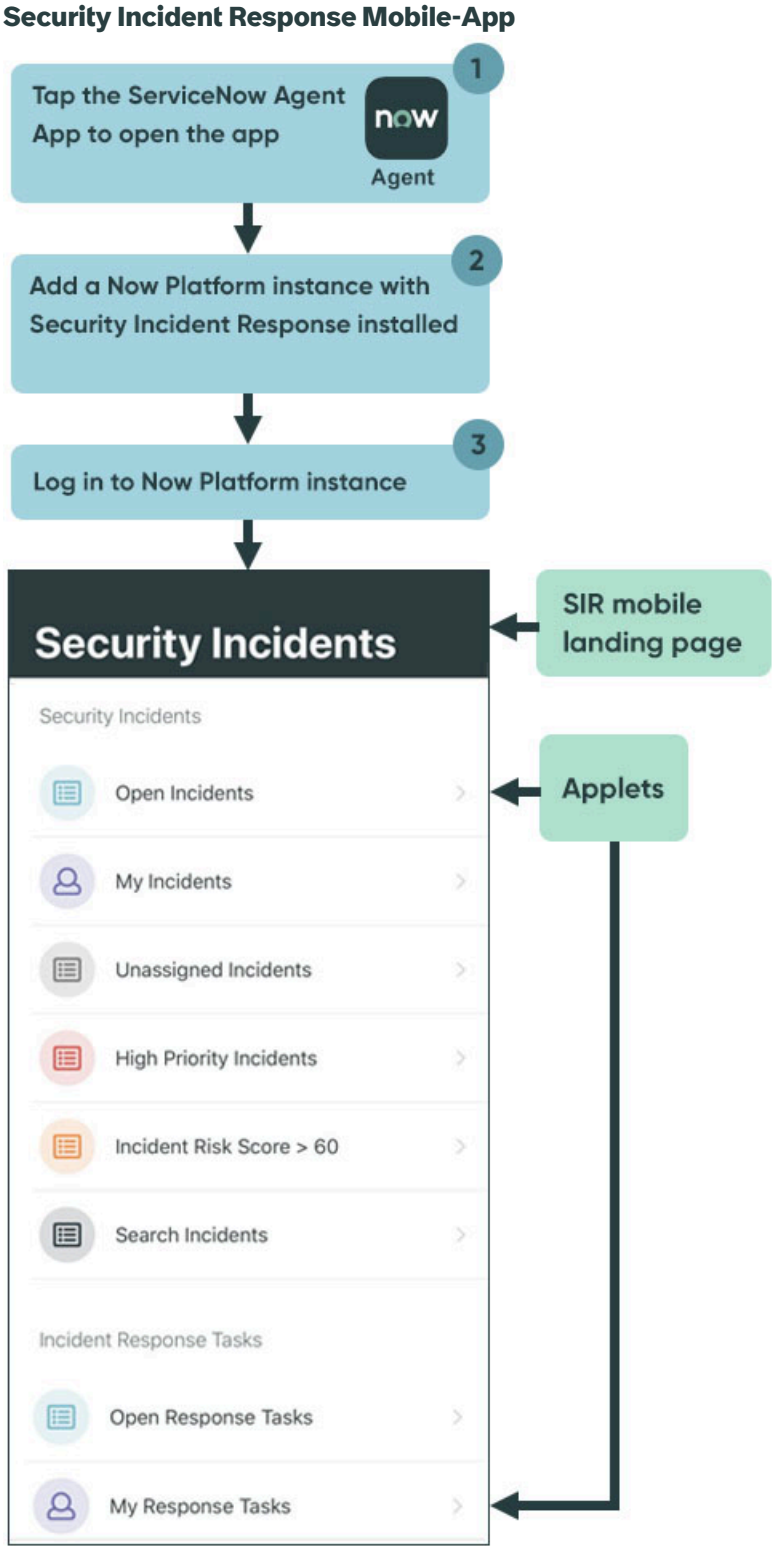
Wenn sie ausgefüllt sind, können Sie die folgenden zugehörigen Listen zu SIR Security Incidents mit Security Incident Response Mobile-Appanzeigen:

- Konfigurationselement
- Betroffener Anwender
- Betroffene Services
- Untergeordnete Security Incidents
- Ähnliche Security Incidents (von Now Platform nicht unterstützt)
- Erkennbare Elemente
- Antwortaufgaben
- Aufgaben
- Aufgaben-SLA
- Anhänge (von Now Platform nicht unterstützt)

Die folgende Abbildung veranschaulicht, wie Sie sich von Ihrem Mobilgerät aus bei der Instanz Now Platform anmelden und wie der Zielbildschirm von Security Incident Response Mobile-App aufgebaut ist, der nach der Anmeldung angezeigt wird.

Schritt-für-Schritt-Anweisungen zum Einrichten der Instanz Now Platform und zur Installation von Security Incident Response Mobile-Appfinden Sie unter Richten Sie eine Prüfliste für ein Security Incident Response Mobile-App. Anweisungen zur Anmeldung finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Anwendungen

Anwendungen sind die ServiceNow® -Softwarekomponenten wie Security Incident Response (SIR), Vulnerability Response (VR) und Governance, Risk und Compliance (GRC), die in Ihrer Instanz Now Platform von bestimmte Funktionen und Funktionalitäten bereitstellen. Nachdem Sie die Core-Anwendung Security Incident Response und Security Incident Response Mobile-App in Ihrer Instanz Now Platform installiert haben, wird nach der Anmeldung das Symbol für die Core-Anwendung auf der Unterseite Ihres Mobilgeräts Android oder iOS angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response Mobile-App Symbol „(Security Incidents)“.

Ordner

Jede Anwendung ServiceNow® Mobile enthält Ordner, die die Applets nach Kategorien trennen. In der vorherigen Abbildung der Zielseite sind **Security Incidents** und **Incident Response-Aufgaben** Ordner.

Applets

Applets sind die verschiedenen Optionen in der Anwendung. Die Symbole unter den Abschnitten **„Security Incidents“** und **„Incident Response-Aufgaben“** sind die verfügbaren Applets von Security Incident Response Mobile-App.

Richten Sie eine Prüfliste für ein Security Incident Response Mobile-App

Die folgende Prüfliste enthält die Einrichtungsaufgaben, die Sie in der Instanz Now Platform® und auf Ihrem Mobilgerät ausführen müssen, bevor Sie Security Incident Response Mobile-Appverwenden.

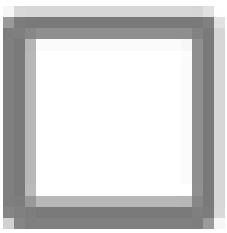
Vorbereitungen

Sie können diese Prüfliste ausdrucken und sich durch die Einrichtungsaufgaben führen lassen, die für Security Incident Response Mobile-Apperforderlich sind. Stellen Sie sicher, dass alle Elemente in der Liste ausgefüllt sind, damit Sie Security Incidents SIR auf Ihrem Mobilgerät anzeigen und bearbeiten können.

Die Prüflistenelemente werden in hervorgehobenem Text angezeigt. Weitere Informationen folgen jedem Element in der rechten Spalte. Geschätzte Zeit für Abschluss dieser Aufgabe: 15–20 Minuten.

Erforderliche Rolle: admin, sn_si.analyst

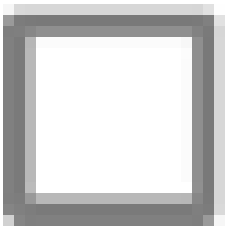
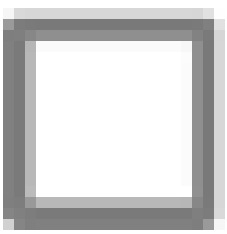
Mobile Prüfliste

Artikel	Beschreibung
	Stellen Sie als Benutzer mit der Administratorrolle sicher, dass die Kernanwendung Security Incident Response auf einer Instanz Now Platform von installiert ist. Dies ist die Instanz Now Platform, die Sie auf Ihrem Mobilgerät anzeigen. **Hinweis:** Die Kernanwendung Security Incident Response und die Instanz Now Platform müssen aus demselben Familien-Release stammen. 1. Um sicherzustellen, dass die Core-Anwendung auf Ihrer Instanz installiert ist, navigieren Sie zu **Plugins**, und suchen Sie nach Security Incident Response. 2. Wenn die Core-Anwendung Security Incident Response noch nicht installiert ist, klicken Sie auf **Installieren**, um sie zu installieren. Weitere Informationen zur Installation der Kernanwendung Security Incident Response finden Sie unter Security Incident Response installieren und konfigurieren. Wenn die Core-Anwendung Security Incident Response nicht in Plugins sichtbar ist, finden Sie weitere Informationen zur Installation von Core-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mobile Prüfliste (Fortsetzung)

Artikel	Beschreibung
	Anwendungen und zu Berechtigungen für Anwendungen unter Security Operations und ServiceNow Store.
	Stellen Sie als Benutzer mit der Administratorrolle sicher, dass Security Incident Response Mobile-App auf der Instanz Now Platform installiert ist, die Sie auf Ihrem Mobilgerät anzeigen möchten. **Hinweis:** Die Instanzen Security Incident Response Mobile-App und Now Platform müssen aus demselben Familien-Release stammen. Laden Sie Security Incident Response Mobile-App aus ServiceNow Store in Ihrer Instanz von Now Platform herunter, und installieren Sie es. Wenn Sie Security Incident Response Mobile-Appinstallieren, werden auch die zugehörigen Abhängigkeiten com.glide.sg und com.glide.sg.agent_native_client installiert. So überprüfen Sie, ob diese Abhängigkeiten installiert sind: **1.** Navigieren Sie zu **Plugins**. **2.** Suchen Sie nach den Plugin-IDs (com.glide.sg und com.glide.sg.agent_native_client). **3.** Wenn sie nicht aktiviert sind, aktivieren Sie diese Plugins. Diese Plugins sind für Security Incident Response Mobile-Apperforderlich. Weitere Informationen zum Installieren von Anwendungen und zu Berechtigungen für Anwendungen finden Sie unter Security Operations und ServiceNow Store.
	Stellen Sie als Benutzer mit der Administratorrolle Now Platform sicher, dass Sie mobilen Benutzern die erforderlichen Rollen in Ihrer Instanz Now Platform zugewiesen haben. **1.** Um die Rollen anzuzeigen, die einem Benutzer zugewiesen sind, navigieren Sie zu **Anwender und Gruppen** > **Anwender**. **2.** Wählen Sie den Anwendernamen gefolgt von der zugehörigen Liste „Rollen“ aus. Alle diesem Anwender zugewiesenen Rollen werden angezeigt. **3.** Überprüfen Sie, ob ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der Rolle IT Infrastructure Library (itil) zu. Benutzer mit der Rolle „itil“ können Security Incidents erstellen, öffnen, aktualisieren und schließen. Nur Benutzern mit der Rolle itil können Aufgaben zugewiesen werden. **4.** Überprüfen Sie, ob ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der Rolle „Sicherheitsanalyst“ (sn_si.analyst) zu. Benutzer mit der Rolle sn_si.analyst können Security Incident-Datensätze lesen und bearbeiten. Diese Rolle wird automatisch hinzugefügt, wenn Sie die Rolle itil zuweisen. **5.** Stellen Sie sicher, dass Sie alle erforderlichen Zuweisungsgruppen erstellt und diesen Gruppen mobile Benutzer zugewiesen haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mobile Prüfliste (Fortsetzung)

Artikel	Beschreibung
	Hinweis: Wenn Sie eine große Anzahl von Benutzern für die mobile -Anwendung haben, können Sie alternativ die Rolle sn_si.analyst einer Gruppe zuweisen. Jeder Anwender, den Sie der Gruppe hinzufügen, erbt diese Rolle. Weitere Informationen zu Sicherheitsanalysten finden Sie unter Sicherheitsanalysten werden zugewiesen. Weitere Informationen zu Benutzern und zum Zuweisen von Rollen zu Benutzern und Gruppen finden Sie unter Benutzeradministration.
☐	Laden Sie als Benutzer mit der Rolle sn_si.analyst die aktuelle ServiceNow® Agent-App auf Ihr Mobilgerät herunter. Die aktuelle Version der Agent-App ist im Apple iOS App Store und im Google Play Store verfügbar.
☐	Als Benutzer mit der Rolle sn_si.analyst können Sie überprüfen, ob Benachrichtigungen auf Ihrem Mobilgerät und in Ihrer Instanz Now Platform aktiviert sind. Benachrichtigungen informieren Sie, wenn Ihnen oder Ihrer Zuweisungsgruppe kritische Security Incidents zugewiesen werden. Um eine rechtzeitige Korrektur zu ermöglichen, klicken Sie nach dem Aktivieren von Benachrichtigungen auf eine Benachrichtigung in Security Incident Response Mobile-App, um direkt zum Security Incident zu navigieren. Führen Sie die folgenden Schritte aus, um Benachrichtigungen in Ihrer Instanz Now Platform zu aktivieren, damit sie auf Ihrem Mobilgerät angezeigt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mobile Prüfliste (Fortsetzung)

Artikel	Beschreibung
	1. Vergewissern Sie sich, dass Sie Security Incident Response Mobile-App in Ihrer Instanz Now Platform von heruntergeladen und installiert haben. 2. Überprüfen Sie in den Systemeinstellungen in der Instanz Now Platform unter „Benachrichtigungen“, ob die **Anwendung ServiceNow Mobile**aktiviert ist. Weitere Informationen zum Festlegen von Benachrichtigungen finden Sie unter Einstellungen für Benutzerbenachrichtigungen in Core-UI festlegen . Now Platform -Benachrichtigungen werden auch auf dem Nachrichtenbildschirm Ihres Mobilgeräts angezeigt. Stellen Sie sicher, dass in den Einstellungen Ihres Mobilgeräts auch Benachrichtigungen aktiviert sind.

Sie haben Ihr Mobilgerät und Now Platform erfolgreich für Security Incident Response Mobile-Appeingerichtet. Als Nächstes müssen Sie sich mit Ihrem Mobilgerät bei der Instanz Now Platform anmelden.

Melden Sie sich bei an Security Incident Response Mobile-App

Öffnen Sie die App Security Incident Response Mobile, und fügen Sie Ihrem Mobilgerät eine Now Platform® -Instanz mit Security Incident Response hinzu.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

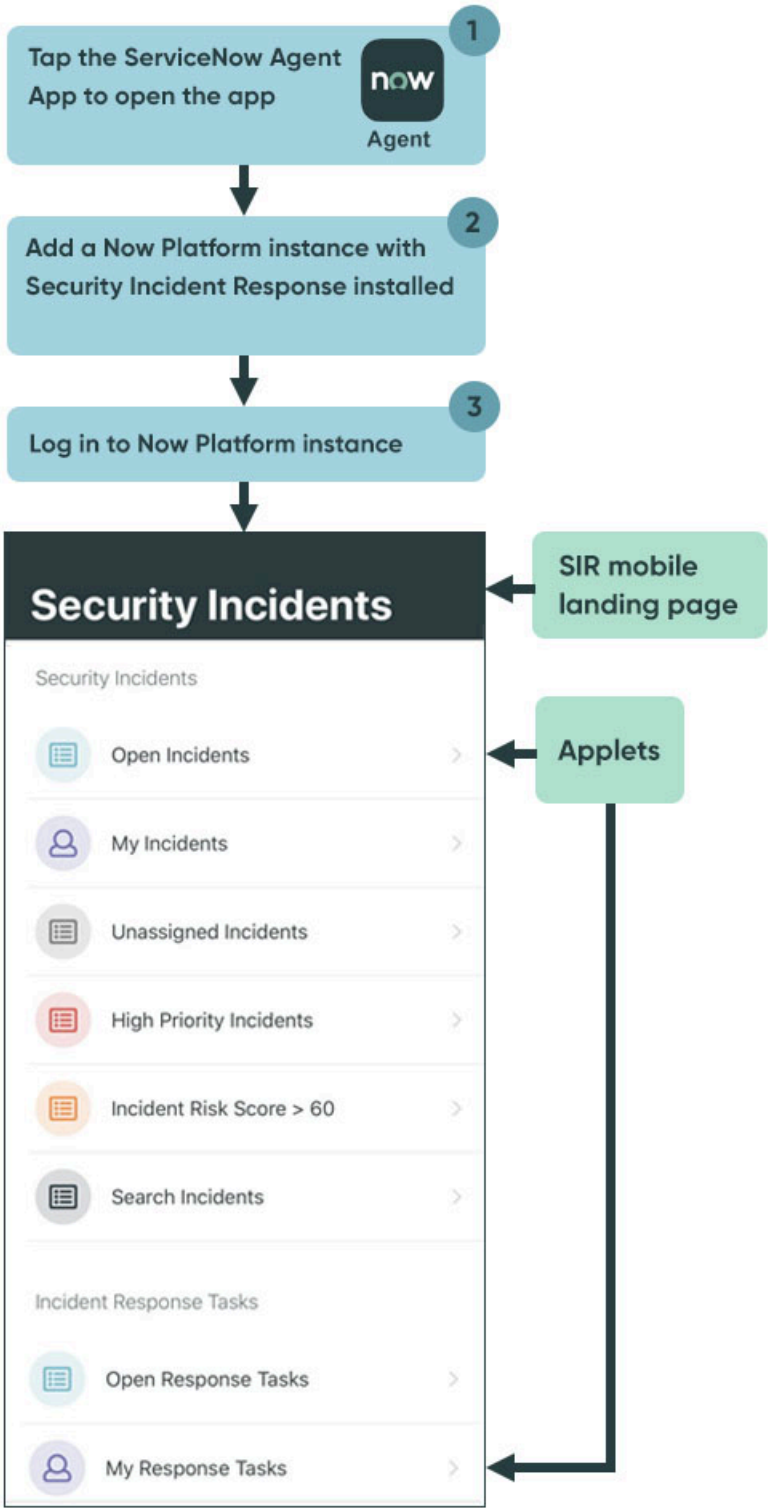
Dauer für diese Aufgabe: 5–10 Minuten.

Stellen Sie sicher, dass Sie die in Richten Sie eine Prüfliste für ein Security Incident Response Mobile-Appbeschriebenen Setup-Schritte abgeschlossen haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

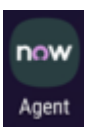
Security Incident Response Mobile-App



Automatische Übersetzung

Prozedur

1. Tippen Sie auf Ihrem Mobilgerät auf die App **ServiceNow Agent,** um sie zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie noch nicht bei einer Instanz Now Platform angemeldet sind, wird der Bildschirm „Instanzen“ angezeigt.

2. Wenn die Instanz Now Platform mit der Core-Anwendung Security Incident Response Ihrem Mobilgerät noch nicht hinzugefügt wurde, führen Sie die folgenden Schritte aus, um sie hinzuzufügen.

   a. Tippen Sie im angezeigten Bildschirm Instanzen auf das .
   Ein Bildschirm wird angezeigt, in dem Sie aufgefordert werden, die Adresse einer Now Platform -Instanz einzugeben und zu speichern.

   b. Füllen Sie die Felder aus.

Feld	Beschreibung
Geben Sie die Instanzadresse ein, oder scannen Sie einen QR-Code.	Wählen Sie eine, um fortzufahren: ▪ Geben Sie vor .service-now.comden Namen Ihrer Instanz Now Platform ein, z. B. sirmobileny. ▪ Geben Sie eine Adresse ein. Diese Adresse ist die URL der Instanz Now Platform, die Sie auf Ihrem Mobilgerät anzeigen möchten, z. B. https://sirmobileny.service-now.com. ▪ Scannen Sie einen QR-Code.
(Optional) Geben Sie einen Kurznamen ein	Geben Sie einen Spitznamen für diese Instanz ein. Wenn dem Gerät mehrere Instanzen hinzugefügt wurden, können Spitznamen Ihnen dabei helfen, eine Now Platform-Instanz schnell zu finden.

   c. Tippen Sie auf **Speichern und anmelden**.

3. Geben Sie im angezeigten Anmeldebildschirm ServiceNow den Anwendernamen und das Passwort für die Instanz Now Platform ein, die Sie hinzufügen möchten, und tippen Sie auf **Anmelden**.
   Der Zielbildschirm Security Incidents wird angezeigt. Sie haben sich erfolgreich bei Security Incident Response Mobile-Appangemeldet.

4. Nach der Anmeldung wird überprüft, ob Benachrichtigungen in Security Incident Response Mobile-Appaktiviert sind.

   a. Tippen Sie im Zielbildschirm unten auf **Benachrichtigung**.

   b. Tippen Sie im Bildschirm **Benachrichtigungen auf Benachrichtigungen aktivieren**, falls die Option nicht aktiviert ist.
   Benachrichtigungen von Now Platform werden auf dem Bildschirm Benachrichtigungen in Security Incident Response Mobile-Appangezeigt.

5. Nachdem Sie sich auf Ihrem Mobilgerät bei einer Instanz angemeldet haben, ist dies die Standardinstanz Now Platform auf dem Gerät.
   Wenn Sie ein anderes Now Platform auf dem Gerät anzeigen möchten, müssen Sie sich von der Standardinstanz abmelden. So melden Sie sich ab:

   a. Tippen Sie auf das Einstellungssymbol.

   b. Tippen Sie auf **Abmelden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Bildschirm Instanzen wird mit allen Now Platform -Instanzen angezeigt, die Sie dem Mobilgerät hinzugefügt haben.

c. **Wahlweise:** Tippen Sie auf eine andere Instanz, um sich anzumelden, oder folgen Sie alternativ den vorherigen Schritten, um eine weitere Instanz hinzuzufügen.

Wenn der Instanzenbildschirm für Security Incident Response Mobile-App nicht angezeigt wird, nachdem Sie auf die App **ServiceNow Agent** auf Ihrem Gerät getippt haben, vergewissern Sie sich, dass **ServiceNow Agent** als vertrauenswürdige App auf Ihrem Gerät zugelassen ist. Um den Zugriff als vertrauenswürdige App zuzulassen, navigieren Sie auf Ihrem Gerät zu den Einstellungen und zur allgemeinen Geräteverwaltung, und tippen Sie auf die Option (Trust-App usw.), um den Zugriff zuzulassen.

Wenn nach der Eingabe Ihrer Anmeldeinformationen im Anmeldebildschirm eine Fehlermeldung angezeigt wird, überprüfen Sie, ob Anwendername und Passwort für die Instanz Now Platform korrekt sind.

Wenn beim Anzeigen des Zielbildschirms Probleme auftreten, überprüfen Sie Ihre Netzwerkverbindung.

Wenn Sie den Bildschirm „Instanzen“ nicht anzeigen können, nachdem Sie auf die App **ServiceNow Agent** getippt haben, versuchen Sie, sie von Ihrem Gerät zu deinstallieren. Stellen Sie sicher, dass Sie die aktuelle Version der App aus dem Apple App Store iOS oder dem Play Store Google haben, und versuchen Sie, sie erneut zu installieren.

Mit können Sie offene Security Incidents anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Als Security Incident-Analyst können Sie offene Security Incident Response (SIR) Security Incidents auf Ihrem Mobilgerät anzeigen, bearbeiten und zuweisen. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

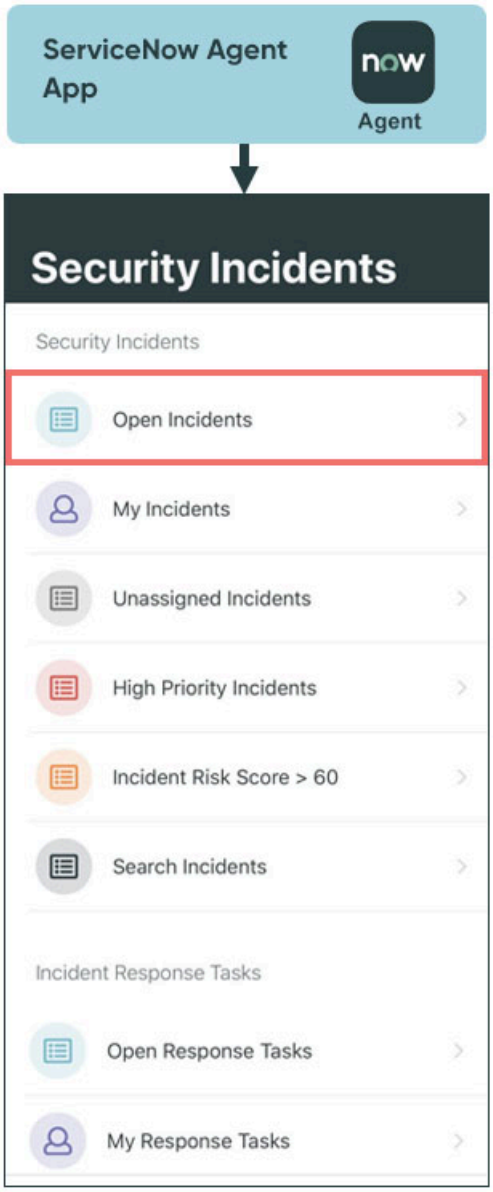
Weisen Sie sich aus der Liste der Datensätze einen offenen Security Incident zu, oder weisen Sie ihn neu zu. Alternativ können Sie sich die Details und zugehörigen Listen des Datensatzes ansehen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Dauer für diese Aufgabe: 5–10 Minuten.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei der Instanz Now Platform angemeldet sind, lesen Sie unter Melden Sie sich bei an Security Incident Response Mobile-Appnach.
2. Tippen Sie bei angezeigter Zielseite Security Incidents **auf Incidents öffnen**.

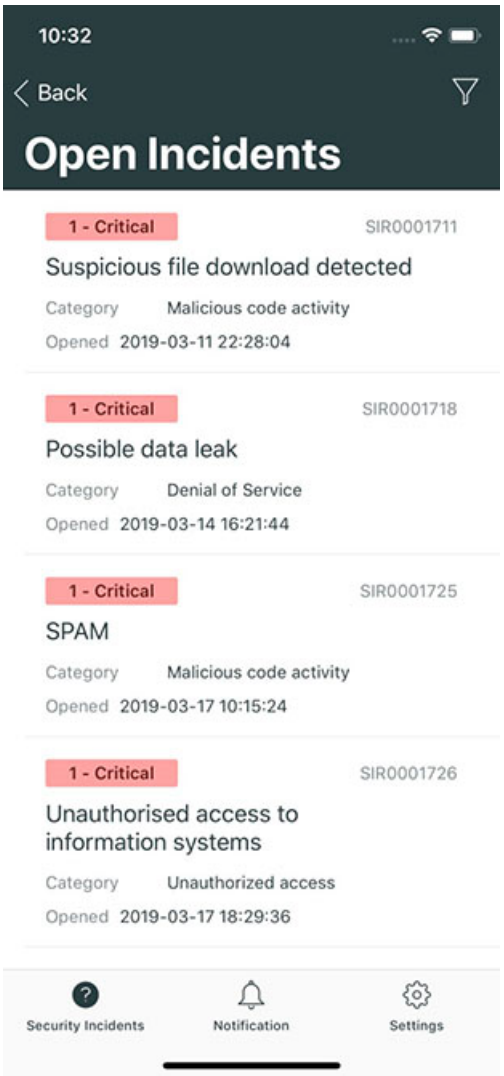
Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Bildschirm Offene Incidents wird mit einer Liste offener Security Incident-Datensätze angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

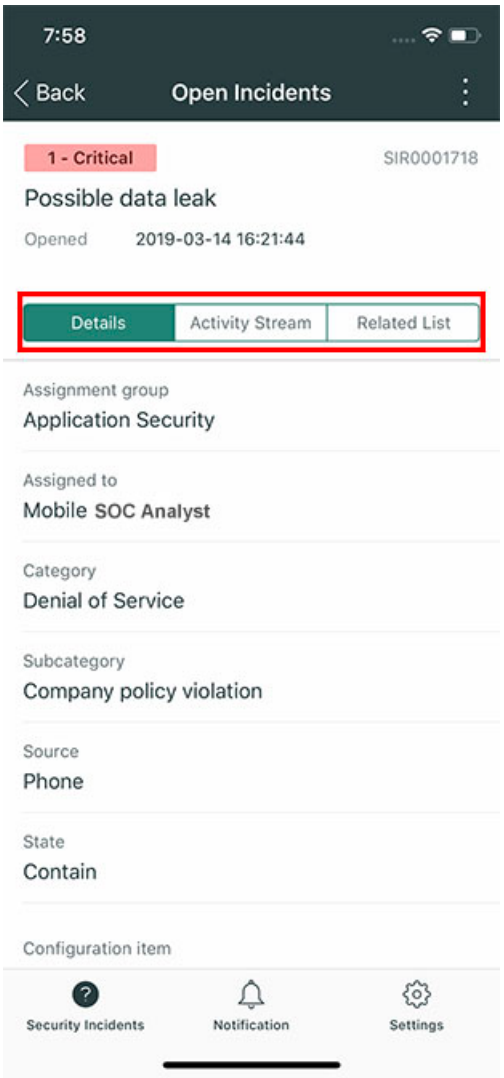


3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.
4. Um sich selbst einen Incident zuzuweisen oder ihn direkt aus der Liste der offenen Security Incidents neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.
5. Wählen Sie eine aus dem angezeigten Menü, um fortzufahren.
6. Alternativ können Sie, um die Details eines offenen Security Incident-Datensatzes und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen, bei angezeigtem Bildschirm Offene Incidents auf einen Datensatz in der Liste tippen.
7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Mit können Sie Security Incidents, die Ihnen zugewiesen sind, anzeigen, bearbeiten und neu zuweisen Security Incident Response Mobile-App

Als Security Incident-Analyst können Security Incident Response Sie (SIR) Incidents, die Ihnen zugewiesen sind, anzeigen, bearbeiten und neu zuweisen. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

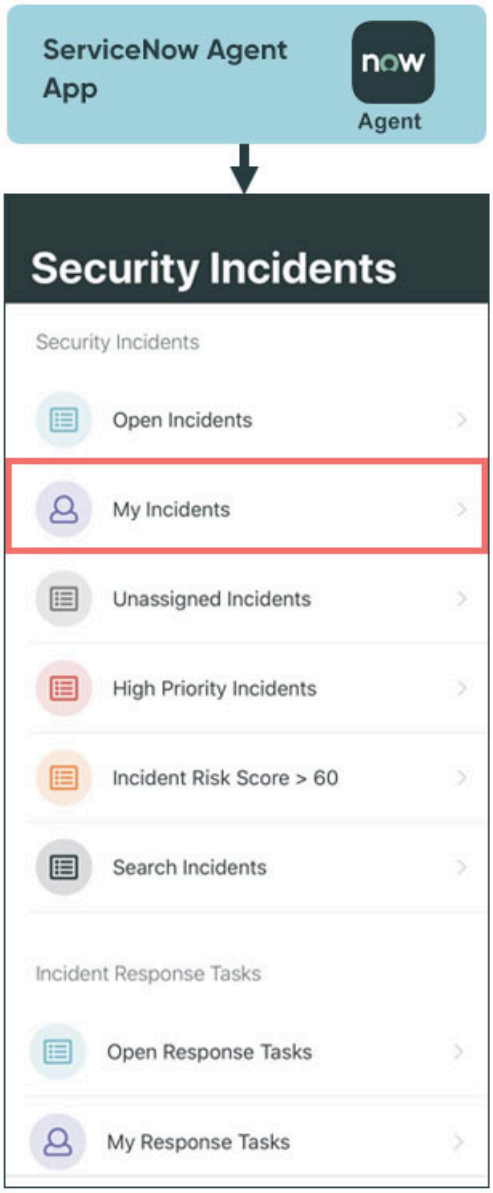
Weisen Sie einen offenen Security Incident aus der Liste der Datensätze einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie sich die Details und zugehörigen Listen des Datensatzes ansehen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Dauer für diese Aufgabe: 5–10 Minuten.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei der Instanz Now Platform angemeldet sind, lesen Sie unter Melden Sie sich bei an Security Incident Response Mobile-Appnach.
2. Tippen Sie bei angezeigtem Zielbildschirm „Security Incidents“ auf **Meine Incidents**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

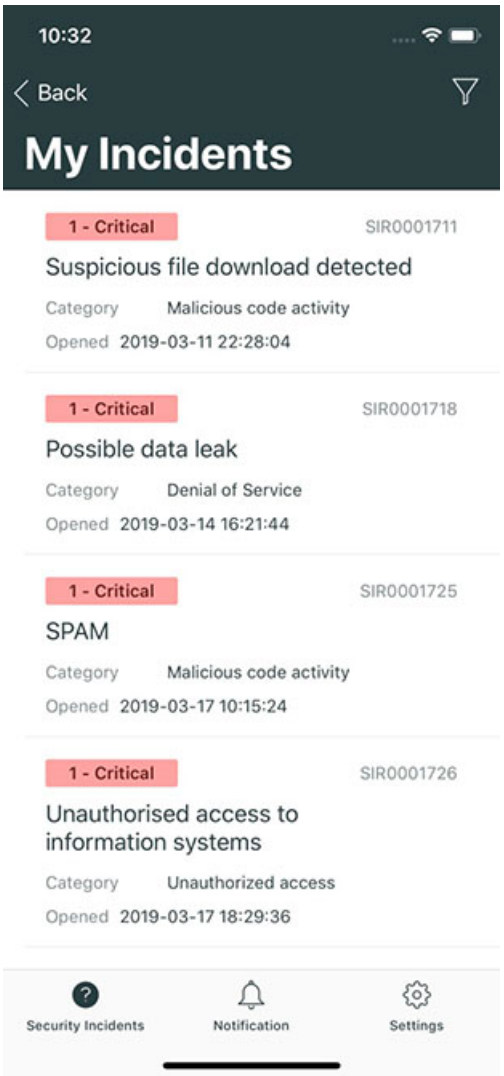
Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm Meine Incidents wird mit einer Liste offener Security Incident-Datensätze angezeigt, die Ihnen zugewiesen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

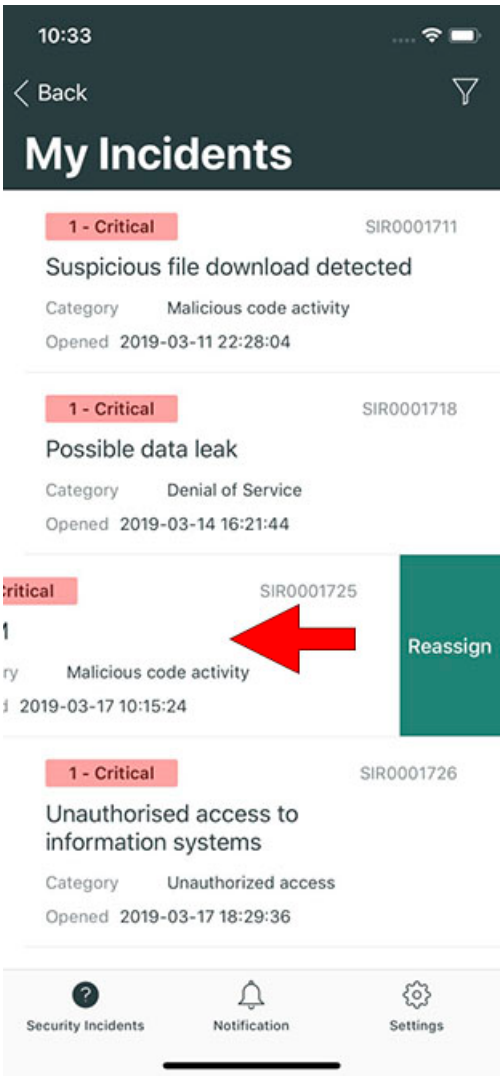


3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

4. Um einen Incident direkt aus der Liste neu zuzuweisen (bei angezeigter Liste offener Security Incident-Datensätze) wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

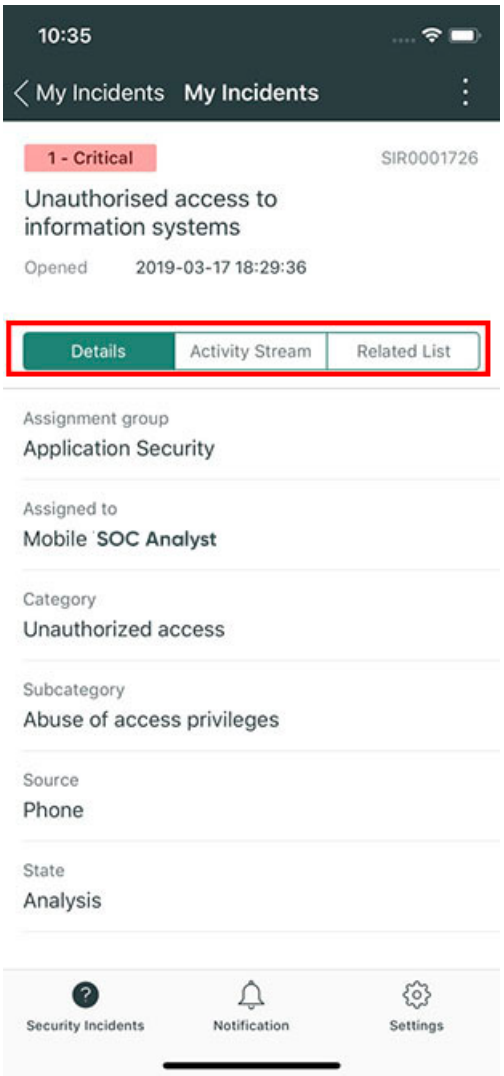


5. Bearbeiten Sie die Felder Zuweisungsgruppe oder Zugewiesen an im angezeigten Menü.

6. Alternativ können Sie, um die Details des geöffneten Security Incident-Datensatzes anzuzeigen, bei angezeigtem Bildschirm Meine Incidents auf einen Datensatz in der Liste tippen.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit können Sie nicht zugewiesene Security Incidents anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Auf Ihrem Mobilgerät können Sie nicht zugewiesene Security Incident Response (SIR) Incidents anzeigen, bearbeiten und zuweisen. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

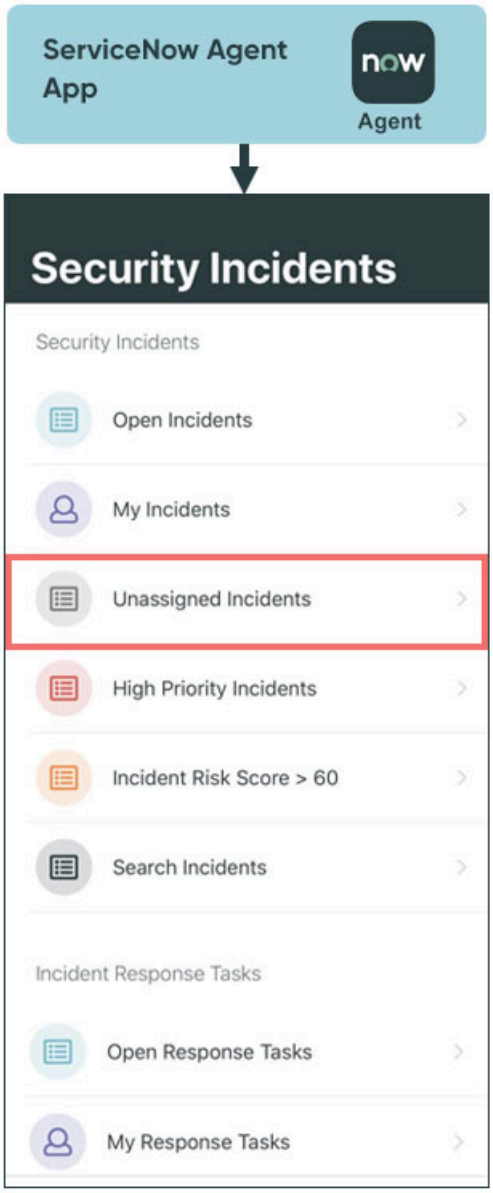
Weisen Sie aus der Liste der Datensätze sich selbst oder einem anderen Analysten in Ihrer Gruppe einen offenen, nicht zugewiesenen Security Incident zu. Alternativ können Sie sich die Details und zugehörigen Listen des Datensatzes ansehen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Dauer für diese Aufgabe: 5–10 Minuten.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie bei angezeigtem Zielbildschirm Security Incidents auf **Nicht zugewiesene Incidents**.

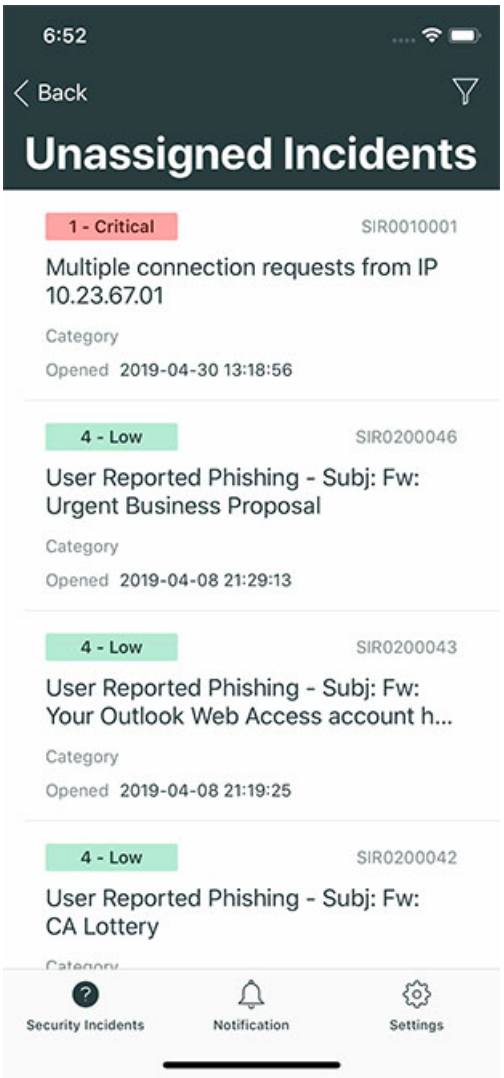
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm Nicht zugewiesene Incidents wird mit einer Liste nicht zugewiesener Security Incident-Datensätze angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

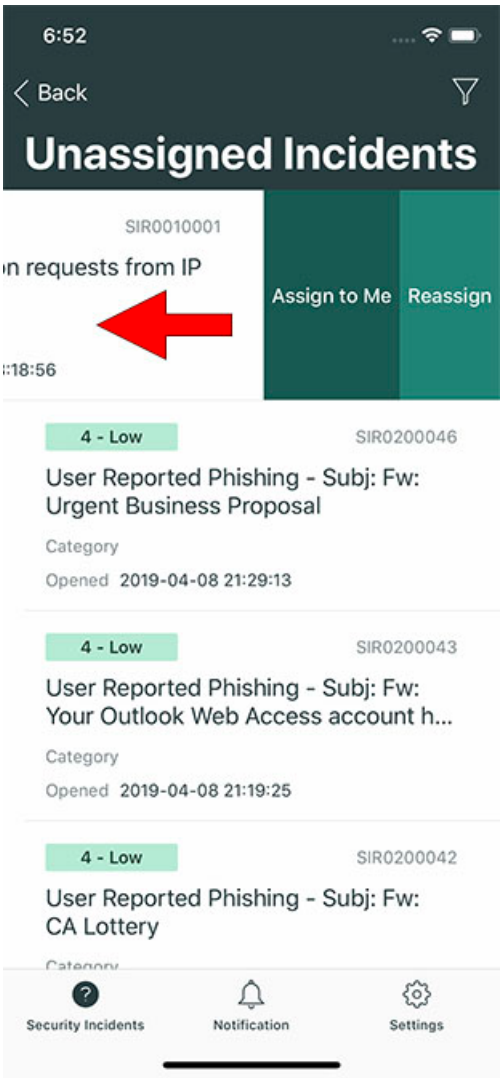


3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

4. Um einen offenen Security Incident-Datensatz direkt aus der Liste bei angezeigter Liste offener, nicht zugewiesener Security Incident-Datensätze zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

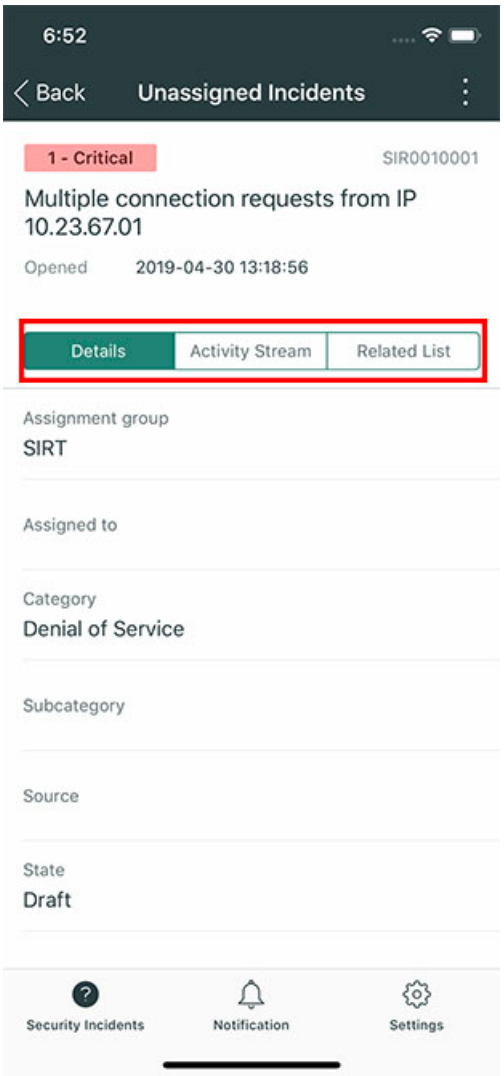


5. Wählen Sie eine aus dem Menü aus, um fortzufahren.

6. Alternativ können Sie bei angezeigtem Bildschirm Nicht zugewiesene Incidents auf einen Datensatz in der Liste tippen.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit können Sie Incidents mit hoher Priorität anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Auf Ihrem Mobilgerät können Sie Incidents mit hoher Priorität Security Incident Response (SIR) anzeigen, bearbeiten und zuweisen. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

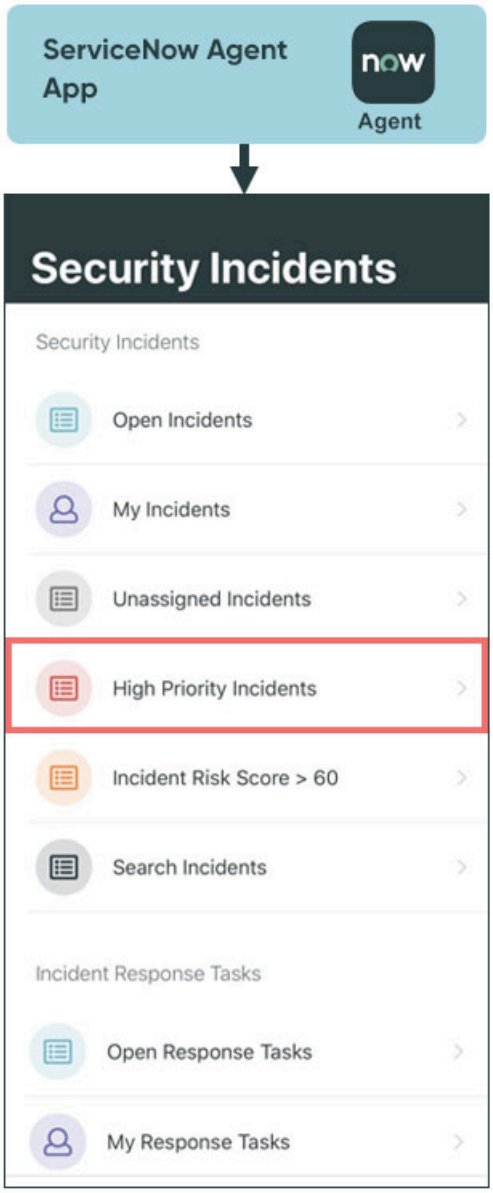
Weisen Sie sich selbst oder einem anderen Analysten in Ihrer Gruppe aus der Datensatzliste einen offenen, kritischen Security Incident zu. Alternativ können Sie sich die Details und zugehörigen Listen des Datensatzes ansehen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Dauer für diese Aufgabe: 5–10 Minuten.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie bei angezeigtem Zielbildschirm Security Incidents auf **Incidents mit hoher Priorität**.

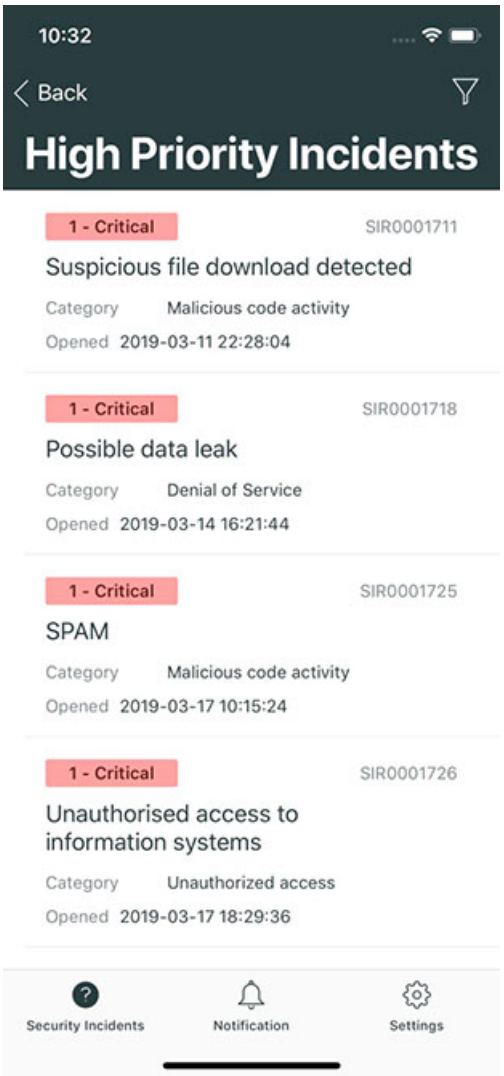
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm Incidents mit hoher Priorität wird mit einer Liste kritischer Security Incidents (mit hoher Priorität) angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

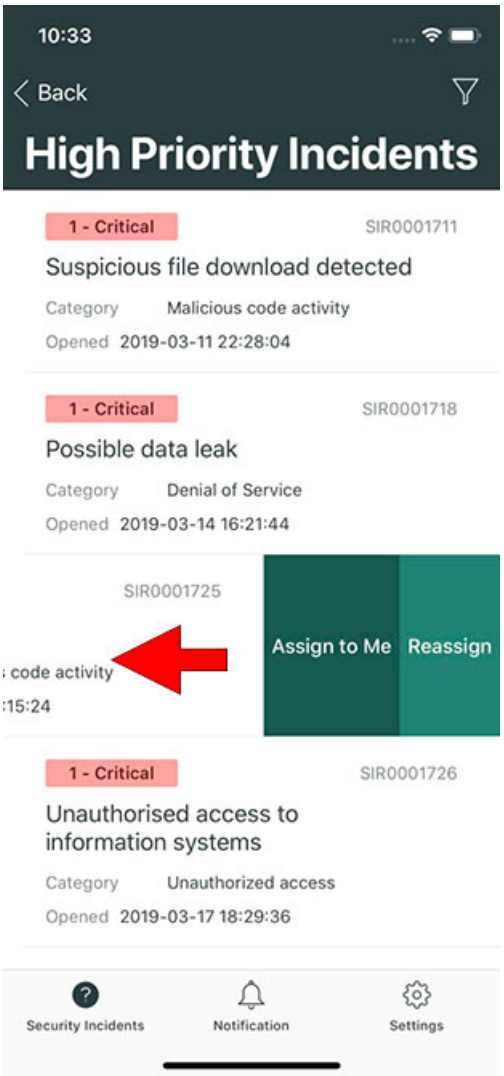


3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

4. Wischen Sie bei angezeigter Liste der offenen Datensätze von Security Incidents mit hoher Priorität auf einem Datensatz nach links, um das Menü zu öffnen.

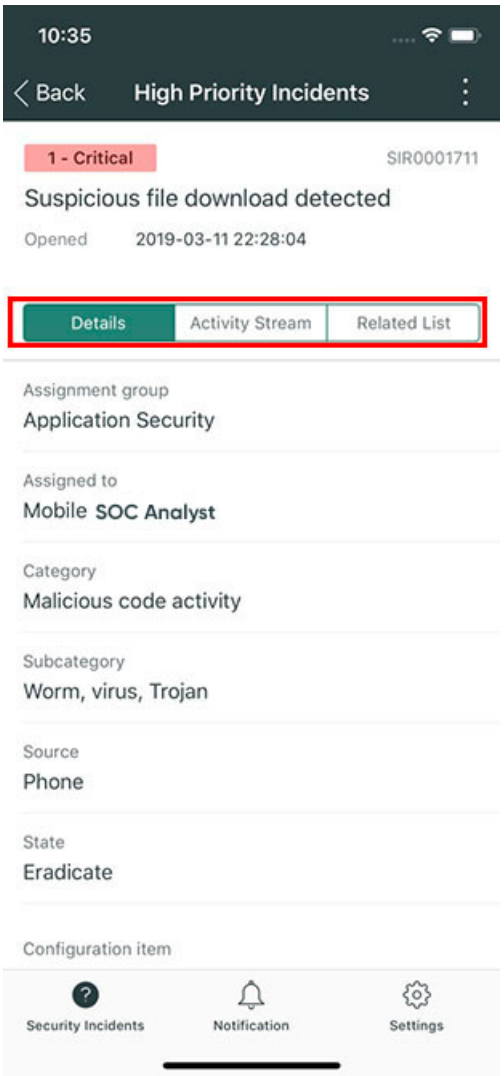
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie eine, um fortzufahren.

6. Tippen Sie auf einen Datensatz in der Liste, um die Details eines offenen Security Incident-Datensatzes und weitere zugehörige Datensätze und zugehörige Listen anzuzeigen, während der Bildschirm Incidents mit hoher Priorität angezeigt wird.
7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit können Sie Security Incidents mit einer Risikopunktzahl von mehr als 60 anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Zeigen Sie auf Ihrem Mobilgerät Security Incident Response (SIR) Incidents an, deren Wert im Feld Risikopunktzahl größer als 60 ist, und bearbeiten Sie sie. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

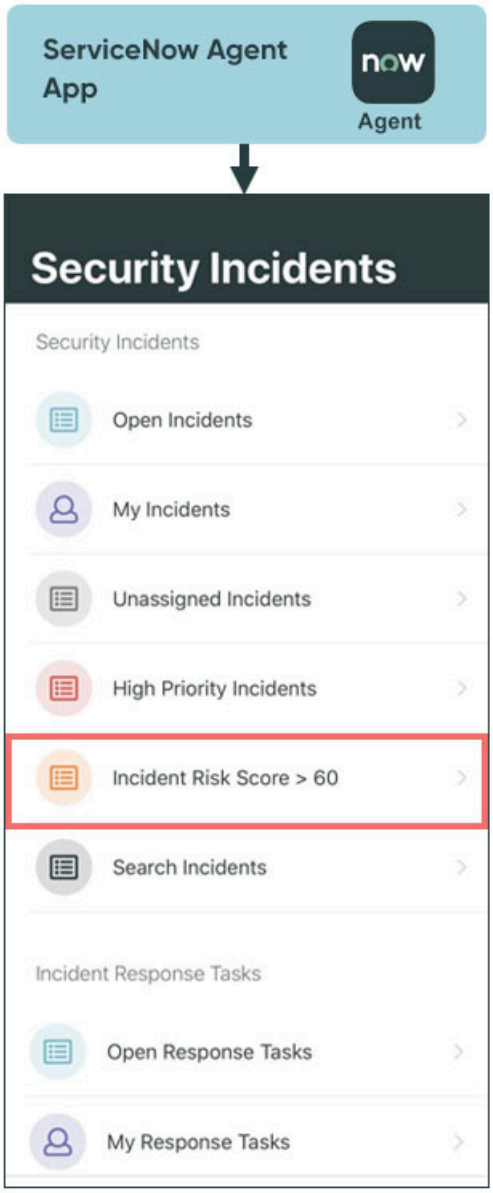
Weisen Sie aus der Liste der Datensätze einen offenen Security Incident mit einer Risikopunktzahl von mehr als 60 an sich selbst oder einen anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie sich die Details und zugehörigen Listen des Datensatzes ansehen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Dauer für diese Aufgabe: 5–10 Minuten.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie bei angezeigtem Zielbildschirm „Security Incidents“ auf **Risikopunktzahl > 60**.

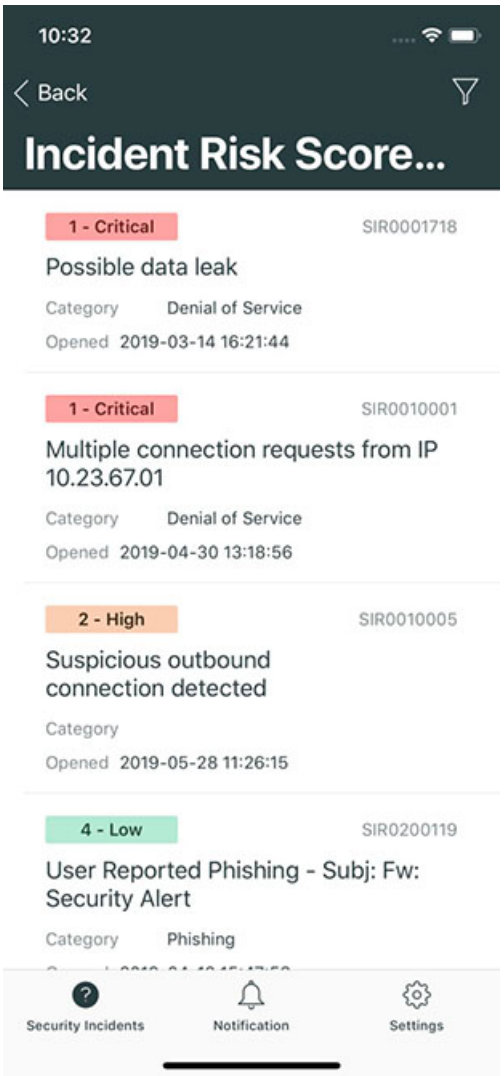
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm „Incident-Risikopunktzahl“ wird mit einer Liste von Security Incidents angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

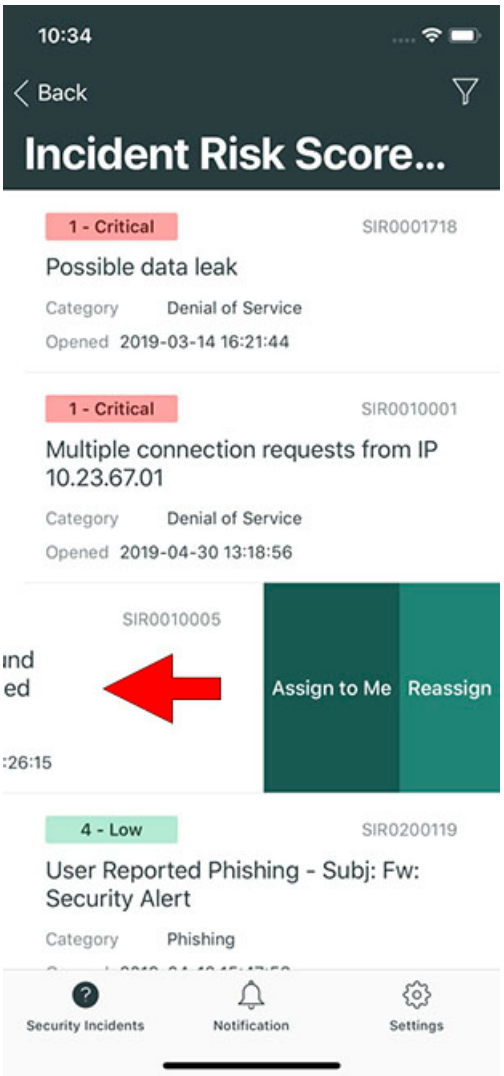


3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

4. Um sich selbst einen Security Incident zuzuweisen oder ihn direkt aus der angezeigten Liste der offenen Security Incident-Datensätze neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

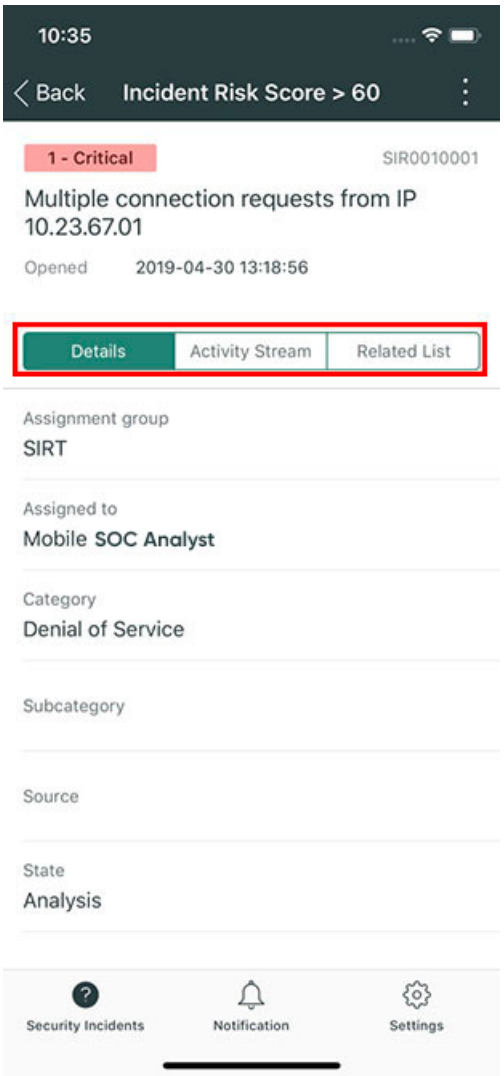
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie eine, um fortzufahren.

6. Alternativ können Sie, um die Details eines offenen Security Incident-Datensatzes und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen, bei angezeigtem Bildschirm Incident-Risikopunktzahl auf einen Datensatz in der Liste tippen.
7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App

Suchen Sie nach Security Incidents vom Security Incident Response Typ (SIR) in einer Instanz Now Platform® vom Typ . Es werden nur Incidents angezeigt, die den von Ihnen eingegebenen Suchkriterien entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

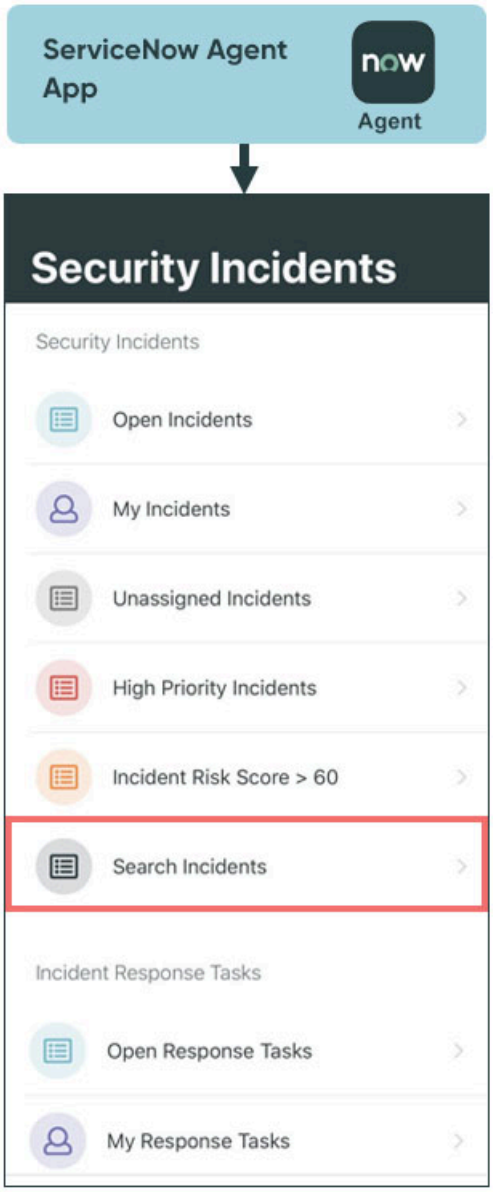
Dauer für diese Aufgabe: 5–10 Minuten.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie bei angezeigtem Zielbildschirm „Security Incidents“ auf **Incidents durchsuchen**.

   Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um die Anzahl der zurückgegebenen Suchergebnisse zu begrenzen, füllen Sie möglicherweise so viele Felder wie möglich im Formular aus.
   Informationen zum Hinzufügen von Suchkriterien finden Sie in der folgenden Tabelle. Befolgen Sie die Anweisungen nach der Tabelle, um vorhandene Suchkriterien zu bearbeiten, Suchkriterien zu löschen oder eine Suche zu senden.

Tippen Sie auf dieses Feld	So fügen Sie einen Eintrag auf Geräten Android hinzu	Zum Hinzufügen eines -Eintrags auf iOS -Geräten
Nummer	Geben Sie einen alphanumerischen Wert für einen Security Incident ein, z. B. SIR0010004. Diese Nummer wird oben rechts im Security Incident angezeigt. Die Funktion sucht nach numerischen Zeichenfolgen	Geben Sie einen alphanumerischen Wert für einen Security Incident ein, z. B. SIR0010004. Diese Nummer wird oben rechts im Security Incident angezeigt. Die Funktion sucht nach numerischen Zeichenfolgen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	So fügen Sie einen Eintrag auf Geräten Android hinzu	Zum Hinzufügen eines -Eintrags auf iOS -Geräten
	und partiellen numerischen Zeichenfolgen. Geben Sie für eine verfeinerte Suche mehr Ziffern ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder um eine Suche zu übermitteln.	und partiellen numerischen Zeichenfolgen. Geben Sie für eine verfeinerte Suche mehr Ziffern ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder **auf Suche**, um eine Suche zu senden.
Kurzbeschreibung	Geben Sie Text in das Feld ein, z. B. Malware. Die Funktion durchsucht Textzeichenfolgen und Teiltextzeichenfolgen aus dem Feld Kurzbeschreibung. Geben Sie für eine verfeinertere Suche mehr Text ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder um eine Suche zu übermitteln.	Geben Sie Text in das Feld ein, z. B. Malware. Die Funktion durchsucht Textzeichenfolgen und Teiltextzeichenfolgen aus dem Feld Kurzbeschreibung. Geben Sie für eine verfeinertere Suche mehr Text ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder **auf Suche**, um eine Suche zu senden.
Priorität	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchen-Symbol, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie **auf Fertig,** um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.
Kategorie	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchen-Symbol, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie **auf Fertig,** um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.
Status	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchen-Symbol, um zum Bildschirm	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie **auf Fertig,**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	So fügen Sie einen Eintrag auf Geräten Android hinzu	Zum Hinzufügen eines -Eintrags auf iOS -Geräten
	„Incidents durchsuchen“ zurückzukehren.	um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.
Zugewiesen an	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.
Zuweisungsgruppe	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.	Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, damit kein Eintrag vorhanden ist, wählen Sie **Keine**aus.

Bei Android -Geräten wählen Sie bei angezeigtem Bildschirm „Incidents suchen“ und Eingabe eines Kriteriums eines aus, um fortzufahren.

4. Wählen Sie bei iOS -Geräten bei angezeigtem Bildschirm „Incidents durchsuchen“ eines aus, um fortzufahren.

5. **Wahlweise:** Wenn Ihre Suche mehrere Datensätze zurückgibt, können Sie Filtern Sie Datensätze mit Security Incident Response Mobile-App, um die Suchergebnisse zu verfeinern.

Mit können Sie offene Antwortaufgaben anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Sie können offene Antwortaufgaben anzeigen, bearbeiten und zuweisen. Ihre Änderungen werden in der Security Incident Response-Aufgabe des übergeordneten Security Incident gespeichert.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

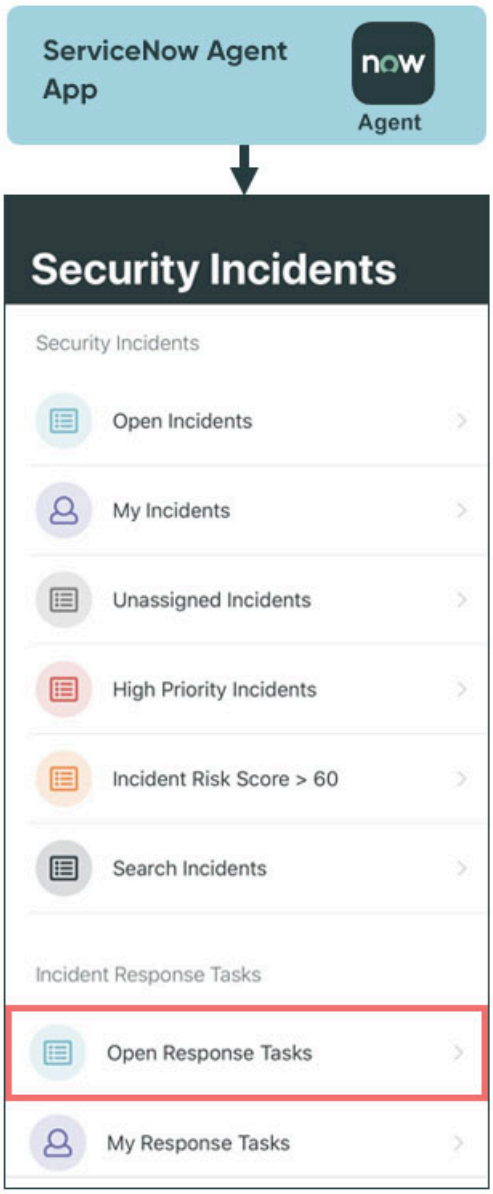
Weisen Sie aus der Liste der Datensätze eine offene, nicht zugewiesene Antwortaufgabe sich selbst oder einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Dauer für diese Aufgabe: 5–10 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie bei angezeigtem Zielbildschirm Security Incidents **auf Offene Antwortaufgaben**.

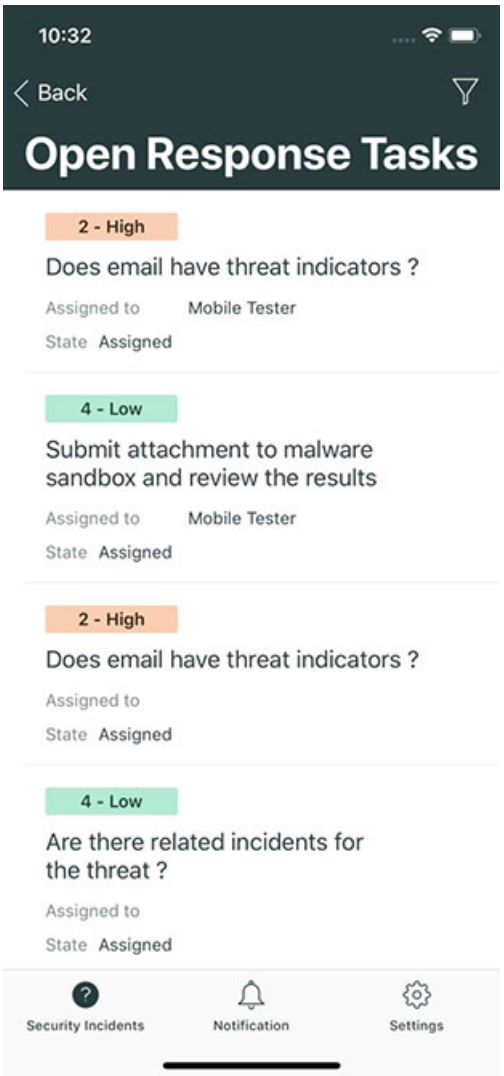
   Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm Offene Antwortaufgaben wird mit einer Liste offener Aufgaben angezeigt.

Automatische Übersetzung

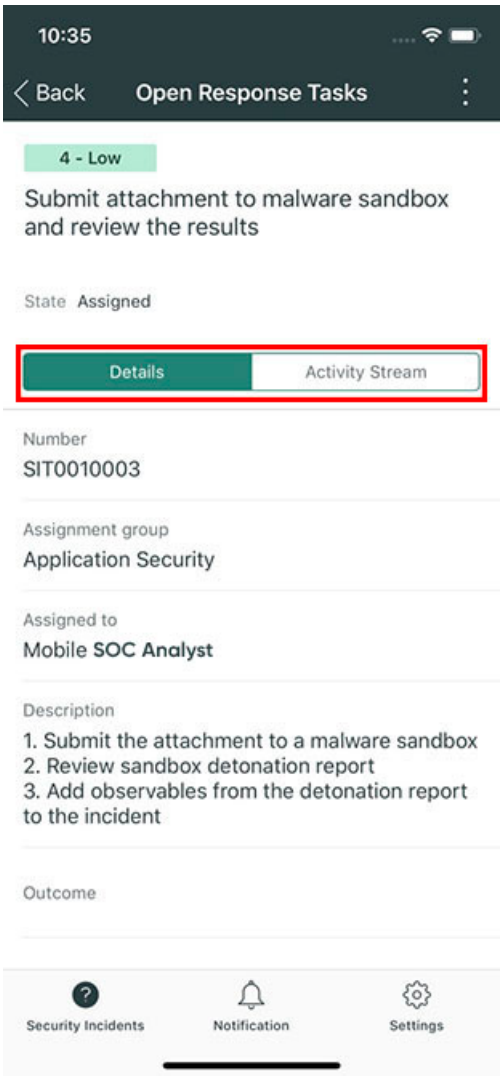
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. **Wahlweise:** Informationen zur Suche nach Aufgaben, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.
4. Wenn die Liste der offenen Antwortaufgaben angezeigt wird, können Sie zum Zuweisen oder erneuten Zuweisen direkt aus der Liste auf einem Datensatz nach links wischen, um das Menü zu öffnen.
5. Wählen Sie eine, um fortzufahren.
6. Alternativ können Sie, um die Details eines offenen Antwortaufgaben-Datensatzes anzuzeigen, bei angezeigtem Bildschirm Offene Antwortaufgaben auf einen Datensatz in der Liste tippen.
7. Wählen Sie bei angezeigten Registerkarten im Antwortaufgaben-Datensatz eine in der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit können Sie Ihre Antwortaufgaben anzeigen, bearbeiten und neu zuweisen Security Incident Response Mobile-App

Ihnen zugewiesene Antwortaufgaben anzeigen, bearbeiten und neu zuweisen Ihre Änderungen werden in der Security Incident Response-Aufgabe des übergeordneten Security Incident gespeichert.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

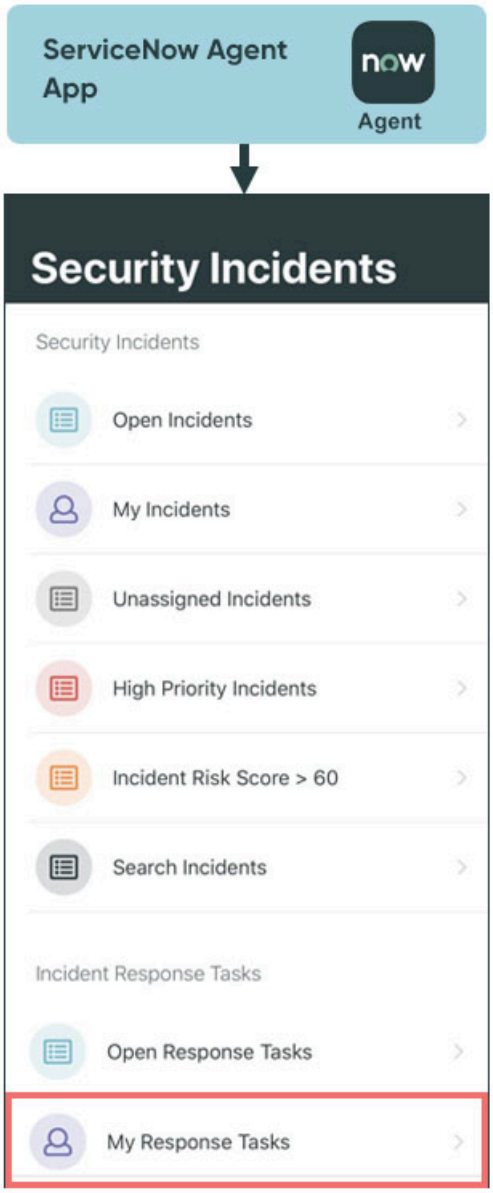
Weisen Sie in der Liste der Datensätze eine Ihnen zugewiesene offene Antwortaufgabe einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details des Datensatzes anzeigen oder vor der Neuzuweisung eine Arbeitsnotiz hinzufügen. Dauer für diese Aufgabe: 5–10 Minuten.

Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie bei angezeigtem Zielbildschirm Security Incidents **auf Meine Antwortaufgaben**.

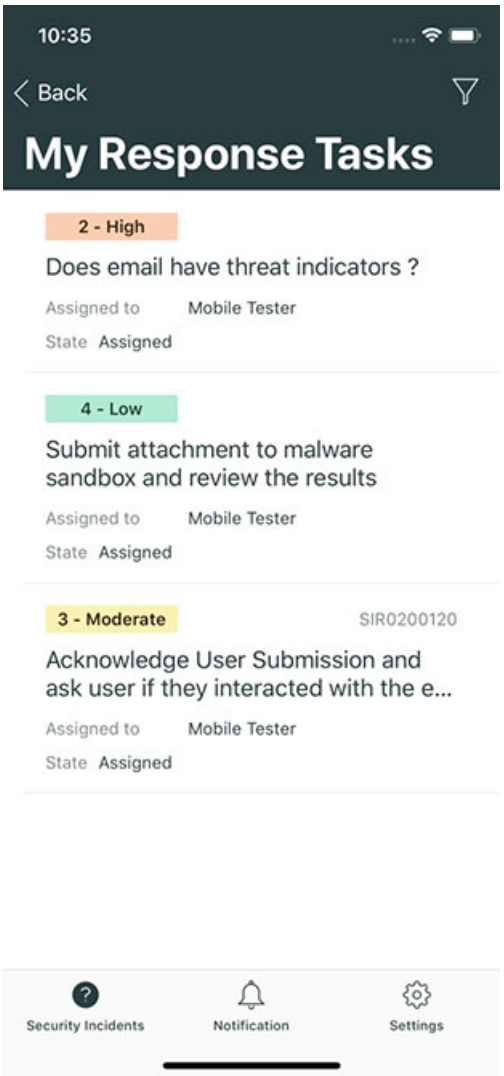
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie nach der Anmeldung von Security Incident Response Mobile-App weg navigieren, tippen Sie jederzeit auf die App Now Agent (Erfüller), um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm Meine Antwortaufgaben wird mit einer Liste der Ihnen zugewiesenen Antwortaufgaben angezeigt.

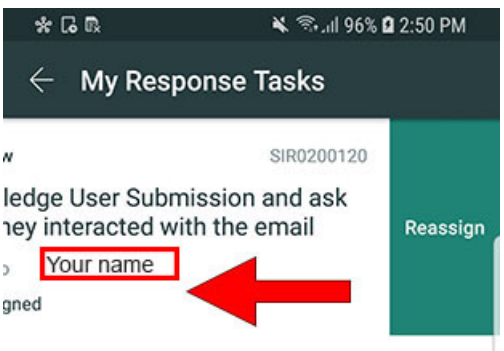
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. **Wahlweise:** Informationen zur Suche nach Aufgaben, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

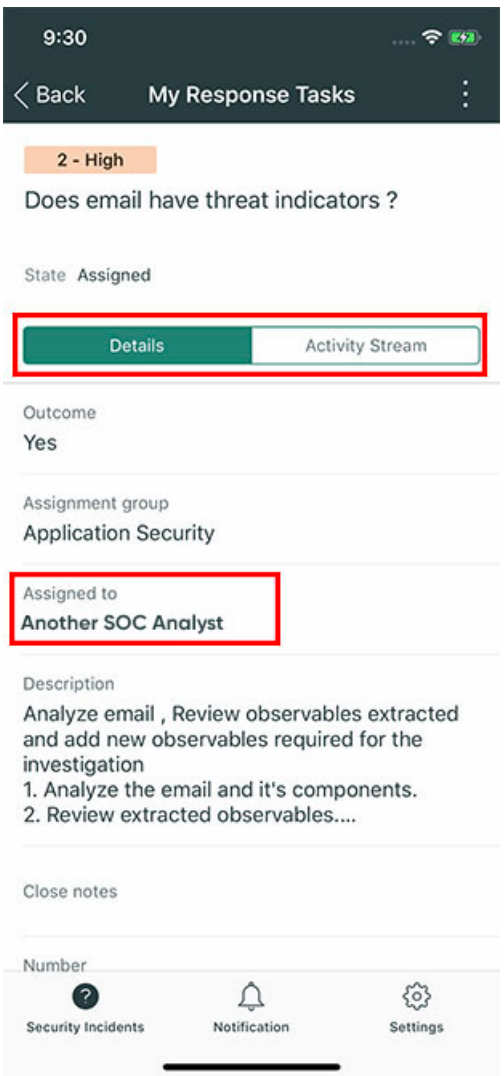
   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der mobilen App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

4. Um eine Aufgabe direkt aus der Liste der Ihnen zugewiesenen Aufgabendatensätze neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Tippen Sie auf **Erneut zuweisen**.
6. Tippen Sie im angezeigten Bildschirm Antwortaufgabe einer anderen Person zuweisen auf ein Feld, um es zu erweitern, und wählen Sie eine andere Gruppe oder einen anderen Benutzer für die Aufgabe aus.
7. Tippen Sie auf das Senden-Symbol ( ) oder **auf Absenden**, um Ihre Änderungen zu speichern und die Antwortaufgabe zu aktualisieren.
   Es wird eine Meldung angezeigt, die bestätigt, dass der Datensatz aktualisiert wurde. Die Aufgabe wird im übergeordneten Security Incident einem neuen Benutzer zugewiesen, und Ihre Instanz Now Platform wird aktualisiert.
8. Um die Details einer offenen Antwortaufgabe und die Arbeitsnotizen anzuzeigen, tippen Sie bei angezeigtem Bildschirm Meine Antwortaufgaben auf einen Datensatz in der Liste.
9. Wählen Sie bei angezeigten Feldern in der Antwortaufgabe eines in der folgenden Tabelle aus, um fortzufahren.



Automatische Übersetzung

Filtern Sie Datensätze mit Security Incident Response Mobile-App

Legen Sie zusätzliche Filter fest, um die Anzahl der Datensätze zu begrenzen, die in einem Bildschirm angezeigt werden. Das Filtern von Datensätzen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Dauer für diese Aufgabe: 5 Minuten.

Prozedur

1. Um Ihre Suchergebnisse weiter zu verfeinern oder zusätzliche Filterkriterien in einer beliebigen Liste von Datensätzen einzugeben, die angezeigt wird, tippen Sie auf das Filtersymbol ( ).
2. Tippen Sie bei angezeigtem Filter-Bildschirm auf ein Feld, um es zu erweitern.
3. Tippen Sie in den angezeigten Optionen auf das Kontrollkästchen, oder tippen Sie auf ein Element für Ihren Filter.
   Für viele der Filter können Sie mehr als eine Option auswählen.
4. Tippen Sie auf den Zurück-Pfeil ( ) oder **auf FERTIG**, um Ihre Änderungen in einem Feld zu speichern.
   Die von Ihnen ausgewählten Kriterien werden im Filter-Bildschirm angezeigt. Die Anzahl der Datensätze, die Ihren Kriterien entsprechen, wird auch oben im Bildschirm angezeigt. Tippen Sie auf **ZURÜCKSETZEN**, um alle Filter zu entfernen und die Standardeinstellung wiederherzustellen.
5. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 4 bei angezeigtem Bildschirm Filter, um mit dem Festlegen Ihrer Filterkriterien fortzufahren.
6. Tippen Sie auf das Schnittmengensymbol um UND-Bedingungen zu erstellen.
   Alternativ tippen Sie auf das Schnittmengensymbol um ODER-Bedingungen zu erstellen.
7. Nachdem Sie alle gewünschten Kriterien hinzugefügt haben, tippen Sie bei angezeigtem Filter-Bildschirm auf **FERTIG**.
   Auf dem Bildschirm werden nur die Datensätze angezeigt, die Ihren Filterkriterien entsprechen.

Security Incident Response Orchestration

Security Incident Response Orchestration -Aktivitäten ermöglichen Benutzern die Interaktion mit und das Abrufen von Daten aus Windows- oder UNIX-basierten Systemen und Umgebungen mithilfe der Workflow-Orchestration.

Security Incident Response Orchestration einrichten

Führen Sie vor der Verwendung von Security Incident Response OrchestrationSchritte aus, um verschiedene Teile des Systems einzurichten, einschließlich CMDB-Auffüllung, Konfiguration des MID-Servers und Konfiguration der Anmeldeinformationen.

Vorbereitungen
Erforderliche Rolle: Administrator
Zur Verwendung von Security Incident Responsebenötigen Sie eine vollständig ausgefüllte CMDB mit Domänennamen. Weitere Informationen finden Sie unter Discovery .

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Aktivieren Sie das Plugin Security Incident Response.
2. Konfigurieren von MID-Servern .
3. Konfigurieren Sie die Anmeldeinformationen für den Windows-MID-Server-Service .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sich mit den Workflows und Workflow-Vorlagen von Security Incident Response Orchestration vertraut machen

Das -Basissystem Security Incident Response enthält eine Reihe von Workflows und Workflow-Vorlagen, die für die Arbeit mit Security Incident-Datensätzen entwickelt wurden.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Warum und wann dieser Vorgang ausgeführt wird

Sie können alle Workflows und Workflow-Vorlagen an Ihre Bedürfnisse anpassen, sofern Sie über die entsprechende Rolle verfügen: sn_sec_cmn.admin. Workflows werden im gesamten Security Operations-System zur Ausführung verschiedener Aufgaben verwendet.
Workflow-Vorlagen werden jedoch durch die Auswahl eines Werts im Feld **Kategorie** in einem Security Incident ausgelöst. In diesem Fall startet die mit der Auswahl verknüpfte Workflow-Vorlage eine Workflow-Vorlage, die die Sicherheitsanalysten über den Umgang mit einem bestimmten Bedrohungstyp informiert.

Wenn Sie beispielsweise in einem Security Incident **Denial of Service** im Feld **Kategorie** auswählen, wird **Security Incident - Denial of Service - Vorlage** ausgeführt, und der Analyst wird angewiesen zu bestimmen, ob das Ziel des DOS geschäftskritisch ist. Wenn dies der Fall ist, bewirkt die nächste Aufgabe, dass die Priorität des Security Incident auf **1 - Kritisch**festgelegt wird, und führt dann die nächste Aufgabe aus. Und so weiter.

Security Incident Response -Workflows und Workflow-Vorlagen sind also im Wesentlichen identisch mit dem Unterschied, dass die Vorlagen für einen bestimmten Satz von Funktionen innerhalb eines Security Incident verwendet werden.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Workflows** > **Sicherheitsworkflows anzeigen**.
2. Eine Liste der im Basissystem enthaltenen Workflows und Workflow-Vorlagen wird angezeigt.
   Alle neuen Workflows, die Sie in der Anwendungssuite Security Operations erstellt haben, werden ebenfalls in die Liste aufgenommen.
3. Klicken Sie auf den Namen des Workflows oder der Workflow-Vorlage, den bzw. die Sie anzeigen möchten.

Hinweis:
Workflows können auf verschiedene Arten ausgelöst werden. Beachten Sie, dass das Verknüpfen eines Workflows mit einem Workflow-Auslöser nicht unbedingt bedeutet, dass der Workflow aktiv ist.

Security Incident Response Orchestration Workflows und Aktivitäten

Security Incident Response Orchestrationenthält mehrere Workflows und Aktivitäten.

Das können nur Benutzer mit der Rolle sn_sec_cmn.admin Workflow-Editor .

Workflow „Suchanforderung für IoC-Changes erstellen“.

Der Flow **„Security Incident Response – Suchanforderung für IoC-Changes erstellen“** wird durch eine Business Rule ausgelöst und wird automatisch ausgeführt, wenn ein IoC hinzugefügt oder geändert wird. Malware-Scans werden nur ausgelöst, wenn neue Daten eingegeben werden, und nur die neuen Daten werden gescannt.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Wenn das IoC leer ist, wird der Workflow nicht ausgeführt. Historische Scans werden beibehalten und auf der Registerkarte **Sicherheitsscananforderungen** und in Arbeitsnotizen des Security Incidents angezeigt. Die vorhandenen Security Incidents werden automatisch aktualisiert.

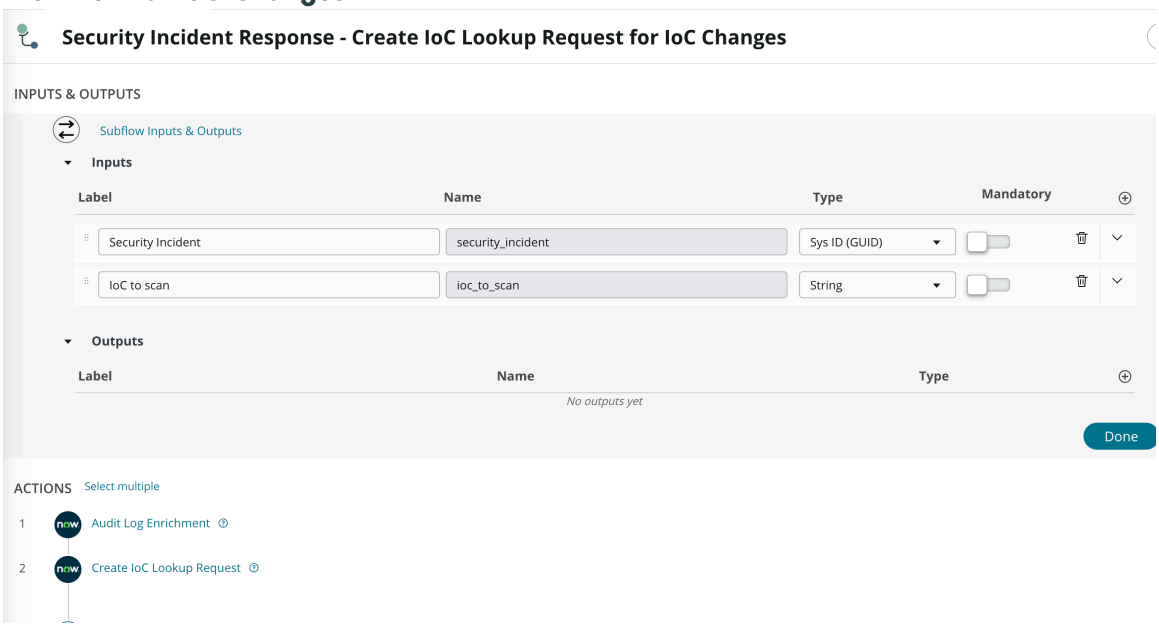
Wichtig:

Der Workflow **„Security Incident Response – Suchanforderung für IoC-Changes erstellen“** wird in den Flow Designer migriert. Der Flow wird nur ausgelöst, wenn sn_ti_scanner mindestens einen Datensatz enthält.

Die Flow Designer-Aktionen umfassen:

- Audit-Protokollergänzung
- Aktivität „IoC-Suchanforderung erstellen“.

Workflow für IoC-Changes



Aktivität „IoC-Suchanforderung erstellen“.

Die Aktivität **„IoC-Suchanforderung erstellen“** kann mit jedem Workflow verwendet werden, um eine Malware-Suchanforderung für hinzugefügte oder geänderte IoC-Felder zu erstellen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Suchanforderung erstellt.
Fehler	Suchanforderung nicht erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
iocString	IoC-Informationen im JSON-Format. IP, Hash, URL.
siId	Systembezeichner für Security Incident

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
scnReqID	Suchanforderungsbezeichner

Security Incident Response – Flow zum Abrufen von Netzwerkstatistiken

Die zugehörigen Listen namens **Security Incident Response** > **Netzwerkstatistiken abrufen** -Flow ruft die Netzwerkstatistiken für eine betroffene Windows-basierte Ressource ab, wenn sie einem Security Incident im **Analysestatus** hinzugefügt wird.

Vorbereitungen

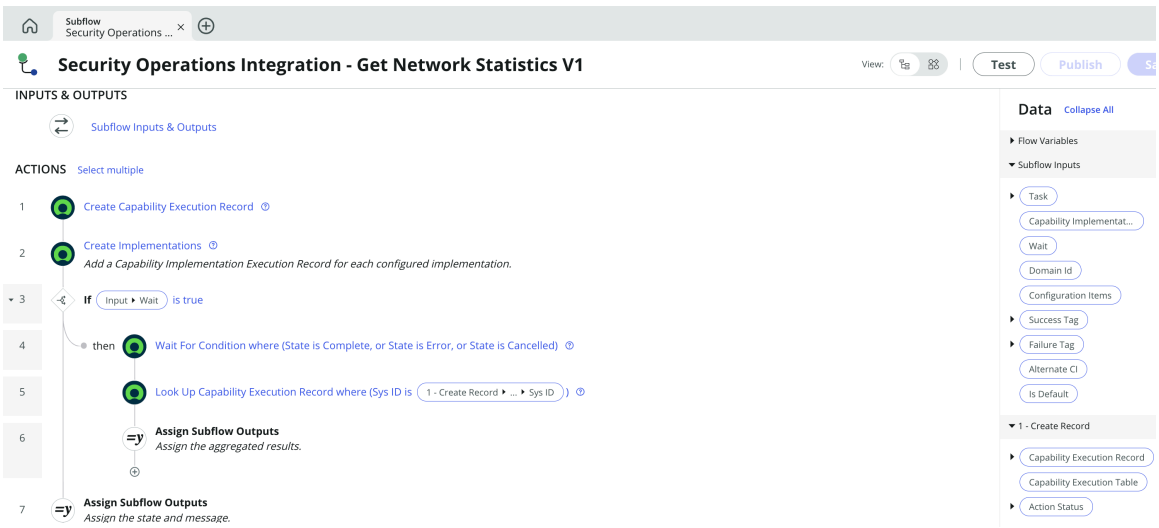
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Bei neuen Security Incidents, die Konfigurationselemente enthalten, wird der Flow automatisch ausgeführt, wenn sich der Status in **Analyse**ändert.

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich im Status **„Analyse** “ befinden und ein neues Configuration Item hinzufügen.

Netzwerkstatistiken abrufen



Zu den Flow-Prozessaktionen gehören:

FQDN-Flow-Aktion für Konfigurationselement abrufen

Shell-Skript nach Betriebssystem bestimmen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die If-Anweisung wird von PowerShell ausgeführt

Ausführungsnachverfolgung: Flow-Aktion beginnen

Flow-Aktion „Netzwerkstatistiken über Netstat“ abrufen

Nachverfolgung der Fähigkeitsausführung: Fehler-Flow-Aktion

Flow-Aktion zum Erstellen von Datensätzen mit Ergänzungsdaten

Nachverfolgung der Fähigkeitsausführung: Fehler-Flow-Aktion Gibt die Ergänzungs-ID zurück.

Nachverfolgung der Fähigkeitsausführung – Flow-Aktion abschließen

Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie bei Bedarf den **Status** auf **Analyse**.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration stellt Netzwerkstatistikinformationen im bereit **Zugehörige Links** > **Ergänzungen zu Security Incidents** Registerkarte Weitere Informationen finden Sie unter Security Operations Zuordnung von Ergänzungsdaten.

Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Workflow „Security Incident Response - Get Laufende Services“.

Der **Workflow „Security Incident Response – Get Laufende Services“** ruft eine Liste der laufenden Services aus Windows-basierten Konfigurationselementen (Configuration Items, CI) ServiceNow] ab. Dieser Workflow wird während Untersuchungen für die Anreicherung von Incidents verwendet.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Der **Workflow Security Incident Response – Get Laufende Services** wird automatisch ausgeführt, wenn Sie einem Windows-Security Incident ein neues Configuration Item hinzufügen, nachdem der Status in **Analyse**geändert wurde. Die Informationen, die dieser Workflow erhält, werden auf den Registerkarten **„Ergänzungsdaten anzeigen“** für den Security Incident angezeigt.

Hinweis:
Wenn der Security Incident im Status **Entwurf** bleibt, wird der **Workflow „Security Incident Response – Laufende Services abrufen“** nicht ausgeführt.

Zu den Workflow-Aktivitäten gehören:

Aktivität „Audit-Protokoll-Ergänzungsskript“.

FQDN-Flow-Aktion für Konfigurationselement abrufen

Bestimmen Sie das Shell-Skript anhand der Betriebssystemaktivität

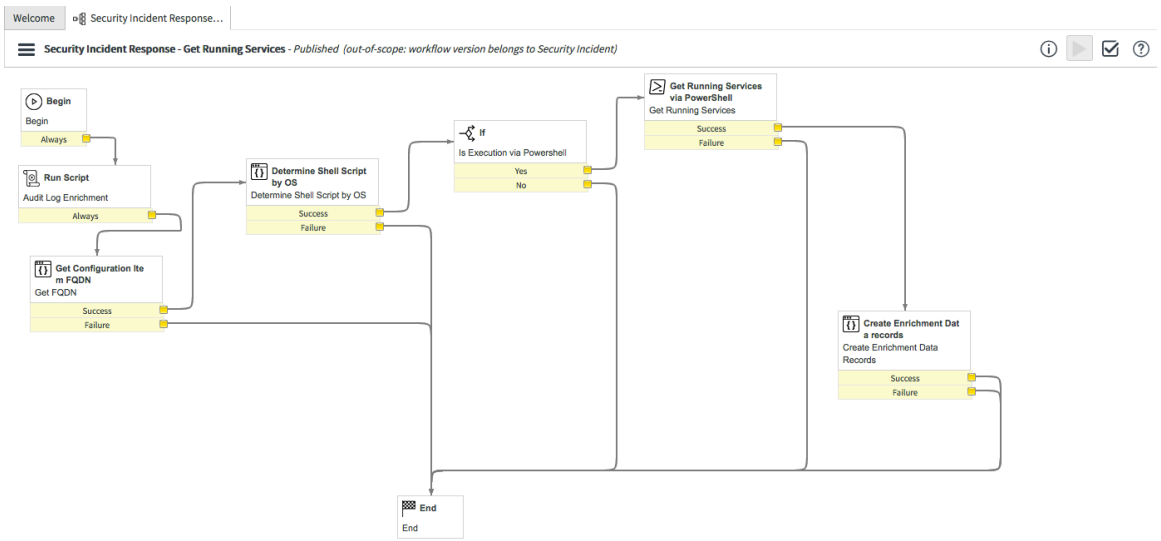
Ist „Ausführung über PowerShell-Aktivität“.

Laufende Services abrufen – WMI-Ergänzungsaktivität

Flow-Aktion zum Erstellen von Datensätzen mit Ergänzungsdaten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laufende Services abrufen



Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie bei Bedarf den **Status** auf **Analyse**.
3. Fügen Sie ein Windows-basiertes Configuration Item (Server, Laptop oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response stellt Informationen zu laufenden Services im bereit **Zugehörige Links** > **Ergänzungen zu Security Incidents**Registerkarte Weitere Informationen finden Sie unter Security Operations Zuordnung von Ergänzungsdaten.

Bestimmen Sie das Shell-Skript anhand der Betriebssystemaktivität

Die Workflow-Aktivität „Shell-Skript nach Betriebssystem bestimmen“ bestimmt, welches Betriebssystem im Workflow verwendet werden soll

Die Aktivität Shell-Skript nach Betriebssystem bestimmen kann mit jedem Workflow verwendet werden, um zu bestimmen, welches Shell-Skript basierend auf dem Betriebssystem des Systems, das das Konfigurationselement enthält, ausgeführt werden soll.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Betriebssystem gefunden.
Fehler	Kein Betriebssystem gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
ciSysId	Systembezeichner des Configuration Item.
processType	Interner Bezeichner, der definiert, welches Skript aus der Tabelle abgerufen werden soll.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
processScript	ECC-Agent, der den laufenden Prozess sammelt.
executesTemplate	Bestimmt, ob das Skript über eine Probe oder mithilfe von PowerShell ausgeführt wird.
„richmentMappingId“	System-ID der Ergänzungszuordnung, die zum Transformieren der Antwortdaten verwendet wird.

Laufende Services abrufen – WMI-Ergänzung

Der Workflow **„Security Incident Response – Get Laufende Services“** sammelt laufende Services für ein Konfigurationselement, das einem Security Incident hinzugefügt wird.

Die Aktivität **„Laufende Services abrufen – WMI-Ergänzung“** wird automatisch gestartet, um Informationen zu laufenden Services für einen Windows-Host abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Ziel [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) des Zielsystems.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Antwort [Zeichenfolge]	Eine JSON-Zeichenfolge, die die aktuell auf dem Zielsystem ausgeführten Services darstellt. JSON-Daten enthalten: **name** Der Name des Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
	pid Der Prozessbezeichner des laufenden Services **service_type** (Optional) Der Typ des laufenden Services. **start_name** Der Systemname für den Service **path** Der Dateipfad der ausführbaren Datei des laufenden Services **start_mode** Der Startmodus des laufenden Services. **display_name** Der Name des laufenden Services, wie er dem Benutzer angezeigt wird

Beschränkungen

Der MID Server muss **PowerShell**unterstützen.

SHA-256-Hash erfordert PowerShell V4.

Führen Sie den procdump-Flow aus

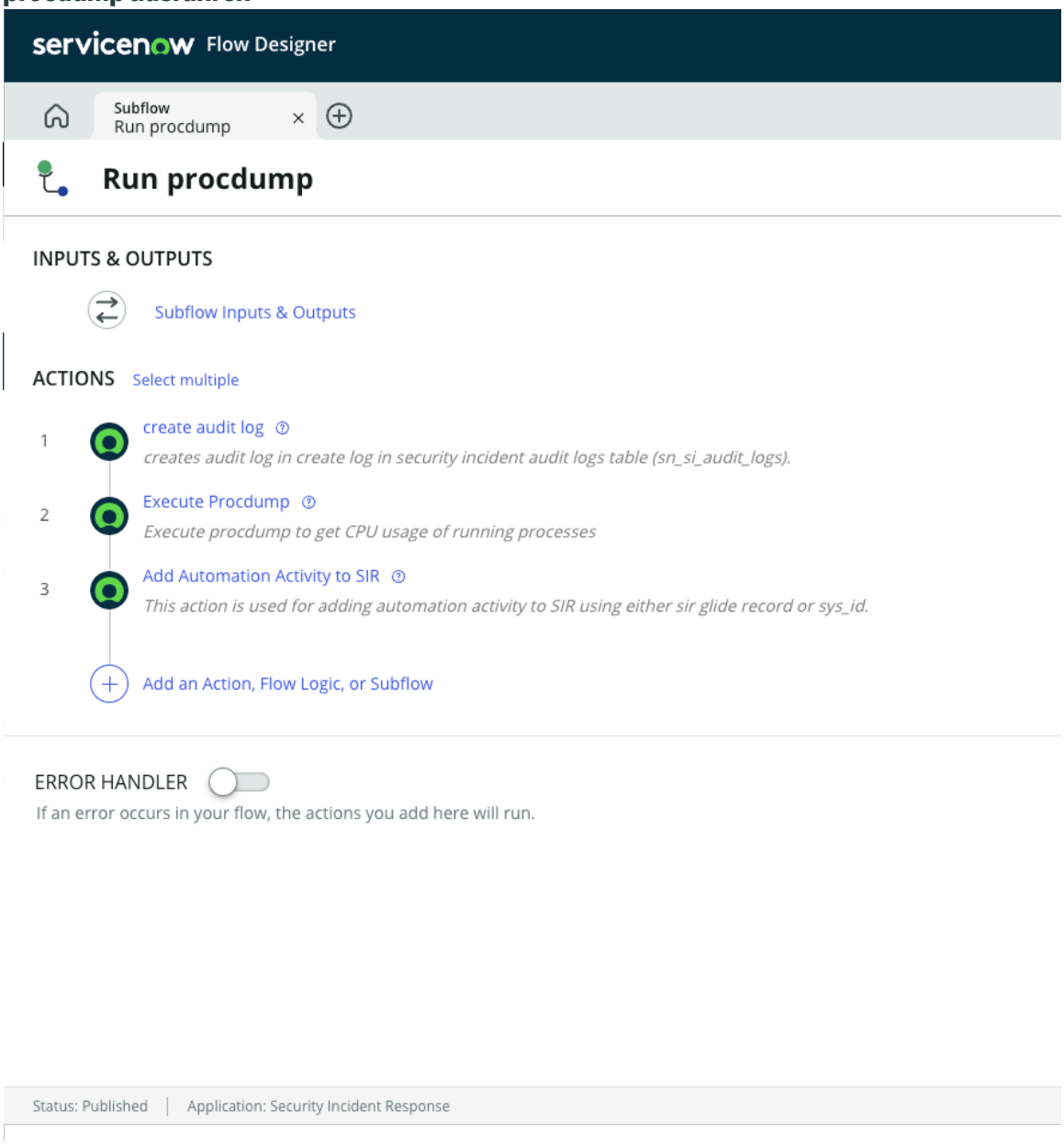
Der Flow **Procdump ausführen** führt eine Prozesssicherung für einen angegebenen Prozess aus und speichert sie in einer Datei, die von Sicherheitsanalysten als Ziel ausgewählt werden kann.

Erforderliche Rolle: sn_si.analyst

Dieser Flow wird ausgelöst, wenn angereicherte Prozesse ausgewählt werden und eine UI-Aktion **„Procdump ausführen“** ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

procdump ausführen



Folgende Gründe können für den Procdump-Fehler verantwortlich sein:

- Ungültiger Dump-Pfad
- Ungültiger Dateifreigabepfad
- Der vollständig qualifizierte Domänenname des Windows-Computers, auf dem der Procdump ausgeführt wird, kann nicht abgerufen werden
- Der Prozessname ist nicht angegeben
- Die PROCDUMP-Umgebungsvariable wurde nicht gefunden
- Eine Kopie der Dump-Datei kann nicht aus dem Dump-Pfad in den Dateifreigabepfad kopiert werden

Führen Sie die procdump-Aktion aus

„Procdump ausführen“ ist eine PowerShell-Aktion, die den Procdump für die ausgewählten Prozesse ausführt, die Daten in eine Datei speichert und sie an eine freigegebene Site in einem internen Netzwerk sendet. Ein Analyst kann dann einen Prozess auf der Deny-Liste

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

anzeigen, der in einem Security Incident rot hervorgehoben ist, und zusätzliche Analysen an der Datei durchführen.

Ergebnisse

Mögliche Ergebnisse für diese Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der procdump wurde erfolgreich unter „process_name“ ausgeführt, und die Details sind in „actionOutput.response“ verfügbar.
Fehler	Der procdump konnte für „process_name“ nicht ausgeführt werden. Die Details sind in „actionOutput.response“ verfügbar.

Eingabevariablen

Eingabevariablen werden verwendet, um die angeforderten Ausgaben zu erstellen.

Eingabevariablen

Variable	Beschreibung
targetId	[Obligatorisch] Die Ziel-ID, für die der Procdump ausgeführt werden soll.
process_name	[Obligatorisch] Der Prozessname für den Procdump.
„dump_path“	[Obligatorisch] Der lokale Dateipfad, in dem die generierte Dump-Datei gespeichert wird.
„dump_filename“	[Obligatorisch] Der Dateiname der vom Procdump generierten Datei. Alle Sonderzeichen werden durch Bindestriche (-) aus dem Namen der Dump-Datei ersetzt, wenn die Datei generiert wird.
Dateifreigabepfad	[Obligatorisch] Der Dateifreigabepfad, in den die Dump-Datei kopiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Share_path	Der Dateifreigabepfad, in den die Sicherungsdatei kopiert wurde.
response	Eine JSON-Darstellung des Ergebnisses des Procdumps.
Ergebnis	Das Ergebnis des procdump.

Security Incident: Workflow zum Bewerten des Ergebnisses der Antwortaufgabe

Der Workflow „Security Incident – Antwort auswerten“ bestimmt die zu verwendende Aufgabe und ruft einen ausgewählten Workflow und ein Bewertungsskript basierend auf dem Ergebnisauswertungsdatensatz auf, der als Eingabe für den ausgewählten Workflow bereitgestellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow soll gleichzeitig mit der auszuwertenden Aktivität „Aufgabe erstellen“ ausgeführt werden. Das Bewertungsskript fragt die Artefakte (z. B. Sichtungssuchdatensätze oder laufende Prozesse) der konfigurierten Fähigkeit anhand von Kontextinformationen aus der Antwortaufgabe (z. B. dem übergeordneten Security Incident) ab, um das entsprechende Ergebnis für die Antwortaufgabe zu ermitteln. Das Ergebnis könnte möglicherweise von der Workflow-Aktivität abhängig sein, lautet jedoch im Allgemeinen **„ja“** oder **„nein“**. Beim Erstellen eines Ergebnisauswerter-Datensatzes stehen nur Fähigkeiten zur Auswahl, für die ein Workflow konfiguriert, das Kontrollkästchen **Ist aufgabenbasierte Fähigkeit** aktiviert und eine Aufgabeneingabevariable festgelegt ist.

Zu den Workflow-Prozessaktivitäten gehören:

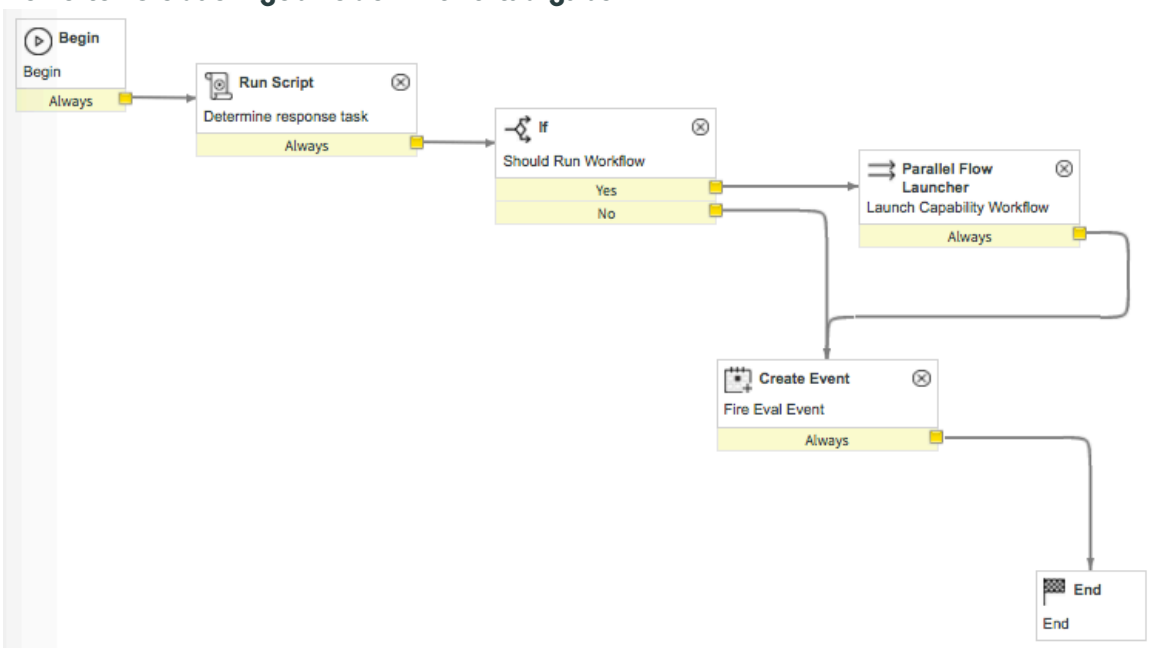
Skript ausführen, um die Antwortaufgabe zu bestimmen

Sollte Workflow ausführen

Workflow für Startfunktionalität des Startprogramms für parallele Flows

Auswertungsereignis erstellen

Bewerten Sie das Ergebnis der Antwortaufgabe



Workflow-Vorlagen für Security Incident Response

Mit Security Incident Response Orchestration werden Workflow-Vorlagen bereitgestellt, mit denen Sie grundlegende Analyseverfahren im Zusammenhang mit dem Sicherheitsvorgang durchführen können. Die Vorlagen können unverändert verwendet werden, oder Sie können sie anpassen, um Workflows zu erstellen, die Ihren spezifischen Anforderungen besser entsprechen. Die Workflow-Vorlagen sind standardmäßig deaktiviert.

Nur Benutzer mit der Rolle sn_sec_cmn.admin können den Workflow-Editor verwenden.

Workflow-Vorlage „Gefahrenpotenzial vertraulicher Daten durch Security Incident“.

Mit der Vorlage „Security Incident – Offenlegung vertraulicher Daten –“ können Sie eine Reihe von Aufgaben ausführen, die darauf ausgelegt sind, mit der Offenlegung vertraulicher Daten umzugehen.

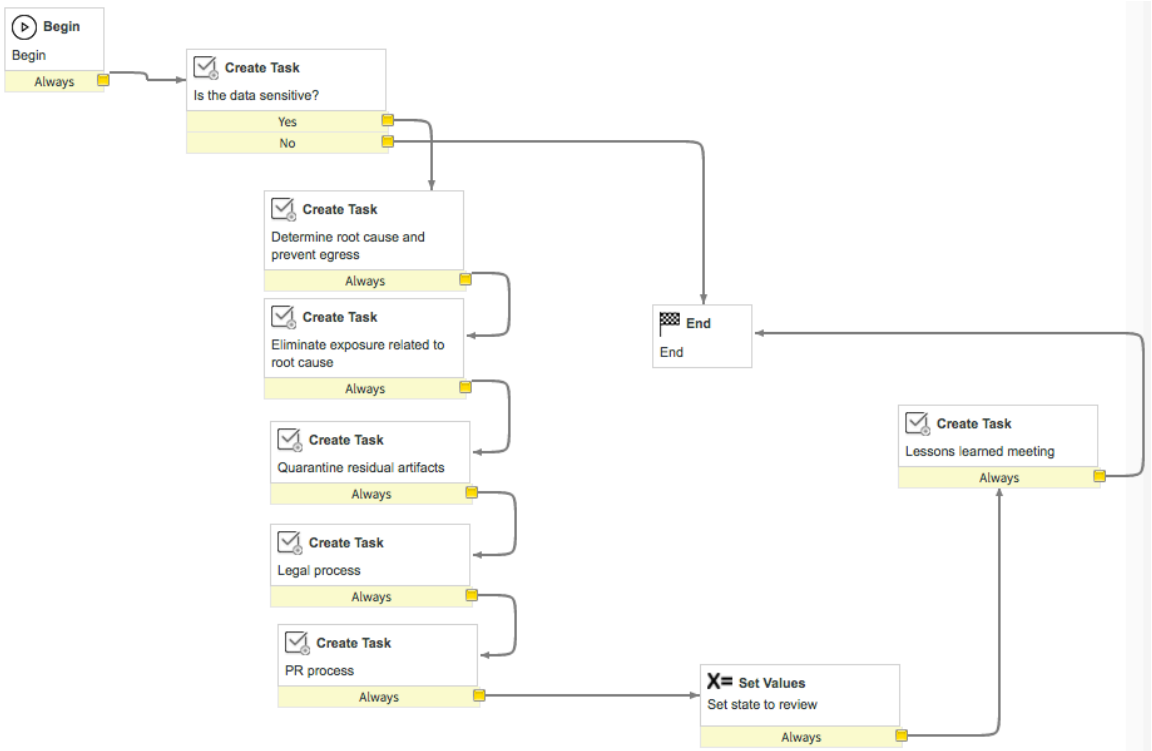
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Offenlegung vertraulicher personenbezogener Daten**festgelegt oder geändert wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Offenlegung von vertraulichen persönlichen Daten



Prozedur
1. Öffnen Sie den Security Incident, für den Sie das Risiko vertraulicher Daten behandeln möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieOffenlegung vertraulicher personenbezogener Daten**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in Vorlage für vertrauliche Daten

Antwortaufgabe	Beschreibung	Ergebnisse
Sind die Daten vertraulich?	Stellen Sie fest, ob die diesem Security Incident zugeordneten Daten vertraulich oder vertraulich sind. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**ausgewählt haben, wird die nächste Antwortaufgabe ausgeführt. Wenn Sie **Nein**ausgewählt haben, wird der Flow beendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Beschreibung	Ergebnisse
Bestimmen Sie die Ursache und verhindern Sie das Verlassen	Ermitteln Sie die Ursache des Angriffs, fügen Sie eine Ausgangsfilterung hinzu, um die Exfilterung zu stoppen, und aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Beseitigen Sie das Risiko im Zusammenhang mit der Ursache	Führen Sie basierend auf der Ursache die Schritte zur Beseitigung des Risikos aus, indem Sie das Feld **„Status“** in der Aufgabe entsprechend aktualisieren.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Restartefakte unter Quarantäne stellen	Führen Sie die Schritte aus, um alle Restartefakte unter Quarantäne zu stellen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Rechtliches Verfahren	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
PR-Prozess	Führen Sie die Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.
Meeting mit gelernten Lektionen	Führen Sie eine Besprechung mit gelernten Lektionen durch, um die mit diesen vertraulichen Daten durchgeführte Arbeit zu selektieren, und aktualisieren Sie das Feld **„Status“** in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, bleibt der Security Incident im Status **Überprüfen**, bis Sie ihn schließen.

Workflow-Vorlage „Security Incident Denial of Service“.

Mit der Vorlage „Security Incident – Denial of Service –“ können Sie eine Reihe von Aufgaben ausführen, die Denial of Service-Angriffe (DOS) abwehren sollen.

Vorbereitungen

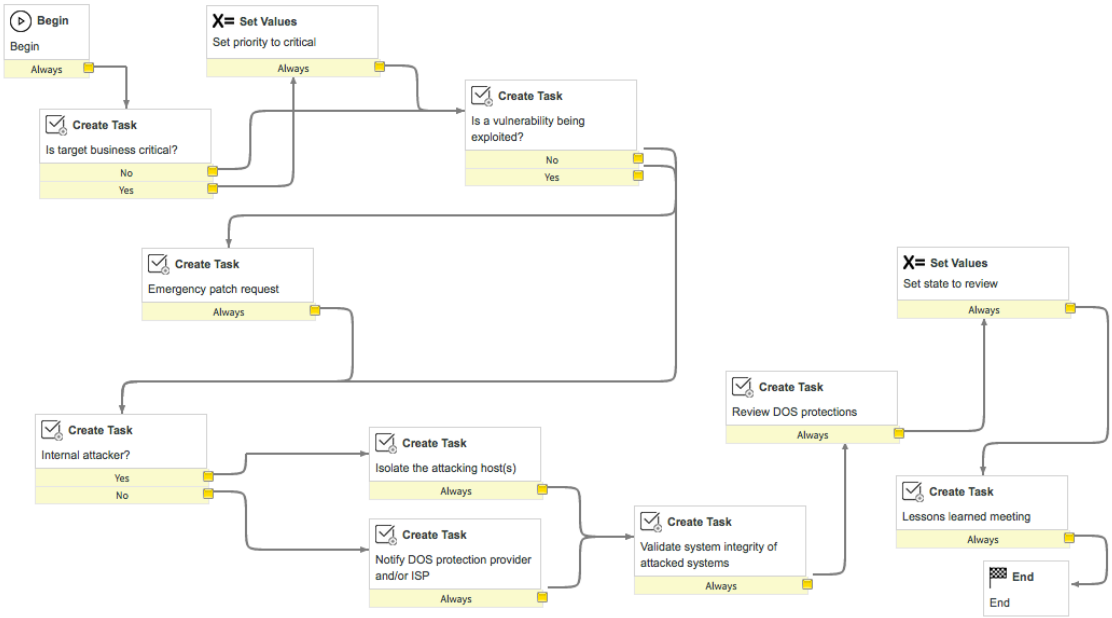
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Denial of Service**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Denial of Service (DOS)



Prozedur

1. Öffnen Sie den Security Incident für diesen Denial of Service-Vorfall, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieDenial of Service**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in der Denial of Service-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Ist Zielgeschäft kritisch?	Stellen Sie fest, ob das Ziel dieses DOS-Angriffs geschäftskritisch ist. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Priorität auf kritisch festlegen** ausgeführt. Wenn Sie **Nein**auswählen, **wird die Meldung Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Legen Sie die Priorität auf „Kritisch“ fest	Keine Aktion erforderlich.	Die **Priorität** des Security Incident wird automatisch in **Kritisch**geändert, und die **Frage Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Wird eine Schwachstelle ausgenutzt?	Ermitteln Sie, ob dieser DOS-Angriff eine Software-Schwachstelle ausnutzt.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Notfall-Patch-Anforderung** ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie in der Aufgabe unter **Ergebnis**Ja oder **Nein**aus.	Wenn Sie **Nein**auswählen, wird das **Feld Interner Angreifer?** Aufgabe wird ausgeführt.
Notfall-Patch-Anforderung	Notfall-Patch-Anforderung für angegriffene Systeme ausgeben. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Interner Angreifer?	Stellen Sie fest, ob die Quelle dieses DOS-Angriffs eine interne Quelle für Ihre Organisation ist. Wählen Sie in der Aufgabe unter **Ergebnis**Ja oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Angreifende(n) Host(s) isolieren** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **Notify DOS-Schutzanbieter und/oder ISP** ausgeführt.
Die angreifenden Hosts isolieren	Führen Sie die erforderlichen Schritte aus, um die internen Hosts zu isolieren, die für den Angriff verantwortlich sind. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Nachdem Sie diesen Schritt abgeschlossen haben, wird die Aufgabe **Systemintegrität angegriffener Systeme validieren** ausgeführt.
DOS-Schutzanbieter und/oder ISP benachrichtigen	Führen Sie die erforderlichen Schritte aus, um Ihren Denial of Service-Schutzanbieter und/oder Ihren Internet Service Provider zu kontaktieren und sie über den Angriff zu benachrichtigen. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Validiert die Systemintegrität angegriffener Systeme	Führen Sie die erforderlichen Schritte aus, um die Integrität der angegriffenen Computer zu bewerten und zu validieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Überprüfen Sie die DOS-Schutzmaßnahmen	Führen Sie eine Überprüfung Ihrer vorhandenen DOS-Schutzmaßnahmen und -Verfahren durch. Führen Sie alle erforderlichen Änderungen durch. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Denial of Service-Incident durchgeführte Arbeit zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet.

Workflow-Vorlage „Security Incident Lost Equipment“.

Mit der Vorlage „Security Incident – Verlorene Geräte –“ können Sie eine Reihe von Aufgaben ausführen, die speziell für den Umgang mit verlorenen Geräten entwickelt wurden.

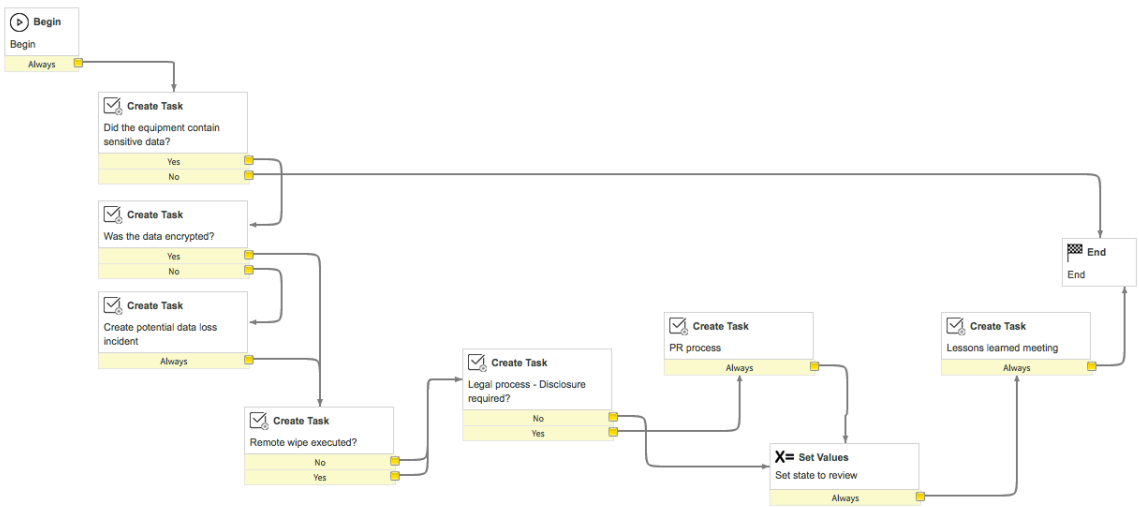
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Geräteverlust**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Geräteverlust



Prozedur

1. Öffnen Sie den Security Incident für den Geräteverlust, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieGeräteverlust**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in Vorlage für verlorene Geräte

Antwortaufgabe	Aktion	Ergebnisse
Enthält das Gerät vertrauliche Daten?	Stellen Sie fest, ob die Geräte, die diesem Security Incident zugeordnet sind, vertrauliche oder vertrauliche Informationen enthalten. Wählen Sie in der Aufgabe je nach Bedarf **Ja** oder **Nein** unter **Ergebnis** aus.	Wenn Sie **Ja** auswählen, **wurden die Daten verschlüsselt?** Aufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird der Flow beendet.
Wurden die Daten verschlüsselt?	Stellen Sie fest, ob die vertraulichen Daten auf dem verlorenen Gerät verschlüsselt wurden. Wählen Sie in der Aufgabe je nach Bedarf **Ja** oder **Nein** unter **Ergebnis** aus.	Wenn Sie **Ja**auswählen, wird die **Remotelöschung erstellt?** Antwortaufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird die Antwortaufgabe **Incident mit potenziellem Datenverlust erstellen**ausgeführt.
Erstellen Sie einen Incident mit potenziellem Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Incident vom Typ „Potenzieller Datenverlust“ zu erstellen. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt.
Remotelöschung erstellt?	Führen Sie die erforderlichen Schritte aus, um eine Remote-Löschung der verlorenen Geräte auszuführen. Wählen Sie in der Aufgabe je nach Bedarf **Ja** oder **Nein** unter **Ergebnis** aus.	Die Aufgabe **„Rechtlicher Prozess – Offenlegung erforderlich“** wird ausgeführt.
Rechtliches Verfahren – Offenlegung erforderlich?	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen. Wählen Sie **„Ja“**, wenn eine rechtliche Offenlegung erforderlich ist, **„Nein“**, wenn dies nicht der Fall ist.	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die Aufgabe **„Status auf Überprüfung festlegen“** wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Legen Sie den Status auf „Überprüfung“ fest	Es ist keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Incident mit verlorenem Gerät durchgeführten Arbeiten zu selektieren. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Der Flow endet.

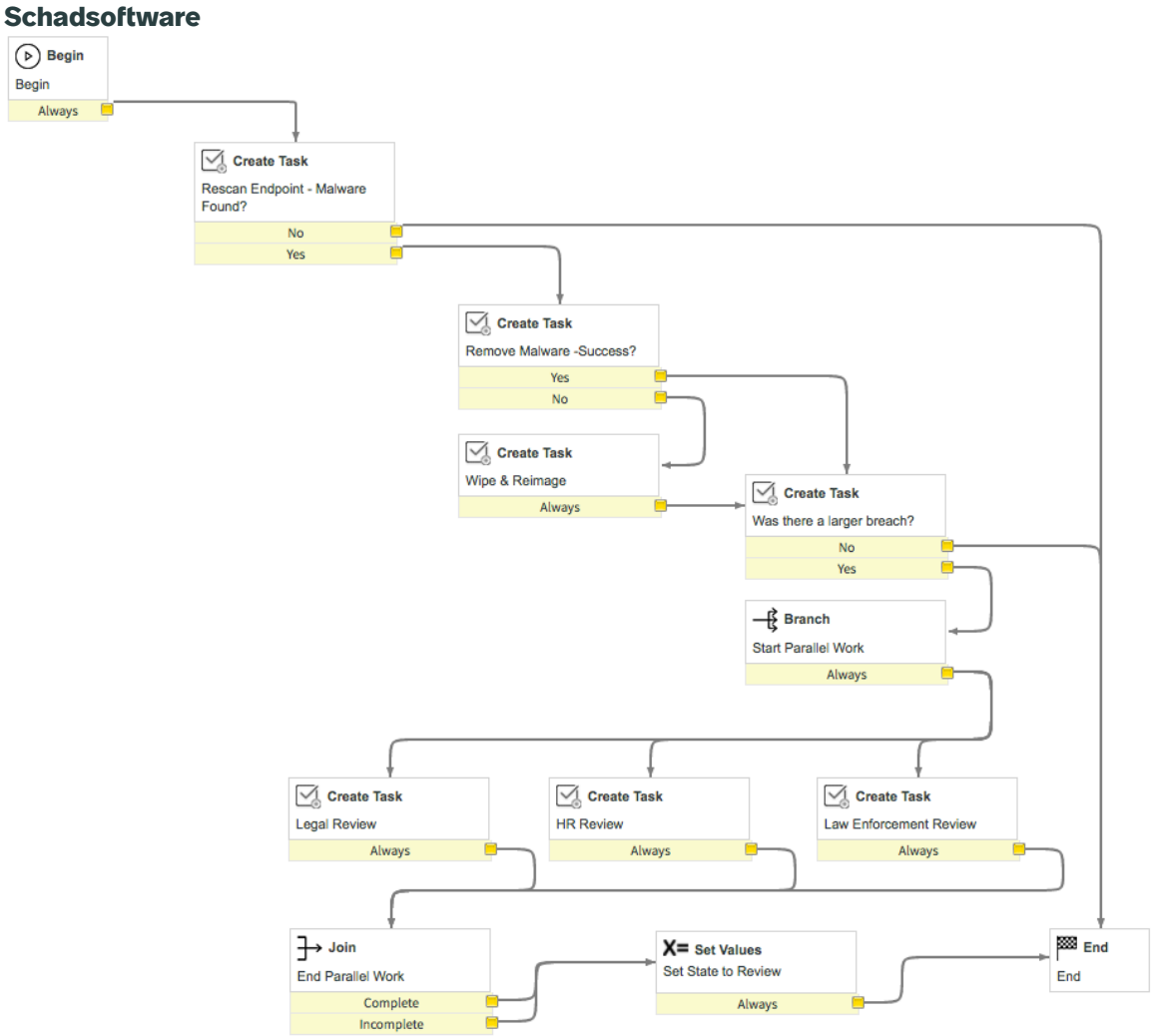
Workflow-Vorlage für böswillige Software für Security Incidents

Mit der Vorlage „Security Incident – Schadsoftware – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die Schadsoftware in Ihrem Netzwerk behandeln.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Böswillige Software**festgelegt ist. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieBöswilliger Code Aktivität**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

Antwortaufgaben in Vorlage für schädliche Software

Antwortaufgabe	Aktion	Ergebnisse
Endpunkt scannen – Malware gefunden?	Bestimmen Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die **Meldung Malware entfernen – Erfolg?** Aufgabe wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Wenn Sie **Nein**auswählen, wird der Flow beendet.
Malware entfernen – Erfolg?	Stellen Sie fest, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, **wird im Feld Gab es einen größeren Verstoß?** Aufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **Löschen und erneut erstellen** ausgeführt.
Löschen und erneut erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie im Rahmen dieser Aufgabe aufgefordert, auf den mit der Malware infizierten Computern einen Löschvorgang und ein erneutes Image durchzuführen.	Nachdem die Aufgabe abgeschlossen wurde, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Gab es einen größeren Verstoß?	Stellen Sie fest, ob der durch die Schadsoftware verursachte Verstoß größer ist als zuerst angenommen. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, werden die folgenden Aufgaben parallel ausgeführt: ○ Rechtliche Überprüfung ○ HR-Überprüfung ○ Überprüfung der Strafverfolgung Wenn Sie **Nein**auswählen, wird der Flow beendet.
Rechtliche Überprüfung HR-Überprüfung Überprüfung der Strafverfolgung	Führen Sie für jede dieser Abteilungen die erforderlichen Schritte aus, um den Prozess zur Beseitigung der Schadsoftware zu überprüfen.	Wenn die Aufgaben abgeschlossen sind, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf Überprüfung fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Prüfung**geändert, und der Flow wird beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow-Vorlage „Security Incident – Phishing“.

Mit der Vorlage „Security Incident – Phishing –“ können Sie eine Reihe von Aufgaben ausführen, die Spear-Phishing-E-Mails in Ihrem Netzwerk behandeln.

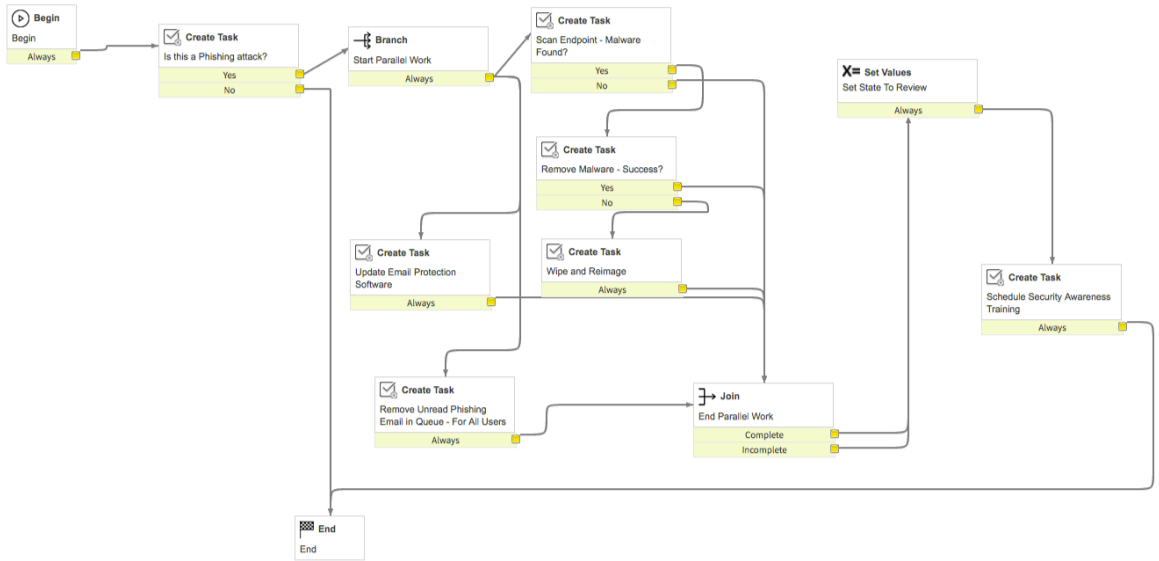
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Spear Phishing**festgelegt ist. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Spear-Phishing



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Spear-Phishing-Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieSpear Phishing**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

Antwortaufgaben in der Spear-Phishing-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Handelt es sich um einen Phishing-Angriff?	Stellen Sie fest, ob dies ein Phishing-Angriff ist. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, werden die folgenden Aufgaben parallel ausgeführt: ○ Endpunkt scannen – Malware gefunden? ○ Aktualisieren Sie die E-Mail-Schutzsoftware

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		○ Ungelesene Phishing-E-Mail aus Warteschlange entfernen – für alle Anwender Wenn Sie **Nein**auswählen, wird der Flow beendet.
Endpunkt scannen – Malware gefunden?	Bestimmen Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die **Meldung Malware entfernen – Erfolg?** Aufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Malware entfernen – Erfolg?	Stellen Sie fest, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **Löschen und erneut erstellen (Reimage)** ausgeführt.
Löschen und erneut erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie im Rahmen dieser Aufgabe aufgefordert, auf den mit der Malware infizierten Computern einen Löschvorgang und ein erneutes Image durchzuführen.	Nachdem die Aufgabe abgeschlossen wurde, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Aktualisieren Sie die E-Mail-Schutzsoftware	Wenn festgestellt wurde, dass es sich um einen Phishing-Angriff handelt, werden Sie aufgefordert, Ihre E-Mail-Schutzsoftware entsprechend zu aktualisieren.	Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Ungelesene Phishing-E-Mail aus Warteschlange entfernen – für alle Anwender	Führen Sie die erforderlichen Schritte aus, um die Phishing-E-Mail, die sich noch in der Warteschlange befindet, für alle Ihre Anwender zu entfernen.	Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf Überprüfung fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Die Aufgabe **„Schulung des Sicherheitsbewusstseins planen“** wird ausgeführt.
Planen Sie eine Schulung zum Sicherheitsbewusstsein	Planen Sie Schulungen, um das Sicherheitsbewusstsein Ihrer Mitarbeiter zu schärfen. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn die Aufgabe abgeschlossen ist, wird der Flow beendet.

Workflow-Vorlage „Verletzung der Richtlinie für Security Incidents“.

Mit der Vorlage „Security Incident – Richtlinienverletzung –“ können Sie eine Reihe von Aufgaben ausführen, die Verstöße gegen Sicherheitsrichtlinien behandeln.

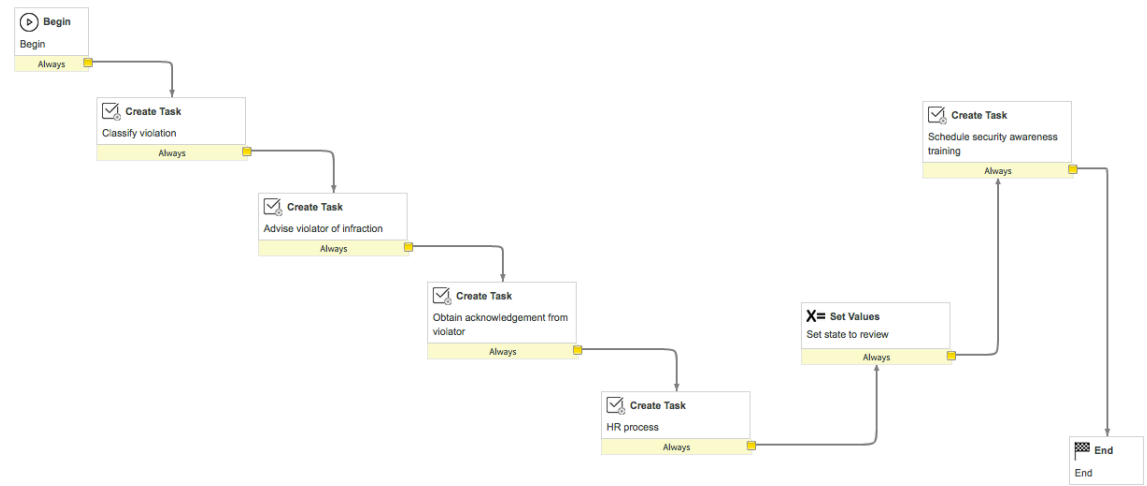
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Richtlinienverstoß**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Richtlinienverstoß



Prozedur

1. Öffnen Sie den Security Incident für den Richtlinienverstoß, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieRichtlinienverstoß**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in Richtlinienverletzungsvorlage

Antwortaufgabe	Aktion	Ergebnisse
Verstoß klassifizieren	Klassifizieren Sie, wie dieser Verstoß gegen die Sicherheitsrichtlinien Ihrer Organisation verstößt. Aktualisieren Sie das Feld **„Status“** in der Aufgabe, nachdem Sie sie abgeschlossen haben.	Die Antwortaufgabe **„Mit Verstoß melden** “ wird ausgeführt.
Den Zuwiderhandelnden über den Verstoß informieren	Teilen Sie dem Verletzer die Art des Verstoßes mit. Aktualisieren Sie das Feld **„Status“** in der Aufgabe, nachdem Sie ihn mitgeteilt haben.	Die Aufgabe **„Bestätigung von Antwort auf Verstoß** einholen“ wird ausgeführt.
Bestätigung vom Verletzer einholen	Fordern Sie eine Bestätigung vom Verletzer des Verstoßes an. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Die **HR-Prozessantwortaufgabe** wird ausgeführt.
HR-Prozess	Teilen Sie HR alle erforderlichen Informationen zu diesem Verstoß mit. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Die Aufgabe **„Status auf Antwort überprüfen“ festlegen** wird ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Es ist keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.
Planen Sie eine Schulung zum Sicherheitsbewusstsein	Führen Sie eine Schulung zum Sicherheitsbewusstsein durch, um die Mitarbeiter zu schulen, wie ähnliche Sicherheitsverletzungen in Zukunft verhindert werden können. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet.

Workflow-Vorlage für Security Incident Reconnaissance

Erkennung ist normalerweise ein vorläufiger Schritt zu einem weiteren Angriff, der ein Gerät oder System ausnutzen soll. Mit der Vorlage „Security Incident - Reconnaissance - Security Incident“ können Sie eine Reihe von Aufgaben ausführen, um die Erkennung in Ihrem Netzwerk zu verarbeiten.

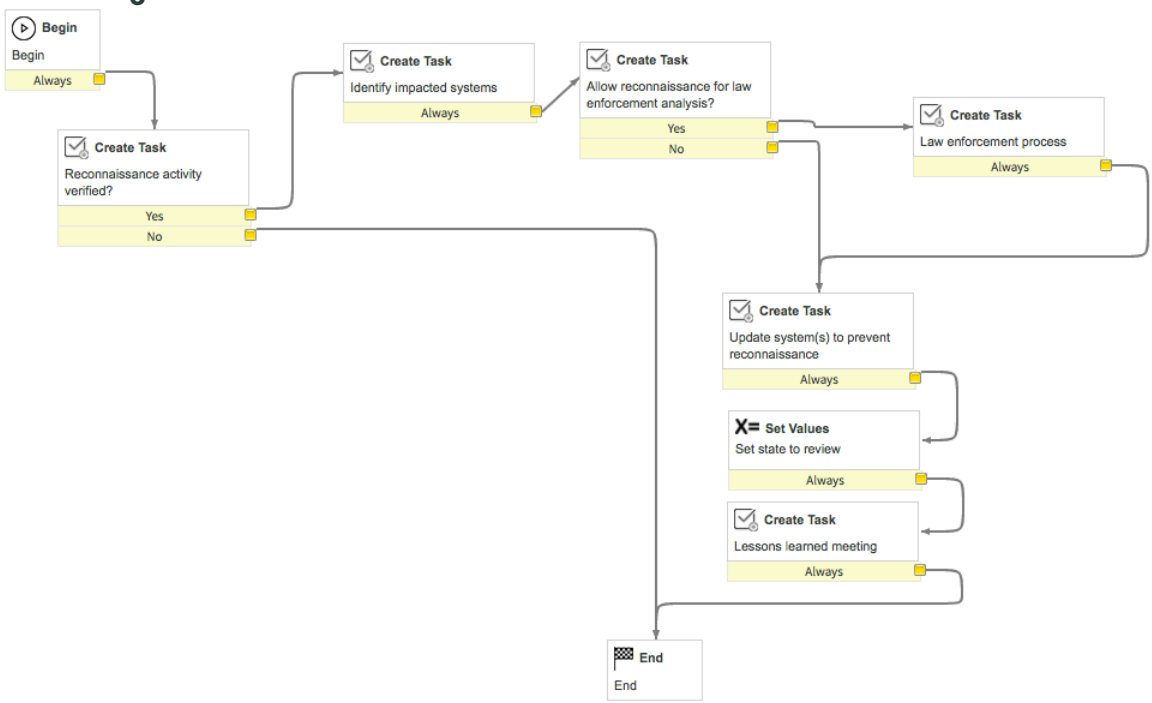
Vorbereitungen
Erforderliche Rolle: sn_si.write

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Aufklärungsaktivität**festgelegt ist. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Aufklärungsaktivität



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategoriedie Option Aufklärungsaktivität**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

Antwortaufgaben in der Aufklärungsvorlage

Antwortaufgabe	Aktion	Ergebnisse
Aufklärungsaktivität verifiziert?	Stellen Sie fest, ob eine beobachtete Aufklärung verifiziert wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Betroffene Systeme identifizieren** ausgeführt. Wenn Sie **Nein**auswählen, wird der Flow beendet.
Identifizieren Sie die betroffenen Systeme	Bestimmen Sie die Systeme, die von der Erkennung betroffen sind.	Wenn diese Aufgabe abgeschlossen ist, **wird im Feld „Aufklärung für Strafverfolgungsanalysen zulassen?“** angezeigt. Aufgabe wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Aufklärung für Strafverfolgungsanalysen zulassen?	Legen Sie fest, ob die Aufklärung von Strafverfolgungsbehörden analysiert werden soll. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **des Strafverfolgungsprozesses** ausgeführt. Wenn Sie **Nein**auswählen, wird die **Aufgabe Systeme aktualisieren, um eine Spähen zu verhindern** ausgeführt.
Strafverfolgungsprozess	Führen Sie den von Ihrem Unternehmen definierten Strafverfolgungsprozess durch.	Wenn diese Aufgabe abgeschlossen ist, wird die **Aufgabe „System(e) aktualisieren, um eine Aufklärung zu verhindern** “ ausgeführt.
Aktualisieren Sie die Systeme, um eine Erkennung zu verhindern	Führen Sie die erforderlichen Schritte aus, um die von der Erkennung betroffenen Systeme zu aktualisieren.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit den gelernten Lektionen durch, um die für diesen Erkennungs-Incident durchgeführte Arbeit zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn diese Aufgabe abgeschlossen ist, wird der Flow beendet.

Workflow-Vorlage für Security Incident Rogue-Server oder -Service

Mit der Vorlage „Security Incident – Rogue-Server oder -Service –“ können Sie eine Reihe von Aufgaben ausführen, die darauf abzielen, Aktivitäten von betrügerischen Servern oder Services zu handhaben, die sich auf Ihr Netzwerk auswirken.

Vorbereitungen

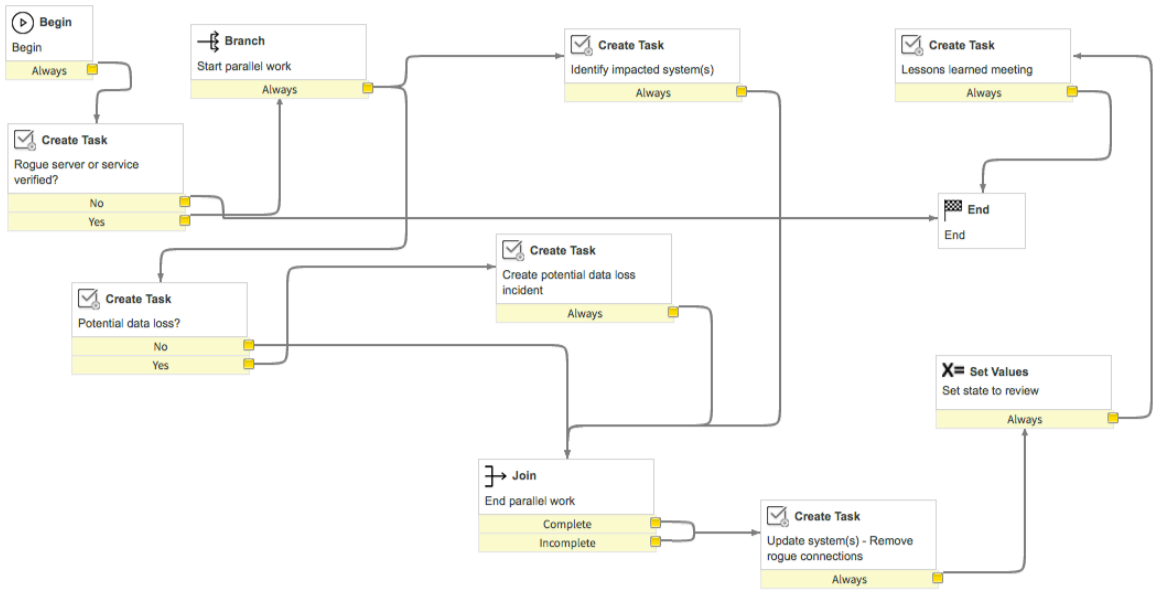
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Nicht autorisierter Server oder Service**festgelegt ist. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht autorisierter Server oder Service



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategoriedie Option Nicht autorisierter Server oder Serviceaktivität**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

Antwortaufgaben in Rogue-Server oder Servicevorlage

Antwortaufgabe	Aktion	Ergebnisse
Betrügerischer Server oder Service verifiziert?	Ermitteln Sie, ob in Ihrem Netzwerk eine Verbindung mit einem nicht autorisierten Server oder Service verifiziert wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, werden die folgenden beiden Aufgaben parallel ausgeführt: ○ **Betroffene Systeme identifizieren** ○ **Potenzieller Datenverlust?** Wenn Sie **Nein**auswählen, wird der Flow beendet.
Betroffene Systeme identifizieren	Ermitteln Sie die Systeme, die durch den Kontakt mit dem nicht autorisierten Server oder Service betroffen sind.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt.
Potenzieller Datenverlust?	Stellen Sie fest, ob die Verbindung mit dem nicht autorisierten Server oder Service potenziellen Datenverlust verursacht hat. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident mit potenziellem Datenverlust erstellen** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **System(e) aktualisieren –**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Nicht autorisierte Verbindungen entfernen ausgeführt.
Erstellen Sie einen Incident mit potenziellem Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den potenziellen Datenverlust zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt.
Systeme aktualisieren: Nicht autorisierte Verbindungen entfernen	Führen Sie die erforderlichen Schritte aus, um die nicht autorisierten Verbindungen zu entfernen.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen betrügerischen Server- oder Service-Incident durchgeführten Arbeiten zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn diese Aufgabe abgeschlossen ist, wird der Flow beendet.

Workflow-Vorlage „Security Incident Spam“.

Mit der Vorlage „Security Incident – Spam – Template“ können Sie eine Reihe von Aufgaben zur Behandlung von E-Mail-Spam in Ihrem Netzwerk ausführen.

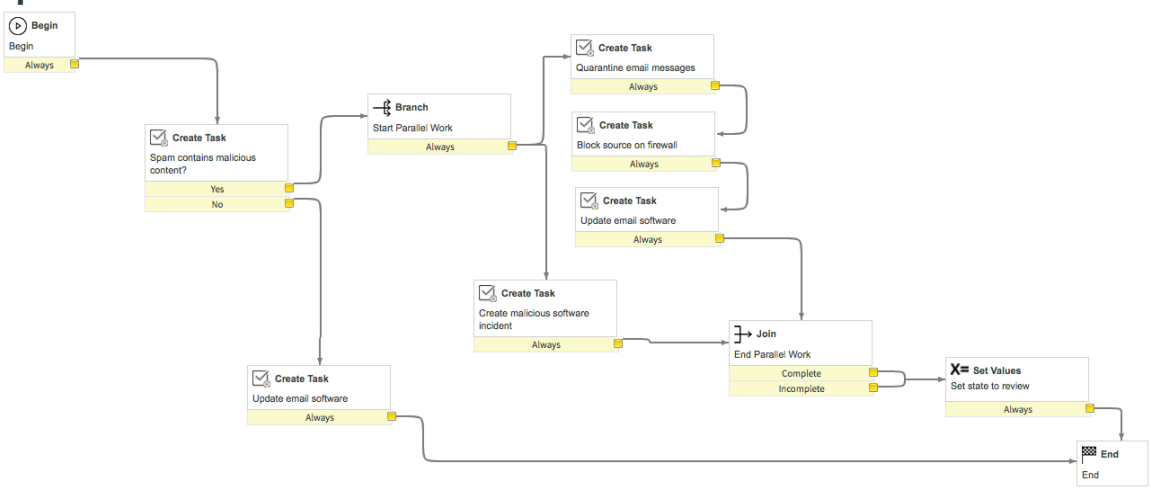
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident in **Spam-Quelle**festgelegt oder geändert wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Spam-Quelle



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie den Security Incident, für den Sie E-Mail-Spam behandeln möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieSpam-Quelle**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

Antwortaufgaben in der Spam-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Enthält Spam schädliche Inhalte?	Stellen Sie fest, ob der Spam schädliche Software enthält. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**ausgewählt haben, werden die folgenden Antwortaufgaben ausgeführt: ○ **E-Mail-Nachricht in Quarantäne stellen** ○ **Erstellen Sie einen Incident für schädliche Software** Wenn Sie **Nein**ausgewählt haben, wird die **Aktualisierung der E-Mail-Software** ausgeführt.
Erstellen Sie einen Incident für schädliche Software	Führen Sie die Schritte zum Erstellen eines Security Incident aus, und aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wartet diese Antwortaufgabe, bis die nächsten drei Antwortaufgaben abgeschlossen sind. Der Status des Security Incident wechselt dann zu **Überprüfen**.
E-Mail-Nachricht in Quarantäne stellen	Führen Sie die Schritte aus, um den Spam unter Quarantäne zu stellen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Quelle in Firewall blockieren	Führen Sie die Schritte zum Blockieren der E-Mail-Adresse in der Firewall aus, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Aktualisieren Sie die E-Mail-Software	Fügen Sie die E-Mail-Adresse Ihrer Sperrliste hinzu, und aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. **Hinweis:** Diese Antwortaufgabe wird auch ausgeführt, wenn Sie die Frage mit **„Enthält Spam schädlichen Inhalt?“mit „Nein“** beantwortet haben. Antwortaufgabe.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.

Workflow-Vorlage für nicht autorisierten Zugriff auf Security Incidents

Mit der Vorlage „Security Incident – Unautorisierter Zugriff – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, um nicht autorisierten Zugriff auf Ihr Netzwerk zu handhaben.

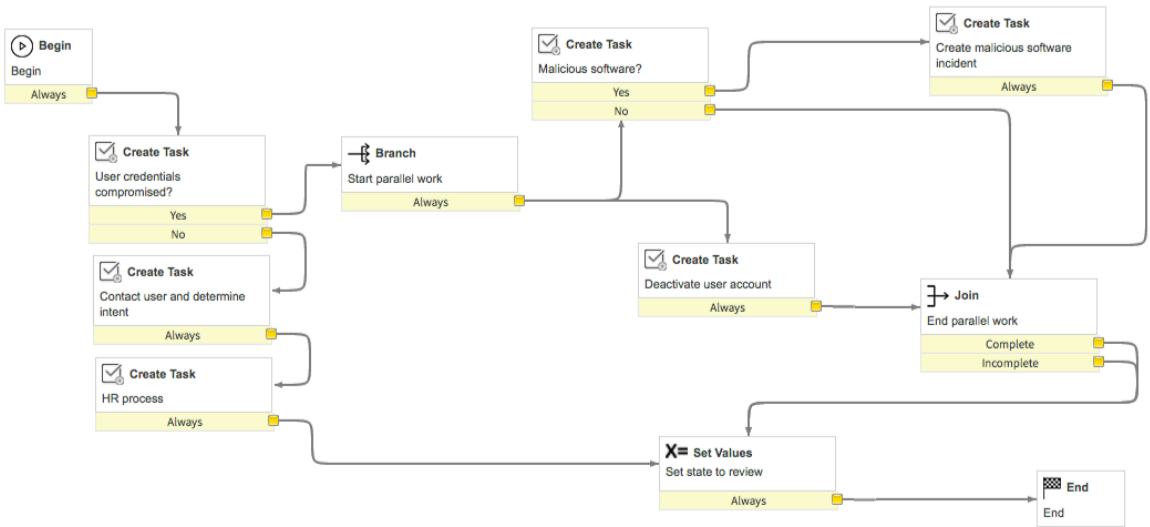
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Nicht autorisierter Zugriff**festgelegt ist. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Nicht autorisierter Zugriff



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategoriedie Option Nicht autorisierter Zugriff**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

Antwortaufgaben in Vorlage für nicht autorisierten Zugriff

Antwortaufgabe	Aktion	Ergebnisse
Sind die Benutzeranmeldeinformationen kompromittiert?	Stellen Sie fest, ob die Anmeldeinformationen von Anwendern gefährdet wurden.	Wenn Sie **Ja**auswählen, werden die folgenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie in der Aufgabe unter **Ergebnis**Ja oder **Nein**aus.	beiden Aufgaben parallel ausgeführt: ○ **Schädliche Software?** ○ **Anwender-Account deaktivieren** Wenn Sie **Nein**auswählen, wird die Aufgabe **Anwender kontaktieren und Absicht bestimmen** ausgeführt.
Schädliche Software?	Stellen Sie fest, ob der nicht autorisierte Zugriff zur Einführung schädlicher Software geführt hat. Wählen Sie in der Aufgabe unter **Ergebnis**Ja oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident für schädliche Software erstellen** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Erstellen Sie einen Incident für schädliche Software	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den nicht autorisierten Zugriff zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Anwender-Account deaktivieren	Führen Sie die erforderlichen Schritte aus, um das gefährdete Anwenderaccount zu deaktivieren.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Kontaktieren Sie den Anwender, und bestimmen Sie die Absicht	Führen Sie die erforderlichen Schritte aus, um den Anwender zu kontaktieren, der für den nicht autorisierten Zugriff verantwortlich ist, und ermitteln Sie den Grund für den Zugriffsversuch.	Wenn diese Aufgabe abgeschlossen ist, wird die **HR-Prozessaufgabe** ausgeführt.
HR-Prozess	Führen Sie die erforderlichen Schritte aus, um die Personalabteilung zu kontaktieren und gegebenenfalls Disziplinarmaßnahmen durchzuführen.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Prüfung**geändert, und der Flow wird beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow-Vorlage für Web/BBS-Defacement für Security Incidents

Mit der Vorlage „Security Incident – Web/BBS-Defacement“ können Sie eine Reihe von Aufgaben ausführen, um Vandalismus zu handhaben, der sich gegen eine der BBS-Websites oder Websites Ihres Unternehmens richtet.

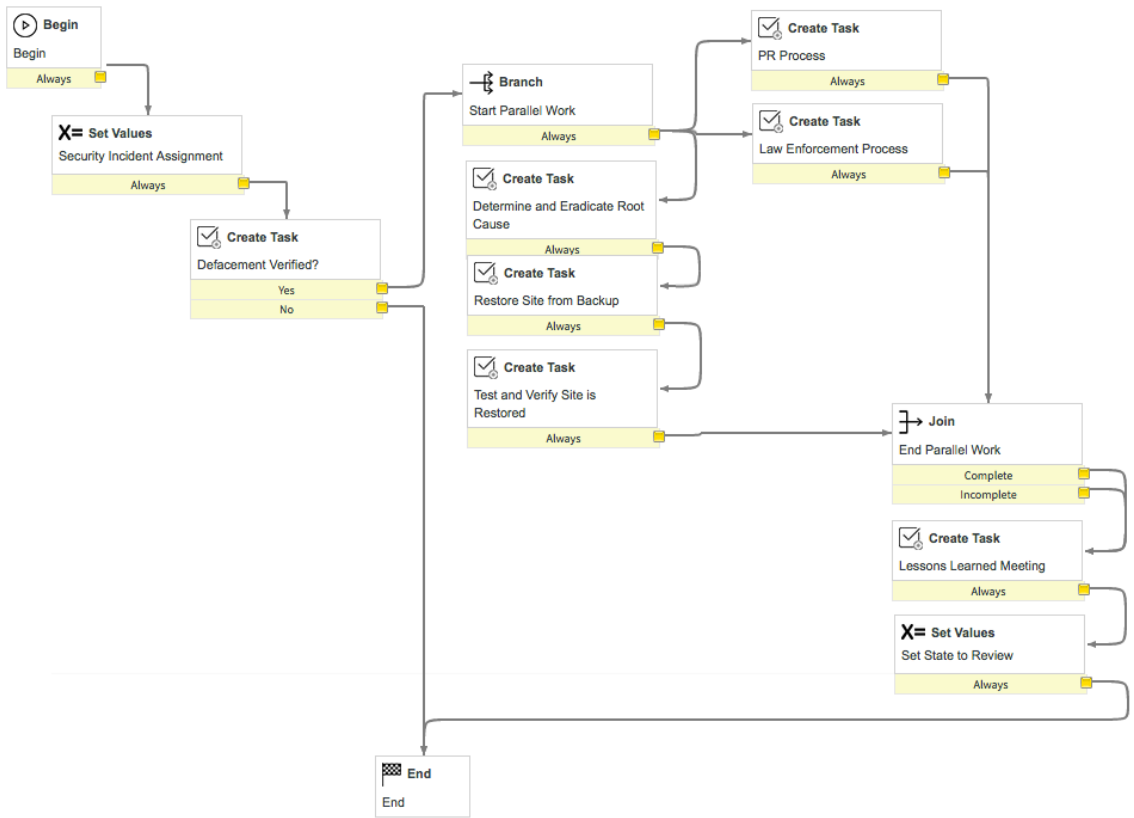
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Web/BBS-Defacement**festgelegt ist. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Unleserlichmachen von Web/BBS



Prozedur

1. Öffnen Sie den Security Incident für dieses Vorkommen der Web- oder BBS-Unleserlichkeit, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieWeb/BBS-Defacement**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in Web/BBS-Defacement-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Zuweisung von Security Incidents	Erstellen Sie einen Security Incident für jeden gemeldeten Incident von Website- oder BBS-Unleserlichmachen.	Die nächste Antwortaufgabe wird ausgeführt.
Unformatierung verifiziert?	Stellen Sie fest, ob die Website oder BBS tatsächlich unleserlich gemacht wurde. Wählen Sie in der Aufgabe unter **Ergebnis** **Ja** oder **Nein** aus.	Wenn Sie **Ja** auswählen, werden die folgenden Antwortaufgaben ausgeführt: ○ **PR-Prozess** ○ **Strafverfolgungsprozess** ○ **Ursache ermitteln und beseitigen** Wenn Sie **Nein** auswählen, wird der Flow beendet.
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die Öffentlichkeit darüber zu informieren, dass die Website oder BBS unkenntlich gemacht wurde. Wenn Sie mit dem PR-Prozess fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Strafverfolgungsprozess	Führen Sie die erforderlichen Schritte aus, um die entsprechenden Strafverfolgungsbehörden bezüglich des Angriffs einzuschalten. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Ursache ermitteln und beseitigen	Führen Sie die erforderlichen Schritte aus, um die Ursache der Unleserlichkeit zu erkennen und zu beseitigen. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen** geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Site aus Sicherung wiederherstellen	Führen Sie die erforderlichen Schritte zum Sichern und Wiederherstellen der Website oder des BBS durch. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen** geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Testen und überprüfen Sie, ob die Site wiederhergestellt ist	Stellen Sie sicher, dass die Site wiederhergestellt ist.	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Website-/BBS-Unleserlichmachen-Incident durchgeführten Arbeiten zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **storniert**ändern, wird die Aufgabe **Status auf Überprüfung** festlegen ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. Der Flow endet.

Flow-Vorlagen für Security Incident Response

Das -Basissystem Security Incident Response enthält eine Reihe von Workflow-Vorlagen, die mit dem Flow Designer erstellt wurden und für die Verarbeitung von Security Incident-Datensätzen geeignet sind.

Nur Anwender mit der Rolle „sn_sec_cmn.admin“ können Security Operations-Workflow-Vorlagen hinzufügen oder bearbeiten. Zum Aktualisieren der Flow-Vorlagen sind Anwender mit der Rolle „sn_si_admin“ erforderlich.

Wichtige Aktivierungsinformationen

Die mit dem Workflow-Editor erstellten Workflow-Vorlagen und die mit dem Flow Designer erstellten Flow-Vorlagen sind standardmäßig deaktiviert. Die Workflow-Vorlagen können mithilfe von Workflow-Auslösernaktiviert werden. Flow Designer-Vorlagen können mit Flow Designer aktiviert werden.

Hinweis:
Sie müssen darauf achten, nicht für jeden Typ dieselbe Vorlage zu aktivieren. Vermeiden Sie beispielsweise die Aktivierung von Workflow-Vorlage „Gefahrenpotenzial vertraulicher Daten durch Security Incident“. und Flow-Vorlage für das Risiko vertraulicher Daten durch Security Incidents. Dies kann zur Ausführung des Workflows und des Flow sowie zur Erstellung von doppelten Informationen führen.

Flow-Vorlage für das Risiko vertraulicher Daten durch Security Incidents

Mit der Vorlage „Security Incident – Offenlegung vertraulicher Daten –“ können Sie eine Reihe von Aufgaben ausführen, die darauf ausgelegt sind, mit der Offenlegung vertraulicher Daten umzugehen.

Vorbereitungen
Erforderliche Rolle: sn_si.write

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Offenlegung vertraulicher personenbezogener Daten**festgelegt oder geändert wird.

Prozedur

1. Öffnen Sie den Security Incident, für den Sie das Risiko vertraulicher Daten behandeln möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieOffenlegung vertraulicher personenbezogener Daten**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Ausführung der nächsten Antwortaufgabe oder das Beenden des Flows.

Antwortaufgaben in Vorlage für vertrauliche Daten

Antwortaufgabe	Beschreibung	Ergebnisse
Sind die Daten vertraulich?	Stellen Sie fest, ob die diesem Security Incident zugeordneten Daten vertraulich oder vertraulich sind. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**ausgewählt haben, wird die nächste Antwortaufgabe ausgeführt. Wenn Sie **Nein**ausgewählt haben, wird der Flow beendet.
Bestimmen Sie die Ursache und verhindern Sie das Verlassen	Ermitteln Sie die Ursache des Angriffs, fügen Sie eine Ausgangsfilterung hinzu, um die Exfilterung zu stoppen, und aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Beseitigen Sie das Risiko im Zusammenhang mit der Ursache	Führen Sie basierend auf der Ursache die Schritte zur Beseitigung des Risikos aus, indem Sie das Feld **„Status“** in der Aufgabe entsprechend aktualisieren.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Restartefakte unter Quarantäne stellen	Führen Sie die Schritte aus, um alle Restartefakte unter Quarantäne zu stellen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Rechtliches Verfahren	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
PR-Prozess	Führen Sie die Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Beschreibung	Ergebnisse
Meeting mit gelernten Lektionen	Führen Sie eine Besprechung mit gelernten Lektionen durch, um die mit diesen vertraulichen Daten durchgeführte Arbeit zu selektieren, und aktualisieren Sie das Feld **„Status“** in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, bleibt der Security Incident im Status **Überprüfen**, bis Sie ihn schließen.

Flow-Vorlage für Denial of Service für Security Incidents

Mit der Vorlage „Security Incident – Denial of Service –“ können Sie eine Reihe von Aufgaben ausführen, die Denial of Service-Angriffe (DOS) abwehren sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Denial of Service**festgelegt wird.

Prozedur

1. Öffnen Sie den Security Incident für diesen Denial of Service-Vorfall, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieDenial of Service**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Bei jeder Speicherung des Datensatzes bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Workflows.

Antwortaufgaben in der Denial of Service-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Ist Zielgeschäft kritisch?	Stellen Sie fest, ob das Ziel dieses DOS-Angriffs geschäftskritisch ist. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Priorität auf kritisch festlegen** ausgeführt. Wenn Sie **Nein**auswählen, **wird die Meldung Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Legen Sie die Priorität auf „Kritisch“ fest	Keine Aktion erforderlich.	Die **Priorität** des Security Incident wird automatisch in **Kritisch**geändert, und die **Frage Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Wird eine Schwachstelle ausgenutzt?	Ermitteln Sie, ob dieser DOS-Angriff eine Software-Schwachstelle ausnutzt. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Notfall-Patch-Anforderung** ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Wenn Sie **Nein**auswählen, wird das **Feld Interner Angreifer?** Aufgabe wird ausgeführt.
Notfall-Patch-Anforderung	Notfall-Patch-Anforderung für angegriffene Systeme ausgeben. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Interner Angreifer?	Stellen Sie fest, ob die Quelle dieses DOS-Angriffs eine interne Quelle für Ihre Organisation ist. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Angreifende(n) Host(s) isolieren** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **Notify DOS-Schutzanbieter und/oder ISP** ausgeführt.
Die angreifenden Hosts isolieren	Führen Sie die erforderlichen Schritte aus, um die internen Hosts zu isolieren, die für den Angriff verantwortlich sind. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Nachdem Sie diesen Schritt abgeschlossen haben, wird die Aufgabe **Systemintegrität angegriffener Systeme validieren** ausgeführt.
DOS-Schutzanbieter und/oder ISP benachrichtigen	Führen Sie die erforderlichen Schritte aus, um Ihren Denial of Service-Schutzanbieter und/oder Ihren Internet Service Provider zu kontaktieren und sie über den Angriff zu benachrichtigen. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Validiert die Systemintegrität angegriffener Systeme	Führen Sie die erforderlichen Schritte aus, um die Integrität der angegriffenen Computer zu bewerten und zu validieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Überprüfen Sie die DOS-Schutzmaßnahmen	Führen Sie eine Überprüfung Ihrer vorhandenen DOS-Schutzmaßnahmen und -Verfahren durch. Führen Sie alle erforderlichen Änderungen durch. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Denial of Service-Incident durchgeführte Arbeit zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet.

Flow-Vorlage für verlorene Geräte durch Security Incident

Mit der Vorlage „Security Incident – Verlorene Geräte –“ können Sie eine Reihe von Aufgaben ausführen, die speziell für den Umgang mit verlorenen Geräten entwickelt wurden.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Geräteverlust**festgelegt wird.

Prozedur

1. Öffnen Sie den Security Incident für diesen Denial of Service-Vorfall, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieGeräteverlust**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in Vorlage für verlorene Geräte

Antwortaufgabe	Aktion	Ergebnisse
Enthält das Gerät vertrauliche Daten?	Stellen Sie fest, ob die Geräte, die diesem Security Incident zugeordnet sind, vertrauliche oder vertrauliche Informationen enthalten. Wählen Sie in der Aufgabe je nach Bedarf **Ja** oder **Nein** unter **Ergebnis** aus.	Wenn Sie **Ja** auswählen, **wurden die Daten verschlüsselt?** Aufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird der Flow beendet.
Wurden die Daten verschlüsselt?	Stellen Sie fest, ob die vertraulichen Daten auf dem verlorenen Gerät verschlüsselt wurden.	Wenn Sie **Ja**auswählen, wird die **Remotelöschung erstellt?** Antwortaufgabe wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie in der Aufgabe je nach Bedarf **Ja** oder **Nein** unter **Ergebnis** aus.	Wenn Sie **Nein**auswählen, wird die Antwortaufgabe **Incident mit potenziellem Datenverlust erstellen**ausgeführt.
Erstellen Sie einen Incident mit potenziellem Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Incident vom Typ „Potenzieller Datenverlust“ zu erstellen. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt.
Remotelöschung erstellt?	Führen Sie die erforderlichen Schritte aus, um eine Remote-Löschung der verlorenen Geräte auszuführen. Wählen Sie in der Aufgabe je nach Bedarf **Ja** oder **Nein** unter **Ergebnis** aus.	Die Aufgabe **„Rechtlicher Prozess – Offenlegung erforderlich“** wird ausgeführt.
Rechtliches Verfahren – Offenlegung erforderlich?	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen. Wählen Sie **„Ja“**, wenn eine rechtliche Offenlegung erforderlich ist, **„Nein“**, wenn dies nicht der Fall ist.	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die Aufgabe **„Status auf Überprüfung festlegen“** wird ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Es ist keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Incident mit verlorenem Gerät durchgeführten Arbeiten zu selektieren. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Der Flow endet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow-Vorlage für böswillige Software für Security Incidents

Mit der Vorlage „Security Incident – Schadsoftware – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die Schadsoftware in Ihrem Netzwerk behandeln.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Böswillige Code-Aktivität**festgelegt ist.

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieBöswilliger Code Aktivität**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in Vorlage für schädliche Software

Antwortaufgabe	Aktion	Ergebnisse
Endpunkt scannen – Malware gefunden?	Bestimmen Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die **Meldung Malware entfernen – Erfolg?** Aufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird der Flow beendet.
Malware entfernen – Erfolg?	Stellen Sie fest, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, **wird im Feld Gab es einen größeren Verstoß?** Aufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **Löschen und erneut erstellen** ausgeführt.
Löschen und erneut erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie im Rahmen dieser Aufgabe aufgefordert, auf den mit der Malware infizierten Computern einen Löschvorgang und ein erneutes Image durchzuführen.	Nachdem die Aufgabe abgeschlossen wurde, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Gab es einen größeren Verstoß?	Stellen Sie fest, ob der durch die Schadsoftware verursachte Verstoß größer ist als zuerst angenommen.	Wenn Sie **Ja**auswählen, werden die folgenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie in der Aufgabe unter **Ergebnis**Ja oder **Nein**aus.	Aufgaben parallel ausgeführt: ○ Rechtliche Überprüfung ○ HR-Überprüfung ○ Überprüfung der Strafverfolgung Wenn Sie **Nein**auswählen, wird der Flow beendet.
Rechtliche Überprüfung HR-Überprüfung Überprüfung der Strafverfolgung	Führen Sie für jede dieser Abteilungen die erforderlichen Schritte aus, um den Prozess zur Beseitigung der Schadsoftware zu überprüfen.	Wenn die Aufgaben abgeschlossen sind, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf Überprüfung fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Prüfung**geändert, und der Flow wird beendet.

Flow-Vorlage für Security Incident-Phishing

Mit der Vorlage „Security Incident – Phishing –“ können Sie eine Reihe von Aufgaben ausführen, die Spear-Phishing-E-Mails in Ihrem Netzwerk behandeln.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Spear Phishing**festgelegt ist.

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Spear-Phishing-Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieSpear Phishing**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in der Spear-Phishing-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Handelt es sich um einen Phishing-Angriff?	Stellen Sie fest, ob dies ein Phishing-Angriff ist. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, werden die folgenden Aufgaben parallel ausgeführt: ○ Endpunkt scannen – Malware gefunden? ○ Aktualisieren Sie die E-Mail-Schutzsoftware ○ Ungelesene Phishing-E-Mail aus Warteschlange entfernen – für alle Anwender Wenn Sie **Nein**auswählen, wird der Flow beendet.
Endpunkt scannen – Malware gefunden?	Bestimmen Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die **Meldung Malware entfernen – Erfolg?** Aufgabe wird ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Malware entfernen – Erfolg?	Stellen Sie fest, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **Löschen und erneut erstellen (Reimage)** ausgeführt.
Löschen und erneut erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie im Rahmen dieser Aufgabe aufgefordert, auf den mit der Malware infizierten Computern einen Löschvorgang und ein erneutes Image durchzuführen.	Nachdem die Aufgabe abgeschlossen wurde, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Aktualisieren Sie die E-Mail-Schutzsoftware	Wenn festgestellt wurde, dass es sich um einen Phishing-Angriff handelt, werden Sie aufgefordert, Ihre E-Mail-Schutzsoftware entsprechend zu aktualisieren.	Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Ungelesene Phishing-E-Mail aus Warteschlange entfernen – für alle Anwender	Führen Sie die erforderlichen Schritte aus, um die Phishing-E-Mail, die sich noch in der Warteschlange befindet, für alle Ihre Anwender zu entfernen.	Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf Überprüfung fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. Die Aufgabe **„Schulung des Sicherheitsbewusstseins planen“** wird ausgeführt.
Planen Sie eine Schulung zum Sicherheitsbewusstsein	Planen Sie Schulungen, um das Sicherheitsbewusstsein Ihrer Mitarbeiter zu schärfen. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn die Aufgabe abgeschlossen ist, wird der Flow beendet.

Flow-Vorlage für Security Incident-Richtlinienverstoß

Mit der Vorlage „Security Incident – Richtlinienverletzung –“ können Sie eine Reihe von Aufgaben ausführen, die Verstöße gegen Sicherheitsrichtlinien behandeln.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Richtlinienverstoß**festgelegt wird.

Prozedur

1. Öffnen Sie den Security Incident für den Richtlinienverstoß, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieRichtlinienverstoß**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in Richtlinienverletzungsvorlage

Antwortaufgabe	Aktion	Ergebnisse
Verstoß klassifizieren	Klassifizieren Sie, wie dieser Verstoß gegen die Sicherheitsrichtlinien Ihrer Organisation verstößt.	Die Antwortaufgabe **„Mit Verstoß melden** “ wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Aktualisieren Sie das Feld **„Status“** in der Aufgabe, nachdem Sie sie abgeschlossen haben.	
Den Zuwiderhandelnden über den Verstoß informieren	Teilen Sie dem Verletzer die Art des Verstoßes mit. Aktualisieren Sie das Feld **„Status“** in der Aufgabe, nachdem Sie ihn mitgeteilt haben.	Die Aufgabe **„Bestätigung von Antwort auf Verstoß** einholen“ wird ausgeführt.
Bestätigung vom Verletzer einholen	Fordern Sie eine Bestätigung vom Verletzer des Verstoßes an. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Die **HR-Prozessantwortaufgabe** wird ausgeführt.
HR-Prozess	Teilen Sie HR alle erforderlichen Informationen zu diesem Verstoß mit. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Die Aufgabe **„Status auf Antwort überprüfen“ festlegen** wird ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Es ist keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.
Planen Sie eine Schulung zum Sicherheitsbewusstsein	Führen Sie eine Schulung zum Sicherheitsbewusstsein durch, um die Mitarbeiter zu schulen, wie ähnliche Sicherheitsverletzungen in Zukunft verhindert werden können. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet.

Flow-Vorlage für Security Incident Reconnaissance

Erkennung ist normalerweise ein vorläufiger Schritt zu einem weiteren Angriff, der ein Gerät oder System ausnutzen soll. Mit der Vorlage „Security Incident - Reconnaissance - Security Incident“ können Sie eine Reihe von Aufgaben ausführen, um die Erkennung in Ihrem Netzwerk zu verarbeiten.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Aufklärungsaktivität**festgelegt ist.

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategoriedie Option Aufklärungsaktivität**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in der Aufklärungsvorlage

Antwortaufgabe	Aktion	Ergebnisse
Aufklärungsaktivität verifiziert?	Stellen Sie fest, ob eine beobachtete Aufklärung verifiziert wurde. Wählen Sie in der Aufgabe unter **Ergebnis** **Ja** oder **Nein** aus.	Wenn Sie **Ja** auswählen, wird die Aufgabe **Betroffene Systeme identifizieren** ausgeführt. Wenn Sie **Nein** auswählen, wird der Flow beendet.
Identifizieren Sie die betroffenen Systeme	Bestimmen Sie die Systeme, die von der Erkennung betroffen sind.	Wenn diese Aufgabe abgeschlossen ist, **wird im Feld „Aufklärung für Strafverfolgungsanalysen zulassen?“** angezeigt. Aufgabe wird ausgeführt.
Aufklärung für Strafverfolgungsanalysen zulassen?	Legen Sie fest, ob die Aufklärung von Strafverfolgungsbehörden analysiert werden soll. Wählen Sie in der Aufgabe unter **Ergebnis** **Ja** oder **Nein** aus.	Wenn Sie **Ja** auswählen, wird die Aufgabe **des Strafverfolgungsprozesses** ausgeführt. Wenn Sie **Nein** auswählen, wird die **Aufgabe Systeme aktualisieren, um eine Spähen zu verhindern** ausgeführt.
Strafverfolgungsprozess	Führen Sie den von Ihrem Unternehmen definierten Strafverfolgungsprozess durch.	Wenn diese Aufgabe abgeschlossen ist, wird die **Aufgabe „System(e) aktualisieren, um eine Aufklärung zu verhindern** “ ausgeführt.
Aktualisieren Sie die Systeme, um eine Erkennung zu verhindern	Führen Sie die erforderlichen Schritte aus, um die von der Erkennung betroffenen Systeme zu aktualisieren.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung** geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit den gelernten Lektionen durch, um die für diesen Erkennungs-Incident durchgeführte Arbeit zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn diese Aufgabe abgeschlossen ist, wird der Flow beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow-Vorlage für Security Incident Rogue-Server oder -Service

Mit der Vorlage „Security Incident – Rogue-Server oder -Service –“ können Sie eine Reihe von Aufgaben ausführen, die darauf abzielen, Aktivitäten von betrügerischen Servern oder Services zu handhaben, die sich auf Ihr Netzwerk auswirken.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Nicht autorisierter Server oder Service**festgelegt ist.

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategoriedie Option Nicht autorisierter Server oder Serviceaktivität**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in Rogue-Server oder Servicevorlage

Antwortaufgabe	Aktion	Ergebnisse
Betrügerischer Server oder Service verifiziert?	Ermitteln Sie, ob in Ihrem Netzwerk eine Verbindung mit einem nicht autorisierten Server oder Service verifiziert wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, werden die folgenden beiden Aufgaben parallel ausgeführt: ○ **Betroffene Systeme identifizieren** ○ **Potenzieller Datenverlust?** Wenn Sie **Nein**auswählen, wird der Flow beendet.
Betroffene Systeme identifizieren	Ermitteln Sie die Systeme, die durch den Kontakt mit dem nicht autorisierten Server oder Service betroffen sind.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt.
Potenzieller Datenverlust?	Stellen Sie fest, ob die Verbindung mit dem nicht autorisierten Server oder Service potenziellen Datenverlust verursacht hat. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident mit potenziellem Datenverlust erstellen** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen** ausgeführt.
Erstellen Sie einen Incident mit potenziellem Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den potenziellen Datenverlust zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Systeme aktualisieren: Nicht autorisierte Verbindungen entfernen	Führen Sie die erforderlichen Schritte aus, um die nicht autorisierten Verbindungen zu entfernen.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen betrügerischen Server- oder Service-Incident durchgeführten Arbeiten zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn diese Aufgabe abgeschlossen ist, wird der Flow beendet.

Flow-Vorlage für Security Incident-Spam

Mit der Vorlage „Security Incident – Spam – Template“ können Sie eine Reihe von Aufgaben zur Behandlung von E-Mail-Spam in Ihrem Netzwerk ausführen.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident in **Spam-Quelle**festgelegt oder geändert wird.

Prozedur

1. Öffnen Sie den Security Incident, für den Sie E-Mail-Spam behandeln möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieSpam-Quelle**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in der Spam-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Enthält Spam schädliche Inhalte?	Stellen Sie fest, ob der Spam schädliche Software enthält. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**ausgewählt haben, werden die folgenden Antwortaufgaben ausgeführt: ○ **E-Mail-Nachricht in Quarantäne stellen** ○ **Erstellen Sie einen Incident für schädliche Software**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Wenn Sie **Nein**ausgewählt haben, wird die **Aktualisierung der E-Mail-Software** ausgeführt.
Erstellen Sie einen Incident für schädliche Software	Führen Sie die Schritte zum Erstellen eines Security Incident aus, und aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wartet diese Antwortaufgabe, bis die nächsten drei Antwortaufgaben abgeschlossen sind. Der Status des Security Incident wechselt dann zu **Überprüfen**.
E-Mail-Nachricht in Quarantäne stellen	Führen Sie die Schritte aus, um den Spam unter Quarantäne zu stellen, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Quelle in Firewall blockieren	Führen Sie die Schritte zum Blockieren der E-Mail-Adresse in der Firewall aus, und aktualisieren Sie dabei gegebenenfalls das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.
Aktualisieren Sie die E-Mail-Software	Fügen Sie die E-Mail-Adresse Ihrer Sperrliste hinzu, und aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. **Hinweis:** Diese Antwortaufgabe wird auch ausgeführt, wenn Sie die Frage mit **„Enthält Spam schädlichen Inhalt?“mit „Nein“** beantwortet haben. Antwortaufgabe.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.

Flow-Vorlage für nicht autorisierten Zugriff auf Security Incidents

Mit der Vorlage „Security Incident – Unautorisierter Zugriff – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, um nicht autorisierten Zugriff auf Ihr Netzwerk zu handhaben.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Nicht autorisierter Zugriff**festgelegt wird.

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategoriedie Option Nicht autorisierter Zugriff**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in Vorlage für nicht autorisierten Zugriff

Antwortaufgabe	Aktion	Ergebnisse
Sind die Benutzeranmeldeinformationen kompromittiert?	Stellen Sie fest, ob die Anmeldeinformationen von Anwendern gefährdet wurden. Wählen Sie in der Aufgabe unter **Ergebnis**Ja oder **Nein**aus.	Wenn Sie **Ja**auswählen, werden die folgenden beiden Aufgaben parallel ausgeführt: ○ **Schädliche Software?** ○ **Anwender-Account deaktivieren** Wenn Sie **Nein**auswählen, wird die Aufgabe **Anwender kontaktieren und Absicht bestimmen** ausgeführt.
Schädliche Software?	Stellen Sie fest, ob der nicht autorisierte Zugriff zur Einführung schädlicher Software geführt hat. Wählen Sie in der Aufgabe unter **Ergebnis**Ja oder **Nein**aus.	Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident für schädliche Software erstellen** ausgeführt. Wenn Sie **Nein**auswählen, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Erstellen Sie einen Incident für schädliche Software	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den nicht autorisierten Zugriff zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Anwender-Account deaktivieren	Führen Sie die erforderlichen Schritte aus, um das gefährdete Anwenderaccount zu deaktivieren.	Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Kontaktieren Sie den Anwender, und bestimmen Sie die Absicht	Führen Sie die erforderlichen Schritte aus, um den Anwender zu kontaktieren, der für den nicht autorisierten Zugriff verantwortlich ist, und ermitteln Sie den Grund für den Zugriffsversuch.	Wenn diese Aufgabe abgeschlossen ist, wird die **HR-Prozessaufgabe** ausgeführt.
HR-Prozess	Führen Sie die erforderlichen Schritte aus, um die Personalabteilung zu kontaktieren	Wenn diese Aufgabe abgeschlossen ist, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	und gegebenenfalls Disziplinarmaßnahmen durchzuführen.	die Aufgabe **„Status auf Überprüfung festlegen“** ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Prüfung**geändert, und der Flow wird beendet.

Flow-Vorlage für Web/BBS-Defacement für Security Incidents

Mit der Vorlage „Security Incident – Web/BBS-Defacement“ können Sie eine Reihe von Aufgaben ausführen, um Vandalismus zu handhaben, der sich gegen eine der BBS-Websites oder Websites Ihres Unternehmens richtet.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Web/BBS-Defacement**festgelegt ist.

Prozedur

1. Öffnen Sie den Security Incident für dieses Vorkommen der Web- oder BBS-Unleserlichkeit, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **KategorieWeb/BBS-Defacement**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe entweder die Erstellung der nächsten Antwortaufgabe oder die Beendigung des Flows.

Antwortaufgaben in Web/BBS-Defacement-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Zuweisung von Security Incidents	Erstellen Sie einen Security Incident für jeden gemeldeten Incident von Website- oder BBS-Unleserlichmachen.	Die nächste Antwortaufgabe wird ausgeführt.
Unformatierung verifiziert?	Stellen Sie fest, ob die Website oder BBS tatsächlich unleserlich gemacht wurde. Wählen Sie in der Aufgabe unter **ErgebnisJa** oder **Nein**aus.	Wenn Sie **Ja**auswählen, werden die folgenden Antwortaufgaben ausgeführt: ○ **PR-Prozess** ○ **Strafverfolgungsprozess** ○ **Ursache ermitteln und beseitigen** Wenn Sie **Nein**auswählen, wird der Flow beendet.
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die Öffentlichkeit darüber zu	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	informieren, dass die Website oder BBS unkenntlich gemacht wurde. Wenn Sie mit dem PR-Prozess fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	
Strafverfolgungsprozess	Führen Sie die erforderlichen Schritte aus, um die entsprechenden Strafverfolgungsbehörden bezüglich des Angriffs einzuschalten. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Ursache ermitteln und beseitigen	Führen Sie die erforderlichen Schritte aus, um die Ursache der Unleserlichkeit zu erkennen und zu beseitigen. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Site aus Sicherung wiederherstellen	Führen Sie die erforderlichen Schritte zum Sichern und Wiederherstellen der Website oder des BBS durch. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt.
Testen und überprüfen Sie, ob die Site wiederhergestellt ist	Stellen Sie sicher, dass die Site wiederhergestellt ist. Wenn Sie fertig sind, legen Sie den Status der Aufgabe je nach Bedarf auf **Abgeschlossen** oder **Unvollständig** fest.	Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt.
Meeting mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Website-/BBS-Unleserlichmachen-Incident durchgeführten Arbeiten zu selektieren. Aktualisieren Sie entsprechend das Feld **Status** in der Aufgabe.	Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **storniert**ändern, wird die Aufgabe **Status auf Überprüfung** festlegen ausgeführt.
Legen Sie den Status auf „Überprüfung“ fest	Keine Aktion erforderlich.	Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. Der Flow endet.

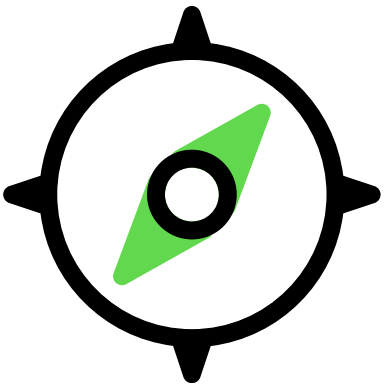
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence

Mit der Anwendung ServiceNow® Threat Intelligence können Sie Kompromittierungsindikatoren (IoC) finden und Security Incidents mit Threat Intelligence-Daten anreichern.

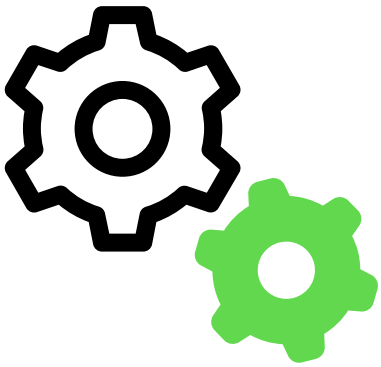
Erste Schritte

Untersuchen



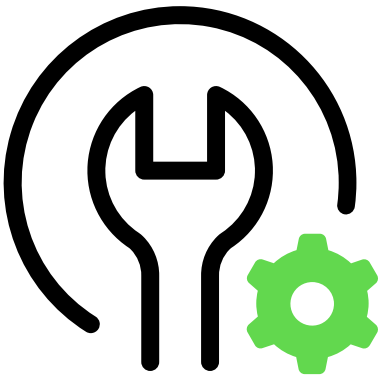
Lernen Sie die Konzepte von Threat Intelligence und ihre wichtigsten Funktionen kennen.

Konfigurieren



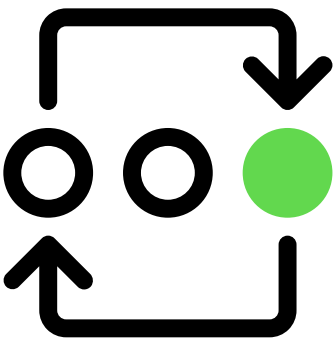
Richten Sie ein, und lernen Sie die installierten Komponenten und Anwenderrollen kennen, die zur Erfüllung Ihrer Geschäftsanforderungen erforderlich sind.

Verwalten



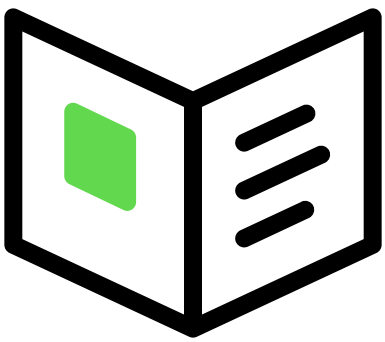
Legen Sie Threat Intelligence-Eigenschaften fest.

integrieren



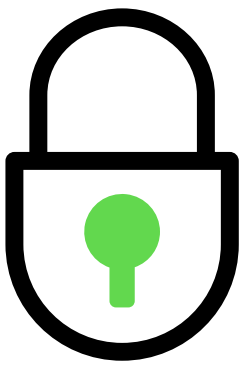
Erweitern Sie die Threat Intelligence-Fähigkeiten durch die Integration mit ServiceNow- und Drittanbieteranwendungen.

Verwenden



Kompromittierungsindikatoren (IoC) und verschiedene Artefakte verwalten.

MITRE ATT&CK-Framework



Verwalten Sie das MITRE-ATT&CK-Framework, um schnell Bedrohungen zu identifizieren und Antworten auf Cyberangriffe zu koordinieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Case Management

Verwalten Sie die Security Case Management durch das Sammeln von Informationen zu verdächtigen Aktivitäten.

Lernressourcen

- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Stellen Sie Fragen, und erkunden Sie andere Ressourcen für Threat Intelligence in ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- Security Operations-Ressourcenbibliothek
- Security Operations-Community

Threat Intelligence verstehen

Mit der Anwendung Threat Intelligence können Sie auf dieSTIX™-Daten (Strukturierte Bedrohungsinformationen) Ihres Unternehmens zugreifen und einen Referenzpunkt dafür bereitstellen. In Threat Intelligence ist die Anwendung Management von Sicherheitsfällen enthalten, die eine Möglichkeit zur Analyse von Bedrohungen für Ihre Organisation bietet, die von gezielten Kampagnen oder staatlichen Akteuren ausgehen.

STIX ist eine Sprache zur standardisierten und strukturierten Beschreibung von Cyberbedrohungsinformationen. Mithilfe von STIX-Daten undTAXII-™Profilen (Trusted Automated Exchange of Indicator Information) können Bedrohungsexperten gemeinsam genutzte Cyberbedrohungsinformationen verwenden, um Bedrohungen zu isolieren, die zuvor von Ihrem Unternehmen und anderen Quellen identifiziert wurden. TAXII ermöglicht einen weit verbreiteten automatisierten Austausch von Informationen zu Cyberbedrohungen.

Threat Intelligence unterstützt die STIX-Versionen 1.1, 2.0 und 2.1.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

STIX™ und TAXII™ sind Marken der MITRE Inc.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Domain Separation und Threat Intelligence

Die Domänentrennung wird im Modul Threat Intelligence unterstützt, das als Teil von Security Incident Response verfügbar ist. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für Domänentrennung .

Übersicht

Im Modul Threat Intelligence (als Teil der Anwendung Security Incident Response) können Service Provider (SPs) durch Domänentrennung das Threat Intelligence-Repository auf folgende Weise erstellen und verwalten:

- Bedrohungsquellen und TAXII-Profile (Trusted Automated Exchange of Indicator Information).
- Erkennbare Elemente
- Kompromittierungsindikatoren
- Bedrohungsangriffsmodi/-methoden und Fallverwaltung für den gesamten Kundenstamm mit niedrigeren Betriebskosten und höherer Servicequalität

Durch separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. wird sichergestellt, dass Kundendaten getrennt und niemals für andere Clients verfügbar gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützung für Domain Separation in Threat Intelligence nach Versions-Release

Die Domänentrennung für das Threat Intelligence-Modul (als Teil der Anwendung Security Incident Response) deckt die folgenden Produktfunktionen ab:

- Erkennbare Elemente für Security Incidents werden an die entsprechende Domäne des Anwenders weitergeleitet, dessen ID/Anmeldeinformationen/Umfang den Incident generiert. Die aus dem Incident extrahierten erkennbaren Elemente werden in der Domäne des Security Incident gespeichert.
- Einrichten von TAXII-Serviceprofilen zum Herunterladen einer oder mehrerer TAXII-Sammlungen, die Feeds mit Informationen zu Cyberbedrohungen bieten. Die Konfiguration wird in der Domäne gespeichert, unter der das Profil eingerichtet wird.
- Setup des Downloads von Bedrohungs-Feeds in das IoC-Repository in der Domäne, unter der die Konfiguration durchgeführt wird.
- Erstellung von Angriffsmodi/Angriffsmethoden in der Domäne der Threat Intelligence-Quelle, die die Informationen automatisch bereitstellt, oder in der Domäne, unter der ein neuer Angriffsmodus/eine neue Angriffsmethode manuell vom Anwender hinzugefügt wird
- Erstellung von Fällen für die langfristige Untersuchung von Incidents, erkennbaren Elementen, CIs, Benutzern und Kompromittierungsindikatoren (IoC), die dem Fall zugeordnet sind. Der Fall wird in der vom Benutzer erstellten Domäne gespeichert.

Hinweis:
In allen oben genannten Fällen gelten die übergeordneten Prinzipien der Transparenz in getrennten Domänen in der NOW Platform. Wie immer kann ein Incident in der übergeordneten Domäne auf Artefakte in der untergeordneten Domäne verweisen, aber nicht umgekehrt.

Funktionsweise der Domänentrennung in Threat Intelligence (als Teil von Security Incident Response)

Threat Intelligence ist Teil von Security Incident Response in den Stufen „Professional“ und „Enterprise“, aber nicht in der Stufe „Standard“. Daher ist ein separates Plugin erforderlich. Das Threat Intelligence-Modul (als Teil der Anwendung Security Incident Response) erstellt und verwaltet die Threat Intelligence-Informationen, die Security Incidents in einer Organisation zugeordnet sind. Die folgenden Anwendungsfälle berücksichtigen die Domänentrennung:

- Erstellung von erkennbaren Elementen für Security Incidents zum Zeitpunkt der Incident-Erstellung
  - Von E-Mail-Parsern (plattformbasiert, von Anwendern gemeldetes Phishing, anwenderdefiniert)
  - Aus Anwendungen in SIEM-Speichern (Security Information and Event Management) von Drittanbietern
  - Durch manuelle Eingabe durch den SOC-Analysten
- Sammlung von erkennbaren Elementen aus Bedrohungs-Feed-Quellen – Threat Intelligence-Quellen aus TAXII-Sammlungen
- Verwalten Sie erkennbare Elemente für Security Incidents
  - Ordnen Sie erkennbare Elemente zugehörigen Indikatoren zu
  - Erkennbare Elemente Security Incidents zuordnen
  - Ordnen Sie erkennbaren Elementen untergeordneten erkennbaren Elementen zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erkennbares Element der Bedrohungs-Feed-Quelle zuordnen
- Fügen Sie erkennbaren Elementen Sicherheitsanmerkungen hinzu

- Kompromittierungsindikatoren verwalten
  - Ordnen Sie Indikatoren zugehörigen erkennbaren Elementen zu
  - Ordnen Sie dem Angriffsmodus/der Angriffsmethode Indikatoren zu
  - Ordnen Sie Indikatoren Indikatortypen zu
  - Ordnen Sie Indikatoren der Bedrohungs-Feed-Quelle zu
  - Fügen Sie -Indikatoren Sicherheitsanmerkungen hinzu
- Verwalten Sie Fälle
  - Fall erstellen (manuell oder aus einem Incident)
  - Neuen Fall bearbeiten, um Details hinzuzufügen (Falltyp und Schweregrad auswählen, Incidents, erkennbare Elemente, Konfigurationselemente, Anwender, Indikatoren hinzufügen)
  - Löschen Sie einen Fall

Domänentrennung – Einrichtung

Das Einrichten der Domänentrennung für Threat Intelligence erfordert keine zusätzlichen Schritte. Alle Threat Intelligence-Tabellen erwerben die Spalte „Domäne“, nachdem die Instanz domänengetrennt wurde.

Domänengetrennte Daten

Daten können domänengetrennt sein. Das bedeutet:

- Erkennbare Elemente von Security Incidents in einer Domäne können nicht im Bereich anderer Domänen angezeigt werden.
- Kompromittierungsindikatoren in einer Domäne können nicht im Bereich anderer Domänen angezeigt werden.
- Angriffsmodi/-methoden, die einer Domäne zugeordnet sind, können nicht im Bereich anderer Domänen angezeigt werden.
- TAXII-Serviceprofile, die einer Domäne zugeordnet sind, können nicht im Bereich anderer Domänen angezeigt werden.
- Einer Domäne zugeordnete Threat Intelligence-Quellen können nicht im Bereich anderer Domänen angezeigt werden.
- Fälle, die einer Domäne zugeordnet sind, können nicht im Bereich anderer Domänen angezeigt werden.

Threat Intelligence-Eigenschaften werden auf globaler Ebene festgelegt und sind daher nicht domänengetrennt. Die Einstellungen umfassen:

- Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs
- Der für den Abruf zu verwendende API-Schlüssel
- Suche in lokalen IoC-Tabellen vor dem Senden an den Remote-Scanner
- Anzahl der Tage, für die lokale erkennbare Elemente berücksichtigt werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Markieren eines Angriffsmodus/einer Angriffsmethode als inaktiv, wenn er/sie nicht von Bedrohungsinformationsquellen empfangen wurde
- Markieren eines Indikators als inaktiv, wenn er für eine angegebene Anzahl von Tagen von keiner Quelle empfangen wurde

Konfiguration

Alle Aspekte der Konfiguration der Threat Intelligence-Funktionen sind in einer domänengetrennten Umgebung eigenständig.

Die folgenden Aufgaben können pro Domäne konfiguriert werden:

1. Erstellung von TAXII-Serviceprofilen
   - Wählen Sie eine Discovery-Servicekonfiguration aus
   - Wählen Sie eine Sammlungsservicekonfiguration aus, um Anwendern und Gruppen von Anwendern Rollen zuzuweisen
2. Erstellung von Threat Intelligence-Quellen
   - Konfigurieren Sie den REST-Service, der die Bedrohungsinformationen bereitstellt
   - Planen Sie den Download von Bedrohungsinformationen
   - Wählen Sie die Bedrohungsdetailinformationen aus, die der Quelle zugewiesen werden sollen
3. Erstellung von Angriffsmodus/Angriffsmethoden (manuell)
   - Quelle, Malware-Typ, Angriffsmechanismus, Typ des Bedrohungsakteurs, Beschreibung, Handhabung, beabsichtigte Wirkung, zuerst gesehen, zuletzt gesehen
   - Zugehörige Indikatoren, untergeordneter Angriffsmodus/-methode, zugehörige Security Incidents

   Hinweis:
   Angriffsmodi/-methoden werden auch automatisch aus den Bedrohungs-Feed-Quellen erstellt.

4. Einstellung von Standardlisten für die folgenden Kategorien von Bedrohungsinformationen:
   - Angriffsmechanismen
   - Discovery-Methoden
   - Feeds
   - Indikatortypen
   - Beabsichtigte Wirkungen
   - Benachrichtigungen
   - Erkennbare Typen
   - Quotengrenzdefinitionen
   - Typen des Bedrohungsakteurs
   - Angriffsmotivationen
   - Infrastrukturtypen
   - Malware-Fähigkeiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schadsoftwaretypen
- Berichtstypen
- Rollen des Bedrohungsakteurs
- Tooltypen

Wie Mandantendomänen ihre eigenen Anwendungsdaten verwalten

- Besitzer der Mandantendomäne können ihre eigenen TAXII-Serviceprofile erstellen.
- Besitzer der Mandantendomäne können ihre eigenen Threat Intelligence-Quellen erstellen.
- Besitzer der Mandantendomäne können ihre eigenen Angriffsmodi/-methoden erstellen.
- Besitzer der Mandantendomäne können ihre eigenen Standardlisten für Bedrohungsinformationskategorien erstellen.

Hinweis:
Geschäftslogik und -prozesse ermöglichen die Domänentrennung von Downloadzeitplänen für Threat Intelligence-Quellen nach Instanzbesitzern.

Zugehörige Informationen

Domänentrennung für Service Provider

Threat Intelligence einrichten

Bevor Sie Threat Intelligence in Ihrer -Instanz ausführen, müssen Sie es von ServiceNow Storeherunterladen. Sie können auch Eigenschaften einrichten und eine Bedrohungsquelle definieren.

Threat Intelligence installieren

Bevor Sie Threat Intelligence in Ihrer -Instanz ausführen, müssen Sie es von ServiceNow Storeherunterladen.

Vorbereitungen
Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setupaufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgaben	Beschreibung
Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz von verfügen.	Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Wenn die Anwendung noch nicht zugewiesen wurde, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle „Bedrohungsadministrator“ [sn_ti.admin] zu. • Der Bedrohungsadministrator [sn_ti.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Administrator

Prozedur

Befolgen Sie die Anweisungen für Herunterladen einer Anwendung aus dem ServiceNow Store.

Nächste Maßnahme

Legen Sie die Eigenschaften Threat Intelligence fest.

Mit Threat Intelligence installierte Komponenten

Bei der Aktivierung des Threat Intelligence-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Bedrohungsadministrator [sn_ti.admin]	Hat vollständige Kontrolle über alle Bedrohungseigenschaften, SLAs und Benachrichtigungen.	sn_ti.write
Bedrohungsleser [sn_ti.read]	Hat Lesezugriff auf Bedrohungsinformationen.	sn.sec_cmn.int_read
Threat Writer [sn_ti.write]	Hat Schreibzugriff auf Bedrohungsinformationen. Angriffsmodi, Indikatoren und erkennbare Elemente dürfen nicht gelöscht werden. Sie können nur von einem Bedrohungsadministrator gelöscht werden.	• sn_sec_cmn.int_write • sn_ti.read
MITRE-Analyst [sn_ti.mitre_analyst]	Diese Rolle ermöglicht den Lesezugriff auf die -Module MITRE-ATT&CK in Threat Intelligence und auf das Modul SIR.	• sn_ti.read • sn_si.read

Installierte Tabellen

Tabelle	Beschreibung
Angriffsmechanismus sn_ti_attack_mechanismus	Organisiert Angriffsmuster hierarchisch basierend auf Mechanismen, die häufig beim Ausnutzen einer Schwachstelle eingesetzt werden. Die Kategorien, die Mitglieder dieser Ansicht sind, stellen die verschiedenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	Techniken dar, die zum Angriff auf ein System verwendet werden.
Angriffsmodus/-methode sn_ti_attack_mode	Angriffsmodi und -methoden sind Darstellungen des Verhaltens von Cyberangreifern. Sie charakterisieren das, was ein Angreifer tut und wie er es tut, in zunehmendem Detailgrad.
Discovery-Methode sn_ti_discovery_method	Ausdruck dafür, wie ein Incident entdeckt wurde.
Feed-Gruppe sn_ti_feed	Wird zur Konfiguration des Bedrohungs-Feeds (RSS) in der Bedrohungsübersicht verwendet.
Indikatorangriffsmodus/-methode [sn_ti_m2m_indicator_attack_mode]	Wird verwendet, um Indikatoren Angriffsmodi/-methoden zuzuordnen.
Kompromittierungsindikator sn_ti_indicator	Wird verwendet, um bestimmte erkennbare Muster in Kombination mit Kontextinformationen zu vermitteln, die Artefakte und/oder Verhaltensweisen darstellen sollen, die in einem Cybersicherheitskontext von Interesse sind.
Indikator für Kompromittierungsmetadaten sn_ti_indicator_metadata	Wird zum Ausfüllen von TAXII-Datensätzen verwendet.
Indikatorquelle sn_ti_m2m_indicator_source	Wird verwendet, um alle Quellen zu erfassen, die den spezifischen Indikator melden.
Indikatortyp sn_ti_indicator_type	Kennzeichnet einen Cyberbedrohungsindikator, der aus einem Muster besteht, das bestimmte erkennbare Bedingungen sowie kontextbezogene Informationen über die Bedeutung des Musters, wie und wann darauf reagiert wird usw. enthält.
Zugehöriger Indikatortyp [sn_ti_m2m_indicator_indicator_type]	Verknüpft Indikatoren mit ihren zutreffenden Typen
Incident-Anzahl sn_ti_observable	Anzahl der Security Incidents, die einem erkennbaren Element zugeordnet sind.
Beabsichtigte Wirkung sn_ti_intended_effect	Wird verwendet, um die beabsichtigte Wirkung eines Bedrohungsakteurs auszudrücken.
IP-Scan-Ergebnis	Wird verwendet, um die Ergebnisse einer IP-Suche anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_ti_ip_result	
Ratenbegrenzung für Malware sn_ti_rate_limit]	Definiert eine Quotenbegrenzung, die für eine Suchquelle verwendet werden soll.
Malware-Scan sn_ti_scan	Eine Suche. Enthält das zu suchende Element, die Suchquelle und eine Zusammenfassung der Suchergebnisse.
Warteschlangeneintrag für Malware-Scan [sn_ti_scan_q_entry]	Ein Suchdatensatz, der sich zur Suche oder Verarbeitung in der Warteschlange befindet. Erleichtert die Anforderungen innerhalb der angegebenen Quotengrenzen.
Malware-Scan-Ergebnis sn_ti_scan_result]	Zeigt das Ergebnis einer Suche an.
Malware-Scanner [sn_ti_scanner]	Definiert Suchquellen von Drittparteien für Suchvorgänge.
Ratenbegrenzung für Malware-Scanner sn_ti_scanner_rate_limit]	Ordnet eine Suchquelle einer Quotenbegrenzung zu.
Malware-Typ sn_ti_malware_type	Wird verwendet, um die Typen von Malware-Instanzen auszudrücken.
Erkennbares Element sn_ti_observable	Erkennbare Elemente in STIX stellen zustandsbehaftete Eigenschaften oder messbare Ereignisse dar, die für den Betrieb von Computern und Netzwerken relevant sind.
Kontexttyp des erkennbaren Elements sn_ti_observable_context_type	Speichert den Kontext (Quelle, Ziel einer IP-Adresse usw.) für ein erkennbares Element.
Indikator für erkennbares Element sn_ti_m2m_observable_indicator]	Wird verwendet, um erkennbare Elemente mit Indikatoren zu verknüpfen.
Quelle erkennbares Element sn_ti_observable_source	Wird verwendet, um erkennbare Elemente mit Bedrohungsquellen zu verknüpfen.
Erkennbarer Typ sn_ti_observable_type	Listet die verschiedenen Arten von erkennbaren Elementen auf, z. B. IP-Adressen.
Typkategorie des erkennbaren Elements sn_ti_observable_type_category	Speichert die erste Kategorisierung von erkennbaren Elementen (z. B. IP-Adressen und URLs). Es wird verwendet, um erkennbare Elemente genauer zu bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Zugehöriger Angriffsmodus/zugehörige Angriffsmethode [sn_ti_m2m_attack_mode_attack_mode]	Wird verwendet, um Angriffsmodi miteinander zu verknüpfen.
Zugehörige erkennbare Elemente sn_ti_m2m_observables]	Wird verwendet, um erkennbare Elemente miteinander zu verknüpfen.
Überprüfungstyp sn_ti_scan_type	Die Definition eines Suchtyps mit ursprünglichen Datensätzen für Datei, URL und IP.
Sicherheitsfall [sn_ti_case]	Speichert mit der Fallverwaltung erstellte Sicherheitsfalldatensätze.
Sicherheitsfall IoC sn_ti_case_ioc	Wird verwendet, um die Beziehung zwischen erkennbaren Elementen und Fällen zu verwalten.
Zugehörige Aufgabe zu Sicherheitsfall sn_ti_m2m_case_task]	Wird verwendet, um die Beziehung zwischen Aufgaben (Security Incidents, Change-Anforderungen usw.) und Sicherheitsfällen zu verwalten.
Sicherheitsfall-Beziehungsausschluss sn_ti_case_relationship_exclusion]	Stellt die Definition für den Einschluss und Ausschluss zugehöriger Datensätze in Sicherheitsfällen bereit.
Sichtung sn_ti_sighting	Der m2m-Link zwischen dem erkennbaren Element und dem Detailergebnis der Sichtungssuche, der bei der Ausführung einer Anforderung einer Sichtungssuche verwendet wird.
Konfigurationselemente der Sichtung sn_ti_m2m_sighting_ci	Ordnet Konfigurationselemente einer Sichtungssuche zu.
Detail der Sichtungssuche sn_ti_sighting_search_detail	Details einer Sichtungssuche, z. B. die Anzahl der gefundenen internen externen Elemente.
Sichtungssuchergebnis sn_ti_sighting_search	Der Header für die Ausführung einer Sichtungssuche.
Unterstützte erkennbare Typen sn_ti_m2m_ind_type_obs_type	Setzt Indikatortypen mit gültigen Typen erkennbarer Elemente in Beziehung.
Unterstützter Scantyp [sn_ti_supported_scan_type]	Ordnet den Suchtyp einer Suchquelle/ Lieferanten-spezifischen Implementierung zu. Gibt an, dass eine bestimmte Suchquelle den Typ unterstützt.
Aufgabenangriffsmodus/-methode	Verknüpft Angriffsmodi mit Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_ti_m2m_task_attack_mode]	
Aufgabenindikator sn_ti_m2m_task_indicator]	Verknüpft Indikatoren mit Aufgaben.
Aufgabe – erkennbares Element sn_ti_m2m_task_observable]	Verknüpft erkennbare Elemente mit Aufgaben.
Aufgabensichtung sn_ti_m2m_task_sighting	Speichert Aufgabendatensätze (Security Incidents und Fälle), die sich auf einen Sichtungsdatensatz beziehen.
TAXII-Sammlung [sn_ti_taxi_collection]	Definiert einen Cyber-Risk Intelligence-Feed, der von einem TAXII-Server importiert werden kann.
TAXII-Profil [sn_ti_taxi_profile]	Definiert ein Repository für die Freigabe von Cyber-Risikoinformationen. Enthält TAXII-Sammlungen.
Bedrohungsakteurtyp [sn_ti_threat_actor_type]	Stellt Merkmale von böswilligen Akteuren (oder Angreifern) bereit, die eine Cyberangriffsbedrohung darstellen, einschließlich der vermuteten Absicht und des bisher beobachteten Verhaltens.
Threat Intelligence-Quelle sn_ti_source	Definiert eine Quelle für den Import von Bedrohungsdaten.
Zugehörige Angriffsmotivation [sn_ti_stix2_m2m_object_attack_motivation]	Erfasst alle Angriffsmotivationen, die einem STIX-Objekt zugeordnet sind
Zugeordneter Infrastrukturtyp [sn_ti_stix2_m2m_infra_type]	Verknüpft Infrastrukturen mit ihren Typen.
Zugehörige Kill Chain-Phase [sn_ti_stix2_m2m_indicator_kill_kette_phase]	Verknüpft Kill Chain-Phasen mit Indikatoren.
Zugehörige Kill Chain-Phase [sn_ti_stix2_m2m_object_kill_kette_phase]	Verknüpft Kill Chain-Phasen mit STIX-Objekten.
Zugehörige Malware-Fähigkeit [sn_ti_stix2_m2m_malware_capability]	Verknüpft Malware mit ihren Fähigkeiten.
Zugeordneter Malware-Typ [sn_ti_stix2_m2m_malware_malware_type]	Verknüpft Malware mit ihren Typen.
Zugehöriges erkennbares Element	Erfasst alle erkennbaren Elemente, die einer Malware zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_ti_stix2_m2m_malware_observable]	
Zugehöriges erkennbares Element [sn_ti_stix2_m2m_observed_data_observable]	Erfasst alle erkennbaren Elemente, die beobachteten Daten zugeordnet sind
Zugeordneter Berichtstyp [sn_ti_stix2_m2m_report_report_type]	Verknüpft Bedrohungsberichte mit ihren Typen.
Zugeordnete Bedrohungsakteurrolle [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	Verknüpft Bedrohungsakteure mit ihren Rollen.
Zugeordneter Bedrohungsakteurtyp [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	Verknüpft Bedrohungsakteure mit ihren Typen.
Zugeordneter Tooltyp [sn_ti_stix2_m2m_tool_tool_type]	Verknüpft Tools mit ihren Typen.
Angriffsmotivation [sn_ti_stix2_attack_motivation]	Die Angriffsmotivation prägt die Stärke und Dauer eines Angriffs. Bedrohungsakteure und Angriffssätze verhalten sich normalerweise in einer Weise, die ihre zugrunde liegende Stimmung oder Situation widerspiegelt, und dies informiert die Abwehrkräfte über die Art des Angriffs.
Angriffsmuster sn_ti_stix2_attack_pattern]	Ein TTP-Typ, der Methoden beschreibt, mit denen Angreifer versuchen, Ziele zu gefährden.
Kampagne sn_ti_stix2_campaign]	Eine Gruppierung von Verhaltensweisen eines Angreifers, die eine Reihe von böswilligen Aktivitäten oder Angriffen (manchmal auch als „Waves“ bezeichnet) beschreiben, die über einen Zeitraum gegen eine bestimmte Gruppe von Zielen auftreten.
Vorgehensweise [sn_ti_stix2_course_of_action]	Eine Empfehlung eines Intelligenzerstellers an einen Verbraucher, welche Aktionen er als Reaktion auf die Intelligenz ergreifen kann.
Externe Referenz sn_ti_stix2_external_reference	Verweist auf Informationen, die außerhalb von STIX dargestellt werden.
Identitätssichtung [sn_ti_stix2_m2m_sighting_identity]	Erfasst alle Identitäten, die einer Sichtung zugeordnet sind
Identität sn_ti_stix2_identity	Tatsächliche Personen, Organisationen oder Gruppen (z. B. ACME, Inc.) sowie Klassen von Personen, Organisationen, Systemen oder Gruppen (z. B. die Finanzbranche).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Externe Referenz des Indikators [sn_ti_stix2_indicator_external_reference]	Stellt externe Referenzen dar, die Indikatoren zugeordnet sind.
Indikatorsichtung [sn_ti_stix2_indicator_sighting]	Stellt Sichtungen von Indikatoren dar.
Infrastrukturtyp sn_ti_stix2_infrastructure_type	Stellt die verschiedenen Infrastrukturtypen dar.
Infrastruktur sn_ti_stix2_infrastructure	Ein TTP-Typ, der alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen beschreibt, die einen bestimmten Zweck unterstützen sollen (z. B. C2-Server, die als Teil eines Angriffs verwendet werden, Geräte oder Server, die Teil der Abwehr sind, Datenbankserver, die im Rahmen eines Angriffs verwendet werden). -Angriff usw.).
Installierte Software [sn_ti_stix2_m2m_malware_analyse_sw]	Erfasst alle Software (SCO-Softwaretypen), die einer Malware-Analyse zugeordnet sind.
Angriffssatz sn_ti_stix2_intrusion_set	Ein gruppierter Satz von Verhaltensweisen und Ressourcen des Angreifers mit gemeinsamen Eigenschaften, von dem angenommen wird, dass er von einer einzelnen Organisation orchestriert wird.
Kill Chain-Phase [sn_ti_stix2_kill_kette_phase]	Stellt Kill Chain-Phasen dar, die einer Kill Chain zugeordnet sind.
Kill Chain sn_ti_stix2_kill_kette	Stellt verschiedene Kill Chains dar.
Standort [sn_ti_stix2_location]	Stellt einen geografischen Standort dar, der über STIX bereitgestellt wird.
Malware-Analyse [sn_ti_stix2_malware_analyse]	Die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse, die für eine Malware-Instanz oder -Familie durchgeführt wurde.
Malware-Fähigkeit [sn_ti_stix2_malware_capability]	Stellt allgemeine Fähigkeiten dar, die eine Malware-Familie oder -Instanz aufweist.
Malware-Betriebssystem [sn_ti_stix2_m2m_malware_operating_system]	Erfasst alle Betriebssysteme (SCO-Softwaretypen), die Malware zugeordnet sind.
Malware	Ein TTP-Typ, der schädlichen Code darstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_ti_stix2_malware]	
Markierungsdefinition sn_ti_stix2_marking_definition	Stellt Verarbeitungs- oder Freigabeanforderungen für STIX-Objekte dar.
Objektsichtung [sn_ti_stix2_object_sighting]	Stellt Sichtungen von STIX-Objekten dar.
Objekt-Indikator-Beziehung [sn_ti_stix2_m2m_object_indicator]	Sammelt alle Beziehungen zwischen STIX-Objekten und STIX-Indikatoren.
Objekt-Objekt-Beziehung [sn_ti_stix2_m2m_object]	Erfasst alle Beziehungen zwischen STIX-Objekten und anderen STIX-Objekten außer den -Indikatoren.
Beziehung von Objekt und erkennbarem Element [sn_ti_stix2_m2m_object_observable]	Erfasst alle Beziehungen zwischen erkennbaren STIX-Elementen und STIX-Objekten.
Beobachtete Datensichtung [sn_ti_stix2_m2m_sighting_observed_data]	Erfasst alle beobachteten Datenobjekte, die einer Sichtung zugeordnet sind
Beobachtete Daten [sn_ti_stix2_observed_data]	Vermittelt Informationen über Entitäten im Zusammenhang mit der Cybersicherheit wie Dateien, Systeme und Netzwerke mithilfe der STIX Cyber-Observable Objects (SCOs).
Berichtstyp sn_ti_stix2_report_type	Stellt den primären Zweck oder Betreff von Bedrohungsberichten dar.
Gemeldetes erkennbares Element [sn_ti_stix2_m2m_malware_anasys_observable]	Erfasst alle erkennbaren Elemente, die der Malware-Analyse zugeordnet sind
STIX V2-Objekt sn_ti_stix2_object]	Gemeinsame übergeordnete Tabelle für STIX-Objekt.
STIX V2-Sichtung sn_ti_stix2_sighting	Gemeinsame übergeordnete Tabelle für STIX-Sichtungstabellen.
Bedrohungsakteurrolle [sn_ti_stix2_threat_actor_role]	Stellt Rollen dar, die von Bedrohungsakteuren übernommen werden können.
Bedrohungsakteur [sn_ti_stix2_threat_actor]	Bedrohungsakteure sind tatsächliche Personen, Gruppen oder Organisationen, von denen angenommen wird, dass sie mit böswilligen Absichten operieren.
Bedrohungsgruppierung	Gruppiert alle STIX-Objekte, die einen gemeinsamen Kontext haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_ti_stix2_threat_grouping]	
Bedrohungshinweis [sn_ti_stix2_threat_note]	Stellt Kontext und zusätzliche Analysen bereit, die nicht im entsprechenden STIX-Objekt enthalten sind.
Bedrohungsmeinung [sn_ti_stix2_threat_opinion]	Bietet eine Bewertung der Genauigkeit von Informationen in einem STIX-Objekt, das von einer anderen Entität erstellt wurde.
Bedrohungsbericht [sn_ti_stix2_threat_report]	Berichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren, z. B. eine Beschreibung eines Bedrohungsakteurs, einer Malware oder einer Angriffstechnik, einschließlich Kontext und zugehöriger Details. Sie werden verwendet, um zugehörige Bedrohungsinformationen zu gruppieren und als umfassende Cyberbedrohungsstory zu veröffentlichen.
Tooltyp sn_ti_stix2_tool_type	Die Kategorien von Tools, die für Angriffe verwendet werden können.
Tool sn_ti_stix2_tool]	Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet wird.
Schwachstelle [sn_ti_stix2_vulnerability]	Stellt eine Schwachstelle oder einen Fehler in den Anforderungen, Designs oder Implementierungen der Berechnungslogik (Beispielcode) dar, die in Software und einigen Hardwarekomponenten (Beispiel-Firmware) vorkommt. Sie können direkt dazu ausgenutzt werden, die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems zu beeinträchtigen.

Legen Sie die Eigenschaften Threat Intelligence fest

Threat Intelligence Mit den Eigenschaften von können Sie steuern, wie verschiedene Aspekte des Systems funktionieren, einschließlich der Einstellung von API-Schlüsseln.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Administration** > **Eigenschaften**.
2. Legen Sie nach Bedarf die folgenden Eigenschaften fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften für Threat Intelligence

Eigenschaft	Beschreibung
Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs sn_ti.ip_lookup.web_site	Der Domänenname, der zum Abrufen zusätzlicher Informationen in Ihrer IoC-Datenbank verwendet werden soll. Diese Eigenschaft wird von der Skripteinbindung `ThreatAdditionalInfo` verwendet, um zusätzliche Informationen in das Formular „Erkennbare Elemente“ einzutragen. Standardwert: http://api.ipinfodb.com/v3/ip-country/ **Hinweis:** Die Drittpartei-API „pininfodb.com“ ist ohne zusätzliche Kosten verfügbar und wird in vielen gewerblichen Softwareprogrammen verwendet. Wenn Sie ihn durch einen anderen Domänennamen ersetzen, müssen Sie auch den API-Schlüssel im nächsten Feld angeben.
Der API-Schlüssel, der für die Domäne verwendet werden soll, falls vorhanden sn_ti.ip_lookup.api_key	Der API-Schlüssel zum Abrufen zusätzlicher Informationen in Ihrer IoC-Datenbank. Diese Eigenschaft wird (zusammen mit der Eigenschaft sn_ti.ip_lookup.web_site) von der Skripteinbindung `ThreatAdditionalInfo` verwendet, um zusätzliche Informationen in das Formular „Erkennbare Elemente“ einzutragen.
Führen Sie keine automatisierte Bedrohungssuche für ein erkennbares Element aus, wenn das erkennbare Element einem IoC zugeordnet ist oder als schädlich eingestuft wird. sn_ti.scan_ioc_before_sending **Hinweis:** Sie müssen die Dauer in der nächsten Eigenschaft (sn_ti.scan_ioc_num_days) definieren.	Option zum Beenden der Ausführung der automatisierten Bedrohungssuche für ein erkennbares Element, wenn das erkennbare Element für die konfigurierte Dauer (in Tagen) als schädlich oder einem IoC zugeordnet erkannt wird. Wenn Sie die Bedrohungssuche für das erkennbare Element dennoch ausführen müssen, können Sie dies manuell tun. Standardwert: Ja
Dauer (in Tagen) sn_ti.scan_ioc_num_days	Option zum Definieren der Dauer, bis die automatisierte Bedrohungssuche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	des erkennbaren Elements übersprungen wird. Standardwert (in Tagen): 30
Führen Sie keine automatisierte Bedrohungssuche für ein erkennbares Element aus, wenn es bereits ausgeführt wird. sn_ti.enable_threat_lookup_bypass **Hinweis:** Sie müssen die Dauer in der nächsten Eigenschaft (sn_ti.threat_lookup_bypass_times) definieren.	Wenn für ein bereits erkennbares Element ein Ergebnis der Bedrohungssuche vorhanden ist, können Sie die erneute Ausführung der automatisierten Bedrohungssuche für dasselbe erkennbare Element überspringen, bis die konfigurierte Dauer verstrichen ist. Standardwert: Nein **Hinweis:** Wenn Sie diese Eigenschaft aktivieren, stellen Sie sicher, dass Sie einen geeigneten Wert hinzufügen.
Dauer (in Minuten) sn_ti.threat_lookup_bypass_time	Option zum Definieren der Dauer, nach der die automatisierte Bedrohungssuche für das erkennbare Element erneut ausgeführt werden kann. Standardwert (in Minuten): 0
Legen Sie eine Gültigkeitsdauer für Anwenderüberschreibungen für die Suche erkennbarer Elemente fest. sn_ti.enable_observable_finding_system_override **Hinweis:** Sie müssen die Gültigkeit in der nächsten Eigenschaft (sn_ti.observable_finding_override_expiry) definieren.	Option zum Festlegen einer Gültigkeitsdauer für Anwenderüberschreibungen der erkennbaren Elementergebnisse. Das Ergebnis der Bedrohungssuche des erkennbaren Elements wird während dieser Gültigkeitsdauer nicht vom Basissystem geändert. Standardwert: Nein **Hinweis:** Wenn Sie diese Eigenschaft aktivieren, stellen Sie sicher, dass Sie einen geeigneten Wert hinzufügen.
Gültigkeit (in Minuten) sn_ti.observable_finding_override_expiry	Option zum Definieren des Gültigkeitszeitraums des Ergebnisses erkennbarer Elemente. Standardwert (in Minuten): keine
Wenn ein Angriffsmodus/eine Angriffsmethode für die angegebene Anzahl von Tagen von keiner Quelle empfangen wurde, markieren Sie ihn/sie als inaktiv sn_ti.attack_mode_inactivate_days	Anzahl der Tage ab dem letzten Empfang eines Angriffsmodus/einer Angriffsmethode, bis der Datensatz als inaktiv markiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Standardwert: 360 **Hinweis:** Das Kontrollkästchen **„Aktiv“** ist im Formular **„Angriffsmodus/ -methode“** standardmäßig nicht sichtbar. Sie können ihn jedoch hinzufügen. Wenn Angriffsmodi/-methoden inaktiv sind, können sie in anderen Formularen nicht ausgewählt werden.
Wenn ein Indikator für die angegebene Anzahl von Tagen von keiner Quelle empfangen wurde, markieren Sie ihn als inaktiv sn_ti.indicator_inactivate_days	Anzahl der Tage ab dem letzten Empfang eines Indikators für den Datensatz, der als inaktiv markiert wird. Standardwert: 180 **Hinweis:** Die Checkbox **Aktiv** ist im **Indikatorformular** standardmäßig nicht sichtbar. Sie können ihn jedoch hinzufügen. Wenn Indikatoren inaktiv sind, können sie in anderen Formularen nicht ausgewählt werden.
Die maximale Nutzlastgröße (in MB) für einen STIX-Anhang, der analysiert werden kann. sn_ti.stix.max_payload_size	Gibt die maximale Nutzlastgröße für den STIX-Anhang an, die Sie analysieren können. Standardwert: keiner Maximal zulässiger Wert: Kein Grenzwert.
Maximale Zeit in Sekunden, die eine ausgehende HTTP-Verbindung wartet, um TAXII-Sammlungsdaten abzurufen sn_ti.taxi.http.max_timeout	Gibt an, wie lange eine ausgehende HTTP-Verbindung maximal wartet, bevor das nächste Paket von TAXII-Sammlungsdaten abgerufen wird. Standardwert: 300
Maximale Anzahl von Objekten, die in einem REST-Aufruf von einem TAXII-Server abgerufen werden (gilt nur für TAXII-Versionen 2.0 und 2.1) sn_ti.taxi.max_page_size	Gibt die maximale Anzahl von Objekten an, die in einem REST-Aufruf vom TAXII-Server für eine Seite abgerufen werden. Standardwert: 5000 Maximal zulässiger Wert: 50.000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Maximale Anzahl von Wiederholungen für einen fehlgeschlagenen TAXII 2.X-REST-Aufruf sn_ti.taxi2.retry_count	Gibt die maximale Anzahl von Wiederholungen für einen fehlgeschlagenen TAXII-REST-Aufruf an. Standardwert: 3

3. Klicken Sie auf **Speichern**.

Definieren Sie eine Bedrohungsquelle

Sie können eine Liste von Threat Intelligence Bedrohungsquellen verwalten. Für jede Quelle lässt sich festlegen, wie häufig eine Quelle abgefragt wird. Sie können auch bei Bedarf eine Bedrohungsquelle ausführen, um die benötigten STIX-Daten (Structured Threat Information eXpression) zu importieren.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Warum und wann dieser Vorgang ausgeführt wird

Threat Intelligence nutzt zwei Technologien zum Importieren von Bedrohungsinformationen: STIX und Trusted Automated Exchange of Indicator Information (TAXII).

STIX bietet eine standardisierte, strukturierte Sprache für die Darstellung eines umfangreichen Satzes von Cyberbedrohungsinformationen, einschließlich Indikatoren für Kompromittierungsaktivitäten (IoC) (z. B. IP-Adressen und Datei-Hashes) sowie kontextbezogene Informationen zu Bedrohungen, z. B. Angriffsmodi/-methoden die zusammen die Motivationen, Fähigkeiten und Aktivitäten eines Cyberangreifers umfassender charakterisieren. Daher liefern STIX-Daten wertvolle Informationen darüber, wie sich Ihr Unternehmen am besten gegen Cyberbedrohungen schützen kann.

Trusted Automated Exchange of Indicator Information (TAXII) wird verwendet, um den automatisierten Austausch von Informationen zu Cyberbedrohungen zu erleichtern. TAXII definiert eine Reihe von Services und Nachrichtenaustauschen, die den Austausch von umsetzbaren Cyberbedrohungsinformationen über Organisations- und Produkt-/Servicegrenzen hinweg ermöglichen, um Cyberbedrohungen zu erkennen, zu verhindern und zu mindern. TAXII-Profile können als Repositorys für die gemeinsame Nutzung von STIX-formatierten Informationen eingerichtet werden. Jedes Profil enthält eine oder mehrere TAXII-Sammlungen oder -Feeds.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **Bedrohungsquellen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Bedrohungsquelle.
Anwendung	Die Anwendung, die diesen Datensatz enthält.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Bedrohungsquelle zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um die Skripts in den Feldern **Integrationswerksskript** und **Berichtsprozessor** anzuzeigen.
Beschreibung	Eine Beschreibung dieser Bedrohungsquelle.

4. Füllen Sie die Felder im Abschnitt **Zeitplan** entsprechend aus.

Feld	Beschreibung
Ausführen	Die Häufigkeit, mit der die Integration ausgeführt werden soll: Täglich, Wöchentlich, Regelmäßig usw. Wie bereits erwähnt, werden nachfolgende Felder basierend auf der Einstellung dieses Felds angezeigt.
Tag	Der Tag, an dem die Integration ausgeführt werden soll. ◦ Wenn Sie **Wöchentlich** im Feld **Ausführen** ausgewählt haben, zeigt dieses Feld die Wochentage an. ◦ Wenn Sie **Monatlich** im Feld **Ausführen** ausgewählt haben, zeigt dieses Feld die Tage des Monats an.
Zeit	Zeitpunkt, zu dem die Integration starten soll.
Wiederholungsintervall	Wenn Sie im Feld **Ausführen** die **Option Regelmäßig** ausgewählt haben, zeigt dieses Feld die Anzahl der Tage und Stunden an, bevor die Integration erneut ausgeführt wird.
Wird gestartet	Wenn Sie im Feld **Ausführen** die **Option Regelmäßig** ausgewählt haben, zeigt dieses Feld die Datums- und Uhrzeitangaben an, die als Ausgangspunkt für regelmäßige Aktualisierungen verwendet werden sollen.
Bedingt	Wählen Sie dieses Feld aus, wenn Sie bedingte Parameter hinzufügen möchten.
Bedingung	Wenn Sie das **Kontrollkästchen** Bedingung aktiviert haben, geben Sie die Bedingungen hier ein.

5. Füllen Sie die Felder im Abschnitt **Bedrohungsdetails** entsprechend aus.

Feld	Beschreibung
Indikator	Der zu verwendende Indikator, wenn die Daten keinen expliziten bereitstellen. Wenn Sperrlisten leer sind, wird für jedes erkennbare Element ein neuer Indikator erstellt.
Indikatortyp	Der Indikatortyp zur Verwendung für Indikatoren, die erstellt werden und deren Daten nicht explizit einen Indikatortyp bereitstellen.
Angriffsmodus/-methode	Der zu verwendende Angriffsmodus/die zu verwendende Angriffsmethode, wenn die Daten keinen explizit bereitstellen.
Erkennbarer Typ	Der erkennbare Typ, der für erkennbare Elemente verwendet werden soll, die erstellt werden und deren Daten nicht explizit einen erkennbaren Typ bereitstellen.[SI1]
Gewichtung	Geben Sie einen Gewichtungswert für diese Quelle ein, der in der Konfidenzberechnung verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Verwendung der Felder **Indikator**, **Indikatortyp**, **Angriffsmodus/Angriffsmethode**und **Typ erkennbarer Elemente** ist abhängig von der Implementierung. Der Standardprozessor SimpleBlocklistProcessor verhält sich wie in den Tooltips beschrieben. Eine TAXII-Bedrohungsquelle ist jedoch vollständig datengesteuert. Jeder anwenderdefinierte Bedrohungsquellprozessor kann seine eigene Strategie verwenden. Diese Felder sind im Grunde Elemente, die der Integration/dem Prozessor zur Verfügung gestellt werden, und die Implementierung entscheidet, wie sie verwendet werden.

6. Füllen Sie die Felder im Abschnitt **Quellendetails** entsprechend aus.

Feld	Beschreibung
Endpunkt	Geben Sie die Webservice-Endpunkt-URL ein, mit der über Threat Intelligenceauf die Bedrohungsquelle zugegriffen wird. Klicken Sie auf das Schlosssymbol, um die URL zu sperren.
Verwenden Sie die REST-Nachricht	Wenn Sie eine REST-Nachricht benötigen, um auf die Bedrohungsquelle zuzugreifen, aktivieren Sie dieses Kontrollkästchen. Die Felder **„REST-Nachricht“** und **„REST-Methode“** werden zu Pflichtfeldern.
REST-Nachricht	Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Nachricht aus der Liste aus, oder klicken Sie auf **Neu,** um eine neue REST-Nachricht zu definieren.
REST-Methode	Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Methode aus der Liste aus, oder klicken Sie auf **Neu**, um eine neue REST-Methode zu definieren.
Integrationsskript	Das standardmäßige -Integrationsskript ist **SimpleRESTSecurityDataIntegration**. Sie führt einen einfachen REST-Aufruf aus, speichert die Antwort als Anhang und gibt den Anhang dann an den Prozessor zurück. Dieses Skript erfüllt die Anforderungen der meisten Organisationen. Wenn Sie möchten, können Sie jedoch auf das Suchsymbol klicken und ein anderes Integrationsskript auswählen oder ein neues definieren.
Integrationswerksskript	Wenn das Kontrollkästchen **Erweitert** aktiviert ist, zeigt dieses Feld das tatsächliche Skript zum Erstellen des Integrationsskripts an. Sie können das Skript nach Bedarf bearbeiten. Diese Fähigkeit ist für anwenderdefinierte Implementierungen nützlich. Integrationen im Basissystem benötigen normalerweise keine anwenderdefinierte Konstruktorlogik.
Berichtsprozessor-Skript	Das standardmäßige -Integrationsskript ist **SimpleBlocklistProcessor**. Dieses Skript ist ein einfacher Prozessor, der eine einfache Sperrliste (einfach, d. h. ein einspaltiges Dokument mit erkennbaren Elementen wie URLs oder IP-Adressen) akzeptiert und erkennbare Elemente erstellt. Es verwendet die verschiedenen Felder **für Bedrohungsdetails**, um zu bestimmen, welche Felder festgelegt werden, wenn erkennbare Elemente erstellt werden.
Prozessorwerksskript	Wenn die Checkbox **Advanced** aktiviert ist, zeigt dieses Feld das tatsächliche Skript zum Erstellen des Prozessors an. Sie können das Skript nach Bedarf bearbeiten. Dieses Skript ist im Allgemeinen für anwenderdefinierte Implementierungen nützlich. Die Integrationen im Basissystem benötigen normalerweise keine anwenderdefinierte Konstruktorlogik.

7. Klicken Sie auf **Absenden**.

Hinweis:
Weitere Informationen zum Konfigurieren der Paginierung der Bedrohungsquelle finden Sie im Artikel KB1213825.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein TAXII-Profil

Sie können TAXII-Profile für die gemeinsame Nutzung von STIX-formatierten Informationen verwalten. Jedes Profil enthält eine oder mehrere TAXII-Sammlungen oder -Feeds.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **TAXII-Profile**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die folgenden Felder entsprechend aus.
4. Füllen Sie die Felder im Abschnitt **Discovery-Servicekonfiguration** entsprechend aus.
5. Füllen Sie die Felder im Abschnitt **Sammlungsservicekonfiguration** entsprechend aus.
6. Klicken Sie auf **Absenden**.

IoC-Repository

Das IoC-Repository enthält STIX-Objekte. Jedes dieser Objekte enthält eine bestimmte Information.

Wenn Sie STIX-Objekte über Beziehungen miteinander kombinieren, ermöglichen Sie einfache oder komplexe Darstellungen von Cyber Threat Intelligence (CTI).

Threat Intelligence unterstützt die STIX-Versionen 1.1, 2.0 und 2.1.

Angriffsmodi und -methoden

Angriffsmodi und -methoden, manchmal auch als Taktiken, Techniken und Verfahren (TTPs) bezeichnet, sind Darstellungen des Verhaltens von Cyberangreifern. Sie charakterisieren das, was diese Angreifer tun und wie sie es tun, mit zunehmendem Detailgrad. Angriffsmodi und -methoden gelten für STIX 1.1.

Ein Angriffsmodus/eine Angriffsmethode könnte beispielsweise darin bestehen, Malware zu verwenden, um Anmeldeinformationen für Kreditkarten zu stehlen. Oder eine andere, zugehörige Taktik (auf einer niedrigeren Detailstufe) könnte darin bestehen, gezielt E-Mails mit Anhängen zu senden, die schädlichen Code enthalten, der beim Öffnen ausgeführt wird, Kreditkarteninformationen durch Tastenanschläge erfasst und HTTP für die Kommunikation mit einem Befehls- und Steuerungsserver verwendet Transferinformationen.

Angriffsmodi und -methoden gelten für STIX 1.1.

Definieren Sie einen Angriffsmodus/eine Angriffsmethode

Angriffsmodi und -methoden werden mit STIX-Daten importiert, Sie können jedoch nach Bedarf neue Modi/Methoden hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie Klassifizierungs-Tags einrichten und aktiviert haben, um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Vertraulichkeit des Angriffsmodus/der Angriffsmethode anzugeben. Wenn Sie keine Klassifizierungs-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Titel	Geben Sie einen beschreibenden Namen für diesen Angriffsmodus/diese Methode ein.
Malware-Typ	Wählen Sie den Malware-Typ für diesen Angriffsmodus/diese Methode aus. Die verfügbaren Malware-Typen werden als STIX-Daten vom Lieferantenserver abgerufen.
Quelle	Wählen Sie die Bedrohungsdatenquelle für diesen Angriffsmodus/diese Methode aus. Einige Datenquellen sind im Basissystem enthalten. Sie können nach Bedarf neue Datenquellen erstellen.
Angriffsmechanismus	Wählen Sie den Angriffsmechanismus für diesen Angriffsmodus/diese Methode aus. Angriffsmechanismen stellen die verschiedenen Techniken dar, die zum Angriff auf ein System verwendet werden. Die verfügbaren Angriffsmechanismen werden als STIX-Daten vom Server des Lieferanten abgerufen.
Erstmals aufgetreten	Dieses Datum wird als STIX-Daten vom Lieferantenserver abgerufen.
Zuletzt aufgetreten	Dieses Datum wird als STIX-Daten vom Lieferantenserver abgerufen.
Typ Bedrohungsakteur	Wählen Sie den Bedrohungsakteurtyp für diesen Angriffsmodus/diese Angriffsmethode aus. Bedrohungsakteurtypen charakterisieren böswillige Akteure (oder Angreifer), die eine Cyberangriffsbedrohung darstellen, einschließlich vermuteter Absichten und historisch beobachtetes Verhalten. Die verfügbaren Bedrohungsakteurtypen werden als STIX-Daten vom Lieferantenserver abgerufen.
Beschreibung	Geben Sie eine Beschreibung des Angriffsmodus/der Angriffsmethode ein.
Handhabung	Geben Sie Anweisungen für den Umgang mit diesem Angriffsmodus/dieser Methode ein.
Beabsichtigte Wirkung	Geben Sie die beabsichtigte Wirkung dieses Angriffstyps ein.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
Sie können eine der folgenden zugehörigen Listen anzeigen, um zusätzliche Informationen anzuzeigen.

Zugehörige Liste	Beschreibung
Zugehörige Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der Bedrohungsquelle identifiziert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Untergeordneter Angriffsmodus/-methode	Listet Angriffsmodi/-methoden auf, die untergeordnete Elemente des übergeordneten Angriffsmodus/der übergeordneten Angriffsmethode sind.
Zugehörige Aufgaben	Listet Changes auf, die dem übergeordneten Angriffsmodus/der übergeordneten Angriffsmethode zugeordnet sind.

Fügen Sie einem Angriffsmodus/einer Angriffsmethode ein IoC hinzu

Zusätzlich zum Import von Indikatoren als STIX-Daten können Sie einem Angriffsmodus/einer manuellen Methode IoCs hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf den Angriffsmodus, dem Sie ein IoC hinzufügen möchten.
3. Klicken Sie auf die **zugehörige Liste Zugehörige Indikatoren**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das IoC zu finden, das Sie hinzufügen möchten.
6. Verwenden Sie den Slushbucket, um das IoC zur Liste **Zugehörige Indikatoren** hinzuzufügen.
7. Klicken Sie auf **Speichern**.

Fügen Sie eine zugehörige Angriffsmodusmethode hinzu

Zusätzlich zum Importieren von Angriffsmodi/-methoden als STIX-Daten können Sie zugehörige Angriffsmodi/-methoden manuell hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf den Angriffsmodus, dem Sie einen zugehörigen Angriffsmodus/eine zugehörige Methode hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste Untergeordneter **Angriffsmodus/-methode**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Angriffsmodus/die Methode zu finden, den Sie mit dem aktuellen verknüpfen möchten.
6. Fügen Sie mithilfe des Slushbucket den Angriffsmodus/die Angriffsmethode der Liste **„Untergeordneter Angriffsmodus/-methode“** hinzu.
7. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einem Angriffsmodus/einer Angriffsmethode die zugeordnete Aufgabe hinzu

Sie können zugehörige Aufgaben (z. B. Changes und Incidents) nicht nur als STIX-Daten importieren, sondern auch manuell einem Angriffsmodus/einer manuellen Methode hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf den Angriffsmodus, dem Sie eine zugehörige Aufgabe hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugeordnete Aufgaben**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu finden, die Sie dem Angriffsmodus/der Angriffsmethode zuordnen möchten.
6. Fügen Sie die Aufgabe mithilfe des Slushbucket der Liste **Zugeordnete Aufgaben** hinzu.
7. Klicken Sie auf **Speichern**.

Kompromittierungsindikatoren

Kompromittierungsindikatoren (IoC) sind Artefakte, die in einem Netzwerk oder Betriebssystem beobachtet werden und wahrscheinlich einen Angriff anzeigen. Typische IoCs sind Virussignaturen und IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen. IoC gilt für STIX 1.1 und 2.x.

Ein IoC kann ein einzelnes erkennbares Element oder eine Sammlung von erkennbaren Elementen sein (z. B. eine einzelne bekanntermaßen ungültige URL oder das Vorhandensein einer bestimmten Datei und einiger spezifischer Registrierungsschlüsselwerte).

Nachdem IoCs im Rahmen der Reaktion auf Incidents und Computerforensik identifiziert wurden, können sie zur Früherkennung zukünftiger Angriffsversuche mithilfe von Angriffserkennungssystemen und Antivirensoftware verwendet werden.

IoC gilt für STIX 1.1 und 2.x.

Zeigen Sie ein IoC an

IoCs, manchmal auch als Indikatoren bezeichnet, werden normalerweise aus einer Bedrohungsdatenquelle als STIX-Daten abgerufen. Bei Bedarf können Sie auch IoCs erstellen.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

Prozedur

1. Nachdem die geplante Aufgabe IoC-Daten aus der definierten Datenquelleabgerufen hat, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
   Die abgerufenen IoCs werden aufgelistet.
2. Klicken Sie auf das IoC, das Sie anzeigen möchten.
3. Die folgenden Informationen werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie Sicherheits-Tags zum Hinzufügen von Metadaten zum Datensatz eingerichtet und aktiviert haben, können Sie ein oder mehrere Tags auswählen, um den Grad der Vertraulichkeit des IoC anzugeben. Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Titel	Ein beschreibender Name für diesen Indikator.
Erstmals aufgetreten	Das erste Datum, an dem dieser Indikator im System beobachtet wurde.
Zuletzt aufgetreten	Das letzte Datum, an dem dieser Indikator im System beobachtet wurde.
Anzahl aufgetretener Werte	Die Anzahl der Fälle, in denen der Indikator gefunden wurde.
Bezogene Anzahl	Die Anzahl der Importe des Indikators aus definierten Bedrohungsquellen.
Notizen	Zusätzliche Hinweise zum Indikator. Dieses Feld kann auch JSON-Schlüssel-Wert-Paare enthalten.

4. Sie können auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die mit dem aktuellen Indikator verknüpft sind.
Zugehöriger Angriffsmodus/ zugehörige Angriffsmethode	Listet zugehörige Angriffsmodi/-methoden auf, die im Zusammenhang mit diesem Indikator identifiziert wurden.
Zugeordneter Typ	Listet andere Indikatortypen auf, die diesem IoC zugeordnet sind.
Indikatorquellen	Listet die Quellen dieses Indikators zusammen mit dem Konfidenzniveau der Quelle auf.
Zugehörige Aufgaben	Listet alle Aufgaben, Changes und Incidents auf, die dem IoC zugeordnet sind.
Indikator-Metadaten	Wenn das Feld **Notizen** gültige JSON-Schlüssel-Wert-Paare enthält, werden sie analysiert und angezeigt. Wenn keine JSON-Schlüssel-Wert-Paare vorhanden sind oder wenn JSON ungültig ist, wird diese zugehörige Liste nicht angezeigt.
Sicherheitsanmerkungen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Externe Referenzen des Indikators	
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.

Fügen Sie einem IoC ein zugehöriges erkennbares Element hinzu

Sie können erkennbare Elemente nicht nur als STIX-Daten importieren, sondern auch zugehörige erkennbare Elemente manuell zu einem IoC hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie ein zugehöriges erkennbares Element hinzufügen möchten.
3. Klicken Sie auf die **zugehörige Liste Zugehörige erkennbare Elemente**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das erkennbare Element zu finden, das Sie mit dem IoC verknüpfen möchten.
6. Verwenden Sie den Slushbucket, um das erkennbare Element der Liste **Zugehörige erkennbare Elemente** hinzuzufügen.
7. Klicken Sie auf **Speichern**.

Fügen Sie einem IoC einen zugehörigen Angriffsmodus/eine zugehörige Angriffsmethode hinzu

Zusätzlich zum Importieren zugehöriger Angriffsmodi/-methoden als STIX-Daten können Sie zugehörige Angriffsmodi/-methoden manuell zu einem IoC hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie einen zugehörigen Angriffsmodus/eine zugehörige Angriffsmethode hinzufügen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die zugehörige Liste **Zugehöriger Angriffsmodus/-methode**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Angriffsmodus/die Methode zu finden, den Sie mit dem IoC verknüpfen möchten.
6. Fügen Sie den Angriffsmodus/die Angriffsmethode mithilfe des Slushbucket der Liste **Zugehöriger Angriffsmodus/-methode** hinzu.
7. Klicken Sie auf **Speichern**.

Identifizieren Sie die zugehörigen Indikatortypen

Wenn für ein IoC keine zugehörigen Indikatortypen definiert sind, werden alle Arten von erkennbaren Elementen nachverfolgt. Wenn Sie jedoch einem IoC einen oder mehrere Arten von Indikatoren zuordnen, schränkt dies die Typen der erkennbaren Elemente ein, die dem IoC zugeordnet werden können.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie einen Indikatortyp zuordnen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugeordneter Typ**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Indikatortyp zu finden, den Sie dem IoC zuordnen möchten.
6. Fügen Sie den Indikatortyp mithilfe des Slushbucket der Liste **Zugeordneter Typ** hinzu.
7. Klicken Sie auf **Speichern**.

Identifizieren Sie Indikatorquellen

Indikatorquellen werden normalerweise automatisch als Teil des Bedrohungsimportvorgangs nachverfolgt, es können jedoch weitere Quellen manuell hinzugefügt werden.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie Indikatorquellen hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Indikatorquellen**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Indikatorquelle zu finden, die Sie dem IoC zuordnen möchten.
6. Fügen Sie die Indikatorquelle mithilfe des Slushbucket der Liste **Indikatorquellen** hinzu.
7. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einem IoC zugeordnete Aufgaben hinzu

Sie können zugeordnete Aufgaben (z. B. Changes und Incidents) nicht nur als STIX-Daten importieren, sondern auch manuell einem IoC hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf das IoC, dem Sie eine zugehörige Aufgabe hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugeordnete Aufgaben**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu finden, die Sie dem IoC zuordnen möchten.
6. Fügen Sie die Aufgabe mithilfe des Slushbucket der Liste **Zugeordnete Aufgaben** hinzu.
7. Klicken Sie auf **Speichern**.

Erkennbare Elemente

Erkennbare Elemente stellen zustandsbehaftete Eigenschaften (z. B. den MD5-Hash einer Datei oder den Wert eines Registrierungsschlüssels) oder messbare Ereignisse (z. B. die Erstellung eines Registrierungsschlüssels oder das Löschen einer Datei) dar, die für den Betrieb von Computern und Netzwerken relevant sind . Erkennbare Elemente gelten für STIX 1.1 und 2.x.

Sätze von erkennbaren Cyberelementen sind nützlich, um Gefährdungsindikatoren zu identifizieren, wenn sie mit kontextbezogenen Informationen kombiniert werden, die das Verhalten von Cyberbedrohungen darstellen.

Erkennbare Elemente gelten für STIX 1.1 und 2.x.

Definieren Sie ein erkennbares Element

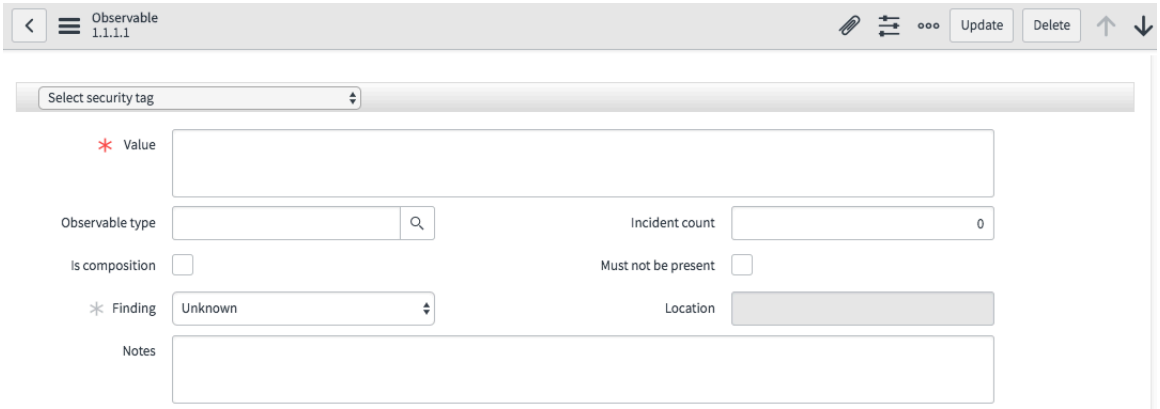
Erkennbare Elemente werden vom Server des Lieferanten als STIX-Daten abgerufen. Sie können jedoch bei Bedarf erkennbare Elemente erstellen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie Sicherheits-Tags zum Hinzufügen von Metadaten zum Datensatz eingerichtet und aktiviert haben, können Sie ein oder mehrere Tags auswählen, um den Grad der Vertraulichkeit des erkennbaren Elements anzugeben. Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Wert	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist. **Hinweis:** Wenn eine Bedrohungsprüfung eine IP-Adresse oder einen Hash durchführt, Malware zurückgegeben oder ein anderer Fehler auftritt, werden die IP-Adresse oder der Hash-Wert automatisch der Tabelle „Erkennbares Element“ [sn_ti_observable] hinzugefügt. Daher kann im Formular „Erkennbare Elemente“ gesucht werden.
Erkennbarer Typ	Wählen Sie die Klassifizierung des erkennbaren Elements aus, z. B. eine IP-Adresse oder einen Datei-Hash. Diese erkennbaren Typen sind im Modul **„Erkennbare Typen“** definiert.
Incident-Anzahl	Die Häufigkeit, mit der der Wert des erkennbaren Elements gefunden wurde.
Ist Zusammensetzung	Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn der **Typ des erkennbaren Elements** auf etwas anderes als **Zusammensetzung des erkennbaren Elements**festgelegt ist und dieses neue erkennbare Element eine Zusammensetzung ist, aktivieren Sie dieses Kontrollkästchen. Wenn der **Typ des erkennbaren Elements** bereits auf **Zusammensetzung des erkennbaren Elements**festgelegt ist, ist das Kontrollkästchen aktiviert und schreibgeschützt. Eine erkennbare Elementzusammensetzung ist ein erkennbares Element, das untergeordnete erkennbare Elemente enthält.
Ergebnis	Wählen Sie eine der folgenden Optionen aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Böswillig**: Gibt an, dass das erkennbare Element für die Organisation schädlich ist. ○ **Verdächtig**: Gibt an, dass das erkennbare Element für die Organisation schädlich sein könnte. ○ **Clean**: Gibt an, dass das erkennbare Element für die Organisation nicht schädlich ist. ○ **Unbekannt**: Gibt an, dass der Fund des erkennbaren Elements noch bestimmt werden muss. ○ Standardwert: Unbekannt. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche. **Hinweis:** Nach einem Upgrade werden vorhandene erkennbare Elemente als schädlich markiert.
Betreiber	Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Ist Zusammensetzung** aktiviert ist. Abhängig von Ihrer Einstellung in diesem Feld werden die erkennbaren Elemente und ihre untergeordneten Elemente bei der Entscheidung, ob ein zugehöriger Indikator vorhanden ist, berücksichtigt. Legen Sie dieses Feld auf **UND** fest, wenn alle untergeordneten erkennbaren Elemente vorhanden sein müssen, damit ein zugeordneter Indikator als vorhanden betrachtet wird. Legen Sie diese Option auf **ODER** fest, wenn eines der untergeordneten erkennbaren Elemente vorhanden ist, damit ein zugeordneter Indikator als vorhanden betrachtet wird.
Darf nicht vorhanden sein	Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn diese Option ausgewählt ist, gibt dieses Feld an, dass das potenzielle Problem in der Abwesenheit des erkennbaren Elements liegt (z. B. in einem fehlenden Registrierungsschlüssel).
Standort	Mit den Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie Laden Sie weitere IoC-Daten in dieses Feld laden.
Notizen	Geben Sie zusätzliche Notizen zum erkennbaren Element ein.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**. Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

Zugehörige Liste	Beschreibung
Zugehörige Indikatoren	Listet Indikatoren auf, die von der Bedrohungsquelle identifiziert wurden.
Zugehörige Aufgaben	Listet Changes auf, die dem erkennbaren Element zugeordnet sind.
Untergeordnete erkennbare Elemente	Listet zugehörige erkennbare Elemente auf, die von der Bedrohungsquelle identifiziert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Übereinstimmende Ressourcen für IP	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die über eine übereinstimmende IP-Adresse verfügen.
Quelle erkennbare Elemente	Listet die Quellen dieses erkennbaren Elements zusammen mit dem Konfidenzniveau der Quelle auf.
Sicherheitsanmerkungen	Listet Sicherheitsanmerkungen auf, die diesem erkennbaren Element hinzugefügt wurden.

Fügen Sie einem erkennbaren Element ein zugehöriges IoC hinzu

Sie können erkennbare Elemente nicht nur als STIX-Daten importieren, sondern auch zugehörige erkennbare Elemente manuell zu einem IoC hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie ein zugehöriges IoC hinzufügen möchten.
3. Klicken Sie auf die **zugehörige Liste Zugehörige Indikatoren**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Indikator zu finden, den Sie mit dem erkennbaren Element verknüpfen möchten.
6. Fügen Sie den Indikator mithilfe des Slushbucket der Liste **Zugehörige Indikatoren** hinzu.
7. Klicken Sie auf **Speichern**.

Fügen Sie einem erkennbaren Element zugeordnete Aufgaben hinzu

Sie können zugehörige Aufgaben (z. B. Changes und Incidents) nicht nur als STIX-Daten importieren, sondern auch manuell zu einem erkennbaren Element hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie eine zugehörige Aufgabe hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugeordnete Aufgaben**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu finden, die dem erkennbaren Element zugeordnet werden sollen.
6. Fügen Sie die Aufgabe mithilfe des Slushbucket der Liste **Zugeordnete Aufgaben** hinzu.
7. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie ein zugehöriges erkennbares Element hinzu

Sie können erkennbare Elemente nicht nur als STIX-Daten importieren, sondern auch zugehörige erkennbare Elemente manuell hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie ein zugehöriges erkennbares Element hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste Untergeordnete **erkennbare Elemente**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das erkennbare Element zu finden, das Sie mit dem aktuellen Element verknüpfen möchten.
6. Fügen Sie das erkennbare Element mithilfe des Slushbucket der Liste **Untergeordnete erkennbare Elemente** hinzu.
7. Klicken Sie auf **Speichern**.

Laden Sie weitere IoC-Daten

Abhängig von den Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie Positionsbestimmungsinformationen für IP-Adressen und Websites im Formular „Erkennbare Elemente“ laden. Mit weiterer Anpassung können Sie auch andere Informationen hinzufügen, z. B. Ländercodes, Ortsnamen.

Vorbereitungen

Die folgenden beiden Eigenschaften müssen festgelegt werden:

- **Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs** [sn_ti.ip_lookup.web_site]
- **Der API-Schlüssel, der für die obige Domäne verwendet werden soll, falls vorhanden** [sn_ti.ip_lookup.api_key]

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf die IP-Adresse oder URL des erkennbaren Elements, für das Sie weitere IoC-Daten anzeigen möchten.
   Das Feld **Standort** zeigt die Positionsbestimmung des IoC an.
3. Klicken Sie auf die Schaltfläche **Daten ergänzen**, um die zusätzlichen IoC-Daten zu laden.
4. Sie können das Formular „Erkennbares Element“ auch so konfigurieren, dass andere standortbezogene Felder hinzugefügt werden, z. B. der Ländercode und der Ortscode.

> **Hinweis:**
> Um weitere standortbezogene Informationen zu laden, bearbeiten Sie die Skripteinbindung **ThreatAdditionalInfo**, und geben Sie den entsprechenden API-Schlüssel von der Website an, die die zusätzlichen Informationen bereitstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifizieren Sie Quellen erkennbarer Elemente

Wenn für ein erkennbares Element keine Quellen definiert sind, werden alle Arten von Quellen verwendet. Wenn Sie jedoch einem erkennbaren Element eine oder mehrere Bedrohungsquellen hinzufügen, werden die verwendeten Quellen eingeschränkt.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie Quellen für erkennbares Element hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **„Quellen erkennbarer Elemente“**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Quelle zu finden, die dem erkennbaren Element zugeordnet werden soll.
6. Verwenden Sie den Slushbucket, um die Quelle des erkennbaren Elements der Liste **Observable Sources (Erkennbare Quellen)** hinzuzufügen.
7. Klicken Sie auf **Speichern**.

Führen Sie Suchen für erkennbare Elemente durch

Sie können Threat Intelligence-Suchen für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Welche Implementierungen von Scans ausgeführt werden, hängt davon ab, welche Sie aktiviert haben.

Vorbereitungen

Bevor Sie Suchvorgänge durchführen können, müssen Sie das Plugin „Threat Intelligence“ aktivieren. Sie müssen auch das Plugin für eine oder mehrere der Scan-Implementierungen installieren:

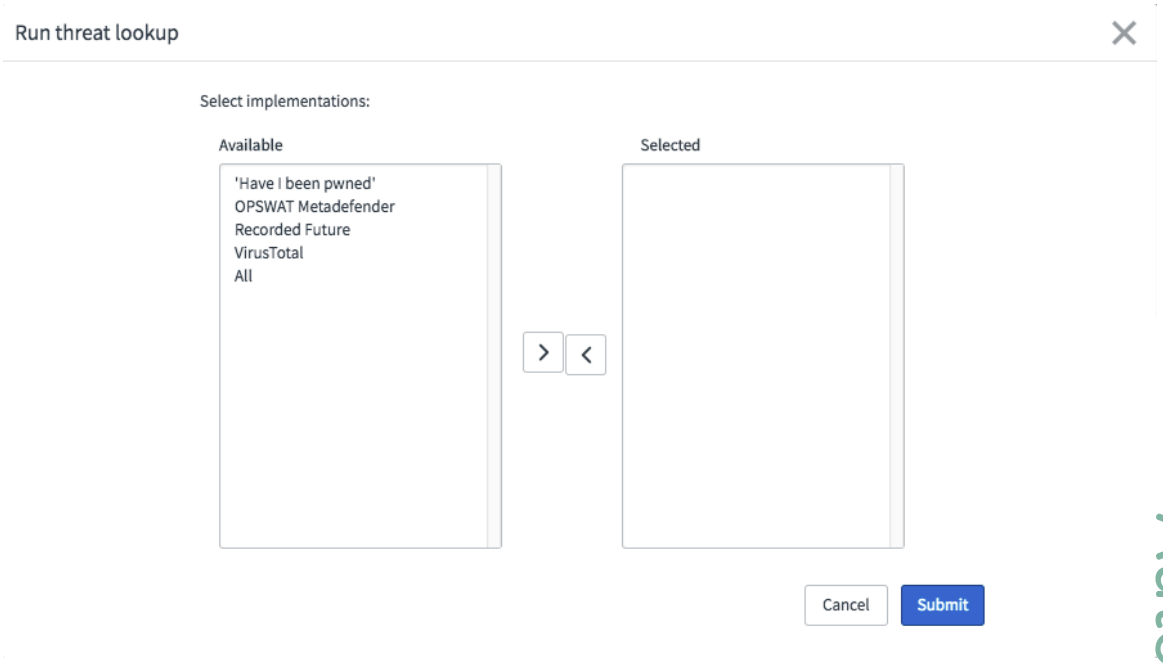
- CrowdStrike Falcon Intelligence-Integration
- OPSWAT Metadefender
- Security Operations – Wurde ich pwned?
- VirusTotal

Erforderliche Rolle: sn_ti.write

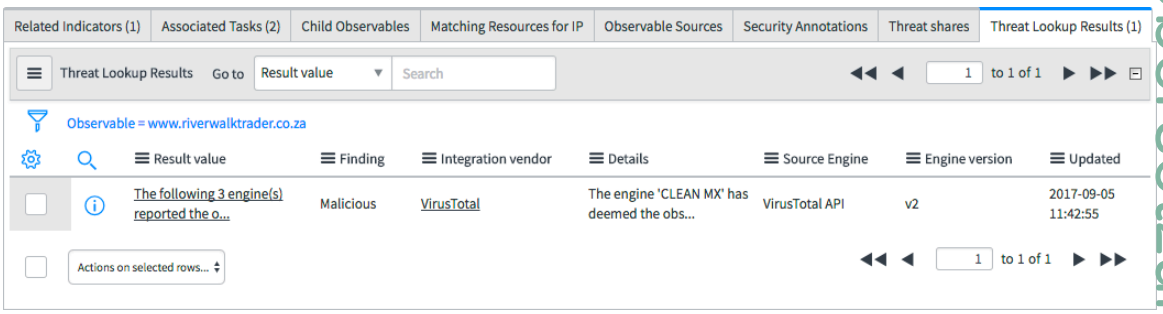
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine Suche für mehr als ein erkennbares Element durchzuführen, wählen Sie die erkennbaren Elemente aus, klicken Sie auf **Aktionen für ausgewählte Zeilen**, und wählen Sie **Suche nach Bedrohungen ausführen**aus.
   - Um eine Suche für ein einzelnes erkennbares Element durchzuführen, öffnen Sie den Datensatz des erkennbaren Elements, und klicken Sie auf den zugehörigen Link **Bedrohungssuche ausführen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie die zu verwendenden Implementierungen der Bedrohungssuche aus, oder wählen Sie **Alle** aus, um Suchen mit allen aktiven Implementierungen durchzuführen, und klicken Sie dann auf **Absenden**. Eine Meldung gibt an, dass die Bedrohungssuchen begonnen haben. Security Operations Integration – Flow zur Bedrohungssuche wird ausgeführt und führt auch die Implementierungs-Workflows für die von Ihnen ausgewählten Implementierungen der Bedrohungssuche aus. Die Suchen werden durchgeführt, und die Ergebnisse werden generiert.
4. Wenn die Suchen abgeschlossen sind, können Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche** klicken, um die Ergebnisse anzuzeigen.



Aktuelles Ergebnis der Bedrohungssuche: Sie können auch die neuesten oder neuesten Ergebnisse der Bedrohungssuche von jedem Integrationsanbieter anzeigen, indem Sie auf die Registerkarte **Aktuelles Ergebnis der Bedrohungssuche** klicken.

Hinweis:
Die Registerkarte **„Ergebnis der aktuellen Bedrohungssuche“** ist nicht Teil des Basissystems.

Um diese Registerkarte zu aktivieren, gehen Sie wie folgt vor:

a. Klicken Sie mit der rechten Maustaste auf den Formularheader.

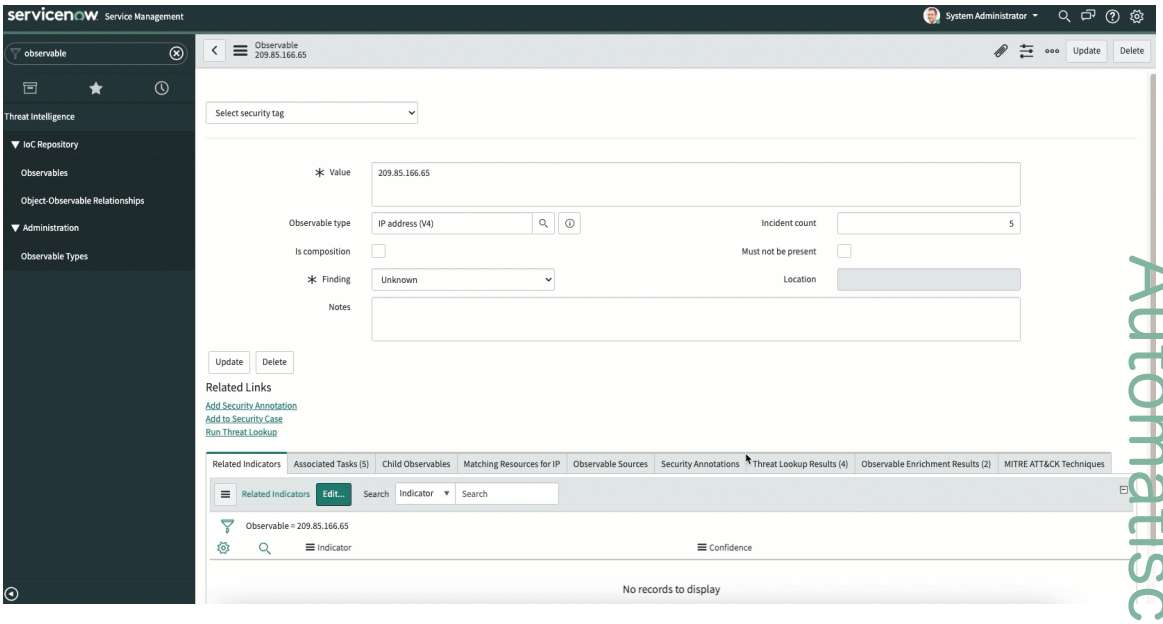
b. Navigieren zu **Konfigurieren** > **Zugehörige Listen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Suchen Sie in der Liste Verfügbar **nach Ergebnissen der Bedrohungssuche,** und verschieben Sie sie in die Liste Ausgewählt.

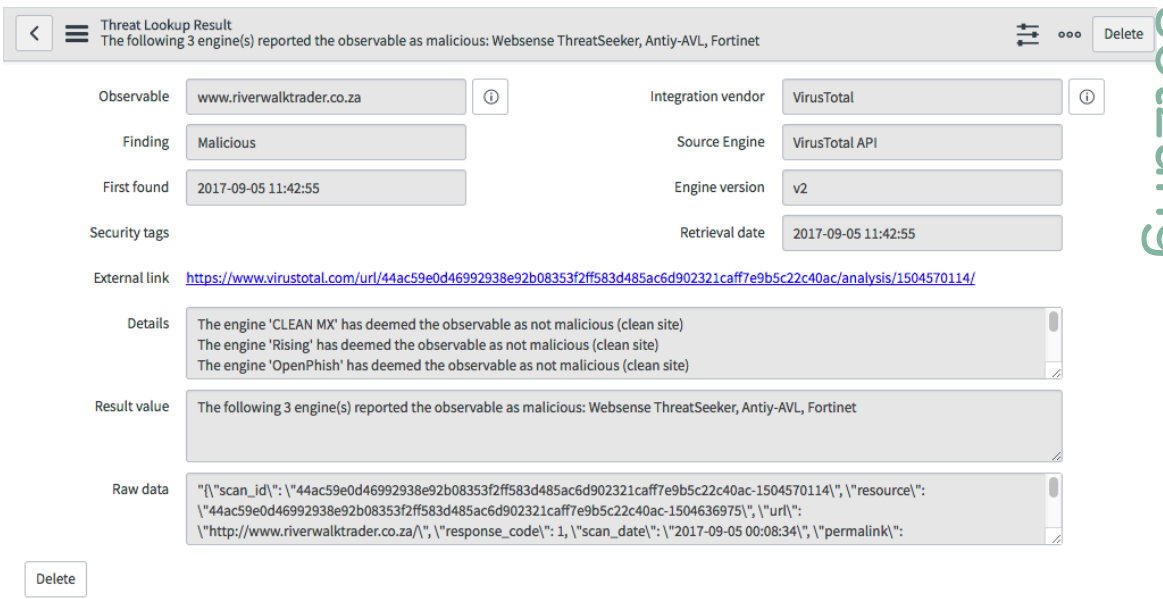
d. Klicken Sie auf **Speichern**.
Sie können jetzt die neuesten Ergebnisse der Bedrohungssuche für jeden Integrationsanbieter auf der Registerkarte **Aktuelles Ergebnis der Bedrohungssuche** anzeigen.



5. Um zusätzliche Details, einschließlich Rohergebnissen für eine bestimmte Suche, anzuzeigen, klicken Sie auf den **Ergebniswert**.

Hinweis:

Wenn die Implementierungen von VirusTotal oder OPSWAT Metadefender verwendet werden, werden die Details wie unten gezeigt konsolidiert.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie eine Bedrohungsanreicherung für erkennbare Elemente durch

Sie können die Threat Intelligence-Anreicherung für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Welche Implementierungen ausgeführt werden, hängt von denen ab, die Sie aktiviert haben.

Vorbereitungen

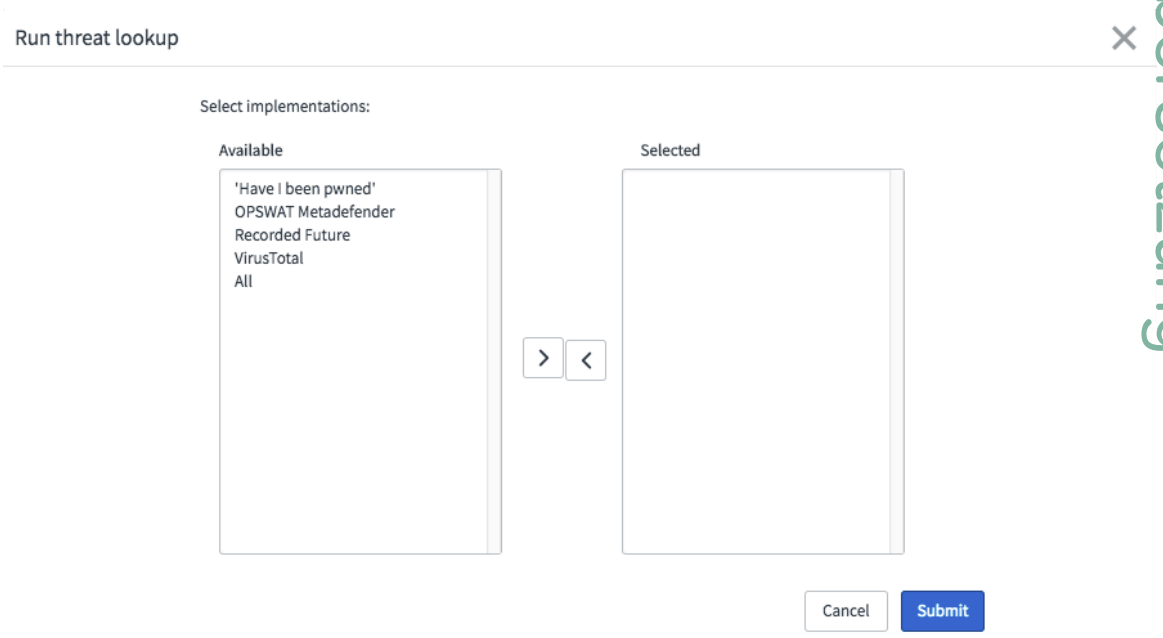
Bevor Sie eine Ergänzung durchführen können, müssen Sie das Plugin „Threat Intelligence“ aktivieren. Sie müssen das Plugin auch für eine oder mehrere Ergänzungsimplementierungen installieren:

- CrowdStrike Falcon Intelligence-Integration
- OPSWAT Metadefender
- Security Operations – Wurde ich pwned?
- VirusTotal
- WhoIs?

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine Suche für mehr als ein erkennbares Element durchzuführen, wählen Sie die erkennbaren Elemente aus, klicken Sie auf **Aktionen für ausgewählte Zeilen**, und wählen Sie **Suche nach Bedrohungen ausführen**aus.
   - Um eine Suche für ein einzelnes erkennbares Element durchzuführen, öffnen Sie den Datensatz des erkennbaren Elements, und klicken Sie auf den zugehörigen Link **Bedrohungssuche ausführen**.



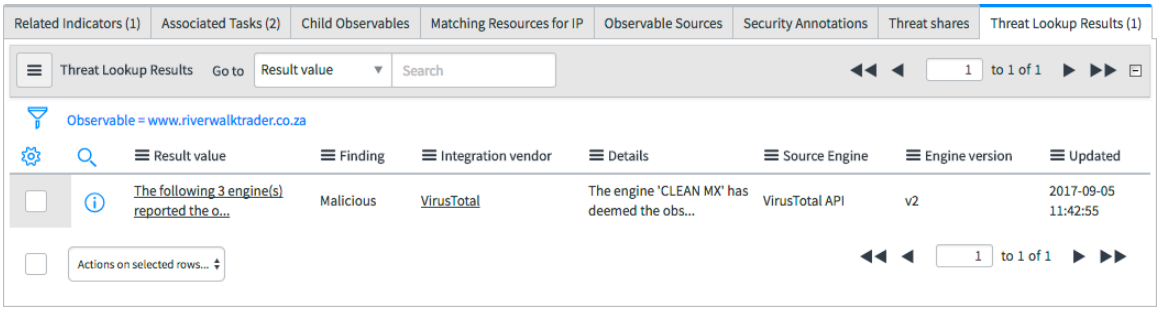
3. Wählen Sie die zu verwendenden Implementierungen der Bedrohungssuche aus, oder wählen Sie **Alle** aus, um Suchen mit allen aktiven Implementierungen durchzuführen, und klicken Sie dann auf **Absenden**. Eine Meldung gibt an, dass die Bedrohungssuchen begonnen haben. Security Operations Integration – Flow zur Bedrohungssuche wird ausgeführt und führt auch die Implementierungs-Workflows für die von Ihnen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

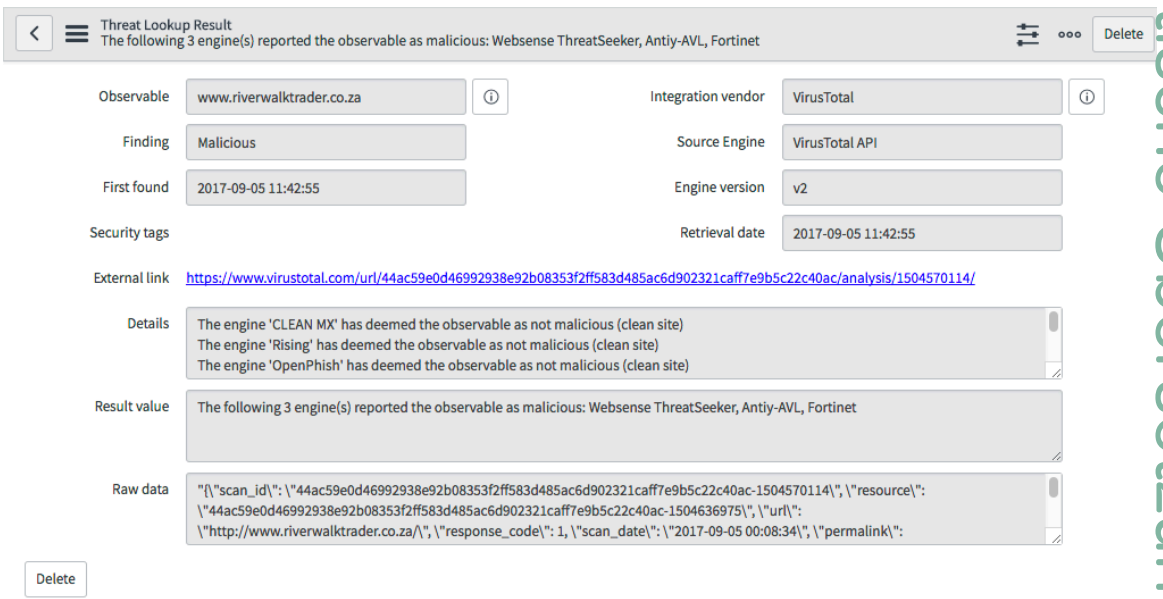
ausgewählten Implementierungen der Bedrohungssuche aus. Die Suchen werden durchgeführt, und die Ergebnisse werden generiert.

4. Wenn die Suchen abgeschlossen sind, können Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche** klicken, um die Ergebnisse anzuzeigen.



5. Um zusätzliche Details, einschließlich Rohergebnissen für eine bestimmte Suche, anzuzeigen, klicken Sie auf den **Ergebniswert**.

Hinweis:
Wenn die Implementierungen von VirusTotal oder OPSWAT Metadefender verwendet werden, werden die Details wie unten gezeigt konsolidiert.



Automatische Übersetzung

Angriffsmuster

Angriffsmuster sind eine Art von Taktiken, Techniken und Verfahren (TTPs), die die Methoden beschreiben, mit denen Angreifer versuchen, Ziele zu gefährden. Angriffsmuster gelten für STIX 2.x.

Angriffsmuster werden zur Kategorisierung von Angriffen verwendet. Sie verallgemeinern bestimmte Angriffe auf die Muster, denen sie folgen, und liefern detaillierte Informationen darüber, wie Angriffe durchgeführt werden.

Spear-Phishing ist beispielsweise eine häufige Art von Angriff, bei der ein Angreifer eine sorgfältig gestaltete E-Mail-Nachricht an eine Partei sendet, um sie dazu zu bringen, auf einen Link zu klicken oder einen Anhang zu öffnen, um Malware zu übermitteln. Angriffsmuster sind spezifischer, z. B. kann Spear-Phishing durch einen bestimmten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungsakteur (z. B. dass das Ziel einen Wettbewerb gewonnen hat) ein Angriffsmuster sein.

Definieren Sie ein Angriffsmuster

Definieren Sie ein Angriffsmuster, um die Kategorisierung von Angriffen zu unterstützen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmuster**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffsmuster zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die mit diesem Objekt verknüpften Aktionen auf, bei denen es sich um technische oder automatisierte Antworten (Patches anwenden, Firewalls neu konfigurieren) handelt, um einen Angriff zu verhindern.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Kampagnen

Eine Kampagne ist eine Gruppierung von Angreiferverhalten. Diese Verhalten beschreiben eine Reihe von böswilligen Aktivitäten oder Angriffen, die im Laufe der Zeit gegen eine bestimmte Gruppe von Zielen auftreten. Kampagnen gelten für STIX 2.x.

Kampagnen haben normalerweise gut definierte Ziele und können Teil eines Angriffssatzes sein.

Kampagnen werden häufig einem Angriffssatz und Bedrohungsakteuren zugeordnet. Die Bedrohungsakteure können die bekannte Infrastruktur aus dem Angriffssatz wiederverwenden oder eine neue Infrastruktur speziell für die Durchführung dieser Kampagne einrichten.

Kampagnen haben ein gemeinsames Ziel in Bezug auf die Incidents, die sie für Personen oder für die auf sie abzielenden Ressourcen verursachen und die sie verwenden.

Beispiel: Ein Verbrechenssyndikat greift die Führungskräfte der ACME Bank an. Sie greifen an, indem sie eine bestimmte Variante von Malware und neue Server verwenden, um geheime Informationen über eine bevorstehende Fusion mit einer anderen Bank zu erhalten.

Definieren Sie eine Kampagne

Definieren Sie eine Kampagne, um das Verhalten von Angreifern zu gruppieren.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Kampagnen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die der Kampagne zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Vorgehensweisen

Eine Vorgehensweise ist eine Aktion, die ausgeführt wird, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren. Vorgehensweisen gelten für STIX 2.x.

Vorgehensweisen beschreibt technische oder automatisierte Antworten (Patches anwenden, Firewalls neu konfigurieren). Es kann auch Aktionen auf höherer Ebene wie Mitarbeiterschulungen oder Richtlinienänderungen beschreiben.

Zum Beispiel könnte eine Vorgehensweise zum Mindern einer Schwachstelle das Anwenden des Patches beschreiben, der die Schwachstelle behebt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie eine Vorgehensweise

Definieren Sie eine Vorgehensweise, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Vorgehensweisen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Vorgehensweise zugeordnet sind.

Zugehörige Links	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Identitäten

Identitäten stellen tatsächliche Personen, Organisationen oder Gruppen (ACME, Inc.) und Klassen von Personen, Systeme oder Gruppen (Finanzsektor) dar. Identitäten gelten für STIX 2.x.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Identitäts-SDO kann grundlegende Identifizierungsinformationen, Kontaktinformationen und die Sektoren erfassen, zu denen die Identität gehört. Identität stellt Angriffsziele, Informationsquellen, Objektersteller und Bedrohungsakteuridentitäten dar.

Definieren Sie Identitäten

Definieren Sie Identitäten, die tatsächliche Personen, Organisationen oder Gruppen darstellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Identitäten**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Identität zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

Infrastruktur

Infrastructure SDO stellt eine Art von Taktiken, Techniken und Verfahren (TTPs) dar. Sie beschreiben alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die einen Zweck eines Angriffs unterstützen sollen. Infrastruktur gilt für STIX 2.x.

Die Elemente eines Angriffs werden durch andere SDOs oder SCOs dargestellt. Das Infrastruktur-SDO stellt jedoch eine benannte Gruppe von Daten dar, die die Infrastruktur bilden.

Beispiele für Infrastrukturen sind C2-Server, die bei einem Angriff verwendet werden, Geräte oder Server, die Teil einer Abwehr sind, oder Datenbankserver, die Ziel eines Angriffs sind.

Definieren Sie die Infrastruktur

Definieren Sie eine Infrastruktur, bei der es sich um alle Systeme, Softwareservices und zugehörigen physischen oder virtuellen Ressourcen handelt, die einen Zweck eines Angriffs unterstützen sollen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Infrastruktur**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen. Sie können der Infrastruktur auch andere Objekte zuordnen.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Zugeordnete Typen	Listet die mit diesem Objekt verknüpften Indikatortypen auf.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.
Zugehörige Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Angriffssatz

Ein Angriffssatz ist ein gruppierter Satz von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften. Ein Angriffssatz betrifft normalerweise eine einzelne Organisation. Der Angriffssatz gilt für STIX 2.x.

Ein Angriffssatz kann mehrere Kampagnen oder andere Aktivitäten erfassen. Diese Aktivitäten teilen Attribute, die auf einen allgemein bekannten oder unbekannten Bedrohungsakteur hindeuten.

Neue Aktivität kann einem Angriffssatz zugeordnet werden, auch wenn die Bedrohungsakteure hinter dem Angriff nicht bekannt sind. Bedrohungsakteure können von der Unterstützung eines Angriffssatzes zu einem anderen oder mehreren Angriffssätzen übergehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Angriffssatz ist das gesamte Angriffspaket und kann über einen längeren Zeitraum in mehreren Kampagnen verwendet werden, um potenziell mehrere Zwecke zu erreichen.

Definieren Sie einen Angriffssatz

Definieren Sie einen Angriffssatz, bei dem es sich um einen gruppierten Satz von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften handelt.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Eingriffssatz**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffssatz zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Angriffsmotivationen	Listet alle sekundären Motivationen auf, warum dieser Angriffssatz etwas erreichen möchte.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Standorte

Ein Standort stellt einen geografischen Standort dar. Standorte werden hauptsächlich verwendet, um anderen SDOs Kontext zu geben. Standorte gelten für STIX 2.x.

Der Standort kann einige oder alle der folgenden Angaben enthalten: Region (Nordamerika), Bürgeradresse (New York, USA), Breitengrad und Längengrad.

Die Standort-SDO kann sich auf eine Identität oder einen Angriffssatz beziehen, um anzuzeigen, dass sich die Identität oder der Angriffssatz an diesem Standort befindet. Es kann sich auch auf eine Malware oder ein Angriffsmuster beziehen, um anzuzeigen, dass sich das Zielopfer an einem bestimmten Ort befindet.

Beispielsweise könnte ein Standort in einer Beziehung verwendet werden, um zu beschreiben, dass der Angriffssatz „Bourgeis Swallow“ aus Osteuropa stammt.

Mindestens eine der folgenden Eigenschaften oder Eigenschaftssätze muss angegeben werden:

- region
- country
- Breitengrad und Längengrad

Definieren Sie den Standort

Definieren Sie einen geografischen Standort, um anderen SDOs mehr Kontext bereitzustellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Standorte**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Standort zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

Malware

Malware ist eine Art von TTP, die schädlichen Code darstellt. Bezieht sich auf ein Programm, das heimlich in ein System eingefügt wird. Malware gilt für STIX 2.x.

Der Zweck einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Die Malware-SDO charakterisiert, identifiziert und kategorisiert Malware-Instanzen und -Familien aus Daten, die aus der Analyse abgeleitet werden. Dieses SDO erfasst detaillierte Informationen darüber, wie die Malware funktioniert und was sie tut.

Definieren Sie eine Malware

Definieren Sie eine Malware, die schädlichen Code darstellt.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Malware**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Malware zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugeordnete Typen	Listet die mit diesem Objekt verknüpften Indikatortypen auf.
Zugehörige Fähigkeiten	Listet die Fähigkeiten auf, die identifiziert und diesem Objekt zugeordnet wurden.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.
Zugehörige Malware	Listet die mit diesem Objekt identifizierte Malware auf.
Zugeordnete Betriebssysteme	Die Betriebssysteme, auf denen das Objekt ausführbar ist. Dies gilt sowohl für virtualisierte Betriebssysteme als auch für solche, die auf Bare-Metal-Basis ausgeführt werden.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die mit diesem Objekt verknüpften Aktionen auf, bei denen es sich um technische oder automatisierte Antworten (Patches anwenden, Firewalls neu konfigurieren) handelt, um einen Angriff zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware-Analyse	Listet Malware-Analysedatensätze auf, die diesem Objekt zugeordnet sind.
Gemeldete erkennbare Elemente	Listet erkennbare Elemente auf, die als Teil dieses Objekts gemeldet wurden.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Malware-Analyse

Die Malware-Analyse erfasst die Metadaten und Ergebnisse einer Malware. Die Malware-Analyse gilt für STIX 2.x.

Die Malware-Analyse umfasst statische oder dynamische Analysen, die für eine Malware-Instanz oder -Familie ausgeführt werden.

Definieren Sie die Malware-Analyse

Definieren Sie eine Malware-Analyse, die die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse erfasst, die für eine Malware-Instanz oder -Familie ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Malware-Analyse**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu den Objekten im Zusammenhang mit der Malware-Analyse anzuzeigen.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Malware	Listet die mit diesem Objekt identifizierte Malware auf.
Gemeldete erkennbare Elemente	Listet erkennbare Elemente auf, die als Teil dieses Objekts gemeldet wurden.
Installierte Software	Listet alle nicht standardmäßigen Software auf, die auf dem Betriebssystem installiert ist und für die dynamische Analyse der Malware-Instanz oder -Familie verwendet wird.

Beobachtete Daten

Beobachtete Daten vermitteln Informationen über Cybersicherheits-bezogene Entitäten wie Dateien, Systeme und Netzwerke mithilfe der STIX Cyber-observable Objects (SCOs). Beobachtete Daten gelten für STIX 2.x.

Unter „Beobachtete Daten“ wird sowohl eine einzelne Beobachtung einer einzelnen Entität (Datei, Netzwerkverbindung) als auch die Zusammenfassung mehrerer Beobachtungen einer Entität erfasst.

Sie können Beobachtete Daten allein (ohne Beziehungen) verwenden, um Rohdaten zu übermitteln, die aus einer beliebigen Quelle gesammelt wurden. Quellen umfassen Analystenberichte, Sandboxen sowie netzwerk- und hostbasierte Erkennungstools.

Beispielsweise können Beobachtete Daten Informationen über eine IP-Adresse, eine Netzwerkverbindung, eine Datei oder einen Registrierungsschlüssel erfassen. Beobachtete Daten sind keine Intelligenzaussage, es sind einfach die Rohinformationen ohne Kontext für das, was sie bedeuten.

Beobachtete Daten definieren

Definieren Sie mithilfe von STIX Cyber-observable Objects (SCOs) beobachtete Daten, die Informationen über Cybersicherheitsentitäten wie Dateien, Systeme und Netzwerke vermitteln.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Beobachtete Daten**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den beobachteten Daten zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.

Bedrohungsakteure

Bedrohungsakteure sind Einzelpersonen, Gruppen oder Organisationen, die mit böswilligen Absichten handeln. Bedrohungsakteure gelten für STIX 2.x.

Ein Bedrohungsakteur ist kein Angriffssatz, kann aber im Laufe der Zeit verschiedene Angriffssätze, Gruppen oder Organisationen unterstützen oder mit ihnen verbunden sein.

Bedrohungsakteure verwenden ihre Ressourcen und die Ressourcen eines Angriffssatzes, um Angriffe durchzuführen und Kampagnen gegen Ziele auszuführen.

Sie können Bedrohungsakteure anhand ihrer Beweggründe, Fähigkeiten, Ziele, ihres Reifegrads, vergangener Aktivitäten, der Ressourcen, auf die sie Zugriff haben, und ihrer Rolle in der Organisation identifizieren.

Definieren Sie Bedrohungsakteure

Definieren Sie Bedrohungsakteure, bei denen es sich um Einzelpersonen, Gruppen oder Organisationen handelt, die mit böswilligen Absichten handeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsakteure**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungsakteur zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugeordnete Typen	Listet die mit diesem Objekt verknüpften Indikatortypen auf.
Zugeordnete Rollen	Listet die mit dem Bedrohungsakteur verknüpften Rollen auf.
Zugehörige Angriffsmotivationen	Listet die zugehörigen Angriffsmotivationen mit dem Bedrohungsakteur auf.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Bedrohungsgruppierungen

Ein Bedrohungsgruppierungsobjekt bestätigt explizit, dass die referenzierten STIX-Objekte einen gemeinsamen Kontext haben. Bedrohungsgruppierungen gelten für STIX 2.x.

Ein Bedrohungsgruppierungsobjekt stellt einen Satz von Daten dar, die bei ausreichender Analyse ausgereift sind, um einen Incident- oder Bedrohungsbericht als STIX-Berichtsobjekt zu übermitteln. Beispielsweise kann eine Gruppierung verwendet werden, um die laufende Untersuchung eines Sicherheitsereignisses oder eines Sicherheitsincidents zu charakterisieren.

Ein Bedrohungsgruppierungsobjekt kann auch verwendet werden, um zu bestätigen, dass die referenzierten STIX-Objekte zu einem laufenden Analyseprozess gehören. Beispielsweise kann ein Bedrohungsanalyst mit anderen in seiner Trust Community zusammenarbeiten, um eine Reihe von Kampagnen und Indikatoren zu untersuchen.

Das SDO für die Bedrohungsgruppierung enthält eine Liste von Verweisen auf SDOs, SCOs und SROs, zusammen mit einer expliziten Beschreibung des vom Inhalt gemeinsam genutzten Kontexts, einer Textbeschreibung und dem Namen der Gruppierung.

Definieren Sie Bedrohungsgruppierungen

Definieren Sie Bedrohungsgruppierungen als Objekte, die einen gemeinsamen Kontext haben.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsgruppierungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsgruppierung zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Gruppierte Objekte	Listet Objekte auf, die als Teil der Bedrohungsgruppierung gruppiert sind.
Gruppierte Indikatoren	Listet Indikatoren auf, die als Teil der Bedrohungsgruppierung gruppiert sind.
Gruppierte erkennbare Elemente	Listet erkennbare Elemente auf, die als Teil der Bedrohungsgruppierung gruppiert sind.

Markierungsdefinitionen

Das Markierungsdefinitionenobjekt stellt eine bestimmte Markierung dar.

Datenmarkierungen stellen Einschränkungen, Berechtigungen und andere Anleitungen für die Verwendung und Freigabe von Daten dar.

Beispielsweise können Daten mit der Einschränkung freigegeben werden, dass sie nicht erneut freigegeben werden dürfen oder im Ruhezustand verschlüsselt werden müssen.

In STIX werden Datenmarkierungen mithilfe des Markierungsdefinitionsobjekts angegeben. Diese Definitionen werden auf STIX-Objekte mithilfe von Objektmarkierungen und auf einzelne Eigenschaften von STIX-Objekten über granulare Markierungen angewendet.

Definieren Sie Markierungsdefinitionen

Definieren Sie Markierungsdefinitionen, die eine bestimmte Datenmarkierung darstellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Markierungsdefinitionen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Markierungsdefinition zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
	Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Markierte Objekte	Listen von Objekten, die mit der Markierungsdefinition markiert sind.
Markierte Indikatoren	Listen der mit der Markierungsdefinition markierten Indikatoren.

Bedrohungshinweise

Ein Bedrohungshinweis übermittelt informativen Text, um zusätzliche Analysen bereitzustellen, die nicht in den STIX-Objekten, Markierungsdefinitionsobjekten oder Sprachinhaltsobjekten enthalten sind, auf die sich der Hinweis bezieht. Bedrohungshinweise gelten für STIX 2.x.

Beispielsweise kann ein Analyst einem von einer anderen Organisation erstellten Kampagnenobjekt eine Notiz hinzufügen. Der Hinweis kann darauf hinweisen, dass in einem Hackerforum Beiträge zu dieser Kampagne gesehen wurden.

Notizen werden in der Regel von menschlichen Analysten erstellt und bestehen aus anwenderdefiniertem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Notiz erstellt hat.

Definieren Sie Bedrohungshinweise

Definieren Sie Bedrohungshinweise, die Informationen vermitteln, um weiteren Kontext oder Analysen bereitzustellen, die in vorhandenen Objekten nicht verfügbar sind.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungshinweise**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungshinweisen zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Zugeordnete Objekte	Listen von Objekten, für die die Bedrohungshinweise gelten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Zugehörige Indikatoren	Listen der Indikatoren, für die die Bedrohungshinweise gelten.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.

Bedrohungsmeinungen

Eine Meinung ist eine Bewertung der Richtigkeit der Informationen in einem STIX-Objekt, die von einer anderen Entität erstellt wurde. Die Bedrohungsmeinungen gelten für STIX 2.x.

Die Meinungseigenschaft erfasst den Grad der Zustimmung oder Nichtübereinstimmung mithilfe einer festen Skala. Die feste Skala unterstützt auch eine numerische Zuordnung, um konsistente statistische Vorgänge über Meinungen hinweg zu ermöglichen.

Beispielsweise kann ein Analyst einer verbrauchenden Organisation sagen, dass er mit einem Kampagnenobjekt „überhaupt nicht einverstanden“ ist, und eine Erklärung dafür angeben.

Meinungen sind subjektiv, und in der Spezifikation wird nicht angegeben, wie sie am besten interpretiert werden können.

Humananalysten erstellen Meinungen und bestehen aus anwenderdefiniertem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Meinung erstellt hat.

Definieren Sie Bedrohungsmeinungen

Definieren Sie Bedrohungsmeinungen als Bewertung der Richtigkeit der Informationen in einem STIX-Objekt.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsmeinungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsstellungnahme zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Zugeordnete Objekte	Liste der Objekte, für die die Bedrohungsmeinung gilt.
Zugehörige Indikatoren	Liste der Indikatoren, für die die Bedrohungsmeinung gilt.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.

Bedrohungsberichte

Bedrohungsberichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren. Bedrohungsberichte gelten für STIX 2.x.

Bedrohungsberichte enthalten die Beschreibung eines Bedrohungsakteurs, der Malware und der Angriffstechnik sowie des Kontexts und zugehörige Details. Sie werden verwendet, um relevante Threat Intelligence-Informationen zu gruppieren, sodass sie als umfassende Cyberbedrohungs-Story veröffentlicht werden können.

Der Bedrohungsbericht-SDO enthält eine Liste von Verweisen auf STIX-Objekte zusammen mit einer Textbeschreibung und dem Namen des Berichts.

Definieren Sie Bedrohungsberichte

Definieren Sie Bedrohungsberichte, die einen Bedrohungsakteur, Malware, Angriffstechnik einschließlich Kontext und zugehörige Details beschreiben.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsberichte**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungsberichten zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Zugeordnete Typen	Listet die mit diesem Objekt verknüpften Indikatortypen auf.
Gemeldete Objekte	Liste der im Bedrohungsbericht gemeldeten Objekte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Gemeldete Indikatoren	Listen von Indikatoren, die im Bedrohungsbericht gemeldet werden.
Gemeldete erkennbare Elemente	Listen der im Bedrohungsbericht gemeldeten erkennbaren Elemente.

Sichtungen

Sichtungen geben an, dass ein Indikator oder Objekt gesehen wurde. Objekte können Malware, ein Tool, ein Bedrohungsakteur usw. sein.

Sichtungen erfassen, wer und was das Ziel ist, wie Angriffe durchgeführt werden und Trends beim Angriffsverhalten.

Das Sichtungsbeziehungsobjekt enthält zusätzliche Eigenschaften, die in den generischen Beziehungsobjekten nicht vorhanden sind. Diese zusätzlichen Eigenschaften stellen spezifische Daten für Sichtungsbeziehungen dar.

Zum Beispiel eine Anzahl, oder die angibt, wie oft etwas gesehen wurde.

Sichtungen werden als Beziehung erfasst, da Sie keine Sichtung haben können, wenn Sie etwas haben, das gesehen wurde.

- Was gesehen wurde, z. B. Malware, Kampagne oder anderes SDO
- Wer es gesehen hat und/oder wo es gesehen wurde, dargestellt als Identität
- Was in Systemen und Netzwerken gesehen wurde, dargestellt als beobachtete Daten

Definieren Sie Indikatorsichtungen

Definieren Sie Sichtungen, die angeben, dass ein Indikator gesehen wurde.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatorsichtungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Indikatorsichtung zugeordnet sind.

Zugehörige Listen	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Listen	Beschreibung
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.

Definieren Sie Objektsichtungen

Definieren Sie eine Objektsichtung, die beschreibt, dass ein Objekt (Malware, Tool, Bedrohungsakteur usw.) erkannt wurde.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objektsichtungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Objektsichtung zugeordnet sind.

Zugehörige Listen	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.

Tools

Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet werden. Tools gelten für STIX 2.x.

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware befinden sich diese Tools oder Softwarepakete häufig auf einem System und dienen berechtigten Zwecken für Power-Benutzer, Administratoren, Netzwerkadministratoren oder sogar normale Benutzer.

Beispielsweise sind Remote Access Tools (RDP) und Network Scan Tools (Nmap) Tools, die ein Bedrohungsakteur während eines Angriffs verwendet.

Tools definieren

Definieren Sie Tools als legitime Software, die zum Ausführen von Angriffen verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Tools**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Tool-Objekt zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Zugeordnete Typen	Listet die mit diesem Objekt verknüpften Indikatortypen auf.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die mit diesem Objekt verknüpften Aktionen auf, bei denen es sich um technische oder automatisierte Antworten (Patches anwenden, Firewalls neu konfigurieren) handelt, um einen Angriff zu verhindern.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.

Schwachstellen

Eine Schwachstelle ist eine Schwachstelle oder ein Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen. Schwachstellen gelten für STIX 2.x.

Die Schwachstelle oder der Fehler liegt in den Anforderungen, Designs oder Implementierungen des Codes, der in einer Software- oder Hardwarekomponente enthalten ist. Diese Schwachstelle wird direkt ausgenutzt, um die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems zu beeinträchtigen.

CVE ist eine Liste von Informationssicherheitsschwachstellen und -risiken, die gängige Namen für öffentlich bekannte Probleme [CVE] bereitstellt.

Wenn beispielsweise eine Malware CVE-2015-12345 ausnutzt, könnte ein Malware-Objekt mit einem Schwachstellenobjekt verknüpft werden, das auf CVE-2015-12345 verweist.

Definieren Sie Schwachstellen

Definieren Sie eine Schwachstelle als eine Schwachstelle oder einen Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Schwachstellen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Schwachstellen-Objekt zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die mit diesem Objekt verknüpften Aktionen auf, bei denen es sich um technische oder automatisierte Antworten (Patches anwenden, Firewalls neu konfigurieren) handelt, um einen Angriff zu verhindern.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

Beziehungen

Verwenden Sie die Beziehungsobjekte, um zwei SDOs oder STIX Cyber-observable Objects (SCOs) miteinander zu verknüpfen und ihre Beziehung zueinander zu beschreiben.

STIX-Beziehungsobjekte (STIX Relationship Objects, SROs) stellen Arten von Beziehungen zwischen verschiedenen STIX-Objekten dar. Die folgenden Beziehungsobjekte sind verfügbar:

- **Objekt-Objekt-Beziehung**: Dieses Objekt definiert Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts. Ein Beispiel für eine definierte Objekt-Objekt-Beziehung ist, dass ein Angriffsmuster Malware übermittelt.
- **Objekt-Indikator-Beziehung**: Dieses Objekt definiert Beziehungen zwischen dem Indikatorobjekt und anderen SDOs. Ein Beispiel für eine durch Objekte und Indikatoren definierte Beziehung ist, dass ein Indikator Hinweise auf eine Kampagne erkennt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Beziehung zwischen Objekt und erkennbarem Element**: Dieses Objekt definiert Beziehungen zwischen SDOs und dem erkennbaren Elementobjekt (SCO). Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus erkennbaren Cyber-Objekten besteht, die Informationen über einen potenziellen Angriff bereitstellen.

STIX-Objektbeziehungen

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
Objekt-Objekt-Beziehungen	Angriffsmuster	Malware	Diese Beziehung beschreibt, dass dieses Angriffsmuster verwendet wird, um diese Malware-Instanz (oder Familie) bereitzustellen.
Objekt-Indikator-Beziehungen	Indikator	Angriffsmuster, Kampagne, Infrastruktur, Angriffssatz, Malware, Bedrohungsakteur, Tool	Diese Beziehung beschreibt, dass der Indikator Hinweise auf das zugehörige Angriffsmuster, die Kampagne, die Infrastruktur, den Angriffssatz, die Malware, den Bedrohungsakteur oder das Tool erkennen kann. Der Nachweis ist möglicherweise nicht direkt. Beispielsweise kann der Indikator sekundäre Nachweise der Kampagne erkennen, z. B. Malware, die häufig von dieser bestimmten Kampagne verwendet wird.
Objekt-Erkennbares Element-Beziehungen	Infrastruktur	Beobachtete Daten	Diese Beziehung beschreibt, dass der Indikator basierend auf Informationen aus einem beobachteten Datenobjekt erstellt wird. Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus erkennbaren Cyber-Objekten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

STIX-Objektbeziehungen (Fortsetzung)

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
			besteht, die Informationen über einen potenziellen Angriff bereitstellen.

Definieren Sie Objekt-Objekt-Beziehungen

Definieren Sie Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Definieren Sie Objekt-Indikator-Beziehungen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen SDOs.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Indikator-Beziehungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Definieren Sie Beziehungen zwischen Objekt und erkennbarem Element

Definieren Sie Beziehungen zwischen SDOs und dem erkennbaren Elementobjekt (SCO).

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Erkennbares-Element-Beziehungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

STIX-Visualizer

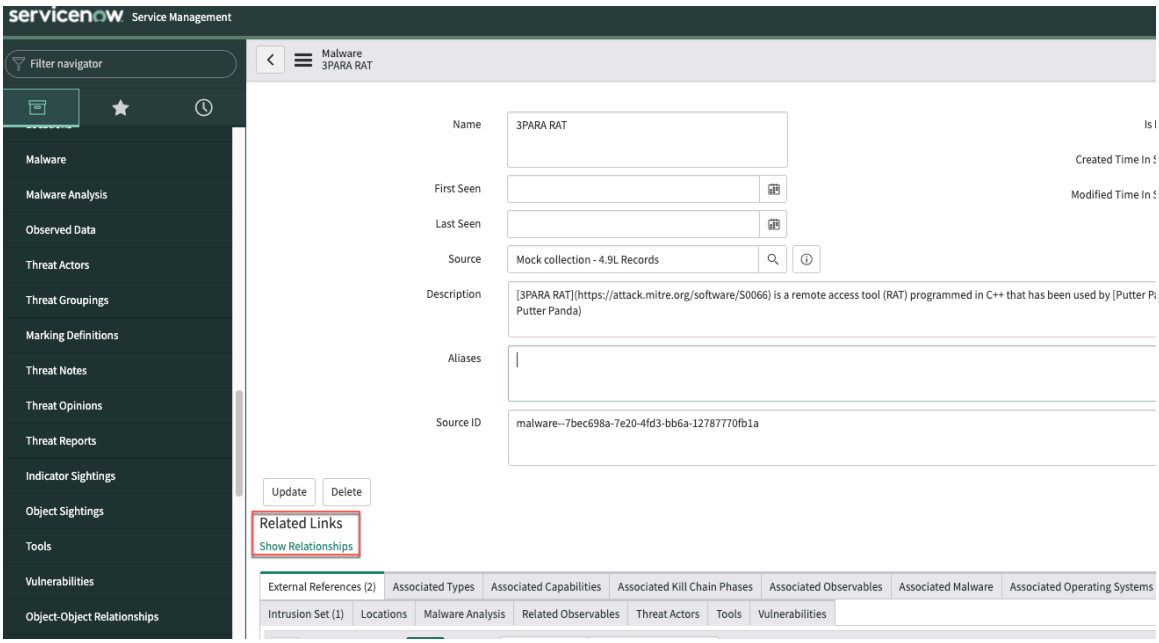
Die STIX-Visualizer stellt die Struktur des STIX-Objekts und seiner Beziehung visuell dar.

Weitere Informationen zum ausgewählten Objekt oder zur ausgewählten Beziehung finden Sie im Detailbereich.

Das Beziehungsdiagramm zeigt die Beziehungen für ein Objekt und bietet Kontext, den Sie untersuchen können. Sie können auf jeden Knoten im Diagramm klicken, um weitere Details anzuzeigen.

Hinweis:
Die STIX-Visualisierung ist für alle SDOs mit Ausnahme der Objekte „Bericht“ und „Beobachtete Daten“ verfügbar.

Greifen Sie auf die STIX-Visualizer zu

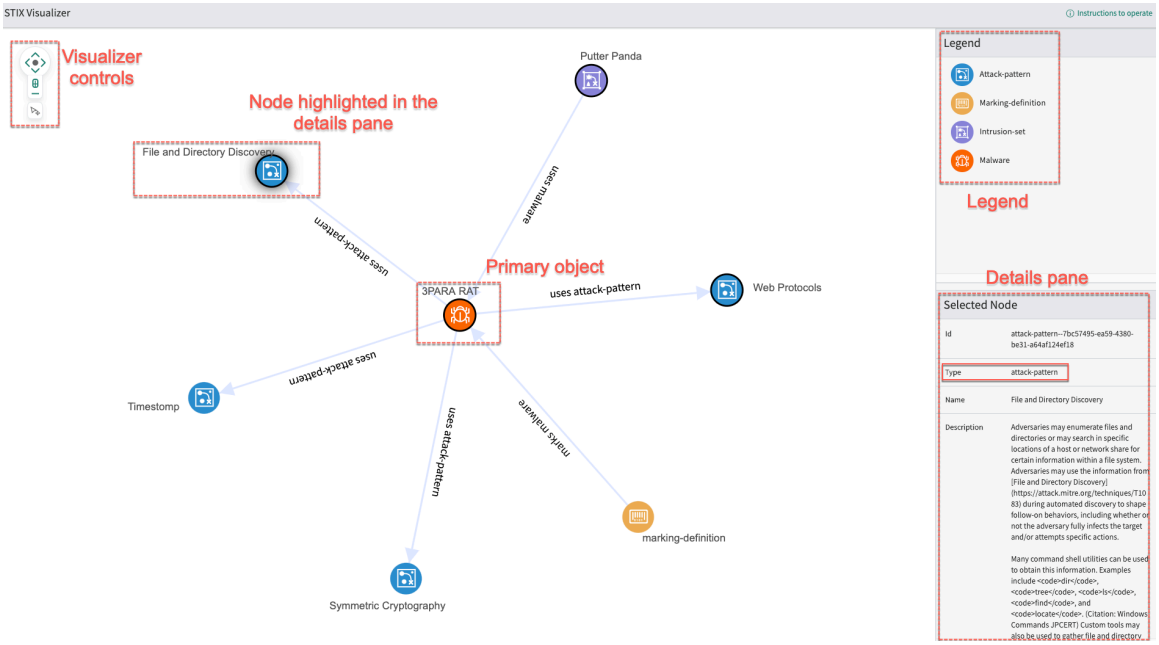


Klicken Sie für alle SDOs im Abschnitt „Zugehörige Links“ auf Beziehungen anzeigen, um die STIX-Visualisierung anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Details in STIX-Visualizer an



In der Visualisierung können Sie das Objekt und seine Beziehung anzeigen, die Kontext für weitere Untersuchungen bieten. In der Visualisierung werden Farben und Symbole verwendet, um verschiedene Informationen zu den Objekten darzustellen.

Sie können ein Objekt vergrößern, die Knoten ziehen oder sie anheften, um den Fokus auf eine bestimmte Beziehung zu legen.

Klicken Sie auf ein beliebiges Objekt, um den Detailbereich zu öffnen. Im Detailbereich erfahren Sie mehr über die dem Objekt zugeordneten Informationen.

MITRE-ATT&CK™ -Framework – Übersicht

Das -Framework MITRE-ATT&CK ist eine Knowledge Base mit allgemeinen Taktiken, Techniken und Verfahren (TTP), auf die Ihr Unternehmen zugreifen kann, um spezifische Bedrohungsmodelle und Methoden gegen Cyberangriffe zu entwickeln.

Übersicht

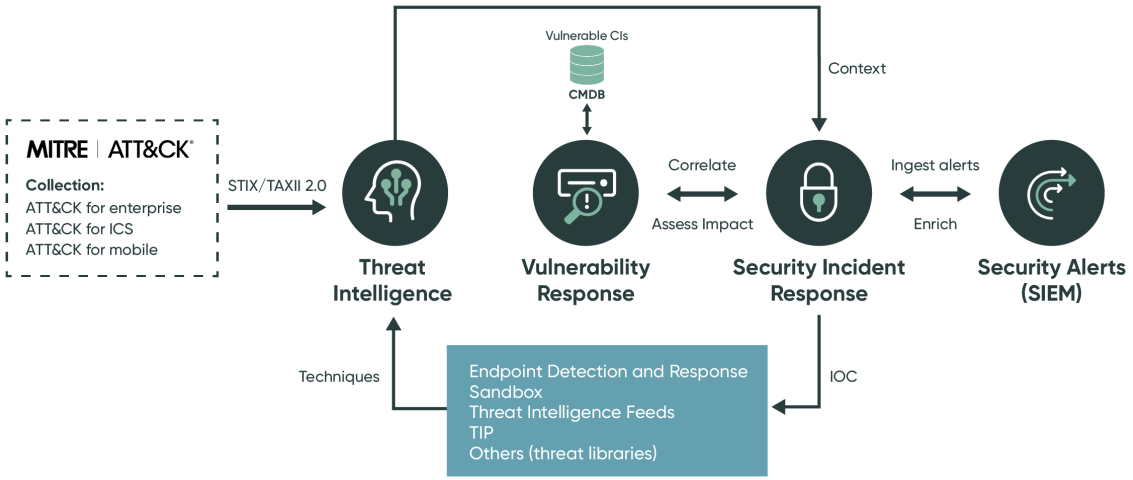
Das MITRE Adversarial Taktics, Techniques, and Common Knowledge (ATT&CK)-Framework dokumentiert und verfolgt verschiedene Angreifertechniken, die während verschiedener Phasen eines Cyberangriffs verwendet werden.

Mithilfe der Knowledge Base des -Frameworks MITRE-ATT&CK kann die Cyberthreat Intelligence-Community Bedrohungen schnell identifizieren und Antworten auf Cyberangriffe koordinieren.

MITRE-ATT&CK und Security Operations

Im folgenden Diagramm können Sie sehen, wie die Informationen MITRE-ATT&CK von mit den Anwendungen Security Operations fließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Die zugehörigen Listen namens vorab geladen TAXII Client stellt eine Verbindung zum Server TAXII her, um die Datensammlungen in Threat Intelligencezu erfassen.
- Vorhandene SIEM-Integrationen (Security Information and Event Manager) erfassen ihre Bedrohungsdaten (Warnungen und Ereignisse) mit relevanten TTPs und sind Security Incidents zugeordnet.
- Wenn ein IoC mit einem Security Incident verknüpft ist, durchsucht Threat Intelligence Bedrohungs-Feeds automatisch nach relevanten Informationen und sendet IoCs zur zusätzlichen Analyse an Drittparteiquellen wie EDR, Sandbox oder TIP.
- Wenn eine Drittanbieterquelle die Informationen MITRE-ATT&CK enthält, dann Threat Intelligence extrahiert die Technikinformationen und bereichert die Daten im Repository Threat Intelligence für Korrelationen und Analysen.
- MITRE-ATT&CK stellt auch CVE-Kontextinformationen für die einzelnen Techniken bereit. Ihr Sicherheitsteam kann die in Vulnerability Response verwendeten Techniken überprüfen, um festzustellen, ob Ihre geschäftskritischen Assets Bedrohungen ausgesetzt sind.

MITRE-ATT&CK Matrizen, Taktiken und Techniken

Der Kern des MITRE-ATT&CK -Frameworks ist eine Matrix aus Angreifertaktiken und -techniken. Die Reihenfolge der Taktiken gibt an, was ein Angreifer in der Phase eines incident zu erreichen versucht. Wenn Ihr Sicherheitsteam diese Sequenz versteht, können Sie den nächsten Schritt des Angreifers vorhersehen und die Kill Chain durchbrechen. ATT&CK besteht aus den folgenden Matrizen:

- Enterprise ATT&CK: Beschreibt die Verhaltensweisen und Aktionen eines Angreifers, um ein Unternehmensnetzwerk und eine Cloud zu kompromittieren und zu agieren.

  Hinweis:
  Die Pre-ATT&CK-Matrix wurde von MITRE als veraltet markiert und wird mit der Enterprise-Matrix zusammengeführt.

- ICS ATT&CK: Beschreibt die Aktionen, die ein Angreifer während des Betriebs in einem ICS-Netzwerk (Industrial Control Systems) ausführt.
- Mobile ATT&CK: Beschreibt die Verhaltensweisen und Aktionen des Angreifers, die sich auf Mobilgeräte konzentrieren.

Taktiken stellen das Warum einer ATT&CK-Technik dar. Es handelt sich um das Taktikziel des Angreifers für die Durchführung einer Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Techniken stellen dar, wie ein Angreifer ein strategisches Ziel erreicht, indem er eine Aktion ausführt.

Techniken können mit mehr als einer Taktik verknüpft sein. Beispielsweise wird die Manipulation von Zugriffstoken von einem Angreifer verwendet, um entweder die Taktik der Berechtigungseskalation oder der Umgehung der Verteidigung zu implementieren.

Verwendung eines absichtsbasierten Ansatzes für die Reaktion auf Incidents

Eine auf Absichten basierende Reaktion verwendet ein dynamisches und kontextbezogenes Kill Chain-Framework, das Ihrem Unternehmen helfen kann, Security Incidents zu korrelieren und eine Vielzahl von Angriffen zu identifizieren. Ihr Sicherheitsteam kann eine absichtsbasierte Reaktion verwenden, um zu verstehen, wie das Unternehmen angegriffen wird und was der Angreifer als Nächstes tun könnte. Mit dieser Art von Reaktion können Sie das Verhalten eines Angreifers vorhersagen, um Ihre Ressourcen effektiv zu konzentrieren.

Mit Security Incident Responsekann Ihr Sicherheitsteam den Lebenszyklus jedes Security Incidents von der Analyse bis zur Eindämmung verwalten, indem es sich auf Kompromittierungsindikatoren (IoCs) wie IP-Adressen, Datei-Hashes und Domänen konzentriert.

Durch die Integration Security Incident Response von in das MITRE-ATT&CK -Framework werden Security Incidents als Links in einem größeren unternehmensweiten Angriff behandelt.

Wie Ihre Organisation von MITRE-ATT&CK in Security Operations profitieren kann

Das MITRE-ATT&CK -Framework kann Ihre Organisation bei folgenden Aufgaben unterstützen:

- statten Sie Sicherheitsanalysten mit MITRE-ATT&CK Taktiken, Techniken und Verfahren (TTPs) aus, um Security Incidents besser analysieren und besser darauf reagieren zu können.
- Automatisieren Sie die Incident-Workflows mit dem Playbook zum Erkennen und Eindämmen von Bedrohungen im Kontext des MITRE-ATT&CK -Frameworks.
- Priorisieren Sie Indikatoren für Kompromittierung und Bedrohungssuche mit Informationen MITRE-ATT&CK.
- Machen Sie sich mit der allgemeinen Sicherheitslage Ihrer Organisation im Kontext des MITRE-ATT&CK -Frameworks vertraut.

MITRE-ATT&CK – Administration

Sie können Datenquellen einrichten, zuordnen, die allgemeine Technikerkennungsabdeckung zuordnen und das -Repository MITRE-ATT&CK in Now Platformverwalten.

Erste Schritte mit MITRE-ATT&CK dem -Framework

Lesen Sie sich die folgenden Informationen durch, bevor Sie mit der Einrichtung Ihres MITRE-ATT&CK -Frameworks beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Setupaufgabe	Beschreibung
Vergewissern Sie sich, dass die erforderlichen Rollen Now Platform, Threat Intelligenceund Security Incident Response zugewiesen wurden.	Die folgenden Rollen werden für die Funktionen MITRE-ATT&CK verwendet: • Der -Administrator (admin) installiert die Anwendungen aus ServiceNow Store und weist die Rollen Security Incident-Administrator (sn_si.admin) und Threat Intelligence-Administrator (sn_ti.admin) zu. • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.write • sn_ti.mitre_analyst: Die MITRE-Analystenrolle wurde eingeführt, um eine übergreifende Navigation für die Funktionen MITRE zwischen Security Incident Response und Threat Intelligence Support Common zu ermöglichen. Mit dieser Rolle können Sie das Modul Threat Intelligence MITRE und das Modul Security Incident Response im schreibgeschützten Modus anzeigen. • sn_si.read Weitere Informationen finden Sie unter Threat Intelligence einrichten.
Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung des Moduls MITRE-ATT&CK erforderlich sind, installiert und aktiviert sind.	Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. • Threat Intelligence Support Common UI Components (sn_ti_seismic) – Version 1.0 oder höher • Threat Intelligence Support Common – Version 12.0 oder höher • Threat Intelligence - Version 12.0 oder höher • Security Incident Response - Version 12.0 oder höher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	Weitere Informationen zum Einrichten Ihrer Instanz Now Platform für die Integration finden Sie unter Berechtigungen für ein Produkt oder eine Anwendung von Security Operations erhalten und eine ServiceNow Store-Anwendung aktivieren.
Domänentrennung	Überprüfen Sie den Abschnitt zur Domänentrennung, wenn Sie Daten, Prozesse und administrative Aufgaben trennen möchten.

Machen Sie sich mit dem Datenmodell MITRE bis STIX vertraut

Überprüfen Sie die von MITRE und STIX verwendete Terminologie, um das Framework MITRE-ATT&CK™ in Now Platformeffizient zu verwenden und zu verstehen.

Zuordnung von ObjektenMITRE zu STIX

STIX ist eine Sprache zur Beschreibung von Cyberbedrohungsinformationen auf standardisierte und strukturierte Weise. Das übergeordnete Datenmodell im Modul Threat Intelligence sind die Objekte STIX. Die MITRE -Objekte sind eine Teilmenge des übergeordneten Datenmodells STIX. Im Framework MITRE-ATT&CK stellt MITRE ähnliche Informationen STIX mit bestimmten Bezeichnungen und Objekten bereit.

Zuordnung von ObjektenMITRE zu STIX

MITRE-Terminologie	STIX-Terminologie
Technik	Angriffsmuster
Mitigation	Vorgehensweise
Gruppen	Angriffssätze
Malware	Malware
Tool	Tool

Daten werden im Modul Threat Intelligence erweitert

Sie können eine Liste von Threat Intelligence Bedrohungsquellen verwalten und die erforderlichen STIX Daten importieren, die eine Vielzahl von Informationen zu Cyberbedrohungen enthalten. Sie können auch die Profile TAXII verwenden, um den automatisierten Austausch von Informationen zu Cyberbedrohungen zu erleichtern.

Hinweis:
Weitere Informationen finden Sie unter Eine Bedrohungsquelle definieren und ein TAXII-Profil erstellen.

Daten werden im Modul MITRE-ATT&CK erweitert

Sie können die Objekte Malware, Gruppe, Verringerung und Tool auf eine Technik im Repository MITRE-ATT&CK erweitern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können ein Objekt erstellen und eine Beziehung zwischen einer Technik und dem neuen Objekt im Modul „MITRE ATT&CK-Repository“ herstellen, aber Sie können den Beziehungstyp in diesem Modul nicht definieren. Um einen Beziehungstyp zu definieren, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

Wenn Sie den Beziehungstyp zwischen einer vorhandenen Technik und einem vorhandenen Objekt zuordnen, müssen Sie die Technik als Zielobjekt und das Objekt als Quellobjekt definieren. Navigieren Sie dazu zu **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

Sie können eine Gruppe erstellen und sie einem Angriffsmuster zuordnen, aber im MITRE ATT&CK-Repository können Sie nur die Beziehung zwischen der Gruppe und dem Angriffsmuster herstellen. Um den Objekt-zu-Objekt-Beziehungstyp zu definieren, müssen Sie dies im IoC-Repository tun.

Hinweis:
Weitere Informationen finden Sie unter erweitern MITRE-ATT&CK Daten - und IoC-Repository.

Domain Separation und MITRE-ATT&CK

Diese Übersicht über die Domänentrennung bezieht sich auf MITRE-ATT&CK. Mit Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe

Support: Standard.

So funktioniert Domain Separation mit MITRE-ATT&CK

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Anwender mit den erforderlichen sn_ti.admin-Rollen in der jeweiligen Domäne.
- Replizieren Sie für jede Domäne Folgendes:
  - TAXII Sammlungen

    Hinweis:
    - Aktivieren Sie die Sammlungen nicht in der globalen Domäne. Aktivieren Sie nur die Sammlungen, die in Ihrer Domäne repliziert und verfügbar sind.
    - Ändern Sie das Feld **Ausführen als** in den Sammlungen in den Benutzer mit der Rolle sn_ti.admin in der entsprechenden Domäne.

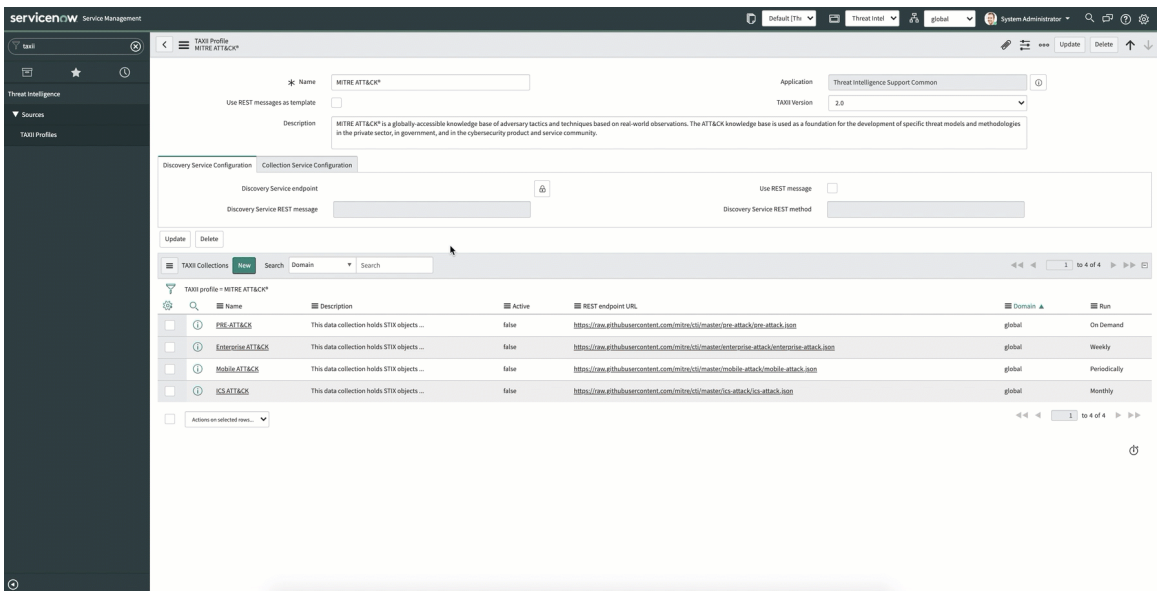
  - Definition der Technikabdeckung
  - Extraktionsregel für Technik
  - Erkennungsregeln – MITRE ATT&CK-Zuordnungen
  - Abdeckung durch Risikominderung
    - Kopieren Sie alle Definitionsdatensätze für die Abdeckung durch Risikominderung.
    - Kopieren Sie den Rechner für die Abdeckungsminderung, oder erstellen Sie einen neuen Rechner für die entsprechende Domäne.
  - Bedrohungsgruppe – Technik-Heatmap-Definitionen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TAXII-Sammlung replizieren

1. Navigieren zu **Threat Intelligence** > **Quellen** > **TAXII-Profile**.
2. Verwenden Sie die Domänenauswahl in der Kopfzeile, um Ihre Domäne auszuwählen.
3. Wählen Sie die TAXII-Sammlung aus, die für Ihre Organisation relevant ist (Enterprise ATT&CK, Mobile ATT&CK oder ICS ATT&CK).
4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Einfügen und bleiben aus**. Die doppelte TAXII-Sammlung wird unter der ausgewählten Domäne erstellt
5. Navigieren Sie zurück zum MITRE ATT&CK TAXII-Profil, um die doppelte TAXII-Sammlung anzuzeigen.

Die folgende Abbildung zeigt, wie Sie die Domäne TOP/Initech auswählen, die TAXII-Sammlung in der Domäne replizieren und die replizierte TAXII-Sammlung überprüfen.



Richten Sie das -Framework MITRE-ATT&CK™ ein

Aktivieren Sie das Profil MITRE-ATT&CK, und richten Sie eine regelmäßige Aufgabe ein, damit Sie MITRE-ATT&CK -Sammlungen für die Bedrohungserkennung in Ihrer Organisation einrichten können.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

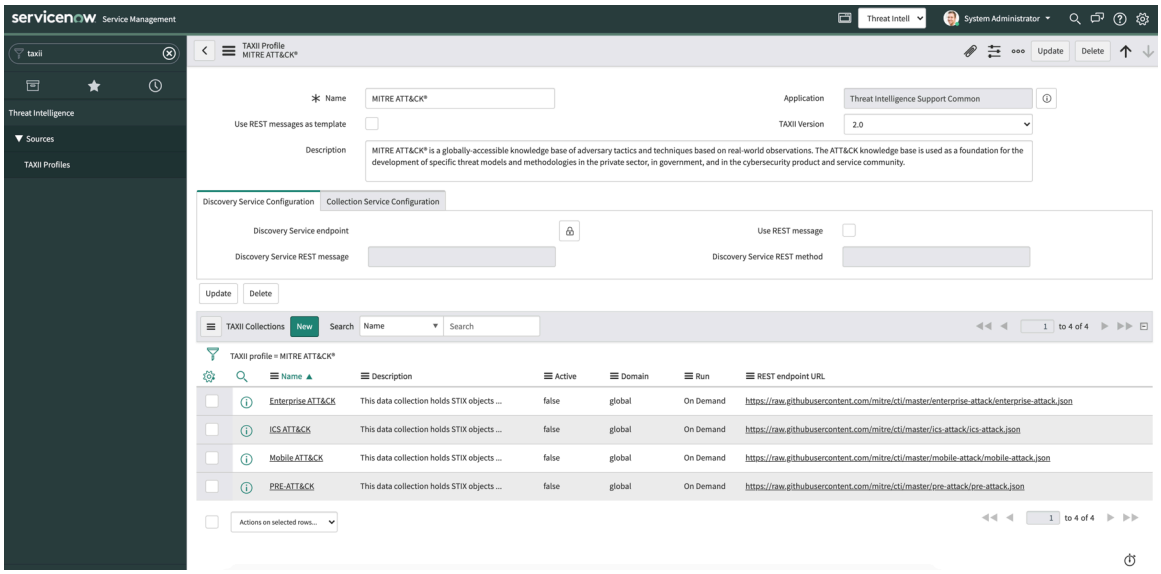
Warum und wann dieser Vorgang ausgeführt wird

Der Ausdruck für strukturierte Bedrohungsinformationen (STIX™) ist eine Sprache zur standardisierten und strukturierten Beschreibung von Cyberbedrohungsinformationen. Mithilfe von STIX-Daten und Profilen für den vertrauenswürdigen automatisierten Austausch von Indikatorinformationen (TAXII™) können Sicherheitsteams gemeinsam genutzte Cyberbedrohungsinformationen verwenden, um Bedrohungen zu isolieren, die zuvor von Ihrem Unternehmen und anderen Quellen identifiziert wurden.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **TAXII-Profile**.
   Sie sehen die verfügbaren Profile TAXII.
2. Klicken Sie auf das **MITRE ATT&CK** -Profil, das mit dem Basissystem bereitgestellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um die TAXII -Sammlung zu aktivieren, legen Sie die Option **Aktiv** für die TAXII -Sammlung, die für Ihre Organisation relevant ist (Enterprise ATT&CK, Mobile ATT&CK oder ICS ATT&CK) auf wahr fest.

TAXII-Sammlung	Beschreibung
Enterprise ATT&CK	Beschreibt die Verhaltensweisen und Aktionen eines Angreifers, um ein Unternehmensnetzwerk und eine Cloud zu kompromittieren und zu operieren. **Hinweis:** Die Pre-ATT&CK-Matrix wurde von MITRE als veraltet markiert und wird mit der Enterprise-Matrix zusammengeführt.
Mobile ATT&CK	Beschreibt die Verhaltensweisen und Aktionen des Angreifers, die sich auf Mobilgeräte konzentrieren.
ICS ATT&CK	Beschreibt die Aktionen, die ein Angreifer während des Betriebs in einem ICS-Netzwerk (Industrial Control Systems) ausführt.

4. Um die Sammlung regelmäßig zu aktualisieren, legen Sie die Option **Ausführen** entsprechend Ihrer Organisation fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig ist diese Option auf Bei Bedarf festgelegt.

Hinweis:

a. Sammlungen werden als Teil des Plugins Threat Intelligence Core paketiert. Durch Installieren oder Aktualisieren von Threat Intelligence Support Common – Version 12.0 oder höher und Threat Intelligence – Version 12.0 oder höher stellen Sie sicher, dass Ihre Sammlungsdaten automatisch gefüllt werden.

b. Aktivieren Sie die Sammlung TAXII nur für die Sammlung, die Sie in Ihrer Organisation verwenden möchten, und deaktivieren Sie die anderen Sammlungen. Wenn Sie beispielsweise die Enterprise ATT&CK-Matrix verwenden möchten, aktivieren Sie Enterprise ATT&CK auf der Sammlungsebene TAXII und auf der Ebene der Matrizen. Deaktivieren Sie die anderen Mobile ATT&CK- und ICS ATT&CK-Matrizen in der Sammlung TAXII und auf Matrizenebene.

c. Wenn Sie in den zugehörigen Listen TAXII Sammlungen die Option Ausführen auf Täglich auswählen, tritt ein Fehler auf, und die Option wird standardmäßig auf Bei Bedarf festgelegt. Dieser Fehler tritt auf, da die Planung der täglichen Aktualisierung von Daten MITRE-ATT&CK eingeschränkt ist, um die Last auf den Servern MITRE zu optimieren. Außerdem aktualisiert MITRE die ATT&CK-Daten nur zweimal pro Jahr.

d. Die TAXII -Sammlungen werden nur aktualisiert, wenn Sie die TAXII -Sammlung aktivieren.

e. Aktualisierungen vorhandener Sammlungen können vom Server MITRE abgerufen werden, indem die Ausführungshäufigkeit in jeder Sammlung geplant wird.

f. Die Anpassungen, die Sie an den Repository-Daten MITRE-ATT&CK (Malware-, Gruppen-, Verringerungs- und Tool-Objekte für eine Technik) vornehmen, werden während geplanten Updates gespeichert.

g. MITRE aktualisiert die Knowledge Base MITRE-ATT&CK, in der einige Objekte als widerrufen oder veraltet gekennzeichnet, neue Objekte hinzugefügt oder vorhandene Objekte geändert werden. Wenn MITRE eine Taktik oder Technik widerruft, werden diese Objekte im Now Platformals widerrufen markiert. Die widerrufenen Objekte werden im Repository beibehalten, können jedoch nicht in Now Platformverwendet werden.

Nächste Maßnahme

Nach Abschluss des TAXII-Profil-Setups werden die Repository-Daten MITRE-ATT&CK in regelmäßigen Abständen in Now Platform® importiert. Sie können diese Daten anzeigen, indem Sie zu navigieren **MITRE ATT&CK-Repository** > **Matrizen** und **MITRE ATT&CK-Repository** > **Techniken**.

Matrizen verwalten

Verwalten Sie die Matrizen, die aus den MITRE TAXII -Sammlungen importiert wurden. Matrizen sind eine Sammlung von Taktiken und Techniken. Sie können die Matrizen anzeigen, um zu überprüfen, ob Ihre Sammlungen im Repository MITRE-ATT&CK verfügbar sind.

Vorbereitungen

Hinweis:

Überprüfen und vergewissern Sie sich, dass nur die Matrix, die Sie in Ihrer Organisation verwenden möchten, auf aktiv festgelegt ist, und deaktivieren Sie die anderen Matrizen. Wenn Sie beispielsweise die Enterprise ATT&CK-Matrix verwenden möchten, muss die Enterprise ATT&CK-Matrix auf der TAXII-Sammlungsebene und auf der Matrizenebene aktiviert werden. Deaktivieren Sie die anderen Mobile ATT&CK- und ICS ATT&CK-Matrizen in der Sammlung TAXII und auf Matrizenebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

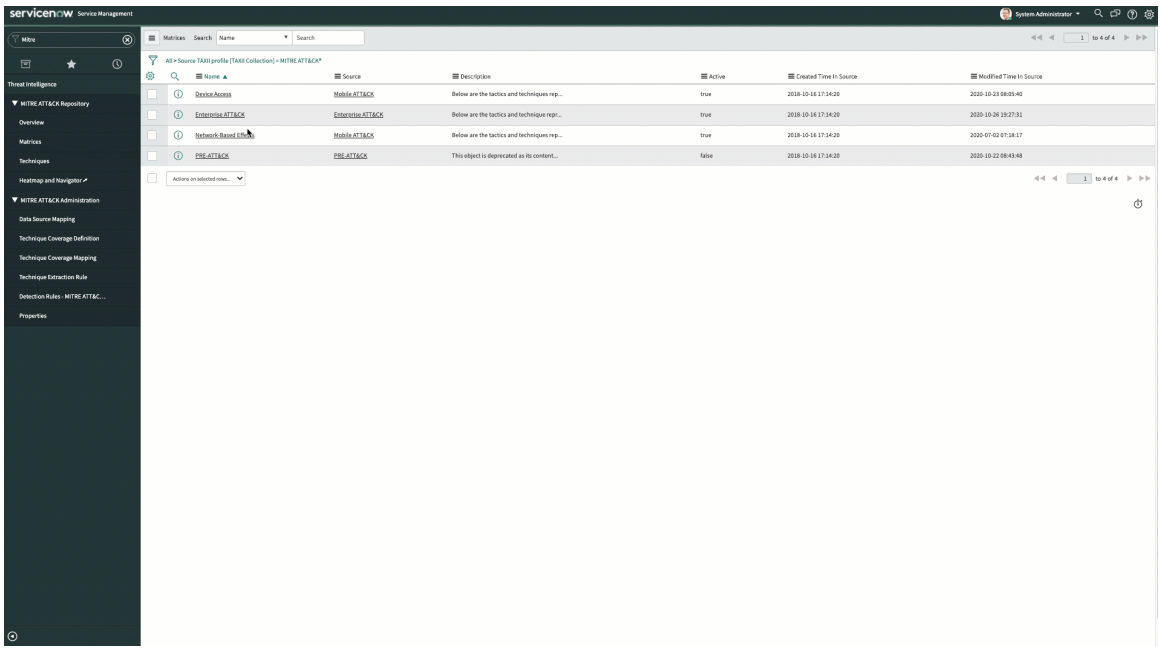
Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Matrizen**.
   Alle Matrizen sind standardmäßig deaktiviert.
2. Um eine Matrix zu aktivieren, zeigen Sie auf **Aktiv**, doppelklicken Sie, und wählen Sie **true**aus.
3. Um alle zugehörigen Informationen anzuzeigen, klicken Sie auf eine Matrix.
4. Um alle Taktiken anzuzeigen, die dieser Sammlung zugeordnet sind, klicken Sie auf die Registerkarte **MITRE-Taktiken**.
5. Klicken Sie auf eine Taktik, um zusätzliche Details und die Techniken anzuzeigen, die einer ausgewählten Taktik zugeordnet sind.
6. Wählen Sie auf der Registerkarte **MITRE ATT&CK-Techniken** eine Technik aus.
7. Zeigen Sie unter den zugehörigen Listen die Zuordnungen an, die für die von Ihnen ausgewählte Technik verfügbar sind.

   In der folgenden Abbildung sehen Sie den Navigationspfad von der Enterprise ATT&CK-Matrix zur Taktik des Erstzugriffs (TA0001) und dann zur Phishing-Technik (T1566). Auf der Seite „Angriffsmuster – Phishing-Technik“ können Sie die zugehörige Liste „Taktik“, „Untertechnik“, „Gruppe“, „Verringerung“, „Externe Referenzen“, „Malware“ und „Tools“ anzeigen.



Nächste Maßnahme

Sie können die Informationen in einigen dieser zugehörigen Listenobjekte basierend auf der von Ihnen ausgewählten Technik erweitern. Sie können beispielsweise neue Informationen für Gruppe, Verringerung, Externe Referenzen, Malware und Tools hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Techniken

Verwalten Sie die Techniken, die aus den MITRE TAXII -Sammlungen importiert wurden. Die Techniken enthalten verschiedene Möglichkeiten, wie Angreifer eine bestimmte Taktik anwenden. Sie können Techniken überprüfen und deaktivieren, die für Ihre Organisation nicht relevant sind. In STIXwerden Techniken als Angriffsmuster bezeichnet.

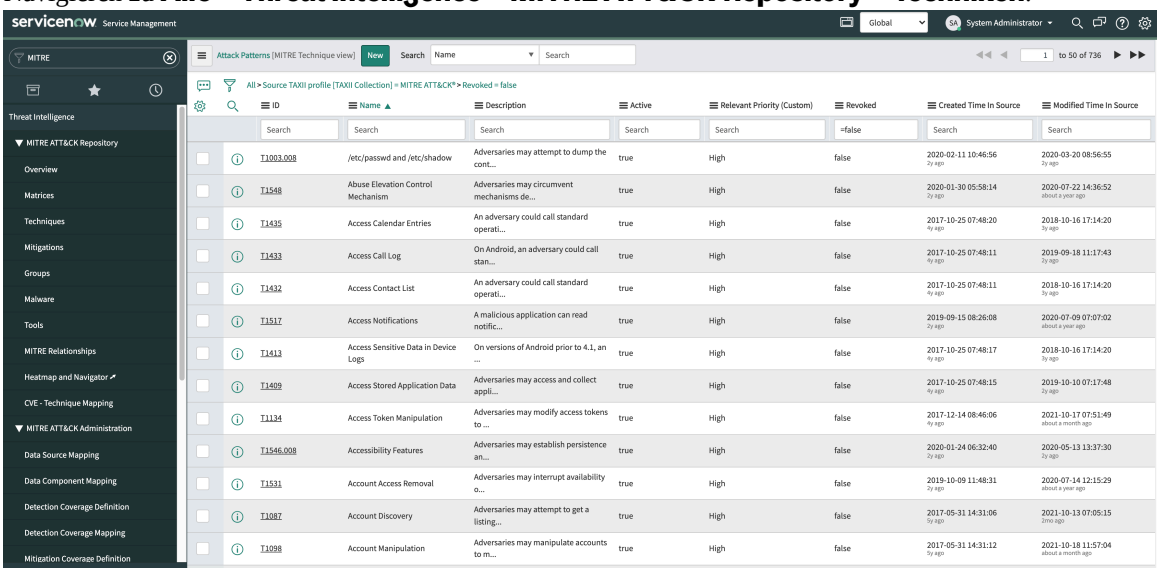
Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Techniken**.



Die Liste der Techniken und Untertechniken ist jetzt aufgelistet.

2. Um Techniken zu überprüfen und zu deaktivieren, die für Ihre Organisation nicht relevant sind, wechseln Sie zur Listenansicht für die ausgewählte Technik, ändern Sie in der Spalte Aktiv die Einstellung in **false**und speichern Sie die Einstellung.
   Deaktivieren Sie die Techniken, die nicht von den anderen Objekten im Repository MITRE-ATT&CK verwendet werden.

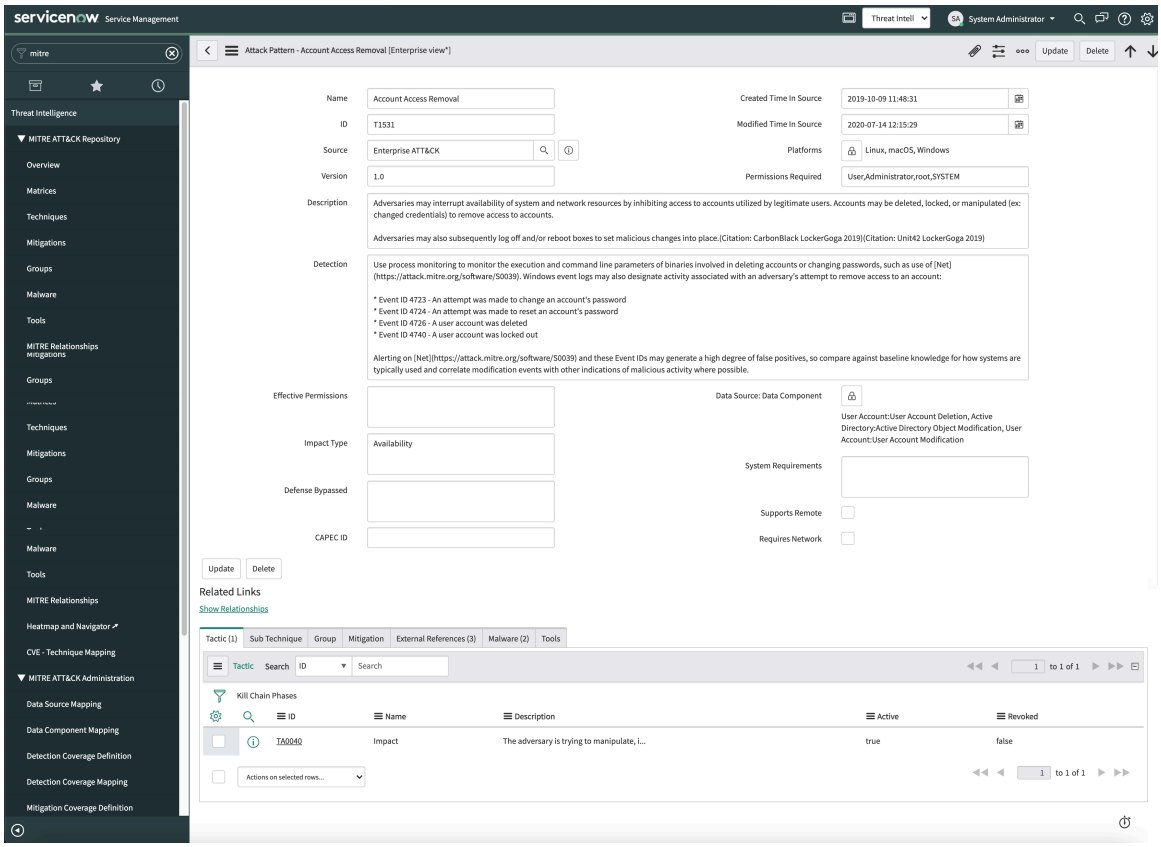
3. Um eine Technik zu priorisieren, weisen Sie im Feld **Relevante Priorität (Anwenderdefiniert)** eine Priorität zu.
   Die relevante Priorität des Basissystems ist auf „Keine“ festgelegt. Das Feld **„Relevante Priorität (anwenderdefiniert)“** wird nicht aus den MITRE-ATT&CK TAXII -Sammlungen importiert, sondern aus einem anwenderdefinierten Feld, das in Now Platformeingeführt wurde. Sie können die relevanten Prioritätsinformationen verwenden, um Techniken in den Dashboards, während der Zuordnung der Datenquelle oder bei der Analyse der Heatmap zu filtern und zu priorisieren.

4. Klicken Sie auf eine Technik, um alle zugehörigen Informationen zu dieser Technik anzuzeigen.

   In der folgenden Abbildung können Sie die Details für jede Technik zum Entfernen des Kontozugriffs, ihre ID, Quelle und andere zugehörige Informationen anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Das Element „Datenquelle: Datenkomponente“, das von MITRE eingeführt wurde, ersetzt das vorherige Feld „Datenquelle“. Die Datenkomponente bietet eine zusätzliche Kontextunterebene für die Datenquellen. Wenn Ihr MITRE-ATT&CK -Repository die alten TAXII -Sammlungen enthält, können Sie das Feld „Datenquelle“ anzeigen. Andernfalls können Sie die Datenquellen mit dem zusätzlichen Kontext von Datenkomponenten im Feld Datenquelle: Datenkomponente anzeigen. Sie können das neue Datenkomponentenfeld nur anzeigen, wenn die Quelle Enterprise ATT&CK ist. Weitere Informationen finden Sie unter Datenkomponentenzuordnung.

5. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie **auf Beziehungen anzeigen**.

Nächste Maßnahme
Sie können die Informationen in einigen dieser zugehörigen Listenobjekte erweitern. Sie können beispielsweise neue Informationen für Gruppe, Verringerung und Externe Referenzen hinzufügen.

Verwalten Sie Risikominderungen

Verwalten Sie die Minderungen, die aus den MITRE TAXII -Sammlungen importiert wurden. Mit Verringerungen können Sie verhindern, dass ein Angreifer erfolgreich Techniken oder Untertechniken gegen Ihre Organisation ausführt. In STIXwerden Minderungen als Vorgehensweisen bezeichnet.

Vorbereitungen
Erforderliche Rolle:

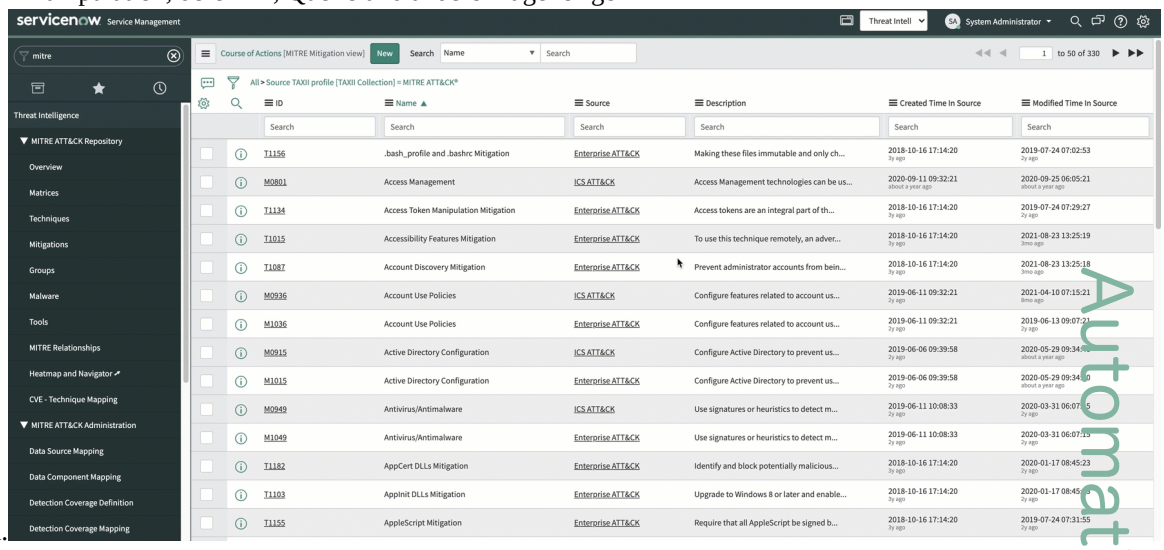
- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Mitigationen**.
   Die Minderungen sind jetzt aufgelistet.
2. Klicken Sie auf eine Verringerung, um alle zugehörigen Informationen anzuzeigen.
   In der folgenden Abbildung sehen Sie die Details zur Minderung der Zugriffs-Token-Manipulation, deren ID, Quelle und anderer zugehöriger Informationen.



3. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie **auf Beziehungen anzeigen**.

Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um die Verringerungsdaten hinzuzufügen oder zu ändern.

Verwalten Sie Gruppen

Verwalten Sie die Gruppen, die aus den MITRE TAXII -Sammlungen importiert wurden. Gruppen sind Sätze zusammengehöriger Angriffsaktivitäten, die in der Sicherheitscommunity unter einem allgemeinen Namen verfolgt werden. Analysten verfolgen Aktivitätscluster anhand verschiedener Begriffe wie Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen. In STIXwerden Gruppen als Angriffssätze bezeichnet.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

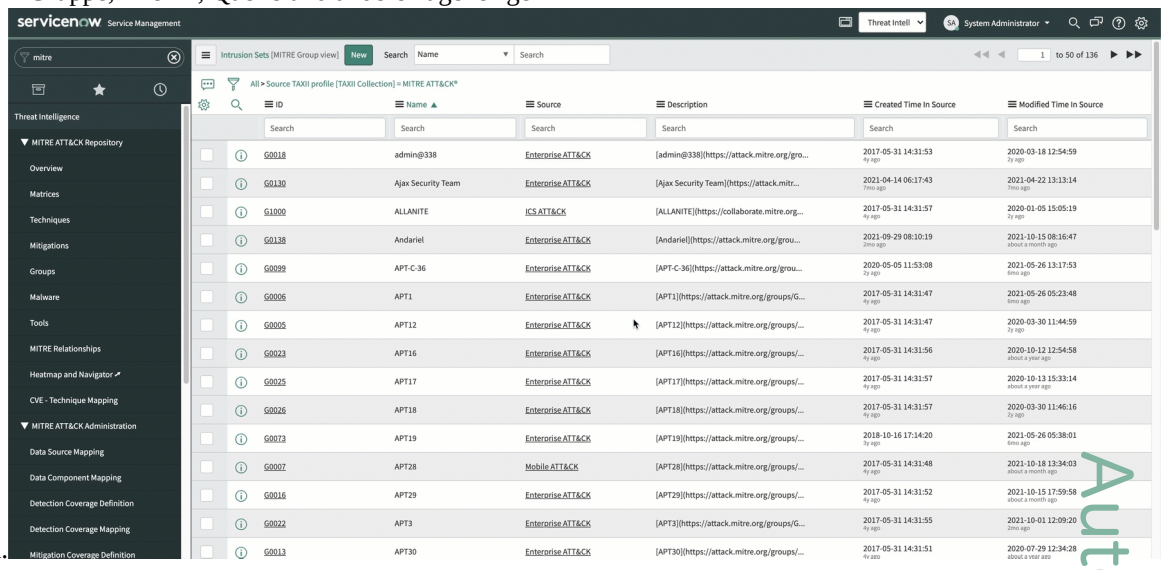
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Gruppen**.
   Sie können die aufgelisteten Gruppen anzeigen.
2. Klicken Sie auf eine Gruppe, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für die Ajax-Sicherheitsteam-Gruppe, ihre ID, Quelle und andere zugehörige Informationen.



3. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie **auf Beziehungen anzeigen**.

> **Hinweis:**
> Um die Bedrohungsgruppen für eine eingehendere Untersuchung einem Sicherheitsfall zuzuordnen, klicken Sie auf **Zu Sicherheitsfall hinzufügen**.

Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um Gruppendaten hinzuzufügen oder zu ändern.

Verwalten Sie Malware

Verwalten Sie die Malware-Informationen, die Sie aus den MITRE TAXII -Sammlungen importiert haben. Malware ist eine Art von TTP, die schädlichen Code darstellt. Bezieht sich auf ein Programm, das heimlich in ein System eingefügt wird. Der Zweck einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

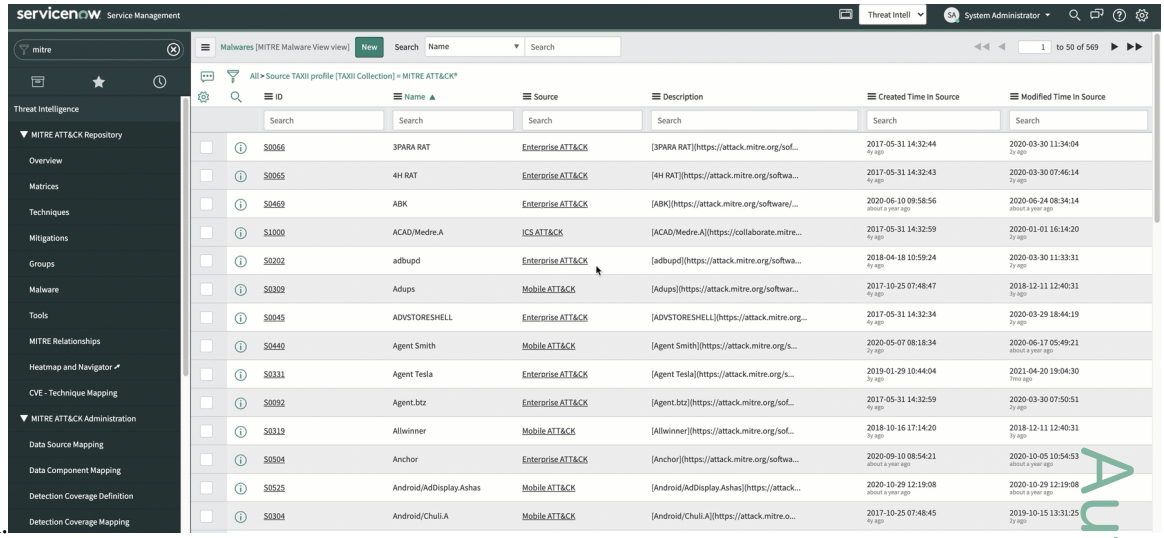
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Malware**.
   Sie können die aufgelistete Malware anzeigen.
2. Klicken Sie auf eine Malware, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für die 3PARA-RAT-Malware, ihre ID, Quelle und andere zugehörige Informationen.



3. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie **auf Beziehungen anzeigen**.

Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um die Malware-Daten hinzuzufügen oder zu ändern.

Tools verwalten

Verwalten Sie die Toolsinformationen, die Sie aus den MITRE TAXII -Sammlungen importiert haben. Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet werden.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

Warum und wann dieser Vorgang ausgeführt wird

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware befinden sich diese Tools oder Softwarepakete häufig auf einem System und dienen berechtigten Zwecken für Power-Benutzer, Administratoren, Netzwerkadministratoren oder sogar normale Benutzer.

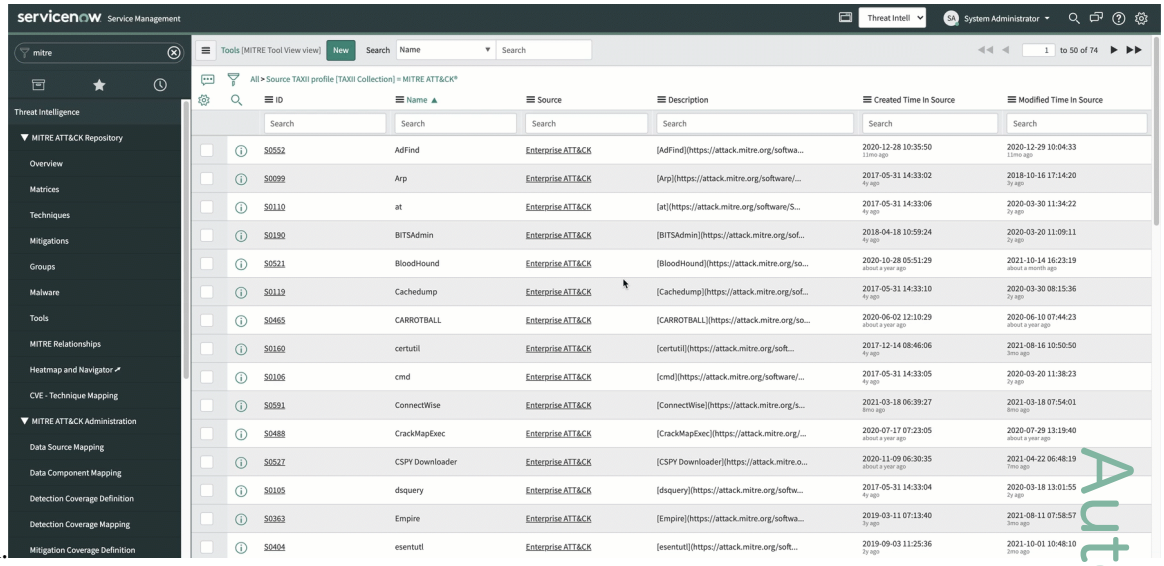
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Tools**.
   Sie können die aufgelisteten Tools anzeigen.
2. Klicken Sie auf ein Tool, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für das Tool CASROTBALL, seine ID, Quelle und andere zugehörige Informationen.



3. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie **auf Beziehungen anzeigen**.

Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um die Tooldaten hinzuzufügen oder zu ändern.

Verwalten Sie MITRE -Beziehungen

Verwalten Sie die MITRE -Beziehungsinformationen, die Sie aus den MITRE TAXII -Sammlungen importiert haben.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

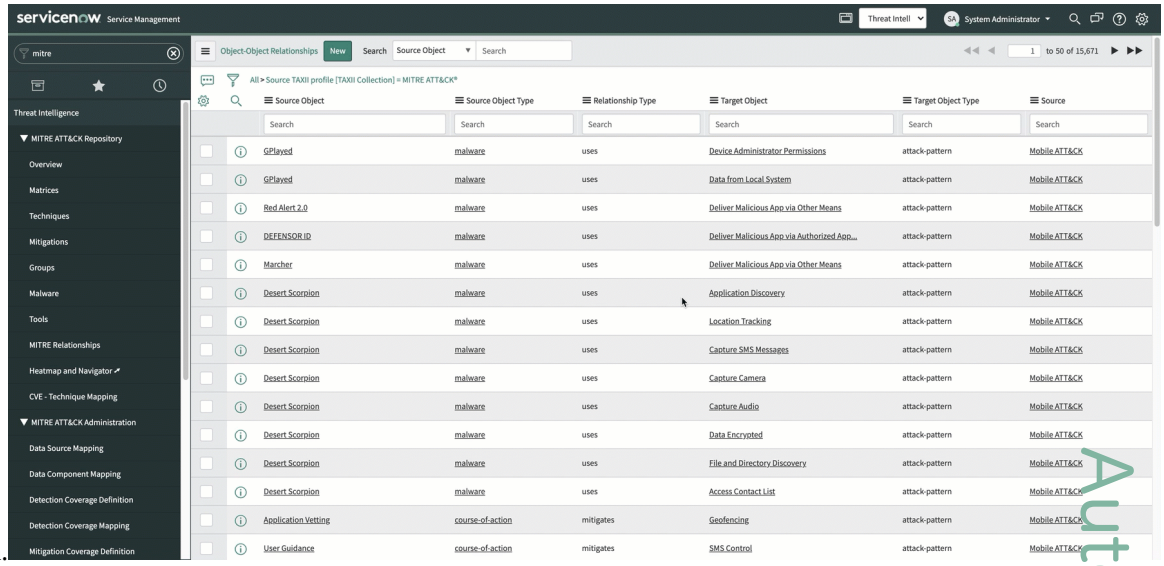
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **MITRE-Beziehungen**. Sie können die aufgelisteten Tools anzeigen.
2. Klicken Sie auf ein Quellobjekt, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für das Objekt Red Alert 2.0, seine ID, Quelle und andere zugehörige Informationen.



3. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie **auf Beziehungen anzeigen**.

Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um MITRE-Beziehungsdaten hinzuzufügen oder zu ändern.

Verwalten Sie die CVE- und Technikzuordnung

Verwalten Sie die CVE- und Technikinformationen, die zugeordnet werden, nachdem Sie die MITRE TAXII -Sammlungen importiert haben.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

Hinweis:
Das Modul **„CVE-Technikzuordnung“** ist nur verfügbar, wenn in Ihrer Umgebung das Produkt Vulnerability Response installiert ist.

Warum und wann dieser Vorgang ausgeführt wird

Sobald Sie die MITRE TAXII -Sammlungen importiert haben, können Sie die CVEs in Ihrer Umgebung und ihre Beziehung zu den zugehörigen MITRE-ATT&CK -Techniken anzeigen. Sie können auch Zuordnungen zu CVEs und zu den Angriffsmustern erstellen.

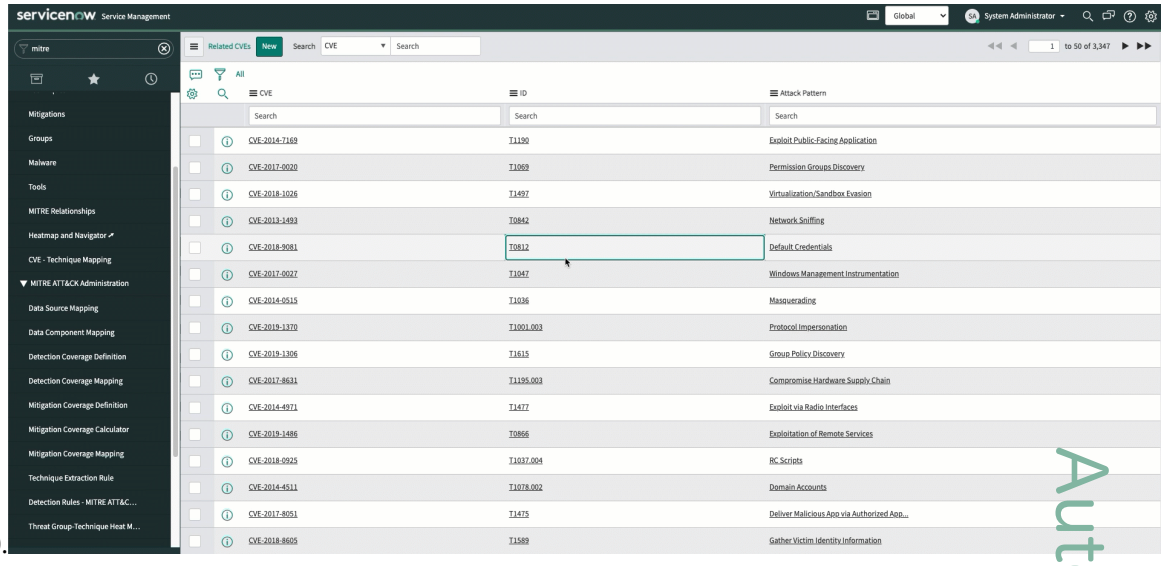
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **CVE – Technikzuordnung**.
   Sie können die aufgelisteten CVEs und Techniken anzeigen.
2. Klicken Sie auf ein CVE, um den Eintrag in der Schwachstellen-Datenbank anzuzeigen.

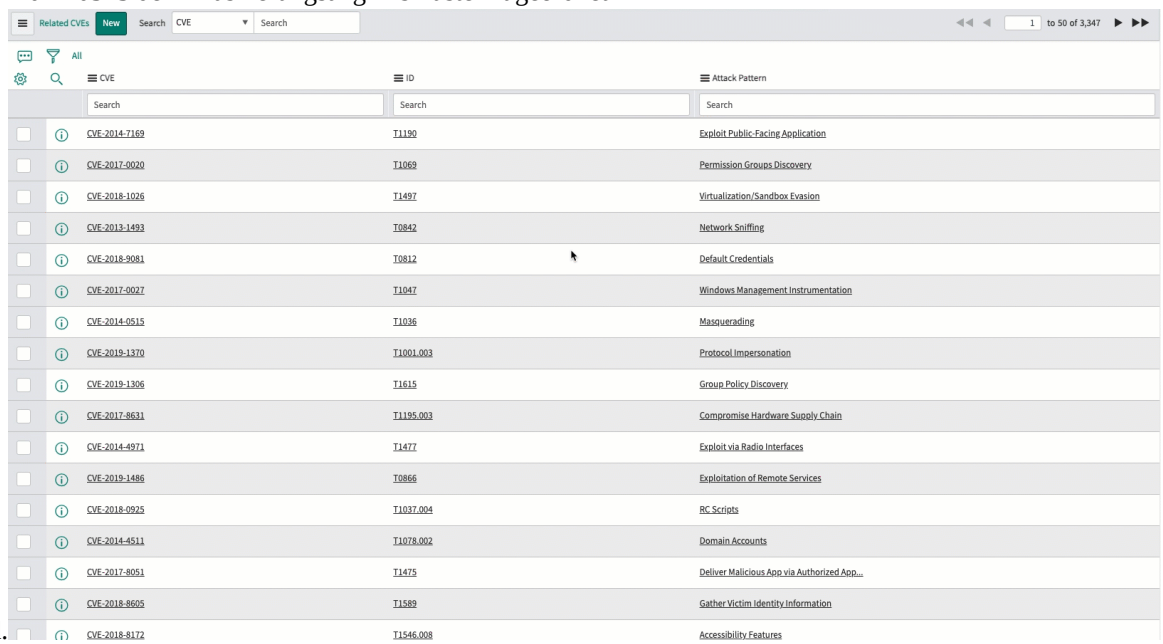
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für die CVE-Liste und den Eintrag in der Schwachstellendatenbank für CVE-2014-7169.



3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, ordnen Sie das CVE einem Angriffsmuster zu, und klicken Sie auf **Absenden**.
   In der folgenden Abbildung wird ein neuer Eintrag erstellt, indem CVE-2014-0515 dem Maskierungsangriffsmuster zugeordnet wird.



Automatische Übersetzung

Erweitern Sie die Daten MITRE-ATT&CK .

Erweitern Sie die Repository-Daten MITRE-ATT&CK in Now Platform durch Anreichern von Daten.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: erstellen, Schreibzugriff

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Objekte Malware, Gruppe, Verringerung und Tool auf eine Technik im Repository MITRE-ATT&CK erweitern.

Sie können ein neues Objekt erstellen und eine Beziehung zwischen einer Technik und dem neuen Objekt im Modul „MITRE ATT&CK-Repository“ herstellen, aber Sie können den Beziehungstyp in diesem Modul nicht definieren. Weitere Informationen zum Definieren von Beziehungstypen finden Sie unter Objekt-zu-Objekt-Beziehungen. Um einen Beziehungstyp zu definieren, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

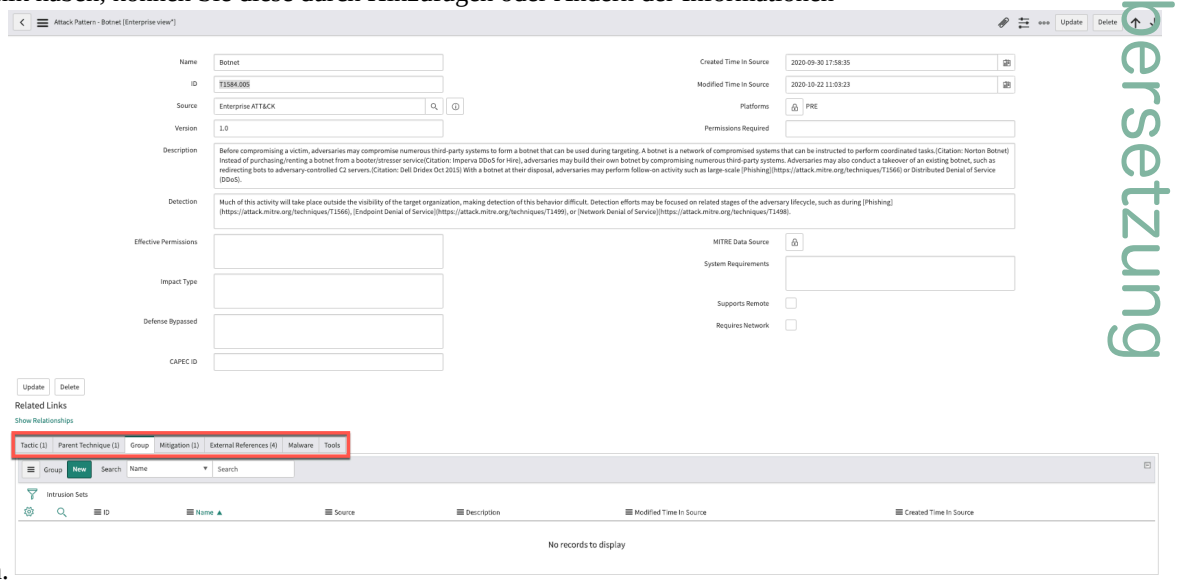
Wenn Sie den Beziehungstyp zwischen einer vorhandenen Technik und einem vorhandenen Objekt zuordnen, müssen Sie die Technik als Zielobjekt und das Objekt als Quellobjekt definieren. Navigieren Sie dazu zu **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

Sie können eine Gruppe erstellen und sie einem Angriffsmuster zuordnen, aber im MITRE ATT&CK-Repository können Sie nur die Beziehung zwischen der Gruppe und dem Angriffsmuster herstellen. Um den Objekt-zu-Objekt-Beziehungstyp zu definieren, müssen Sie dies im IoC-Repository tun.

Hinweis:
Alle Anpassungen, die Sie an den -Objekten vornehmen, werden während geplanter Updates gespeichert.

Prozedur

1. Navigieren zu **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Techniken**.
2. Klicken Sie auf eine Technik oder Untertechnik, um alle zugehörigen Informationen zu dieser Technik anzuzeigen.
   In der folgenden Abbildung können Sie sehen, dass die Botnet-Technik (T1584.005) keiner Gruppe zugeordnet ist. Wenn Sie zusätzliche Informationen zu einer Technik oder Untertechnik haben, können Sie diese durch Hinzufügen oder Ändern der Informationen

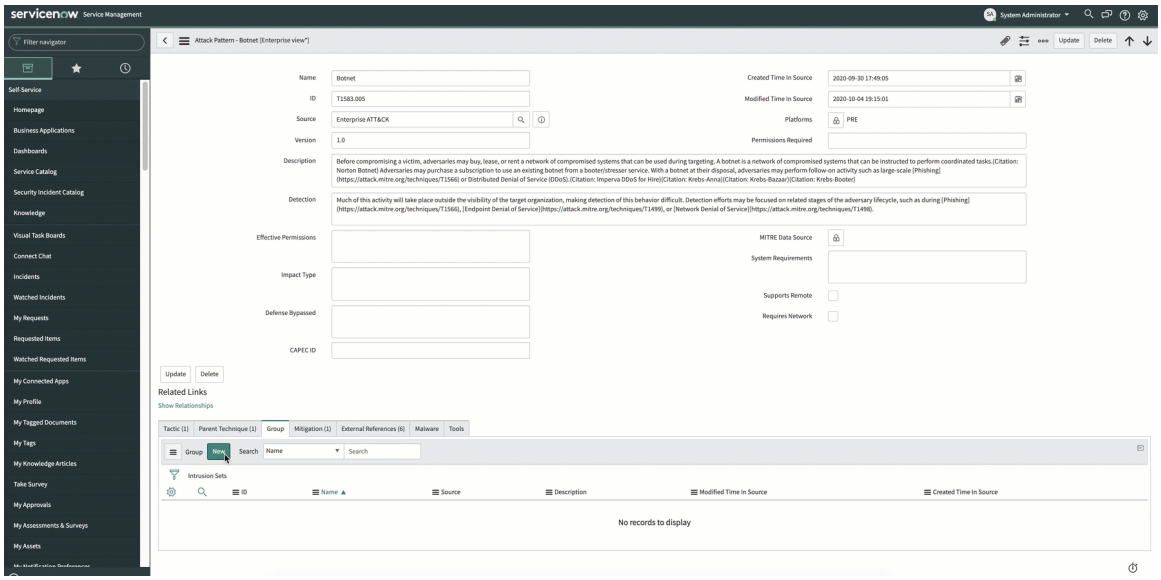


   bereichern.
3. Klicken Sie auf eine zugehörige Liste, um ihre Daten zu ergänzen und sie einer neuen Gruppe zuzuordnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung wurde die Gruppe Custom1 der Botnet-Untertechnik zugeordnet.



Definieren Sie die Zuordnung von Datenquelle und Erkennungstool

Definieren Sie die Zuordnung von Datenquelle und Erkennungstool für MITRE-ATT&CK -Taktiken und -Techniken. Die Datenquellenzuordnung bietet Ihnen Einblick in die Relevanz und Verfügbarkeit der Datenquellen und der Erkennungstools für die Überwachung der Datenquellen in Ihrer Umgebung.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Datenquellen und Erkennungstools identifizieren, die Ihre Organisation benötigt, um die Techniken effektiv zu erkennen.

Wenn sich Ihre Organisation beispielsweise auf 5 Techniken konzentriert, benötigen Sie möglicherweise 10 Datenquellen und 10 Erkennungstools, um diese Quellen zu überwachen. Angenommen, Sie stellen fest, dass Ihre Organisation nicht über zwei Datenquellen und fünf Erkennungstools verfügt. Diese Übung gibt Ihnen Einblick in die Datenquellen und ihre Relevanz für Ihr Unternehmen sowie zur Identifizierung von Lücken in der Abdeckung. Sie können sich auch auf die Verbesserung Ihrer Umgebung mit den richtigen Datenquellen und Erkennungstools konzentrieren.

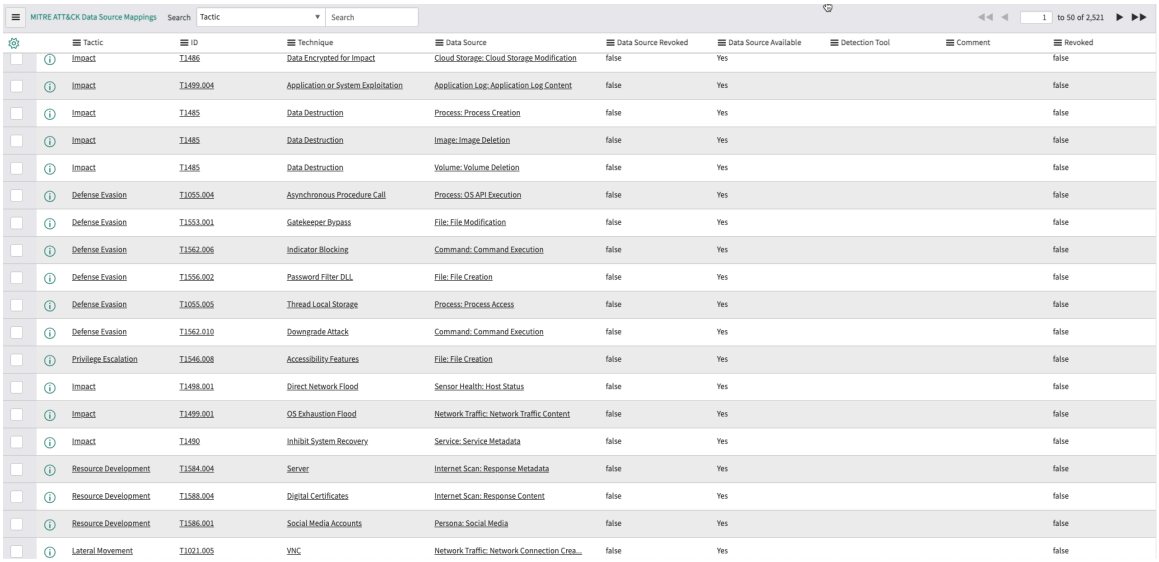
Alle aktiven Taktiken, Techniken, IDs und Datenquellen werden basierend auf Ihren Datenquellen automatisch ausgefüllt TAXII Profil

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Datenquellenzuordnung**.

   Die folgende Abbildung zeigt die Liste der Taktiken, Techniken und ihre IDs, die basierend auf Ihren Sammlungsaktualisierungen ausgefüllt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Taktik	Ziel des Angreifers oder der Grund für die Durchführung einer Aktion
ID	Eindeutige Identität der Technik.
Technik	Wie ein Angreifer ein strategisches Ziel durch eine Aktion erreicht.
Datenquelle	Datenquelle, die der Technik zugeordnet ist.
Datenquelle widerrufen	Datenquelle wird widerrufen, wenn sie auf „wahr“ festgelegt ist, die Datenquellenzuordnung wird jedoch weiterhin beibehalten. Wenn der Datenquellenwert nicht in MITREgefunden wird, wird der Wert Datenquelle widerrufen automatisch als „wahr“ markiert. Die Datenquellenzuordnung für einen Datensatz wird widerrufen, wenn die Beziehungen für Technik und Datenquelle in den aktualisierten Daten MITRE fehlen. Standardwert: false
Datenquelle verfügbar	Verfügbarkeit der Datenquelle.
Erkennungstool	Tool, das die Datenquelle ergänzt, indem es die verwendeten Techniken erkennt. Das Erkennungstool wird dem Warnungssensor in SIRzugeordnet.
Widerrufen	Die Datenquellenzuordnung für einen Datensatz wird widerrufen, wenn die Beziehungen für Technik und Datenquelle in den aktualisierten Daten MITRE fehlen. Standardwert: false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Überprüfen Sie die aufgelisteten Datenquellen, und ändern Sie den Wert im Feld **Datenquelle verfügbar** entsprechend Ihrer Umgebung.

3. **Hinweis:**
   Sie können diesen Eintrag nicht in der Listenansicht bearbeiten.

   Führen Sie im Feld **Erkennungstool** die folgenden Schritte aus:

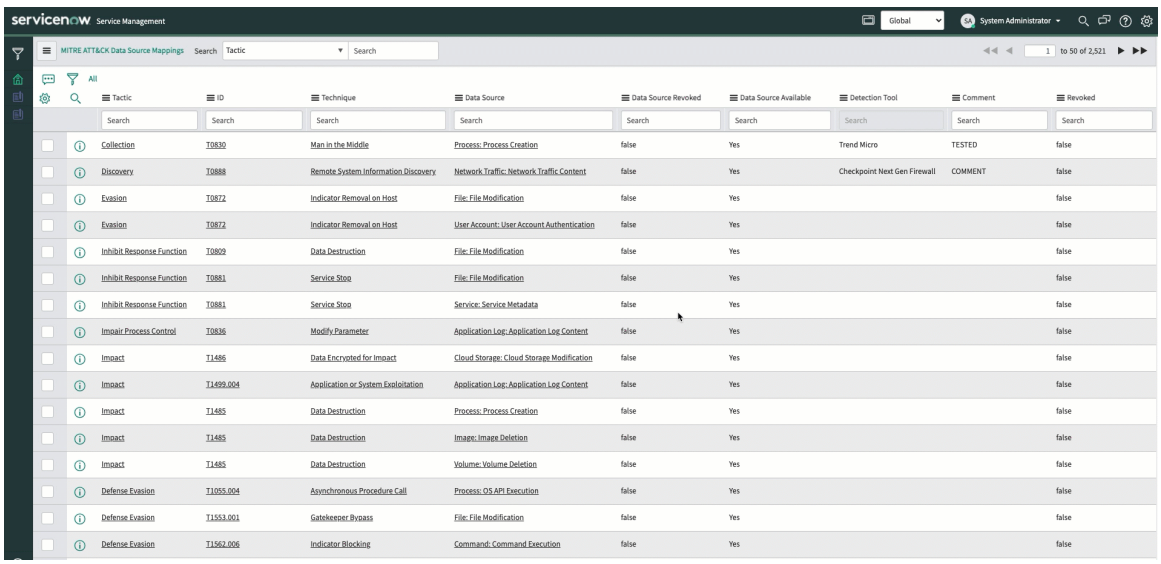
   a. Klicken Sie auf das Informationssymbol und anschließend auf **Datensatz öffnen**.

   b. Entsperren Sie den Eintrag **des Erkennungstools**.

   c. Verwenden Sie die Nachschlageliste, um ein Erkennungstool auszuwählen. Erkennungstools können mehrfach ausgewählt werden.

   d. Klicken Sie auf **Aktualisieren**.

   In der folgenden Abbildung werden mehrere Erkennungstools hinzugefügt, um die Datenquelle zu überwachen.



Definieren Sie die Datenquellen- und Datenkomponentenzuordnung

Verwenden Sie die Datenkomponentenzuordnung, wenn Sie die neuesten TAXII -Sammlungen verwenden und eine Beziehung zwischen den Datenquellen, Datenkomponenten und den verschiedenen Techniken aufrechterhalten möchten. Ordnen Sie die Datenquellen mit dem zusätzlichen Kontext von Datenkomponenten zu, der den Datenquellen eine zusätzliche Unterebene des Kontexts bietet, sodass Sie das Verhalten des Angreifers in MITRE-ATT&CK besser verstehen können.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Die Zuordnung der Datenquellen und Datenkomponenten bietet Einblick in die Datenquellen oder -komponenten und -techniken, die für Ihre Organisation relevant sind.

Wenn sich Ihre Organisation beispielsweise auf 7 Techniken konzentriert, benötigen Sie möglicherweise 5 Datenquellen und 10 Datenkomponenten, um diese Quellen zu

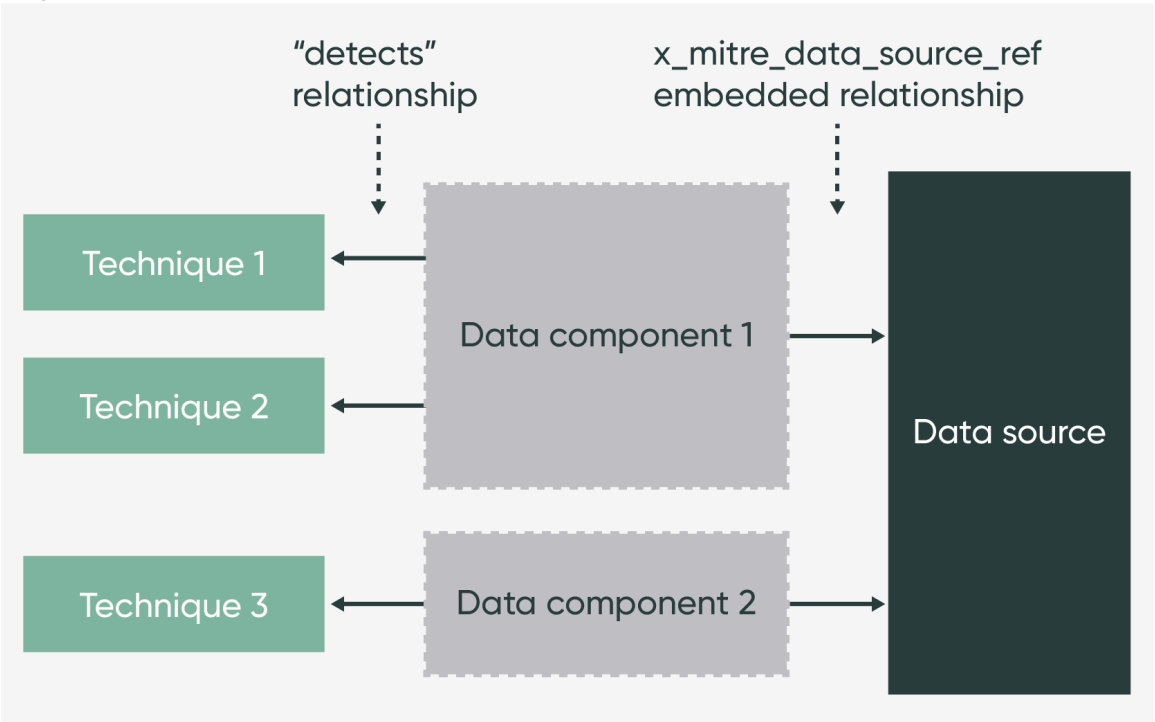
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

überwachen. Ihre Bewertung interner Tools zeigt, dass Ihre Organisation nicht über zwei Datenquellen und vier Datenkomponenten verfügt. Diese Zuordnungsübung bietet Einblick in die Datenquellen, Komponenten und Techniken, ihre Relevanz für Ihr Unternehmen und identifiziert die Lücken in der Abdeckung. Sie können Ihre Investitionen auf die richtigen Datenquellen und Warnungssensoren konzentrieren, um Angreiferbedrohungen zu erkennen und zu entschärfen.

Das Framework MITRE-ATT&CK enthält eine aktualisierte Struktur für die Datenquellen Datenquelle: Datenkomponente. Diese neue Form der Datenquelle bietet einen zusätzlichen Kontext für die Datenquellen. Das Datenquellenobjekt enthält den Namen der Datenquelle sowie wichtige Details zu den gesammelten Daten (Datei, Prozess, Netzwerkverkehr usw.) und bestimmte Werte oder Eigenschaften, die zur Erkennung des Angreiferverhaltens erforderlich sind.

Die folgende Abbildung zeigt die MITRE-ATT&CK STIX™ -Strukturdarstellung für Datenquellen und Datenkomponenten. Sie können sowohl die Datenquellen als auch die Datenkomponenten anzeigen, die als anwenderdefinierte Objekte STIX™ erfasst wurden. Die Abbildung zeigt, dass jede Datenquelle eine oder mehrere Datenkomponenten enthält und jede Datenkomponente eine oder mehrere Techniken erkennt.

Allgemeine Struktur von Datenquellen und Datenkomponenten

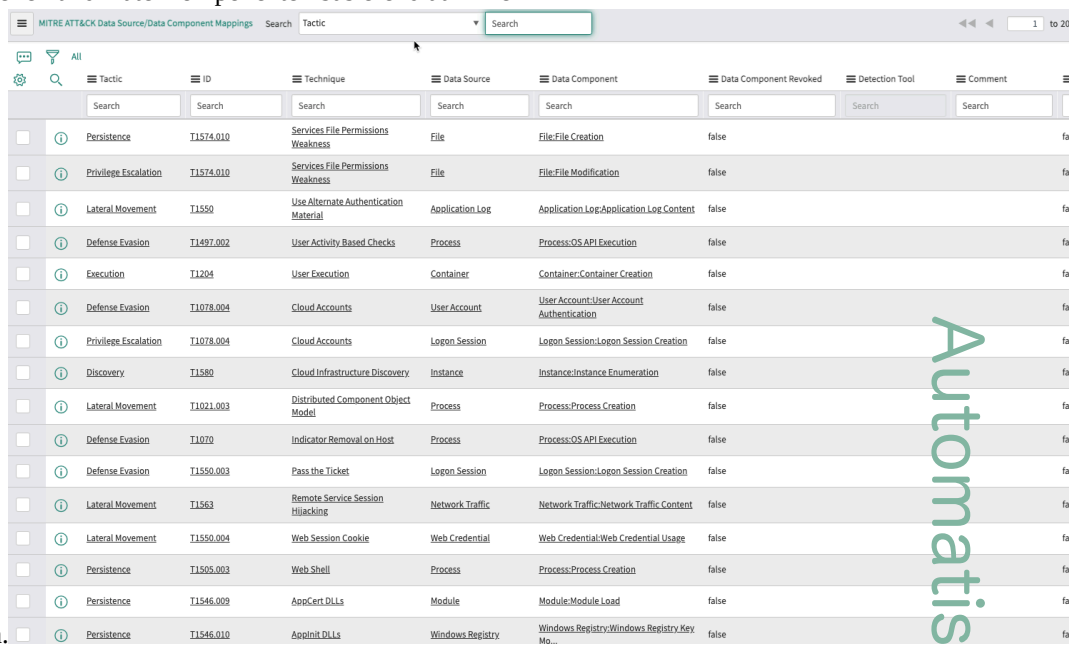


Sie können die Datenquellenzuordnung weiterhin verwenden, wenn Ihr -Repository MITRE-ATT&CK die alten TAXII -Sammlungen enthält und Sie Ihre Datenquellen verschiedenen Techniken zugeordnet haben. Verwenden Sie jedoch die Datenkomponentenzuordnung, wenn Sie die neuesten TAXII -Sammlungen verwenden und eine Beziehung zwischen den Datenquellen, Datenkomponenten und den verschiedenen Techniken aufrechterhalten möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Datenkomponentenzuordnung**.
   Die folgende Abbildung zeigt die Liste der Taktiken, IDs, Techniken zusammen mit den Datenquellen und Datenkomponenten basierend auf Ihren Sammlungsaktualisierungen.



Feld	Beschreibung
Taktik	Ziel des Angreifers oder der Grund für die Durchführung einer Aktion
ID	Eindeutige Identität der Technik.
Technik	Wie ein Angreifer ein strategisches Ziel durch eine Aktion erreicht.
Datenquelle	Datenquelle, die der Technik zugeordnet ist.
Datenkomponente	Datenkomponente, die der Datenquelle zugeordnet ist. Eine Datenkomponente kann nur eine übergeordnete Datenquelle haben.
Datenkomponente widerrufen	Gibt an, ob die Datenkomponente in der Knowledge Base MITRE-ATT&CK widerrufen wurde.
Erkennungstool	Tool, das die Datenquelle ergänzt, indem es die verwendeten Techniken erkennt. Das Erkennungstool wird dem Warnungssensor in SIRzugeordnet.
Kommentar	Beschreibung zur Zuordnung von Datenquelle und Datenkomponente.
Widerrufen	Gibt an, ob die Datenkomponente für die Technikzuordnung von MITRE-ATT&CKwiderrufen wird.

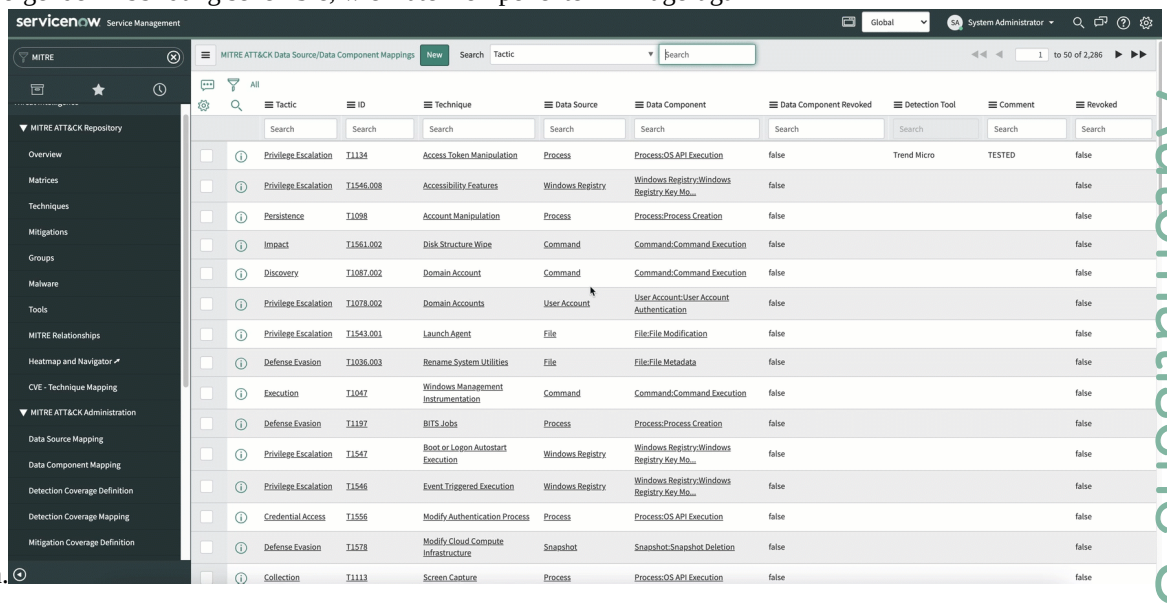
2. Überprüfen Sie die aufgelisteten Datenquellen und Datenkomponenten, und ändern Sie die Werte entsprechend Ihrer Umgebung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie diese Schritte aus, um eine Datenkomponente hinzuzufügen.
   a. Navigieren zu **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Techniken**.
   b. Klicken Sie auf eine Technik, mit der Sie die Datenquelle ändern möchten: Datenkomponenteninformationen.
   c. Datenquelle entsperren: Datenkomponente.
   d. Verwenden Sie die Nachschlageliste, um MITRE-ATT&CK Datenkomponenten auszuwählen.
   e. Datenquelle für Sperre: Datenkomponente.
   f. Klicken Sie auf **Aktualisieren**.

In der folgenden Abbildung sehen Sie, wie Datenkomponenten hinzugefügt werden.



Definieren Sie die Abdeckung der Technikerkennung

Definieren Sie die Abdeckung der Technikerkennung, die Ihre Organisation messen muss, um bestimmte Angreifertechniken zu erkennen.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreibzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

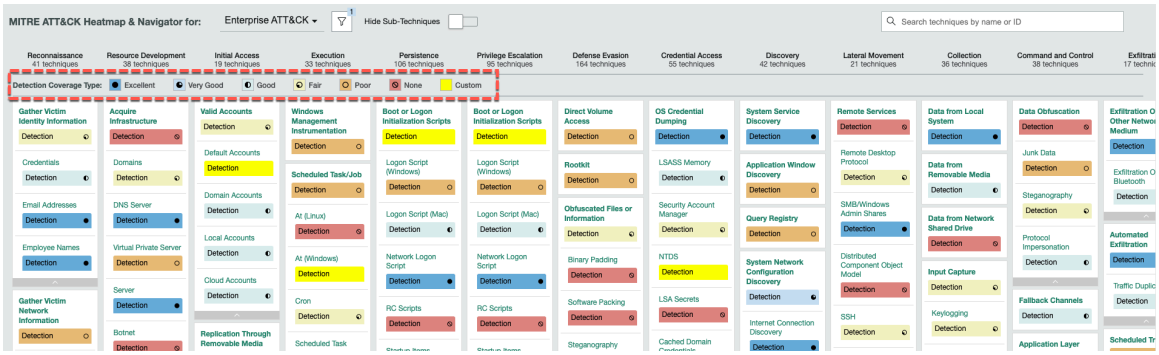
Die Definitionen der Technikabdeckung werden in der allgemeinen Zuordnung der Technikerkennung verwendet. Sie können die Basissystem-Technikabdeckung verwenden. Die Abdeckung des Basissystems Technik besteht aus den Abdeckungstypen Keine, Schwach, Mittel, Gut, Sehr gut und Ausgezeichnet.
Die Technikabdeckung des Basissystems ist auch mit vordefinierten Farben verknüpft. Sie können die Abdeckungstypeinträge und Farben anpassen oder eigene Einträge erstellen. Sie können beispielsweise die Deckungsarten des Basissystems in Nicht zutreffend, Teilweise Deckung und Vollständige Deckung ändern. Alternativ können Sie auch numerische Maßnahmen für die Abdeckungstypen wie 0–25 Prozent, 25–50 Prozent und 50–100 Prozent erstellen. Die Art der an der Basissystemabdeckung vorgenommenen Änderungen ist nicht auf die freigegebenen Beispiele beschränkt.

Die Anpassungen, die Sie am Abdeckungstyp und an der Farbe vornehmen, werden in der gesamten Technikerkennungszuordnung und in der Heatmapverwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie die Abdeckungsdefinition des Basissystems ändern, werden die Symbole für Abdeckungstypen nicht mit den Techniken in der Heatmap angezeigt. Die Heatmap funktioniert wie erwartet, wenn Sie dieselben Felder wie die im Basissystem definierte Technikerkennungsabdeckung und die Abdeckungsfarben ändern. Wenn Sie jedoch vorhandene Felder aus der allgemeinen Technikerkennungsabdeckung löschen, werden die Symbole für die Abdeckungstypen in der Heatmap nicht angezeigt.



Prozedur

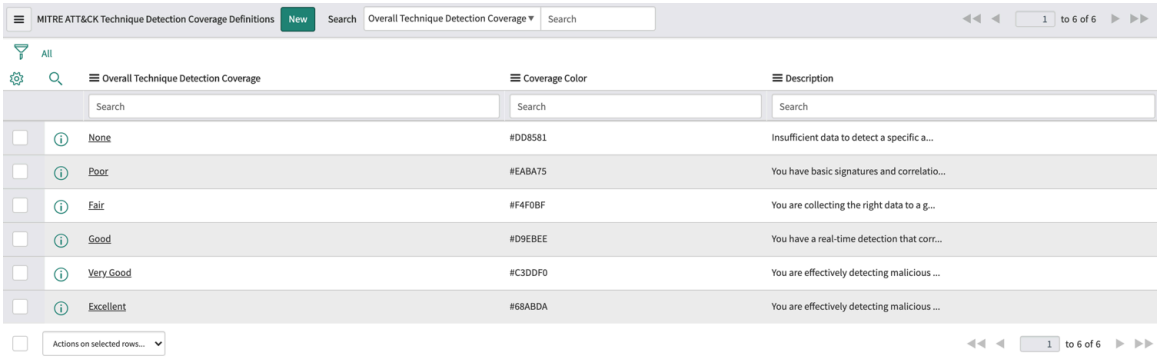
1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Erkennungsabdeckung**.
2. Überprüfen Sie die allgemeinen Technikerkennungseinträge, und passen Sie die Einträge für Ihre Umgebung an.

Definition der Erkennungsabdeckung

Feld	Beschreibung
Gesamtabdeckung für Technik-Erkennung	Name der allgemeinen Technik-Erkennungsabdeckung. Die Abdeckung der Basistechnik besteht aus Keine, Schwach, Mittel, Gut, Sehr gut oder Ausgezeichnet.
Abdeckungsfarbe	Farbe, die der Punktzahl für die Erkennungsabdeckung zugewiesen ist. Die von Ihnen definierte Farbe wird für die Technikerkennungsabdeckung in der Heatmap verwendet. Sie können die Farben mit HEX-Codes und RGB(A)-Werten anpassen.
Beschreibung	Allgemeine Abdeckung der Technik-Erkennung. Die Basissystemdefinition finden Sie in der Bewertungsdefinition.

Die folgende Abbildung zeigt die Liste „Definition der Erkennungsabdeckung“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, füllen Sie die Einträge aus, und klicken Sie auf **Absenden**.

MITRE-ATT&CK Bewertungsdefinition

Definieren Sie das Bewertungssystem MITRE-ATT&CK Ihrer Organisation, damit Sie messen können, wie effektiv Ihre Organisation bestimmte Angreifertechniken erkennen kann.

Bewertungsdefinition

Punktzahl	Punktzahlzuordnung	Beschreibung
Keine	0	Unzureichende Daten, um eine bestimmte Angreifertechnik zu erkennen.
Mangelhaft	1	Es sind grundlegende Signaturen und Korrelationsregeln vorhanden, um bestimmte Angreifertechniken zu erkennen. Die Bedrohungserkennung erfolgt nicht in Echtzeit und deckt nur eine minimale Anzahl von Aspekten einer Technik ab. Beispiel: Die Suche erfolgt jeweils nur an einem Endpunkt. Ihre Organisation verfügt möglicherweise noch über Tausende oder Hunderte von Ereignissen, die von Bearbeitern überprüft und mit anderen Ereignissen korreliert werden müssen, um Sonderfälle zu ermitteln. Die Anzahl der falsch positiven Ergebnisse ist hoch.
Befriedigend	2	Es werden in großem Umfang die richtigen Daten gesammelt, und die Datenqualität ist fair. Beispielsweise könnte Ihre Organisation damit beginnen, Sysmon-Protokolle, ETW, PowerShell-Protokolle und Ähnliches hinzuzufügen. Die Bedrohungserkennung erfolgt jedoch immer noch nicht in Echtzeit. Ihre Organisation verfügt möglicherweise nicht über die richtigen Tools, um die Daten effektiv zusammenzufassen und zu analysieren. Um die Daten genau zu analysieren, müssen sie manuell Abfragen ausführen und korrelieren. Die Anzahl der falsch positiven Ergebnisse ist hoch.
Gut	3	Echtzeiterkennung, die mehrere Daten über Ihre Endpunkte hinweg korreliert und integriert. Die Bedrohungserkennung deckt viele Aspekte der Verfahren einer Technik ab. Ihre Angreifer können möglicherweise die Erkennung durch Umgehung und Verschleierung umgehen. Ihre Organisation kann Falschmeldungen leicht identifizieren und herausfiltern. Ihre Organisation verwendet grundlegende Data-Science-Techniken, um die Daten im zentralen Repository zu analysieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertungsdefinition (Fortsetzung)

Punktzahl	Punktzahlzuordnung	Beschreibung
Sehr gut	4	Erkennen Sie schädliche Techniken effektiv und in Echtzeit, und decken Sie die meisten Aspekte der Verfahren einer Technik ab. Die Möglichkeit, dass Ihre Angreifer die Erkennung mit Umgehungs- und Verschleierungsmethoden umgehen, ist schwerwiegender als auf der Stufe „Gut“. Ihre Organisation kann Falschmeldungen leicht identifizieren und herausfiltern. Ihre Organisation verwendet hochentwickelte Data-Science-Techniken, um die Angreifertechniken zu erkennen.
Ausgezeichnet	5	Erkennen Sie schädliche Techniken effektiv und in Echtzeit, und decken Sie alle Aspekte der Verfahren einer Technik ab. Ihre Organisation versteht Ihre Umgebung mit der richtigen Automatisierung und Qualität der Daten gut. Die Möglichkeit, dass Ihre Angreifer die Erkennung mit Umgehungs- und Verschleierungsmethoden umgehen, ist auf dieser Ebene nicht möglich. Die Anzahl der falsch negativen Ergebnisse ist niedrig.

Ordnen Sie Ihre Technikerkennungsabdeckung einer Technik zu

Ordnen Sie Ihre allgemeine Technikerkennungsabdeckung der Technik zu, mit der Ihre Organisation bestimmte Angreifertechniken erkennen kann.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreibzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Technik-Erkennungsabdeckung verwenden, um einen Überblick über die allgemeine Technik-Erkennungsabdeckung Ihrer Organisation zu erhalten. Wenn beispielsweise ein Angreifer Ihre Organisation angreift, sehen Sie die Art der Abdeckung, die Sie benötigen, um die Techniken des Angreifers zu erkennen.

Die Technik und die ID werden automatisch für alle Sammlungen und Techniken ausgefüllt, die Sie aktiviert haben. Der Abdeckungstyp und die von Ihnen definierte Bewertungsdefinition sind für als Option verfügbar, die Sie in der allgemeinen Technikerkennungsabdeckung auswählen können.

Sie können die allgemeine Technik-Erkennungsabdeckung der Technik zuordnen, um die Zuordnung abzuschließen. Sie können eine Technik nur mit einer einzigen allgemeinen Technik-Erkennungsabdeckung verknüpfen.

Die von Ihnen definierte Zuordnung der Abdeckung der Technikerkennung wird in der Abdeckungsvisualisierung in der Heatmapverwendet.

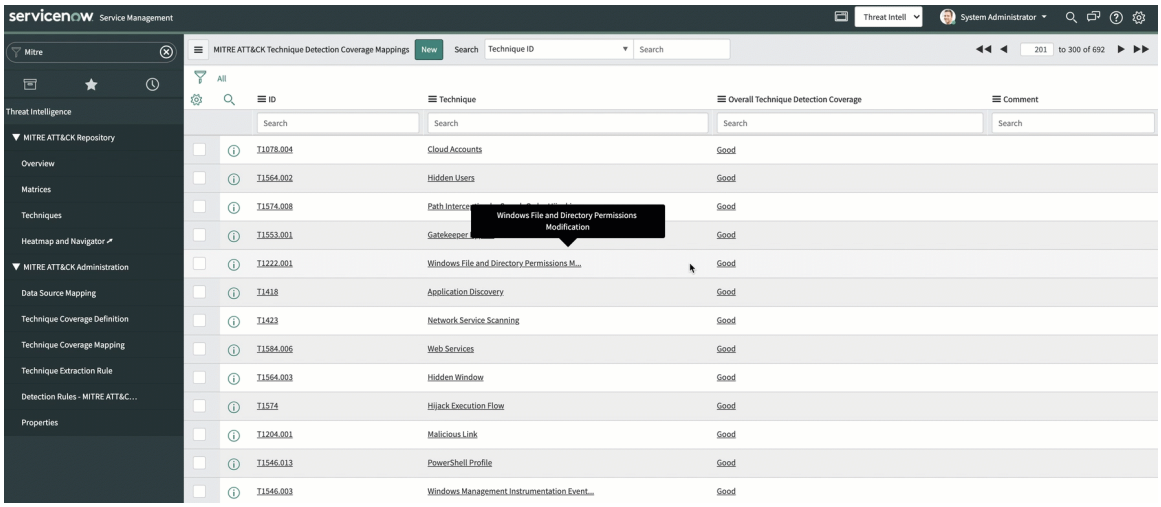
Hinweis:
Zur allgemeinen Abdeckung der Technikerkennung können Sie mithilfe Ihrer organisatorischen Berechnungen gelangen. Sie können alle BAS-Produkte (Breach & Attack Simulation), das Cyber Analytics Repository (PAR) oder andere Methoden nach Bedarf verwenden, um die Bewertungsdefinition zu definieren, und sie in diesem Verfahren für die allgemeine Zuordnung der Technikerkennungsabdeckung verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Zuordnung der Abdeckung durch Erkennung**.

   In dieser Abbildung sehen Sie, dass die Untertechnik Cloud-Accounts (T1078.004) in der Organisation sehr gut abgedeckt ist und dass die allgemeine Technik-Erkennungsabdeckung **Ausgezeichnet**zugeordnet ist.



2. Überprüfen Sie jede Technik, und ordnen Sie Ihre allgemeine Technik-Erkennungsabdeckung basierend auf Ihrer Definition der Erkennungsabdeckung und der Verfügbarkeit der Abdeckung in Ihrer Organisation zu.

Definieren Sie die Abdeckung durch die Risikominderung

Definieren Sie die Abdeckung durch die Risikominderung für jede Risikominderung, die einer Technik zugeordnet ist, um Einblick zu erhalten, wie gut Ihre Organisation die Angriffe verhindern kann, die aufgrund einer bestimmten Technik auftreten.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Die Definitionen der Abdeckung durch Risikominderung werden in der allgemeinen Zuordnung der Abdeckung durch Risikominderung und Technik verwendet. Sie können die Abdeckung durch Basissystemminderung verwenden. Die Abdeckung durch die Basissystemminderung besteht aus den Abdeckungstypen Keine, Schwach, Mittel, Gut, Sehr gut und Ausgezeichnet. Die Abdeckung durch die Basissystemminderung ist auch mit vordefinierten Farben und Abdeckungsprozentsätzen verknüpft. Sie können die Abdeckungstypen (Abdeckungstypen hinzufügen oder entfernen), die Prozentsätze der Abdeckung für Unter- und Obergrenzen und die Farben anpassen oder Ihre anwenderdefinierte Abdeckung für Risikominderungen erstellen.

Die Anpassungen, die Sie an den Abdeckungstypen, Farben oder Prozentsätzen vornehmen, werden in der Zuordnung der Abdeckung durch Risikominderung und in der Heatmapverwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Abdeckung durch Risikominderung**.
2. Überprüfen Sie die Erkennungseinträge für die Verringerung, und passen Sie die Einträge für Ihre Umgebung an.

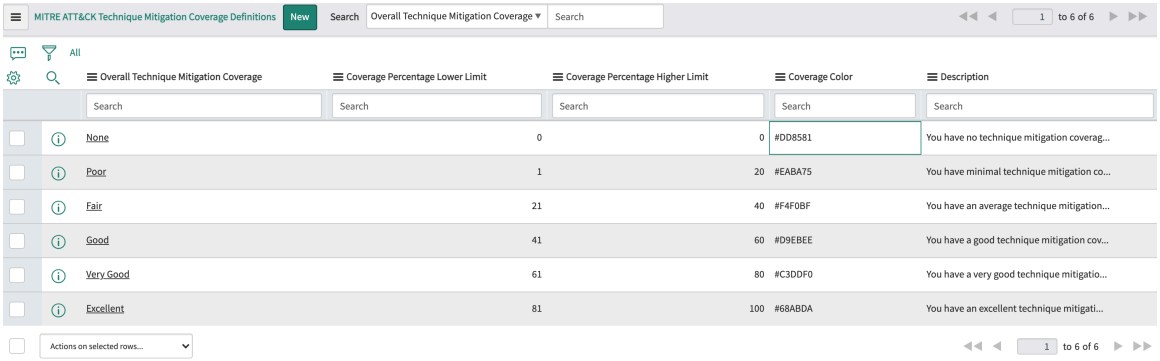
Technik – Definition der Abdeckung durch Risikominderung

Feld	Beschreibung
Allgemeine Abdeckung durch Technik zur Risikominderung	Name der Abdeckung der Technik durch Risikominderung. Die Abdeckung durch die Verringerung des Basissystems besteht aus Keine, Schwach, Mittel, Gut, Sehr gut oder Ausgezeichnet.
Unterer Grenzwert des Abdeckungsprozentsatzes	Der untere Prozentsatzgrenzwert der Abdeckung durch Risikominderung. Definieren Sie numerische Werte zwischen 0 und 100.
Oberer Grenzwert des Abdeckungsprozentsatzes	Die höhere prozentuale Grenze der Abdeckung durch Risikominderung. Definieren Sie numerische Werte zwischen 0 und 100.
Abdeckungsfarbe	Farbe, die der Punktzahl für die Erkennungsabdeckung zugewiesen ist. Die von Ihnen definierte Farbe wird für die Technikminderungsabdeckung in der Heatmap verwendet. Sie können die Farben mit HEX-Codes und RGB(A)-Werten anpassen.
Beschreibung	Gesamtabdeckung der Erkennung durch Risikoverringerung. Weitere Informationen finden Sie in der Definition des Basissystems in der Definition der Technik für die Abdeckung durch Risikominderung.

Hinweis:
Stellen Sie sicher, dass Sie die Prozentbereiche der Abdeckung nicht überschneiden, wenn Sie die Prozentgrenzen (niedriger oder höher) anpassen. Wenn beispielsweise ein Abdeckungsdatensatz die Bereiche 0 bis 20 aufweist, muss der nächste nachfolgende Datensatz einen unteren Grenzwertbereich von 21 oder höher haben, um eine Überlappung des Abdeckungsprozentsatzbereichs zu vermeiden.

Die folgende Abbildung zeigt die Liste der Definitionen der Abdeckung durch Risikominderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, füllen Sie die Einträge aus, und klicken Sie auf **Absenden**.

Definitionen der Technik für die Abdeckung durch Risikominderung

Definieren Sie die Abdeckung durch Risikominderung, damit Sie bestimmte Angreifertechniken effektiv messen und erkennen können.

MITRE ATT&CK-Technik – Definitionen der Abdeckung durch Risikominderung

Allgemeine Abdeckung durch Technik zur Risikominderung	Unterer Grenzwert des Abdeckungsprozent	Oberer Grenzwert des Abdeckungsprozent	Abdeckungsfarbe	Beschreibung
Keine	0	0	#DD8581	Sie verfügen nicht über eine Abdeckung durch Technikverringerung, und Ihre Verteidigungssteuerungen können in keinem Szenario einen Angriff verhindern.
Mangelhaft	1	20	#EABA75	Sie haben eine minimale Abdeckung durch Technikminderung. Die Wahrscheinlichkeit eines Angriffs ist sehr hoch, und Ihre Verteidigungskontrollen können einen Angriff in 0 bis 20 Prozent der Szenarien verhindern.
Befriedigend	21	40	#F4F0BF	Sie haben eine durchschnittliche Abdeckung durch Technikverringerung. Die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE ATT&CK-Technik – Definitionen der Abdeckung durch Risikominderung (Fortsetzung)

Allgemeine Abdeckung durch Technik zur Risikominderung	Unterer Grenzwert des Abdeckungsprozent	Oberer Grenzwert des Abdeckungsprozent	Abdeckungsfarbe	Beschreibung
				Wahrscheinlichkeit eines Angriffs ist hoch, und Ihre Verteidigungssteuerungen können einen Angriff in 21 bis 40 Prozent der Szenarien verhindern.
Gut	41	60	#D9EBEE	Sie verfügen über eine gute Abdeckung durch Technikminderung. Die Wahrscheinlichkeit eines Angriffs ist jedoch relativ hoch, und Ihre Verteidigungskontrollen können einen Angriff in 41 bis 60 Prozent der Szenarien verhindern.
Sehr gut	61	80	#C3DDF0	Sie verfügen über eine sehr gute Abdeckung durch Technikminderung. Die Wahrscheinlichkeit eines Angriffs ist gering, und Ihre Verteidigungskontrollen können einen Angriff in 61 bis 80 Prozent der Szenarien verhindern.
Ausgezeichnet	81	100	#68ABDA	Sie verfügen über eine hervorragende Abdeckung durch Technikminderung, und die Wahrscheinlichkeit eines Angriffs mit dieser Technik ist sehr

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE ATT&CK-Technik – Definitionen der Abdeckung durch Risikominderung (Fortsetzung)

Allgemeine Abdeckung durch Technik zur Risikominderung	Unterer Grenzwert des Abdeckungsprozent	Oberer Grenzwert des Abdeckungsprozent	Abdeckungsfarbe	Beschreibung
				gering, und Ihre Verteidigungssteuerungen können einen Angriff in 81 bis 100 Prozent der Szenarien verhindern.

Ordnen Sie Ihre Abdeckung durch Risikominderung einer Technik zu

Ordnen Sie Ihre Abdeckung durch Risikominderung der Technik zu, mit der Sie die allgemeine Risikomanagementstrategie Ihrer Organisation erkennen können.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreib-, Löschzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Mit Verringerungen können Sie verhindern, dass ein Angreifer erfolgreich Techniken oder Untertechniken gegen Ihre Organisation ausführt. Jede MITRE-ATT&CK -Technik enthält Ausgleichsmaßnahmen, die Sie in Ihrer Organisation bereitstellen können, um das Risiko von Angriffen zu verringern. Sie können die Abdeckung durch Risikominderung verwenden, um einen Überblick über die allgemeine Risikominderungsstrategie Ihrer Organisation zu erhalten. Wenn beispielsweise ein Angreifer Ihre Organisation angreift, sehen Sie die Art der Abdeckung, die Sie benötigen, um die Techniken des Angreifers abzuwehren.

Die Technik und die Minderungsinformationen werden automatisch für alle Sammlungen und Techniken ausgefüllt, die Sie aktiviert haben. Die von Ihnen definierte Definition der Abdeckung durch Risikominderung steht Ihnen in der Technik-Abdeckung zur Risikominderung zur Auswahl.

Sie können Minderungen identifizieren, die für Ihre Organisation relevant sind. Wenn eine Verringerung relevant ist, können Sie definieren, ob die Verringerungsstrategien bereitgestellt wurden. Sie können angeben, ob die Strategien als Teil der SOC-Richtlinie Ihrer Organisation angewendet werden. Sie können auch feststellen, ob Ihre Organisation über vorbeugende Tools verfügt, um die Techniken eines Angreifers abzuschwächen, und Sie können alle Sicherheitskontrollen zuordnen, die Ihre Organisation bereitgestellt hat, um Sicherheitsrisiken zu minimieren. Füllen Sie die Abdeckung durch die Verringerung (Prozentsatz) für jeden Datensatz aus.

Nach der Zuordnung der Informationen für jede der Techniken füllt der Rechner für die Abdeckung durch Risikominderung das Feld Berechnete Technik Abdeckung durch Risikominderung automatisch aus. Um die Gesamtabdeckung der Risikominderung für eine Technik zu berechnen, müssen die Zuordnungsdatensätze für die Technikminderung aktiv und für die Organisation relevant sein. Die Datensätze, die inaktiv und nicht relevant sind, werden bei der Berechnung der gesamten Technikverringerungsabdeckung nicht berücksichtigt. Basierend auf den Werten in Berechnete Technik – Abdeckung durch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikominderung und in der Definition der Abdeckung durch Risikominderungwird Ihre allgemeine Technik – Abdeckung durch Risikominderung (berechnet) ausgefüllt.

Die Anpassungen, die Sie an den Abdeckungstypen, Farben oder Prozentsätzen vornehmen, werden in der Zuordnung der Abdeckung durch Risikominderung und in der Heatmapverwendet.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Zuordnung der Abdeckung durch Risikominderung**.
2. Überprüfen Sie die Zuordnungen von Technik zu Risikominderung, und aktualisieren Sie die **Abdeckung durch Risikominderung (Prozentsatz),** um die Verfügbarkeit der Abdeckung durch Ihre Organisation zu berechnen.

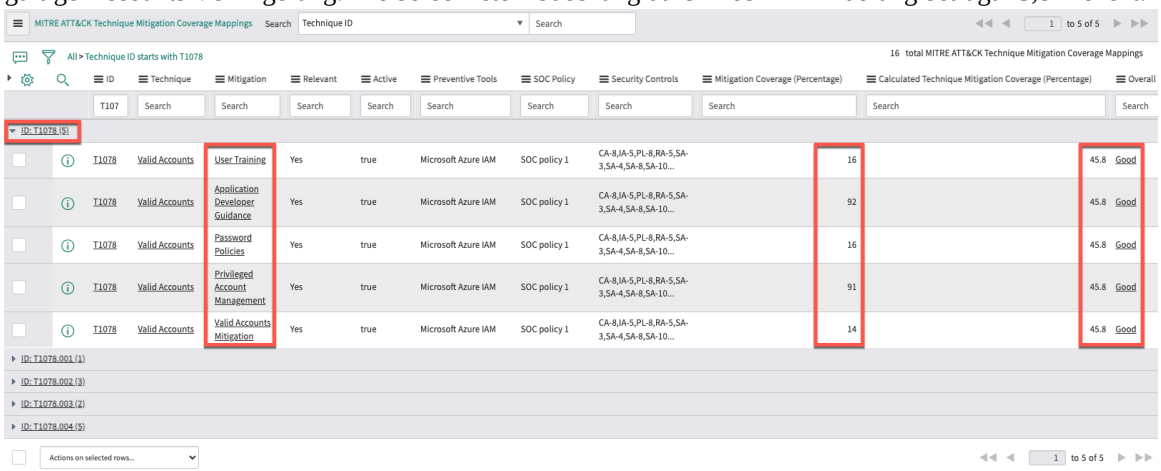
Technik – Zuordnungen der Abdeckung durch Risikominderung

Feld	Beschreibung
ID	Eindeutige Identität der Technik. Die IDs für alle Sammlungen und Techniken, die Sie aktiviert haben, werden automatisch ausgefüllt.
Technik	Wie ein Angreifer ein strategisches Ziel durch eine Aktion erreicht. Die Technikinformationen werden automatisch für alle Sammlungen und Techniken ausgefüllt, die Sie aktiviert haben.
Mitigation	Minderungen, mit denen Sie verhindern können, dass ein Angreifer Techniken oder Untertechniken erfolgreich gegen Ihre Organisation ausführt. Die Minderungsinformationen werden automatisch für alle Sammlungen und Techniken ausgefüllt, die Sie aktiviert haben.
Relevant	Option, um anzugeben, ob die Verringerung für Ihre Organisation relevant ist.
Aktiv	Option, um anzugeben, ob in Ihrer Organisation Minderungsstrategien bereitgestellt werden. Dies ist eine erforderliche Option, die zur Berechnung der Abdeckung durch Technikminderung erforderlich ist.
Tools zur Vorbeugung	Option, um anzugeben, ob Ihre Organisation über vorbeugende Tools verfügt, um die Techniken eines Angreifers abzuwehren.
SOC-Richtlinie	Die SOC-Richtlinien, die die Verringerungsstrategien in Ihrer Organisation definieren.
Sicherheitskontrollen	Die Sicherheitskontrollen Ihrer Organisation enthalten Risikominderungsstrategien zur Minimierung von Sicherheitsrisiken.
Abdeckung durch Risikominderung (Prozentsatz)	Ein Bewertungssystem zur Berechnung der Abdeckung der Technik durch Risikominderung. Definieren Sie numerische Werte zwischen 0 und 100. Dies ist eine erforderliche Option,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die zur Berechnung der Abdeckung durch Technikminderung erforderlich ist.
Berechnete Technik – Abdeckung durch Risikominderung (Prozentsatz)	Die berechnete Abdeckung der Technikminderung in Prozent. Dieser Wert wird basierend auf der Formel bestimmt, die im Rechner für die Abdeckung durch Risikominderungdefiniert ist.
Gesamtabdeckung Technikverringerung (berechnet)	Die allgemeine Abdeckung der Technik durch Risikominderung. Dieser Wert wird basierend auf der für Ihre Organisation definierten Abdeckung durch Risikominderungbestimmt.
Kommentar	Beschreibung der Zuordnung von Technik und Abdeckung durch Risikominderung.
Widerrufen	Die Zuordnung von Technik zu Abdeckung durch Risikominderung wird widerrufen.

In dieser Abbildung sehen Sie, dass der Technik Gültige Accounts fünf Minderungen zugeordnet sind, jeweils mit einer Minderungsabdeckung von 16 für Benutzerschulungen, 92 für Anleitungen für Anwendungsentwickler, 16 für Passwortrichtlinien, 91 für die Verwaltung privilegierter Accounts und 14 für gültige Accounts Verringerung. Die berechnete Abdeckung durch Technikminderung beträgt 45,8 Prozent.



Rechner für allgemeine Abdeckung der Technikminderung

Die Gesamtabdeckung der Technikverringerung wird basierend auf der Formel bestimmt, die im Rechner für die Abdeckung durch Risikominderung definiert ist.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

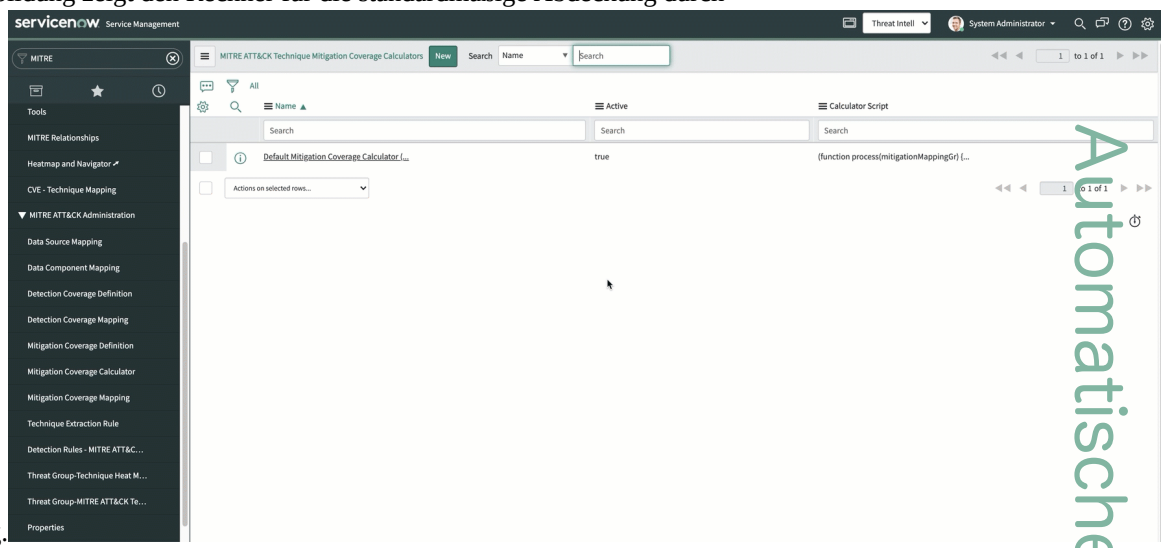
- Sie können nur einen Rechner für Verringerungsabdeckung pro Domäne als aktiv festlegen.
- Der Rechner für die Abdeckung des Basissystems für die Verringerung ist ein Durchschnittsrechner.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle Anpassungen am Rechnerskript sollten sicherstellen, dass die endgültige Ausgabe ein numerischer Wert zwischen 0 und 100 ist.
- Die Definition der Abdeckung durch Risikominderung wird basierend auf dem Bereich der endgültigen Ausgabe angewendet.

Prozedur

Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Rechner für Abdeckung durch Risikominderung**.
Die folgende Abbildung zeigt den Rechner für die standardmäßige Abdeckung durch Risikominderung.



Erkennungsregeln erstellen und zuordnen

Erstellen Sie Erkennungsregeln, und ordnen Sie sie den Taktiken und Techniken zu. Mit dieser Zuordnung können Sie die Abdeckung für die Erkennungsregeln in Ihrer Organisation anzeigen.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

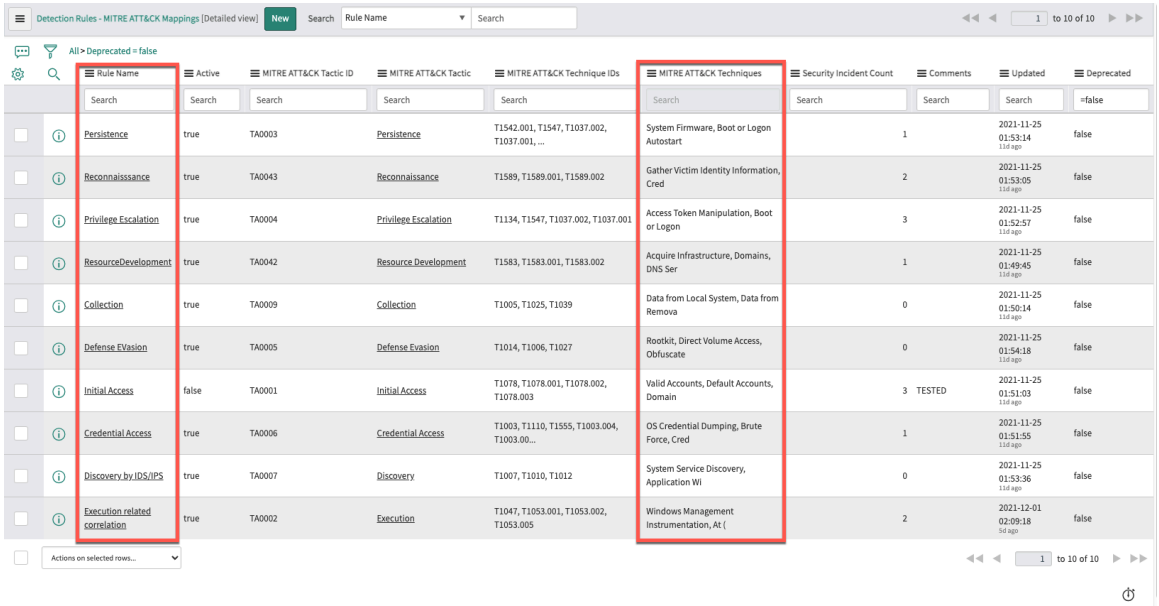
Mithilfe der Zuordnung von Erkennungsregeln kann Ihr Unternehmen sehen, welche Erkennungsregeln zur Identifizierung bestimmter Techniken verfügbar sind.

Der Hauptzweck der Zuordnung besteht darin, Transparenz zu schaffen, wenn Ihre Organisation über die erforderlichen Erkennungsregeln verfügt, um zu identifizieren, wenn eine Warnung oder ein Ereignis infolge eines Angriffs eines Angreifers mit einer bestimmten Technik ausgelöst wird.

Betrachten Sie beispielsweise die folgende Abbildung, die eine Liste der Erkennungsregeln zeigt, die verschiedenen Techniken zugeordnet sind. Sie können diese Informationen auch in anzeigen der/die/das MITRE-ATT&CK -Navigator.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie die automatischen SIEM-Extraktionsregeln des Basissystems nicht verwenden möchten, aktivieren Sie das automatische Rollup von MITRE-ATT&CK TTPs basierend auf der Erkennungsregelzuordnung. Sie können die Warnungs- oder Ereignisregel, die den Security Incident auslöst, im Feld Name der Warnungsregel ausfüllen. Sie können das Feld „Warnungsregelname " auch ausfüllen, indem Sie die SIEM-Integration, E-Mail-Analyse, manuelle Erstellung usw. verwenden. Weitere Informationen finden Sie unter Rollup der Informationen MITRE-ATT&CK aus Erkennungsregeln.

Hinweis:

Die Funktion „Erkennungsregeln" wurde aktualisiert und umfasst nun die Zuordnung einer einzelnen Taktik zu mehreren Techniken. Zuvor konnten Sie eine einzelne Taktik einer einzelnen Technik zuordnen. Wenn Sie das Plugin Threat Intelligence von Version 12.0.4 auf eine höhere Version aktualisieren, lesen Sie die folgenden Punkte, bevor Sie die Erkennungsregeln im Modul MITRE-ATT&CK verwenden.

- Sie finden mehrere Datensätze in einem einzigen Datensatz zusammengeführt, wenn die Felder Regelname, Warnungssensor, Quelle, Kategorie, Unterkategorie und Taktik MITRE-ATT&CK allgemein sind.
- Die alten Datensätze werden in der Spalte „veraltet" als „wahr" und in der Spalte „aktiv" als „falsch" markiert.
- Die neuen zusammengeführten Datensätze können verwendet werden und sind in der Spalte „veraltet" als falsch und in der Spalte aktiv als wahr markiert.
- Nachdem Sie das Upgrade verifiziert haben und feststellen, dass alle Ihre Erkennungsregeln erfolgreich migriert wurden, können Sie die alten Datensätze löschen, die in der Spalte veraltet als true markiert sind.

Prozedur

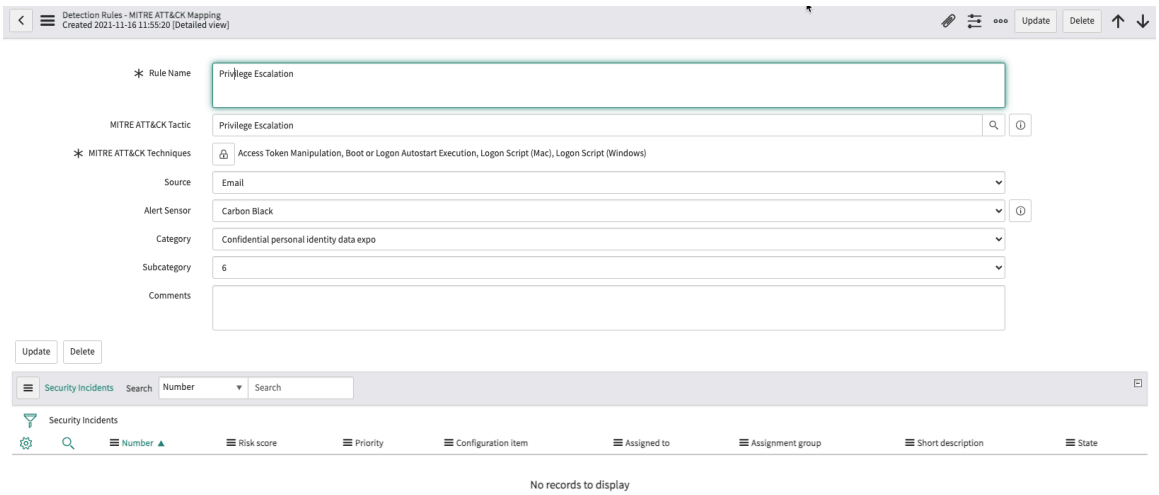
1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Erkennungsregeln – MITRE ATT&CK-Zuordnungen**.
2. Verwenden Sie eine der folgenden Methoden, um Ihre Erkennungsregel zu erstellen:
   Methode 1: Erstellen Sie manuell Erkennungsregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Neu** und füllen Sie im Formular die Felder aus.

Erkennungsregeln – Zuordnung MITRE-ATT&CK .

Feld	Beschreibung
Regelname	Name der Erkennungsregel.
MITRE-ATT&CK Taktik	Relevante MITRE-ATT&CK -Taktik.
MITRE-ATT&CK Techniken	Relevante MITRE-ATT&CK -Technik. Sie können mehrere Techniken für eine einzige Taktik auswählen.
Quelle	Quelle des Security Incidents, z. B. E-Mail, Firewall, Netzwerküberwachung usw.
Warnungssensor	Sicherheitsintegration, über die Sie Warnungs- oder Ereignisdaten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen.
Unterkategorie	Unterkategorie, die das Problem weiter definiert.
Kategorie	Kategorie, die den Typ des Sicherheitsproblems identifiziert.
MITRE-ATT&CK Technik	Relevante MITRE-ATT&CK -Technik. Sie können mehrere Techniken für eine einzige Taktik auswählen.
Anzahl der Security Incidents	Die Anzahl der Security Incidents, an die die Techniken angehängt sind. Diese Anzahl wird angezeigt, wenn Sie das automatische Rollup von Informationen über MITRE-ATT&CK aus Warnungsregeln für Security Incidents aktiviert haben.
Überholt	Die Erkennungsregelzuordnung ist veraltet.
Aktiv	Option, um anzugeben, ob die Erkennungsregel aktiv ist und in Ihrer Umgebung bereitgestellt wird.



b. Klicken Sie auf **Absenden**.

Methode 2: Erkennungsregeln importieren und erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

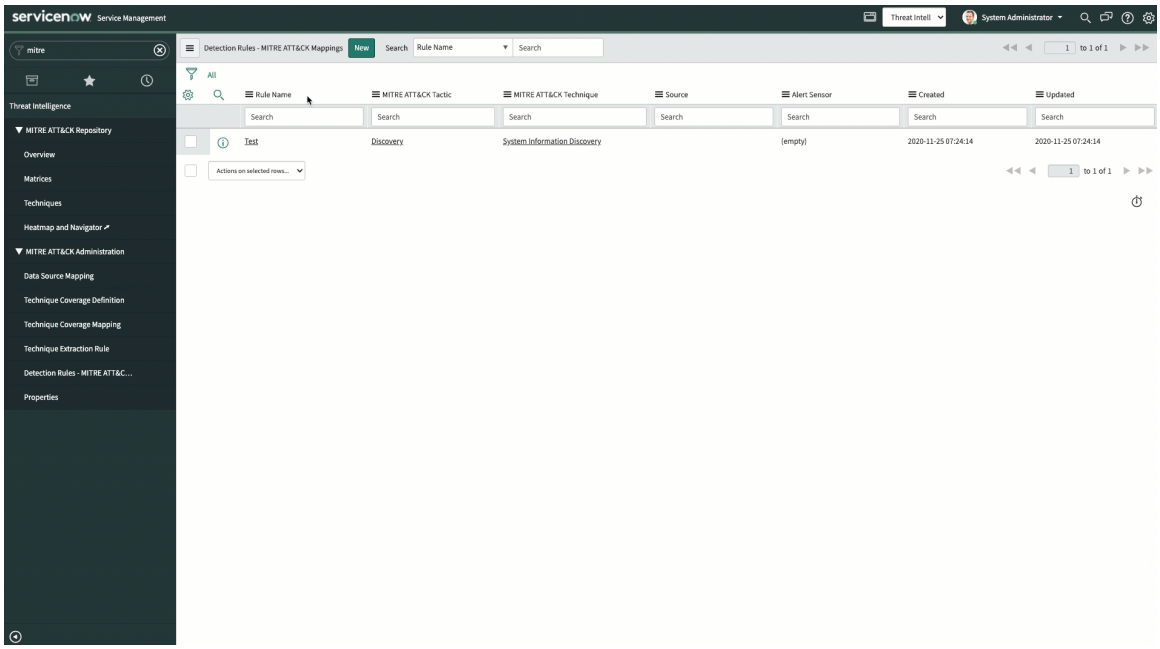
a. Klicken Sie mit der rechten Maustaste auf den Spaltenheader Regelname.

b. Klicken Sie in der Liste auf **Importieren**.

c. Klicken Sie auf **Excel-Vorlage erstellen**.

d. Klicken Sie nach Abschluss des Exports **auf Download**. Eine Excel-Vorlage mit dem Dateinamen sn_ti_alert_rules_mitre_attack_technique_mapping wird auf Ihren Computer heruntergeladen.

In der folgenden Abbildung sehen Sie, wie Sie die Excel-Vorlage exportieren, die Details in die Tabelle eintragen, die Datei hochladen, eine Vorschau der Felder anzeigen und sie dann wieder in Now Platformimportieren.



e. Öffnen Sie die Tabelle, wählen Sie die zweite Blattregisterkarte aus, und überprüfen Sie Ihre Eingaben. Füllen Sie die Felder des Formulars aus, und speichern Sie dann Ihre Datei.

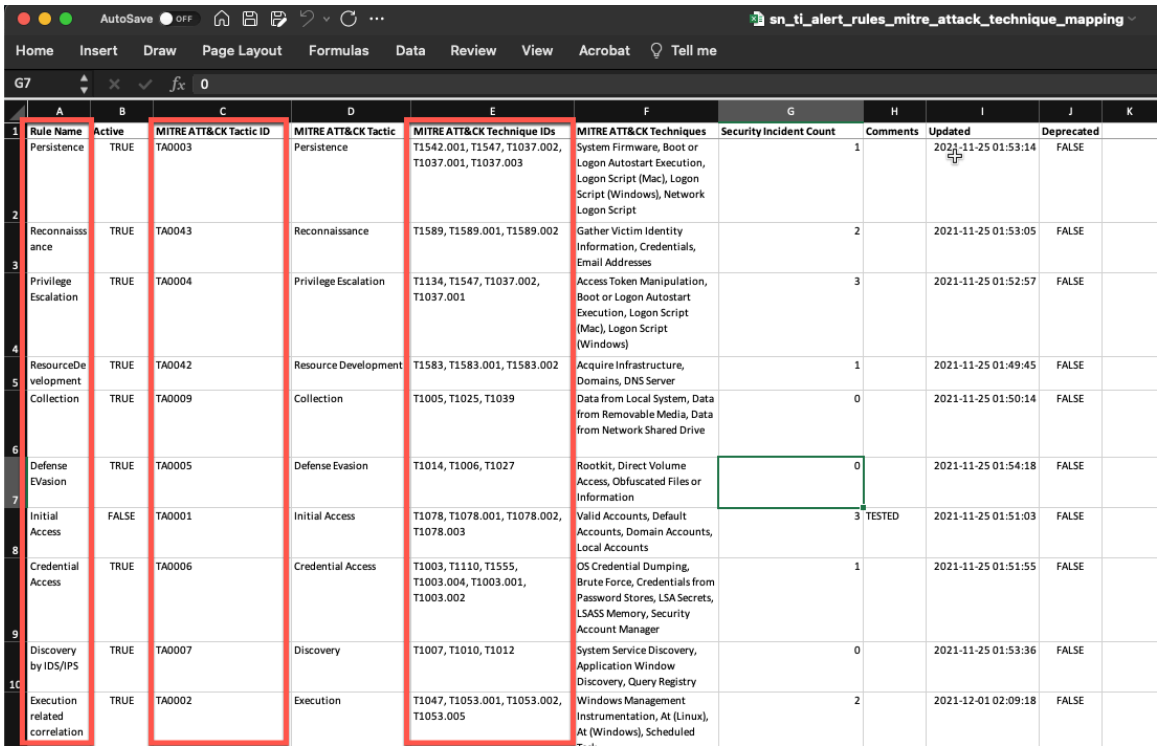
Vorlage importieren

Feld	Beschreibung
Regelname	Name der Erkennungsregel.
Aktiv	Option, um anzugeben, ob die Erkennungsregel aktiv ist und in Ihrer Umgebung bereitgestellt wird.
Warnungssensor	Sicherheitsintegration, über die Sie Warnungs- oder Ereignisdaten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen.
Kategorie	Kategorie, die den Typ des Sicherheitsproblems identifiziert.
Kommentare	Beschreibung der Erkennungsregel.
Überholt	Die Erkennungsregelzuordnung ist veraltet.
MITRE-ATT&CK Technik-IDs	MITRE-ATT&CK Technik-ID, z. B. T1546.008, für Barrierefreiheitsfunktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MITRE-ATT&CK Taktik-ID	MITRE-ATT&CK Taktik-ID, z. B. TA0003, für Persistenz.
Anzahl der Security Incidents	Die Anzahl der Security Incidents, an die die Techniken angehängt sind. Diese Anzahl wird angezeigt, wenn Sie das automatische Rollup von Informationen über MITRE-ATT&CK aus Warnungsregeln für Security Incidents aktiviert haben und die Erkennungsregel aktiv ist.
Quelle	Quelle des Security Incidents, z. B. E-Mail, Firewall, Netzwerküberwachung usw.
Unterkategorie	Unterkategorie, die das Problem weiter definiert.
MITRE-ATT&CK Taktik	Relevante MITRE-ATT&CK -Taktik.
MITRE-ATT&CK Technik	Relevante MITRE-ATT&CK -Technik.

Die folgende Abbildung zeigt die Tabellenvorlage. Die Pflichtfelder sind rot hervorgehoben: Regelname, MITRE-ATT&CK Taktik-ID und MITRE-ATT&CK Technik-ID.



Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated
Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE
Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE
Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE
ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE
Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE
Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE
Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE
Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE
Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE
Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE

f. Klicken Sie auf **Datei auswählen**, und wählen Sie die Tabelle auf Ihrem Computer aus.

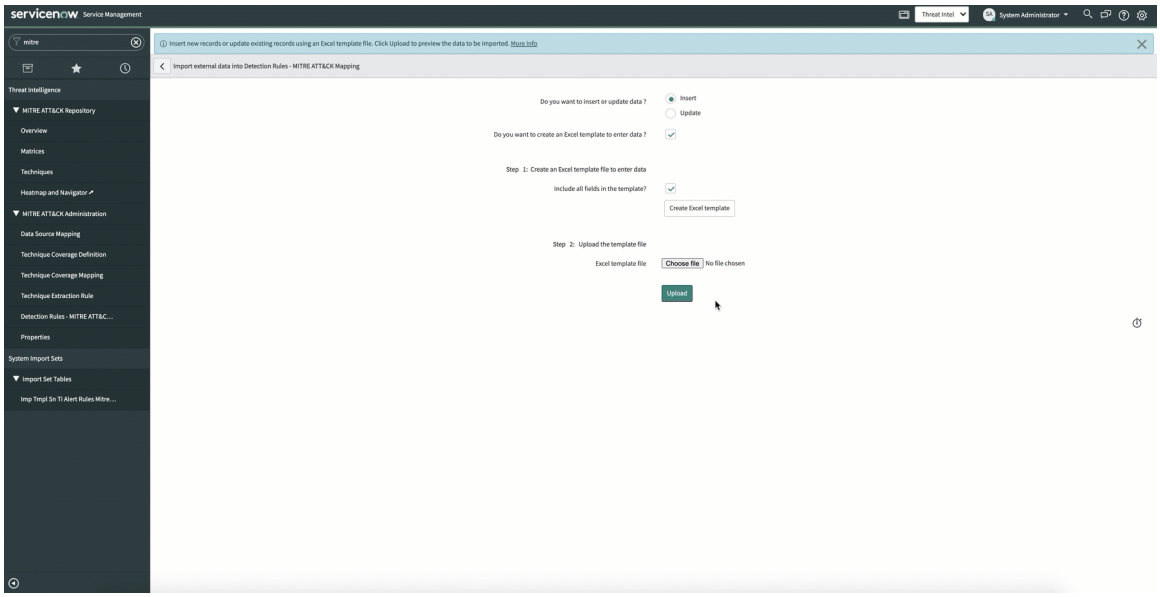
g. Klicken Sie auf **Hochladen**.

h. Klicken Sie **auf Vorschau der importierten Daten anzeigen**.

i. Zeigen Sie eine Vorschau der Zuordnungen an, und klicken Sie auf **Import abschließen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, wie Sie die Tabelle hochladen, eine Vorschau der Daten anzeigen, Fehler überprüfen und den Importvorgang für die Erkennungsregelzuordnung abschließen.



Extrahieren Sie automatisch Technikregeln für den Import von MITRE-ATT&CK -Informationen

Verwenden Sie die automatischen Extraktionsregeln des Basissystems, um die Informationen MITRE-ATT&CK aus vorhandenen Drittanbieterintegrationen zu importieren.

Verwenden Sie die automatischen Extraktionsregeln für die Bedrohungssuche

Verwenden Sie die automatischen Extraktionsregeln für die Bedrohungssuche, um die MITRE-ATT&CK -Informationen aus vorhandenen Threat Intelligence -Drittparteiintegrationen zu importieren.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Threat Intelligence -Integration (z. B. Sandbox oder TIP) das Framework MITRE-ATT&CK unterstützt und die Informationen für MITRE-ATT&CK auf jeder Integrationsebene analysiert werden, werden die Informationen in jedem Ergebnisdatensatz der Bedrohungssuche angezeigt. Allerdings analysieren nicht alle Threat Intelligence -Integrationen die MITRE-ATT&CK -Informationen. Die globale automatische Extraktionsregel für die Bedrohungssuche kann MITRE-ATT&CK Informationen aus allen Threat Intelligence Integrationen extrahieren.

Sie können festlegen, dass die Informationen MITRE-ATT&CK automatisch aus den Ergebnissen der Bedrohungssuche zu einem Security Incident zusammengefasst werden. Für ein automatisches Rollup der Ergebnisse der Bedrohungssuche in Security Incidents aktivieren Sie die Systemeigenschaft. Alternativ können Sie die Informationen für jede einzelne Bedrohungssuche manuell zusammenfassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Basissystem Threat Intelligence extrahiert automatisch die Informationen MITRE-ATT&CK aus der Rohnutzlast der Drittanbieterintegrationen für den Ergebnisdatensatz der Bedrohungssuche, wenn die Integration Threat Intelligence Ihnen Informationen zu MITRE-ATT&CK wie die Technik oder Taktik bereitstellt.

Wenn die Informationen MITRE-ATT&CK im Feld „Rohnutzlast“ des Bedrohungssuchdatensatzes nicht verfügbar sind, müssen Sie eine eigene Regel für die automatische Extraktion aus der Drittanbieterintegration definieren.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Extraktionsregel für Technik**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Technik-Extraktionsregel“.

Feld	Beschreibung
Name	Name der Regel für automatische Extraktion.
Regeltyp	Regeltyp für automatische Extraktion. Wählen Sie **Bedrohungssuche**aus.
Automatische Extraktion ignorieren	Einstellung, dass standardmäßig deaktiviert ist. Diese Einstellung ermöglicht die automatische Extraktion von MITRE-ATT&CK -Techniken.
Quell-Engine	Quell-Engine.
Global	Einstellung der Quell-Engine. Wenn Sie die Quell-Engine auf **Global**festlegen, wird die Extraktion für alle Ergebnisse der Integration der Bedrohungssuche ausgeführt.
Beschreibung	Beschreibung der Regel für automatische Extraktion.
Prozessmethode	Regulärer Ausdruck oder eine Skriptmethode, die Sie angeben, um die Technikinformationen aus der Rohnutzlast zu verknüpfen.
Extraktion des regulären Ausdrucks	Option, die Sie für das **Zielfeld** angeben, wenn Sie die Extraktionsmethode für reguläre Ausdrücke verwenden. Regulärer Ausdruck ist der Standardwert.
Skriptextraktion	Prozess, den Sie beim Ausführen eines Skripts auswählen Das Skript überprüft Folgendes: ○ ThreatLookupResultSysId: sys_id des Ergebnisdatensatzes der Bedrohungssuche ○ sourceName: Name der Quelle für die Bedrohungssuche.
Taktikextraktion	Option, die Sie angeben, um taktikbezogene Informationen aus der Rohnutzlast zu extrahieren. Wenn eine Nutzlast bestimmte Informationen im Zusammenhang mit Taktiken und Techniken enthält,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	können Sie diese Informationen extrahieren und an den Security Incident anhängen.

4. Klicken Sie auf **Absenden**.

Verwenden Sie SIEM-Regeln für automatische Extraktion

Verwenden Sie die SIEM-Regeln für automatische Extraktion, um die Informationen MITRE-ATT&CK aus vorhandenen Security Operations SIEM-Drittparteiintegrationen zu importieren.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Die Technikextraktionsregel ist für alle SIEM-Integrationen des Basissystems Security Operations verfügbar, z. B. Splunk-, IBM QRadar- und ArcSight-Integrationen. Wenn Now Platform Warnungs- oder Ereignisdaten aus diesen SIEM-Integrationen erfasst und diese Informationen MITRE-ATT&CK enthalten, verarbeitet Now Platform die Rohnutzlast und extrahiert die Informationen MITRE-ATT&CK automatisch.

Wenn Ihr Now Platform SIEM-Integrationen für das Basissystem enthält, bedeutet dies, dass die Regeln zur Technikextraktion bereits im Modul MITRE-ATT&CK erstellt wurden. Sie sollten die Regeln nach Bedarf überprüfen und ändern.

Aktivieren Sie jeweils entweder die automatische SIEM-Extraktionsregel oder die Warnungsregel.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Extraktionsregel für Technik**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

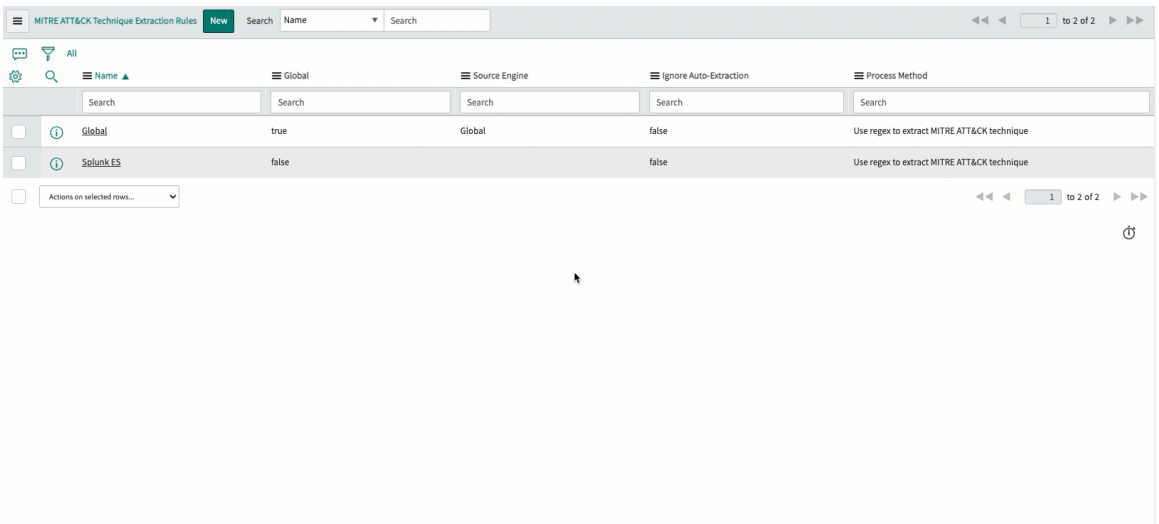
Formular „Technik-Extraktionsregel“.

Feld	Beschreibung
Name	Name der Regel für automatische Extraktion.
Regeltyp	Regeltyp für automatische Extraktion. Wählen Sie **SIEM**aus.
Automatische Extraktion ignorieren	Einstellung, die standardmäßig deaktiviert ist. Diese Einstellung ermöglicht die automatische Extraktion von MITRE-ATT&CK -Techniken.
Tabelle importieren	Importtabelle, die für SIEM-Integrationen des Basissystems automatisch zugeordnet wird. Überprüfen Sie dieses Feld für andere SIEM-Integrationen für die Informationen MITRE-ATT&CK, und ordnen Sie sie entsprechend zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Feld importieren	Importfeld, das für SIEM-Integrationen des Basissystems automatisch zugeordnet wird. Überprüfen Sie dieses Feld für andere SIEM-Integrationen für die Informationen MITRE-ATT&CK, und ordnen Sie sie entsprechend zu.
Beschreibung	Regel für automatische Extraktion.
Prozessmethode	Regulärer Ausdruck oder eine Skriptmethode, die Sie angeben, um die Technikinformationen aus der Rohnutzlast zu verknüpfen.
Extraktion des regulären Ausdrucks	Option, die Sie für das **Zielfeld** angeben, wenn Sie die Methode des regulären Ausdrucks verwenden. Die Extraktion des regulären Ausdrucks ist die Standardprozessmethode.
Skriptextraktion	Skriptprozessmethode, die Sie verwenden, wenn Sie anpassen möchten, wie die Informationen MITRE-ATT&CK extrahiert werden.
Taktikextraktion	Option, die Sie angeben, um taktikbezogene Informationen aus der Rohnutzlast zu extrahieren. Wenn eine Nutzlast bestimmte Informationen im Zusammenhang mit Taktiken und Techniken enthält, können Sie diese Informationen extrahieren und an den Security Incident anhängen.

In der folgenden Abbildung sehen Sie ein Beispiel für die Extraktionsregel für SIEM-Technik Splunk Enterprise in der Formularansicht. Diese Regel ähnelt allen anderen Extraktionsregeln für SIEM-Techniken.



4. Klicken Sie auf **Absenden**.

Überprüfen Sie die Zuordnung der Bedrohungsgruppe und der Techniken MITRE-ATT&CK .

Überprüfen Sie die Zuordnungsinformationen für Objekt-zu-Objekt-Beziehungen der Bedrohungsgruppe und der Techniken, die aus den MITRE TAXII -Sammlungen importiert wurden. Mit dieser Zuordnung können Sie die Technikgruppe und die entsprechende Technikzuordnung anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

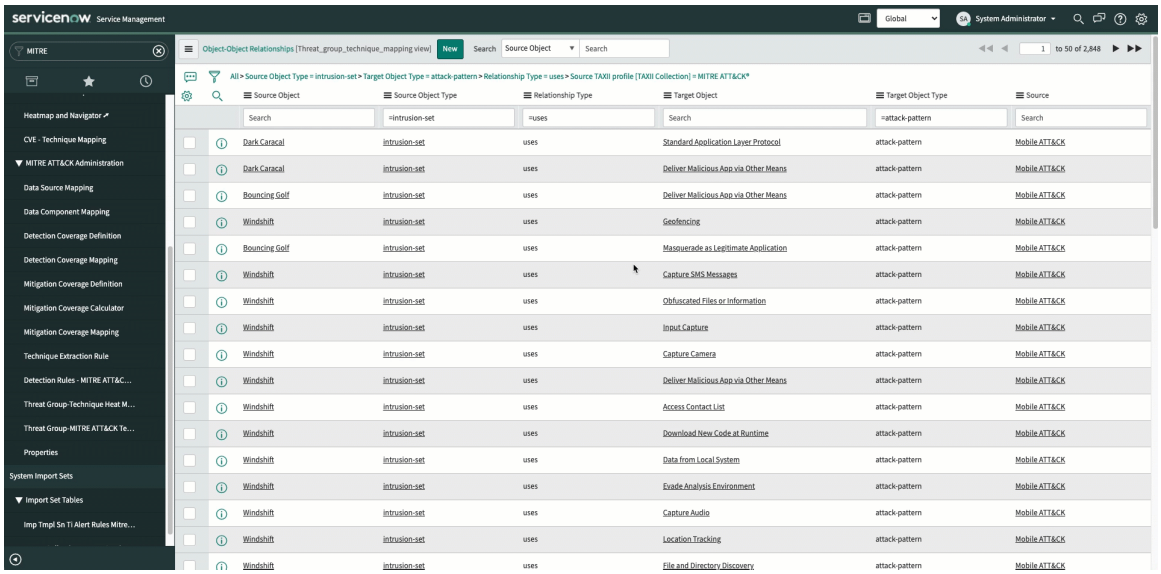
Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Erstellungs-, Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Bedrohungsgruppe – MITRE ATT&CK-Techniken**.
2. Klicken Sie mit der rechten Maustaste auf das **Quellobjekt**, und wählen Sie **„Nach Quellobjekt gruppieren“,** um alle Angriffsmuster anzuzeigen, die einer Bedrohungsgruppe zugeordnet sind.

   Die folgende Abbildung zeigt die Bedrohungsgruppe „admin@338“ und die verschiedenen Angriffsmuster, die von dieser Bedrohungsgruppe übernommen werden und Teil der Enterprise-Angriffsquelle sind.



Definition von Bedrohungsgruppe zu Technik-Heatmap

Definieren Sie die Definition der Bedrohungsgruppe für die Technik-Heatmap, damit Sie in der Heatmap die Angriffsmuster messen und erkennen können, die von Bedrohungsgruppen für Angriffe auf Ihre Organisation verwendet werden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik erhöht sich, wenn die Anzahl der Angreifer hoch ist.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreibzugriff
- sn_ti.read: Lesezugriff

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Bedrohungsgruppentechnik-Heatmap**.
2. Überprüfen Sie die Definition der Heatmap für die Bedrohungsgruppe für die Technik, und passen Sie die Einträge für Ihre Umgebung an.

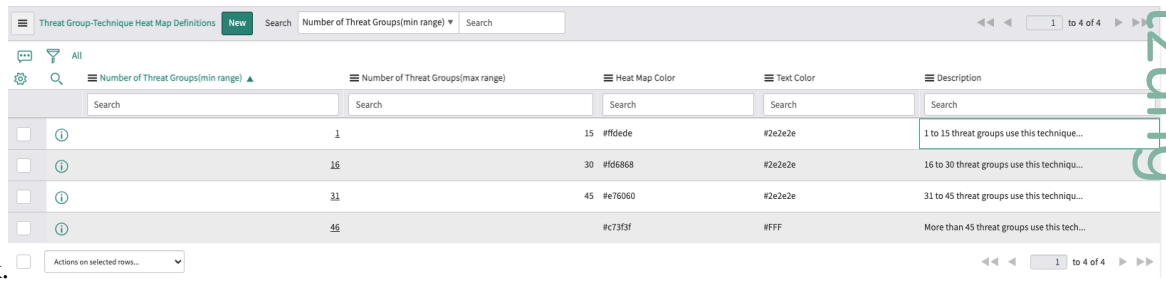
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definitionen der Bedrohungsgruppentechnik-Heatmap

Feld	Beschreibung
Anzahl der Bedrohungsgruppen (Mindestbereich)	Die Mindestanzahl der Bedrohungsgruppen, die eine bestimmte Technik verwenden.
Anzahl der Bedrohungsgruppen (maximaler Bereich)	Die maximale Anzahl von Bedrohungsgruppen, die eine bestimmte Technik verwenden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik erhöht sich, wenn die Anzahl der Angreifer hoch ist.
Heatmap-Farbe	Farbe, die der Bedrohungsgruppenkategorie zugewiesen ist. Die von Ihnen definierte Farbe wird verwendet, um die Bedrohungsgruppenkategorie in der Heatmap hervorzuheben. Sie können die Farben mit HEX-Codes und RGB(A)-Werten anpassen.
Textfarbe	Farbe, die dem Bedrohungsgruppentext zugewiesen ist. Die von Ihnen definierte Farbe wird verwendet, um die Bedrohungsgruppen in der Heatmap hervorzuheben. Sie können die Farben mit HEX-Codes und RGB(A)-Werten anpassen.
Beschreibung	Beschreibung des Bedrohungsgruppenbereichs und der Definition.

Hinweis:
Achten Sie darauf, dass Sie die Anzahlbereiche für Bedrohungsgruppen nicht überlappen, wenn Sie den Bedrohungsgruppenbereich (Min. oder Max.) anpassen.

Die folgende Abbildung zeigt die Definitionsliste für die Heatmap-Definitionen für die Bedrohungsgruppe für die



Technik.

3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, füllen Sie die Einträge aus, und klicken Sie auf **Absenden**.

Überprüfen Sie die Systemeigenschaften für MITRE-ATT&CK .

Überprüfen Sie die Werte der Systemeigenschaft MITRE-ATT&CK.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin, sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Eigenschaften**.
2. Füllen Sie die Felder des Formulars aus.

MITRE-ATT&CK Formular „Eigenschaften“.

Feld	Beschreibung
Führt ein automatisches Rollup von MITRE ATT&CK-Informationen von erkennbaren Elementen zu Security Incidents durch [sn_ti.rollup_mitre_att&ck_technique_observable_si]	Rollup von MITRE-ATT&CK Informationen von erkennbaren Elementen bis zum Security Incident. Weitere Informationen hierzu finden Sie unter MITRE ATT&CK-Informationen erkennbaren Elementen zuordnen. Standardwert: Ja
Führt ein automatisches Rollup von MITRE ATT&CK-Informationen aus den Ergebnissen der Bedrohungssuche zum Security Incident durch [sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si]	Rollup von MITRE-ATT&CK Informationen aus Ergebnissen der Bedrohungssuche für den Security Incident. Weitere Informationen finden Sie unter Automatische Extraktion der Bedrohungssuche. Standardwert: Ja
Führt einen automatischen Rollup von MITRE ATT&CK-Informationen aus Warnungsregeln zu Security Incidents durch [sn_ti.rollup_mitre_att&ck_technique_alert_rule_si]	Führt einen automatischen Rollup von MITRE-ATT&CK TTP-Informationen aus Warnungsregeln zu Security Incidents durch. Weitere Informationen finden Sie unter Erkennungsregeln zuordnen. Standardwert: Nein
Führt ein automatisches Rollup von MITRE ATT&CK-Informationen von untergeordneten Security Incidents zu übergeordneten Security Incidents durch [sn_ti.rollup_mitre_att&ck_technique_child_si_sta]	Führt ein automatisches Rollup von MITRE-ATT&CK -Informationen aus untergeordneten Security Incidents zu übergeordneten Security Incidents durch. Standardwert: Ja
Durch Aktivieren dieser Eigenschaft können Sie Security Incident-Felder wie Kategorie und Unterkategorie zu Erkennungsregeln in der Tabelle „Erkennungsregeln – MITRE ATT&CK-Zuordnung“ zuordnen [sn_ti.enable_category_mapping_with_alert_rule]	Kategorie und Unterkategorie auf der Zuordnungsseite „Erkennungsregeln – MITRE ATT&CK“. Standardwert: Nein
Zeit (in Stunden) zur Berechnung von „CVE – VUL-Anzahl“ [sn_ti.time_to_calculate_cve_vits_count]	Die geplante Zeit in Stunden zur Berechnung der CVE- und VUL-Informationen. Standardwert: 24

3. Klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE-ATT&CK zum Erkennen und Analysieren von Bedrohungen verwenden

Verwenden Sie das -Framework MITRE-ATT&CK im gesamten -Modul Threat Intelligence und SIR, um Bedrohungen für Ihre Organisation zu erkennen und zu analysieren.

Ordnen Sie Informationen MITRE-ATT&CK™ Security Incidents zu

Ordnen Sie die Taktiken und Techniken MITRE-ATT&CK dem -Security Incident zu, um die Analyse von Security Incidents und Bedrohungen zu verbessern.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie dem Security Incident die Informationen zu den Taktiken und Techniken MITRE-ATT&CK hinzu, damit Sie Ihre Security Incident- und Bedrohungsinformationen für eine bessere Analyse korrelieren können. Beispielsweise kann Ihre Organisation Informationen im Zusammenhang mit Taktiken, Techniken und Verfahren (TTP) von Ihren Drittparteiquellen erhalten, z. B. von Threat Intelligence -Mitarbeitern oder anderen Quellen außerhalb von Security Incident Response. Anschließend fügen Sie diese Informationen wieder SIR hinzu, um die Korrelation und Bedrohungsanalyse zu verbessern.

Sie können die Informationen MITRE-ATT&CK automatisch aus den Ergebnissen der automatischen Extraktion der Bedrohungssuche, aus erkennbaren Elementen oder aus einem untergeordneten Security Incident zu einem Security Incident zusammenfassen. Aktivieren Sie für das automatische Rollup von Security Incidents die Systemeigenschaft. Alternativ können Sie die Informationen für jede einzelne Bedrohungssuche und jedes erkennbare Elementmanuell zusammenfassen.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie auf den **zugehörigen Link MITRE ATT&CK-Technik** zuordnen.
   Der Bereich MITRE ATT&CK-Technik zuordnen wird angezeigt.

   Diese Abbildung zeigt, wie Sie zur zugehörigen Liste navigieren und nach Technik zum Zuordnen MITRE-ATT&CK suchen, die Enterprise ATT&CK-Enterprise-Quelle überprüfen, eine Taktikauswirkung hinzufügen und eine Technik „System herunterfahren/neu starten“ hinzufügen.

   MITRE-Informationen dem Security Incident zuordnen
4. Wählen Sie **Quelle**aus.

   Hinweis:
   In der Quellenliste werden nur die Sammlungen und Matrizen angezeigt, die aktiviert wurden.

   Die Taktiken und Techniken, die der Quelle zugeordnet sind, können ausgewählt werden. Sie können auch mehrere Quellen zuordnen.
5. Wählen Sie **Taktik** und **Technik**aus.
6. **Wahlweise:** Überprüfen Sie die Informationen basierend auf der Relevanz für den Security Incident, und gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Zuordnung vollständig zu entfernen, klicken Sie auf das Papierkorbsymbol. Durch Klicken auf dieses Symbol werden die Quelle und die zugehörigen Taktiken und Techniken gelöscht.
- Um eine Taktik zu entfernen, klicken Sie auf das Minus-Symbol neben der Taktik.
- Um eine Technik zu entfernen, klicken Sie auf das x-Symbol neben der Technik.

7. Klicken Sie auf **Speichern**.

Ergebnisse

Die Informationen MITRE-ATT&CK sind dem Security Incident zugeordnet. Sie können jetzt die zugehörigen Informationen auf der **MITRE ATT&CK-Karte**anzeigen.

Ordnen Sie Informationen MITRE-ATT&CK geschlossenen Security Incidents zu

Sie können jetzt den geschlossenen Security Incidents die Taktiken und Techniken MITRE-ATT&CK zuordnen, um Security Incidents und Bedrohungen besser analysieren zu können.

MITRE-Informationen dem Security Incident zuordnen

Verwenden der Karte MITRE-ATT&CK, um zugehörige Informationen in einem Security Incident anzuzeigen

Sie können die Karte MITRE-ATT&CK verwenden, um die MITRE-ATT&CK -bezogenen Informationen in einem Security Incident anzuzeigen.

Nachdem für die Informationen ein Rollup aus einer Bedrohungssuche, einem erkennbaren Element oder einer SIEM-Integration durchgeführt wurde, werden sie dem Security Incident hinzugefügt. Anschließend werden die zusammengefassten Informationen auf der Karte MITRE-ATT&CK angezeigt. Die **MITRE ATT&CK-Karte** bietet zwei Ansichten:

- Navigatoransicht: Diese Ansicht, die dem Navigator MITRE-ATT&CK ähnelt, zeigt alle Techniken, die manuell hinzugefügt oder aus den Tabellen für erkennbare Elemente oder Bedrohungssuchen zusammengefasst wurden. **„Ursprung der Techniken anzeigen“** zeigt die Quelle der Technik an, wenn sie manuell oder über eine Quelle aufgerollt wurde. **„ID anzeigen“** zeigt die ID der Technik an.

  Die folgende Abbildung zeigt, wie Sie zur Ansicht **MITRE ATT&CK Card** Navigator navigieren. Durch Klicken auf einen der verfügbaren Links werden die Informationen im Modul Threat Intelligence geöffnet.

  MITRE ATT&CK-Karte: Navigatoransicht und Listenansicht

- Listenansicht: Diese Ansicht zeigt die Daten im Listen- oder Tabellenformat. In dieser Ansicht können Sie alle Daten anzeigen, die auf verschiedene Tabellen und Gruppen verteilt sind.

  Die folgende Abbildung zeigt, wie Sie zur MITRE ATT&CK-Kartenlistenansicht navigieren. Durch Klicken auf einen der verfügbaren Links werden die Informationen im Modul Threat Intelligence geöffnet.

Ordnen Sie Informationen MITRE-ATT&CK erkennbaren Elementen zu

Ordnen Sie MITRE-ATT&CK -Taktiken und -Techniken einem erkennbaren Element zu, um Security Incidents und Bedrohungsanalysen auf granularer Ebene zu verbessern.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

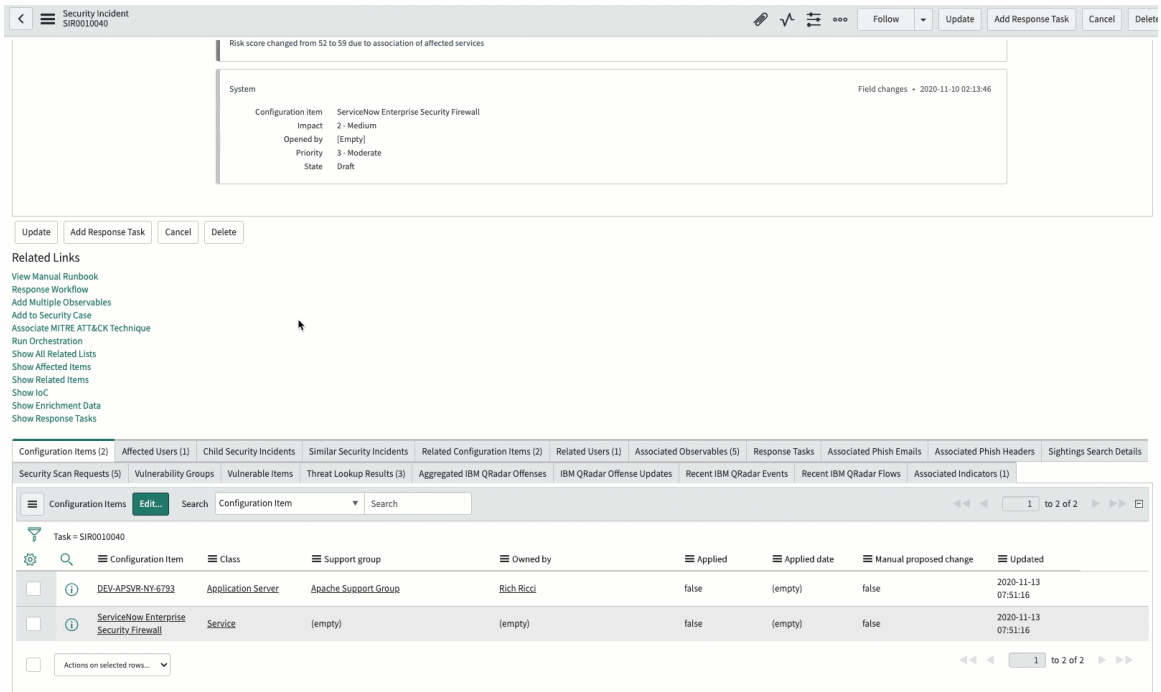
Einige SIEMs können Informationen MITRE-ATT&CK mit Ereignissen, Warnungen oder erkennbaren Elementen bereitstellen. Um die MITRE-ATT&CK -Informationen auf granularer Ebene zuzuordnen, können Sie die Informationen mit einem erkennbaren Element hinzufügen.

Sie können ein Rollup der Informationen MITRE-ATT&CK automatisch von den erkennbaren Elementen zu einem Security Incident durchführen. Aktivieren Sie für das automatische Rollup von erkennbaren Elementen zu Security Incidents die Systemeigenschaft. Alternativ können Sie die Informationen für jedes erkennbare Element manuell zusammenfassen.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete erkennbare Elemente**.
4. Zeigen Sie auf das erkennbare Element, das Sie zuordnen möchten, klicken Sie mit der rechten Maustaste, und wählen Sie **MITRE ATT&CK-Technik zuordnen**aus.

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu **MITRE ATT&CK-Technik**zuordnen navigieren, die Quelle überprüfen und eine Taktik und Technik hinzufügen.



5. Überprüfen Sie in den Quellenlisten die **Quelle**.

   Hinweis:
   In der Quellenliste werden nur die Sammlungen und Matrizen angezeigt, die aktiviert wurden.

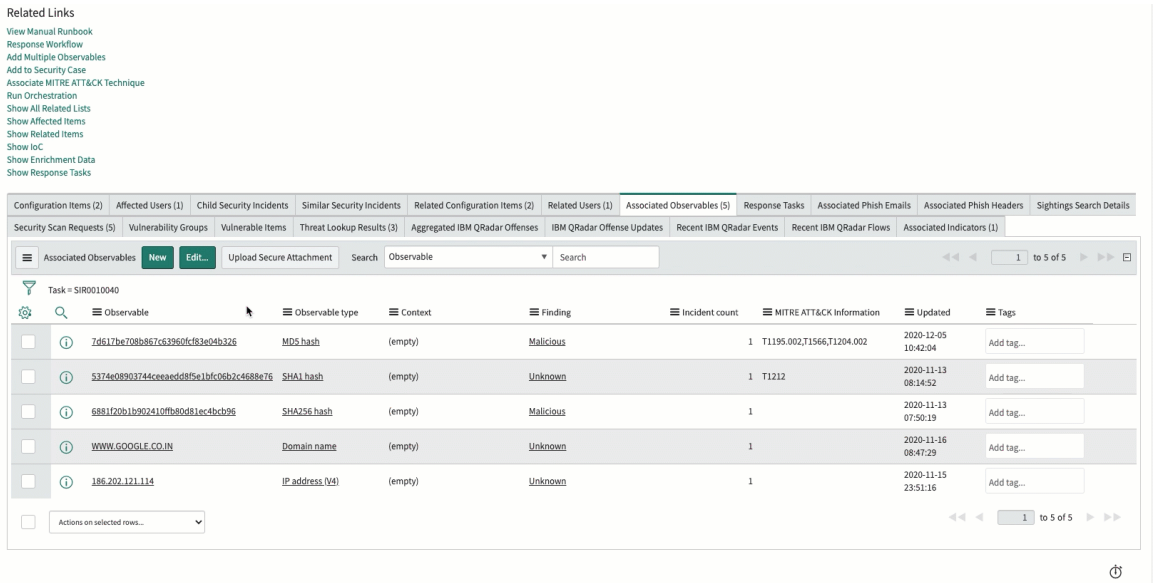
6. Überprüfen Sie die **Taktik** und **die Techniken**, und fügen Sie sie basierend auf der Relevanz für das erkennbare Element hinzu, oder entfernen Sie sie.
7. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die von Ihnen hinzugefügten Taktiken und Techniken werden in der Spalte MITRE-ATT&CK „Informationen“ in der zugehörigen Liste der erkennbaren Elemente angezeigt.

8. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü „Aktionen **“ auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Wenn Sie aktiviert haben automatisches Rollup von MITRE-ATT&CK Informationen von erkennbaren Elementen bis hin zu Security Incidents, werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben,müssen Sie dies manuell durchführen.

   Die folgende Abbildung zeigt, wie Sie ein erkennbares Element auswählen und die Informationen MITRE-ATT&CK zu einem Security Incident zusammenfassen.



9. Um eine zusammengefasste Ansicht der Techniken anzuzeigen, die den erkennbaren Elementen zugeordnet sind, wählen Sie zwei oder mehr erkennbare Elemente aus der Liste aus, und klicken Sie dann im Menü „ **Aktionen“** in der Liste der ausgewählten Zeilen **auf MITRE ATT&CK-Informationen anzeigen**.

Ergebnisse

Eine zusammengefasste Ansicht der MITRE ATT&CK-Informationen für die ausgewählten erkennbaren Elemente wird angezeigt.

Ordnen Sie die Informationen MITRE-ATT&CK dem Sicherheitsfall zu

Ordnen Sie MITRE-ATT&CK Taktiken und Techniken einem Sicherheitsfall zu, um das Management von Sicherheitsfällen und die Bedrohungsanalyse auf granularer Ebene zu verbessern.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

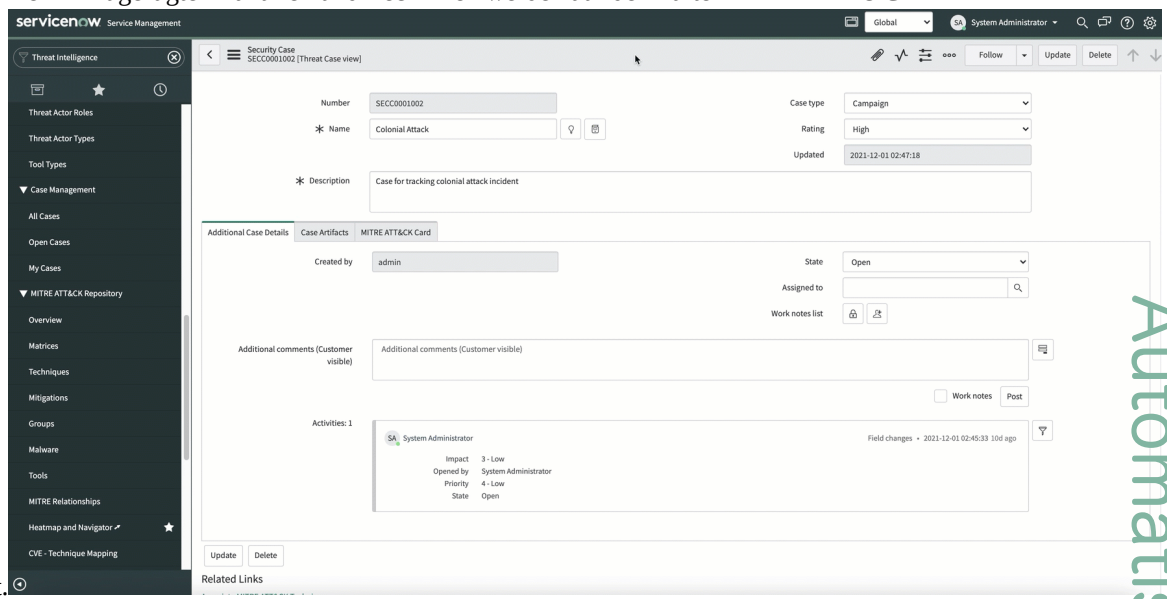
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**.
2. Wählen Sie den Sicherheitsfall aus, den Sie mit den MITRE-ATT&CK-Informationen anreichern möchten.
3. Klicken Sie in der zugehörigen Liste **auf MITRE ATT&CK-Technik zuordnen**.

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu **MITRE ATT&CK-Technik**zuordnen navigieren, die Quelle überprüfen und eine Taktik und Technik hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Überprüfen Sie in den Quellenlisten die **Quelle**.
5. Überprüfen Sie die **Taktik** und **die Techniken**, und fügen Sie sie basierend auf der Relevanz für den Fall hinzu, oder entfernen Sie sie.
6. Klicken Sie auf **Speichern**.
   Die von Ihnen hinzugefügten Taktiken und Techniken werden auf der Karte MITRE-ATT&CK angezeigt.



Rollup der Informationen MITRE-ATT&CK anhand der Ergebnisse der Bedrohungssuche

Wenn Sie das automatische Rollup von Informationen MITRE-ATT&CK nicht aktiviert haben, können Sie dies manuell durchführen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

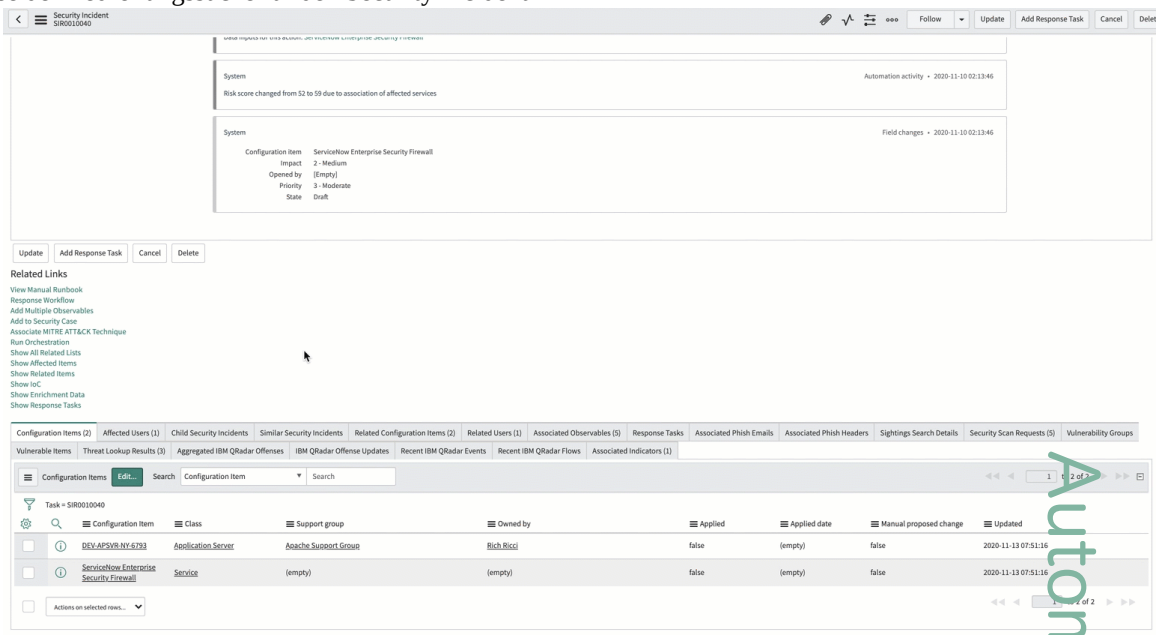
Wenn Sie aktiviert haben automatisches Rollup von MITRE-ATT&CK Informationen aus Ergebnissen der Bedrohungssuche zu Security Incident werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie dies manuell tun.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Ergebnisse der Bedrohungssuche**.
4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü „Aktionen **“ auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Sie können mehrere erkennbare Elemente auswählen und die Informationen zusammenfassen.
5. Klicken Sie auf **Neu laden**, um die Änderungen zu bestätigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, wie Sie ein erkennbares Element auswählen und die Ergebnisse der Bedrohungssuche für den Security Incident



zusammenfassen.
Sie können die Karte MITRE-ATT&CK anzeigen, um zu bestätigen, dass für die Ergebnisse der Bedrohungssuche ein Rollup für den Security Incident durchgeführt wurde.

Rollup der Informationen MITRE-ATT&CK aus Erkennungsregeln

Aktivieren Sie das Rollup von MITRE-ATT&CK -Informationen aus den Erkennungsregeln für Security Incidents, um Security Incidents und Bedrohungen besser analysieren zu können.

Vorbereitungen

Erforderliche Rolle: keine

Vergewissern Sie sich, dass Sie Folgendes durchgeführt haben:

- Aktivieren Sie die Eigenschaft Rollup MITRE ATT&ack-Informationen automatisch von Warnungsregeln zu Security Incidents durchführen im Modul Eigenschaften. Standardmäßig ist diese Option deaktiviert. Weitere Informationen finden Sie unter MITRE-ATT&CK-Systemeigenschaften überprüfen.
- Führen Sie die Zuordnung von Erkennungsregeln zu MITRE-ATT&CK TTPs im Modul Erkennungsregeln – MITRE ATT&CK-TTP-Zuordnung durch. Der Name der Erkennungsregel muss mit dem Namen der Warnungsregel übereinstimmen, die den Security Incident auslöst. Weitere Informationen finden Sie unter Erkennungsregeln erstellen und zuordnen.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die automatischen SIEM-Extraktionsregeln des Basissystems nicht verwenden möchten, aktivieren Sie das automatische Rollup von MITRE-ATT&CK TTPs basierend auf der Erkennungsregelzuordnung. Sie können die Warnungs- oder Ereignisregel, die den Security Incident auslöst, im Feld Name der Warnungsregel ausfüllen. Sie können das Feld „Warnungsregelname “ auch ausfüllen, indem Sie die SIEM-Integration, E-Mail-Analyse, manuelle Erstellung usw. verwenden.

Automatische Übersetzung

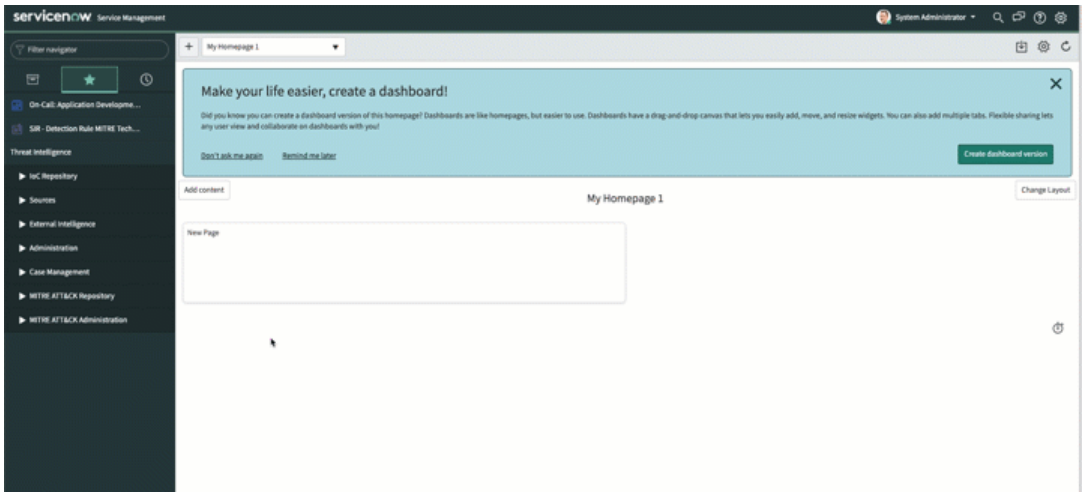
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **MITRE ATT&CK-Administration** > **Eigenschaften**.
2. Aktivieren Sie die Eigenschaft Rollup MITRE ATT&ack-Informationen automatisch von Warnungsregeln zu Security Incidents durchführen, und klicken Sie auf **Speichern**.
   Standardmäßig ist diese Option deaktiviert.
3. Sie müssen das Feld Name der **Warnungsregel** des Security Incident mit den erforderlichen Warnungsregeln ausfüllen.

   Hinweis:
   Stellen Sie sicher, dass Sie den genauen Namen der Warnungsregel hinzufügen. Um mehrere Regeln hinzuzufügen, müssen Sie die Regeln mit einem Kommatrennzeichen hinzufügen.

4. Klicken Sie mit der rechten Maustaste auf das Formular, und wählen Sie **Speichern**aus.
   Wenn der Wert des Namens der Warnungsregel im Security Incident mit einem Datensatz im Modul „Erkennungsregel – MITRE ATT&CK TTP Mapping“ übereinstimmt, werden die entsprechenden Techniken und Taktiken, die der Warnungsregel zugeordnet sind, automatisch mit dem Security Incident verknüpft.



5. Öffnen Sie den Security Incident, wählen Sie die **MITRE ATT&CK-Karte** aus, und überprüfen Sie, ob ein Rollup für die Techniken durchgeführt wird.
6. Aktivieren Sie die Option **Ursprung der Techniken anzeigen,** um den Ursprung der Techniken anzuzeigen.
   Der Ursprung der Techniken muss Erkennungsregelsein.

Rollup von Informationen MITRE-ATT&CK aus untergeordneten Security Incidents

Wenn Sie das automatische Rollup von Informationen MITRE-ATT&CK nicht aktiviert haben, können Sie dies manuell durchführen.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

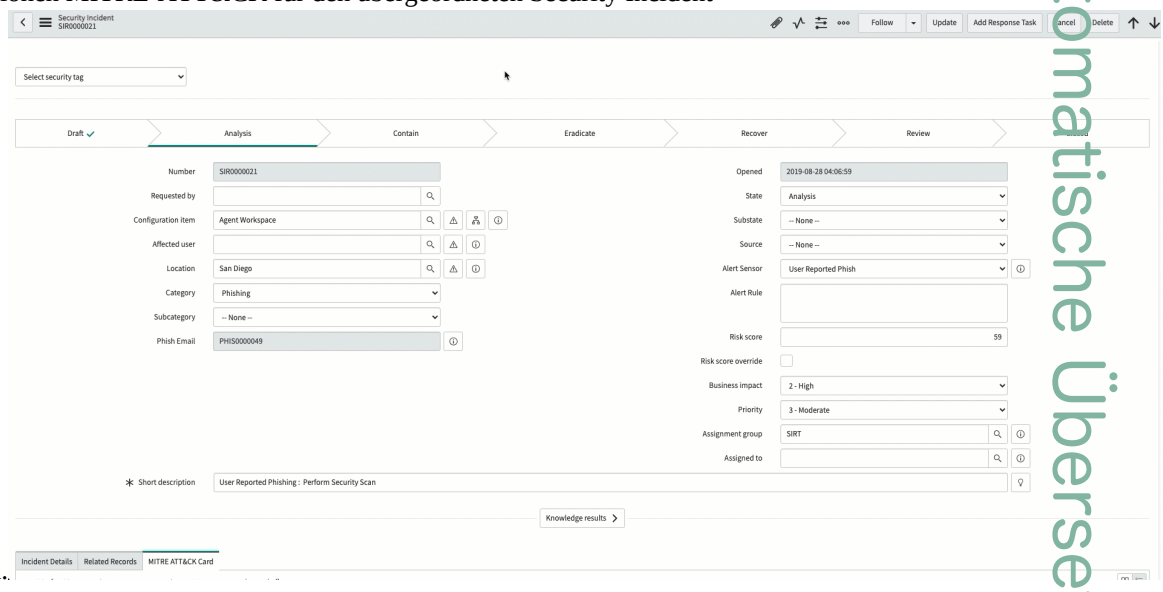
Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie aktiviert haben automatisches Rollup von MITRE-ATT&CK Informationen aus untergeordneten Security Incidents, werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie dies manuell tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den übergeordneten Security Incident aus, den Sie mit den untergeordneten MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und dann auf die Registerkarte **Untergeordnete Security Incidents**.
4. Wählen Sie den untergeordneten Security Incident aus, und klicken Sie dann im Menü „Aktionen **" auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Sie können **auf MITRE ATT&CK-Informationen anzeigen** klicken, um die MITRE-Informationen des untergeordneten Security Incident anzuzeigen, bevor Sie ein Rollup für die MITRE ATT&CK-Informationen durchführen.
5. Klicken Sie auf **Neu laden**, um die Änderungen zu bestätigen.
6. Klicken Sie auf die **Karte MITRE ATT&CK,** um den Ursprung der Techniken anzuzeigen.
   Die folgende Abbildung zeigt, wie Sie den untergeordneten Security Incident auswählen und die Informationen MITRE-ATT&CK für den übergeordneten Security Incident zusammenfassen.



   Sie können die MITRE-ATT&CK-Karte anzeigen, um zu bestätigen, dass die Informationen zum untergeordneten Security Incident MITRE-ATT&CK für den übergeordneten Security Incident zusammengefasst wurden.

Automatische Übersetzung

Führen Sie Linkanalysen und Bedrohungssuche mit MITRE-ATT&CK -spezifischen Filtern durch

Korrelieren Sie erkennbare Elemente, Security Incidents und MITRE-ATT&CK -bezogene Informationen, und führen Sie Linkanalysen für diese durch, damit Ihre Organisation nach Bedrohungen suchen kann.

Vorbereitungen

Erforderliche Rolle: sn_ti.mitre_analyst, sn_si.read

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie die Security Incidents den Informationen MITRE-ATT&CK zugeordnet haben, können Sie die spezifischen Filter für MITRE-ATT&CK für die Bedrohungssuche verwenden. Verwenden Sie die Filter MITRE-ATT&CK mit den vorhandenen Filtern Security Incident Response, um zu korrelieren und Linkanalysen durchzuführen.

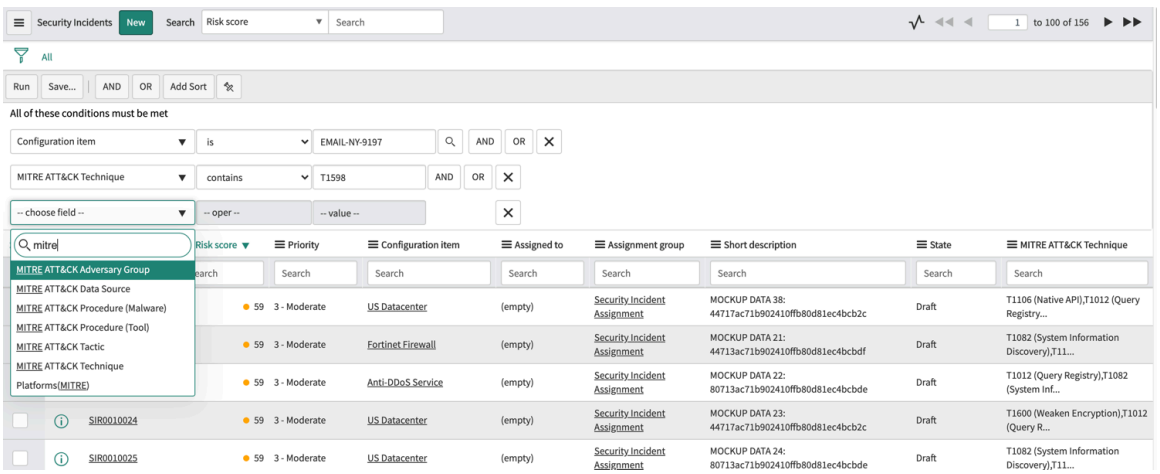
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Klicken Sie auf **Personalisierte Liste aktualisieren**, um die Spalten MITRE hinzuzufügen.
3. Wählen Sie eine Filterbedingung aus, damit Sie MITRE -bezogene Informationen und Zuordnungen zu Security Incidents oder erkennbaren Elementen anzeigen können:
   - MITRE-ATT&CK Angreifergruppe
   - MITRE-ATT&CK Datenquelle
   - MITRE-ATT&CK Eingriff (Malware)
   - MITRE-ATT&CK Vorgehensweise (Tools)
   - MITRE-ATT&CK Taktik
   - MITRE-ATT&CK Technik
4. Erstellen Sie eine Filterbedingung, die auf den obigen Kriterien basiert, und klicken Sie auf **Ausführen**, um eine Linkanalyse oder Korrelation zwischen Security Incidents, erkennbaren Elementen und MITRE-ATT&CK -bezogenen Informationen durchzuführen.

Hinweis:
Die Daten MITRE-ATT&CK werden als Zeichenfolge gespeichert, und Sie können nur „ **enthält"** als Operator für Filterbedingungen verwenden.

Wenn Sie beispielsweise überprüfen möchten, ob ein Configuration Item (CI) gefährdet ist, wählen Sie ein CI aus. Anschließend korrelieren Sie das CI mit den vorhandenen Techniken, indem Sie eine MITRE-ATT&CK Technik-ID hinzufügen. Anschließend können Sie mit dem Erstellen Ihrer Filterkriterien zur Korrelation der Informationen und für die Bedrohungssuche fortfahren.



MITRE-ATT&CK Heatmap und Navigator

Sie können die Heatmap und den Navigator MITRE-ATT&CK für die grundlegende Navigation und zur Visualisierung Ihrer allgemeinen Technikerkennungsabdeckung verwenden.

Übersicht über die Heatmap und den Navigator MITRE-ATT&CK

Sie können den Navigator mit den primären Filtern für die grundlegende Navigation und Beobachtung von ATT&CK-Matrizen verwenden. Die Heatmap hebt das Spektrum der Erkennungsabdeckung hervor, einschließlich der toten Winkel, die Ihre Organisation nicht abdeckt. Dies ist verfügbar, nachdem Sie die Technik-Erkennungsabdeckung zugeordnet haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Heatmap und der Navigator bieten folgende Möglichkeiten:

- Identifizieren Sie schnell und effizient die Erkennungsfähigkeiten Ihrer Organisation, und heben Sie Lücken in der Abdeckung der Technikerkennung hervor.
- Suchen Sie nach Bedrohungen, und führen Sie eine Bedrohungskorrelation mithilfe zugehöriger Funktionen durch.

Greifen Sie auf die Heatmap und den Navigator MITRE-ATT&CK zu

Greifen Sie auf die Heatmap und den Navigator MITRE-ATT&CK zu, um die Matrix anzuzeigen, mit der Sie ATT&CK verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_ti.read, sn_ti.mitre_analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Heatmap überprüfen, die Filter für die Korrelation verwenden und eine Linkanalyse der MITRE-ATT&CK -Informationen, der erkennbaren Elemente und der Security Incidents in Ihrer Organisation durchführen.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Heatmap und Navigator**.
   Heatmap und Navigator werden in einer neuen Registerkarte geöffnet.
2. Wählen Sie die Quelle aus, um die Heatmap auszufüllen.

   Hinweis:
   In der Quellenliste werden nur die Sammlungen und Matrizen angezeigt, die aktiviert wurden.

   In der folgenden Abbildung sehen Sie, wie Sie zur Heatmap und zum Navigator navigieren und die Quelle auswählen, in diesem Beispiel Enterprise ATT&CK.

   Navigieren Sie zu, und wählen Sie die Quelle aus, um die Heatmap auszufüllen
3. Verwenden Sie das Suchfeld, um anhand des Namens oder der ID schnell eine bestimmte Taktik oder Technik zu finden.

   Die folgende Abbildung zeigt, wie Sie nach einer Taktik, Technik oder den darin enthaltenen Informationen suchen können. Verwenden Sie die Suche, um schnell zu einer bestimmten Taktik oder Technik zu gelangen.
4. Klicken Sie auf **Filter**, und wählen Sie einen Filter unter Primären oder Erweiterten Filtern aus.
5. Klicken Sie auf **Übernehmen** und steuern Sie die Filter wie folgt:
   - Um Ihre Filter zu speichern, erstellen Sie eine anwenderdefinierte Ansicht. Sie können drei anwenderdefinierte Ansichtenerstellen und speichern.
   - Um die ausgewählten Filter zu entfernen, klicken Sie auf **„Standardfilter wiederherstellen“,** um Ihre standardmäßige gespeicherte Ansicht zu laden.
   - Um alle Filter und die vorhandene Ansicht zu löschen, klicken Sie auf **Alle Filter löschen**.

   Hinweis:
   Die Ansichten, die Sie speichern, sind spezifisch für einen Benutzer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie **auf Untertechniken ausblenden,** um alle Untertechniken aus der Heatmap-Ansicht zu entfernen.
   Wenn eine Technik Untertechniken hat, können Sie auf das Erweiterungssymbol klicken, um die Untertechniken anzuzeigen.

Anwenderdefinierte Ansichten verwenden

Anwenderdefinierte Ansichten in der Heatmap MITRE-ATT&CK und im Navigator helfen Ihnen, Ihre Lieblingsfilter zu speichern und anzuzeigen, wenn Sie das nächste Mal auf die Heatmap zugreifen.

Hinweis:
Sie können drei anwenderdefinierte Ansichten für jede MITRE-ATT&CK Sammlung pro Benutzer erstellen und speichern.

Erstellen Sie eine -Ansicht

Nachdem Sie die erforderlichen Filter unter Primären Filtern oder Erweiterten Filtern ausgewählt haben, klicken Sie im Header Filter auf die Schaltfläche mit den Auslassungspunkten (⋯), und wählen Sie **Neue Ansicht erstellen**aus. Geben Sie den Namen für die anwenderdefinierte Ansicht ein, und **speichern Sie die Ansicht**.

Standardansichten

Klicken Sie auf **Als Standardansicht speichern speichern,** um die Ansicht direkt zu laden, wenn Sie das nächste Mal auf die Heatmap zugreifen. Sie können für jede der Sammlungen eine Standardansicht festlegen.

Hinweis:
Wenn Sie das Plugin Threat Intelligence von einer älteren Version aktualisieren, wird die vorhandene Standardansicht der alten Version als anwenderdefinierte Ansicht angezeigt.

Die Abbildung zeigt, wie eine anwenderdefinierte Ansicht in der Heatmap erstellt wird

Aktualisiert eine Ansicht

Sie können Aktualisierungen an einer vorhandenen anwenderdefinierten Ansicht vornehmen, indem Sie die erforderlichen Filter „Primär“ oder „Erweitert“ ändern. Wählen Sie eine anwenderdefinierte Ansicht aus, aktualisieren Sie die Filter nach Bedarf, klicken Sie im Header Filter auf die Schaltfläche mit den Auslassungspunkten (⋯), und wählen Sie **Ansicht aktualisieren** aus, um die Filter zu speichern.

Diese Abbildung zeigt, wie eine anwenderdefinierte Ansicht aktualisiert wird.

Verwalten Sie anwenderdefinierte Ansichten

Verwenden Sie die Kontrollkästchen neben jeder anwenderdefinierten Ansicht, um den ausgewählten anwenderdefinierten Ansichtsfilter anzuwenden.

Klicken Sie auf die Schaltfläche mit den Auslassungspunkten (⋯) neben dem Namen jeder anwenderdefinierten Ansicht, um die anwenderdefinierten Ansichten wie folgt zu steuern:

- Legen Sie eine Standardansicht fest.
- Entfernen Sie eine anwenderdefinierte Ansicht als Standardansicht. Dadurch wird die anwenderdefinierte Ansicht nicht gelöscht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Benennen Sie die anwenderdefinierte Ansicht um.
- Löschen Sie die anwenderdefinierte Ansicht.

Diese Abbildung zeigt, wie anwenderdefinierte Ansichten verwaltet werden.

Exportieren Sie eine gespeicherte Ansicht

Um die gespeicherten anwenderdefinierten Ansichten in JSON-Dateien zu exportieren, klicken Sie im Header Filter auf die Auslassungspunkte (⋯), und wählen Sie **Gespeicherte Ansichten exportieren**aus. Klicken Sie auf das Download-Symbol für die anwenderdefinierte Ansicht, die Sie auf Ihren lokalen Computer herunterladen möchten.

Diese Abbildung zeigt, wie anwenderdefinierte Ansichten exportiert werden.

Importieren Sie eine Ansicht

Sie können nur JSON-Dateien importieren. Um die anwenderdefinierten Ansichten zu importieren, klicken Sie im Header Filter auf die Schaltfläche mit den Auslassungspunkten (⋯), und wählen Sie **Import view(json)**aus.

Überprüfen Sie beim Importieren von Ansichten die folgenden Bedingungen:

- Sie können nur das JSON-Dateiformat importieren.
- Sie können jeweils nur eine Ansicht oder Datei importieren.
- Sie können nicht importieren, wenn Sie bereits drei anwenderdefinierte Ansichten in Ihren Filtern haben. Löschen Sie eine anwenderdefinierte Ansicht, und importieren Sie eine Ansicht.
- Sie können eine Ansicht mit einem vorhandenen anwenderdefinierten Ansichtsnamen nicht importieren. Benennen Sie eine Ansicht vor dem Import um.

Diese Abbildung zeigt, wie eine -Ansicht importiert wird.

Navigator mit primären Filtern

Verwenden Sie die primären Filter, um Techniken im Navigator MITRE-ATT&CK zu filtern. Die Informationen im Repository MITRE-ATT&CK stehen zur Auswahl.

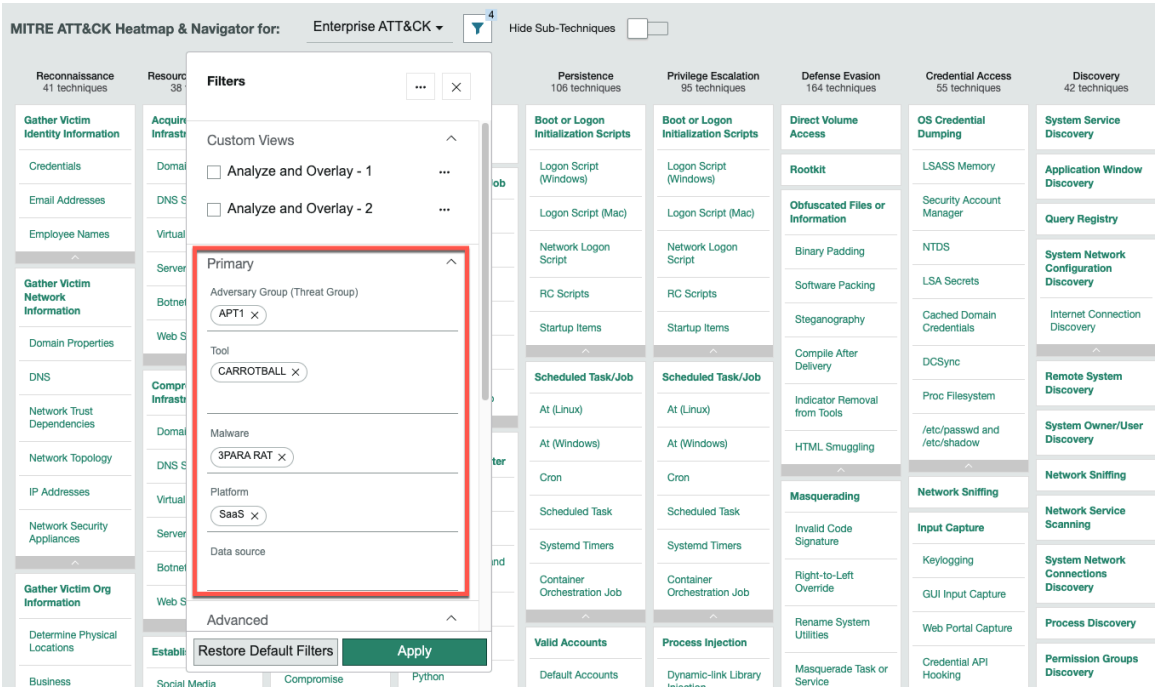
Filter	Beschreibung
Angreifergruppe (Bedrohungsgruppe)	Sätze zugehöriger Angriffsaktivitäten, die in der Sicherheitscommunity unter einem allgemeinen Namen verfolgt werden. Unter Gruppen versteht man verschiedene Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen. Sie können dem Filter **„Angreifergruppe“ (Bedrohungsgruppe)** mehrere Gruppen hinzufügen. Sie fügen beispielsweise „APT1“ und „AT12“ hinzu, da beide Bedrohungsgruppen sind, die China zugeordnet werden. Auch wenn beide Gruppen unterschiedliche Quellen anvisieren, könnten sie doch ähnliche Techniken verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter	Beschreibung
Tool	Legitimität der Software, die von Bedrohungsakteuren für Angriffe verwendet wird. Sie können verstehen, wie Bedrohungsakteure Kampagnen ausführen, wenn Sie wissen, wie und welche Tools Bedrohungsakteure verwenden. „Tools“ umfasst sowohl Software, die sich nicht auf einem Unternehmenssystem befindet, als auch Software, die als Teil eines Betriebssystems verfügbar ist, das bereits in einer Umgebung vorhanden ist, z. B. Microsoft Windows-Dienstprogramme. Beispielsweise ist gsecdump ein öffentlich verfügbarer Dumper für Anmeldeinformationen, den die APT11-Angreifergruppe verwendet, um Passwort-Hashes und LSA-Geheimnisse (Local Security Authority) von Microsoft Windows-Betriebssystemen abzurufen.
Malware	Kommerzielle, anwenderdefinierte Closed Source- oder Open Source-Software, die von Angreifern für böswillige Zwecke verwendet werden soll. Beispiele sind PluginX, CHOPSTICK usw
Plattform	Taktiken und Techniken, die MITRE-ATT&CK auf einer bestimmten Plattform repräsentieren. Beispielsweise unterstützt MITRE-ATT&CK diese Plattformen in der Enterprise ATT&CK-Matrix: Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Network.
Datenquelle	Datenquellen, die Sie in Ihrer Umgebung sammeln und zur Erkennung von MITRE-ATT&CK -Techniken verwenden. Beispiele sind DLL-Überwachung und Browsererweiterungen.

Die folgende Abbildung zeigt alle im Navigator MITRE-ATT&CK verfügbaren primären Filter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mithilfe einer Heatmap mit primären und erweiterten Funktionen

Sie können eine Heatmap mit erweiterten Filtern verwenden, um eine Analyse durchzuführen, indem Sie Security Incidents mit den Informationen MITRE-ATT&CK korrelieren.

Zeigen Sie die Technik-IDs an

Sie können die MITRE-ATT&CK Technik-IDs mit den Techniknamen anzeigen, wenn Sie den Filter **Technik-IDs anzeigen** auswählen.

Zeigen Sie Technik-IDs in einer Heatmap an

Zeigen Sie relevante Techniken nach Priorität an

Um die Techniken anhand ihrer relevanten Priorität im Navigator zu filtern, wählen Sie **Nach Prioritätsfilter für Technik filtern** und anschließend im Menü die **relevante Priorität** aus. Sie können mehrere Filterprioritäten zuweisen. Sie können auch auf die Techniken in der Heatmap zeigen, um die Priorität der Technik zu erfahren.

Die relevanten Prioritätsinformationen hängen von der Priorisierung ab, die Sie im Feld Technik relevante Priorität festgelegt haben.

Diese Abbildung zeigt die Filterung nach relevanter Priorität.

Zeigen Sie die Abdeckung der Technikerkennung an

Um die allgemeine Technikerkennungsabdeckung in der Heatmap anzuzeigen, wählen Sie den Filter **Technikerkennungsabdeckung anzeigen** aus. Die Heatmap hebt das visuelle Spektrum der Erkennungsabdeckung hervor, einschließlich der toten Winkel, in denen Sie keine Abdeckung haben. Die Bewertungsdefinition des Basissystems und die Farben wurden in der Abdeckung der Technikerkennungdefiniert. Die Informationen wurden automatisch aus der allgemeinen Technikerkennungsabdeckung extrahiert.

Beispielsweise weisen rot markierte Bereiche der Heatmap auf einen Mangel an Erkennung hin. Blau markierte Bereiche zeigen an, dass vollständige Erkennungsfunktionen vorhanden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sind. Bereiche, die in Orange, Gelb und Hellblau markiert sind, spiegeln teilweise Erkennungsfunktionen wider.

- Die Farbvisualisierung basiert auf der von Ihnen definierten Technikdefinition und Farbcodierung.
- Die Abdeckungsvisualisierung basiert auf der von Ihnen definierten Zuordnung der Technikerkennungsabdeckung.
- Wenn Sie die Abdeckungsdefinition des Basissystems ändern, werden die Symbole für Abdeckungstypen nicht mit den Techniken in der Heatmap angezeigt.

Hinweis:
Die Heatmap funktioniert wie erwartet, wenn Sie dieselben Felder wie die im Basissystem definierte Technikerkennungsabdeckung und die Abdeckungsfarben ändern.

In dieser Abbildung sehen Sie die Technikerkennungsabdeckung für alle Techniken und Untertechniken und den Abdeckungstyp mit ihren Farben und Symbolen.

Heatmap-Technik-Erkennungsabdeckung

Zeigen Sie die Abdeckung durch Technikminderung an

Um die Gesamtabdeckung der Technikminderung in der Heatmap anzuzeigen, wählen Sie den Filter Technikminderungsabdeckung anzeigen aus. Die Heatmap hebt das visuelle Spektrum der Abdeckung durch die Verringerung hervor, einschließlich der Bereiche, die Sie nicht abdecken. Die Abdeckung durch die Verringerung, die Farben und die Prozentbereiche wurden in der Definition der Abdeckung durch die Verringerungdefiniert. Die Informationen werden aus der allgemeinen Technik-Abdeckung durch Risikominderungextrahiert.

Rot hervorgehobene Techniken zeigen beispielsweise keine Abdeckung durch die Verringerung an, Orange bedeutet eine geringe Abdeckung durch die Verringerung und Blau bedeutet eine hervorragende Abdeckung durch die Verringerung.

- Die Farbvisualisierung basiert auf der Definition der Technikminderung und der Farbcodierung, die Sie definieren.
- Die Abdeckungsvisualisierung basiert auf der von Ihnen definierten Zuordnung der Technik zur Abdeckung durch Risikominderung.
- Wenn Sie die Definition der Abdeckung durch Risikominderung im Basissystem ändern, werden die Symbole für Abdeckungstypen für die Verringerung nicht mit den Techniken in der Heatmap angezeigt.

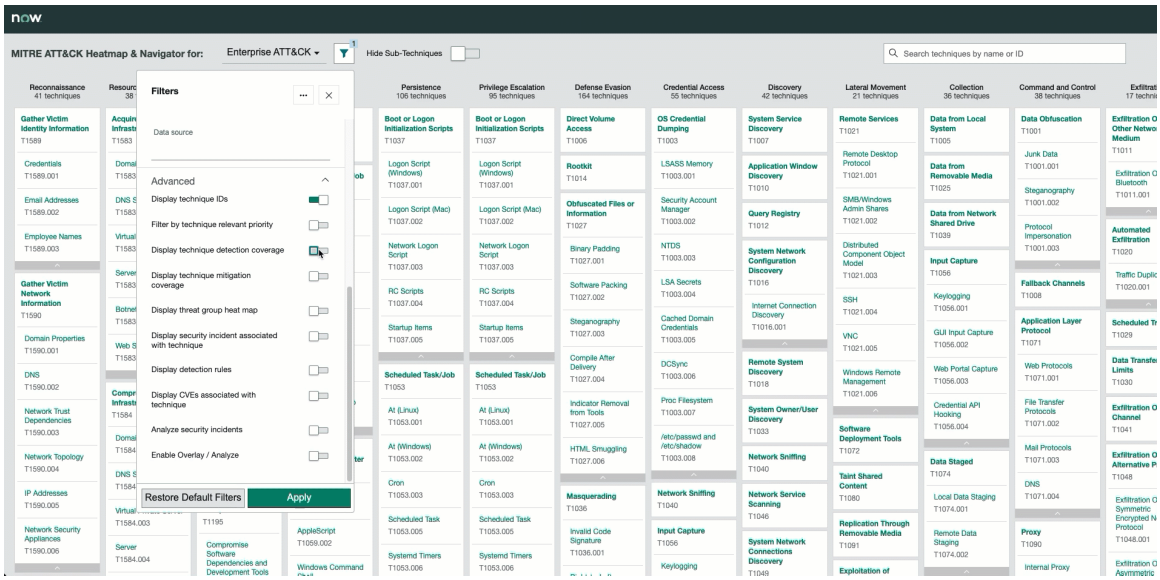
Hinweis:
Die Heatmap funktioniert wie erwartet, wenn Sie dieselben Felder wie die im Basissystem definierte Technikminderungsabdeckung und die Abdeckungsfarben ändern.

Diese Abbildung zeigt die Heatmap der Technik-Abdeckung durch Risikominderung

Zeigen Sie die Abdeckung für Erkennung und Verringerung an

Sie können die Filter für Technikerkennung und Abdeckung durch Technikminderung zusammen verwenden, um einen Einblick in die Relevanz der Technikerkennung zu erhalten und die Abdeckung für Ihr Unternehmen zu mindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Diese Abbildung zeigt, wie der Erkennungs- und der Verringerungsfilter zusammen verwendet werden.

Zeigen Sie die Bedrohungsgruppe an

Um Informationen von der Bedrohungsgruppe zur Technik in der Heatmap anzuzeigen, wählen Sie **Heatmap der Bedrohungsgruppe anzeigen**aus. Sie können die Anzahl der Bedrohungsgruppen messen, die eine bestimmte Technik verwenden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik erhöht sich, wenn die Anzahl der Angreifer hoch ist. Die Bedrohungsgruppenbereiche und die Farben der Heatmap wurden in der Heatmap-Definition der Bedrohungsgruppentechnikdefiniert.

- Die Farbvisualisierung für die Heatmap und den Text basiert auf der Heatmap-Definition von Bedrohungsgruppe zu Technik.
- Die Visualisierung des Bedrohungsgruppenbereichs basiert auf der Zuordnung von Bedrohungsgruppe zu Technik.
- Sie können den **Heatmap-Filter für Bedrohungsgruppen anzeigen** nicht verwenden, wenn die Technik-Erkennungsabdeckung oder die Technik-Minderungsabdeckung aktiviert ist.
  Diese Abbildung zeigt die Bedrohungsgruppeninformationen in einer Heatmap.

Zeigen Sie Security Incidents an, die einer Technik zugeordnet sind

Um die Techniken anzuzeigen, die in Ihrer Organisation häufig eingesetzt werden und zu Security Incidents geführt haben, klicken Sie auf **Security Incident anzeigen, der der Technik zugeordnet ist**. Sie können weitere Informationen zu jedem der zugehörigen Security Incidents anzeigen, indem Sie auf den Link klicken, der in einem neuen Fenster zur Analyse geöffnet wird. Security Incidents, die einer Technik zugeordnet sind.

- Priorität: Wählen Sie **Security Incident Priority (Priorität von** Security Incidents), um nach der Priorität des Security Incidents zu filtern.
- Datumsbereich: Wählen Sie den **Datumsbereich für Security Incident** aus, um Sicherheitsprobleme nach Datumsbereich zu filtern.
- Falsch positive Meldungen: Wählen Sie **Security Incidents falsch positive Meldungen filtern** aus, um falsch positive Probleme zu entfernen. Durch Auswahl dieses Filters wird die Anzahl der Security Incidents reduziert, die in der Heatmap angezeigt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie diesen Filter mit dem Filter **„Abdeckung für Technikerkennung anzeigen“** verwenden, erhalten Sie einen Einblick in die Relevanz der Abdeckung für Technikerkennung für Ihre Organisation bis zum ausgewählten Datum.

Wenn Sie beispielsweise beide Filter aktivieren, können Sie sehen, dass die Maskierungstechnik unter der Taktik der Verteidigungsumgehung nicht abgedeckt wird. Genauer betrachtet bezieht sich die Maskierungstechnik auf die Maskierungsaufgabe oder den Maskierungsservice, der bzw. dem ein Security Incident zugeordnet ist. Dies zeigt, dass in der Technikerkennungsabdeckung für die Maskierungstechnik eine Lücke besteht, und Sie sollten möglicherweise die allgemeine Technikerkennungsabdeckung überarbeiten.

Erkennungsregeln anzeigen

Um anzuzeigen, ob Sie die Erkennungsregeln für eine bestimmte Technik definiert haben, klicken Sie auf **Erkennungsregeln anzeigen**. Sie können auch alle zugehörigen Erkennungsregeln mit ihrer Definition anzeigen.

Diese Informationen basieren auf der von Ihnen definierten Zuordnung von Erkennungsregeln. Zeigen Sie die zugeordneten Erkennungsregeln an.

CVEs anzeigen, die der Technik zugeordnet sind

Um die Informationen zu Common Vulnerabilities and Exposures (CVE), die den einzelnen Techniken zugeordnet sind, anzuzeigen, klicken Sie auf **CVEs anzeigen, die der Technik zugeordnet sind**. Die Informationen von CVE zu Technik basieren auf den Informationen, die im Modul „CVE – Technikzuordnung“verfügbar sind. Dies gewährt Ihnen Einblicke in bekannte Schwachstellen und zeigt Ihnen, ob Angreifer Ihre Organisation potenziell angreifen können.

Wichtig:
Die Heatmap wird so erweitert, dass nur die relevanten CVEs angezeigt werden, die den VITs zugeordnet sind

Um VITs anzuzeigen, die CVEs und Techniken zugeordnet sind, wählen Sie **VITs anzeigen, die CVE und Techniken zugeordnet sind**. Um Techniken ohne VITs weiter zu filtern, wählen Sie außerdem **Techniken ohne VITs ausblenden**aus. Die von Ihnen angezeigten CVE- und VIT-Informationen werden aus dem -Produkt Vulnerability Response in Ihrer Umgebung abgerufen. Sie können die gefilterte Liste der CVEs und VITs in der Heatmap anzeigen und aus der Heatmap zu jedem CVE oder VIT für jede Technik navigieren.

Hinweis:

- Die **der -Technik zugeordneten CVEs anzeigen** ist nur verfügbar, wenn das Produkt Vulnerability Response in Ihrer Umgebung installiert ist.
- Die VIT- und CVE-Informationen werden basierend auf der geplanten Aufgabe berechnet, die Sie im festgelegt haben MITRE-ATT&CK Eigenschaften. Die geplante Aufgabe des Basissystems ist auf 24 Stunden festgelegt.

Wenn Sie diesen Filter mit dem Filter **Security Incident anzeigen, der der Technik zugeordnet ist**, erfahren Sie, ob die bekannten Schwachstellen in Ihrer Organisation Security Incidents verursacht haben.

Sie können weitere Informationen zu jedem CVE anzeigen, um zu analysieren, ob das CVE für Ihre Organisation relevant ist. Zeigen Sie dazu die angreifbaren Elemente an. Wenn angreifbare Elemente erstellt werden, können Sie im Modul Vulnerability Response weitere Informationen zu zugehörigen CI-Informationen anzeigen. Sie können auch den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregrad und die Priorität überprüfen, um fundierte Entscheidungen zu treffen.
Überprüfen Sie CVEs, um fundierte Entscheidungen zu treffen.

Analysieren Sie Security Incidents

Um Security Incidents zu analysieren und die Techniken zu überprüfen, die von einem Angreifer für einen Angriff verwendet werden, klicken Sie auf **Security Incidents analysieren**. Sie können mehrere Security Incidents zur Analyse hinzufügen, indem Sie durch Kommas getrennte Zeichenfolgen verwenden.

Mit diesem Filter können Sie einen Security Incident analysieren. Sie erfahren, warum der Incident aufgetreten ist, welche Techniken ausgenutzt wurden, ob bekannte Bedrohungsakteure beteiligt waren, ob die Bedrohungsakteure eine bestimmte Sequenz für einen Angriff verwendet haben usw. Da Sie mehrere Security Incidents gleichzeitig analysieren können, können Sie die Informationen korrelieren, um zu sehen, ob sie zusammenhängen oder ob sie einen isolierten Incident darstellen. Wenn die Security Incidents miteinander zusammenhängen und Sie ein Muster beobachten, können Sie den Fortschritt der Incidents in der Kill Chain überprüfen, um den Angriff zu stoppen oder eine Verteidigungsstrategie für Ihre Organisation zu entwickeln.

Wenn Sie den Filter **„Security Incidents analysieren“** mit primären Filtern verwenden, z. B. einer **Angreifergruppe**, können Sie korrelieren, ob bekannte Angreifer beteiligt sind. Wenn beispielsweise mehrere Security Incidents analysiert werden, werden die Techniken, die den Security Incidents zugeordnet sind, in Form einer Kill Chain angezeigt. Wenn Sie die Informationen mit dem Angreifer überschneiden, werden Sie eine Überschneidung zwischen den Techniken, die dem Security Incident zugeordnet sind, und den Techniken, die dem Angreifer zugeordnet sind, feststellen. Wenn beide Filter aktiviert sind, werden nur die Informationen zur überlappenden Technik angezeigt.

Analysieren Sie Security Incidents

Per Overlay können Sie Security Incidents und Angreifergruppen analysieren

Verwenden Sie den Filter **„Überlagerung aktivieren/Analysieren“,** um das Verhalten des Angreifers anzuzeigen, einen oder mehrere Security Incidents zu analysieren und die Informationen zu korrelieren, um zu sehen, ob es sich bei einem Angriff um einen isolierten Incident oder einen koordinierten Angriff eines bekannten Angreifers handelt.

Beispielsweise können Sie jetzt die Security Incidents und das Kill Chain-Verhalten des Bedrohungsgegners in derselben Ansicht anzeigen. Diese Ansicht enthält Überlappungsinformationen, die Sie über den Angriff und das bekannte Verhalten des Angreifers informieren. Auf diese Weise können Sie analysieren, ob es sich um einen isolierten Angriff oder einen koordinierten Angriff eines bekannten Angreifers handelt.

Durch Aktivieren des Überlagerungsanalysefilters werden alle primären Filter mit Ausnahme des **Angreifergruppenfilters** und des erweiterten **Filters „Nach technikrelevanter Priorität filtern“** beim Generieren einer Ansicht ignoriert.

Sobald Sie den Überlagerungsanalysefilter aktiviert haben, verwenden Sie die Farbpalette, um Farben für Folgendes zuzuweisen:

- Security Incident analysieren
- Angreifergruppe
- Überlagerung

Die folgende Abbildung zeigt, dass die Angreifergruppe APT18 über mehrere Techniken und Taktiken in der Kill Chain verteilt ist. Die Analyse zeigt auch, dass es drei Techniken

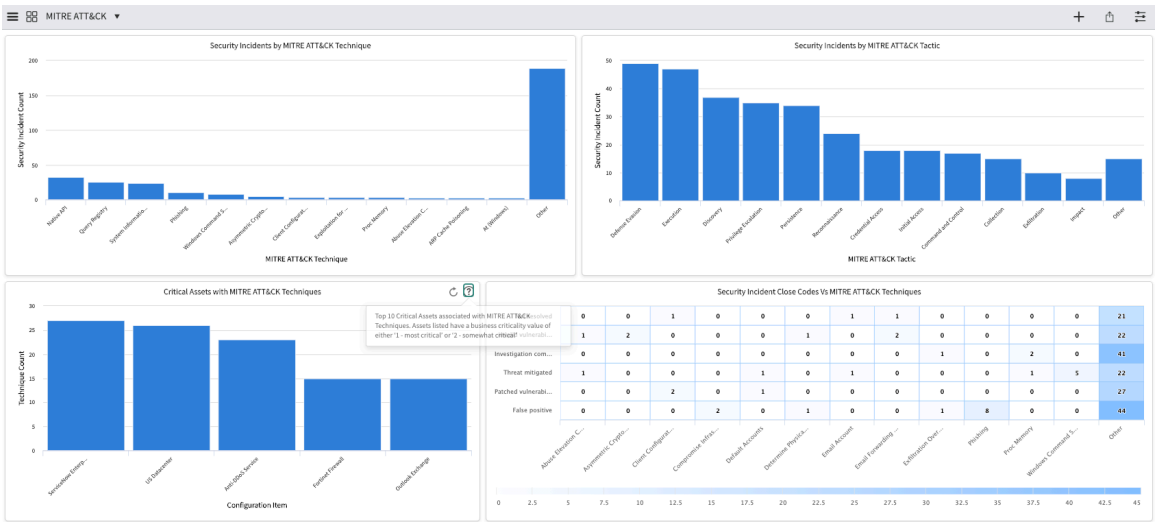
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gibt, die die von Ihnen nachverfolgte Angreifergruppe und die Security Incidents überlagern. Diese Abbildung zeigt die Überlagerungsinformationen für Angreifer und Security Incidents.

Über das Dashboard MITRE-ATT&CK

Das Dashboard MITRE-ATT&CK bietet eine Ausführungsansicht der Datenquellenabdeckung sowie der Taktiken und Techniken, die in Ihrer Organisation verwendet werden.

Das Modul MITRE-ATT&CK – Übersicht zeigt Informationen MITRE-ATT&CK zu Security Incidents an, einschließlich Trends und Berichte. Sie können auf jeden Teil eines Widgets klicken (Balken, Datenpunkt, Tabelle usw.), um Daten anzuzeigen, die für diesen Teil spezifisch sind.



Verwenden Sie das -Dashboard MITRE-ATT&CK, um Ihre sicherheitsbezogenen Daten anzuzeigen

Verwenden Sie das Dashboard MITRE-ATT&CK, um sich einen Überblick über die Abdeckung von Datenquellen, Taktiken und Techniken zu verschaffen, die in Ihrer Organisation verwendet werden.

Vorbereitungen

Erforderliche Rolle: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Übersicht**.
2. Klicken Sie auf eines der folgenden Widgets, um zusätzliche Details anzuzeigen:
   - Security Incidents nach MITRE-ATT&CK -Technik
   - Taktik der Security Incidents nach MITRE-ATT&CK .
   - Kritische Assets mit MITRE-ATT&CK Techniken
   - Lösungscodes für Security Incidents im Vgl. zu Techniken für MITRE-ATT&CK .
   - MITRE-ATT&CK-Techniken nach Erkennungsabdeckung
   - MITRE-ATT&CK-Techniken nach Verringerungsabdeckung
   - Bedrohungsgruppen nach MITRE-ATT&CK-Technik
   - CVEs nach MITRE-ATT&CK-Technik

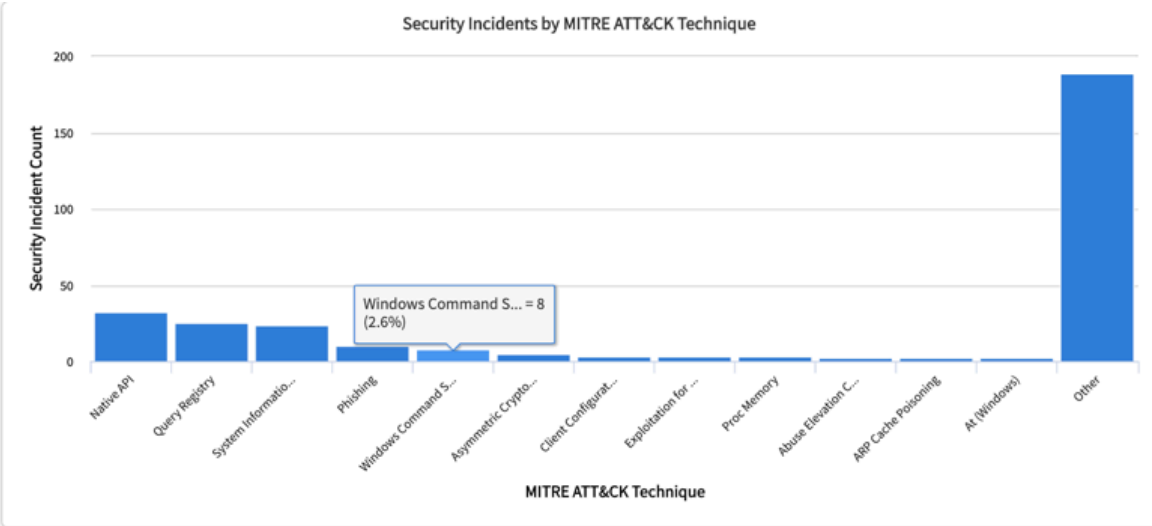
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE-ATT&CK Widgets

Das Übersichtsmodul MITRE-ATT&CK besteht aus Widgets, mit denen Sie die Informationen MITRE-ATT&CK mit den Security Incident-Informationen in Ihrer Umgebung korrelieren können.

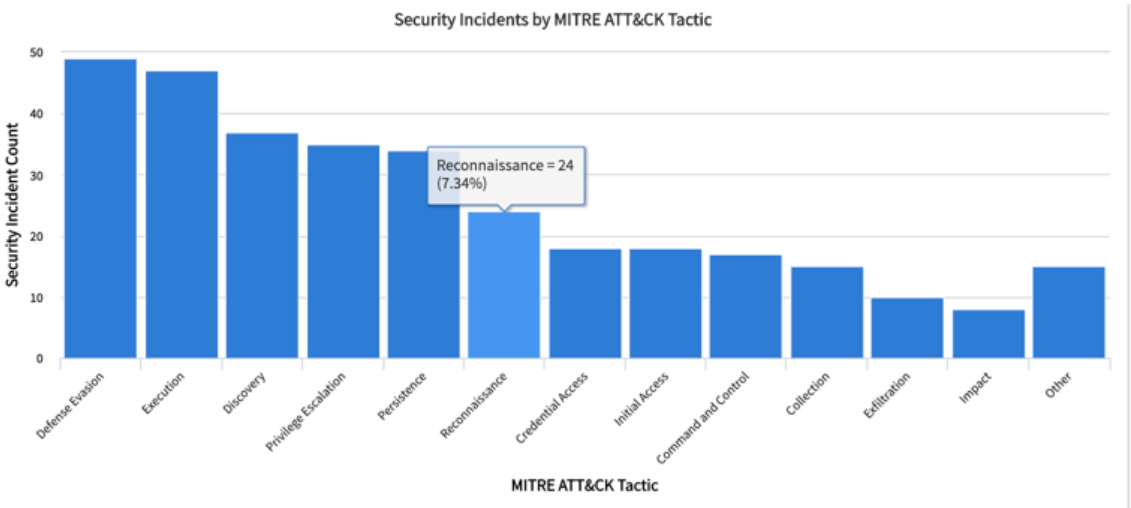
Beispiel für Security Incidents nach MITRE-ATT&CK -Technik

In diesem Beispiel zeigt das Widget **„Security Incidents nach MITRE ATT&CK-Technik“** die Techniken nach Security Incident in der Umgebung einer Organisation in den letzten 90 Tagen an.



Beispiel für die Taktik „Security Incidents nach MITRE-ATT&CK“.

In diesem Beispiel zeigt das Widget **„Security Incidents nach MITRE ATT&CK-Taktik“** die Top-Taktiken nach Security Incident in der Umgebung einer Organisation in den letzten 90 Tagen an.

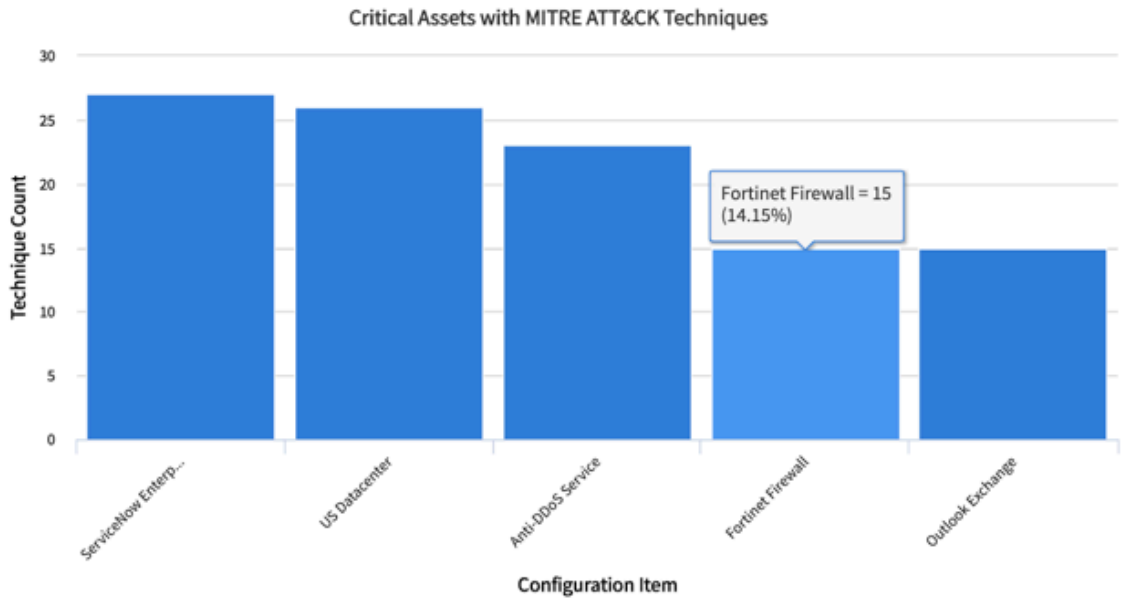


Beispiel für kritische Assets mit MITRE-ATT&CK Techniken

In diesem Beispiel zeigt das Widget **„Kritische Assets mit MITRE ATT&CK-Techniken“** die 10 wichtigsten kritischen Assets an, die den Techniken MITRE-ATT&CK zugeordnet sind. Die Assets haben eine Geschäftskritikalität von entweder 1 (äußerst kritisch) oder 2 (kritisch).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

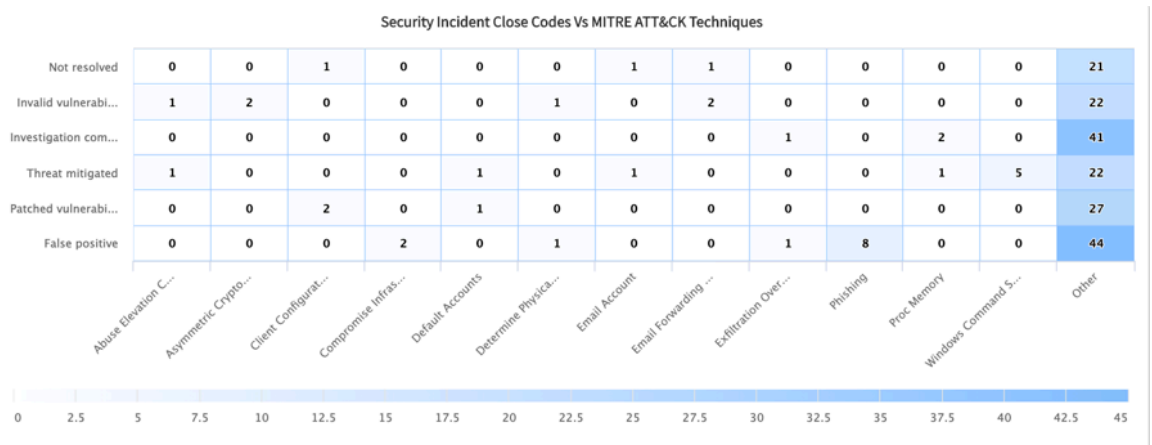
Mit diesem Bericht kann eine Organisation die Arten und die Anzahl der Techniken anzeigen, die für Angriffe auf kritische Assets verwendet werden.



Beispiel für Lösungscodes für Security Incidents im Vgl. zu MITRE-ATT&CK Techniken

In diesem Beispiel zeigt das Widget **„Abschlusscodes für Security Incident vs. *MITRE-ATT&CK* -Techniken“** die Abschlusscodes für Security Incidents an, die den identifizierten Top-Techniken in der Umgebung einer Organisation zugeordnet wurden.

Die x-Achse zeigt die Top-Techniken an, die für Angriffe auf das Unternehmen verwendet wurden, und die y-Achse zeigt die geschlossenen Codes.

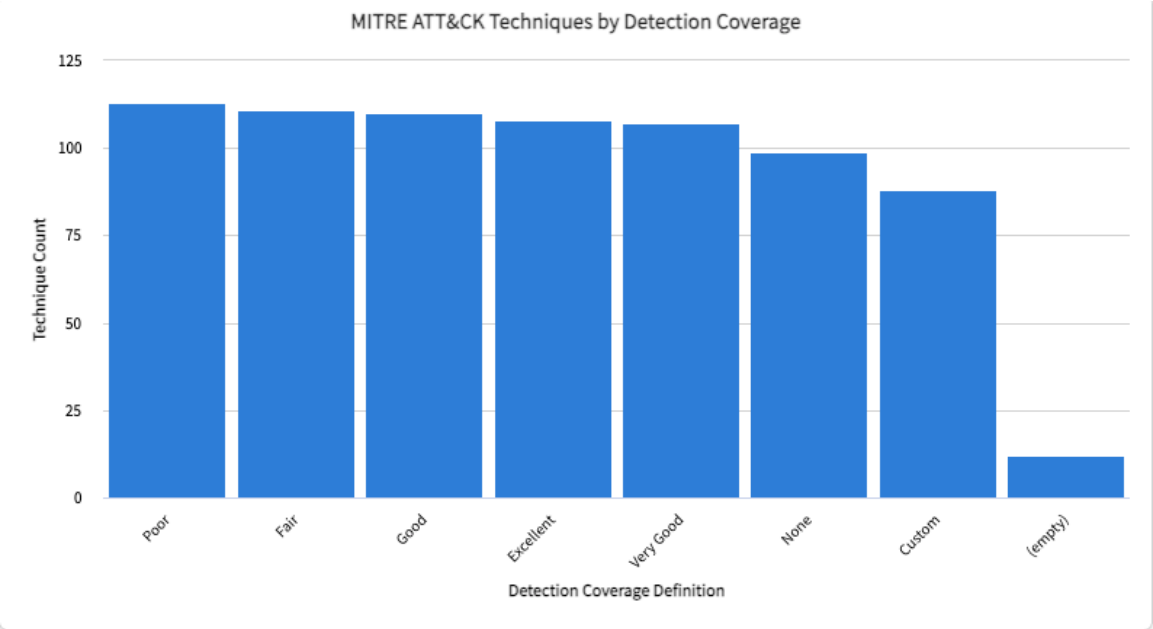


Beispiel für Erkennungsabdeckung durch Techniken MITRE-ATT&CK .

In diesem Beispiel zeigt das Widget **„MITRE-ATT&CK-Techniken nach Erkennungsabdeckung“** die Technikanzahl nach Erkennungsabdeckung in Ihrer Umgebung an.

Die x-Achse zeigt die Technikanzahl und die y-Achse die Erkennungsabdeckungstypen an.

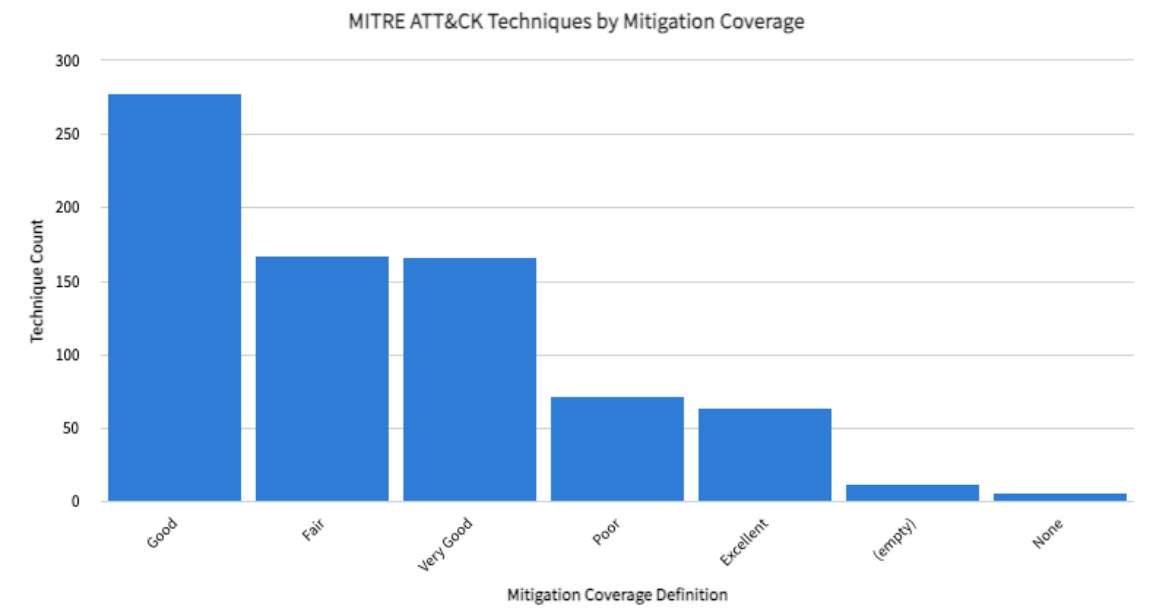
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beispiel für Abdeckung durch Risikominderung durch MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget **MITRE-ATT&CK-Techniken nach Verringerungsabdeckung** die Technikanzahl nach Verringerungsabdeckung in Ihrer Umgebung an.

Die x-Achse zeigt die Anzahl der Techniken an, und die y-Achse zeigt die Arten der Abdeckung durch Risikominderung.

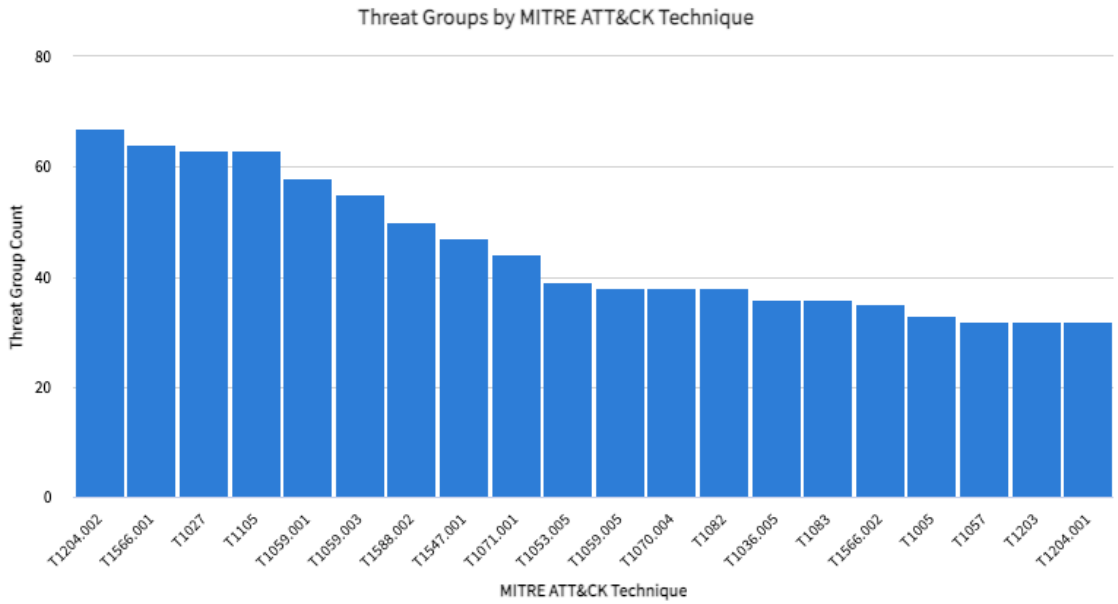


Beispiel für Bedrohungsgruppen nach MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget **„Bedrohungsgruppen nach MITRE-ATT&CK-Technik“** die Techniken nach Anzahl der Bedrohungsgruppen an. Dieses Widget zeigt 20 Techniken mit der höchsten Bedrohungsgruppenanzahl an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

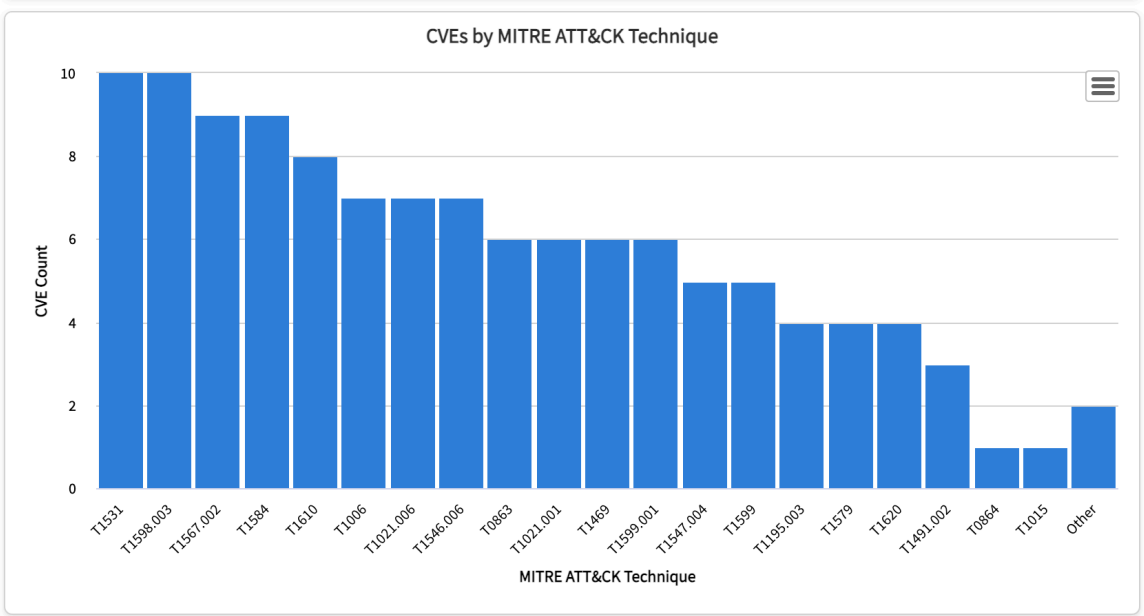
Die x-Achse zeigt die Anzahl der Bedrohungsgruppen an, und die y-Achse zeigt die Techniken MITRE-ATT&CK an.



Beispiel für CVEs nach MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget **CVEs nach MITRE-ATT&CK-Technik** die Techniken mit der relevanten CVE-Anzahl in Ihrer Umgebung an.

Die x-Achse zeigt die relevante CVE-Anzahl an, und die y-Achse zeigt die Techniken MITRE-ATT&CK an.



Threat Intelligence – Administration

Das Basissystem Threat Intelligence kann bei der Aktivierung verwendet werden. Bestimmten Modulen können Sie im Anwendungsmenü „Administration“ Datensätze hinzufügen, die meisten enthalten jedoch bereits branchenübliche Informationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Anwendungen sind im **Administrations** -Modul der Threat Intelligence -Navigationsleiste verfügbar:

Threat Intelligence-Verwaltungsanwendungen

Anwendung	Beschreibung
Eigenschaften	Threat Intelligence Mit den Eigenschaften von können Sie steuern, wie verschiedene Aspekte des Systems funktionieren, einschließlich der Einstellung von API-Schlüsseln.
Angriffsmechanismen	Dieses Modul organisiert Angriffsmuster hierarchisch, basierend auf Mechanismen, die häufig beim Ausnutzen einer Schwachstelle eingesetzt werden.
Angriffsmotivationen	In diesem Modul werden die möglichen Angriffsmotivationen aufgelistet, die die Stärke eines Angriffs durch einen Bedrohungsakteur oder Angriffssatz bestimmen.
Discovery-Methoden	Dieses Modul beschreibt, wie Security Incidents erkannt werden.
Feeds	Diese Funktion ist veraltet.
Indikatortypen	Dieses Modul wird verwendet, um Cyberbedrohungsindikatoren zu charakterisieren, die aus Mustern bestehen, die bestimmte erkennbare Bedingungen identifizieren, sowie kontextbezogene Informationen über die Bedeutung der Muster und wie und wann darauf reagiert wird.
Infrastrukturtypen	Dieses Modul listet die möglichen Klassifizierungen von Infrastruktur auf.
Beabsichtigte Wirkungen	Diese Anwendung wird verwendet, um die beabsichtigte Wirkung eines Bedrohungsakteurs auszudrücken.
Malware-Fähigkeiten	Dieses Modul listet die möglichen Fähigkeiten von Malware auf.
Schadsoftwaretypen	Dieses Modul listet die möglichen Klassifizierungen von Malware auf.
Benachrichtigungen	Dieses Modul wird zum Erstellen von verwendet E-Mail-Benachrichtigungen . Dabei wird angegeben, wann sie gesendet werden, wer sie erhält und was sie enthalten.
Erkennbare Typen	Dieses Modul listet die möglichen Klassifizierungen eines erkennbaren Elements auf, z. B. eine IP-Adresse oder einen Datei-Hash.
Berichtstypen	Dieses Modul listet die möglichen Klassifizierungen von Bedrohungsberichten auf.
Bedrohungsakteurrollen	In diesem Modul werden die Rollen aufgelistet, die die Bedrohungsakteure spielen.
Bedrohungsakteurtypen	Dieses Modul charakterisiert böswillige Akteure (oder Angreifer), die eine Cyberangriffsbedrohung darstellen, einschließlich vermuteter Absichten und bisher beobachtetem Verhalten.
Rechner für Funde der Bedrohungssuche	Dieses Modul berechnet die Ergebnisse basierend auf den erhaltenen Antworten. Bei Drittanbieterintegrationen, die die berechneten Ergebnisse bereitstellen, ordnet der Rechner für Ergebnisse der Bedrohungssuche die Ergebnisse unterstützten Ergebnissen im System zu. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche.
Tooltypen	Dieses Modul listet die mögliche Klassifizierung von -Tools auf.

Rechner für Funde der Bedrohungssuche

Der Rechner für Ergebnisse der Bedrohungssuche hilft Ihnen, die Ergebnisse erkennbarer Elemente basierend auf den empfangenen Antworten zu berechnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können einen Rechner für Ergebnisse der Bedrohungssuche für Ihre Integration erstellen und ein Skript verwenden, um zu bestimmen, wie die verschiedenen Ergebnisse erkennbarer Elemente identifiziert werden sollen. Der Rechner für Ergebnisse der Bedrohungssuche enthält ein Beispielskript, das im Basissystem enthalten ist und das Sie verwenden können, um die Ergebnisse erkennbarer Elemente zu identifizieren. Alternativ können Sie dieses Skript entsprechend Ihren Anforderungen ändern.

Bei Drittanbieterintegrationen, die die berechneten Ergebnisse bereitstellen, ordnet der Rechner für Ergebnisse der Bedrohungssuche die Ergebnisse unterstützten Ergebnissen im Basissystem zu.

Rollup der Ergebnisse der Bedrohungssuche

Wenn Sie mehrere Ergebnisse der Bedrohungssuche für ein erkennbares Element von den verschiedenen Integrationsanbietern haben, werden die aktuellen Ergebnisse der Bedrohungssuche von allen Anbietern berücksichtigt, und die Gesamtergebnisse der erkennbaren Elemente werden wie folgt gekennzeichnet:

Rollup der Ergebnisse der Bedrohungssuche

Neuestes Ergebnis erkennbarer Elemente	Gesamtergebnis erkennbarer Elemente
Böswillig	Wenn einer der Integrationslieferanten das erkennbare Element als böswillig meldet, wird der gesamte Fund des erkennbaren Elements als böswillig gekennzeichnet.
Verdächtig	Wenn keiner der Integrationsanbieter das erkennbare Element als schädlich meldet, meldet einer von ihnen es als verdächtig. Anschließend wird der gesamte Fund des erkennbaren Elements als verdächtig markiert.
Clean	Wenn alle Integrationslieferanten das erkennbare Element als „Sauber“ melden, wird das gesamte Ergebnis des erkennbaren Elements als „Sauber“ markiert.
Unbekannt	Wenn keiner der Integrationslieferanten das erkennbare Element als schädlich oder verdächtig und einer von ihnen als unbekannt meldet, wird der Gesamtbefund des erkennbaren Elements als unbekannt markiert.

Verwenden von Rechnern für die Ergebnisse der Bedrohungssuche

Verwenden Sie den Rechner für Ergebnisse der Bedrohungssuche, um die Ergebnisse erkennbarer Elemente für Ihre Integration zu berechnen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Administration** > **Rechner für Funde der Bedrohungssuche**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.
4. Klicken Sie auf **Aktualisieren**.

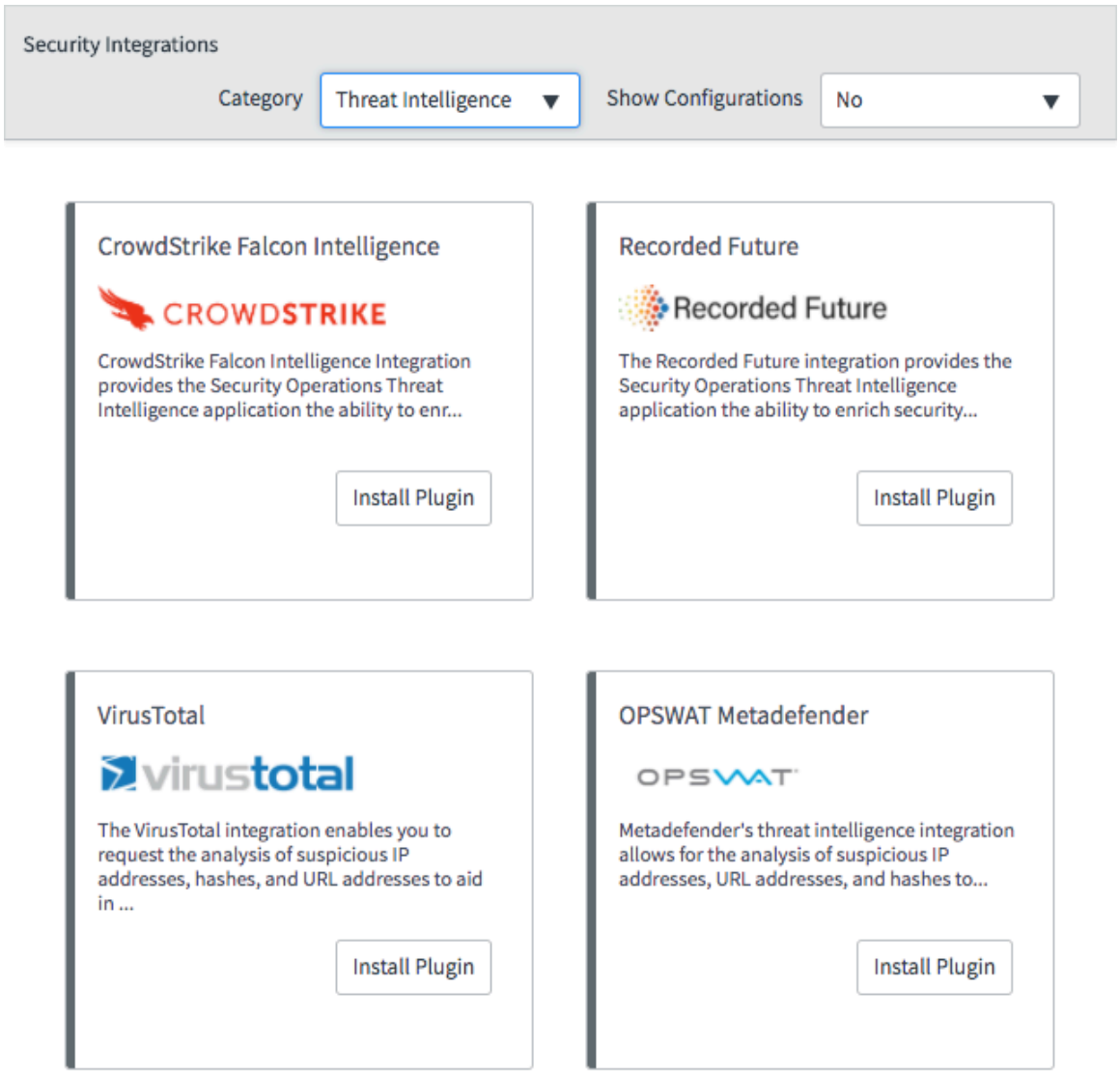
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Integrationen

Das -Basissystem Threat Intelligence enthält Integrationen für Malware-Erkennungssoftwarepakete von Drittanbietern. Dieser Abschnitt enthält Anweisungen zum Aktivieren der -Plugins und zum Konfigurieren von ServiceNow und Drittanbieterintegrationen. Außerdem enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten im Basissystem enthaltenen Integrationen.

Integrationskonfigurationen

Das Basissystem enthält eine Reihe von „Karten“ für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von Plugins Security Operations aufweisen. Die Integrationskarten können durch Auswahl von angezeigt werden **Security Operations** > **Integrationskonfigurationen**.



Sie können die sichtbaren Integrationen mithilfe des Dropdown-Menüs **Kategorie** filtern. Im Dropdown-Menü **Konfigurationen anzeigen** werden mehrere Instanzen von Implementierungen angezeigt, die deren Erstellung ermöglichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schaltflächen auf Integrationskarten

Je nach Status der Integration und Quelle der Karte werden auf Integrationskarten unterschiedliche Schaltflächen angezeigt.

Schaltfläche	Beschreibung
Plugin installieren	Klicken Sie auf diese Schaltfläche, um das entsprechende Plugin zu installieren und die Integration zu aktivieren. Nachdem das Plugin installiert ist, ändert sich die Schaltfläche in **Konfigurieren**.
Konfigurieren	Klicken Sie auf diese Schaltfläche, um Informationen zum Konfigurieren der Integration einzugeben. Für einige Integrationen müssen Sie möglicherweise API-Schlüssel oder URLs eingeben, die Sie auf der Website der Drittanbieterintegration erworben haben.
Neu	Bei bestimmten Integrationen (z. B. Carbon Black und IBM QRadar) können Sie mehrere Implementierungen derselben Integration definieren. Klicken Sie bei diesen Integrationen auf **Neu**, nachdem das Plugin aktiviert wurde. Mit den Karten können Sie Plugins installieren (falls zutreffend) und die zu verwendenden Implementierungen konfigurieren.
Seite öffnen	Im Basissystem führt Ihre Instanz von eine Abfrage an den ServiceNow Store für alle Anwendungen durch, die von den Plugins Security Operations abhängig sind. Wenn diese Anwendungen gefunden wurden und die zugehörigen Anwendungs-Plugins aktiviert sind, werden Integrationskarten für sie zusammen mit den anderen Sicherheitsintegrationskarten angezeigt. Klicken Sie **auf Seite öffnen**, um auf die Website der Drittanbieteranwendung zuzugreifen und die Integration zu konfigurieren. Nachdem Sie die Konfiguration abgeschlossen haben, ändert sich die Schaltfläche **Seite öffnen** in **Konfigurieren**.

CrowdStrike Falcon Intelligence-Integration

CrowdStrike Falcon Intelligence ergänzt Threat Intelligence mit Daten für Security Incidents und zugehörige erkennbare Elemente.

Erkunden

- Integrationsüberblick CrowdStrike Falcon Intelligence
- Security Incident Response-Integrationen

Einrichten

Aktivieren und konfigurieren Sie die CrowdStrike Falcon Intelligence -Integration

---

Verwenden

- Führen Sie Suchen für erkennbare Elemente durch
- Bedrohungssuche – Flows CrowdStrike Falcon Intelligence.

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Integrationsüberblick CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence bietet Cybersicherheitsinformationen, die sich problemlos in Security Operationsintegrieren lassen.

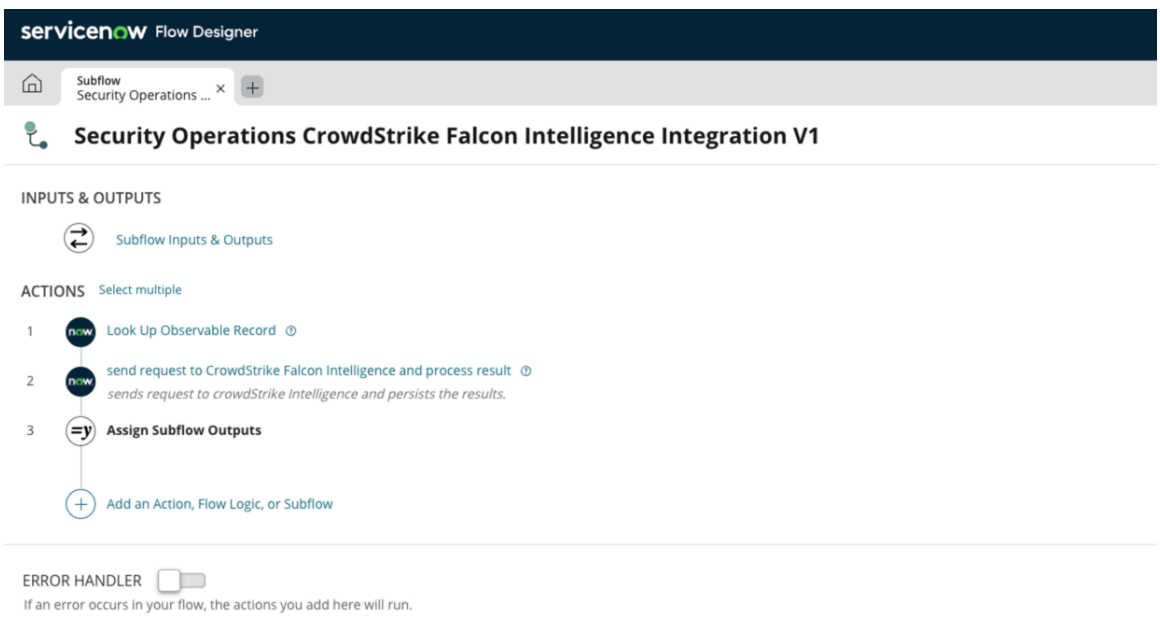
Hinweis:
Das Plugin Threat Intelligence ist erforderlich, um die Integration CrowdStrike Falcon Intelligence zu implementieren.

Bedrohungssuche – Flows CrowdStrike Falcon Intelligence.

Der Flow Designer „Bedrohungssuche – CrowdStrike Falcon Intelligence “ führt eine Suche für ausgewählte erkennbare Elemente durch. Wenn es sich bei den erkennbaren Elementen um einen von CrowdStrike Falcon Intelligenceerkannten Typ handelt, werden sie auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Dieser Flow wird von Security Operations-Integration – Funktionalität zur Bedrohungssuche ausgelöst, wenn Sie ein oder mehrere erkennbare Elemente in einer Beobachtungsliste veröffentlichen und die CrowdStrike Falcon Intelligence-Implementierung ausgewählt ist. Nach der Veröffentlichung können die Beobachtungslisten in der CrowdStrike Falcon Host-Software angezeigt werden.

Erforderliche Rolle: Administrator



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zu den von diesem Flow Designer verwendeten Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Aktivieren und konfigurieren Sie die CrowdStrike Falcon Intelligence -Integration

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der CrowdStrike Falcon Intelligence -Integration, schnell aktivieren und einrichten. Bevor Sie CrowdStrike Falcon Intelligenceverwenden können, müssen Sie es von ServiceNow Store herunterladen und den entsprechenden API-Schlüssel und die ID hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

- Das Plugin Threat Intelligence muss installiert und aktiviert werden, bevor Sie die CrowdStrike Falcon Intelligence -Integration verwenden können.
- Rufen Sie die API-Client-ID und das API-Client-Geheimnis in Ihrem Profil CrowdStrike Falcon Intelligence ab.
- Wenn Sie CrowdStrike Falcon Intelligence die -Integration von einer früheren Version aktualisieren, müssen Sie die vorhandene Konfiguration löschen und eine neue Konfiguration einrichten. Die -Integration unterstützt die OAuth2-Authentifizierung. Dieses Update erfordert die Eingabe der **API-Client-ID** und des **API-Clientgeheimnisses,** um sich zu authentifizieren und die Konfiguration abzuschließen.
- Aktivieren Sie in den **API-Bereichen**des Portals CrowdStrike Falcon Intelligence die Einstellung **Lesen** für **Indikatoren (Falcon X)** oder **IoCs (Indicators of Compromise)**.

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte CrowdStrike Falcon Intelligence auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus, um die Konfiguration abzuschließen:

CrowdStrike Falcon Intelligence Konfiguration

Feld	Beschreibung
Name	Name der Integration, z. `B. demo-1`.
API-Client-ID	Client-ID, die Sie im Abschnitt mit den Einstellungen Ihres Kontoprofils im Portal CrowdStrike Falcon Intelligence abrufen.
API-Client-Geheimnis	Der geheime Clientschlüssel, den Sie im Abschnitt mit den Einstellungen Ihres

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Kontoprofils im Portal CrowdStrike Falcon Intelligence erhalten.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nach der Konfiguration kann CrowdStrike Falcon Intelligence für die Durchführung von Suchen für erkennbare Elemente in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

Zugehörige Informationen

Führen Sie Suchen für erkennbare Elemente durch

Have I Been Pwned? Integration

Mit der Security Operations Have I Been Pwned? -Integration können Sie Suchvorgänge für Domänennamen und E-Mail-Adressen übermitteln, um festzustellen, ob die persönlichen Daten des Anwenders durch Datenschutzverletzungen gefährdet wurden.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Integrationssetup für Security Operations Have I Been Pwned? .
- Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? .

Verwenden

Führen Sie Suchen für erkennbare Elemente durch Bedrohungssuche – Flow Have I Been Pwned?.

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationssetup für Security Operations Have I Been Pwned? .

Have I Been Pwned? ist eine kostenlose Ressource, mit der bewertet werden kann, ob jemand gefährdet wurde, weil sein Online-Konto bei einer Datenschutzverletzung gefährdet oder „pwned“ wurde. Es lässt sich problemlos in Security Operationsintegrieren.

Bevor Sie die -Integration Have I Been Pwned? verwenden können, müssen Sie das Plugin aktivieren. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Die Plugins Security Incident Response, Threat Intelligenceund Security Operations Have I Been Pwned? sind erforderlich, um die Integration Security Operations Have I Been Pwned? zu implementieren.

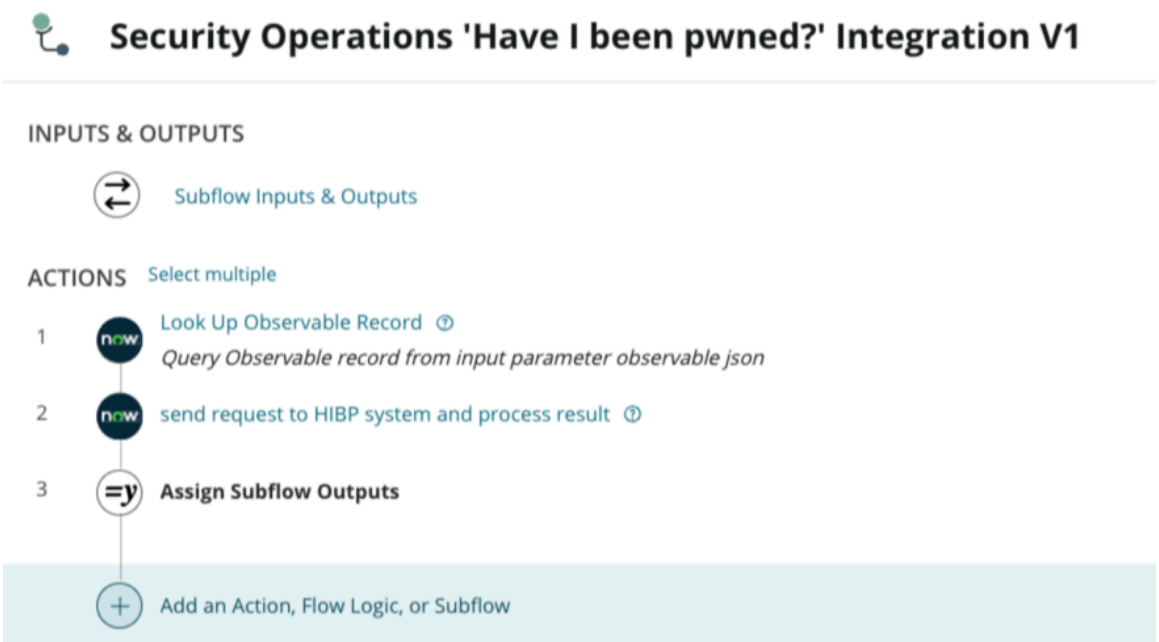
Bedrohungssuche – Flow Have I Been Pwned?.

Der Flow „Bedrohungssuche – Have I Been Pwned? “ führt eine Suche für ausgewählte erkennbare Elemente durch. Wenn es sich bei den erkennbaren Elementen um einen von Have I Been Pwned?erkannten Typ handelt, werden sie auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Erforderliche Rolle: sn_si_admin

Dieser Flow wird von Security Operations-Integration – Funktionalität zur Bedrohungssuche ausgelöst, wenn Sie eine Bedrohungssuche für mindestens ein erkennbares Element durchführen und die Implementierung Have I Been Pwned? ausgewählt ist. Weitere Informationen finden Sie unter Führen Sie Suchen für erkennbare Elemente durch.

Wurde ich pwned Flow



Informationen zu den von diesem Flow verwendeten Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? .

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der Security Operations Have I Been Pwned? -Integration, schnell aktivieren und einrichten. Bevor Sie die Have I Been Pwned? -Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Das Plugin Threat Intelligence muss installiert und aktiviert werden, bevor Sie die Security Operations Have I Been Pwned? -Integration verwenden können.

Erforderliche Rolle: sn_si_admin

Prozedur

Laden Sie die -Integration aus dem herunter ServiceNow Store.
Diese Integration unterstützt eine offene API und erfordert keine weitere Konfiguration. Have I Been Pwned? kann jetzt für die Suche nach erkennbaren Elementen in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

Zugehörige Informationen

Führen Sie Suchen für erkennbare Elemente durch

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Fälle, in denen das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erwerben Sie das SSL-Zertifikat von einem Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) wie folgt von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie auf **Weitere Informationen** und anschließend auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen** und anschließend auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Export**, um die PEM-Datei in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu** und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.

b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.

c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.

d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.

6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn ein Zertifikat abgelaufen ist, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .

MISP integration for Security Operations

Mit MISP integration for Security Operationskönnen Sie Security Incidents mit Sichtungssuchen und der Ergänzung erkennbarer Elemente untersuchen und Ereignisse in MISPerstellen oder aktualisieren. Mit MISPkönnen Sie gezielte Angriffe schneller untersuchen, das Erkennungsverhältnis verbessern und die Anzahl der Falschmeldungen in Ihrer Umgebung reduzieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

MISP Übersicht

MISP, das für Malware Information Sharing Platformsteht, ermöglicht Ihnen den Austausch von Bedrohungsdaten und Kompromittierungsindikatoren (IoCs) zu gezielter Malware und Angriffen innerhalb Ihrer Community vertrauenswürdiger Mitglieder. Sie können Informationen MISP auch für private oder offene Communities freigeben. Durch den Austausch von MISP -Informationen können Sie gezielte Angriffe schneller untersuchen, das Erkennungsverhältnis verbessern und die Anzahl der Falschmeldungen in Ihrer Umgebung reduzieren.

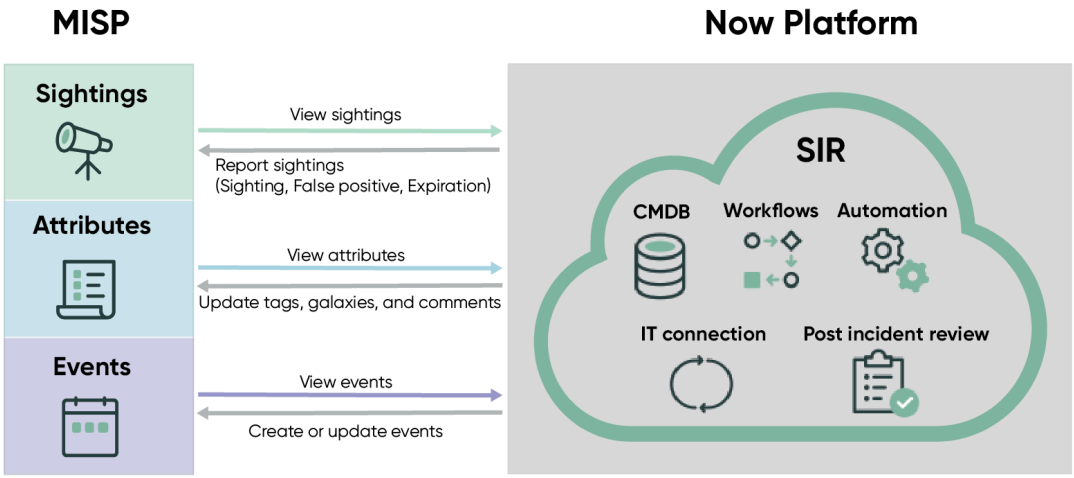
MISP und Security Operations

Im folgenden Beispiel erfahren Sie, wie die Informationen MISP mit Security Operations-Anwendungen fließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über MISP und Security Operations

Now Platform - MISP integration overview



Schlüsselfunktionen

Diese Integration umfasst die MISP folgenden Funktionen:

- Stellen Sie eine Verbindung mit privat und öffentlich her MISP instances.
- Unterstützt die manuelle und automatische Sichtungssuche von erkennbaren Elementen.
- Führen Sie eine Sichtungssuche über die Fallverwaltung aus.
- Sichtungen für ein Attribut melden oder aktualisieren:
  - Erkennbares Element als Sichtung melden (global)
  - Erkennbares Element als falsch positiv melden (global)
  - Melden Sie ein erkennbares Element als abgelaufen
- Unterstützt die manuelle und automatische Anreicherung erkennbarer Elemente. Ergebnisse enthalten das Attribut MISP und Ereignisinformationen, die den erkennbaren Elementen zugeordnet sind.
- Attributanreicherung in MISP, die das Hinzufügen oder Aktualisieren von Tags, Galaxienoder Kommentarenumfasst.
- Ereigniserstellung in MISP von SIR: Unterstützt die manuelle und die automatische Erstellung von Ereignissen in MISP aus SIR.
- Aktualisiert ein MISP -Ereignis aus SIR, das das Hinzufügen oder Aktualisieren von Tags, Galaxienoder Attributenumfasst.
- Fügen Sie einem Security Incident zugeordnete erkennbare Elemente als Attribute hinzu MISP event.
- Automatisch extrahieren MITRE-ATT&CK™ Informationen aus MISP attributes und ordnen Sie die Informationen den Security Incidents SIR zu.
- Automatisch hinzufügen SIR MITRE-ATT&CK™ Informationen als Galaxien zu MISP event.

Schlüsselkonzepte

Diese Integration enthält die folgenden Schlüsselkonzepte, die Sie kennen müssen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MISP ist eine Threat Intelligence-Plattform (TIP). Sie verwenden TIPs, um Sicherheitsbedrohungsdaten in Echtzeit zu sammeln, zu korrelieren, zu kategorisieren, freizugeben und zu integrieren, um die Priorisierung von Aktionen zu unterstützen und die Verhinderung, Erkennung und Reaktion von Angriffen zu unterstützen.
- MISP ist ein Threat Intelligence Management (TIM). Sie verwenden TIMs, um Bedrohungsdaten durch Kontext in Threat Intelligence umzuwandeln und Bedrohungen automatisch anhand von anwenderdefinierter Bewertung und Relevanz zu priorisieren.
- MISP Datenschicht
  - Ereignisse sind Kapseln für kontextbezogene verknüpfte Informationen.
  - Attribute sind einzelne Datenpunkte, die Indikatoren oder Unterstützungsdaten sein können.
  - Objekte sind anwenderdefinierte Vorlagenattribut-Kompositionen.
  - Objektreferenzen sind die Beziehungen zwischen den anderen Bausteinen.
  - Sichtungen sind zeitspezifische Vorkommen eines erkannten Datenpunkts.
- MISP Kontextebene
  - Tags sind Bezeichnungen, die Ereignissen oder Attributen angehängt sind und aus Taxonomien stammen können.
  - Galaxien-Cluster sind Knowledge Base-Elemente, mit denen Sie Ereignisse oder Attribute kennzeichnen können, die von Galaxien stammen.
  - Clusterbeziehungen bezeichnen vordefinierte Beziehungen zwischen Clustern.
- Indikatoren enthalten ein Muster, mit dem Sie verdächtige oder böswillige Cyberaktivitäten erkennen können.
- Attribute in MISP können Netzwerkindikatoren (IP-Adresse), Systemindikatoren (eine Zeichenfolge im Speicher) oder sogar Bankkontodetails sein. Die Attribute in MISP werden in anderen SIEMs oder Formaten wie STIXals erkennbare Elemente bezeichnet.
  - Ein Typ beschreibt das Attribut. Zum Beispiel MD5 oder eine URL.
  - Die Attributkategorie beschreibt ein Attribut. Zum Beispiel eine Payload-Lieferung.
  - Ein IDS-Tag bestimmt, ob ein Attribut automatisch für die Erkennung verwendet werden kann.

Hinweis:
Weitere Informationen zu den Konzepten MISP finden Sie auf der MISP-Dokumentationswebsite

Wie Ihr Unternehmen von profitieren kann MISP integration for Security Operations

Sicherheitsanalysten müssen ein situatives Bewusstsein für die Bedrohungslandschaft entwickeln und aufrechterhalten. Das bedeutet, dass sie eine überwältigende Menge von Bedrohungsdaten manuell konsolidieren und integrieren müssen. Das Sammeln, Konsolidieren und Integrieren dieser Daten nimmt wertvolle Zeit in Anspruch, was die Erkennung und Analyse von Bedrohungen verlangsamt. MISP integration for Security Operations ermöglicht es Analysten, mehr Bedrohungen zu erkennen und schneller zu reagieren, indem sie die MISP Security Intelligence in eine vorhandene Now Platform -Instanz integrieren.

Mit MISP integration for Security Operationskann Ihre Organisation die folgenden Aktionen ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ermöglichen Sie Ihren Sicherheitsanalysten, schnell und im richtigen Kontext zu reagieren.
- Verbessern Sie die Effizienz Ihres Sicherheitsteams, indem Sie die Incident-Flows zum Erkennen und Eindämmen von Bedrohungen automatisieren.
- Reduzieren Sie die Zeit für manuelle Recherchen, und ermöglichen Sie Sicherheitsanalysten, -Indikatoren von Now Platformaus zu operationalisieren und zu kuratieren.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
MISP Dokumentationswebsite	MISP-Dokumentationswebsite
ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

MISP – Administration

Sie können die MISP -Integration in Now Platform einrichten, um eine Sichtungssuche und die Ergänzung erkennbarer Elemente durchzuführen und Ereignisse in MISPzu erstellen und zu aktualisieren.

Erste Schritte mit MISP integration for Security Operations

Lesen Sie sich die folgenden Informationen durch, bevor Sie MISP integration for Security Operationseinrichten.

Prüfliste

Setupaufgabe	Beschreibung
Vergewissern Sie sich, dass die erforderlichen Rollen Now Platform, Threat Intelligenceund Security Incident Response zugewiesen wurden.	Die folgenden Rollen werden für die -Funktionen von MISP in Now Platformverwendet: • Der -Administrator (admin) installiert die Anwendungen aus ServiceNow Store und weist die Rollen Security Incident-Administrator (sn_si.admin) und Threat Intelligence-Administrator (sn_ti.admin) zu. • sn_si.admin und sn_ti.admin können die Integration konfigurieren und die Profile für die automatische Erstellung von MISP -Ereignissen einrichten. • sn_sec_misp.write: Die Analystenrolle MISP verfügt über Lese- und Schreibberechtigungen für Daten MISP, einschließlich der Ereignis- und Attributdaten. Weitere Informationen finden Sie unter Threat Intelligence einrichten.
Weisen Sie die erforderlichen MISP Anwenderrollen zu.	Überprüfung des folgenden Elements: MISP Rollen und Berechtigungen, die für die Verwendung von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	erforderlich sind MISP integration for Security Operations. **Hinweis:** Weitere Informationen zu den Anwenderrollen in MISPfinden Sie im Abschnitt „Rollen“ auf der MISP-Dokumentationswebsite .
Stellen Sie sicher, dass Sie MISP Version 2.4.137 oder höher verwenden.	MISP integration for Security Operations wird mit mindestens getestet MISP Version 2.4.137 .
Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung des Moduls MISP erforderlich sind, installiert und aktiviert sind.	Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. • Security Incident Response • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) • ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) Weitere Informationen zum Einrichten Ihrer Instanz Now Platform für die Integration finden Sie unter Berechtigungen für ein Produkt oder eine Anwendung von Security Operations erhalten und eine ServiceNow Store-Anwendung aktivieren.
Domänentrennung	Überprüfen Sie den Abschnitt zur Domänentrennung, wenn Sie Daten, Prozesse und administrative Aufgaben trennen möchten.

MISP Anwenderrollen und Berechtigungen

Überprüfen Sie die Anwenderrollen, die in der Integration MISP integration for Security Operations erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anreicherung erkennbarer Elemente und Berechtigungen für die Sichtungssuche

Hinweis:

- *Alle* **ServiceNow** *MISP-Integrationsfunktionen benötigen die Standardberechtigungen für* **die Verwaltung von Organisationsereignissen** *und* **den Zugriff auf Auth-Schlüssel**. *Stellen Sie sicher, dass Sie über diese grundlegenden Berechtigungen verfügen, bevor Sie fortfahren.*
- *Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert, zur Hostorganisation des entsprechenden MISP-Servers gehören.*

MISP-Fähigkeit	Tagger	Tag-Editor
Anreicherung erkennbarer Elemente (schreibgeschützt)	#	#
Sichtungssuche (schreibgeschützt)	#	#

Sichtungsberechtigungen für Berichte

MISP-Fähigkeit	Sichtungsersteller
Sichtung melden	#

Attribut- und Ereignisberechtigungen

MISP-Fähigkeit	Tagger	Tag-Editor
Bearbeiten Sie Ereignis-/Attribut-Tags	#	#
Ereignis-/Attribut-Galaxien bearbeiten	#	#
Attributkommentare bearbeiten	#	#
Fügen Sie dem Ereignis ein neues Attribut hinzu	#	#
Erstellt ein Ereignis in MISP	#	#

Installieren und konfigurieren Sie den MISP integration for Security Operations

Installieren und konfigurieren Sie MISP integration for Security Operations über ServiceNow Store in Ihrer Instanz Now Platform, damit Sie Security Incidents anhand der Daten von MISP untersuchen können.

Vorbereitungen

Stellen Sie sicher, dass Sie gültige SSL-Zertifikate auf dem MISP-Server installiert haben.

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie MISP integration for Security Operations von ServiceNow Store herunter, und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel MISP -SIR/TI-Integration, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

MISP Formular „SIR/TI-Integrationskonfiguration“.

Feld	Beschreibung
Name	Name für die Konfiguration der Instanz MISP
MISP Server-URL	URL für den Server MISP, die als REST-Endpunkt für den Server MISP dient.
API-Schlüssel	API-Schlüssel, der für Ihr Benutzerkonto auf dem Server MISP konfiguriert ist. Der API-Schlüssel entspricht dem **Authkey** auf dem Server MISP.
Lokale Bereitstellung	Option, die Sie auswählen können, wenn Ihr -Server MISP in einer lokalen Instanz bereitgestellt wird. Wenn Sie die Option **Lokale Bereitstellung** auswählen, müssen Sie den MID-Server verwenden, um eine Verbindung zum Server MISP herzustellen.
MID-Anwendung	Zeichenfolgenfeld, das den MID-Anwendungsnamen identifiziert, der für die Kommunikation mit MISPverwendet wird. Dieses Feld ist erforderlich, wenn Sie die Option **Lokale Bereitstellung** auswählen. Informationen zur Konfiguration des MID-Servers für Ihre Anwendung finden Sie unter MID-Server für jede Anwendung konfigurieren

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird MISP – SIR/TI-Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Überprüfen Sie die Integrationseinstellungen für MISP .

Überprüfen Sie die MISP integration for Security Operations -Einstellungen, und ändern Sie die Standardsystemeigenschaften entsprechend Ihrer Umgebung.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Integrationseinstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MISP-Integrationseinstellungen

Eigenschaftsname		Beschreibung
Ergänzung erkennbarer Elemente	Zeit (in Stunden) bis zum Abrufen neuer Daten	Zeit in Stunden, bis Sie neue Daten abrufen können. Typ: Ganzzahl Standardwert: 24
Sichtungssuche	Führt automatisch eine Sichtungssuche aus, wenn dem Security Incident neue erkennbare Elemente zugeordnet werden	Sichtungssuche, die ausgeführt wird, wenn ein neues erkennbares Element einem Security Incident zugeordnet wird. Standardwert: Ja
	Suchintervall (in Tagen) für die Sichtungssuche in MISP	Anzahl der Tage, an denen die Sichtungssuchdaten in MISPdurchsucht werden. Verwenden Sie diese Option nur für die automatische Sichtungssuchfunktion. Standardwert: 90
Datensynchronisierung	Intervallzeitraum (in Minuten) für Tags, die abgerufen und mit MISP synchronisiert werden sollen	MISP Tags, die zum Zeitpunkt der Integrationskonfiguration abgerufen werden. Nachdem sich die Daten im Now Platformbefinden, definiert diese Eigenschaft die Häufigkeit, mit der die Daten mit dem Server MISP synchronisiert werden. Der Wert wird in Minuten definiert. Standardwert: 1440 (Minuten oder 24 Stunden)
	Intervallzeitraum (in Minuten) zum Aktualisieren von MISP-Galaxien aus konfigurierten Quellen	MISP Galaxien, die zum Zeitpunkt der Integrationskonfiguration abgerufen werden. Nachdem sich die Daten im Now Platformbefinden, definiert diese Eigenschaft die Häufigkeit, mit der die Daten mit dem Server MISP synchronisiert werden. Der Wert wird in Minuten definiert. Standardwert: 1440 (Minuten oder 24 Stunden)
	Intervallzeitraum (in Minuten) für Organisationen, die abgerufen und	MISP Organisationen, die zum Zeitpunkt der Integrationskonfiguration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname		Beschreibung
	mit MISP synchronisiert werden sollen	abgerufen werden. Nachdem sich die Daten im Now Platformbefinden, definiert diese Eigenschaft die Häufigkeit, mit der die Daten mit dem Server MISP synchronisiert werden. Der Wert wird in Minuten definiert. Standardwert: 1440 (Minuten oder 24 Stunden)
MITRE™ Extraktionstechnik	Führt ein automatisches Rollup von Techniken MITRE-ATT&CK aus MISP-Datenanreicherungs-Ergebnissen erkennbarer Elemente (Tags) zu Security Incidents durch	Rollup von MITRE-ATT&CK Informationen aus MISP Ergänzungsergebnissen erkennbarer Elemente (Tags) zum Security Incident Standardwert: Ja
	Führt einen automatischen Rollup von MITRE-ATT&CK -Techniken aus MISP-Datenanreicherungs-Ergebnissen erkennbarer Elemente (Galaxien) zu Security Incidents durch	Rollup von MITRE-ATT&CK -Informationen aus den MISP -Ergänzungsergebnissen erkennbarer Elemente (Galaxien) für den Security Incident. Standardwert: Ja

Hinweis:

- Um die MITRE™ -Technikextraktionsfunktionen in MISPzu verwenden, müssen Sie aktivieren Sie die MITRE-ATT&CK Funktion in Threat Intelligence Modul.
- Mit MISP integration for Security Operations werden zwei Basissystem-Extraktionsregeln für die MITRE-ATT&CK -Technik für MISP - MISP - Galaxien und MISP -Tags eingeführt. Weitere Informationen zu automatischen Extraktionsregeln in MITRE-ATT&CKfinden Sie unter Technikregeln für automatisches Extrahieren für den Import von MITRE-ATT&CK-Informationen.

3. Klicken Sie auf **Speichern**.

Ergebnisse

Ihre geänderten Integrationseinstellungen werden gespeichert und angewendet.

Konfigurieren Sie MISP Sichtungssuchen

Konfigurieren Sie Now Platform, um Sichtungssuchen nach erkennbaren Elementen in der Instanz MISP durchzuführen. Mit diesen Informationen können Sie bestimmen, wie häufig Bedrohungen auftreten.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen die für die Verwendung der bidirektionalen MISP -Funktionen erforderlich sind.
- Erforderliche Rolle: sn_si.admin, sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow „Security Operations Integration - Sichtungssuche“ führt die Sichtungssuchen aus. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, sucht nach implementierenden Fähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchen aus, die auf dem konfigurierten Workflow basieren.

MISP integration for Security Operations stellt ein Sichtungssuchprofil für das Basissystem bereit, mit dem Sie automatische Sichtungssuchen konfigurieren können. Mit diesem Profil können Sie auf die zugehörigen Sichtungsinformationen für erkennbare Elemente einer Organisation zugreifen und auch die externen Sichtungen anderer Organisationen anzeigen.

Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Sichtungssuche: Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Konfigurationen für Sichtungssuche“.

Feld	Beschreibung
Name	Name des Fähigkeitsprofils.
Ist gespeicherte Suche	Suchkonfiguration, die gespeichert wird, wenn Sie diese Option auswählen. Die gespeicherten Suchkonfigurationsabfragen sind Beispielabfragen. Sie können sie durch die Parameter für Ihre Umgebung ersetzen und bei Bedarf zusätzliche gespeicherte Suchkonfigurationen erstellen.
Sichtungssuchquelle	Quelle für die Sichtungssuche. Wählen Sie den Protokollspeicher MISP als Quelle aus.
Aktiv	Mit dieser Option wird die gespeicherte Suchkonfiguration aktiviert. Nur aktive Suchkonfigurationen können eine Sichtungssuche durchführen.
Erkennbarer Typ	Typ erkennbarer Elemente wie IP-Adresse, Hash-Wert, URL und Domänenname.
Maximales erkennbares Element pro Suche	Maximale Anzahl erkennbarer Elemente, die Sie in einer Suchabfrage anzeigen können.
Suchen	Standardsuchzeichenfolge, die `$(observable)` ist. Sie definieren jedoch Ihre eigene Suchabfrage, indem Sie die vom Protokollspeicher MISP unterstützten Parameter angeben.

4. Klicken Sie auf **Absenden**.

Ergebnisse

Sie haben ein Konfigurationsprofil für die Sichtungssuche MISP erstellt.

Konfigurieren Sie, wie ein automatisches Event erstellt wird

Konfigurieren Sie Now Platform so, dass automatisch Ereignisse in MISPerstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen die für die Verwendung der bidirektionalen MISP -Funktionen erforderlich sind.
- Erforderliche Rolle: sn_si.admin, sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Profile für die automatische Erstellung von Ereignissen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Namensformular

Feld	Beschreibung
Name	Name des Profils zur automatischen Ereigniserstellung.
Beschreibung	Kurze Beschreibung des Profils. Eine detailliertere Beschreibung wird durch die Attribute in der nächsten Phase der Ereigniserstellung geteilt.
Bestellung	Reihenfolge des Profils, wenn Auslösebedingungen erfüllt sind. Der Standardwert ist 100. Belassen Sie diese Einstellung auf dem Standard. Wenn Sie mehrere Profile erstellen, bietet dieser Wert eine Laufzeit-Ausführungspriorität, wenn zwei oder mehr Profile auslösende Bedingungen gemeinsam nutzen. Das Profil mit der niedrigsten Nummer hat die höchste Priorität.
Quelle	MISP Quelle für die Ereigniserstellung.
Aktiv	Option, die angibt, ob das Profil aktiv oder inaktiv ist. Standardmäßig ist die Option deaktiviert, um anzuzeigen, dass das Profil deaktiviert ist. Dieses Profil ist erst aktiv, wenn Sie alle Profilkonfigurationsschritte abgeschlossen haben und auf **„Fertigstellen“**klicken.

4. Klicken Sie auf **Fortsetzen**.

Konfigurieren Sie Bedingungen für die Auslösung von Ereignissen

Konfigurieren Sie die Auslösebedingungen für Ereignisse in Now Platform, damit Sie automatisch ein Ereignis in MISP auslösen können, wenn die Bedingungen erfüllt sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Füllen Sie im Formular „Auslösebedingungen“ die Details aus, die ein Ereignis auslösen können. Sie können eine zusammengesetzte Logik erstellen, indem Sie die Auslöserbedingungen angeben, die auf Feldern für Security Incidents oder erkennbaren Elementen basieren. Sie können auch Ereignisse in MISP erstellen, wenn erkennbare Elemente kein entsprechendes Ereignis in MISPhaben. Sie können eine zusammengesetzte Logik erstellen, indem Sie eine Kombination der drei Auslöserbedingungen verwenden – Auslöser basierend auf Feldern von Security Incidents, Auslöser basierend auf Feldern erkennbarer Elemente und MISP-Ereignis erstellen, wenn ein erkennbares Element keine entsprechenden Ereignisse in MISP enthält. Wenn Sie mehrere Auslöser auswählen, können Sie sie mithilfe der UND-Bedingung verbinden. Erwägen Sie das Erstellen eines Profils mit neuen Bedingungen, wenn Sie die ODER-Bedingung verwenden müssen.

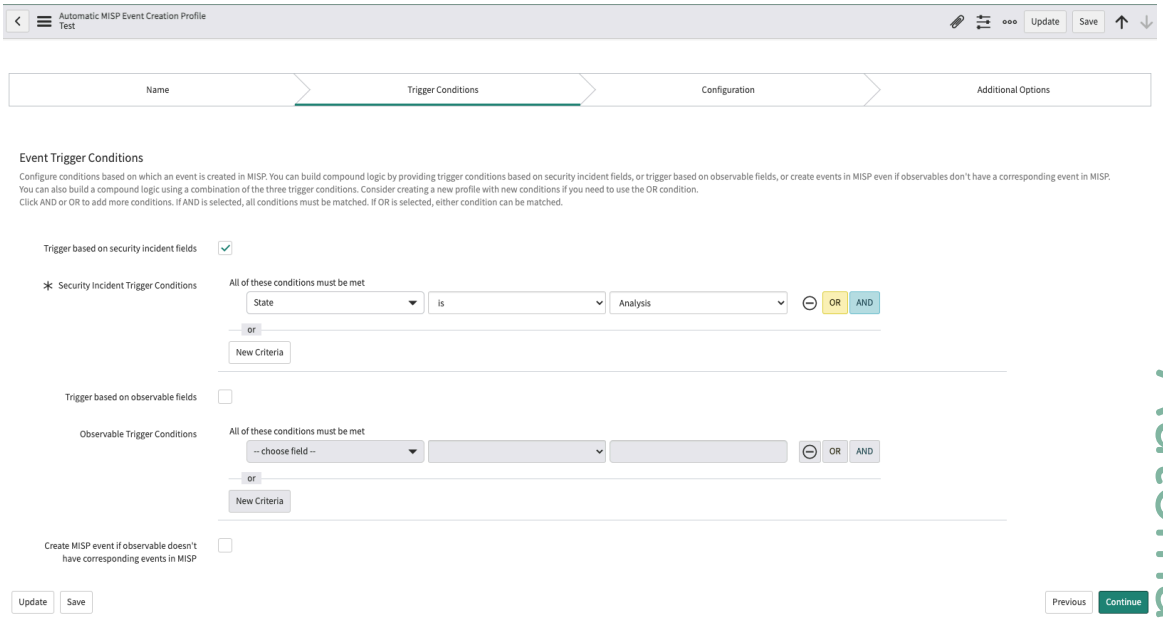
Formular „Ereignisauslösebedingungen“.

Feld	Beschreibung
Auslöser basierend auf Security Incident-Feldern	MISP Ereignis, das Sie erstellen können, wenn alle Auslösebedingungen für Security Incidents erfüllt sind.
Auslösebedingungen für Security Incident	Filter in der ersten Zeile, die Sie mithilfe der Listen und Felder des Bedingungsgenerators festlegen können. Um weitere Bedingungen hinzuzufügen, klicken Sie auf AND oder OR. Wenn AND ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn ODER ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.
Auslöser basierend auf erkennbaren Feldern	MISP Ereignis, das Sie erstellen können, wenn alle Auslöserbedingungen für erkennbare Elemente erfüllt sind.
Auslösebedingungen für erkennbare Elemente	Filter in der ersten Zeile, die Sie mithilfe der Listen und Felder des Bedingungsgenerators festlegen können. Um weitere Bedingungen hinzuzufügen, klicken Sie auf AND oder OR. Wenn AND ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn ODER ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.
Erstellen Sie ein MISP-Ereignis, wenn das erkennbare Element keine entsprechenden Ereignisse in MISP enthält.	MISP Ereignis, das Sie erstellen können, wenn ein erkennbares Element keine entsprechenden Ereignisse in MISPhat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auslösebedingungen für Ereignisse

Das folgende Beispiel zeigt die Bedingungen für den Auslöser des Ereignisses beim Einrichten des Profils MISP zur Erstellung des Ereignisses.



2. Klicken Sie auf **Fortsetzen**.

Ordnen Sie die Ereignisfelder MISP zu

Ordnen Sie die Ereignisfelder MISP in Now Platform zu, damit Informationen zu Security Incidents verfügbar sind, wenn Ereignisse MISP vom Typ erstellt werden.

Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Füllen Sie die Felder des Formulars aus.

Standardmäßiges Feldzuordnungsformular für MISP-Ereignis

Feld	Beschreibung
Information zum Ereignis	Ereignisinformationen, die automatisch aus dem Now Platform Security Incident Responseerstellt werden. Das Feld **„Ereignisinformationen“** unterstützt Substitutionsvariablen durch Verwendung von ${SIR FIELD LABEL}$. Während der Erstellung eines Ereignisses werden diese Variablen durch die tatsächlichen Feldwerte des Security Incidents ersetzt. Die Substitutionsvariable ${URL}$ wird durch die URL des Security Incident ersetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

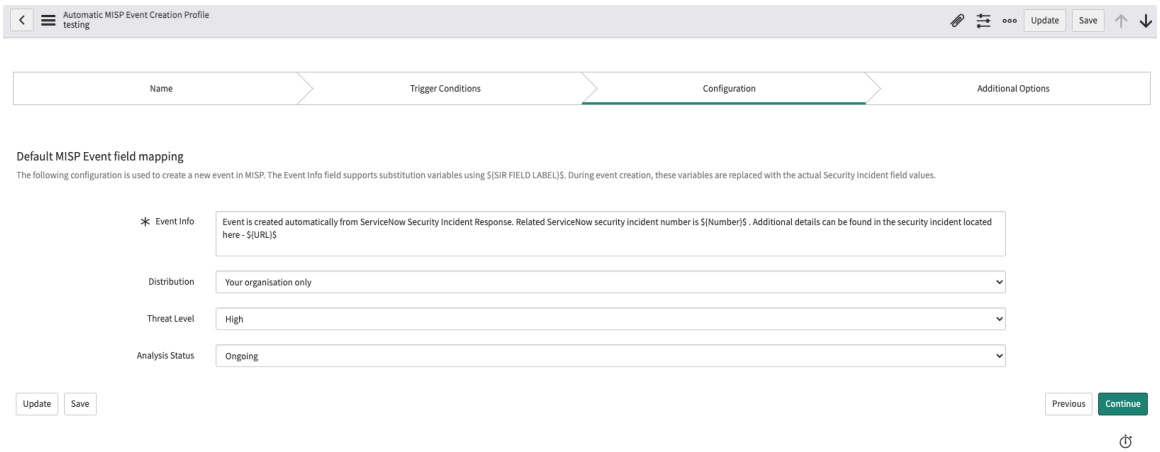
Feld	Beschreibung
Verteilung	Option, die steuert, wer dieses Ereignis anzeigen kann, nachdem das Ereignis veröffentlicht wurde. Diese Option steuert auch, ob das Ereignis mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen geerbt, und die restriktivste Einstellung gewinnen. Die Verteilungsoptionen lauten wie folgt: ○ Nur Ihre Organisation: Ermöglicht nur Mitgliedern Ihrer Organisation, dieses Ereignis anzuzeigen. Das Ereignis kann von einem Ihrer Organisationsmitglieder in eine andere Instanz verschoben werden, in der nur Ihre Organisation darauf zugreifen kann. Ereignisse mit dieser Einstellung werden nicht synchronisiert. ○ Nur diese Community: Ermöglicht Anwendern, die Teil Ihrer MISP -Community sind, einschließlich Ihrer eigenen Organisation, von Organisationen auf diesem MISP -Server und von Organisationen, die MISP -Server ausführen, die mit diesem Server synchronisiert werden, das Ereignis anzuzeigen. Alle anderen Organisationen, die eine Verbindung zu Ihren Verbindungsservern herstellen, können das Ereignis nicht anzeigen. ○ Verbundene Communities: Ermöglicht Anwendern, die Teil Ihrer Community MISP sind, das Ereignis anzuzeigen, einschließlich aller Organisationen auf diesem Server MISP, aller Organisationen auf den Servern MISP, die mit diesem Server synchronisiert werden, und der Hosting-Organisationen von Servern, die eine Verbindung zu einem beliebigen Server herstellen das ist zwei Hops entfernt. Alle anderen Organisationen, die mit den zwei Hops entfernten Verbindungsservern verbunden sind, können das Ereignis nicht anzeigen. ○ Alle Communities: Gibt das Ereignis für alle MISP -Communitys frei.
Bedrohungsstufe	Feld, das die Risikostufe des Ereignisses angibt. Sie können Incidents in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) einteilen. Dieses Feld kann auch als undefiniert belassen werden. Die folgenden Optionen stehen zur Verfügung:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Niedrig: Allgemeine Massen-Malware ○ Mittel: Advanced Persistent Threats (APT) ○ Hoch: Ausgereifte APTs und 0-Tage-Angriffe
Analysestatus	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: ○ Anfänglich: Die Analyse beginnt gerade erst ○ Laufend: Die Analyse wird ausgeführt ○ Abgeschlossen: Die Analyse ist abgeschlossen

Das folgende Beispiel zeigt das Formular, mit dem Sie ein Ereignis in MISP erstellen können.

Standardmäßige MISP-Ereignisfeldzuordnung



2. Klicken Sie auf **Fortsetzen**.

Ordnen Sie SIR erkennbare Elemente als Attribute zu MISP -Ereignissen zu oder ordnen Sie sie zu

Ordnen Sie die erkennbaren Elemente Security Incident Response den Attributtypen MISP zu, da die Attributtypen MISP und die erkennbaren Elemente SIR unterschiedlich sein können.

Vorbereitungen
Erforderliche Rolle: sn_sec_misp.write

Warum und wann dieser Vorgang ausgeführt wird
MISP integration for Security Operations stellt eine Basissystemzuordnung bereit, die Sie verwenden, wenn Sie erkennbare Elemente SIR als Attribute zu einem Ereignis MISP hinzufügen.

Sie können die Basissystemzuordnung an Ihre Umgebung anpassen. Beispielsweise können Sie mehrere SIR erkennbare Elemente nur einem MISP Attributtyp zuordnen. Wenn keine erkennbaren Typen zugeordnet sind, wird standardmäßig der **andere** MISP Attributtyp ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

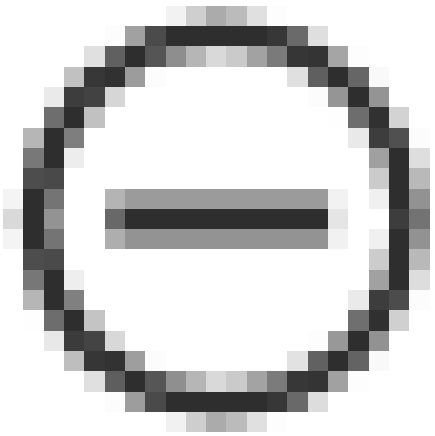
Prozedur

1. Ordnen Sie im Formular „Zusätzliche Optionen“ die Attributtypen SIR erkennbares Element und MISP zu.
2. Ordnen Sie die erkennbaren Elementtypen Security Incident Response den Attributtypen MISP zu, wie in der folgenden Tabelle beschrieben.

Zuordnung von erkennbarem SIR- und MISP-Attributtyp

Feld	Beschreibung
Alle zugehörigen erkennbaren Elemente als Attribute hinzufügen	Option zum Hinzufügen verfügbarer erkennbarer Elemente in einem Security Incident zu einem MISP -Ereignis als Attribute. Diese Option aktiviert die Zuordnung im Abschnitt „Zuordnung von erkennbarem Elementtyp zu Attributtyp“.
Zuordnung erkennbarer Elemente zu Attributtyp	Option zum Zuordnen der erkennbaren Elemente SIR zu den Attributtypen MISP. Sie können beispielsweise die CVE-Nummer in SIR dem Schwachstellenattribut in MISPzuordnen. Sie können einen erkennbaren Elementtyp SIR nur einem einzigen MISP -Attributtyp hinzufügen. Das Basissystem bietet eine Zuordnung der erkennbaren Elemente SIR zu den Attributtypen MISP. Wenn erkennbare SIR -Typen keinem Attributtyp MISP zugeordnet sind, wird das erkennbare Element dem **anderen** Attributtyp in MISPzugeordnet. Um eine neue Zuordnung hinzuzufügen, klicken Sie auf **Add Observable Type (Erkennbaren Typ hinzufügen)**, suchen Sie nach dem erkennbaren Elementtyp SIR, und ordnen Sie ihn dann dem entsprechenden Attributtyp MISP zu. Klicken Sie auf das Symbol Zuordnung entfernen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

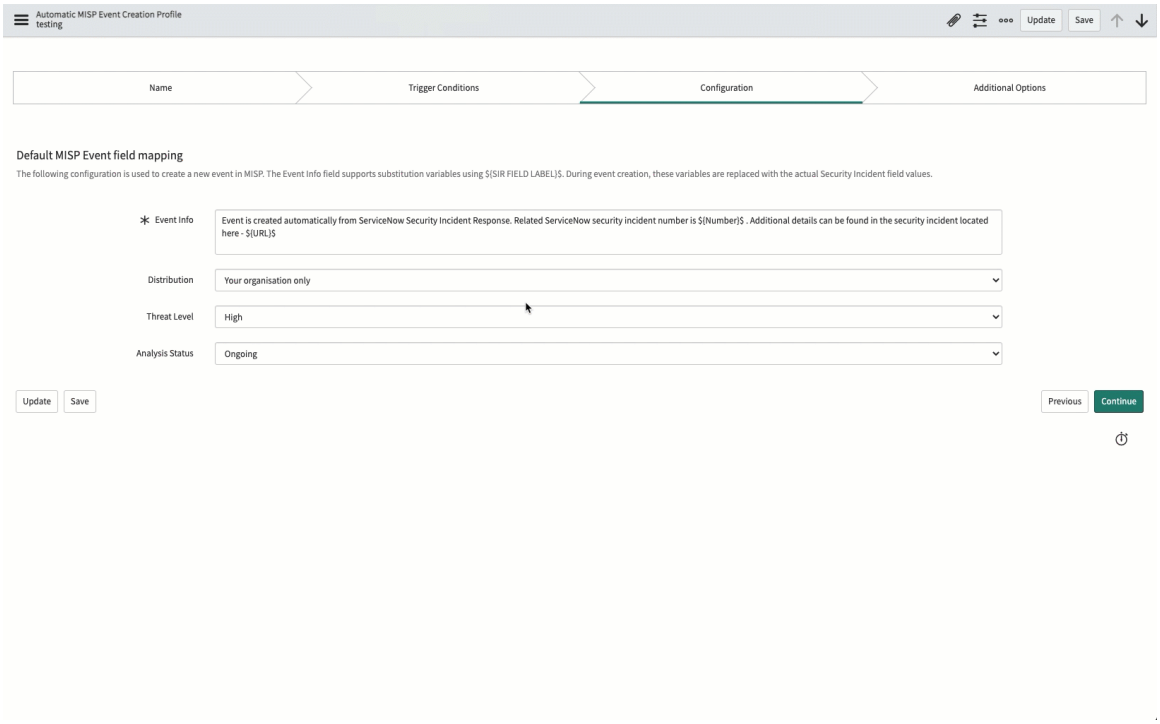
Feld	Beschreibung
	 um die Zuordnung der Attributzuordnung SIR und MISP zu entfernen. **Hinweis:** Weitere Informationen zu Attributtypen MISP finden Sie in der MISP-Dokumentation .
Erkennbare Elemente anhand von Sicherheits-Tags filtern	Option zum Filtern der erkennbaren Elemente basierend auf den ausgewählten Sicherheits-Tags. **Sicherheits-Tags**: Fügen Sie Tags hinzu, um die erkennbaren Elemente zu filtern. Wenn Sie beispielsweise ein Tag mit der Bezeichnung „Freigabe blockieren“ oder „TLP: White“ hinzufügen, werden diese erkennbaren Elemente, wenn eines der erkennbaren Elemente mit einem dieser Tags verknüpft ist, dem MISP-Ereignis während des MISP nicht als Attribut hinzugefügt Ereigniserstellung.
Legen Sie die Attribut-IDS-Kennzeichnung fest, wenn die Erkennung von erkennbaren Elementen schädlich ist.	Option, die Sie darüber informiert, dass, wenn ein erkennbares Element in SIRals schädlich markiert ist, für das entsprechende Attribut in MISP die IDS-Kennzeichnung aktiviert ist. Wenn die IDS-Kennzeichnung nicht festgelegt ist, gilt das Attribut als kontextbezogene Information und wird nicht für die automatische Angriffserkennung verwendet.

Das folgende Beispiel zeigt, wie Sie zur Seite mit zusätzlichen Optionen navigieren. Auf dieser Seite können Sie die Zuordnung von erkennbaren SIR-Elementen und MISP-Attributtypen aktivieren, neue erkennbare Elementtypen SIR hinzufügen, z. B. das IPV6-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerk und das IPV4-Netzwerk, und sie der Domänen-IP-Adresse des Attributtyps MISP zuordnen.

Zuordnung von SIR erkennbaren Elementen und MISP Attributtypen



Synchronisieren Sie MITRE-ATT&CK -Informationen mit MISP -Ereignissen

Synchronisieren Sie die MITRE-ATT&CK -Informationen mit MISP den -Attributen, um Security Incidents und Bedrohungsanalysen zu verbessern.

Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

Prozedur

Überprüfen Sie im Formular „Zusätzliche Optionen“ die Optionen zum Synchronisieren der MITRE-ATT&CK -Informationen mit den MISP -Attributen.

Formular „Erweiterte Optionen“

Feld	Beschreibung
Techniken des Security Incident MITRE-ATT&CK™ als lokale Galaxien im Ereignis MISP synchronisieren	Option zum Synchronisieren der Now Platform SIR Security Incident-Techniken MITRE-ATT&CK™ als lokale Galaxien im Ereignis MISP. **Hinweis:** Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert hat, zur Hostorganisation des entsprechenden Servers MISP gehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Techniken des Security Incident MITRE-ATT&CK™ als globale Galaxien im Ereignis MISP synchronisieren	Option zum Synchronisieren der Now Platform SIR Security Incident-Techniken MITRE-ATT&CK™ als globale Galaxien im Ereignis MISP.

Ergebnisse
Sie haben ein Profil erstellt, mit dem Sie automatisch Ereignisse in MISP über Now Platformerstellen können. Sie können jetzt die Ereignisse in der zugehörigen Liste „Zugeordnete MISP-Ereignisse“ anzeigen.

Fügen Sie Ereignissen MISP-Tags hinzu

Fügen Sie den erstellten MISP-Ereignissen MISP-Tags hinzu.

Vorbereitungen
Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren Sie im Formular „Zusätzliche Optionen“ zu **MISP-Tags auswählen, die dem Ereignisabschnitt in der Formularansicht hinzugefügt werden sollen**.
2. Überprüfen Sie die Optionen zum Hinzufügen von Tags zu den erstellten Ereignissen.

Formular „Erweiterte Optionen“

Feld	Beschreibung
Erstelltem MISP-Ereignis Tags hinzufügen	Option zum automatischen Hinzufügen von MISP-Tags zu Ereignissen, die in ServiceNow erstellt werden.
Tags (lokal)	Die ausgewählten Tags werden dem MISP-Ereignis als lokale Tags hinzugefügt.
Tags (global)	Die ausgewählten Tags werden dem MISP-Ereignis als globale Tags hinzugefügt.

3. Klicken Sie auf **Speichern**.

Ergebnisse
Das Hinzufügen von MISP-Tags hilft bei der Klassifizierung des Ereignisses.

MISP Ereignisdaten

Sie können die MISP -Ereignisdaten überprüfen, um detaillierte Informationen zu den MISP -Ereignissen anzuzeigen.

MISP Ereignisdaten in der Listenansicht

Greifen Sie auf die Listenansicht über zu **MISP** > **MISP-Ereignis-Daten**.

Verwenden Sie die Listenansicht, um eine schnelle Übersicht über die MISP Ereignisdaten zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listenansicht „MISP-Ereignisse“.

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die von MISP zugewiesen wird, wenn das Ereignis zum ersten Mal auf dem Server MISP erstellt oder importiert wurde.
Information	Kurze Beschreibung des Ereignisses.
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: • Anfänglich: Die Analyse beginnt gerade erst • Laufend: Die Analyse wird ausgeführt • Abgeschlossen: Die Analyse ist abgeschlossen
Bedrohungsstufe	Risikostufe des Ereignisses. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) eingeteilt werden. Dieses Feld kann als nicht definiert gelassen werden. Die folgenden Optionen stehen zur Verfügung: • Niedrig: Allgemeine Massen-Malware • Mittel: Advanced Persistent Threats (APT) • Hoch: Ausgereifte APTs und 0-Tage-Angriffe
MISP-Tags	Tags, die dem Ereignis MISP zugeordnet sind.
MISP-Galaxien	Galaxien, die dem Ereignis MISP zugeordnet sind.
Besitzerorganisation	Organisation, die das Ereignis in der Instanz MISP besitzt. Dieses Feld ist nur für Administratoren sichtbar.
Erstellerorganisation	Organisation, die das Ereignis in der Instanz MISP erstellt hat.
Verteilung	Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis.
MISP-Ereignis-Hyperlink	Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.

MISP Ereignisdaten in der Formularansicht

Verwenden Sie die Formularansicht, um detaillierte Informationen zu den MISP -Ereignissen zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularansicht „MISP-Ereignis“.

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die von MISP zugewiesen wird, wenn das Ereignis zum ersten Mal auf dem Server MISP erstellt oder importiert wurde.
UUID	ID, die Ereignisse und Attribute eindeutig identifiziert.
Erstellerorganisation	Organisation, die das Ereignis in der Instanz MISP erstellt hat.
Besitzerorganisation	Organisation, die das Ereignis in der Instanz MISP besitzt. Dieses Feld ist nur für Administratoren sichtbar.
Erstelleranwender	Anwender, der das Ereignis in MISPerstellt hat.
Letzter Change	Datum, an dem das Ereignis zuletzt geändert wurde.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.
Erstellungsdatum (in MISP)	Datum, an dem das Ereignis erstellt oder zuerst auf den Server MISP importiert wurde.
Bedrohungsstufe	Risikostufe des Ereignisses. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) eingeteilt werden. Dieses Feld kann als nicht definiert gelassen werden. Die folgenden Optionen stehen zur Verfügung: • Niedrig: Allgemeine Massen-Malware • Mittel: Advanced Persistent Threats (APT) • Hoch: Ausgereifte APTs und 0-Tage-Angriffe
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: • Anfänglich: Die Analyse beginnt gerade erst • Laufend: Die Analyse wird ausgeführt • Abgeschlossen: Die Analyse ist abgeschlossen
Verteilung	Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis.
Veröffentlicht	Status, ob das Ereignis veröffentlicht wurde oder nicht. Durch die Veröffentlichung können die Attribute des Ereignisses für alle berechtigten Exporte verwendet werden, und es werden Anwender benachrichtigt, die die Ereigniswarnungen abonniert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularansicht „MISP-Ereignis“. (Fortsetzung)

Feld	Beschreibung
MISP-Ereignis-Hyperlink	Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist.
Information	Kurze Beschreibung des Ereignisses.
Tags (lokal)	Tags, die in der Instanz MISP der Hostorganisation verfügbar sind, um Tagging für die Synchronisierungs- und Exportfilterung zu aktivieren. MISP Ereignisse werden nicht geändert, wenn Sie lokale Tags verwenden. Lokale Tags werden vor der Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communitys immer entfernt.
Tags (global)	Tags, die global für die Freigabe und Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communities verfügbar sind. Wenn Sie Instanzen MISP globale Tags hinzufügen, können Sie Ereignisse ändern.
Galaxien (lokal)	Galaxien, die in der Instanz MISP der Hostorganisation für die Synchronisierung und Exportfilterung verfügbar sind. MISP Ereignisse werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese lokalen Galaxien werden immer entfernt, bevor sie mit anderen MISP -Instanzen und Freigabe-Communitys synchronisiert werden.
Galaxien (global)	Galaxien, die global für die Freigabe und Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communitys verfügbar sind. Wenn Sie globale Galaxien hinzufügen, MISP, können Sie Ereignisse ändern.

Zugeordnete MISP Ereignisse

Sie können die zugeordnete Ereignislistenansicht MISP verwenden, um die Ereignisse anzuzeigen, die manuell oder automatisch im Kontext eines Security Incident erstellt wurden.

Zugeordnete MISP-Ereignisse

Feld	Beschreibung
Security Incident	SIR Security Incident. Klicken Sie auf den Security Incident, um ihn anzuzeigen.
MISP-Ereignis	MISP Ereignis-ID. Klicken Sie auf das Ereignis MISP, um das Ereignis MISP in Now Platformanzuzeigen.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugeordnete MISP-Ereignisse (Fortsetzung)

Feld	Beschreibung
	Klicken Sie auf die Quelle MISP, um die Quelle anzuzeigen.
Ereigniserstellungsmodus	Status, der angibt, ob das Ereignis manuell oder automatisch mit dem Ereigniserstellungsprofil erstellt wurde. Klicken Sie auf das Ereignis MISP, um das zugehörige Ereignis MISP anzuzeigen.
Profil für die automatische Erstellung von Ereignissen	Ereigniserstellungsprofil, das zum Erstellen des automatischen Ereignisses verwendet wird. Klicken Sie auf das Profil, um das Profil für die automatische Erstellung von MISP-Ereignissen anzuzeigen.

MISP Benutzerinformationen

Sie können die -Benutzerinformationsseite MISP verwenden, um alle zugeordneten Benutzer für Now Platform MISP integration for Security Operationsanzuzeigen.

MISP-Anwenderinformationen

Feld	Beschreibung
Quelle	Quelle MISP des Anwenderaccounts.
Anwender-ID	Anwender-ID, die vom Server MISP zugewiesen wird, wenn ein Anwenderaccount erstellt wird.
Anwender-E-Mail	E-Mail-Adresse eines Anwenders. Nur Organisationsadministratoren können die E-Mail-Adressen der Benutzer ihrer eigenen Organisation anzeigen.
Organisation	Organisation, der ein Anwender angehört.
Rollenname	Rollenname, der die Anwenderberechtigungen definiert, die einem Anwender zugeordnet werden. Weitere Informationen zu Rollen in MISPfinden Sie in der MISP-Dokumentation .
Rollen-ID	Anwenderrollen-ID in MISP. Zum Beispiel „Perm Admin“, „Perm Audit“ oder „Perm Tagger“ usw.
Berechtigung	Berechtigungen, über die ein Benutzer verfügt. Folgende Berechtigungen sind in MISP verfügbar: • Schreibgeschützt • Eigene Ereignisse verwalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MISP-Anwenderinformationen (Fortsetzung)

Feld	Beschreibung
	• Verwalten Sie Organisationsereignisse • Verwalten Sie Ereignisse zum Veröffentlichen von Organisationen
Sichtungsberechtigung	Berechtigung, die es einem Anwender ermöglicht, Sichtungssuchen durchzuführen.
Tagger-Berechtigung	Berechtigung, die einem Anwender Tagging ermöglicht.

Domain Separation und MISP

Die Domänentrennung wird in MISP unterstützt. Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe

Support: Standard.

So funktioniert Domain Separation mit MISP

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit den erforderlichen Rollen in Ihrer Domäne.
- Führen Sie die Verfahren MISP integration for Security Operations in Ihrer Domäne aus.

Problembehandlung bei der MISP-Integration

Dieser Abschnitt enthält wichtige Tipps zur Problembehandlung, die Ihnen helfen können, häufige Probleme zu beheben, die beim Einrichten oder Ausführen der MISP-Integration auftreten können.

SSL-Probleme

Wenn Sie eine Verbindung über die MISP-Integration herstellen, stellen Sie sicher, dass Sie ein gültiges CA-Zertifikat auf dem MISP-Server installiert haben, das nicht abgelaufen ist. Sie können RSA-Zertifikate oder eigene Zertifikate in die Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie den MISP integration for Security Operations und MISP Anwenderrollen und Berechtigungen.

MISP zum Untersuchen und Analysieren von Bedrohungen verwenden

Sie können die Daten MISP im gesamten Modul Now Platform Threat Intelligence und im Modul Now Platform SIR verwenden, um Bedrohungen für Ihre Organisation zu untersuchen und zu analysieren.

Sichtungssuchen in MISP

Sie können Sichtungssuchen für erkennbare Elemente in der Instanz MISP durchführen, um zu bestimmen, wie häufig bestimmte Arten von Angriffen, z. B. Phishing-Angriffe oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kommunikation mit einer schädlichen IP oder URL, in Ihrem Netzwerk auftreten. Jedes Auftreten gilt als Sichtung.

Sichtungen in MISP

Sichtungen geben an, dass ein Indikator, ein Objekt oder ein Attribut gesehen wurde und dessen Gültigkeit bestätigt wird. Sichtungen in MISP sind ein System, mit dem Sie auf Attribute für ein Ereignis reagieren können. Es soll Ihren Anwendern eine einfache Methode bieten, um zu bestätigen, dass sie ein bestimmtes Attribut gesehen haben, wodurch es glaubwürdiger wird. Sie können ein Attribut mehrmals sichten.

Hinweis:
Erkennbare Elemente werden in MISP als Attribute bezeichnet.

Einige Attribute werden als falsch positiv betrachtet, was bedeutet, dass sie keine gültigen Sichtungen sind. Andere Attribute sind nur für eine bestimmte Dauer gültig, z. B. eine Phishing-Kampagne, die nur eine Woche lang ausgeführt wird. Sie können den Attributen, die für eine bestimmte Dauer gültig sind, ein Ablaufdatum zuweisen, aber jede Organisation kann einem Attribut nur ein gültiges Ablaufdatum zuweisen.

Sichtungen, die in MISP von Benutzern von Organisationen erstellt werden, die auf dem entsprechenden MISP-Server als lokal gekennzeichnet sind, werden als interne Sichtungen bezeichnet. Sichtungen, die in MISP von Benutzern von Organisationen erstellt werden, die auf dem entsprechenden Server MISP als Remote markiert sind, werden als externe Sichtungen bezeichnet.

Sichtungssuchen in SIR

Der Workflow „Security Operations Integration - Sichtungssuche“ führt die Sichtungssuche aus. Dieser Flow akzeptiert eine Liste von erkennbaren Elementen, findet implementierte Fähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchen aus, die auf dem konfigurierten Flow basieren.

Sichtungssuchen helfen Analysten, die Verbreitung einer Bedrohung im Zeitverlauf zu bestimmen. Sie können einzelne oder mehrere erkennbare Elemente und den Datumsbereich für Ihre Suche aus einem Security Incident auswählen. Ergebnisse sind in den zugehörigen Listen Security Incident Sichtungen, Sichtungssuchergebnisseund Sichtungssuchdetails enthalten.

Wenn Sie mit der Analyse eines Incidents beginnen, können Sie Now Platform so einrichten, dass automatisch eine Sichtungssuche oder manuell eine Sichtungssuche nach erkennbaren Elementen durchgeführt wird, um andere Anwender in Ihrer Organisation zu identifizieren, die von demselben Phishing-Angriff betroffen sind.

Aktivieren Sie die automatische Sichtungssuche in MISP

Aktivieren Sie die automatische Ausführung der Sichtungssuche in MISP, damit der Workflow „Security Operations Integration – Sichtungssuche“ ausgelöst wird, wenn neue erkennbare Elemente einem Security Incident zugeordnet werden.

Vorbereitungen
Stellen Sie sicher, dass Konfigurationsprofil für die Sichtungssuche für MISP ist aktiv.

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie die Sichtungssuchfunktion zur automatischen Ausführung in der MISP Integrationskonfigurationwird die Sichtungssuche in MISP ausgelöst, wenn einem Security Incident neue erkennbare Elemente zugeordnet

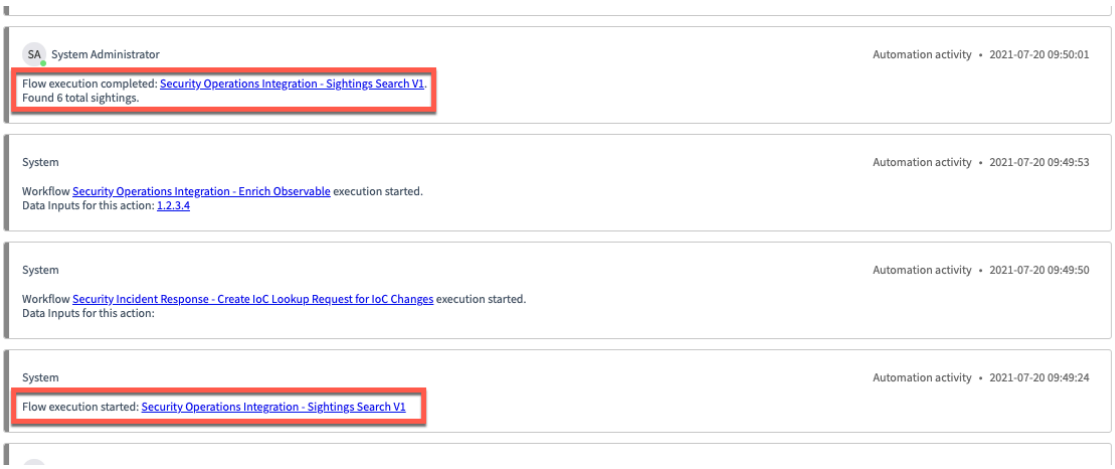
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden. Standardmäßig ist die **Option Sichtungssuche automatisch ausführen, wenn dem Security Incident neue erkennbare Elemente zugeordnet werden** aktiviert.

Prozedur

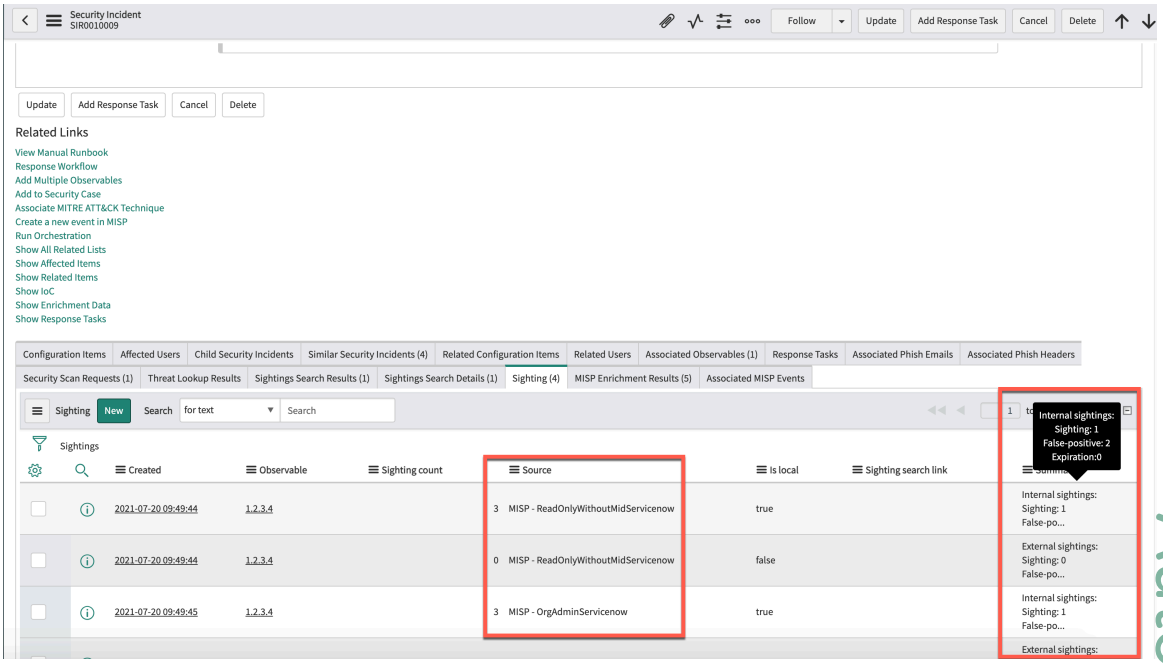
1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, die Sie in den Sichtungssuchdaten MISP anzeigen möchten.
3. Überprüfen Sie die Arbeitsnotizen, nachdem dem Security Incident neue erkennbare Elemente zugeordnet wurden.
   Eine Arbeitsnotiz wird veröffentlicht, wenn der Workflow „Security Operations Integration – Sichtungssuche“ ausgelöst wurde.

   Das folgende Beispiel zeigt den Abschnitt „Arbeitsnotizen“.



4. Zeigen Sie die aggregierten Informationen von erkennbaren Elementen an, die für alle Ereignisse (global) sichtbar und nach ihrer internen oder externen Sichtung kategorisiert sind, nachdem die Workflow-Ausführung abgeschlossen wurde.
   Zeigen Sie die Informationen in den zugehörigen Listen Sichtungen, Sichtungssuchergebnisse und Sichtungssuchdetails an. Das folgende Beispiel zeigt den Sichtungssuchdatensatz, der in der zugehörigen Liste Sichtungen erstellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sichtungssuche-Datensatz

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Erstellung des Datensatzes für die Sichtungssuche.
Erkennbares Element	Erkennbares Element, nach dem von der Abfrage gesucht wird.
Sichtungsanzahl	Anzahl der internen und externen Sichtungen.
Quelle	Quelle des erkennbaren Elements. Wenn das erkennbare Element aus einer Organisation MISP stammt, werden dem Datensatz die Wörter MISPvorangestellt.
Ist lokal	Status, der angibt, ob die Sichtung von einem internen Anwender gemeldet wurde.
Sichtungssuchlink	Sichtungssuchlink in der Instanz MISP.
Zusammenfassung	Typ der Sichtungen, die dem Datensatz zugeordnet sind. Die drei Arten von Sichtungen sind „Sichtung“, „Falsch positiv“ und „Ablauf“. Die Spalte „Zusammenfassung“ wird nur angezeigt, wenn MISP integration for Security Operations installiert ist. Wenn andere Quellen als MISP angezeigt werden, ist der Spalteneintrag „Zusammenfassung“ für diesen Datensatz leer.

Führen Sie eine manuelle Sichtungssuche in durch MISP

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in der Anwendung Now Platform MISP integration for Security Operations durch, um die Verbreitung einer Bedrohung im Zeitverlauf zu bestimmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Erforderliche Rolle: sn_si.analyst

Prozedur

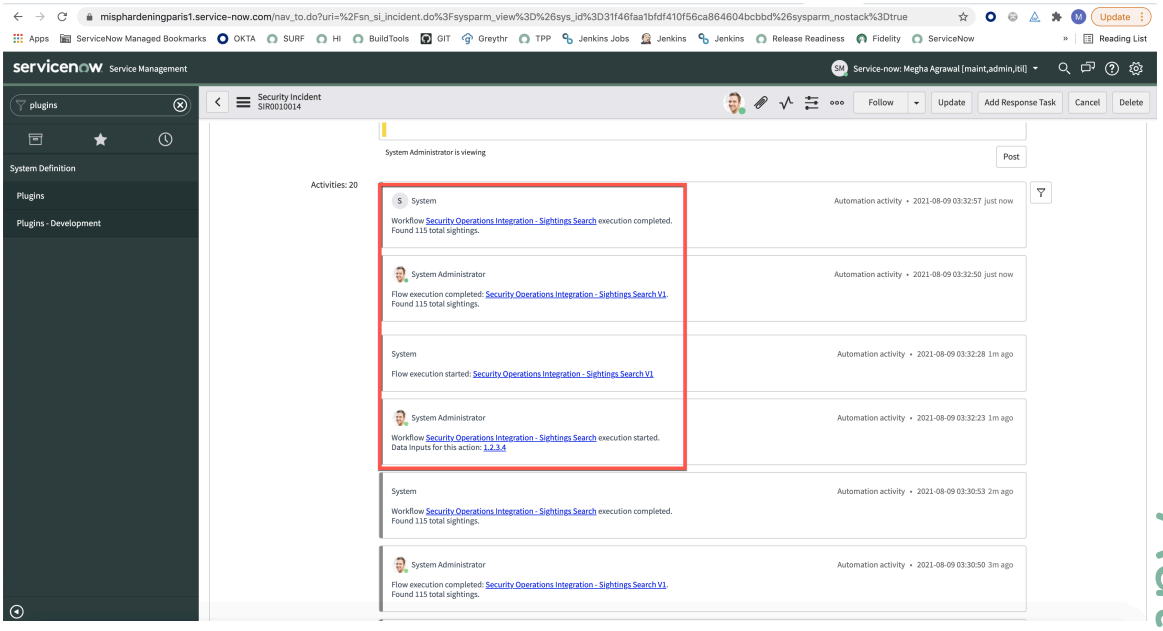
1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, nach denen Sie die Sichtungssuche MISP ausführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete erkennbare Elemente**.
4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü Aktionen **auf Sichtungssuche ausführen**.
   Sie können mehrere erkennbare Elemente für eine Sichtungssuche auswählen.
   Das Dialogfeld „Sichtungssuche ausführen“ wird geöffnet.
5. Geben Sie den Datumsbereich für die Suche nach Sichtungssuchdaten an.

Dialogfeld „Sichtungssuche ausführen“.

Feld	Beschreibung
Letzter	Anzahl der Stunden oder Tage vor der Erstellung des zu durchsuchenden Incidents. Der Standardwert ist 7 Tage. Das Limit beträgt 99 Stunden oder Tage.
zwischen	Datumsbereich für die Suche. Standarddaten sind wie folgt: ○ Datum und Uhrzeit der Erstellung des Incidents. ○ Datum und Uhrzeit, die sieben Tage vor der Eröffnung des incident liegen.

6. Klicken Sie auf **Suche**.
   Das folgende Beispiel zeigt die Ergebnisse der manuellen Sichtungssuche in den Arbeitsnotizen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ergebnisse

Ein Datensatz für die Sichtungssuche wird erstellt. Nachdem die Workflow-Ausführung abgeschlossen ist, können Sie die aggregierten Informationen von erkennbaren Elementen anzeigen, die für alle Ereignisse (global) sichtbar und nach ihren internen oder externen Sichtungen kategorisiert sind. Zusammengefasste und zugehörige Sichtungsdaten werden im Security Incident unter den zugehörigen Listen Sichtungen, Sichtungssuchergebnisseund Sichtungssuchdetails angezeigt.

Melden Sie Sichtungen an MISP

Melden Sie Sichtungen in Bedrohungsdaten, damit Sie auf falsch positive Meldungen in Ihren Daten reagieren können, und erhöhen Sie Ihr Bewusstsein, wenn eine wirklich positive Bedrohung auftritt. Sie können auch ein Ablaufdatum für ein bestimmtes erkennbares Element oder Attribut hinzufügen.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Mit MISP integration for Security Operations können Sie Sichtungen für MISP global über alle Ereignisse hinweg melden. Um eine Sichtung für ein bestimmtes Ereignis zu melden, müssen Sie die Instanz MISP verwenden und die Sichtung lokal melden.

Um eine Sichtung an MISPzu melden, muss das erkennbare Element oder das Attribut in der Instanz MISP verfügbar sein.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie die Sichtungen an MISP melden möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die zugehörige Liste Sichtungen.
4. Wählen Sie das erkennbare Element aus, und wählen Sie im Menü Aktionen eine der folgenden Optionen aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wahlweise:** Wenn Sie die Option **MISP: Sichtung erkennbarer Elemente melden** ausgewählt haben, müssen Sie die Felder im Dialogfeld „Sichtungen erkennbarer Elemente an MISP melden“ ausfüllen.

Dialogfeld „Sichtung erkennbarer Elemente an MISP melden

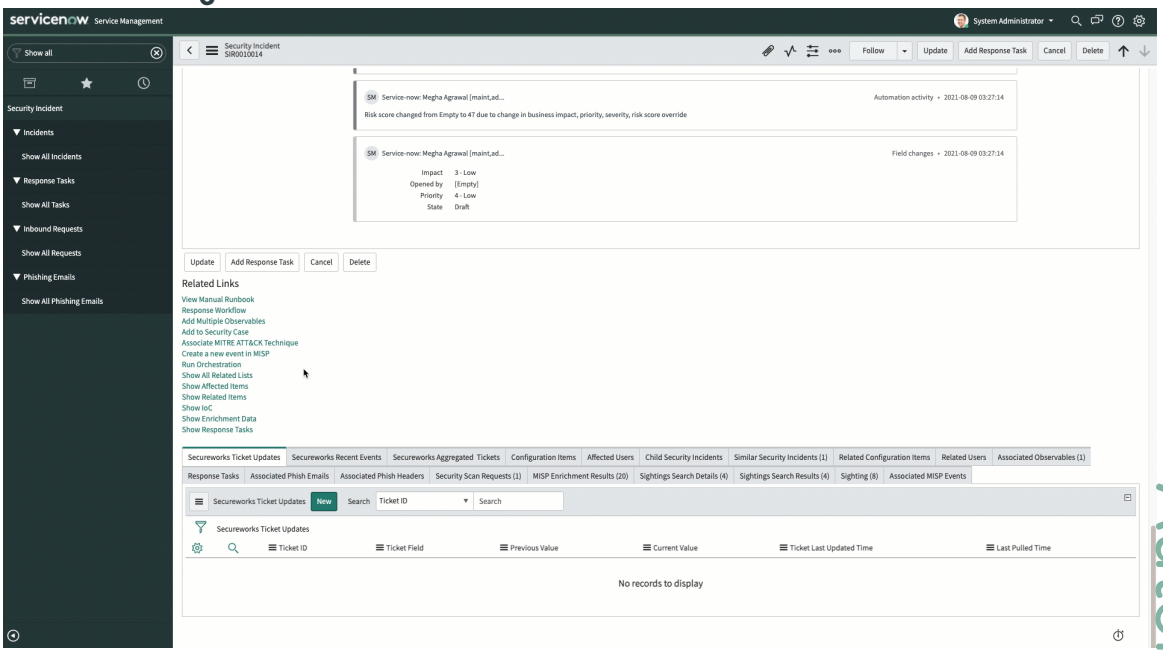
Feld	Beschreibung
Quelle	Quellfeld, das der Quelle MISP der Sichtung entspricht.
Datum	Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element sichtbar wurde. Wenn das Datum leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in MISPausgefüllt.

Das folgende Beispiel zeigt, wie Sie zur zugehörigen Liste „Sichtungen“ im Security Incident navigieren. Aus dieser Liste können Sie ein erkennbares Element auswählen und die Sichtung des erkennbaren Elements an MISPmelden. Die Erfolgsmeldung gibt an, dass die Sichtung erfolgreich an MISPübermittelt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Meldet Sichtungen erkennbarer Elemente an MISP



a. Klicken Sie **auf Sichtung melden**.

6. **Wahlweise:** Wenn Sie die Option **MISP: Erkennbares Element als falsch positiv melden** ausgewählt haben, müssen Sie die Felder des Dialogfelds „Erkennbares Element als falsch positiv melden“ für MISP ausfüllen.

Dialogfeld „Erkennbares Element als falsch positiv an MISP melden

Feld	Beschreibung
Quelle (optional)	Quellfeld, das der Quelle MISP entspricht. Verwenden Sie dieses Feld, um das erkennbare Element als falsch positiv zu deklarieren.
Datum	Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element als falsch positiv eingestuft wurde. Wenn das Datum leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in MISPausgefüllt.

a. Klicken Sie auf **Falsch positives Ergebnis melden**.

7. **Wahlweise:** Wenn Sie die Option **MISP: Report Observable as Expired (Erkennbares Element als abgelaufen melden)** ausgewählt haben, müssen Sie die Felder des Dialogfelds „Ablauf erkennbaren Elements melden bis MISP “ ausfüllen.

Dialogfeld „Ablauf erkennbarer Elemente an MISP melden“.

Feld	Beschreibung
Quelle	Quellfeld, das der Quelle MISP entspricht. Verwenden Sie dieses Feld, um ein erkennbares Element als abgelaufen festzulegen.
Datum	Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element abgelaufen ist. Wenn das Datum

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in MISPausgefüllt.

a. Klicken Sie auf **Ablauf melden**.

Ergebnisse

Die Sichtungen wurden erfolgreich auf den Server MISP aktualisiert.

Ergänzung erkennbarer Elemente in MISP

Indem Sie bei Untersuchungen zur Reaktion auf Incidents erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen MISP -Quellen anreichern, können Sie identifizierte Bedrohungen eindämmen.

Aktivieren Sie die automatische Ergänzung erkennbarer Elemente in MISP

Aktivieren Sie die automatische Ergänzung erkennbarer Elemente in Now Platform MISP, wenn dem Security Incident neue erkennbare Elemente zugeordnet werden.

Vorbereitungen

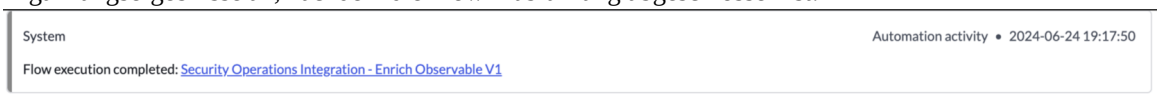
- Aktivieren Sie die Systemeigenschaft Security Incident Response für die Option **Aktiviert oder deaktiviert die geplante Aufgabe „Nach erkennbaren Security Incident-Elementen suchen“,** um die Fähigkeit zum Anreichern erkennbarer Elemente in SIRauszulösen.
- Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie die Daten erkennbarer Elemente in MISP ergänzen möchten.
3. Überprüfen Sie die Arbeitsnotizen, nachdem dem Security Incident neue erkennbare Elemente zugeordnet wurden.

   Das folgende Beispiel zeigt, dass eine Arbeitsnotiz gepostet wird, wenn der Flow „Security Operations Integration – Erkennbares Element ergänzen“ ausgelöst wird.

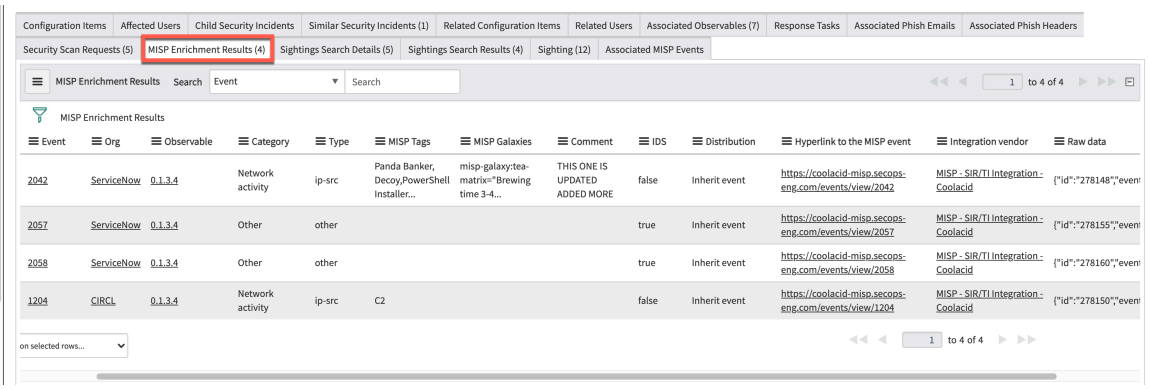
4. Zeigen Sie in der zugehörigen Liste MISP Ergänzungsergebnisse des Security Incidents die Ergänzungsergebnisse an, nachdem die Flow-Ausführung abgeschlossen ist.

   Hinweis:
   Sie müssen konfigurieren, dass die zugehörige Liste MISP Ergänzungsergebnisse in den zugehörigen Listen für Security Incidents angezeigt wird. Weitere Informationen finden Sie unter Konfiguration der zugehörigen Liste.

   Das folgende Beispiel zeigt die Ergänzungsergebnisse in MISP.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Tabelle zeigt die MISP-Ergänzungsergebnisse.

MISP-Datenanreicherungs-Ergebnisse

Feld	Beschreibung
Ereignis	ID des Ereignisses. Klicken Sie auf „Öffnen“, um den Datensatz in der Instanz Now Platform anzuzeigen.
Org	Organisation, die das Ereignis ursprünglich erstellt hat.
Erkennbares Element	Erkennbares Element, das dem Ereignis zugeordnet ist.
Kategorie	Kategorie des Attributs. Zeigen Sie die Liste der Kategorien in der MISP-Dokumentation an .
Typ	Typ des Attributs. Zeigen Sie die Liste der Typen in der MISP-Dokumentation an .
MISP-Tags	Liste der Tags, die dem Attribut MISP zugeordnet sind.
MISP-Galaxien	Liste der Galaxien, die dem Attribut MISP zugeordnet sind.
Kommentar	Kontextbezogener Kommentar zur weiteren Beschreibung des Attributs. Diese Kommentare werden nicht zur Korrelation verwendet und sind rein informativer Natur.
IDS	Kompromittierungsindikator, der es ermöglicht, ihn in alle berechtigten Exporte aufzunehmen.
Verteilung	Verteilung des Attributs nach der Veröffentlichung. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis. In beiden Fällen wird die niedrigste Verteilungsebene verwendet.
Hyperlink zum MISP-Ereignis	Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist.
IntegrationsVendor	Integrationslieferant, der die Daten für die Ergänzung bereitstellt.
Rohdaten	Rohdaten, die dem Attribut MISP zugeordnet sind.

Führen Sie eine manuelle Anreicherung erkennbarer Elemente in durch MISP

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Anreicherung erkennbarer Elemente durch, um erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen MISP -Quellen zu ergänzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

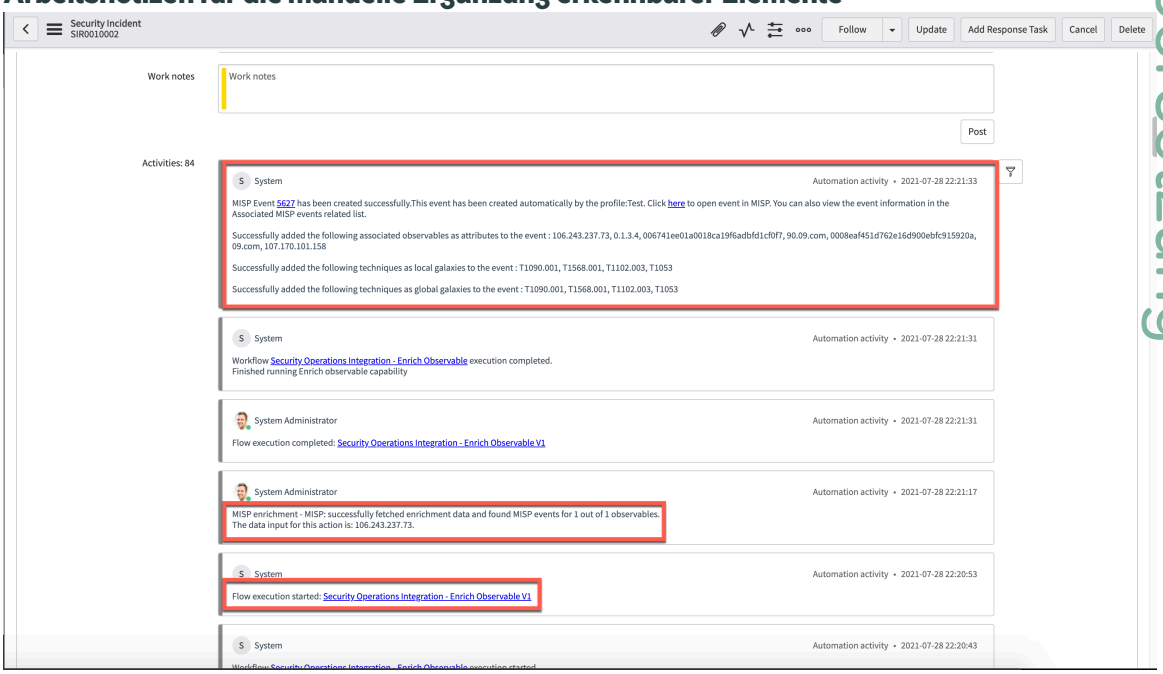
- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Erforderliche Rolle: sn_si.analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie die Ergänzung durchführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete erkennbare Elemente**.
4. Wählen Sie das erkennbare Element aus, und klicken Sie im Menü Aktionen **auf Anreicherung erkennbarer Elemente ausführen**.
   Sie können mehrere erkennbare Elemente für eine Sichtungssuche auswählen.
   Das Dialogfeld „Anreicherung erkennbarer Elemente ausführen“ wird angezeigt.
5. Wählen Sie eine Quelle MISP und dann in der Spalte Ausgewählt eine Implementierung aus, um die ausgewählten erkennbaren Elemente anzureichern.
6. Klicken Sie auf **Absenden**.
   Eine Arbeitsnotiz zeigt, dass der Workflow „Security Operations Integration – Erkennbares Element ergänzen“ ausgelöst wurde. Die zugeordneten Implementierungs-Workflows werden ausgeführt, um die Anreicherung durchzuführen. Sie können die Arbeitsnotizen im Security Incident anzeigen, um den Status anzuzeigen.

   Das folgende Beispiel zeigt, wie Sie die Arbeitsnotizen für eine manuelle Ergänzung erkennbarer Elemente anzeigen.

Arbeitsnotizen für die manuelle Ergänzung erkennbarer Elemente



In der Ergänzungsnachricht wird das erstellte Ereignis aufgelistet. Sie können das Ereignis in der Instanz Now Platform oder in der Instanz MISP anzeigen und die Details des Datensatzes auf der Registerkarte MISP-Ergänzungsergebnisse anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Tags für MISP -Attribute hinzu, oder entfernen Sie sie

Fügen Sie Tags in MISP hinzu, oder entfernen Sie sie, um Ereignisse oder Attribute zu klassifizieren. Sie können Tagging global verwenden, um Ihre Klassifizierung zu aktivieren, oder Tags lokal verwenden, wenn MISP -Ereignisse während der Klassifizierung nicht geändert werden sollen.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Stellen Sie sicher, dass das Attribut, das Sie bearbeiten, zu derselben Organisation gehört wie der Benutzer MISP.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf der Quelle MISP und ihren Verteilungsberechtigungen basieren.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente, Attribute oder Ereignisse enthält, für die Sie die Tags hinzufügen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die zugehörige Liste MISP-Ergänzungsergebnisse.
4. Klicken Sie auf das Vorschausymbol ⓘ neben einem Datensatz, und klicken Sie dann auf **Datensatz öffnen**.
   Das folgende Beispiel zeigt, wie Sie die **MISP-Ergänzungsergebnisse** überprüfen und einen MISP -Ergänzungsdatensatz öffnen.

   MISP-Ergänzungsergebnisdatensatz
   Der MISP-Ergänzungsergebnisdatensatz wird geöffnet

5. Überprüfen Sie den Datensatz des MISP-Ergänzungsergebnisses.

MISP-Anreicherungsergebnis

Feld	Beschreibung
Erkennbares Element	
Ereignis	Ereignis-ID, die vom Server MISP zugewiesen wurde, als das Ereignis zum ersten Mal erstellt oder in MISPimportiert wurde. Zeigen Sie eine Vorschau des Ereignisses an, oder klicken Sie auf den Datensatz, um die Ereignisdaten auf der Seite MISP Ereignisdaten anzuzeigen.
Org	Organisation, die das Attribut MISP erstellt hat.
Kategorie	Kategorie des Attributs, das Sie dem bestimmten Ereignis in MISPhinzufügen. Sie können eine Option wie „interne Referenz“, „Netzwerkaktivität“, „Finanzbetrug“ usw. auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	Typ des MISP -Attributs.
IntegrationsVendor	Integrationsanbieter, der die Daten für die Ergänzung erkennbarer Elemente bereitstellt.
Erstellungsdatum (in MISP)	Datum, an dem das Ereignis zum ersten Mal in MISPerstellt oder importiert wurde.
IDS	Status, der angibt, ob ein erkennbares Element in SIRals schädlich markiert ist. Das entsprechende Attribut in MISP ist ebenfalls als „true“ gekennzeichnet.
Verteilung	Steuerungen für Verteilungsoptionen, z. B. wer dieses Ereignis anzeigen kann, nachdem es veröffentlicht wurde. Diese Option steuert auch, ob das Ereignis mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen geerbt, und die restriktivste Einstellung gewinnen. Die Verteilungsoptionen lauten wie folgt: ○ Nur Ihre Organisation: Ermöglicht nur Mitgliedern Ihrer Organisation, dieses Ereignis anzuzeigen. Das Ereignis kann von einem Ihrer Organisationsmitglieder in eine andere Instanz verschoben werden, auf die nur Ihre Organisation zugreifen kann. Ereignisse mit dieser Einstellung werden nicht synchronisiert. ○ Nur diese Community: Ermöglicht Anwendern, die Teil Ihrer MISP -Community sind, einschließlich Ihrer eigenen Organisation, von Organisationen auf diesem MISP -Server und von Organisationen, die MISP -Server ausführen, die mit diesem Server synchronisiert werden, das Ereignis anzuzeigen. Alle anderen Organisationen, die mit diesen Verbindungsservern verbunden sind, können das Ereignis nicht anzeigen. ○ Verbundene Communities: Ermöglicht Anwendern, die Teil Ihrer Community MISP sind, das Ereignis anzuzeigen, einschließlich aller Organisationen auf diesem Server MISP, aller Organisationen auf Servern MISP von , die mit diesem Server synchronisiert werden, und der Hosting-Organisationen von Servern, die eine Verbindung zu einem beliebigen Server herstellen zwei Hops entfernt). Alle anderen Organisationen, die mit den zwei Hops entfernten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Verbindungsservern verbunden sind, können das Ereignis nicht anzeigen. ○ Alle Communities: Gibt das Ereignis für alle MISP Communities frei, wodurch das Ereignis frei verfügbar ist.
Hyperlink zum MISP-Ereignis	Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist.
Rohdaten	Rohdetails für den Ergänzungsdatensatz des erkennbaren Elements.
Kommentar	Kommentare, die Sie für die Attribute hinzufügen. Diese Kommentare dienen nur zu Informationszwecken und werden nicht zur Korrelation verwendet.
Tags (lokal)	Tags, die in der Instanz MISP der Hostorganisation verfügbar sind, um Tagging für die Synchronisierungs- und Exportfilterung zu aktivieren. MISP Ereignisse werden nicht geändert, wenn Sie lokale Tags verwenden. Diese Tags werden vor der Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communitys immer entfernt.
Tags (global)	Tags, die global für die Freigabe und Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communities verfügbar sind. Wenn Sie Instanzen MISP globale Tags hinzufügen, ändern Sie Ereignisse.
Galaxien (lokal)	Galaxien, die in der Instanz MISP der Hostorganisation für die Synchronisierung und Exportfilterung verfügbar sind. MISP Ereignisse werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese Galaxien werden immer entfernt, bevor sie mit anderen MISP -Instanzen und Freigabe-Communitys synchronisiert werden.
Galaxien (global)	Galaxien, die global für die Freigabe und Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communitys verfügbar sind. Wenn Sie globale Galaxien hinzufügen, werden MISP Ereignisse geändert.

6. Um ein lokales oder globales Tag zu bearbeiten, klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen:

   - **Tags (lokal)**
   - **Tags (global)**

7. Geben Sie im Dialogfeld MISP-Attribut-Tags den Namen des zu suchenden Tags ein, und fügen Sie es hinzu.
8. Klicken Sie auf **Tags auf MISP-Attribut aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Tags die Tags C3, Adware, C2 und Botnet 3101 suchen und hinzufügen und den MISP-Server mit den Tags aktualisieren können. Die Bestätigungsmeldung zeigt, dass alle Tags in MISPaktualisiert wurden.

Hinzufügen lokaler Tags im MISP-Attribut.
Die Tags wurden erfolgreich auf dem Server MISP aktualisiert.

9. Um die Änderungen im Datensatz anzuzeigen, klicken Sie in der Erfolgsmeldung auf **Formular neu laden**.

Fügen Sie einem Ereignis oder Attribut MISP Galaxien hinzu, oder entfernen Sie es

Fügen Sie Galaxien in MISP hinzu, oder entfernen Sie sie, damit Sie diese Objekte als Cluster in MISP klassifizieren und an MISP -Ereignisse oder -Attribute anhängen können.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert hat, zur Hostorganisation des entsprechenden Servers MISP gehören.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf der Quelle MISP und ihren Verteilungsberechtigungen basieren.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen.

   - **Galaxien (lokal)**
   - **Galaxien (global)**

2. Füllen Sie im Dialogfeld „MISP-Ereignis-Galaxien“ die Details aus.

Dialogfeld „MISP-Ereignis-Galaxien“.

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die vom Server MISP zugewiesen wurde, als das Ereignis zum ersten Mal erstellt oder in MISPimportiert wurde.
Namespace	Namespace, in dem die Galaxie gespeichert ist. Sie können Namespaces verwenden, um ähnliche Galaxien zu gruppieren.
Galaxien	Galaxie, in der Sie die Clusterinformationen speichern.
Cluster	Informationen zu den Clustern in der Galaxie.

3. Klicken Sie auf **Galaxien auf MISP-Attribut aktualisieren**.
   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Galaxien den veralteten Namespace und dann die Galaxie „Enterprise Attack – Angriffsmuster“ auswählen und die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Clusterinformationen hinzufügen können. Nachdem die Galaxie-Informationen aktualisiert wurden, können Sie die Erfolgsmeldung anzeigen.

Galaxie-Informationen werden in MISP über die Now Platform hinzugefügt

4. Um die Änderungen im Datensatz anzuzeigen, klicken Sie in der Erfolgsmeldung auf **Formular neu laden**.

Ergebnisse
Die Galaxie-Informationen wurden auf dem Server MISP erfolgreich aktualisiert.

Fügen Sie dem Attribut MISP Kommentare hinzu

Fügen Sie Kommentare für die MISP -Attribute hinzu. Die von Ihnen hinzugefügten Kommentare dienen nur zu Informationszwecken und werden nicht für die Korrelation von MISP -Daten verwendet.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Stellen Sie sicher, dass das Attribut, das Sie bearbeiten, zu derselben Organisation gehört wie der Benutzer MISP.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Klicken Sie auf das Bearbeitungssymbol im Feld Kommentar.
2. Geben Sie Ihren Kommentar in das Feld Attributkommentar ein.
3. Klicken Sie auf **Kommentar auf MISP-Attribut aktualisieren**.
   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol neben dem Kommentarfeld einen Kommentar hinzufügen und dann das Attribut MISP aktualisieren können. Nachdem der Kommentar aktualisiert wurde, können Sie die Erfolgsmeldung anzeigen.

   Galaxie-Informationen werden in MISP über die Now Platform hinzugefügt.
4. Um die Änderungen im Datensatz anzuzeigen, klicken Sie in der Erfolgsmeldung auf **Formular neu laden**.

Ergebnisse
Der Kommentar wurde erfolgreich auf dem Server MISP aktualisiert.

Verwalten von Ereignissen in MISP

Sie können Ereignisse in MISP automatisch oder manuell über Now Platformerstellen. Sie können die Ereignisdaten in MISP auch über Now Platformbearbeiten.

Automatisch erstellte Ereignisse in werden überprüft MISP

Sie können die automatisch erstellten Ereignisse überprüfen, nachdem Sie das Ereigniserstellungsprofil in Ihrer Instanz Now Platform konfiguriert haben.

Profil zur automatischen Ereigniserstellung

Die Konfiguration des Profils für die automatische Ereigniserstellung erfolgt durch die Anwenderrollen sn_si.admin oder sn_ti.admin in **MISP-Integration** > **Profile für die automatische Erstellung von Ereignissen** Modul.

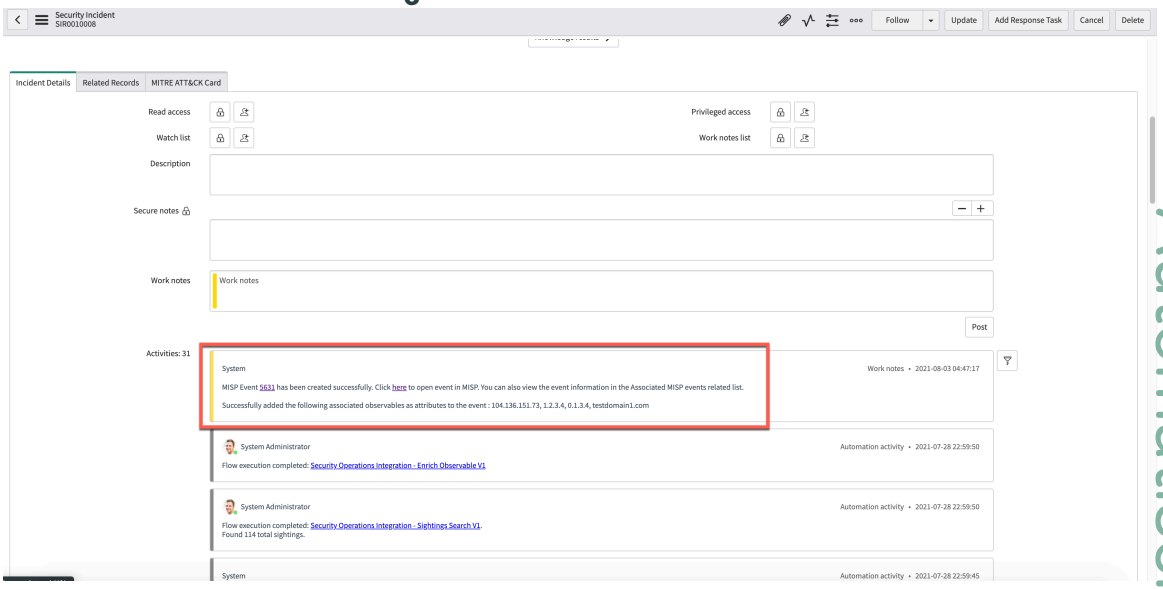
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisdaten MISP werden angezeigt

Sie können die erstellten Ereignisse folgendermaßen anzeigen:

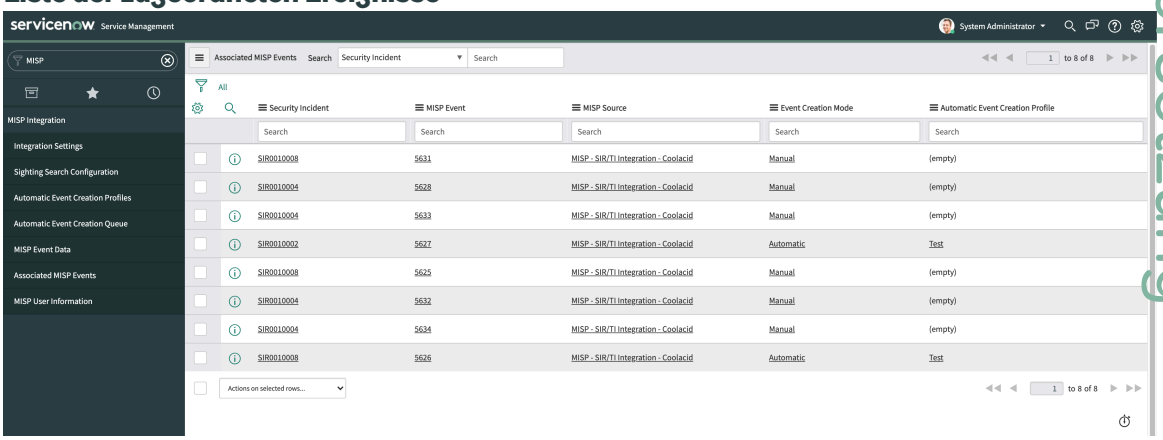
- Zeigen Sie die Arbeitsnotizen für die erstellten Ereignisse an. Sie können die Ereignisdetails in der Instanz Now Platform und auch so anzeigen, wie sie auf dem Server MISP angezeigt werden (siehe folgendes Beispiel).

Arbeitsnotizen für erstellte Ereignisse



- Klicken Sie auf die zugehörige Liste Zugeordnete MISP-Ereignisse. Hier können Sie das Ereignis in Bezug auf den Security Incident und die Ressourcen MISP anzeigen (siehe folgendes Beispiel).

Liste der zugeordneten Ereignisse

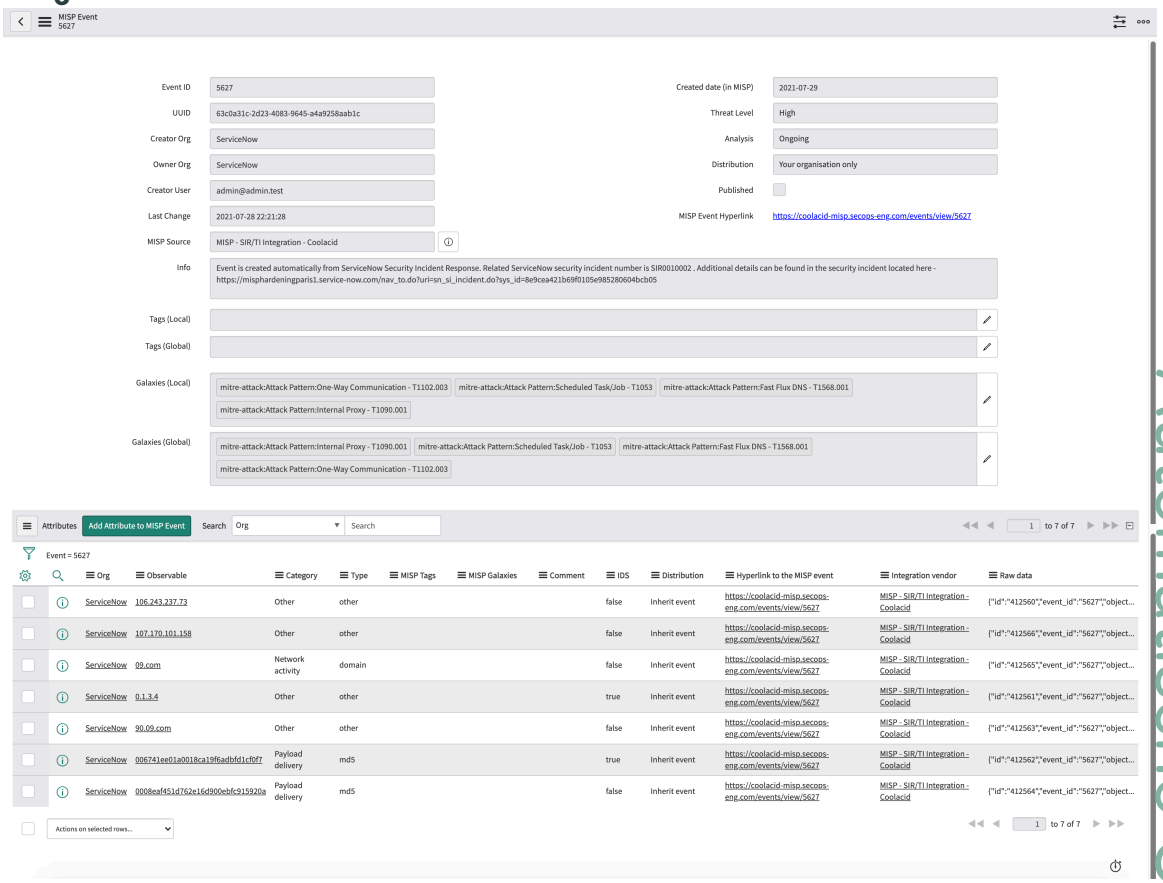


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie die MISP -Ereignisdaten in der Formularansicht an, um die detaillierten Informationen zu den MISP -Ereignissen zu überprüfen, wie im folgenden Beispiel gezeigt.

Ereignisdaten in der Formularansicht



Erstellen Sie manuell ein Ereignis in MISP

Erstellen Sie manuell Ereignisse in MISP aus dem Now Platform, um kontextbezogene Informationen zu erfassen, die als Attribute und Objekte dargestellt werden.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie ein Ereignis erstellen möchten.
3. Klicken Sie auf **Ein neues Ereignis in MISP erstellen**.
4. Füllen Sie im Dialogfeld „Neues Ereignis in MISP erstellen“ die Details aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Ereignis im Dialogfeld „MISP“.

Feld	Beschreibung
Datum	Erstellungsdatum des Ereignisses in MISP.
Information zum Ereignis	Ereignisinformationen, die automatisch aus dem Now Platform Security Incident Responseerstellt werden.
Bedrohungsstufe	Risikostufe des Ereignisses. Sie können die Incidents in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) einteilen. Dieses Feld kann auch als undefiniert belassen werden. Die folgenden Optionen stehen zur Verfügung: ○ Niedrig: Allgemeine Massen-Malware ○ Mittel: Advanced Persistent Threats (APT) ○ Hoch: Ausgereifte APTs und 0-Tage-Angriffe
Quelle	MISP Quelle für die Ereigniserstellung.
Verteilung	Option, die steuert, wer dieses Ereignis anzeigen kann, nachdem das Ereignis veröffentlicht wurde. Diese Option steuert auch, ob das Ereignis mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen geerbt. Die restriktivste Einstellung gewinnen. Die Verteilungsoptionen lauten wie folgt: ○ Nur Ihre Organisation: Ermöglicht nur den Mitgliedern Ihrer Organisation, dieses Ereignis anzuzeigen. Das Ereignis kann von einem Ihrer Organisationsmitglieder in eine andere Instanz verschoben werden, auf die nur Ihre Organisation zugreifen kann. Ereignisse mit dieser Einstellung werden nicht synchronisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Nur diese Community: Ermöglicht Anwendern, die Teil Ihrer MISP -Community sind, einschließlich Ihrer eigenen Organisation, von Organisationen auf diesem MISP -Server und von Organisationen, die MISP -Server ausführen, die mit diesem Server synchronisiert werden, das Ereignis anzuzeigen. Alle anderen Organisationen, die mit Verbindungsservern verbunden sind, können das Ereignis nicht anzeigen. ○ Verbundene Communities: Ermöglicht Anwendern, die Teil Ihrer Community MISP sind, das Ereignis anzuzeigen, einschließlich aller Organisationen auf diesem Server MISP, aller Organisationen auf Servern MISP von , die mit diesem Server synchronisiert werden, und der Hosting-Organisationen von Servern, die eine Verbindung zu einem beliebigen Server herstellen das ist zwei Hops entfernt. Alle anderen Organisationen, die mit den Verbindungsservern verbunden sind und zwei Hops von diesem Server entfernt sind, können das Ereignis nicht anzeigen. ○ Alle Communities: Gibt das Ereignis für alle MISP -Communitys frei.
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld		Beschreibung
		○ Anfänglich: Die Analyse beginnt gerade erst ○ Laufend: Die Analyse wird ausgeführt ○ Abgeschlossen: Die Analyse ist abgeschlossen
Erweiterte Optionen	Alle SIR-zugeordneten erkennbaren Elemente als Attribute zum MISP-Ereignis hinzufügen	Option zum Hinzufügen verfügbarer erkennbarer Elemente in einem Security Incident zu einem MISP -Ereignis als Attribute. Mit dieser Option wird die **Option „Attribut-IDS-Kennzeichnung festlegen, wenn erkennbares Element schädlich ist** “ aktiviert.
	Legen Sie die Attribut-IDS-Kennzeichnung fest, wenn die Erkennung von erkennbaren Elementen schädlich ist.	Erkennbares Element, das in SIRals schädlich markiert ist. Das entsprechende Attribut in MISP ist ebenfalls als „true“ markiert.
	Erkennbare Elemente anhand von Sicherheits-Tags filtern	Option zum Filtern der erkennbaren Elemente basierend auf den ausgewählten Sicherheits-Tags. Mit dieser Option können Sie die MISP-Ereignisse in Threat Intelligence unterscheiden und verwalten. **Sicherheits-Tags**: Fügen Sie Tags hinzu, um die erkennbaren Elemente zu filtern. Wenn Sie beispielsweise ein Tag mit der Bezeichnung „Freigabe blockieren“ oder „TLP: White“ hinzufügen, werden diese erkennbaren Elemente, wenn eines der erkennbaren Elemente mit einem dieser Tags verknüpft ist, dem MISP-Ereignis während des MISP nicht als Attribut hinzugefügt Ereigniserstellung.
	Synchronisieren Sie MITRE ATT&CK-Techniken des Security Incident als lokale Galaxien im MISP-Ereignis	Option zum Synchronisieren der Now Platform SIR Security Incident-Techniken MITRE-ATT&CK™ als lokale Galaxien im Ereignis MISP.

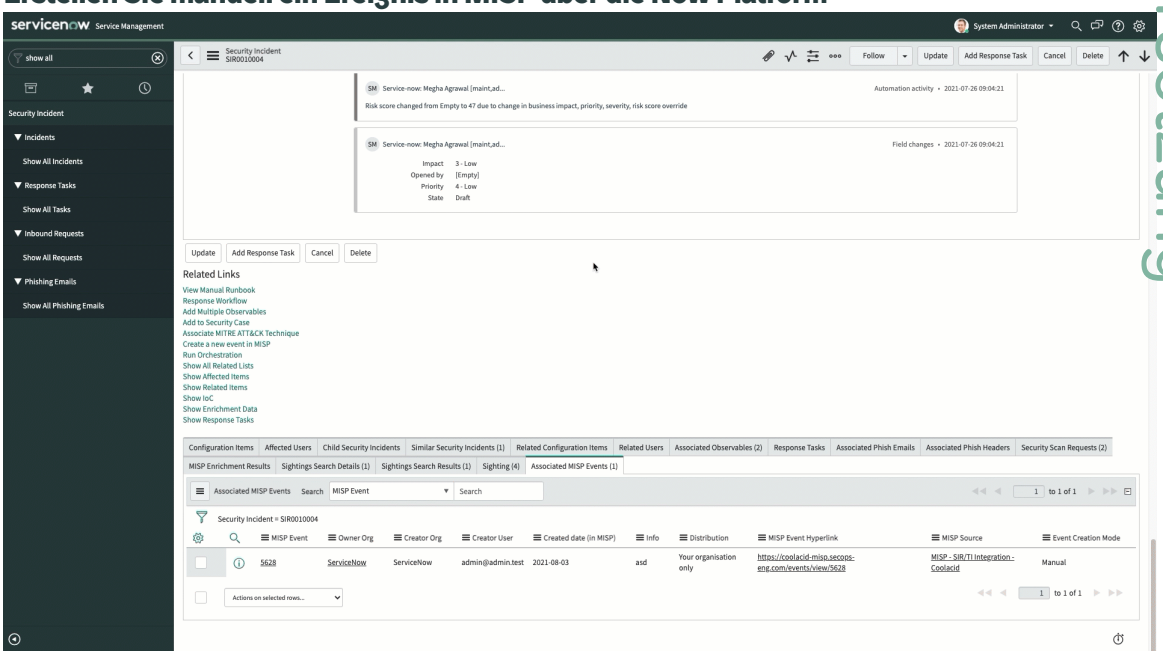
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld		Beschreibung
	MITRE ATT&CK-Techniken des Security Incident als globale Galaxien im MISP-Ereignis synchronisieren	Option zum Synchronisieren der Now Platform SIR Security Incident-Techniken MITRE-ATT&CK™ als globale Galaxien im Ereignis MISP.
	MISP-Ereignis Tags hinzufügen	Option, mit der Sie den in ServiceNow erstellten Ereignissen MISP-Tags hinzufügen können. Diese Option zeigt die folgenden Optionen an: ○ **Lokal (Tags):**Die ausgewählten Tags werden dem MISP-Ereignis als lokale Tags hinzugefügt. ○ **Global (Tags):**Die ausgewählten Tags werden dem MISP-Ereignis als globale Tags hinzugefügt.

5. Klicken Sie auf **Neues MISP-Ereignis erstellen**.

Das folgende Beispiel zeigt, dass Sie durch das Erstellen eines Ereignisses in MISPdie Ergebnisse im Security Incident anzeigen können. Sie können auch die Arbeitsnotizen, das Ereignis in der Instanz Now Platform und das Ereignis auf dem Server MISP anzeigen (siehe folgendes Beispiel).

Erstellen Sie manuell ein Ereignis in MISP über die Now Platform



Sie können die Ergebnisse auf folgende Weise anzeigen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Oben auf der Seite des Security Incidents wird eine Erfolgsmeldung angezeigt. Sie können die Ereignisdetails in der Instanz Now Platform und auch auf dem Server MISP anzeigen.
- In den Arbeitsnotizen können Sie die Erfolgsmeldung mit weiteren Details anzeigen. Sie können die Ereignisdetails auch in der Instanz Now Platform und auf dem Server MISP anzeigen.
- In der zugehörigen Liste „Zugeordnete MISP-Ereignisse“ können Sie das Ereignis in Bezug auf den Security Incident und die Ressourcen MISP anzeigen.

Fügen Sie einem Ereignis MISP Attribute hinzu

Fügen Sie einem Ereignis Attribute hinzu, z. B. den Typ, die Kategorie und andere kontextbezogene Informationen zum Ereignis.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Vergewissern Sie sich, dass das Ereignis, für das Sie das Attribut hinzufügen oder aktualisieren, zu derselben Organisation gehört wie der Benutzer MISP.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **MISP** > **Zugeordnete MISP-Ereignisse**.
   Sie können auch in jedem Security Incident zur zugehörigen Liste Zugeordnetes MISP-Ereignis navigieren.
2. Klicken Sie auf das MISP-Ereignis, für das Sie ein Attribut hinzufügen möchten.
3. Klicken Sie auf **Attribut zu MISP-Ereignis hinzufügen**.
4. Füllen Sie im Dialogfeld „Attribute zu Ereignis hinzufügen“ die Details aus.

Dialogfeld „Attribut zu Ereignis hinzufügen“.

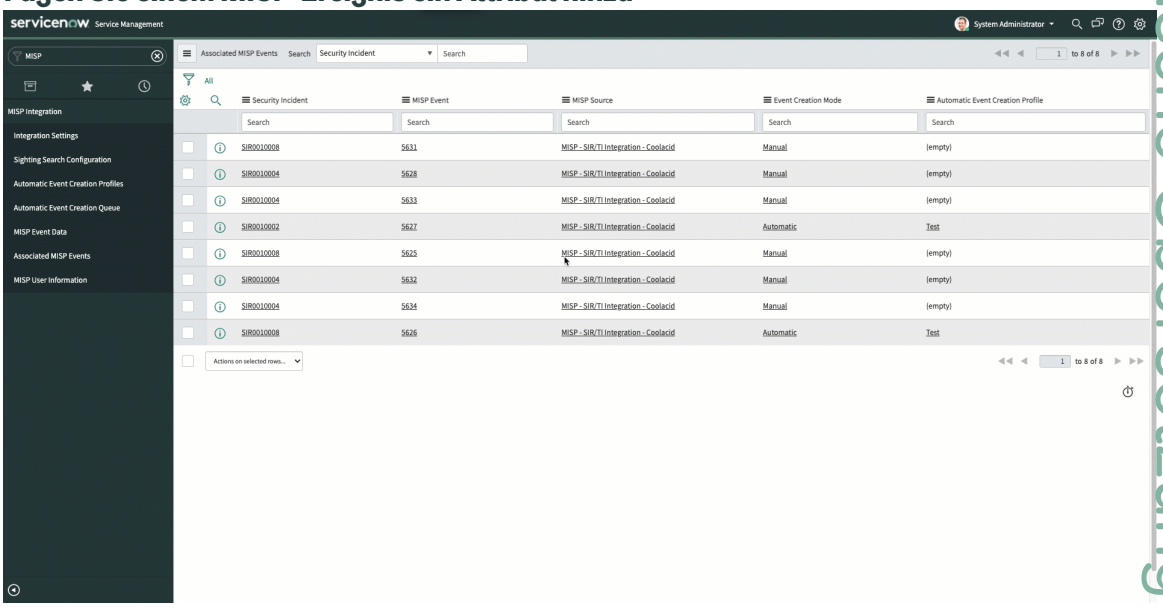
Feld	Beschreibung
Wert	Ist-Wert des Attributs. Geben Sie Daten zum Wert ein, die darauf basieren, was für den ausgewählten Attributtyp gültig ist. Für ein Attribut vom Typ ip-src (Quell-IP-Adresse) ist beispielsweise 11.11.11.11 ein gültiger Wert. **Hinweis:** Sie können nur Attribute oder erkennbare Elemente auswählen, die den Kontext mit dem Ereignis gemeinsam nutzen. Die erkennbaren Elemente dürfen nicht bereits ein Attribut in MISPhaben.
Kategorie	Kategorie des Attributs. Die Kategorie beschreibt den Aspekt der Malware für dieses Attribut. Ein Beispiel wären die Persistenzmechanismen der Malware oder Netzwerkaktivität.
Typ	Typ, der die Kategorie erklärt. Wenn ein Angreifer beispielsweise eine IP-Adresse für einen Angriff

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	verwendet, kann eine Quell-E-Mail-Adresse oder eine über einen Anhang gesendete Datei die Nutzlastbereitstellung einer Malware beschreiben. Diese Arten von Attributen gehören zur Kategorie der Nutzlastbereitstellung.
Verteilung	Anwender, die dieses Attribut anzeigen können. Die Verteilung wird von Attributen geerbt. Die restriktivste Einstellung gewinnen.
Attribut als IDS-Signatur verwenden	Erkennbares Element, das in SIRals schädlich markiert ist. Das entsprechende Attribut in MISP ist ebenfalls als „true“ markiert.
Kommentare	Kommentare, die Sie für die Attribute hinzufügen.

Das folgende Beispiel zeigt, dass Sie durch Navigieren von der Liste Zugeordnete MISP-Ereignisse den Ereignisdatensatz 5627 anzeigen und dem Ereignis Attribute hinzufügen können. Die Attribute umfassen den Wert (testdomain.com), die Kategorie als externe Analyse und den Typ als Domäne. Sie können auch IDS aktivieren. Die Erfolgsmeldung im Ereignisdatensatz zeigt, dass das Attribut dem Ereignis hinzugefügt wird (siehe folgendes Beispiel).

Fügen Sie einem MISP-Ereignis ein Attribut hinzu



5. Klicken Sie auf **Attribut zu MISP-Ereignis hinzufügen**.

Ergebnisse

Sie können das hinzugefügte Attribut im Abschnitt Attribute anzeigen.

Fügen Sie einem Ereignis MISP Tags hinzu

Fügen Sie Tags in Now Platform MISP hinzu, um Ereignisse oder Attribute zu klassifizieren. Sie können Tagging global verwenden, um Ihre Klassifizierung zu aktivieren, oder Tags lokal verwenden, wenn MISP -Ereignisse während der Klassifizierung nicht geändert werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen zur Verwendung der bidirektionalen MISP -Funktionen.
- Stellen Sie sicher, dass das Ereignis, das Sie bearbeiten, zu derselben Organisation gehört wie der Benutzer MISP.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf der Quelle MISP und ihren Verteilungsberechtigungen basieren.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der das Ereignis enthält, für das Sie Tags hinzufügen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die zugehörige Liste MISP-Ergänzungsergebnisse.
4. Klicken Sie in der Liste der Ergänzungsergebnisse auf die Ereignis-ID.
   Sie können auch von navigieren **MISP** > **Zugeordnete MISP-Ereignisse** Modul.
5. Überprüfen Sie den MISP-Ereignisdatensatz.

Formularansicht „MISP-Ereignis“.

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die von MISP zugewiesen wird, wenn das Ereignis zum ersten Mal auf dem Server MISP erstellt oder importiert wurde.
UUID	ID, die Ereignisse und Attribute eindeutig identifiziert.
Erstellerorganisation	Organisation, die das Ereignis in der Instanz MISP erstellt hat.
Besitzerorganisation	Organisation, die das Ereignis in der Instanz MISP besitzt. Dieses Feld ist nur für Administratoren sichtbar.
Erstelleranwender	Anwender, der das Ereignis in MISPerstellt hat.
Letzter Change	Datum, an dem das Ereignis zuletzt geändert wurde.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.
Erstellungsdatum (in MISP)	Datum, an dem das Ereignis erstellt oder zuerst auf den Server MISP importiert wurde.
Bedrohungsstufe	Risikostufe des Ereignisses. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) eingeteilt werden. Dieses Feld kann als nicht definiert gelassen werden. Die folgenden Optionen stehen zur Verfügung:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Niedrig: Allgemeine Massen-Malware ○ Mittel: Advanced Persistent Threats (APT) ○ Hoch: Ausgereifte APTs und 0-Tage-Angriffe
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: ○ Anfänglich: Die Analyse beginnt gerade erst ○ Laufend: Die Analyse wird ausgeführt ○ Abgeschlossen: Die Analyse ist abgeschlossen
Verteilung	Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis.
Veröffentlicht	Status, ob das Ereignis veröffentlicht wurde oder nicht. Durch die Veröffentlichung können die Attribute des Ereignisses für alle berechtigten Exporte verwendet werden, und es werden Anwender benachrichtigt, die die Ereigniswarnungen abonniert haben.
MISP-Ereignis-Hyperlink	Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist.
Information	Kurze Beschreibung des Ereignisses.
Tags (lokal)	Tags, die in der Instanz MISP der Hostorganisation verfügbar sind, um Tagging für die Synchronisierungs- und Exportfilterung zu aktivieren. MISP Ereignisse werden nicht geändert, wenn Sie lokale Tags verwenden. Lokale Tags werden vor der Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communitys immer entfernt.
Tags (global)	Tags, die global für die Freigabe und Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communities verfügbar sind. Wenn Sie Instanzen MISP globale Tags hinzufügen, können Sie Ereignisse ändern.
Galaxien (lokal)	Galaxien, die in der Instanz MISP der Hostorganisation für die Synchronisierung und Exportfilterung verfügbar sind. MISP Ereignisse werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese lokalen Galaxien werden immer entfernt, bevor sie mit anderen MISP -Instanzen und Freigabe-Communitys synchronisiert werden.
Galaxien (global)	Galaxien, die global für die Freigabe und Synchronisierung mit anderen MISP -Instanzen und Freigabe-Communitys verfügbar sind. Wenn Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	globale Galaxien hinzufügen, MISP, können Sie Ereignisse ändern.

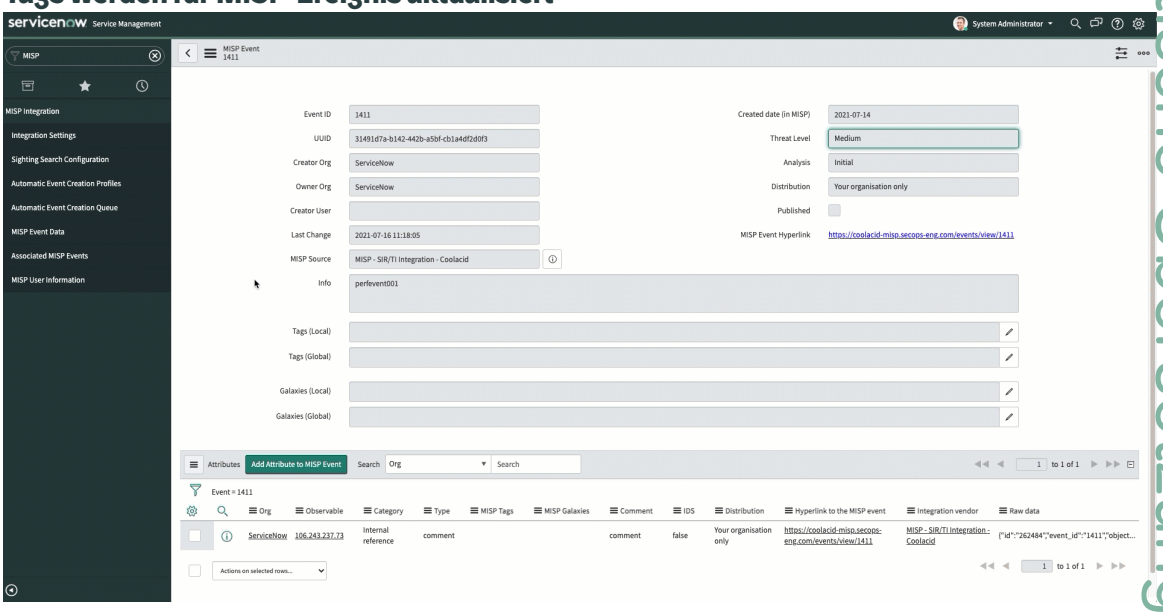
6. Um ein lokales oder globales Tag zu bearbeiten, klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen:

   - **Tags (lokal)**
   - **Tags (global)**

7. Geben Sie im Dialogfeld „MISP-Ereignis-Tags“ den Tag-Namen ein, um die Tags zu suchen und hinzuzufügen.
8. Klicken Sie auf **Tags auf MISP-Ereignis aktualisieren**.

   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Tags die Tags C3, Adware, C2 und Botnet 3101 suchen und hinzufügen und den MISP-Server mit den Tags aktualisieren können. Die Bestätigungsmeldung zeigt, dass alle Tags in MISPaktualisiert wurden.

   Tags werden für MISP-Ereignis aktualisiert



9. Klicken Sie in der Erfolgsmeldung auf **Formular neu laden,** um die Änderungen im Datensatz anzuzeigen.

Ergebnisse

Die Tags wurden auf dem Server MISP erfolgreich aktualisiert.

Aktualisiert Galaxien auf ein MISP -Ereignis oder -Attribut

Fügen Sie Galaxien in Now Platform MISP hinzu, oder entfernen Sie sie, damit Sie diese Objekte als Cluster in der Instanz MISP klassifizieren und an MISP Ereignisse oder Attribute anhängen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen ist für die Verwendung der bidirektionalen MISP -Funktionen erforderlich.
- Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert hat, zur Hostorganisation des entsprechenden Servers MISP gehören.
- Die Ihnen zur Verfügung stehenden Tags und Galaxien basieren auf der Quelle MISP und ihren Verteilungsberechtigungen.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

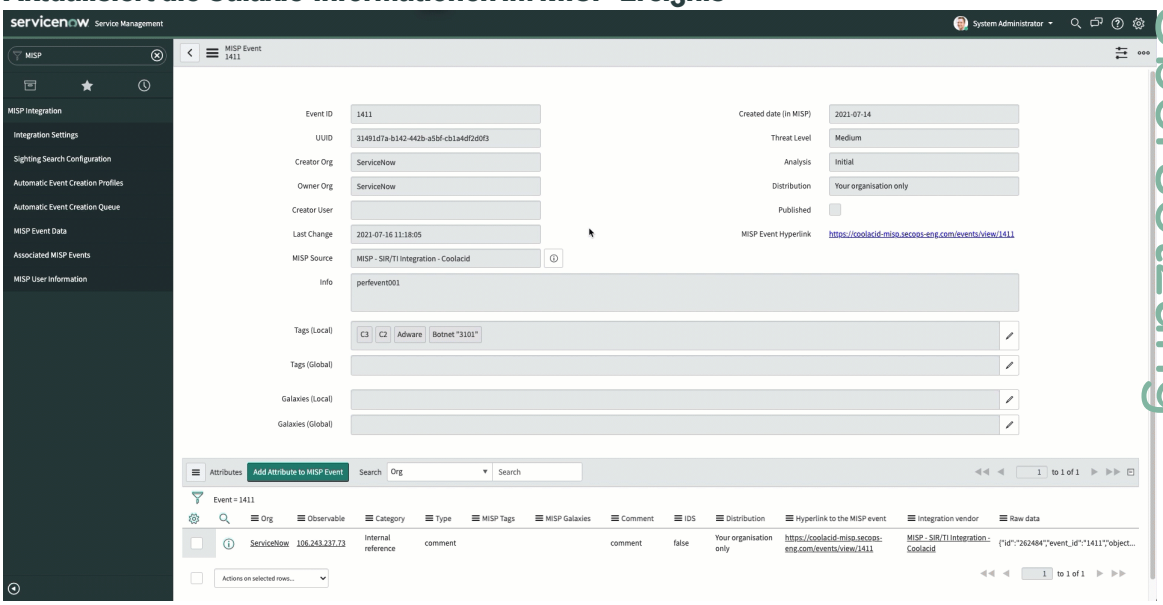
1. Klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen.

   - **Galaxien (lokal)**
   - **Galaxien (global)**

2. Geben Sie im Dialogfeld „MISP-Ereignis-Galaxien“ Text ein, und suchen Sie, um die Tags hinzuzufügen.
3. Klicken Sie auf **Galaxien auf MISP-Ereignis aktualisieren**.

   Das folgende Beispiel zeigt, wie Sie auf das Bearbeitungssymbol für die lokalen Galaxien klicken, den veralteten Namespace auswählen, die Galaxie „Enterprise Attack – Angriffsmuster“ auswählen und Clusterinformationen hinzufügen. Nachdem die Galaxie-Informationen aktualisiert wurden, können Sie die Erfolgsmeldung anzeigen.

   Aktualisiert die Galaxie-Informationen im MISP-Ereignis



   Die Galaxien wurden auf dem Server MISP erfolgreich aktualisiert.

4. Klicken Sie in der Erfolgsmeldung auf **Formular neu laden,** um die Änderungen im Datensatz anzuzeigen.

Ein Rollup von MITRE-ATT&CK -Informationen mithilfe von MISP -Ergänzungsergebnissen durchführen

Führen Sie ein manuelles Rollup der MISP-Ergänzungsergebnisse durch, wenn Sie das automatische Rollup von Informationen zu MISP nicht aktiviert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

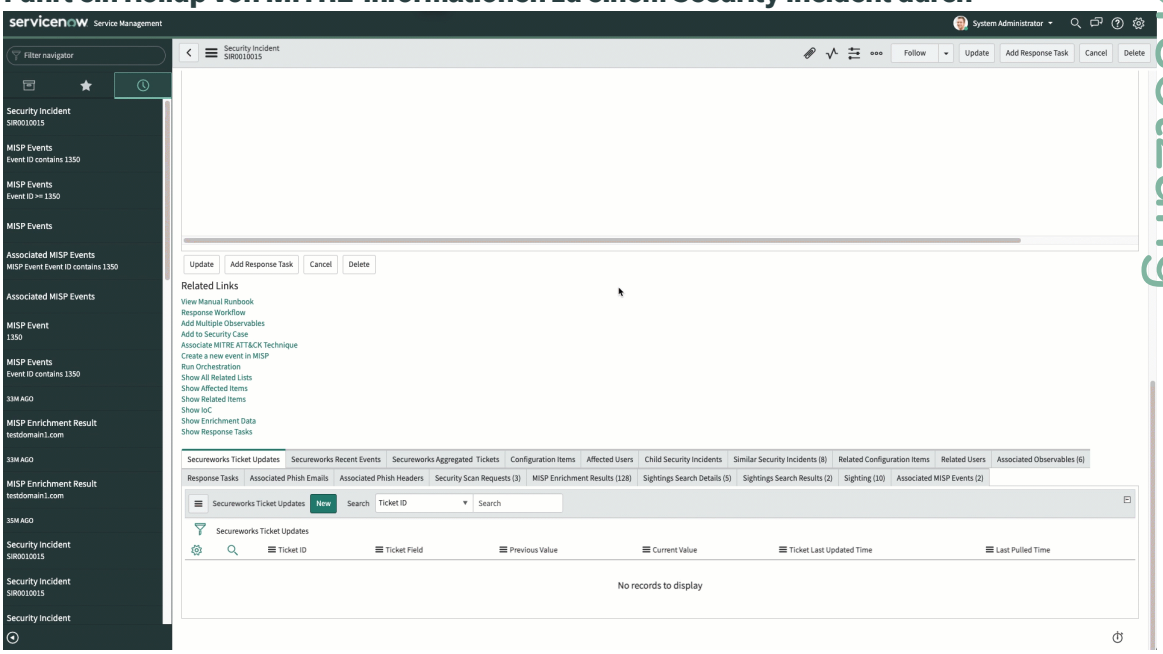
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie die automatischen Extraktionsregeln des Basissystems, um die MITRE-ATT&CK -Informationen aus der MISP -Integration zu importieren. Mit MISP integration for Security Operations werden zwei Basissystem-Extraktionsregeln für die MITRE-ATT&CK -Technik für MISP - MISP - Galaxien und MISP -Tags eingeführt. Weitere Informationen zu automatischen Extraktionsregeln in MITRE-ATT&CKfinden Sie unter Technikregeln für automatisches Extrahieren für den Import von MITRE-ATT&CK-Informationen.

Wenn Sie aktiviert haben automatisches Rollup von MITRE-ATT&CK Informationen mithilfe von MISP Datenanreicherungsergebnisse zu einem Security Incident werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie diese Aufgabe manuell ausführen.

Prozedur
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **MISP-Ergänzungsergebnisse**.
4. Wählen Sie das erkennbare Element aus, und klicken Sie im Menü „Aktionen **“ auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Sie können mehrere erkennbare Elemente auswählen und dann die Informationen zusammenfassen.
5. Um die Änderungen zu bestätigen, klicken Sie auf **Neu laden**.
   Das folgende Beispiel zeigt, wie Sie ein erkennbares Element auswählen und die MISP -Ergänzungsergebnisse für den Security Incident zusammenfassen.

Führt ein Rollup von MITRE-Informationen zu einem Security Incident durch



Ergebnisse
Sie können die Karte MITRE-ATT&CK anzeigen, um zu bestätigen, dass für die MISP-Ergänzungsergebnisse ein Rollup für den Security Incident durchgeführt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OPSWAT Metadefender Integration (Integration von OPSWAT Metadefender).

OPSWAT Metadefender ermöglicht das Herunterladen von Bedrohungsdaten, die vom Drittanbieter-Scanner Metadefender erkannt wurden, in die Anwendung Threat Intelligence zu Nachverfolgungs-, Priorisierungs- und Lösungszwecken.

Erkunden	Einrichtung
• Integrationsüberblick OPSWAT Metadefender • Threat Intelligence-Integrationen	Aktivieren und konfigurieren Sie die OPSWAT Metadefender -Integration
Verwenden	**Entwickeln**
Führen Sie Suchen für erkennbare Elemente durch	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten
Problembehandlung und Hilfe	
• Problembehandlung bei Integration • Stellen oder beantworten Sie Fragen in der Security Operations-Community • Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Kontakt Kundenservice und Support	

Integrationsüberblick OPSWAT Metadefender

OPSWAT Metadefender ist eine Sicherheitslösung, die Zugriff auf mehrere Anti-Malware-Computer bietet und sich problemlos in Security Operationsintegrieren lässt.

Bevor Sie die -Integration OPSWAT Metadefender verwenden können, müssen Sie das Plugin aktivieren und die Integration konfigurieren. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Flow „Bedrohungssuche – OPSWAT Metadefender“.

Der Flow „Bedrohungssuche – OPSWAT Metadefender“ führt eine Suche für ausgewählte erkennbare Elemente durch. Wenn es sich bei den erkennbaren Elementen um einen von OPSWAT Metadefender erkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

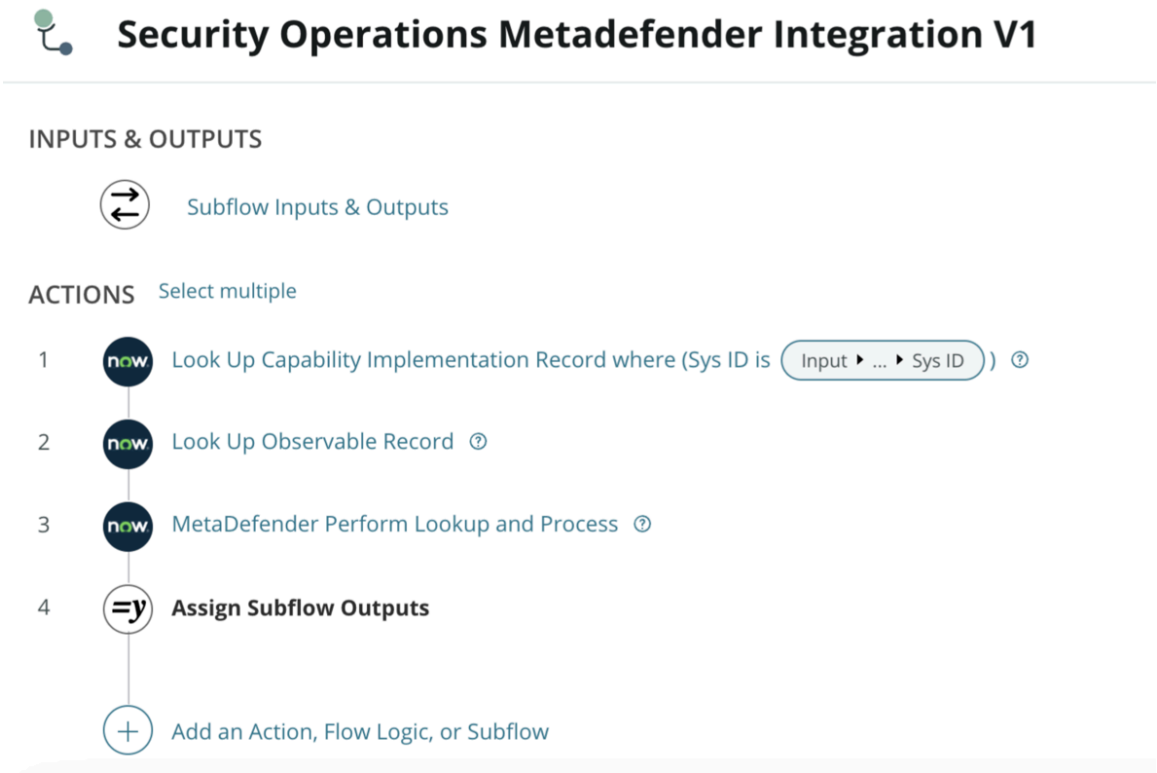
Dieser Flow wird von Security Operations-Integration – Funktionalität zur Bedrohungssuche ausgelöst, wenn Sie eine Bedrohungssuche für mindestens ein erkennbares Element durchführen und die OPSWAT Metadefender-Implementierung ausgewählt ist. Weitere Informationen finden Sie unter Führen Sie Suchen für erkennbare Elemente durch.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_si.admin

Flow „Bedrohungssuche – OPSWAT Metadefender“.



Informationen zu den von diesem Flow verwendeten Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Aktivieren und konfigurieren Sie die OPSWAT Metadefender -Integration

Bevor Sie die OPSWAT Metadefender -Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn die Integration abgeschlossen ist, greifen Sie auf das OPSWAT-Portal zu, und rufen Sie den Metadefender-Cloud-API-Schlüssel ab
3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte „OPSWAT Metadefender“ auf **Konfigurieren**.
5. Geben Sie den **API-Schlüssel** ein, den Sie im OPSWAT-Portal erworben haben, oder fügen Sie ihn ein.
6. Klicken Sie auf **Absenden**.

Ergebnisse

Nach der Konfiguration kann OPSWAT Metadefender für die Suche nach erkennbaren Elementen in Threat Intelligence und erkennbaren Elementen in Security Incidents ausgewählt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Führen Sie Suchen für erkennbare Elemente durch

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Fälle, in denen das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erwerben Sie das SSL-Zertifikat von einem Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) wie folgt von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie auf **Weitere Informationen** und anschließend auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen** und anschließend auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Export**, um die PEM-Datei in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu** und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn ein Zertifikat abgelaufen ist, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration mit VirusTotal

Mit der VirusTotal -Integration können Sie die Analyse verdächtiger IP-Adressen, Dateien, Datei-Hashes und URL-Adressen anfordern, um Ihre Untersuchung hinsichtlich ihrer Schädlichkeit zu erleichtern.

Erkunden	Einrichten
Threat Intelligence-Integrationen	• VirusTotal Integrationen-Setup • Aktivieren und konfigurieren Sie die VirusTotal-Integration
Verwenden	**Entwickeln**
• Führen Sie Suchen für erkennbare Elemente durch • Workflow „Bedrohungssuche – VirusTotal“.	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten
Problembehandlung und Hilfe	
• Problembehandlung bei Integration • Stellen oder beantworten Sie Fragen in der Security Operations-Community • Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Kontakt Kundenservice und Support	

VirusTotal Integrationen-Setup

VirusTotal ist ein kostenlosen Service, der verdächtige Dateien und URLs analysiert und die schnelle Erkennung von Viren, Würmern, Trojanern und Malware aller Arten ermöglicht. Es lässt sich problemlos in Security Operationsintegrieren.

Bevor Sie die -Integration VirusTotal verwenden können, müssen Sie das Plugin aktivieren und den entsprechenden API-Schlüssel hinzufügen. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Wenn die Suchquelle VirusTotal verwendet wird und Malware gefunden wird, wird ein erkennbares Element erstellt. Für IP-Suchen wird eine zusätzliche Liste von URLs erstellt, die die IP-Adresse gemeinsam nutzen, und für jede der URLs werden erkennbare Elemente erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Das Plugin Threat Intelligence ist erforderlich, um die Integration VirusTotal zu implementieren.
- Die VirusTotal -Integration wurde auf Version 3 APIs aktualisiert.

Aktivieren und konfigurieren Sie die VirusTotal-Integration

Bevor Sie die VirusTotal-Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

Vorbereitungen

Erforderliche Rolle: Administrator
Threat Intelligence muss installiert und aktiviert sein, bevor Sie VirusTotal verwenden können.
Die VirusTotal -Integration wurde auf Version 3 APIs aktualisiert.

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, rufen Sie VirusTotal auf, und rufen Sie den API-Schlüssel in Ihrem VirusTotal-Profil ab.
3. Navigieren Sie in Ihrer -Instanz zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte VirusTotal auf **Konfigurieren**.

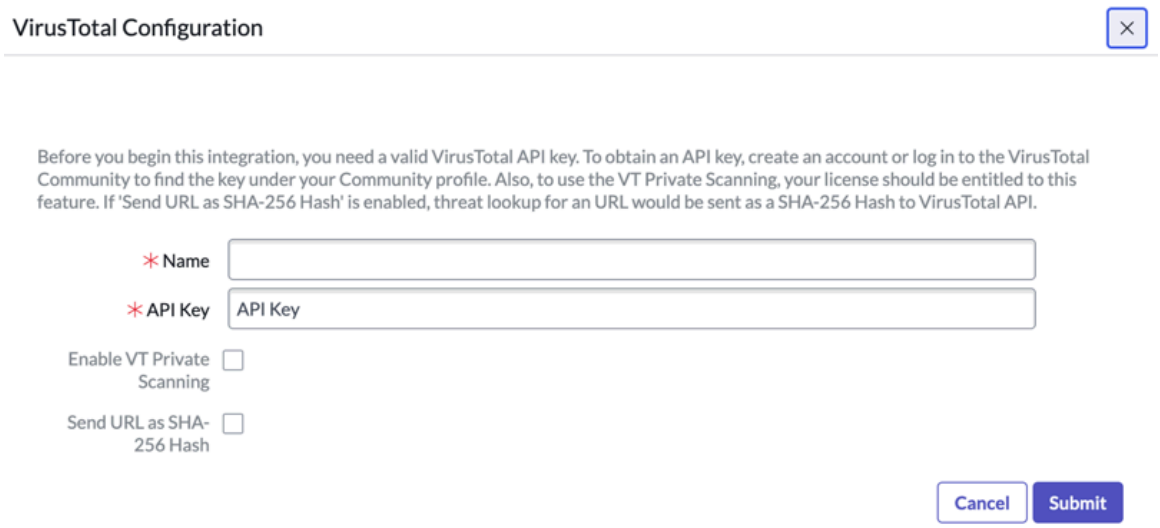
VirusTotal-Konfiguration

Feld	Beschreibung
Name	Name der Integration Beispiel: VirusTotal.
API-Schlüssel	Geben Sie den **API-Schlüssel** ein, den Sie auf der VirusTotal-Website erworben haben, (oder fügen Sie ihn ein).
VT Private Scanning aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Dateien mit VirusTotal datenschutzkonform zu analysieren. Die über dieses Angebot hochgeladenen Dateien werden nicht für Personen außerhalb Ihrer Organisation freigegeben und verbleiben nur für einen kurzen Zeitraum in VirusTotal. Die resultierenden Analysen sind ebenfalls flüchtig und nur für Ihre VirusTotal-Gruppe sichtbar. **Wichtig:** Zur Verwendung von VT Private Scanning muss Ihre VirusTotal-Lizenz für diese Funktion berechtigt sein.
URL als SHA-256-Hash senden	Aktivieren Sie dieses Kontrollkästchen, um die URLs als Hashes für die Bedrohungssuche zu senden und die Privatsphäre der Anwender in der Integration zu schützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Falls deaktiviert, wird die URL als Base64-Codierung an die VirusTotal-API gesendet.

5. Klicken Sie auf **Absenden**.



Ergebnisse

Nach der Konfiguration kann VirusTotal für die Durchführung von Suchen für erkennbare Elemente in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

Zugehörige Informationen

Führen Sie Suchen für erkennbare Elemente durch

Workflow „Bedrohungssuche – VirusTotal“.

Der Workflow „Bedrohungssuche – VirusTotal “ führt eine Suche für ausgewählte erkennbare Elemente durch. Wenn es sich bei den erkennbaren Elementen um einen von VirusTotalerkannten Typ handelt, werden sie auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Vorbereitungen

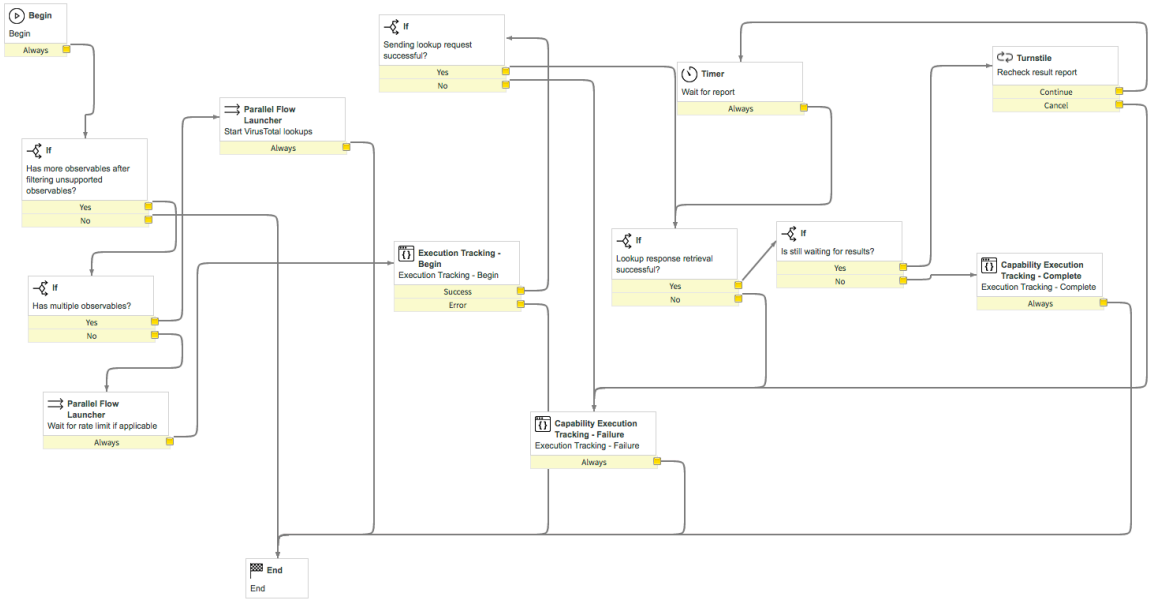
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird von Security Operations-Integration – Funktionalität zur Bedrohungssuche ausgelöst, wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen und die Implementierung VirusTotal ausgewählt ist. Weitere Informationen finden Sie unter Führen Sie Suchen für erkennbare Elemente durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow „Bedrohungssuche – VirusTotal“.



Informationen zu den von diesem Workflow verwendeten Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

WhoisXML-API-Integration

Mit der WhoisXML-API-Integration können Sie Whois-Suchen für Domänennamen und URLs übermitteln, um Kontext für erkennbare URL-Elemente zu erhalten und Bedrohungen besser zu bestimmen.

Erkunden	Einrichten
Threat Intelligence-Integrationen	• Setup der WhoisXML-API-Integration • Aktivieren und konfigurieren Sie die Whois-Integration von Security Operations
Verwenden	**Entwickeln**
Threat Intelligence - IoC-Such-Workflow ausführen	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie mit einer Anwendung installierte Komponenten

Problembehandlung und Hilfe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Problembehandlung bei Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Setup der WhoisXML-API-Integration

Bevor Sie die Whois-Integration verwenden können, müssen Sie das Plugin aktivieren und die Anmeldeinformationen hinzufügen. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Die Plugins Threat Intelligence und WhoisXML-API-Integration sind erforderlich, um die WhoisXML-API-Integration zu implementieren.

Aktivieren und konfigurieren Sie die Whois-Integration von Security Operations

Mit der Funktion „Integrationskonfiguration“ können Sie die Sicherheitsintegrationen von Drittparteien, einschließlich der Whois-Integration von Security Operations, schnell aktivieren und einrichten. Bevor Sie die Whois-Integration von Security Operations verwenden können, müssen Sie sie von ServiceNow Storeherunterladen, und Sie benötigen einen gültigen Account aus der WhoisXML-API.

Vorbereitungen

Threat Intelligence muss installiert und aktiviert werden, bevor Sie die Whois-Integration von Security Operations verwenden können.

Erforderliche Rolle: Administrator

Prozedur

1. Laden Sie die -Integration aus dem herunter ServiceNow Store.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationskonfiguration**. Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte Whois API auf **Konfigurieren**.
4. Geben Sie den Anwendernamen und das Passwort aus Ihrem WhoisXML-API-Konto ein.
5. Klicken Sie auf **Absenden**.

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Fälle, in denen das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erwerben Sie das SSL-Zertifikat von einem Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) wie folgt von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie auf **Weitere Informationen** und anschließend auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen** und anschließend auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Export**, um die PEM-Datei in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu** und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn ein Zertifikat abgelaufen ist, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .

Ergänzen Sie den WhoIs-Workflow für erkennbare Elemente

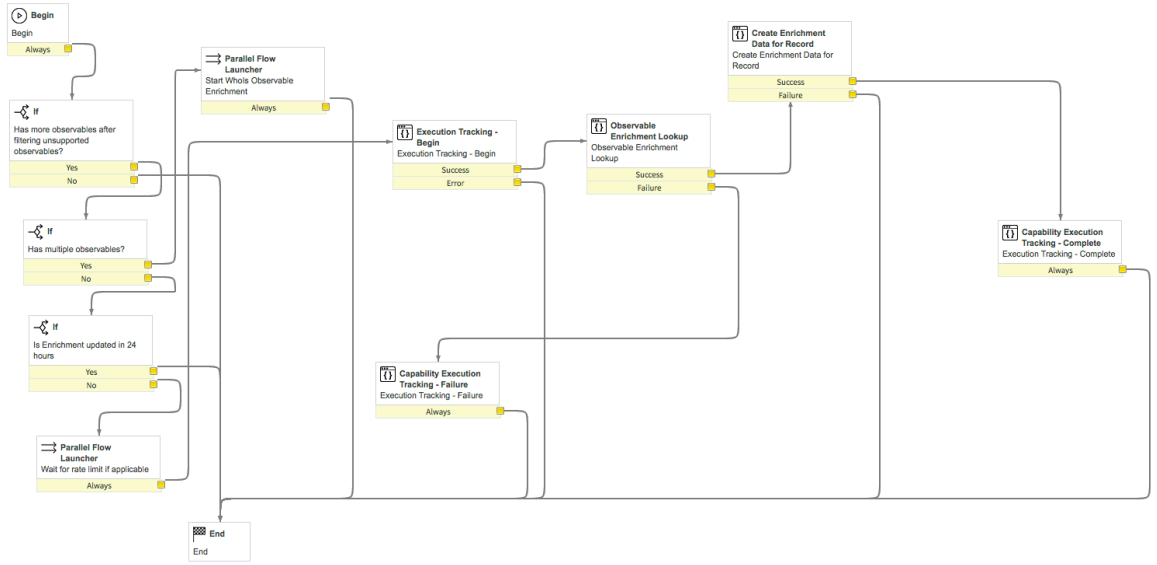
Der **WhoIs-Workflow „Erkennbares Element ergänzen“** bereichert ausgewählte erkennbare Elemente. Wenn die erkennbaren Elemente von einem Typ sind, der von WhoisXML-API-Integrationerkannt wird, werden die erkennbaren Elemente angereichert.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird von Security Operations-Integration: Fähigkeit „Erkennbares Element ergänzen“. ausgelöst, wenn Sie die Anreicherung für ein oder mehrere erkennbare Elemente durchführen und die WhoIs-Implementierung ausgewählt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergänzen Sie den WhoIs-Workflow für erkennbare Elemente



Spezifische Aktivitäten für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Aktivität „Anreicherung erkennbarer Elemente suchen“.

Die Workflow-Aktivität **„Anreicherung erkennbarer Elemente – Suche“** initiiert den Anreicherungsprozess für erkennbare Elemente.

Die Aktivität **„Anreicherung erkennbarer Elemente – Suche“** kann mit jedem Workflow für erkennbare Elemente verwendet werden, um mit der Ergänzung zu beginnen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Die Suche ist erfolgreich.
Fehlgeschlagen	Beim Versuch, die Suche durchzuführen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Implementation_id	System-ID der Implementierung, die für die Suche verwendet wird.
domain_id	Der Domänenbezeichner für die Domäne, in der die Suche ausgeführt wird.
observable_ids	Ein oder mehrere erkennbare Elemente, für die die gewünschte Aktion ausgeführt werden soll Die IDs werden als Workflow-Eingabe verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
capabilityExcutionId	Systembezeichner der Fähigkeit, die den Implementierungs-Workflow gestartet hat. Nur erforderlich für Workflows zur Implementierung von Integrationsfähigkeiten wie Splunk, Elasticsearch.
task_sys_id	System-ID für eine dem Workflow zugeordnete Aufgabe

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response_data	Vom API-Endpunkt der Implementierung für die angegebene Domäne zurückgegebene Rohdaten.
mapping_id	Der Bezeichner für die Ergänzungszuordnung. Beispielsweise gibt die WhoIs-Integration Daten in zwei verschiedenen Formaten zurück, IP und URL, mit einer Zuordnungs-ID für jedes.

Threat Intelligence Orchestration

Threat Intelligence Orchestration Mithilfe von Workflow-Orchestration können Benutzer mithilfe von Workflow-Orchestration mithilfe von Workflow-Orchestration-Lösungen ermitteln, ob eine Bedrohung bereits in anderen Security Incidents oder auf anderen Systemen erkannt wurde.

Weitere Informationen zum Bearbeiten von Security Incident Response Orchestration -Workflows oder zum Erstellen von anwenderdefinierten Workflows finden Sie unter Erste Schritte mit Workflows und Workflow-Editor Workflow-Editor .

Richten Sie Threat Intelligence Orchestration ein

Führen Sie vor der Verwendung von Threat Intelligence OrchestrationSchritte aus, um verschiedene Teile des Systems einzurichten, einschließlich CMDB-Auffüllung, Konfiguration des MID-Servers und Konfiguration der Anmeldeinformationen.

Vorbereitungen

Erforderliche Rolle: Administrator

Zur Verwendung von Threat Intelligence Orchestration benötigen Sie eine vollständig ausgefüllte CMDB mit Domänennamen. Weitere Informationen finden Sie unter Discovery .

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Aktivieren Sie das Threat Intelligence Plugin.
2. Konfigurieren Sie den MID-Server
3. Konfigurieren Sie die Anmeldeinformationen für den MID-Server-Service
   Sie können jetzt Threat Intelligence Orchestration -Aktivitäten in einem Workflow verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflows und Aktivitäten von Threat Intelligence Orchestration

Das Basissystem enthält Workflows und Workflow-Aktivitäten, mit denen Sie Aktionen in Ihrer -Instanz automatisieren können.

Threat Intelligence - IoC-Such-Workflow ausführen

Der Workflow **„Threat Intelligence – IoC-Suche ausführen“** überprüft, ob ein nicht abgelaufenes erkennbares Element vorhanden ist. Wenn dies der Fall ist, wird die Suche auf **Abgeschlossen** gesetzt und mit den Daten des erkennbaren Elements aktualisiert.

Vorbereitungen

Erforderliche Rolle: sn_si.basic

Hinweis:

Dieser Workflow ersetzt Threat Intelligence Orchestration Business-Regeln (**Mit vorhandenen IoC-Tabellen ausfüllen**, **Suche in Warteschlange stellen**und **Erkennbares Element aktualisieren**) durch Aktivitäten.

Wenn eine Suche eingefügt oder aktualisiert wird und die Bedingungen erfüllt, löst die Geschäftsregel Suche diesen Workflow aus.

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow **„Threat Intelligence – IoC-Suche ausführen“** überprüft, ob ein nicht abgelaufenes erkennbares Element vorhanden ist. Wenn dies der Fall ist, wird die Suche auf **Abgeschlossen** gesetzt und mit den Daten des erkennbaren Elements aktualisiert. Alle dem erkennbaren Element zugeordneten Indikatoren werden erneut aktiviert.

Wenn das erkennbare Element abgelaufen ist, führt der Workflow die Suchvorgänge aus und erhöht die **Sichtungsanzahl** im vorhandenen, abgelaufenen erkennbaren Element.

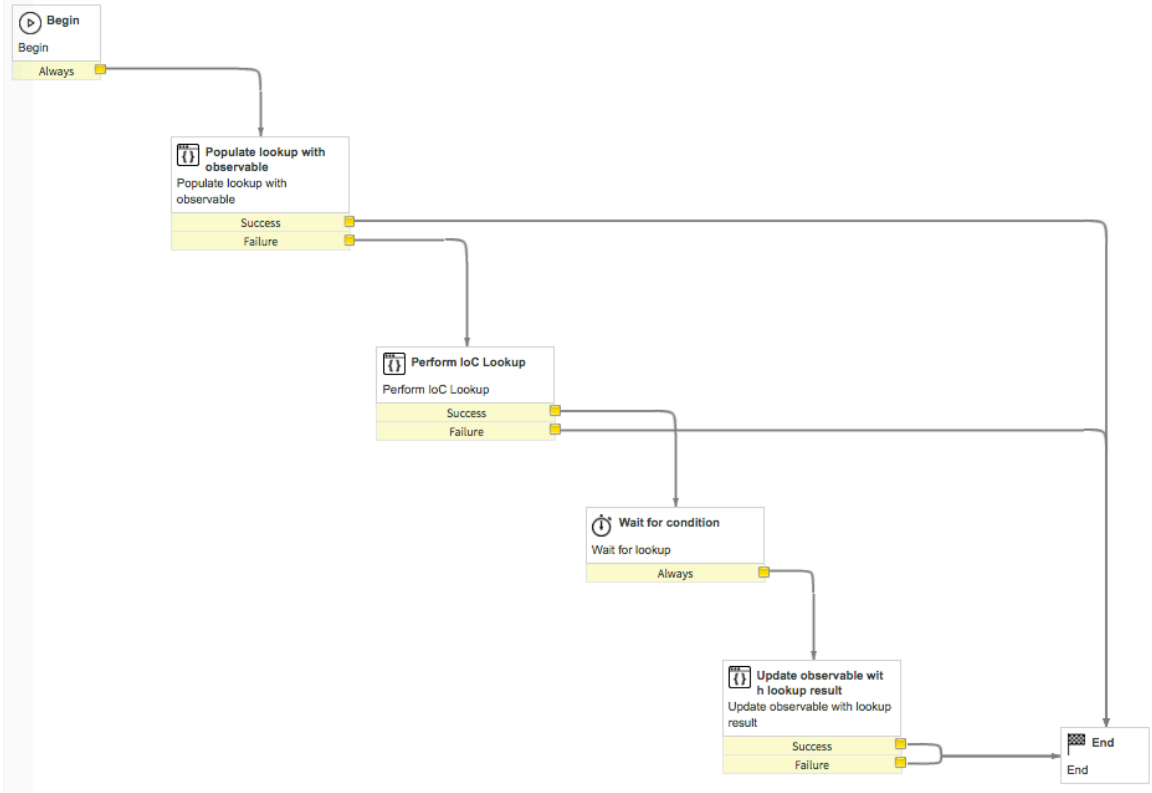
Wenn kein korrelierendes erkennbares Element vorhanden ist, wird ein neues erkennbares Element mit Indikator erstellt.

Zu den Workflow-Prozessaktivitäten gehören:

- Füllen Sie die Suche mit der Aktivität erkennbarer Elemente aus
- Führen Sie die Aktivität „IoC-Suche“ durch
- Auf Suche warten (Kernaktivität)
- Erkennbares Element mit Suchergebnisaktivität aktualisieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence: IoC-Such-Workflow ausführen



Füllen Sie die Suche mit der Aktivität erkennbarer Elemente aus

Wenn ein nicht abgelaufenes erkennbares Element gefunden wird, **liefert die Workflow-Aktivität Threat Intelligence Orchestration – Suche mit erkennbarem Element** ausfüllen Daten aus einem vorhandenen erkennbaren Element für eine Suche. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Bei Auslösung durch einen Workflow versucht **„Suche mit erkennbarem Element füllen“** ein vorhandenes erkennbares Element für eine Suche zu finden, das dem **Wert** und **Typ** der Suche entspricht, die der Aktivität als Eingabe bereitgestellt wurde.

Wenn das erkennbare Element vorhanden und nicht abgelaufen ist, diese Aktivität:

- Aktualisiert die Suche mit den im erkennbaren Element gefundenen Informationen
- Reaktiviert einen Indikator, wenn er inaktiv ist, erhöht die **Anzahl der ermittelten Werte**und aktualisiert das Datum **der letzten Anzeige**
- Legt **den Status** auf „Abgeschlossen“ fest.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen	Beschreibung
scanID[Zeichenfolge]	Suchbezeichner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen	Beschreibung
wahr	Gültiges erkennbares Element gefunden und Suche aktualisiert.
falsch	Es wurde kein gültiges erkennbares Element gefunden. Erkennbares Element fehlt oder ist abgelaufen.

Führen Sie die Aktivität „IoC-Suche“ durch

Die Workflow-Aktivität **„Threat Intelligence Orchestration – IoC-Suche durchführen“** führt eine bestimmte Suche durch. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Wenn dies von einem Workflow ausgelöst wird, verwendet **„IoC-Suche durchführen“** eine scanID, sucht den Suchdatensatz und fügt die Suche der Warteschlange hinzu, indem ein Suchwarteschlangeneintrag erstellt wird.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
scanID[Zeichenfolge]	Suchbezeichner

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
wahr	Die Suche wurde ausgelöst.
falsch	Die Suche wurde nicht ausgelöst.

Erkennbares Element mit Suchergebnisaktivität aktualisieren

Die Workflow-Aktivität **„Threat Intelligence Orchestration – Erkennbares Element mit Suchergebnis aktualisieren“** aktualisiert den Datensatz des erkennbaren Elements. Wenn eines nicht vorhanden ist, wird ein neues erkennbares Element erstellt. Diese Aktivität ist nützlich, um Informationen zu protokollieren.

Wird dies von einem Workflow ausgelöst **, aktualisiert Erkennbares Element mit Suchergebnis** aktualisieren ein vorhandenes erkennbares Element mit der neuen **Sichtungsanzahl**, fügt eine Notiz hinzu und reaktiviert Indikatoren, falls inaktiv. Die **Anzahl erkannter Elemente** und das Datum **der letzten Anzeige** im Indikator werden ebenfalls aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn kein korrelierendes erkennbares Element vorhanden ist, erstellt der Workflow wie folgt ein neues erkennbares Element mit dem folgenden Indikator:

- Führt die IoC-Suchen aus
- Erstellt ein neues erkennbares Element
- Erstellt einen Indikator für das erkennbare Element
- Fügt dem erkennbaren Element eine **Sichtungsanzahl** hinzu
- Fügt dem Indikator eine **Anzahl erkannter Elemente** und ein Datum **der letzten Anzeige** hinzu
- Fügt eine Nachricht hinzu, die angibt, aus welcher Suche sie erstellt wurde

.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
scanID[Zeichenfolge]	Suchbezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
wahr	Die Aktualisierung oder Erstellung des erkennbaren Elements war erfolgreich.
falsch	Fehler beim Aktualisieren oder Erstellen des erkennbaren Elements.

Führen Sie die Aktivität „Standard-IoC-Suchquellen“ aus

Wenn dies von einem Workflow ausgelöst wird, akzeptiert Threat Intelligence - **Standard-IoC-Suchquellen** ausführen eine Suchanforderungs-ID und erstellt abhängig von den eingegebenen Datenwerten mehrere Suchvorgänge.

Für jeden Datentyp wird die **Scan-Spalte „include_in_bulk“** der Tabelle der unterstützten Suchtypen jeder Suchquelle ausgewertet. Bei „wahr“ wird der Suchanforderung eine Suche hinzugefügt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
scan_request_id	Systembezeichner für Suchanforderung

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Anzahl der erstellten Scans	Ganzzahl

Security Case Management

Management von Sicherheitsfällen bietet Sicherheitsanalysten, die an der Bedrohungssuche beteiligt sind, die Möglichkeit, Informationen über verdächtige Aktivitäten in ihrer Umgebung zu sammeln. Fallbezogene Datensätze, wie z. B. Security Incidents, erkennbare Elemente, CIs und betroffene Benutzer, können Fällen hinzugefügt werden, um eine umfassende und spezifische Analyse zu ermöglichen.

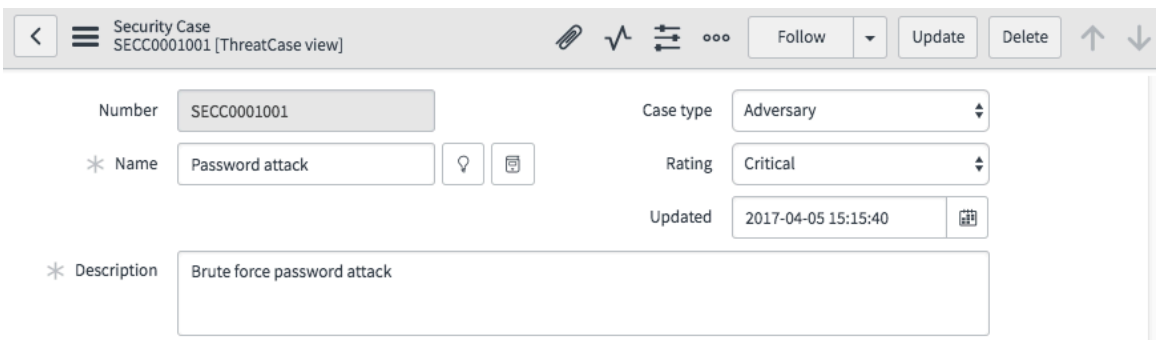
Mit der Möglichkeit, einfach durch die Datensätze und zugehörigen Informationen zu navigieren, können Analysten beurteilen, ob sie einer gezielten Kampagne, einer erweiterten persistenten Bedrohung oder Ähnlichem ausgesetzt sind.

Sicherheitsfälle können aus verschiedenen Quellen in Ihrer Instanz erstellt werden, einschließlich Management von Sicherheitsfällen, Security Incident Responseund Threat Intelligence. Sie können auch Fälle aus Konfigurationselementen und betroffenen Benutzern in den Tabellen Konfigurationselemente [cmdb.ci] und Benutzer [sys.user] erstellen. Nachdem Fälle erstellt wurden, können jede dieser Quellen auch verwendet werden, um vorhandenen Fällen wertvolle Analyseressourcen hinzuzufügen.

Jeder Sicherheitsfall besteht aus drei Hauptabschnitten, einem Headerabschnitt, einem Abschnitt mit zusätzlichen Falldetails und einem Abschnitt mit Fallartefakten, der eine Sammlung von Datensätzen enthält, die beim Aufbau eines Arguments für die Identifizierung und Behandlung bestimmter Bedrohungen helfen.

Fallheader

Headerabschnitt des Falls

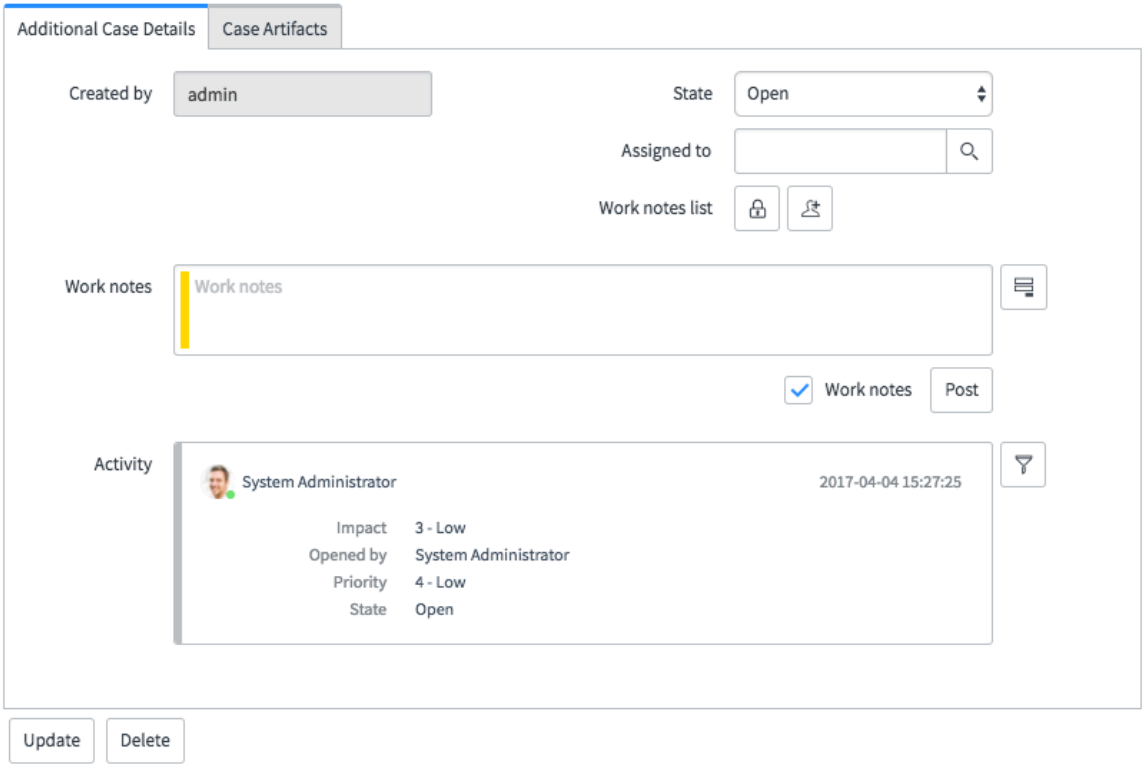


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Fall-Header enthält grundlegende Informationen, die zum Identifizieren und Klassifizieren des Sicherheitsfalls verwendet werden. Die Fallnummer verwendet das Präfix SECC.

Zusätzliche Falldetails

Abschnitt „Zusätzliche Falldetails“.



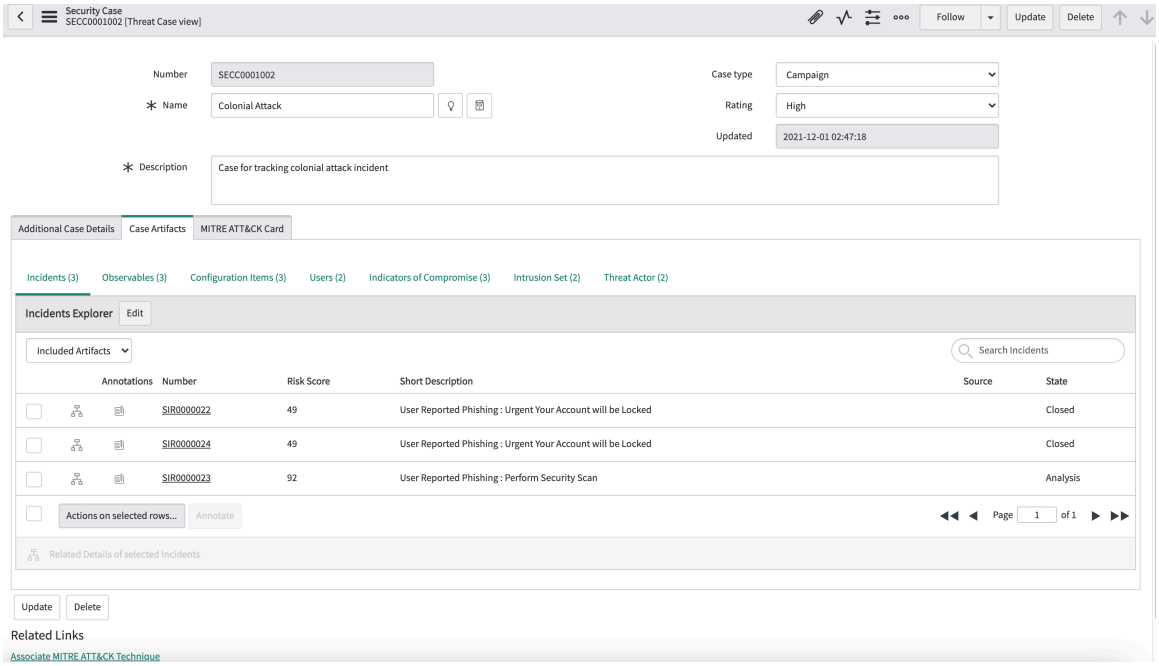
Der Abschnitt **„Zusätzliche Falldetails“** enthält spezifische Informationen zu der Analyse, die bereits für den Fall durchgeführt wurde, einschließlich des aktuellen Status sowie der für den Fall aufgezeichneten Arbeitsnotizen und Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fallartefakte

Abschnitt „Fallartefakte“.



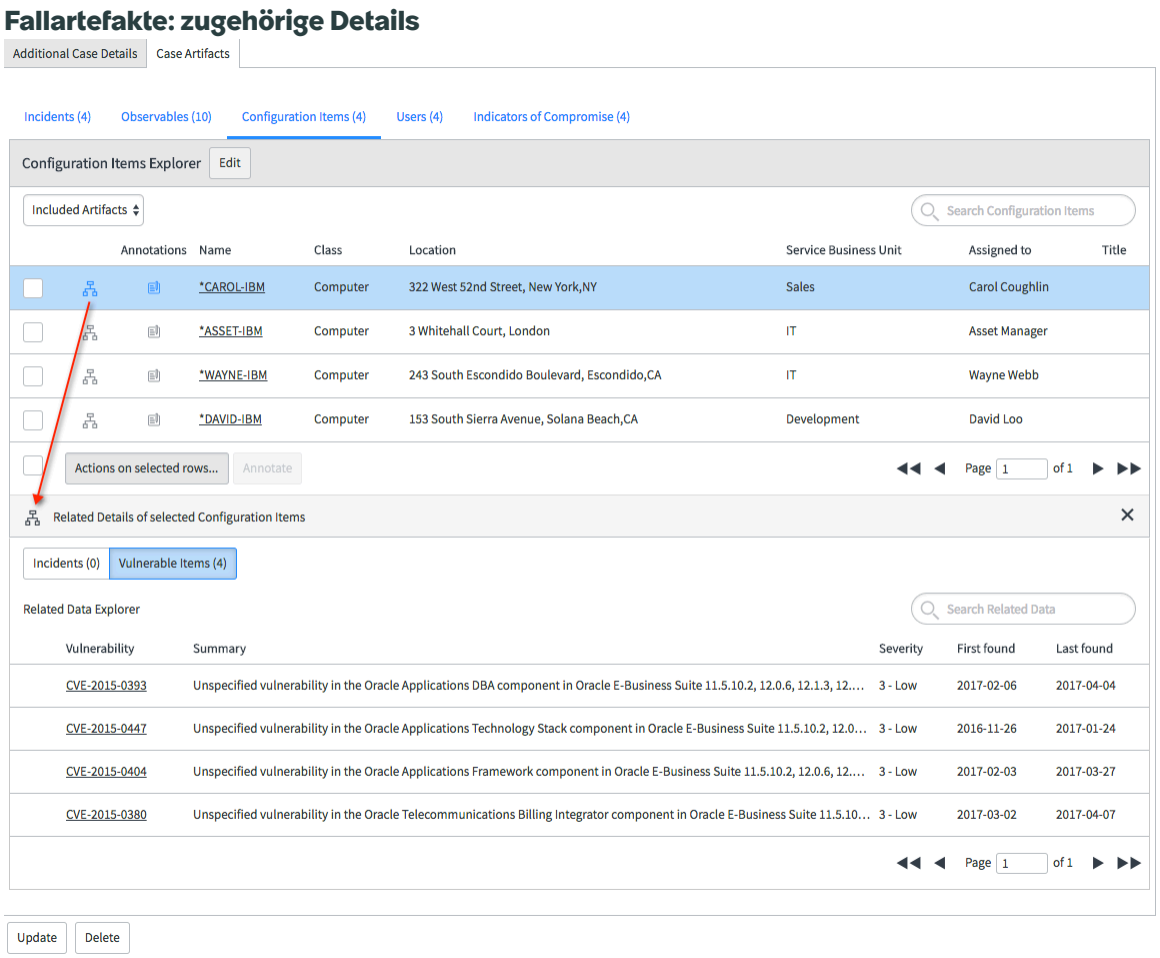
Der Abschnitt **„Fallartefakte“** enthält eine Reihe von Registerkarten mit Informationen, die im Sicherheitsfall enthalten sind.

Sie können im Inhalt jeder Registerkarte Suchen durchführen. Sie können auch bestimmte Datensätze ausschließen, die Sie bereits als sicher eingestuft haben oder die für Ihre Untersuchung keinen Wert haben. Die ausgeschlossenen Datensätze werden nicht gelöscht, sind jedoch ausgeblendet. Bei Bedarf können Sie ausgeschlossene Datensätze anzeigen und wieder hinzufügen.

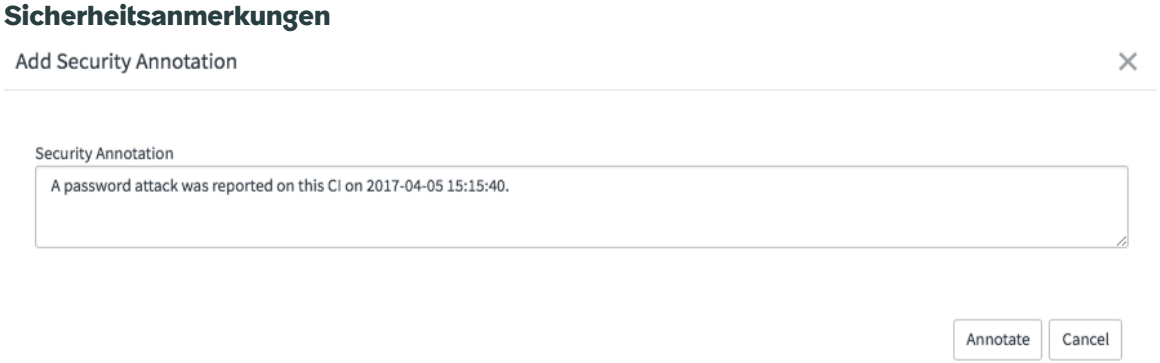
Auf jeder Registerkarte können Sie auf das Symbol „Zusätzliche Details“ klicken, um zugehörige Informationen für den ausgewählten Datensatz anzuzeigen. Wenn Sie beispielsweise auf die Registerkarte **Konfigurationselemente** klicken, um den Konfigurationselemente-Explorer anzuzeigen, und für ein bestimmtes CI auf Zusätzliche Details klicken, können Sie Incidents, angreifbare Elemente und Anmerkungen anzeigen, die diesem CI zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können auch einen Datensatz auswählen und für ein fallbezogenes Artefakt auf die Schaltfläche **Kommentieren** klicken, um dem Datensatz Anmerkungen hinzuzufügen. Anmerkungen sind einfach Notizen, die jeder Analyst zu einem bestimmten Artefakt machen kann.



Andere Tools, die der Analyst zur Untersuchung von Fällen verwenden kann, sind:

- Führt eine Sichtungssuche für erkennbare Elemente in einem Fall durch
- Suchen Sie nach Sicherheitsartefakten

Erstellen Sie Fälle in der Verwaltung von Sicherheitsfällen

Fälle werden verwendet, um Informationen über eine Kampagne oder einen staatlichen Akteur nachzuverfolgen, die Ihre Organisation bedrohen. Nachdem ein Fall erstellt wurde,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie Artefakte hinzufügen, mit denen Sie alle zugehörigen Informationen in einem einzigen Falldatensatz überprüfen und analysieren können.

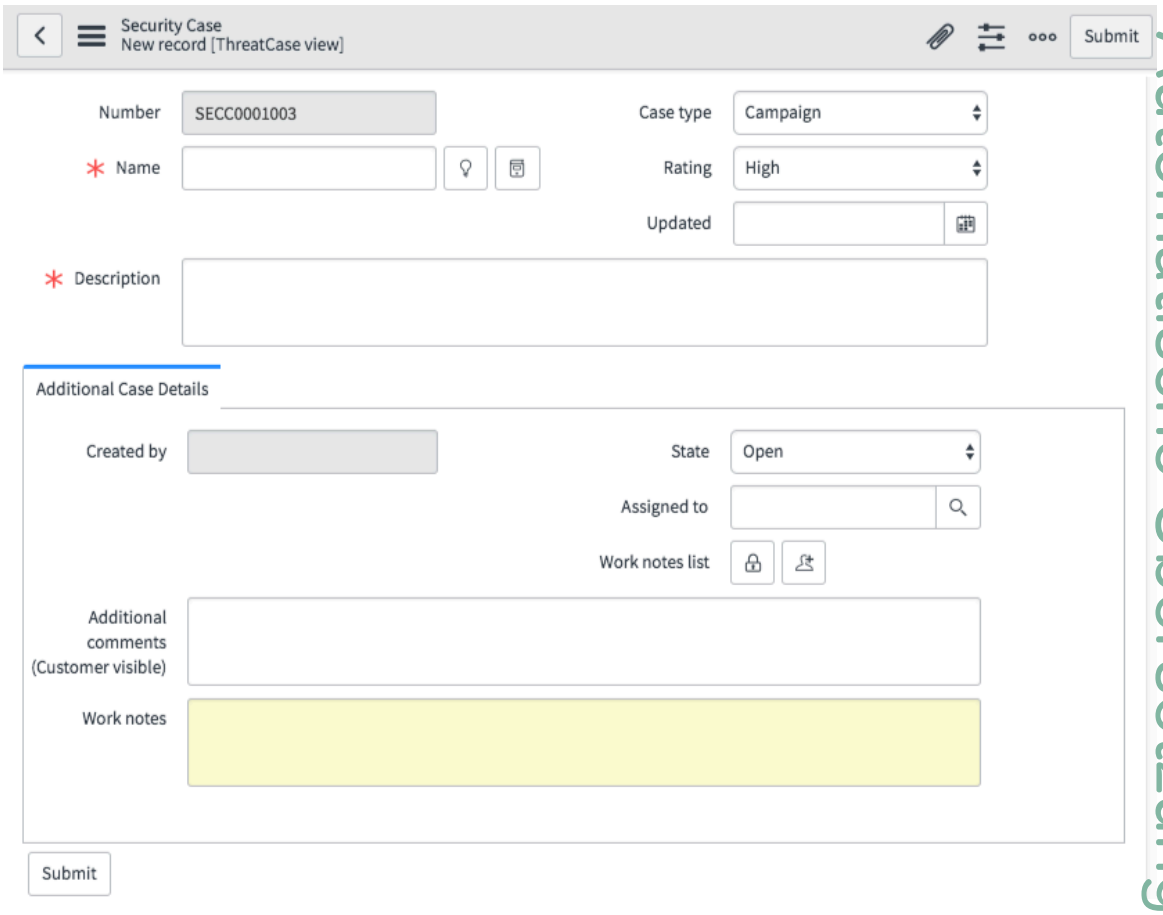
Vorbereitungen

Erforderliche Rolle: sn_ti.case_use

r

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**.
   Die Liste der Sicherheitsfälle wird geöffnet.
2. Klicken Sie auf **Neu**.
   Der Bildschirm „Security Cases“ wird geöffnet.



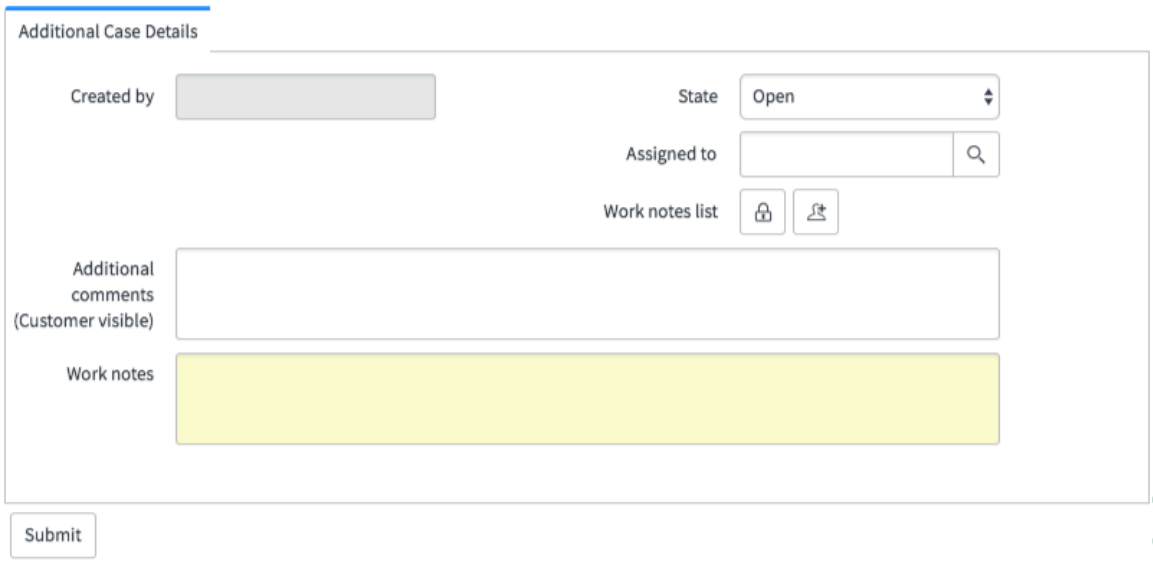
Automatische Übersetzung

3. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Fallnummer	[Schreibgeschützt] Die Fallnummer.
Fallname	Geben Sie einen beschreibenden Namen für den Fall ein.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus.
Bewertung	Wählen Sie die Wichtigkeit dieses Falls aus (von „Kritisch“ bis „Niedrig“).
Letztes Update	[Schreibgeschützt] Datum und Uhrzeit der letzten Aktualisierung des Falls.
Kurzbeschreibung	Eine kurze Beschreibung des Falls.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **Zusätzliche Falldetails**.



5. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Erstellt von	[Schreibgeschützt] Der Name des Anwenders, der diesen Fall erstellt hat.
Status	Aktueller Status des Falls. Bei der Fallerstellung wird standardmäßig der Status auf Entwurf festgelegt.
Zugewiesen an	Klicken Sie auf das Suchsymbol, und weisen Sie den Fall einem Analysten zu.
Arbeitsnotizenliste	Klicken Sie auf das Sperrsymbol, und fügen Sie interne Benutzer hinzu, die Arbeitsnotizen anzeigen können.
Zusätzliche Anmerkungen	Geben Sie nach Bedarf Notizen zum Fall ein, die für den Kunden sichtbar sind.
Arbeitsnotizen	Geben Sie bei Bedarf eine Arbeitsnotiz für den Fall ein.

6. Klicken Sie auf **Absenden**.
   Nachdem der Datensatz gespeichert wurde, können Sie auf die Registerkarte **Fallartefakte** klicken und dem Fall Artefakte hinzufügen.

Fügen Sie einem Fall Artefakte hinzu

Nachdem Sie einen Fall erstellt haben, können Sie ihm Artefakte hinzufügen, z. B. Security Incidents, CIs und Kompromittierungsindikatoren. Diese Artefakte dienen als Hinweise zur Lösung des Falls.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

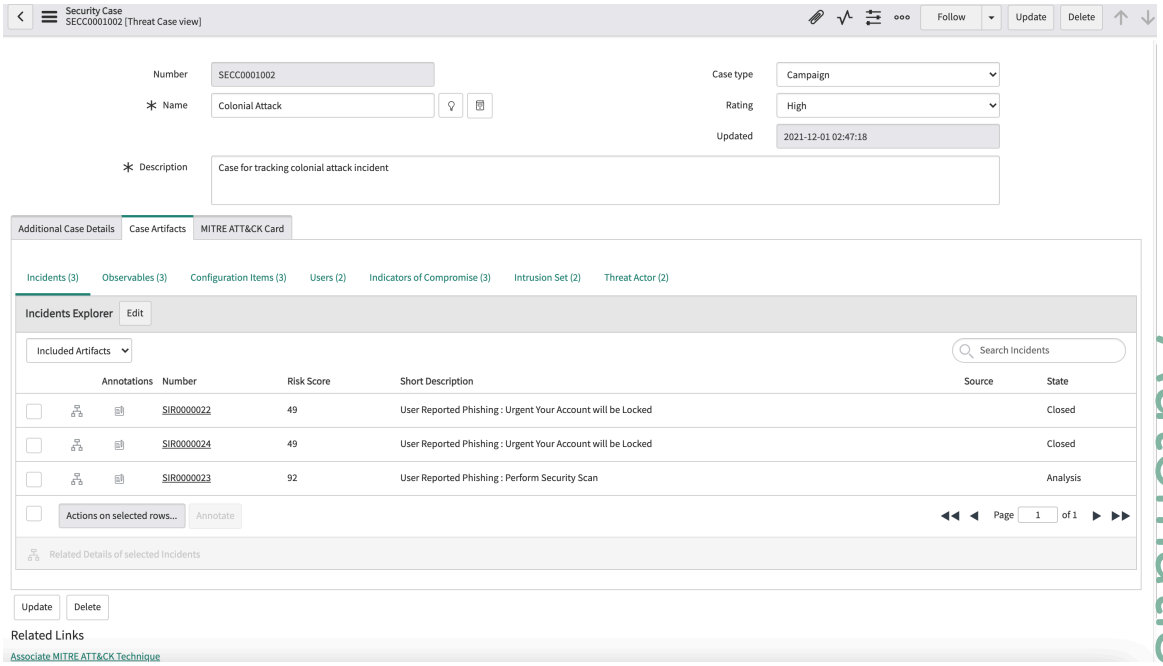
Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

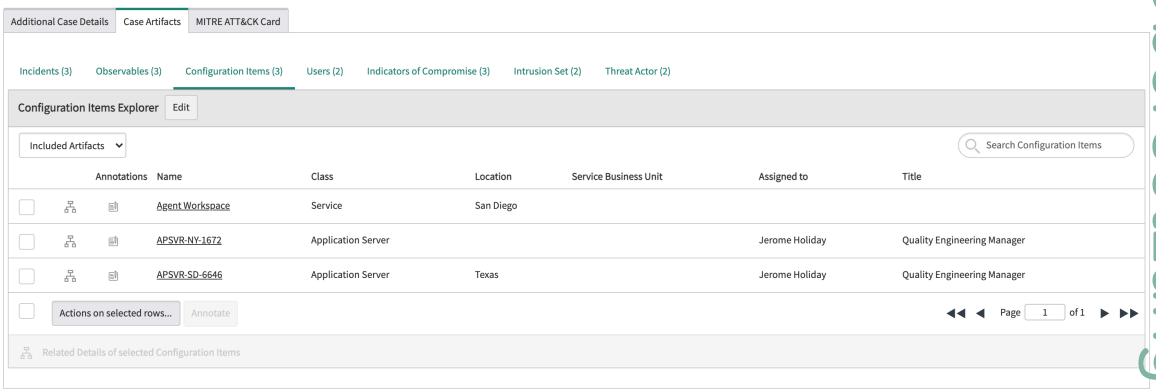
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie einen Fall, dem Sie Artefakte hinzufügen möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.



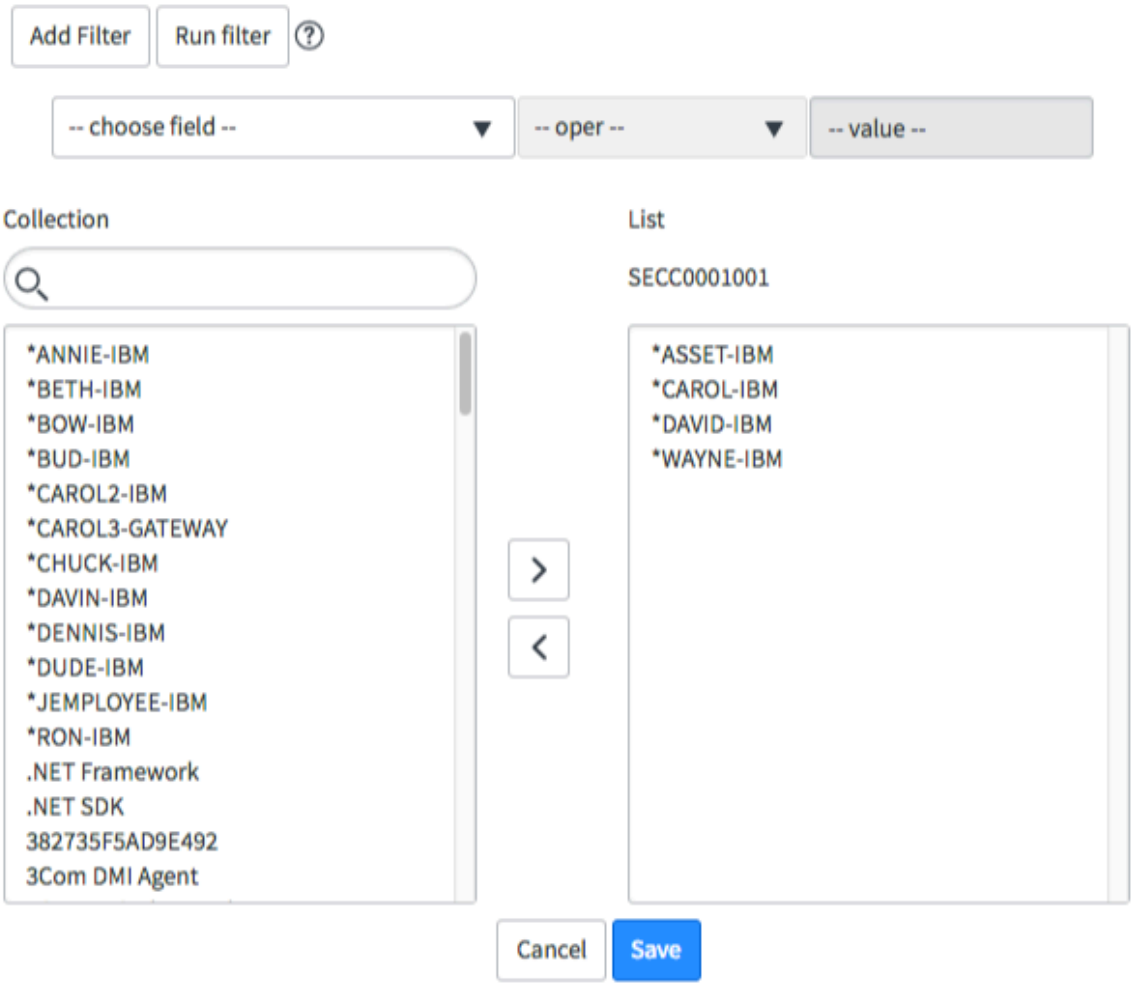
3. Klicken Sie auf die Registerkarte, die dem Artefakttyp zugeordnet ist, das Sie dem Fall hinzufügen möchten. Klicken Sie beispielsweise auf **Configuration Items (Konfigurationselemente)**, um dem Fall ein oder mehrere CIs hinzuzufügen.



4. Klicken Sie auf **Bearbeiten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Suchen Sie mithilfe des Slushbucket und der Filter nach den Artefaktdatensätzen, die Sie dem Fall hinzufügen möchten, verschieben Sie sie aus dem Bucket Sammlung in den Bucket Liste, und klicken Sie auf **Speichern**.
   Die Liste wird auf der ausgewählten Registerkarte angezeigt, und die ausgewählten Artefakte werden der Liste hinzugefügt.

Zugehörige Informationen

Fügen Sie einem vorhandenen Fall IoCs und erkennbare Elemente hinzu

Fügen Sie einem vorhandenen Fall Security Incidents hinzu

Fügen Sie CIs zu vorhandenen Fällen hinzu

Fügen Sie betroffene Anwender zu vorhandenen Fällen hinzu

Ordnen Sie die Informationen MITRE-ATT&CK dem Sicherheitsfall zu

Ordnen Sie MITRE-ATT&CK Taktiken und Techniken einem Sicherheitsfall zu, um das Management von Sicherheitsfällen und die Bedrohungsanalyse auf granularer Ebene zu verbessern.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

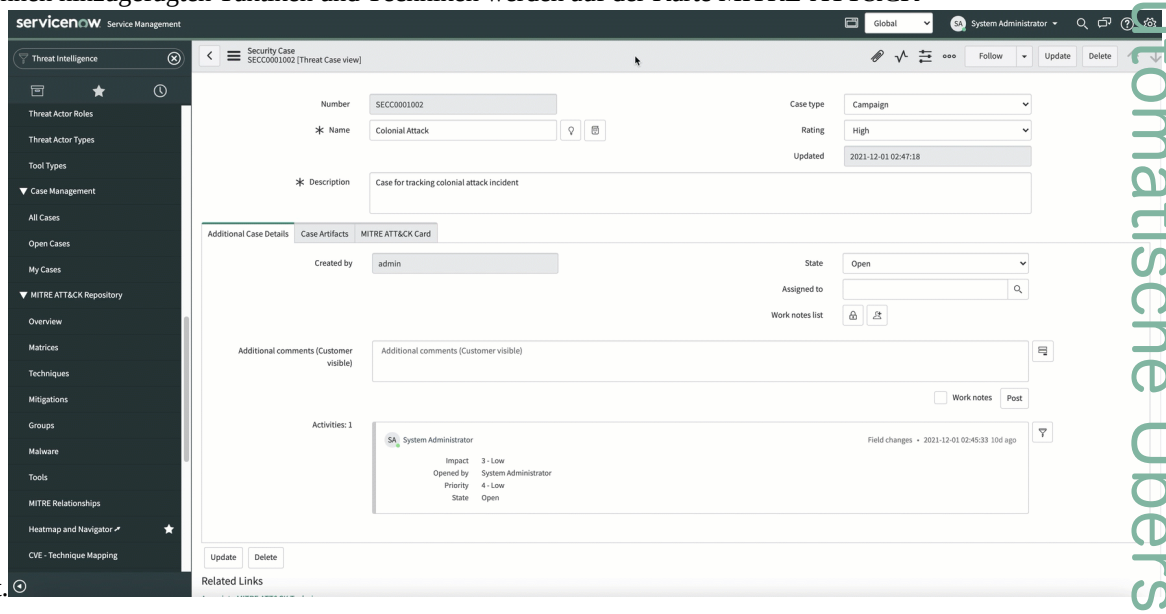
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**.
2. Wählen Sie den Sicherheitsfall aus, den Sie mit den MITRE-ATT&CK-Informationen anreichern möchten.
3. Klicken Sie in der zugehörigen Liste **auf MITRE ATT&CK-Technik zuordnen**.

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu **MITRE ATT&CK-Technik**zuordnen navigieren, die Quelle überprüfen und eine Taktik und Technik hinzufügen.

4. Überprüfen Sie in den Quellenlisten die **Quelle**.
5. Überprüfen Sie die **Taktik** und **die Techniken**, und fügen Sie sie basierend auf der Relevanz für den Fall hinzu, oder entfernen Sie sie.
6. Klicken Sie auf **Speichern**.
   Die von Ihnen hinzugefügten Taktiken und Techniken werden auf der Karte MITRE-ATT&CK angezeigt.



Fallerstellung aus Sicherheitsartefakten

Neben der manuellen Erstellung von Fällen über Management von Sicherheitsfällenkönnen Sie auch Fälle aus Sicherheitsartefakten wie Security Incidents, Kompromittierungsindikatoren, betroffenen Benutzern und Konfigurationselementen erstellen.

IoCs und erkennbare Elemente in Fällen

In Threat Intelligencekönnen Sie Fälle aus IoCs und erkennbaren Elementen erstellen sowie vorhandenen IoCs und erkennbaren Elementen hinzufügen. Sie können erkennbare Elemente auch direkt aus einem Fall erstellen.

Erstellen Sie einen Fall aus IoCs oder erkennbaren Elementen

In Threat Intelligencekönnen Sie einen Fall aus Artefakten (IoCs oder erkennbare Elemente) erstellen. Nachdem die IoCs oder erkennbaren Elemente zum Erstellen eines Falls verwendet wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

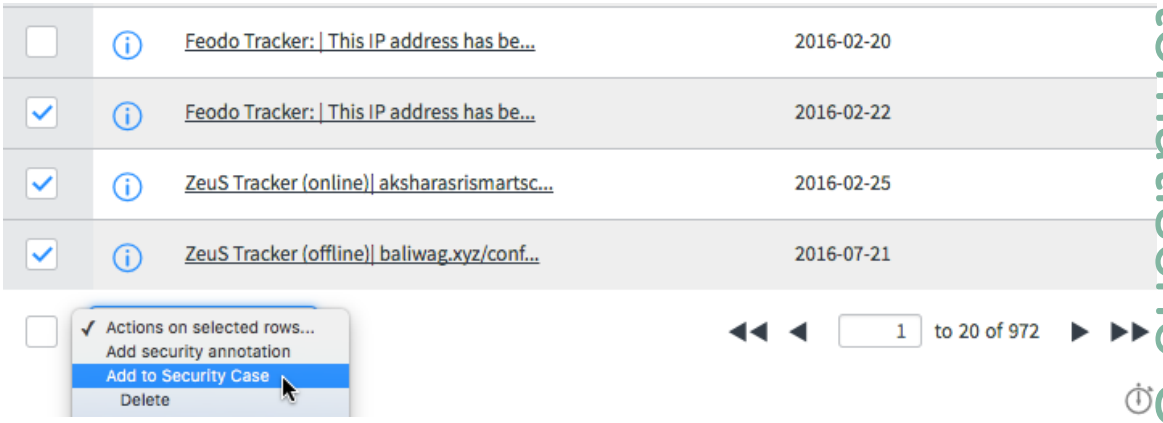
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

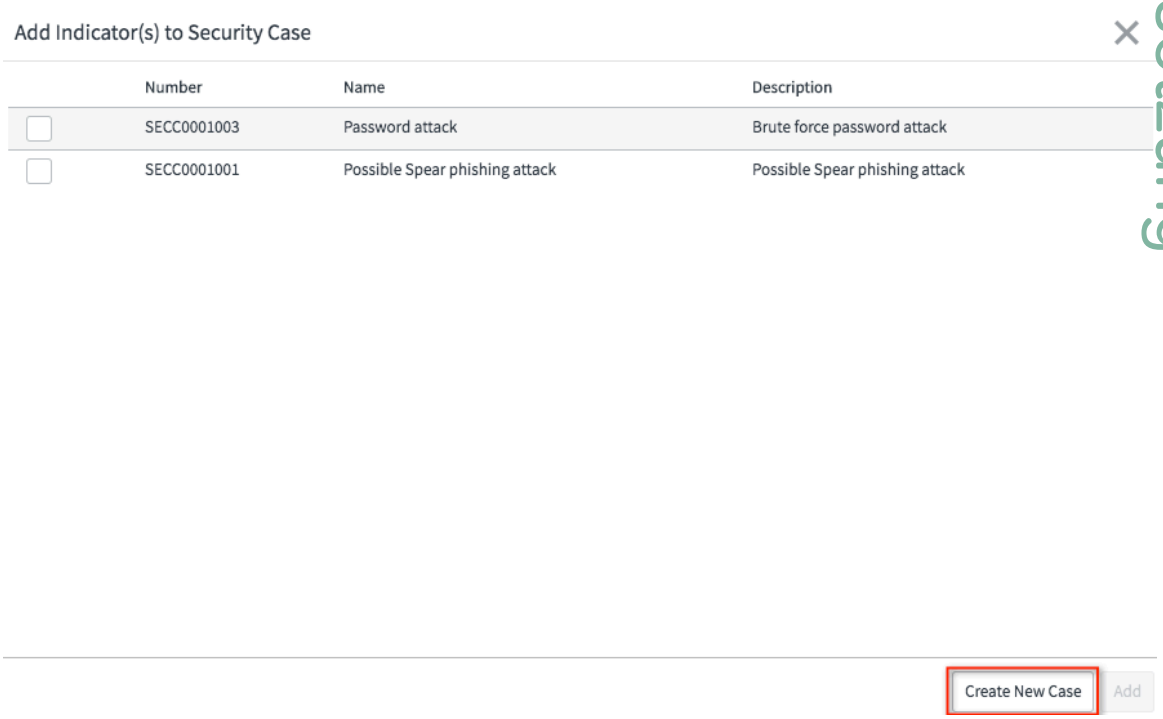
1. Navigieren Sie zu den Artefakten (IoCs oder erkennbaren Elemente), die Sie zum Erstellen eines Falls verwenden möchten.
   - Um einen Fall aus IoCs zu erstellen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
   - Um einen Fall aus erkennbaren Elementen zu erstellen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Wählen Sie in der Liste die Artefakte aus, die Sie einem neuen Fall hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere IoCs oder erkennbare Elemente auswählen, werden sie alle dem Fall hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.



Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte.

6. Klicken Sie auf **Absenden**.
   Eine Meldung oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie einem vorhandenen Fall IoCs und erkennbare Elemente hinzu

Sie können IoCs und erkennbaren Elemente zu vorhandenen Fällen hinzufügen. Nachdem die Security Incidents zu Fällen hinzugefügt wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

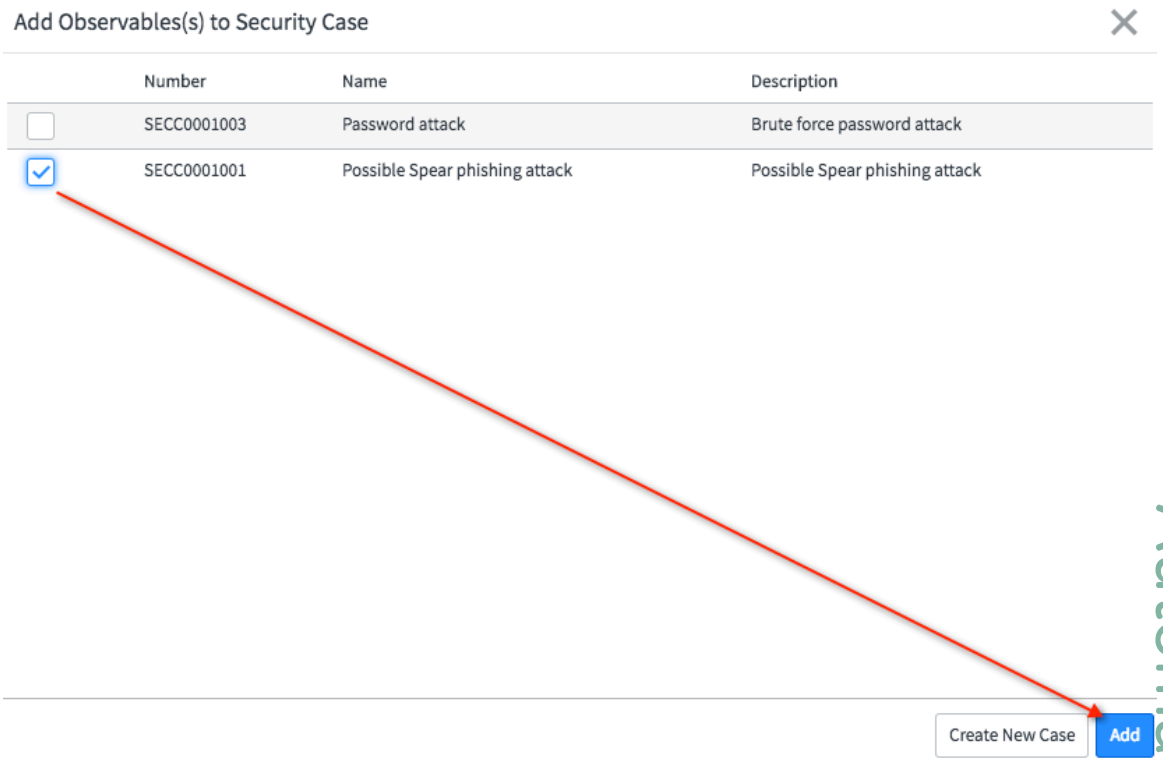
Prozedur

1. Navigieren Sie zu den Artefakten (IoCs oder erkennbaren Elemente), die Sie vorhandenen Fällen hinzufügen möchten.
   - Um einem oder mehreren Fällen IoCs hinzuzufügen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
   - Um einem oder mehreren Fällen erkennbare Elemente hinzuzufügen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Wählen Sie in der Liste die Artefaktdatensätze aus, die Sie vorhandenen Fällen hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere Fälle auswählen, werden die ausgewählten IoCs oder erkennbaren Elemente jedem der ausgewählten Fälle hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.
   Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.
4. Wählen Sie die Fälle aus, denen Sie die ausgewählten IoCs oder erkennbaren Elemente hinzufügen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Hinzufügen**.
   Eine Meldung zeigt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Erstellt ein erkennbares Element aus einem Fall

Neue erkennbare Elemente können aus Fällen in Management von Sicherheitsfällenerstellt werden.

Vorbereitungen

Erforderliche Rolle: sn_ti.case_user

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**.
   Die Liste der Sicherheitsfälle wird geöffnet.
2. Öffnen Sie entweder einen vorhandenen Fall, oder klicken Sie auf **Neu,** um einen neuen Fall zu erstellen.
3. Klicken Sie auf den zugehörigen Link **Fallartefakte** und anschließend auf die Registerkarte **Erkennbare Elemente**.
4. Klicken Sie auf **Neu** und geben Sie die erforderlichen Informationen ein.

Feld	Beschreibung
Wert	[Schreibgeschützt] Die Fallnummer.
Erkennbarer Typ	Geben Sie einen beschreibenden Namen für den Fall ein.
Typkategorie erkennbarer Elemente	Wählen Sie den Typ des untersuchten Falls aus.
Incident-Anzahl	Wählen Sie die Wichtigkeit dieses Falls aus (von „Kritisch“ bis „Niedrig“).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ergebnis	[Schreibgeschützt] Datum und Uhrzeit der letzten Aktualisierung des Falls.
Notizen	Eine kurze Beschreibung des Falls.

5. Klicken Sie auf die Registerkarte **Zusätzliche Falldetails**.
6. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Erstellt von	[Schreibgeschützt] Der Name des Anwenders, der diesen Fall erstellt hat.
Status	Aktueller Status des Falls. Bei der Fallerstellung wird standardmäßig der Status auf Entwurf festgelegt.
Arbeitsnotizenliste	Aktivieren Sie das Kontrollkästchen, um die Arbeitsnotizen im Abschnitt Zusätzliche Falldetails des Falldatensatzes anzuzeigen.
Arbeitsnotizen	Geben Sie bei Bedarf eine Arbeitsnotiz für den Fall ein. Wenn die **Liste Arbeitsnotizen** ausgewählt ist, wird die Arbeitsnotiz im Abschnitt Zusätzliche Falldetails des Falldatensatzes angezeigt.

7. Klicken Sie auf **Absenden**.
   Bei Bedarf können Sie auf die Registerkarte **Fallartefakte** klicken und dem Fall Artefakte hinzufügen.

Führt eine Sichtungssuche für erkennbare Elemente in einem Fall durch

Sie können mit der Sichtungssuche nach erkennbaren Elementen suchen, um zu bestimmen, wie häufig sie vorkommen. Jedes Auftreten gilt als *Sichtung*. Sie können die Suche auf die Anzahl der Sichtungen innerhalb einer ausgewählten Anzahl von Tagen oder innerhalb eines Datumsbereichs beschränken.

Vorbereitungen

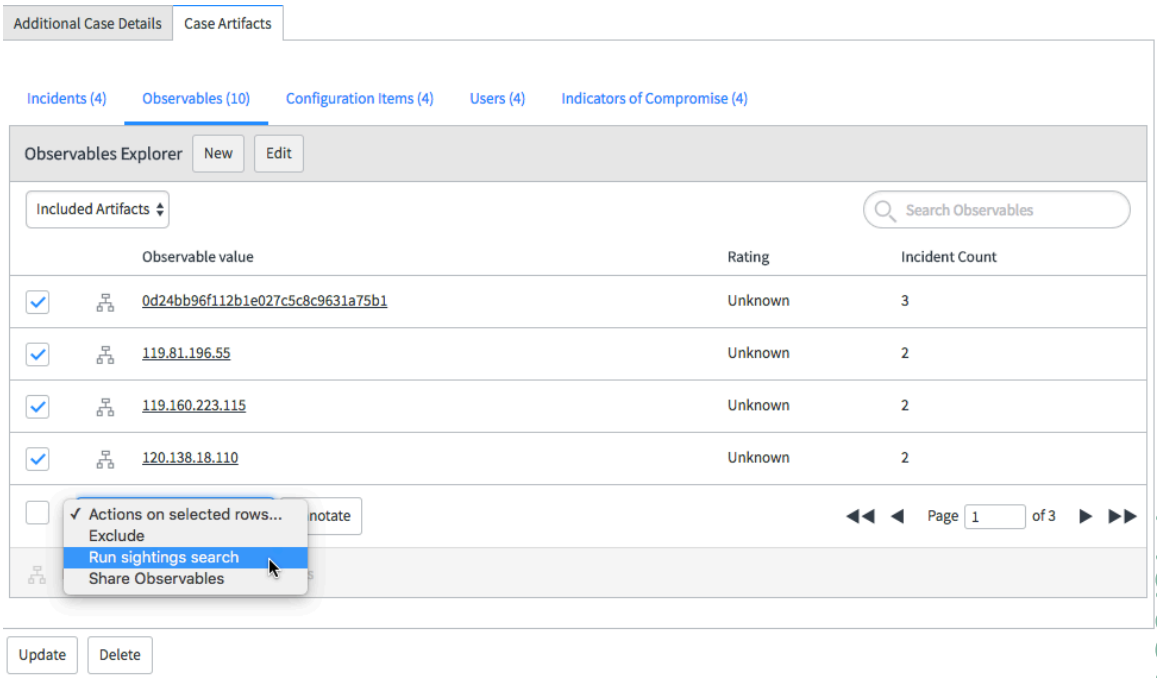
Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

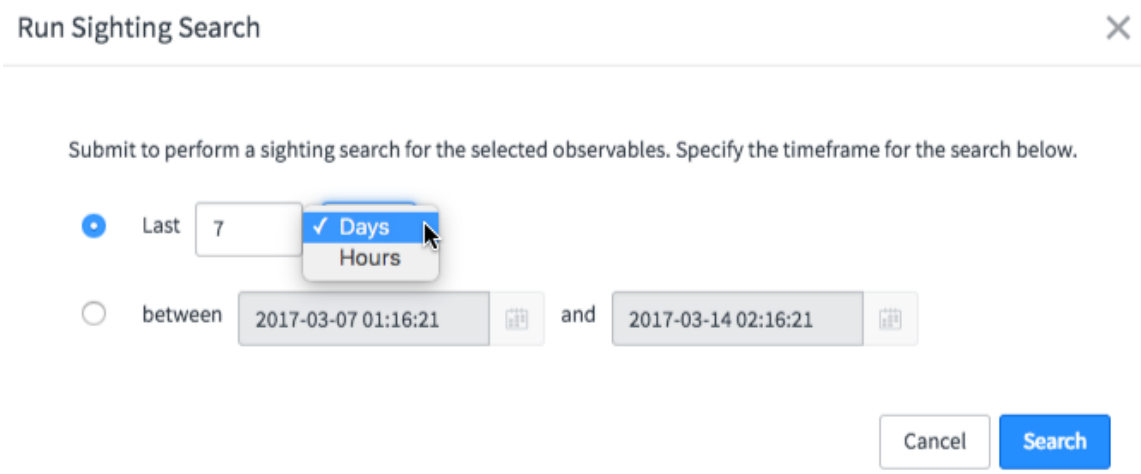
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**.
2. Öffnen Sie den Fall, der erkennbare Elemente enthält, für die Sie eine Sichtungssuche ausführen möchten.
3. Klicken Sie auf den zugehörigen Link **Fallartefakte**.
4. Klicken Sie auf die Registerkarte **Erkennbare Elemente**.
5. Wählen Sie ein oder mehrere erkennbare Elemente aus, für die Sie nach Sichtungen suchen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Sichtungssuche ausführen aus**.
   Das Dialogfeld **„Sichtungssuche ausführen“** wird angezeigt.



7. Geben Sie entweder die Anzahl der Tage oder Stunden ein, nach denen Sie nach Sichtungen der ausgewählten erkennbaren Elemente suchen möchten, oder wählen Sie einen Datumsbereich aus.
8. Klicken Sie auf **Suche**.

Security Incidents in Fällen

In Security Incident Responsekönnen Sie Fälle aus Security Incidents, CIs und betroffenen Anwendern erstellen und diese Artefakte zu vorhandenen Fällen hinzufügen.

Erstellen Sie einen Fall aus Security Incidents

In Security Incident Responsekönnen Sie Fälle aus Security Incidents erstellen. Nachdem die Security Incidents zum Erstellen eines neuen Falls verwendet wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

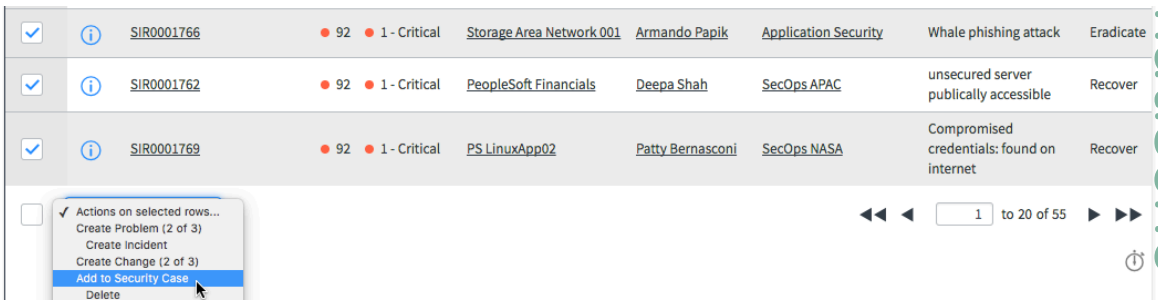
Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

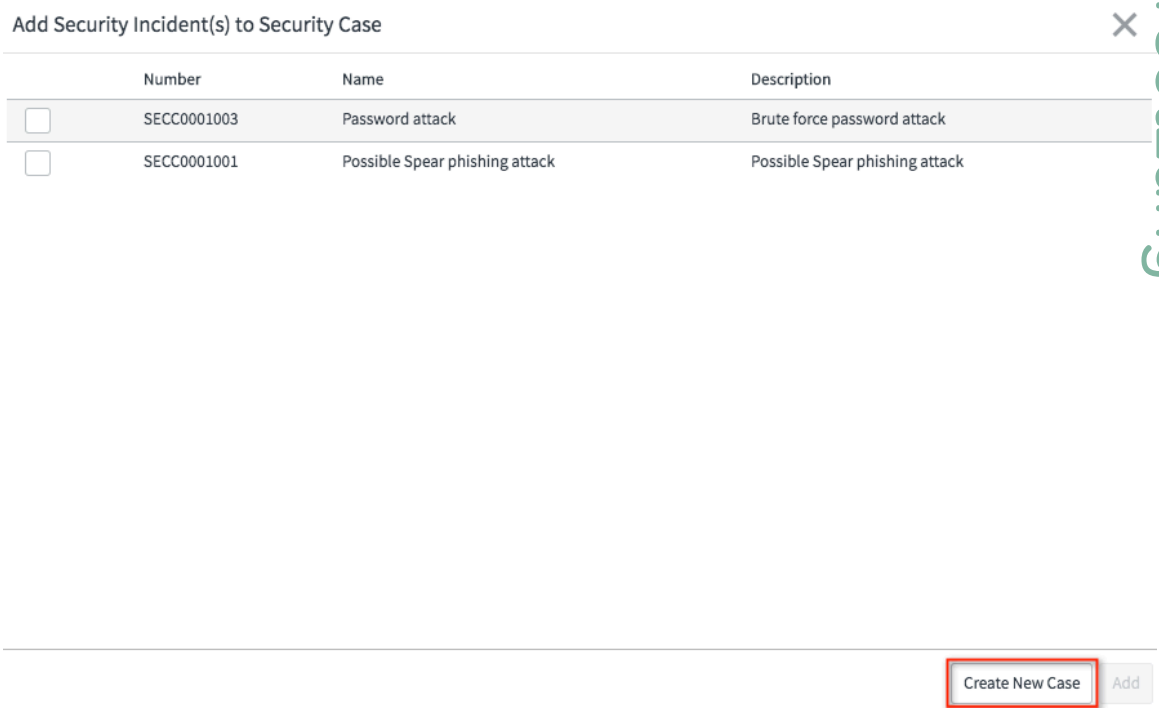
Sie müssen zu den Security Incidents navigieren, die Sie zum Erstellen von Fällen verwenden möchten.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
   Die Liste der Security Incidents wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren Security Incidents erstellen oder Sie können einen bestimmten Security Incident auswählen und über das Formular einen neuen Fall erstellen.
2. Um einen Fall aus der Liste zu erstellen, wählen Sie die Artefakte aus, die Sie einem neuen Fall hinzufügen möchten.
3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.



Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte.

6. Klicken Sie auf **Absenden**.
   Eine Meldung oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie einem vorhandenen Fall Security Incidents hinzu

Sie können Security Incidents zu einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem die Security Incidents zu Fällen hinzugefügt wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Security Incidents navigieren, die Sie vorhandenen Fällen hinzufügen möchten.

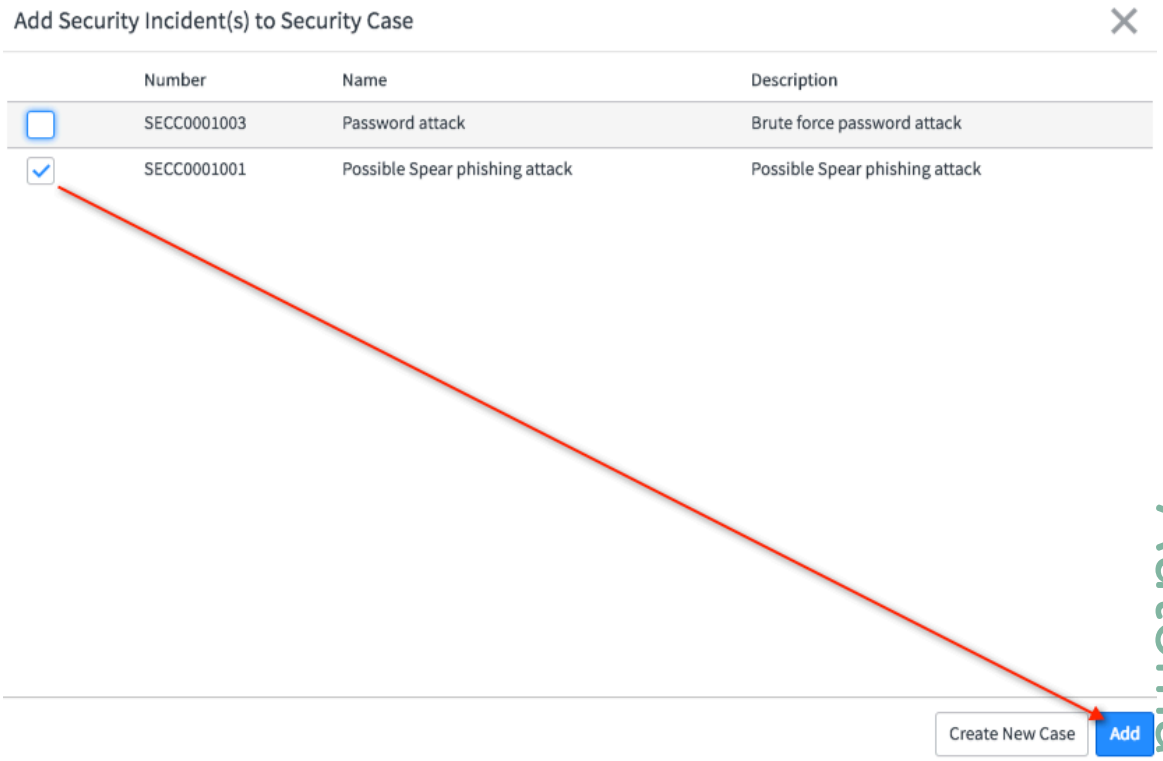
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
   Die Liste der Security Incidents wird geöffnet.
2. Wählen Sie in der Liste mindestens einen Security Incident aus, den Sie vorhandenen Fällen hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere Security Incidents auswählen, werden die ausgewählten Security Incidents jedem der ausgewählten Fälle hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.
   Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Fälle aus, denen Sie die ausgewählten Security Incidents hinzufügen möchten.
5. Klicken Sie auf **Hinzufügen**.
   Eine Meldung zeigt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Konfigurationselemente in Fällen

Sie können einen neuen Fall aus einem oder mehreren Configuration Items (CI) in der Tabelle „Configuration Item“ [cmdb_ci] erstellen. Sie können CIs auch zu vorhandenen Fällen hinzufügen.

Erstellt einen Fall aus CIs

Sie können einen Sicherheitsfall aus Configuration Items in der Tabelle „Configuration Item“ [cmdb_ci] erstellen. Nachdem die CIs zum Erstellen eines neuen Falls verwendet wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Configuration Items navigieren, die Sie zum Erstellen eines Falls verwenden möchten.

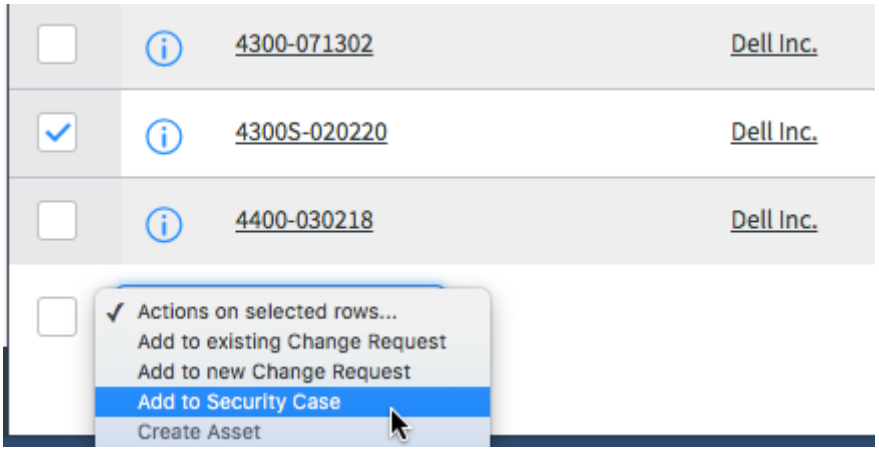
Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Basiselemente** > **Computer** um CIs für Computer anzuzeigen.
   Die Liste für den ausgewählten CI-Typ wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren CIs erstellen oder Sie können ein bestimmtes CI auswählen und einen neuen Fall über das Formular erstellen.

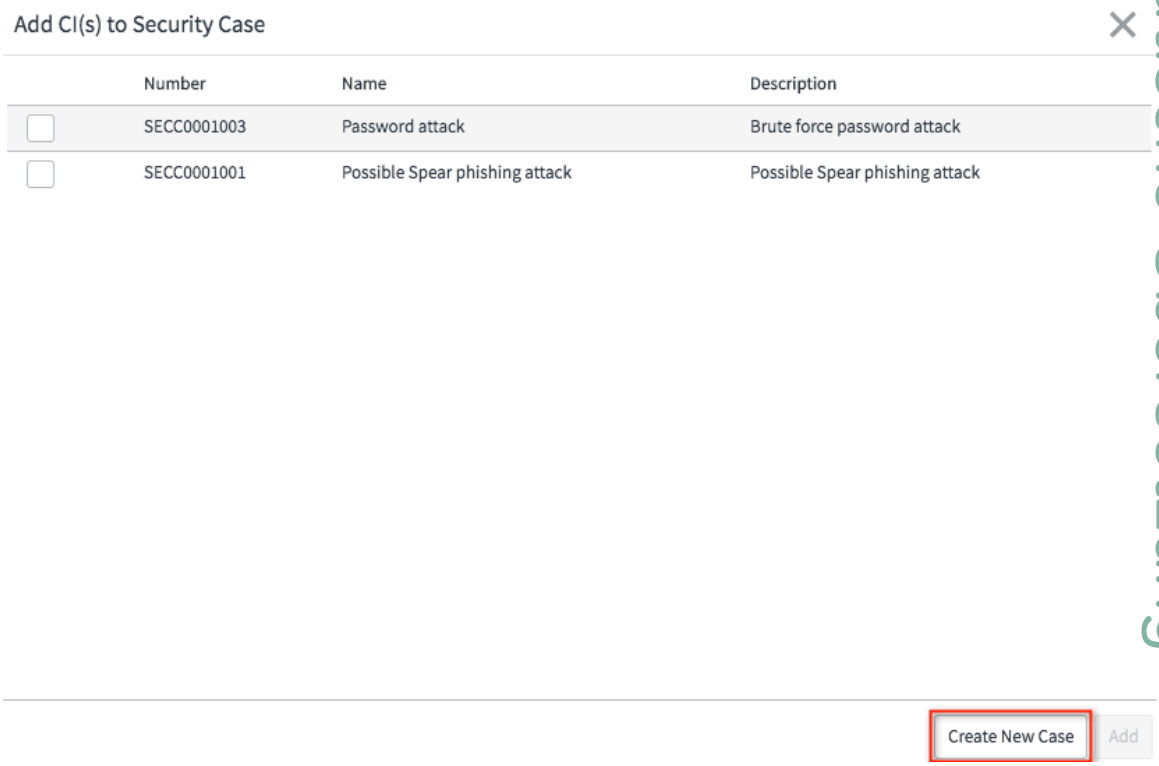
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie in der Liste die CIs aus, die Sie einem neuen Fall hinzufügen möchten.
3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.



Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.



4. Klicken Sie auf **Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
   Eine Meldung oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie CIs zu vorhandenen Fällen hinzu

Sie können Konfigurationselemente zu einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem die CIs zu Fällen hinzugefügt wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den CIs navigieren, die Sie den vorhandenen Fällen hinzufügen möchten.

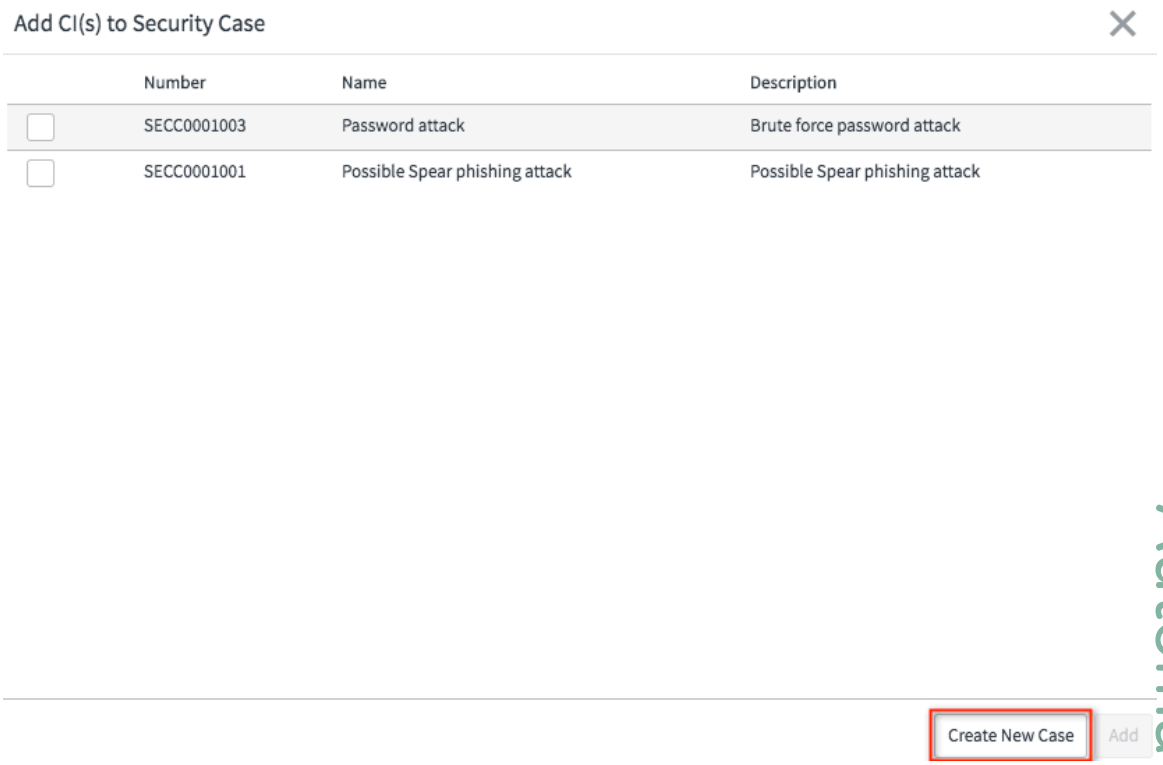
Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Basiselemente** > **Computer** um CIs für Computer anzuzeigen.
   Die Liste der ausgewählten CIs wird geöffnet.
2. Wählen Sie in der Liste mindestens ein CI aus, das Sie vorhandenen Fällen hinzufügen möchten.

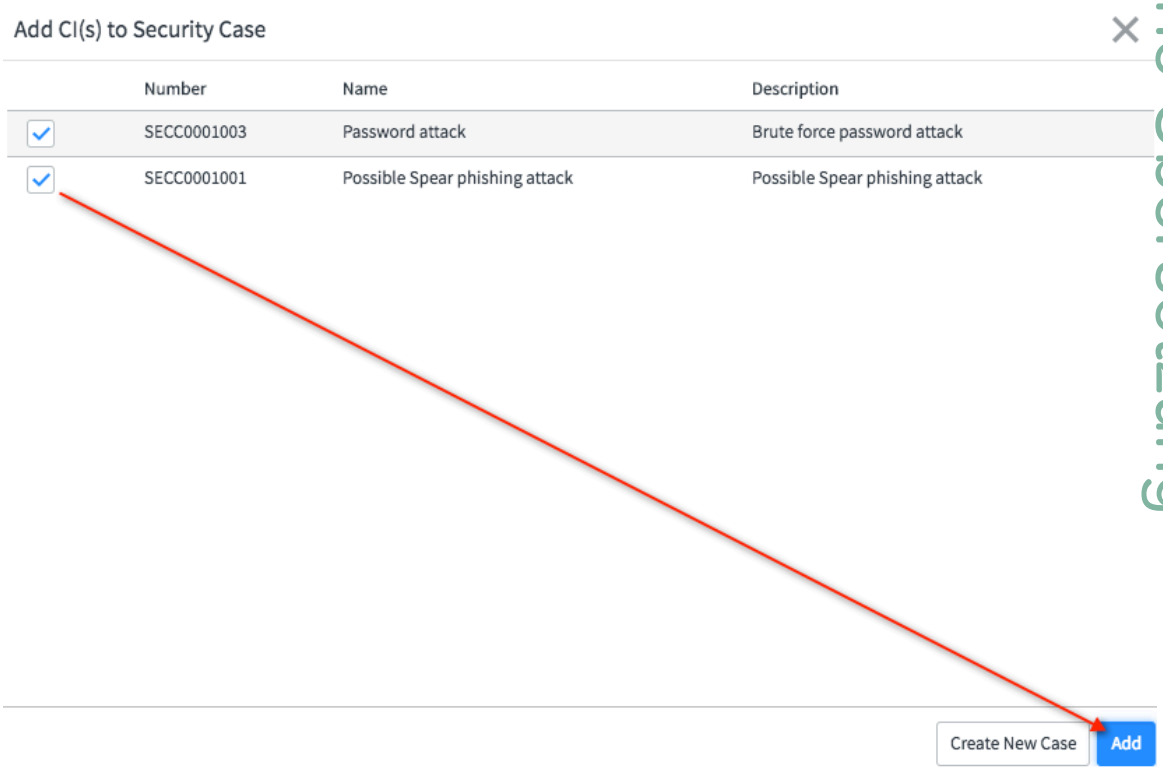
   Hinweis:
   Wenn Sie mehrere CIs auswählen, werden die ausgewählten CIs jedem der ausgewählten Fälle hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.
   Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Fälle aus, denen Sie die ausgewählten CIs hinzufügen möchten.



5. Klicken Sie auf **Hinzufügen**.
Eine Meldung zeigt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betroffene Anwender in Fällen

Sie können einen neuen Fall aus einem oder mehreren betroffenen Benutzern in der Tabelle „Benutzer“ [sys_user] erstellen. Sie können Benutzer auch zu vorhandenen Fällen hinzufügen.

Erstellt einen Fall aus betroffenen Anwendern

In der Tabelle „Benutzer“ [sys_user] können Sie einen Sicherheitsfall aus betroffenen Benutzern erstellen. Nachdem die betroffenen Benutzer zum Erstellen eines neuen Falls verwendet wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

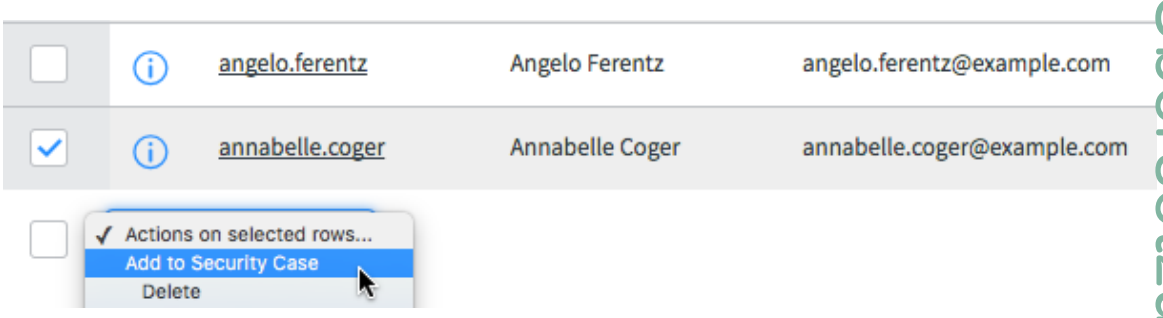
Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Anwendern navigieren, die Sie zum Erstellen eines Falls verwenden möchten.

Prozedur

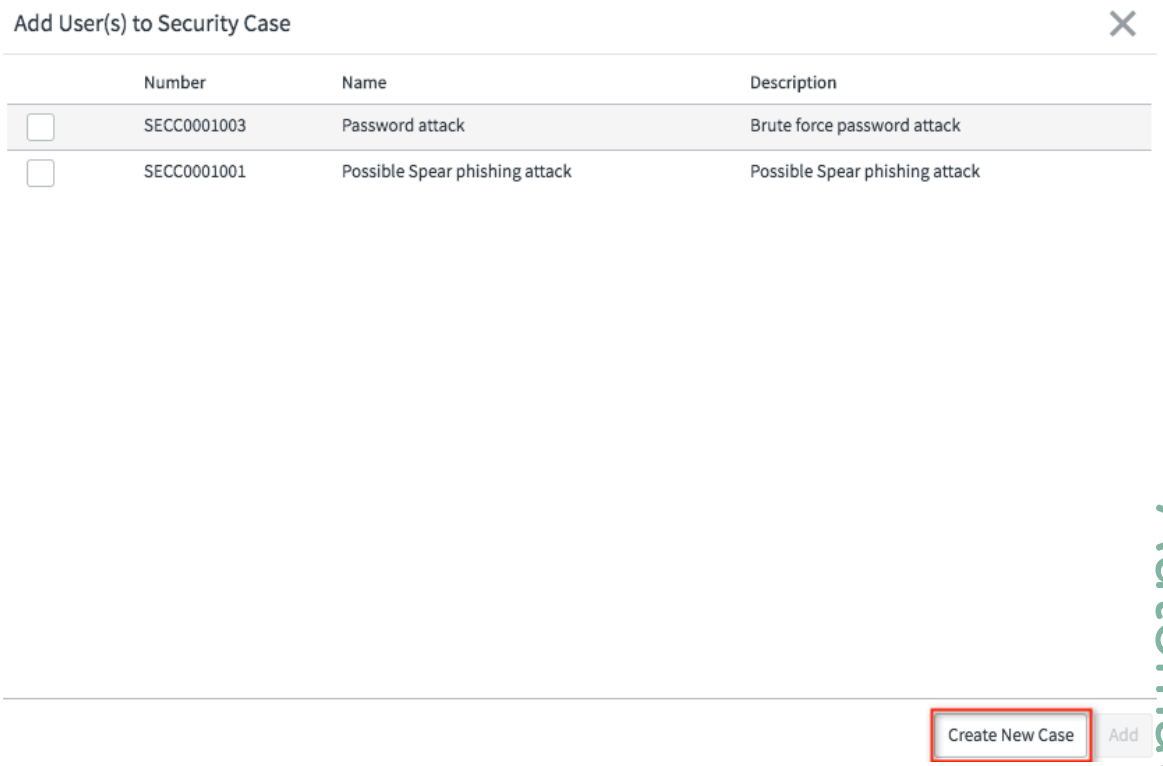
1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**.
   Die Liste für die ausgewählten Benutzer wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren Benutzerdatensätzen erstellen, oder Sie können einen bestimmten Benutzerdatensatz auswählen und über das Formular einen neuen Fall erstellen.
2. Wählen Sie in der Liste die Anwender aus, die Sie einem neuen Fall hinzufügen möchten.
3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.



Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte.

6. Klicken Sie auf **Absenden**.
   Eine Meldung oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie betroffene Anwender zu vorhandenen Fällen hinzu

Sie können betroffene Anwender zu einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem die Benutzerdatensätze zu Fällen hinzugefügt wurden, können Sie die Daten mit Management von Sicherheitsfällen analysieren.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Benutzerdatensätzen navigieren, die Sie vorhandenen Fällen hinzufügen möchten.

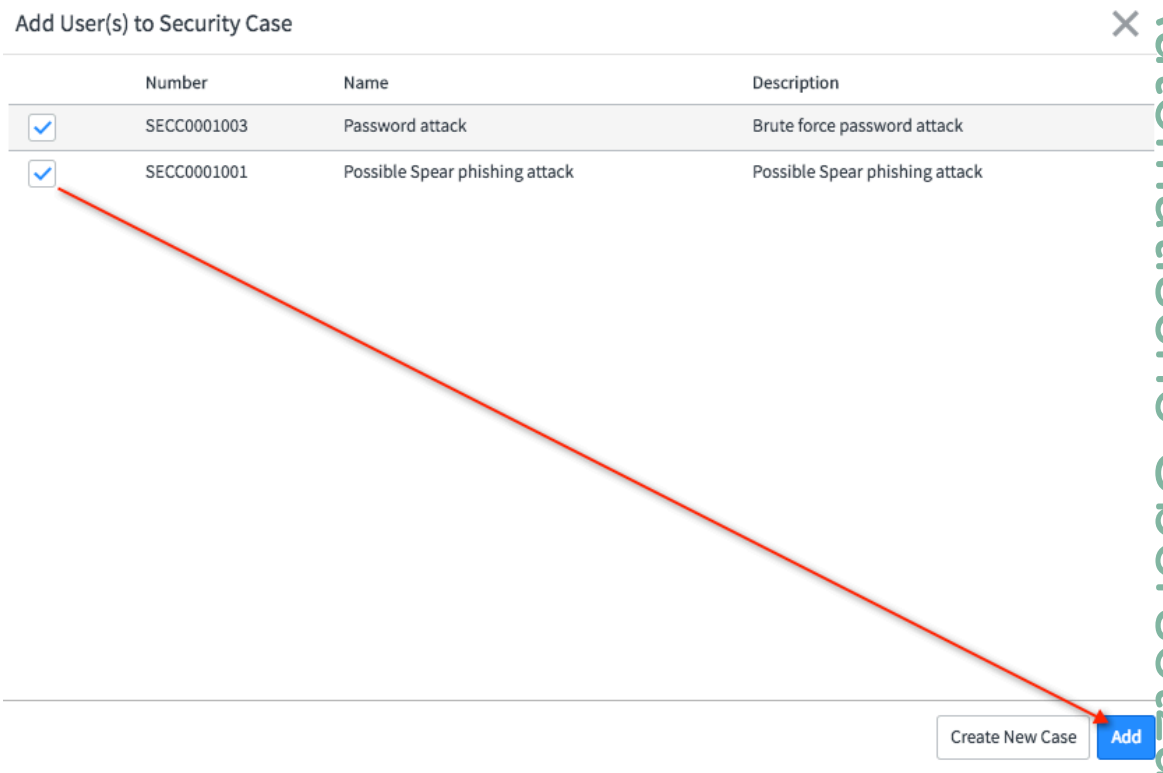
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**.
   Die Liste der Benutzerdatensätze wird geöffnet.
2. Wählen Sie in der Liste mindestens einen Anwender aus, den Sie vorhandenen Fällen hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere Benutzer auswählen, werden die ausgewählten Benutzerdatensätze jedem der ausgewählten Fälle hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elementedie Option Zu Sicherheitsfall hinzufügen aus**.
   Das Dialogfeld **„Dem Sicherheitsfall hinzufügen“** wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.



4. Wählen Sie die Fälle aus, denen Sie die ausgewählten Anwender hinzufügen möchten.
5. Klicken Sie auf **Hinzufügen**.
   Eine Meldung zeigt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Analyse der Sicherheitsartefakte

Nachdem Sie Fälle erstellt haben, entweder mit Management von Sicherheitsfällenoder aus Artefakten wie IoCs, erkennbaren Elementen, Security Incidents usw., können Sie weiterhin Artefakte hinzufügen, um die Analyse der identifizierten Bedrohungen zu unterstützen.

Zugehörige Details für Fallartefakte

Wenn Sie einem Fall Artefakte hinzufügen, können automatisch zusätzliche zugehörige Details für jedes Artefakt hinzugefügt werden. Wenn Sie beispielsweise einen Security Incident hinzufügen, kann er betroffene CIs und Benutzerdatensätze enthalten. Sie können

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

schnell die zugehörigen Details für ein ausgewähltes Artefakt anzeigen, ohne die Liste der Artefakte zu verlassen.

Zeigen Sie zugehörige Details für ein Security Incident-Artefakt an

Wenn Ihr Fall Security Incident-Artefakte enthält, können Sie alle zugehörigen Details anzeigen, die in jedem Security Incident enthalten sind, auf den der Fall verweist.

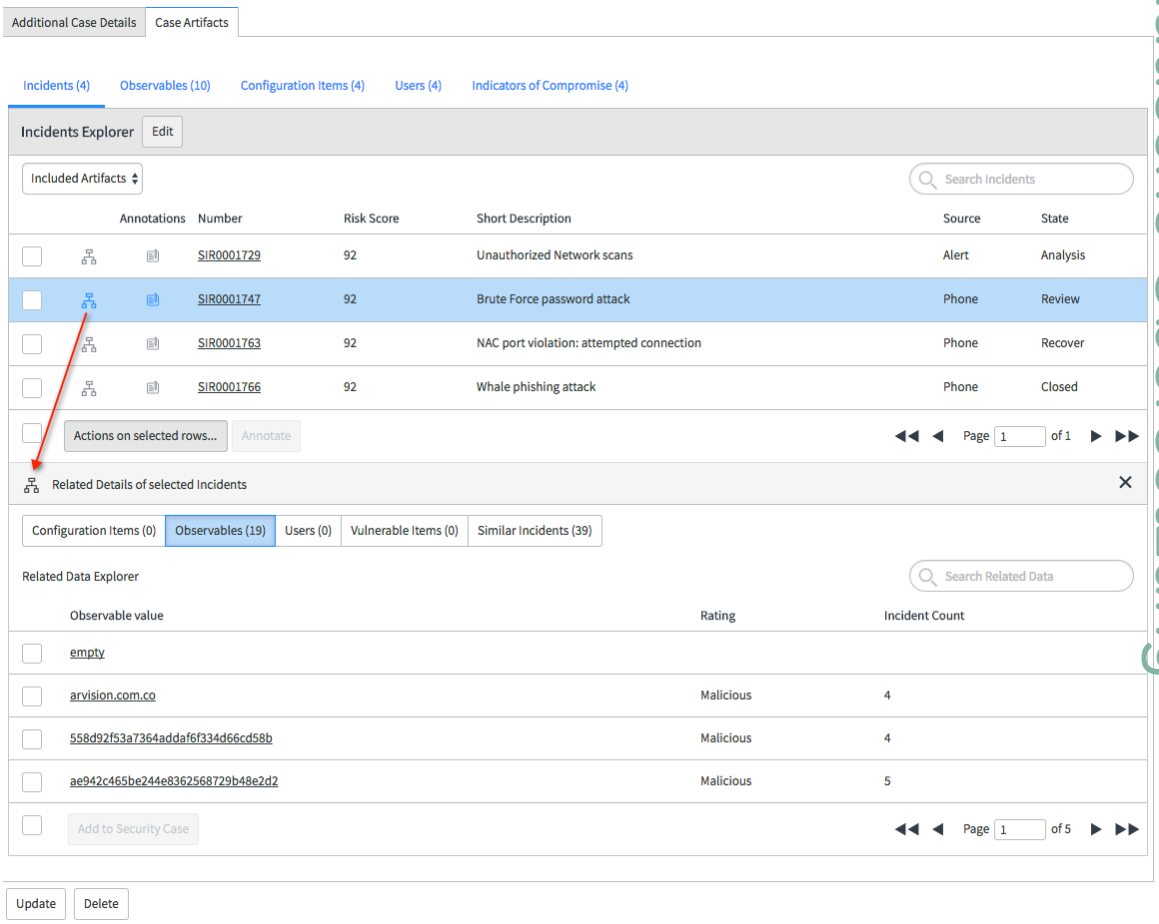
Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der Security Incident-Artefakte enthält.
2. Klicken Sie auf die Registerkarte **Incidents**.
3. Klicken Sie auf das Symbol „Zusätzliche Details“ für den Security Incident, für den Sie zugehörige Details anzeigen möchten.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie zugehörige Details für ein Configuration Item-Artefakt an

Wenn Ihr Fall Configuration Item-Artefakte enthält, können Sie alle zugehörigen Details anzeigen, die in jedem CI enthalten sind, auf das der Fall verweist.

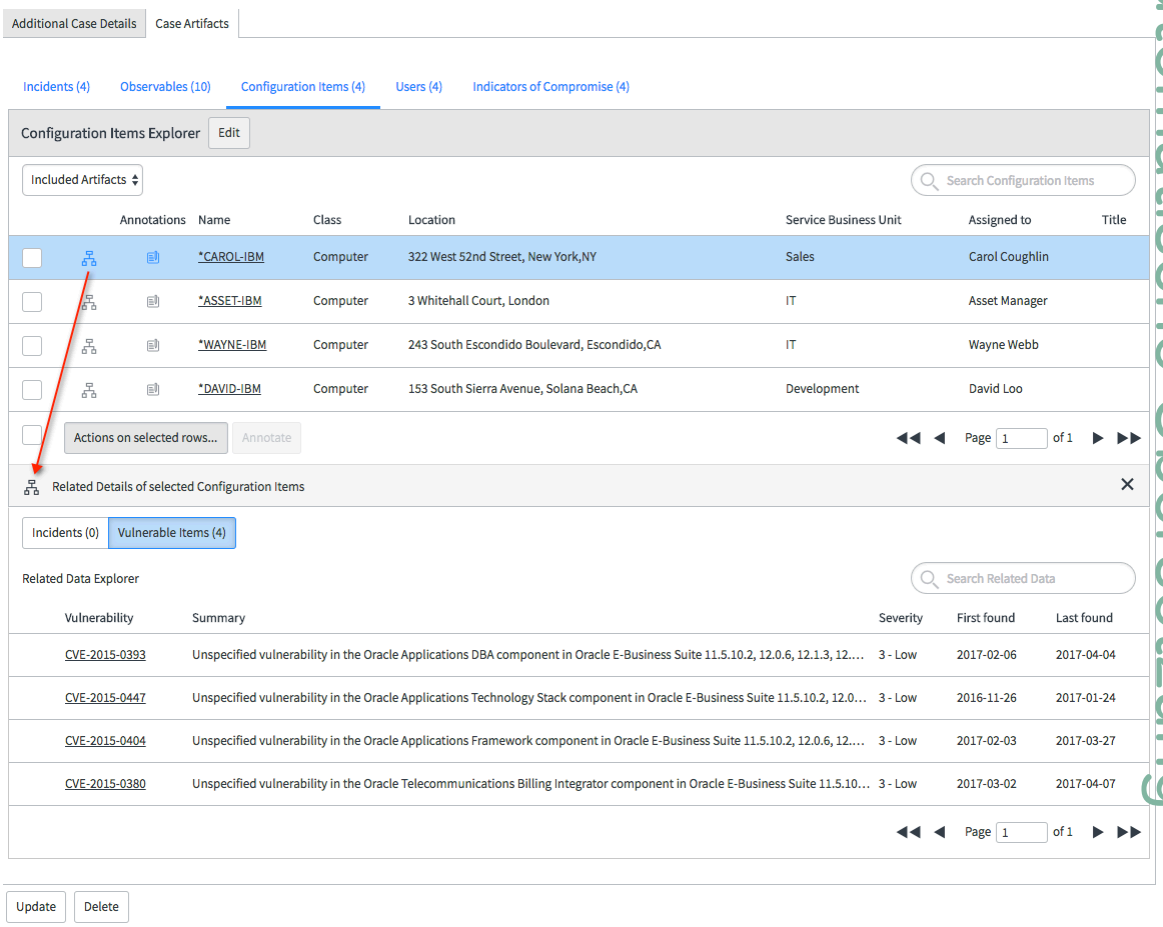
Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der CI-Artefakte enthält.
2. Klicken Sie auf die Registerkarte **Configuration Items**.
3. Klicken Sie für das CI-Artefakt, für das Sie zugehörige Details anzeigen möchten, auf Zusätzliche Details.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

Zeigen Sie zugehörige Details für ein IoC-Artefakt an

Wenn Ihr Fall IoC-Artefakte (Indikatoren für Kompromittierung) enthält, können Sie alle zugehörigen Details anzeigen, die in jedem vom Fall referenzierten IoC enthalten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

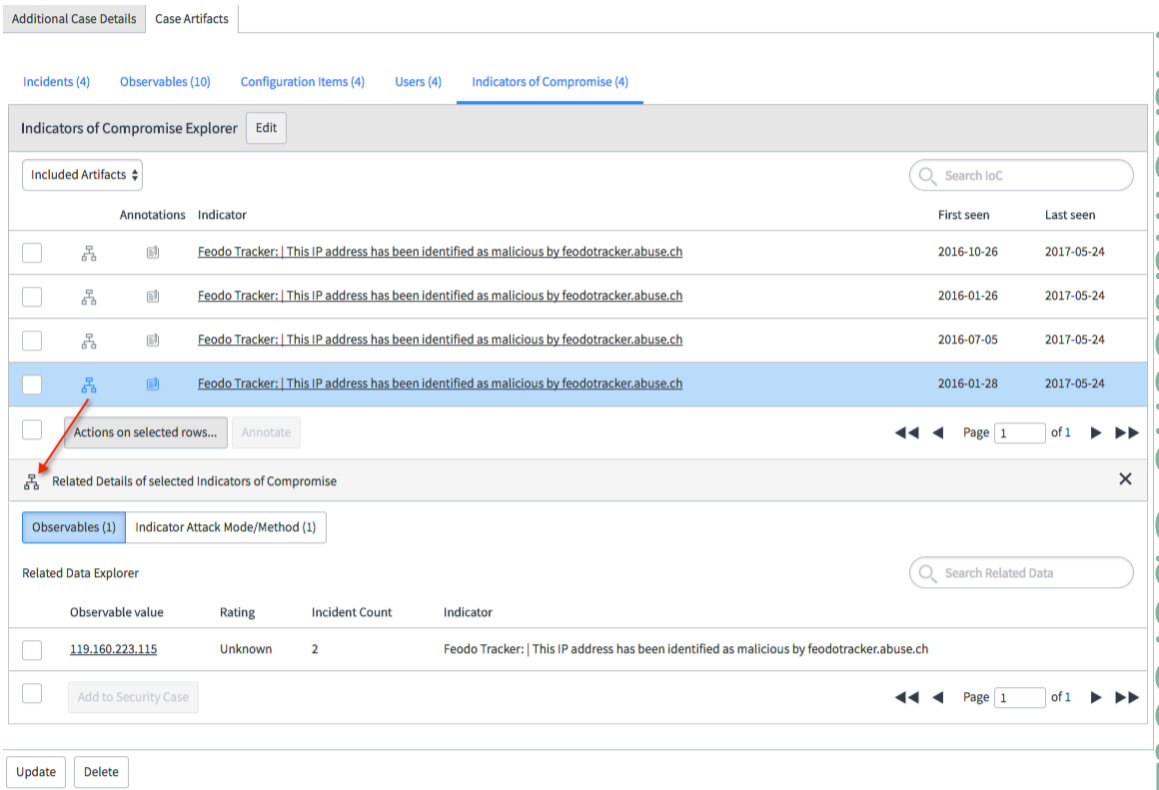
Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der IoC-Artefakte enthält.
2. Klicken Sie auf die Registerkarte **Kompromittierungsindikatoren**.
3. Klicken Sie auf das Symbol Zusätzliche Details für das IoC-Artefakt, für das Sie zugehörige Details anzeigen möchten.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

Zeigen Sie zugehörige Details für ein betroffenes Benutzerartefakt an

Wenn Ihr Fall Artefakte betroffener Benutzer enthält, können Sie alle zugehörigen Details anzeigen, die in jedem betroffenen Benutzer enthalten sind, auf den der Fall verweist.

Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

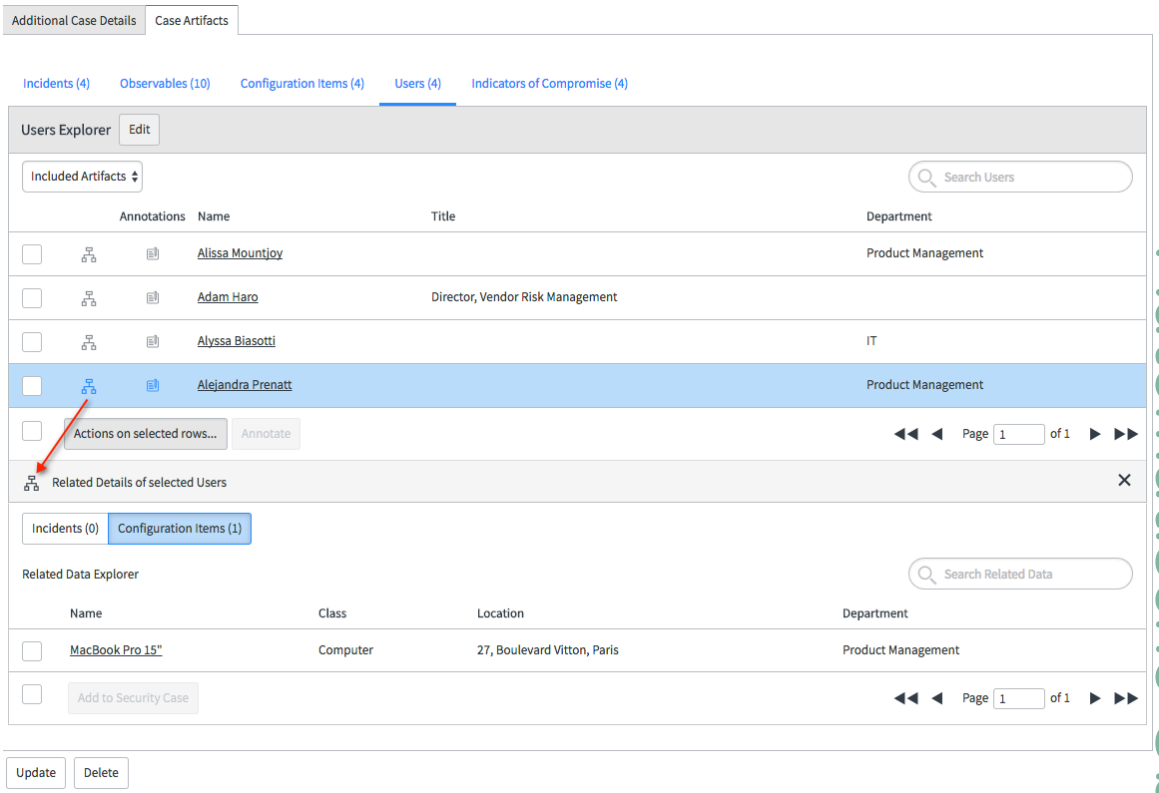
Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie einen Fall, der betroffene Benutzerartefakte enthält.
2. Klicken Sie auf die Registerkarte **Benutzer**.
3. Klicken Sie für das betroffene Anwenderartefakt, für das Sie zugehörige Details anzeigen möchten, auf Zugehörige Details.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

Zeigen Sie zugehörige Details für ein erkennbares Elementartefakt an

Wenn Ihr Fall Artefakte erkennbarer Elemente enthält, können Sie alle zugehörigen Details anzeigen, die in jedem erkennbaren Element enthalten sind, auf das der Fall verweist.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

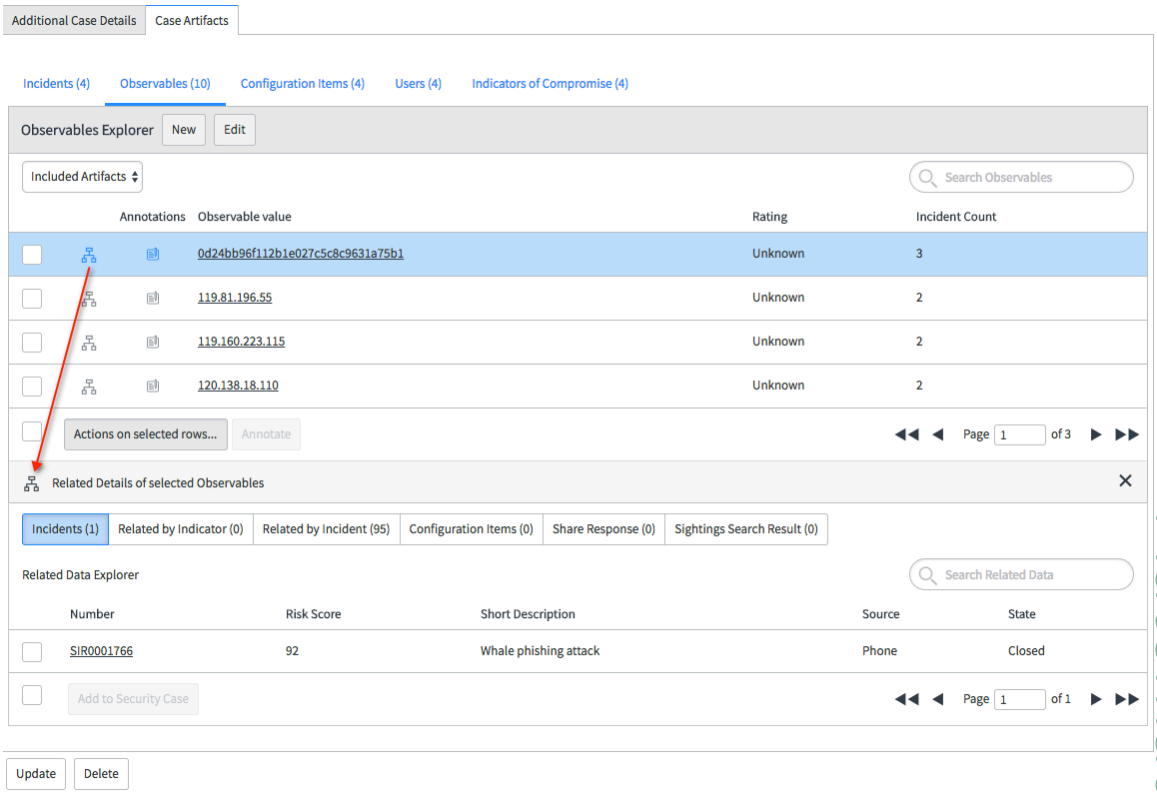
Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der erkennbare Artefakte enthält.
2. Klicken Sie auf die Registerkarte **Erkennbare Elemente**.
3. Klicken Sie für das erkennbare Elementartefakt, für das Sie zugehörige Details anzeigen möchten, auf das Symbol Zusätzliche Details.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

Ausschluss und Einschluss von Sicherheitsartefakten

Die Listen der unterstützenden Artefakte, die einem Fall zugewiesen sind, können manchmal lang werden, und es gibt Fälle, in denen Sie bestimmte Artefakte aus einer Liste entfernen möchten. Anstatt Artefakte dauerhaft zu entfernen, können Sie sie aus der Liste ausschließen und bei Bedarf zu einem späteren Zeitpunkt wieder zur Liste hinzufügen.

Sicherheitsartefakte aus einem Fall ausschließen

Sie können Artefakte aus den Listen der unterstützenden Artefakte entfernen. Sie werden nicht dauerhaft entfernt und können bei Bedarf an den Fall zurückgegeben werden.

Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

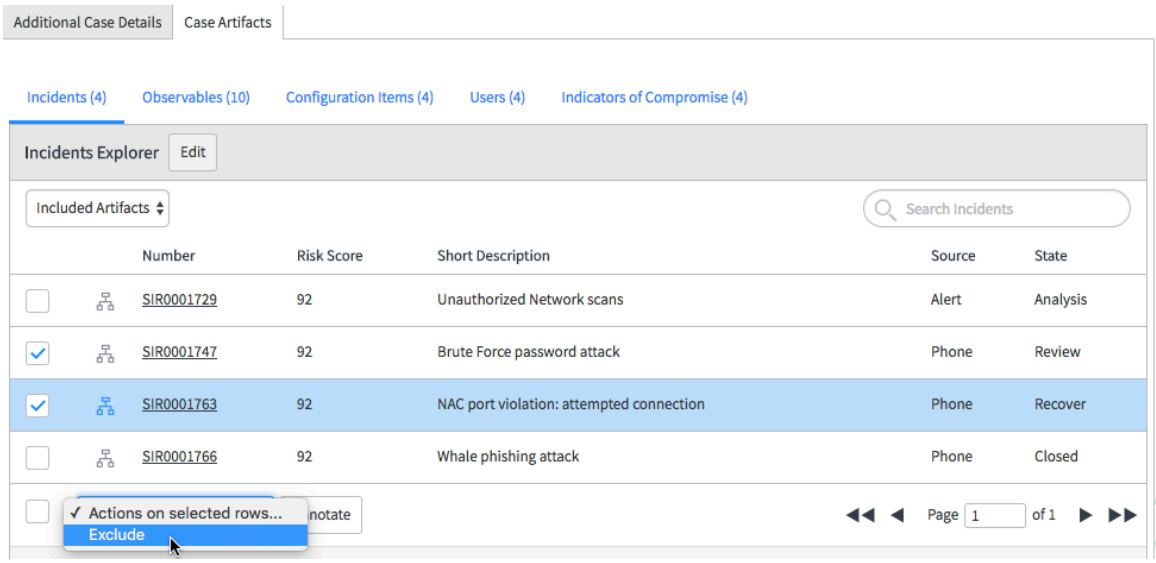
Prozedur

1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie aus einer Liste ausschließen möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.
3. Klicken Sie auf die Registerkarte für die Artefakte, die Sie ausschließen möchten.
   Klicken Sie beispielsweise auf **Incidents**, um Security Incidents aus der Liste auszuschließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie einen oder mehrere Artefaktdatensätze aus, die Sie ausschließen möchten.



5. Wählen Sie **in der Dropdown-Liste Aktionen für ausgewählte Elemente** die Option **Ausschließen aus**.
6. Klicken Sie im Bestätigungsfeld **auf Ausschließen**.
   Die ausgewählten Artefakte werden aus der Liste entfernt.

Geben Sie ausgeschlossene Sicherheitsartefakte an einen Fall zurück

Nachdem Sie Artefakte in einem Fall aus einer Liste ausgeschlossen haben, können Sie sie an den Fall zurückgeben und weiter an ihnen arbeiten.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

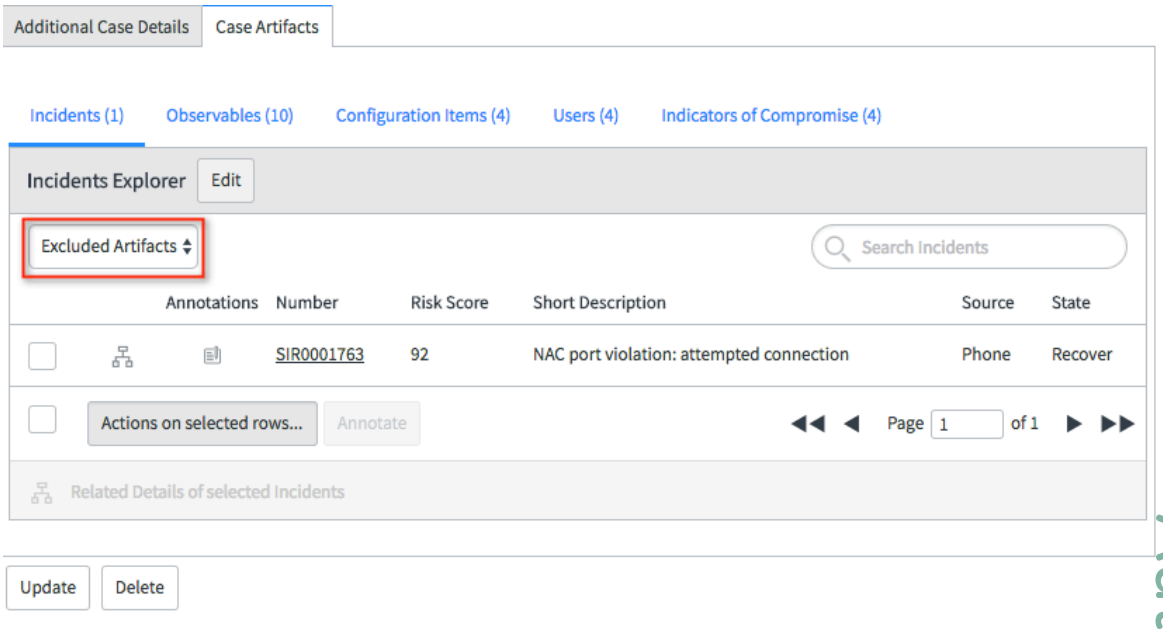
Erforderliche Rolle: sn_ti.case_user_write

Prozedur

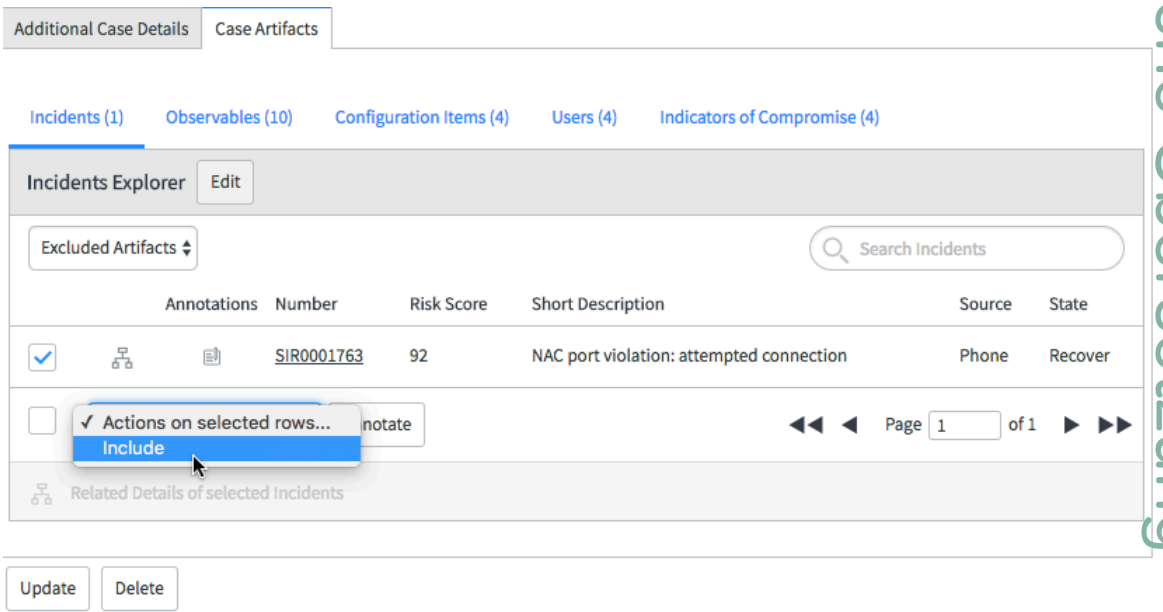
1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie zuvor aus einer Liste ausgeschlossen haben, die Sie wieder in die Liste aufnehmen möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie zur Liste zurückführen möchten.
4. Klicken Sie auf die Dropdown-Liste Artefaktfilter, und wählen Sie **Ausgeschlossene Artefakte**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie einen oder mehrere Artefaktdatensätze aus, die Sie an die Liste Einschließen zurückgeben möchten.
6. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die **Option Einbeziehen aus**.



7. Klicken Sie im Bestätigungsfeld **auf Einbeziehen**.
   Die ausgewählten Artefakte werden aus der Liste der ausgeschlossenen Artefakte entfernt und an die Liste der im Fall enthaltenen Artefakte zurückgegeben.

Versehen Sie Sicherheitsartefakte mit Anmerkungen

Während Sie einen Fall analysieren, können Sie jedem Artefakt Anmerkungen hinzufügen.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Automatische Übersetzung

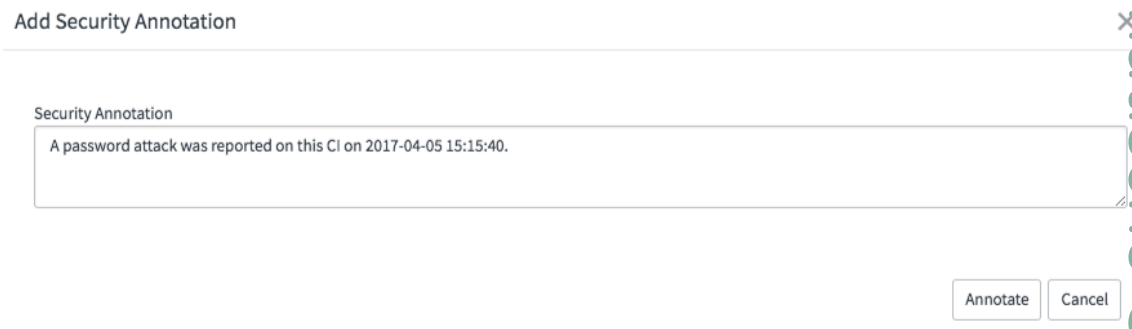
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle:

- sn_ti.case_user_write zum Hinzufügen von Anmerkungen
- sn_ti.case_user_read, um Anmerkungen anzuzeigen

Prozedur

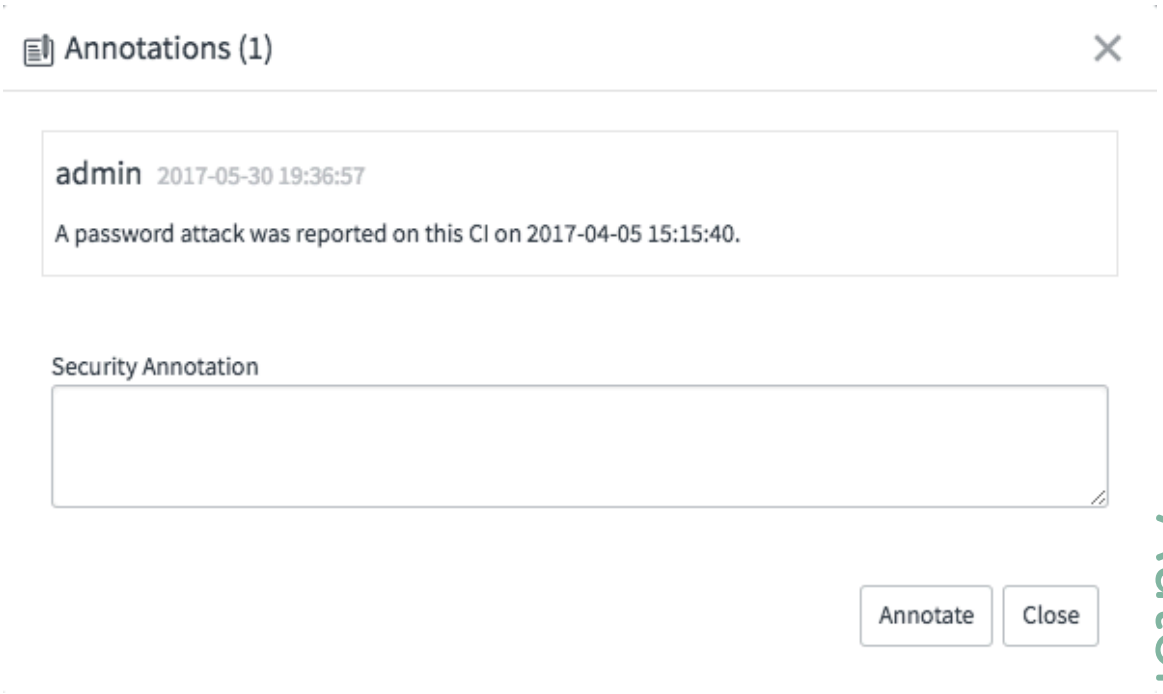
1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie mit Anmerkungen versehen möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie kommentieren möchten. Klicken Sie beispielsweise auf **Kompromittierungsindikatoren**, um Anmerkungen zu IoCs hinzuzufügen.
4. Um einem oder mehreren Artefakten eine Anmerkung hinzuzufügen, gehen Sie wie folgt vor:
   a. Wählen Sie die Artefakte aus, denen Sie eine Anmerkung hinzufügen möchten.
   b. Klicken Sie auf **Kommentieren**.



   c. Geben Sie die Anmerkung ein, und klicken Sie auf **Kommentieren**.
   Die Anmerkung wird den ausgewählten Artefakten hinzugefügt.
5. Um Anmerkungen für ein Artefakt anzuzeigen, klicken Sie auf das Symbol Anmerkungen anzeigen ( ).
   Die vorhandenen Anmerkungen werden im Dialogfeld Anmerkungen angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Sie können auch eine neue Anmerkung für das Artefakt im Feld **Sicherheitsanmerkung** eingeben und **auf Kommentieren**klicken.

Suchen Sie nach Sicherheitsartefakten

Sie können eine Stichwortsuche in jeder Sicherheitsartefaktliste durchführen.

Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Management von Sicherheitsfällenverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der Sicherheitsartefakte enthält.
2. Klicken Sie auf die Registerkarte für die Sicherheitsartefakte, für die Sie eine Stichwortsuche durchführen möchten.
3. Beginnen Sie im Feld **Stichwortsuche** mit der Eingabe des Namens des Artefakts, das Sie suchen möchten.
   Wenn Artefakte gefunden werden, die mit Ihrem Eintrag übereinstimmen, werden sie angezeigt.

Sicherheitsstatus-Überwachung

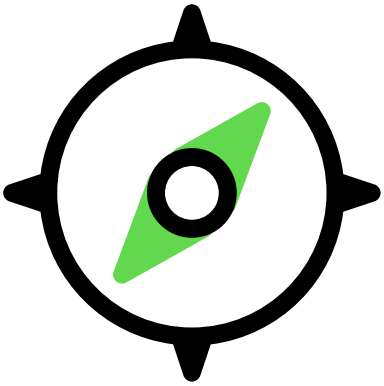
Verschaffen Sie sich einen Überblick über den Bestand an Unternehmens-Assets und über die Abdeckung von Sicherheitstools. Verwenden Sie mit dem Produkt bereitgestellte Richtlinien, oder erstellen Sie eigene, um Assets zu identifizieren, für die wichtige Sicherheitstools fehlen, z. B. Endpunktschutz, Konfigurationsverwaltung und Schwachstellen-Scans. Überwachen Sie Assets auf Sicherheitstool-Konfigurationen, die für Ihre Umgebung spezifisch sind, und automatisieren Sie den Workflow zur Behebung von Sicherheitslücken in der Anwendung Konfigurations-Compliance.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

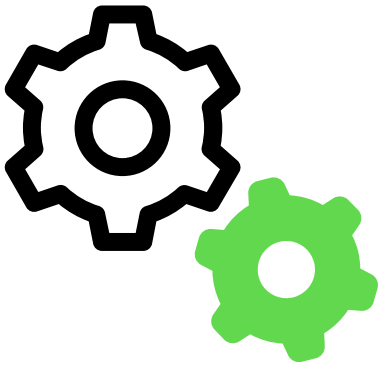
Erste Schritte

Untersuchen



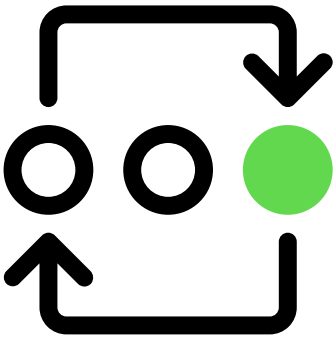
Erfahren Sie mehr über die Konzepte und Funktionen von Security Posture Control

Installieren



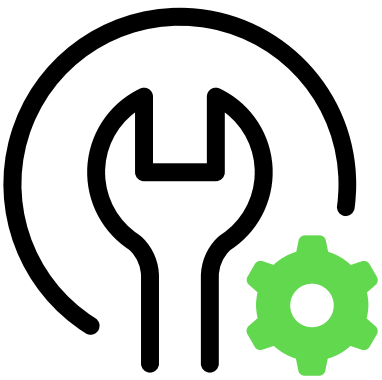
Installieren Sie Anwendungen zur Kontrolle des Sicherheitsstatus

integrieren



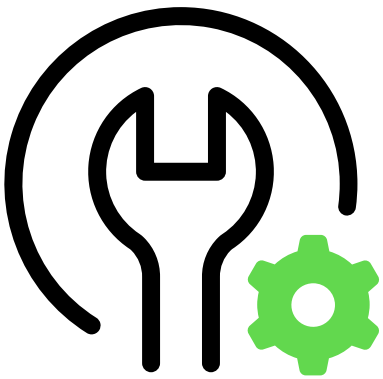
Integrieren Sie Service Graph Connectors in die Sicherheitsstatus-Überwachung

Verwenden



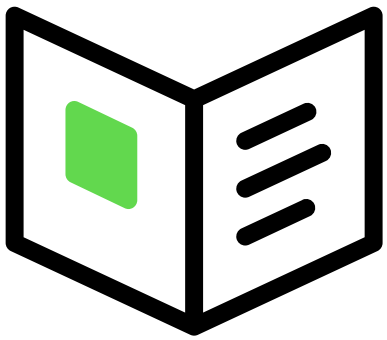
Erfahren Sie, wie Sie mit dem -Arbeitsbereich Ihre Assets durchsuchen und Sicherheitslücken identifizieren können

Überwachung der Steuerungen zur Risikominderung



Erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen gemindert werden

Referenz



Rufen Sie Details zu Szenarien ab, mit denen Sie bestimmte Arten von Lücken bei der Toolabdeckung identifizieren können. Sehen Sie sich Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien an, und sehen Sie sich eine Liste der unterstützten Hardware- und Software-Service Graph Connectors an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Sicherheitsstatus-Überwachung erkunden

Sicherheitsstatus-Überwachung ermöglicht es Cybersicherheitsteams, Einblick in den gesamten Bestand von Unternehmens-Assets zu erhalten und ihre allgemeine Sicherheitslage zu bestimmen.

Sicherheitsanalysten erhalten Einblicke in die Art und Weise, wie Sicherheitstools bereitgestellt und ihre Assets abgedeckt werden, basierend auf dem Asset-Bestand und importierten Daten aus Service Graph Connectors und ServiceNow-Produkten wie Hardware Asset Management (HAM) und ITOM Discovery.

Sicherheitsanalysten können auch anwenderdefinierte Richtlinien erstellen und Einblicke konfigurieren, um die Compliance von Assets mit internen Sicherheitsstandards zu überwachen. Schwachstellenmanager können Einblicke von Sicherheitsstatus-Überwachung (SSÜ) verwenden, um die Behebung von Schwachstellen bei Assets mit hohem Risiko zu priorisieren.

Das SPC-Produkt basiert auf Cloud Security Posture Management (CSPM) und Cyber Asset Hygiene Management (CAHM). Sicherheitsstatus-Überwachung besteht aus zwei -Anwendungen, die über ein separates Abonnement von ServiceNow® Storeverfügbar sind.

Freigabeversion	Release-Hinweise
Sicherheitsstatus-Überwachung Core: v 6.0, v5.0, v4.0, v3.0, v2.0	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Releaseschemaänderungen Security Posture Control release notes
Sicherheitsstatus-Management für Assets: v5.3, v5.0, v4.0, v3.0, v2.0	
Überwachung der Ausgleichssteuerungen v3.0, v2.0	

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Mit dem Produkt SSÜ können Info-Sec-Teams die folgenden Aufgaben ausführen:

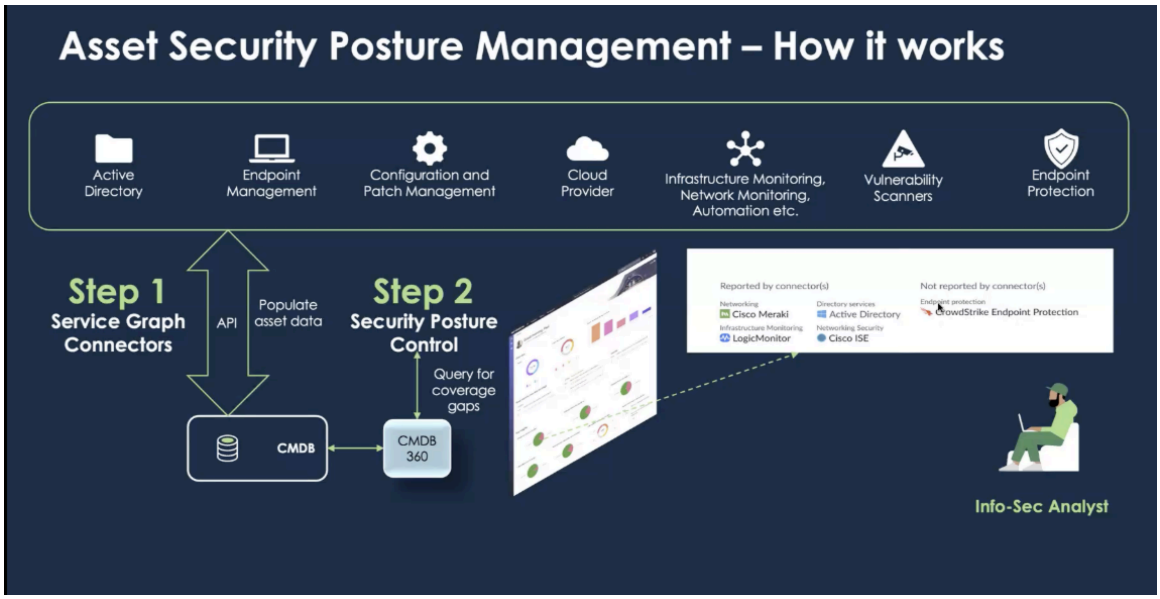
- Zeigen Sie Einblicke zur Sicherheitslage für Ihre lokalen und Cloud-Assets an. SSÜ hilft Ihren Info-Sec-Teams, Assets ohne Endpunktschutz, nicht verwaltete Assets, Assets, die dem Internet ausgesetzt sind, und Kombinationen mit hohem Risiko und Schwachstellen zu identifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überwachen Sie Ihre Assets auf Compliance mit internen Standards für die Konfiguration von Sicherheitstools. Stellen Sie beispielsweise sicher, dass die aktuelle Version eines Endpunktschutzprodukts verwendet wird.
- Automatisieren Sie Ihren Nachbesserungs-Workflow für die gefundenen Sicherheitsstatuslücken mit der Anwendung ServiceNow Configuration Compliance.
- Erstellen Sie anwenderdefinierte Richtlinien und Einblicke basierend auf Asset-Metadaten, Daten zur Abdeckung von Sicherheitstools und Schwachstellendaten.
- Verschaffen Sie sich mit der Überwachung der MinderungssteuerungenEinblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen gemindert werden, je nachdem, wie verschiedene Sicherheitstools konfiguriert sind.

Funktionsweise von Sicherheitsstatus-Management für Assets



Asset Security Posture Management (ASPM) identifiziert Lücken bei der Abdeckung von Sicherheitstools in Assets durch die Verwendung von API-Integrationen mit verschiedenen Tools von Drittanbietern (Service Graph Connectors) zusammen mit ServiceNow-Produkten.

ASPM basiert auf Daten, die in Ihrer CMDB zu Ihren Assets hinterlegt sind. Die Asset-Daten werden von verschiedenen Kategorien von Überwachungstools importiert und verglichen, um potenzielle Sicherheitslücken zu identifizieren.

Angenommen, in der CMDB sind Asset-Daten ausgefüllt, die von Tools gemeldet werden, die Infrastrukturüberwachungs- und Netzwerktools abdecken. Diese Daten für dieselben Assets werden jedoch nicht von Endpunktschutz-Tools ausgefüllt oder gemeldet. Wenn Sie die von diesen verschiedenen Tools gemeldeten Asset-Daten vergleichen, können Sie sehen, dass für bestimmte Assets ein Endpunktschutz-Agent fehlt.

Sicherheitsstatus-Management für Assets identifiziert Abdeckungslücken bei Sicherheitstools in Assets mithilfe von API-Integrationen mit verschiedenen Tools (Service Graph Connectors) und ServiceNow-Produkten. Die Kategorien sind unter anderem:

- Digitale Mitarbeiter-Experience
- Discovery
- Endpunktverwaltung
- IT Asset Management

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Infrastrukturüberwachung
- Netzwerk
- Netzwerksicherheit
- Netzwerkleistungsüberwachung
- Konfigurations- und Patchverwaltung
- Endpunktschutz
- Cloud-Provider
- Application Performance Monitoring
- Directory Services
- Schwachstellenbewertung

Der Workflow Sicherheitsstatus-Überwachung .

Das Identifizieren von Lücken in Sicherheitstools umfasst die folgenden Schritte:

1. Richten Sie API-Verbindungen mit einem der Tools ein, die Sie in verschiedenen Kategorien verwenden. Sie können Service Graph Connectors für Produkte verwenden, die im ServiceNow Store für die erforderlichen API-Verbindungen verfügbar sind. Weitere Informationen zu den unterstützten Service Graph Connectors finden Sie unter Service Graph Connectors . Unterstützte Service Graph Connectors sind im ServiceNow® Store mit separaten Abonnements verfügbar.
2. Aktivieren Sie die mit der Anwendung Sicherheitsstatus-Überwachung gelieferten Richtlinien. Das Produkt Sicherheitsstatus-Überwachung findet Sicherheitstool-Lücken, indem es die folgenden Aufgaben ausführt:
   a. Identifiziert die Liste aller eindeutigen Assets, die von verschiedenen Service Graph Connectors in der CMDB ausgefüllt werden.
   b. Identifiziert Assets, die nicht von bestimmten Kategorien aus diesem Asset-Pool gemeldet werden, z. B. Endpunktschutz. Assets werden basierend auf der aktiven Richtlinie identifiziert, die ausgewertet wird.
   c. Assets, die von bestimmten Kategorien als nicht gemeldet identifiziert wurden, werden in der Anwendung Konfigurations-Compliance als „Ergebnisse“ oder „Testergebnisse“ gemeldet.
3. Weisen Sie „Ergebnisse“ mit der Anwendung „Konfigurations-Compliance“ automatisch verschiedenen Teams zur Korrektur zu.

Kombinationen mit hohem Risiko

Mit Sicherheitsstatus-Management für Assetskönnen Sie auch Assets identifizieren, die Kombinationen mit hohem Risiko aufweisen. Ein Beispiel für eine Kombination mit hohem Risiko könnte Assets zeigen, für die Sicherheitstools fehlen, die kritische Schwachstellen aufweisen und die im Internet verfügbar gemacht werden.

Einige der mit der Anwendung Sicherheitsstatus-Überwachung gelieferten Richtlinien suchen nach diesen risikoreichen Kombinationen aus kritischen Schwachstellen und Abdeckungslücken für Sicherheitstools. Damit diese kombinierten Richtlinien funktionieren, müssen jedoch die Anwendung Vulnerability Response und mindestens ein Integrationsprodukt für Schwachstellenscanner wie z. B. Qualys, Rapid7oder die Anwendung Tenable Vulnerability

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration installiert sein. Diese Anwendungen sind mit separaten Abonnements im ServiceNow Store verfügbar.

Überwachung von Risikominderungsmaßnahmen

Im Arbeitsbereich Sicherheitsstatus-Überwachung (SSÜ) erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Steuerungen zur Risikominderung gemindert werden, je nach Konfiguration verschiedener Sicherheitstools. Weitere Informationen finden Sie unter Überwachung der Ausgleichssteuerungen.

Installieren Sie die unterstützten Anwendungen für die Sicherheitsstatus-Überwachung

Die für diese Integration erforderlichen Anwendungen sind unter ServiceNow Storeverfügbar. Einige Anwendungen haben Abhängigkeiten, die Sie separat herunterladen und installieren müssen.

Vorbereitungen

Erforderliche Rolle: admin zum Herunterladen, Installieren und Aktivieren aller -Anwendungen.

Prozedur

1. Laden Sie die erforderlichen Anwendungen aus ServiceNow Store in Ihre Instanz von ServiceNow herunter.

   Die Anwendung Sicherheitsstatus-Überwachung (SSÜ Core) stellt das Core-Framework bereit und ist für Sicherheitsstatus-Management für Assets (ASPM) erforderlich. Mit der Anwendung Konfigurations-Compliance und ihren Abhängigkeiten können Sie Korrekturaufgaben für die Sicherheitskontrolllücken erstellen, die Sie mit Sicherheitsstatus-Management für Assetsfinden.

Anwendungen für das Sicherheitsstatus-Management für Assets

Anwendung	App-ID
Sicherheitsstatus-Management für Assets	(Plugin-ID: sn_sec_caasm)
ITOM Discovery-Lizenz	(Plugin-ID: com.snc.itom.discovery.license)
Sicherheitsstatus-Überwachung Core	(Plugin-ID: sn_sec_spc_core)
Überwachung von Risikominderungsmaßnahmen	(Plugin-ID: sn_sec_mit_ctr)
Konfigurations-Compliance (enthält die untergeordnete App „secops_shared_components“)	(Plugin-ID: sn_vulc)
Lizenzierung und Nutzung von Vulnerability Response	(Plugin-ID: sn_vul_licensing)

Cloud Security Posture Management-Anwendungen

Anwendung	App-ID
Discovery-Plugin	(Plugin-ID: com.snc.discovery)
Governance für Cloud-Konfigurationen	(Plugin-ID: sn_itom_ccg)
CCG-Inhaltspaket	(Plugin-ID: sn_itom_ccg_cp)
CMDB CI Class Models	(Plugin-ID: sn_cmdb_ci_class)
Cloud-Aktionsbibliothek	(Plugin-ID: com.sn.itom.cal)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie in den folgenden Themen:

- Laden Sie eine Anwendung zum ersten Mal von ServiceNow Store herunter.
- Aktivieren Sie eine ServiceNow Store -Anwendung.

2. Nachdem Sie die Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
3. Suchen Sie die heruntergeladenen Anwendungen, und wählen Sie **Installieren**, um sie zusammen mit ihren Abhängigkeiten zu aktivieren.
   Alle abhängigen Anwendungen, die zusammen mit einer Anwendung automatisch installiert werden, werden im Dialogfeld „Anwendungsinstallation“ angezeigt. Wenn Sie jedoch während der Installation aufgefordert werden, Abhängigkeits-Plugins zu installieren, befolgen Sie die bereitgestellten Eingabeaufforderungen. Stellen Sie sicher, dass alle in der vorherigen Tabelle aufgeführten Anwendungen und Abhängigkeiten installiert und aktiviert sind.

   Ein Dialogfeld wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

   Weitere Informationen zum Herunterladen und Installieren von Anwendungen von ServiceNow Store:

   - Um ServiceNow -Produkte zu aktivieren, führen Sie die Schritte in Opt in to the ServiceNow Store products aus.
   - Um eine Anwendung zu installieren, die Sie bei ServiceNow Storeerworben haben, führen Sie die Schritte in Install a ServiceNow Store application aus.
   - Wenn Sie Ihre Berechtigung für die -Anwendungen in anderen Now Platform -Instanzen verwalten möchten, führen Sie alternativ die Schritte in Manage entitlements from your ServiceNow instance aus.
4. Nachdem Sie die Anwendungen installiert und aktiviert haben, weisen Sie den folgenden Sicherheitskontrollgruppen Benutzer zu:

   Diese Gruppen erben alle Rollen, die zum Lesen und Bearbeiten von SPC-Datensätzen erforderlich sind.

   SPC-Administratorgruppe

   Benutzer in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, einschließlich Lizenzierungsinformationen. Granulare Rollen für diese Gruppe sind: [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin und sn_sec_spc_core.configure].

   SPC-Analystengruppe

   Anwender in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Granulare Rollen für diese Gruppe umfassen [pa_power_user und sn_sec_spc_core.analyst].

   Schreibgeschützte SPC-Analystengruppe

   Anwender in dieser Gruppe haben vollständigen Lesezugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Granulare Rollen für diese Gruppe sind [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read und cmdb_ms_user].

   Unterstützende Anwendungsrollen

   Die folgenden Rollen sind für die in der vorherigen Tabelle aufgeführten Anwendungen erforderlich, die SSÜ und Sicherheitsstatus-Management für Assetsunterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurations-Compliance Administrator [sn_vulc.admin]: Konfiguriert die Anwendung Konfigurations-Compliance, hat Einblick in alle Datensätze und kann Eigenschaften ändern. Weist Rollen in der Anwendung Konfigurations-Compliance zu.
- Vulnerability Response Administrator [sn_vulc.admin]: Konfiguriert die Anwendung Vulnerability Response und die Schwachstellenrisiko-Rechner.
- MID-Server [mid_server]: Konfiguriert einen MID-Server.

5. **Wahlweise:** Legen Sie die Systemeigenschaft **„ignoreCIClass** “ [sn_sec_cmn.ignoreCIClass] fest, um einige CI-Klassen (Configuration Item, Konfigurationselement) bei der Ausführung von CI-Suchregeln zu ignorieren.

   (Optional) Als SPC-Administrator und SPC-Analyst müssen Sie möglicherweise bestimmte Hardware- oder virtuellen Klassen ignorieren, damit Sie keine Informationen zu Assets erfassen, die Sie nicht steuern möchten. Siehe Erstellt eine Vulnerability Response-CI-Suchregel und CI-Klassen ignorieren, um weitere Informationen zu erhalten.

6. Ändern Sie den Abgleich, und berechnen Sie CMDB-Datenquellen neu, um die Quelle der Wahrheit für Attributwerte festzulegen.

   Das CMDB 360-Dashboard bietet Zusammenfassungen und Analysen von CMDB 360-Daten. CMDB 360 sammelt Daten zu allen Discovery-Quellen, die Attributwerte für CIs melden. Verwenden Sie die CMDB 360-Ansicht im CMDB-Arbeitsbereich (Configuration Management Database), um Aktivitäten nachzuverfolgen und potenzielle Probleme mit Discovery-Quellen zu identifizieren. Weitere Informationen finden Sie unter CMDB 360 view in CMDB Workspace .

Service Graph Connectors für Sicherheitsstatus-Überwachung

Sicherheitsstatus-Überwachung verwendet API-Integrationen oder Service Graph Connectors als wichtige Quelle für die Asset-Daten, die zur Identifizierung von Sicherheitslücken verwendet werden.

Sicherheitsstatus-Überwachung unterstützt derzeit Service Graph Connectors (SGC), die Ihnen eine Vielzahl von Daten zu Ihren Assets bereitstellen können. Diese Integrationsanwendungen sind unter ServiceNow Storeverfügbar.

Wählen Sie die Connectors aus, die Sie verwenden möchten, laden Sie die Anwendungen herunter, und aktivieren Sie sie. Die Liste der unterstützten Connectors im Store wird erweitert, wenn Sicherheitsstatus-Überwachung mehr Connectors unterstützt.

Um die Funktionen von Sicherheitsstatus-Überwachung vollständig zu nutzen, sollten Sie die folgenden Service Graph Connector-Produkte herunterladen und aktivieren, um die unten aufgeführten Kategorien zu unterstützen.

Von Sicherheitsstatus-Überwachung unterstützte Service Graph Connectors umfassen derzeit die folgenden Kategorien:

- Digitale Mitarbeiter-Experience
- Discovery
- Endpunktverwaltung: Microsoft Intune oder Jamf Device and Endpoint Management.
- IT Asset Management
- Infrastrukturüberwachung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Netzwerk
- Netzwerksicherheit
- Netzwerkleistungsüberwachung
- Konfigurations- und Patchverwaltung: MicrosoftMicrosoft Azure Event Hubs SCCM oder IBM Bigfix.
- Endpunktschutz: CrowdStrike oder SentinelOne.
- Cloud-Anbieter: Amazon AWS Cloud, Microsoft Azure, GCP.

Hinweis:
Wenn Cloud-Discovery aktiviert ist, sind diese Service Graph Connector-Produkte nicht erforderlich.

- Application Performance Monitoring
- Verzeichnisservices (Active Directory) Microsoft Active Directory
- Schwachstellenbewertung: Qualys, Rapid7oder Tenable.

Nach der Installation können Sie die Connectors und ihre Kategorien in der Connector-Tabelle [sn_sec_spc_core_connector] in Ihrer Instanz anzeigen.

In der Tabelle [sn_sec_spc_core_asset_type_connector] können Sie Asset-Typen und ihre Zuordnung zu CI-Klassen und Connectors anzeigen.

Weitere Informationen und Beispiele für diese Tabellen finden Sie unter Unterstützte Hardware-Service Graph Connectors für Sicherheitsstatus-Überwachung und Unterstützte Softwareservice Graph Connectors für Sicherheitsstatus-Überwachung. Die Listen sind zwar nicht umfangreich, Sie können jedoch sehen, wie die unterstützten Connectors eine große Vielfalt an Daten bereitstellen.

Sicherheitsstatus-Überwachung unterstützt ServiceNow-Produkte wie Software Asset Management (SAM) und Hardware Asset Management (HAM), die Sie zusammen mit Service Graph Connectors verwenden können, um nach Diskrepanzen zwischen der von Ihren Schwachstellenscanner-Produkten gemeldeten installierten Software und der zu suchen Von Scannern gemeldete Software, die bereits in SAM und anderen ServiceNow-Produkten berücksichtigt wird.

Weitere Informationen zum Herunterladen, Konfigurieren und Aktivieren von unterstützten Anwendungen für Service Graph Connectors finden Sie in den folgenden Themen:

- Service Graph Connectors .
- Laden Sie eine Anwendung zum ersten Mal von ServiceNow Store herunter.
- Aktivieren Sie eine ServiceNow Store -Anwendung.

Richtlinien für Sicherheitsstatus-Überwachung

Richtlinien prüfen Ihre Assets basierend auf Daten, die aus Ihren Service Graph Connectors importiert werden, um Sie bei der Suche nach potenziellen Verstößen zu unterstützen.

Richtlinien

Sicherheitsstatus-Überwachung -Richtlinien basieren auf einem Datenmodell für Asset-Beziehungen-Eigenschaften. Es gibt Richtlinien, die in der Anwendung enthalten sind, und Sie können eigene Richtlinien erstellen, um nach bestimmten Kriterien zu suchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Kriterien für Richtlinien können entweder in Form von Bedingungen für die Eigenschaften dieses Assets oder für die Eigenschaften einer zugehörigen Entität angegeben werden. Im Richtliniengenerator im Modul Richtlinien und Ergebnisse im Arbeitsbereich können Sie Richtlinien definieren, um nach einem Asset-Typ (Hardware, Software) und einer Verbindung (Gemeldet von, Nicht gemeldet von) oder einer Entität (Asset-Quelle, Service Graph) zu suchen (Connector-Produkt oder CMDB-Metadaten) oder Sie können andere Arten bestimmter Kriterien abgleichen.

Unterstützung beim Ändern oder Erstellen von Richtlinien:

- Legen Sie Ihre Bedingungen im Modul Asset-Suche fest, und suchen Sie nach Assets anhand bestimmter Service Graph Connector-Produkte oder nach Assets, deren bestimmte Daten von einem Connector gemeldet werden. Sie können Ihre Suchen als Richtlinien speichern.
- Klonen Sie die in der Anwendung enthaltenen Richtlinien, um umfangreichere Richtlinien zu erstellen. Sie können die Bedingungen einer vorhandenen Richtlinie kopieren und dann verfeinern, ohne sie erneut eingeben zu müssen.
- Erstellen Sie neue Richtlinien (untergeordnete Richtlinien) anhand von Basisrichtlinien, die Sie als Ausgangspunkt für neue Richtlinien auswählen.

Asset-Typen und Richtlinien

Sie verwenden diese primären Asset-Typen bzw. Asset-Typen der obersten Ebene als Ausgangspunkt für die Definition von Richtlinien.

Hardware-Asset

Hardware-Asset ist eine Abstraktion, die jedes Gerät darstellt, einschließlich persönlicher Computergeräte, Server, Netzwerkgeräte, virtueller Cloud-Maschinen und anderer Hardware. Richtlinien prüfen Ihre Assets auf potenzielle Verstöße basierend auf den importierten Daten aus Service Graph Connector-Produkten und ServiceNow® -Produkten wie Software Asset Management (SAM) und ITOM Discovery.

Software Asset

Mit Software-Asset können Sie nach Diskrepanzen suchen, die zwischen der installierten Software, die von importierten Daten aus Service Graph Connectors gemeldet wird, Ihren Schwachstellen-Scanner-Produkten und der von Scannern gemeldeten Software bestehen, die bereits in Software Asset Management (SAM) und anderen ServiceNow-Instanzen berücksichtigt wird Produkte.

Entitäten und ihre Beziehungen zu sekundären Entitäten

Entität	Beziehung	Zielentität	Beschreibung
Hardware-Asset	Gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die dieses Asset an CMDB gemeldet hat.
Hardware-Asset	Wird nur von gemeldet	Asset-Quelle	Stellt die einzige Quelle dar, die dieses Asset an CMDB meldet.
Hardware-Asset	Nicht gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die dieses Asset nicht an CMDB gemeldet hat.
Hardware-Asset	Mit IRM-Ausnahme	IRM-Ausnahme	Stellt einen Ausnahmedatensatz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entitäten und ihre Beziehungen zu sekundären Entitäten (Fortsetzung)

Entität	Beziehung	Zielentität	Beschreibung
			in Integrated Risk Management dar
Hardware-Asset	Mit Schwachstelle	Schwachstelle	Stellt eine für dieses Asset gefundene Schwachstelle dar.
Hardware-Asset	Hat Konfigurationsergebnis	Konfiguration	Stellt ein Konfigurations- und ein Compliance-Problem dar, das bei diesem Asset gefunden wurde.
Hardware-Asset	Mit CMDB-Metadaten	CMDB-Metadaten	Stellt die Sammlung von CMDB-CI-Eigenschaften für dieses Asset dar.
Hardware-Asset	Mit Connector-Daten	Service Graph Connector	Stellt eine Sammlung von Eigenschaften dar, die vom ausgewählten Service Graph Connector für dieses Asset gemeldet wurden.
Hardware-Asset	Mit aggregierten Daten	Aggregierte Daten	Sammlung von Eigenschaften mit zusammengefassten Werten, die von verschiedenen Quellen für ein bestimmtes Asset gemeldet wurden. Ein Beispiel ist OS.
Hardware-Asset	Aus CI-Klasse	CMDB-CI-Klasse	Wird zum Definieren von Bedingungen für bestimmte CI-Klasseneigenschaften verwendet.
Hardware-Asset	Hat Cloud-Metadaten	Cloud-Metadaten	Stellt Cloud-Metadaten dar (gilt für Cloud-VMs).
Hardware-Asset	Port für das Internet verfügbar gemacht	OpenPort	Stellt einen für das Internet offenen Port dar (gilt für Cloud-VMs).
Software	Gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die diese Software gemeldet hat.
Software	Wird nur von gemeldet	Asset-Quelle	Stellt die einzige Quelle dar, die diese Software meldet.
Software	Nicht gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die diese Software nicht gemeldet hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entitäten und ihre Beziehungen zu sekundären Entitäten (Fortsetzung)

Entität	Beziehung	Zielentität	Beschreibung
Software	Mit Softwaredetails	Software	Stellt die Sammlung von Softwareeigenschaften wie z. B. Herausgeber und Version dar.

Beispiel für Richtlinien-Audit und Datenauffüllung: CI-Klassen in der CMDB

Wenn eine Richtlinie versucht, eine Asset-Klasse abzurufen, die von einem bestimmten Service Graph Connector gemeldet oder nicht gemeldet wird, ordnet die Sicherheitsstatus-Überwachung alle relevanten CI-Klassen (Configuration Item, Konfigurationselement) zu, die sich auf diese Asset-Klasse in der CMDB beziehen und ausgefüllt sind oder die nicht von diesem Service Graph Connector oder dieser Connector-Kategorie ausgefüllt sind.

Angenommen, eine Richtlinie sucht nach allen Hardware-Assets, die von Service Graph Connector Jamf Pro gemeldet werden. Es gilt die folgende Logik.

1. Die Sicherheitsstatuskontrolle identifiziert, welche CI-Klassen in der CMDB der Klasse „Hardware-Asset“ für Jamf Pro zugeordnet sind.

   Hinweis:
   Verschiedene Service Graph Connectors füllen unterschiedliche CI-Klassen in der CMDB, und die Zuordnung zu CI-Klassen aus „Hardware-Asset“ variiert von einem Service Graph Connector zum anderen.

2. Sicherheitsstatus-Überwachung bestimmt, dass die CI-Klassen „Computer“, „Server“ und „Drucker“ in der CMDB der Asset-Klasse „Hardware-Asset“ für Service Graph Connector Jamf Pro zugeordnet werden.
3. Sicherheitsstatus-Überwachung fragt dann alle Asset-Datensätze ab, die in einer der drei CI-Klassen Server, Computer und Drucker von Jamf Pro Service Graph Connector in der CMDB ausgefüllt werden, und gibt diese Assets zurück.

   Die Spalte „Von SPC unterstützte CI-Klassen“ in der folgenden Tabelle gibt an, welche Klassen von CI-Datensätzen während einer Abfrage durch das Produkt Security Posture Control im Rahmen einer Richtlinienbewertung berücksichtigt werden. Diese Tabelle ist keine vollständige Liste, Sie können sie jedoch verwenden, um zu sehen, wie erfasste Daten aus verschiedenen Kategorien und Quellen im Allgemeinen zugeordnet und abgefragt werden.

Erstellen eigener Richtlinien

Unter Erstellen eigener Richtlinien in der Anwendung Sicherheitsstatus-Überwachung finden Sie weitere Informationen zum Erstellen eigener Richtlinien.

Beispielrichtlinien finden Sie unter Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung finden Sie weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte SGCs

Eine Liste einiger der unterstützten Service Graph Connectors finden Sie unter Unterstützte Hardware-Service Graph Connectors für Sicherheitsstatus-Überwachung und Unterstützte Softwareservice Graph Connectors für Sicherheitsstatus-Überwachung.

Richtlinien für ausgleichende Steuerungen

Im Arbeitsbereich Sicherheitsstatus-Überwachung (SSÜ) erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Steuerungen zur Risikominderung gemindert werden, je nach Konfiguration verschiedener Sicherheitstools. Weitere Informationen finden Sie unter Steuerungen und Richtlinien zur Risikominderung in Sicherheitsstatus-Überwachung.

In der Anwendung Sicherheitsstatus-Überwachung enthaltene Richtlinien

Es gibt einige Richtlinien, die in der Anwendung Sicherheitsstatus-Überwachung enthalten sind, die an wichtige Anwendungsfälle gebunden sind und letztendlich als wichtige Einblicke im Dashboard auf der Zielseite (Homepage-Modul) im Arbeitsbereich SSÜ angezeigt werden.

Richtlinien werden angezeigt

Um diese Richtlinien anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Alle**.

Diese Richtlinien sind standardmäßig deaktiviert. Sie müssen sie aktivieren, um zurückgegebene Ergebnisse (Ergebnisse) anzeigen zu können. Sie können diese Richtlinien nicht bearbeiten, aber Sie können sie verwenden, um andere Richtlinien zu erstellen, indem Sie ihre Bedingungen als Ausgangspunkt klonen. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.

Sie können diese Richtlinien klonen, um Ihre eigenen anwenderdefinierten Richtlinien zu erstellen. Beachten Sie jedoch, dass von Ihnen geklonte Richtlinien nicht als wichtige Einblicke im Dashboard auf der Zielseite der Homepage mit den in der Anwendung enthaltenen wichtigen Einblicken wiedergegeben werden. Sie können jedoch Ergebnisse für diese geklonten Richtlinien konfigurieren und die von diesen Richtlinien zurückgegebenen Ergebnisse anzeigen.

Sie können anwenderdefinierte Einblicke oder Berichte für die geklonten Richtlinien konfigurieren oder alternativ Ergebnisse für diese geklonten Richtlinien konfigurieren, um die Remediation zu verwalten. Sie können auch Ihre eigenen anwenderdefinierten Richtlinien von Grund auf neu erstellen, um die Abdeckung der Sicherheitskontrollen gemäß Ihren internen Anforderungen zu überwachen.

Die mit der Anwendung gelieferten Richtlinien umfassen die folgenden Kategorien:

- Richtlinien, die die Abdeckung von Sicherheitskontrollen überwachen (Endpunktschutz und Schwachstellenscanner).
- Richtlinien, die nicht verwaltete Geräte identifizieren.
- Richtlinien, die toxische Kombinationen überwachen, die kritische Kombinationen wie fehlende Sicherheitskontrollen, Internet-Gefahrenpotenzial usw. betreffen.
- Richtlinien für die SSÜ API-Integrationen für die Überwachung von Ausgleichssteuerungen.

Nachdem Sie die von Ihnen erstellten Richtlinien geklont und aktiviert haben, müssen Sie im Modul „Generator für anwenderdefinierten Einblicke“ (dem letzten Modul im Navigationsbereich) einen eigenen anwenderdefinierten Einblicksdatensatz erstellen. Erst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dann können Sie die Daten aus Ihren Richtlinien im Dashboard für anwenderdefinierte Einblicke (zweites Symbol von oben im Arbeitsbereich) anzeigen.

Erstellen eigener Richtlinien

Unter Erstellen eigener Richtlinien in der Anwendung Sicherheitsstatus-Überwachung finden Sie weitere Informationen zum Erstellen eigener Richtlinien.

Beispielrichtlinien finden Sie unter Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung finden Sie weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

Unter Steuerungen und Richtlinien zur Risikominderung in Sicherheitsstatus-Überwachung finden Sie weitere Informationen zu Richtlinien, die für die Überwachung von Ausgleichssteuerungen verwendet werden.

Erstellen eigener Richtlinien in der Anwendung Sicherheitsstatus-Überwachung

Sie können Ihre eigenen anwenderdefinierten Richtlinien erstellen, um Daten zu überwachen, die für die Assets in Ihrer Umgebung spezifisch sind. Diese Richtlinien basieren auf Daten, die Sie aus den verschiedenen Service Graph Connectors importieren, die Sie installiert und aktiviert haben.

So starten Sie

Sie können vorhandene Richtlinien klonen und ihnen weitere Bedingungen hinzufügen oder eine Richtlinie von Grund auf neu erstellen. Für Ihre anwenderdefinierten Richtlinien können Sie Kriterien für allgemeine CMDB-Eigenschaften einbeziehen, die von verschiedenen Service Graph Connectors gefüllt werden.

Alternativ können Sie eine Basisrichtlinie als Ausgangspunkt verwenden und Bedingungen für genehmigte Ausnahmen mit Richtlinien hinzufügen, z. B. für die Anwendung Governance, Risk, and Compliance (GRC). Diese Ausnahmen gelten für Assets, die Sie nicht überwachen und in Ihre Asset-Anzahlen aufnehmen möchten.

Für Ihre anwenderdefinierten Richtlinien können Sie Bedingungen für Metadaten wie Betriebssystem, BS-Version und FQDN einbeziehen, z. B. um Sie bei der Überwachung von Assets mit älterer Software zu unterstützen. Beachten Sie, dass es sich bei diesen Eigenschaften um allgemeine CMDB-Eigenschaften handelt, die von verschiedenen Service Graph Connectors für ein bestimmtes Asset ausgefüllt werden.

Unter In der Anwendung Sicherheitsstatus-Überwachung enthaltene Richtlinien finden Sie weitere Informationen zu Asset-Typen der obersten Ebene und ihren Beziehungen im Richtlinienbedingungsgenerator für Ihre Policen.

Beispielrichtlinien finden Sie unter Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung finden Sie weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

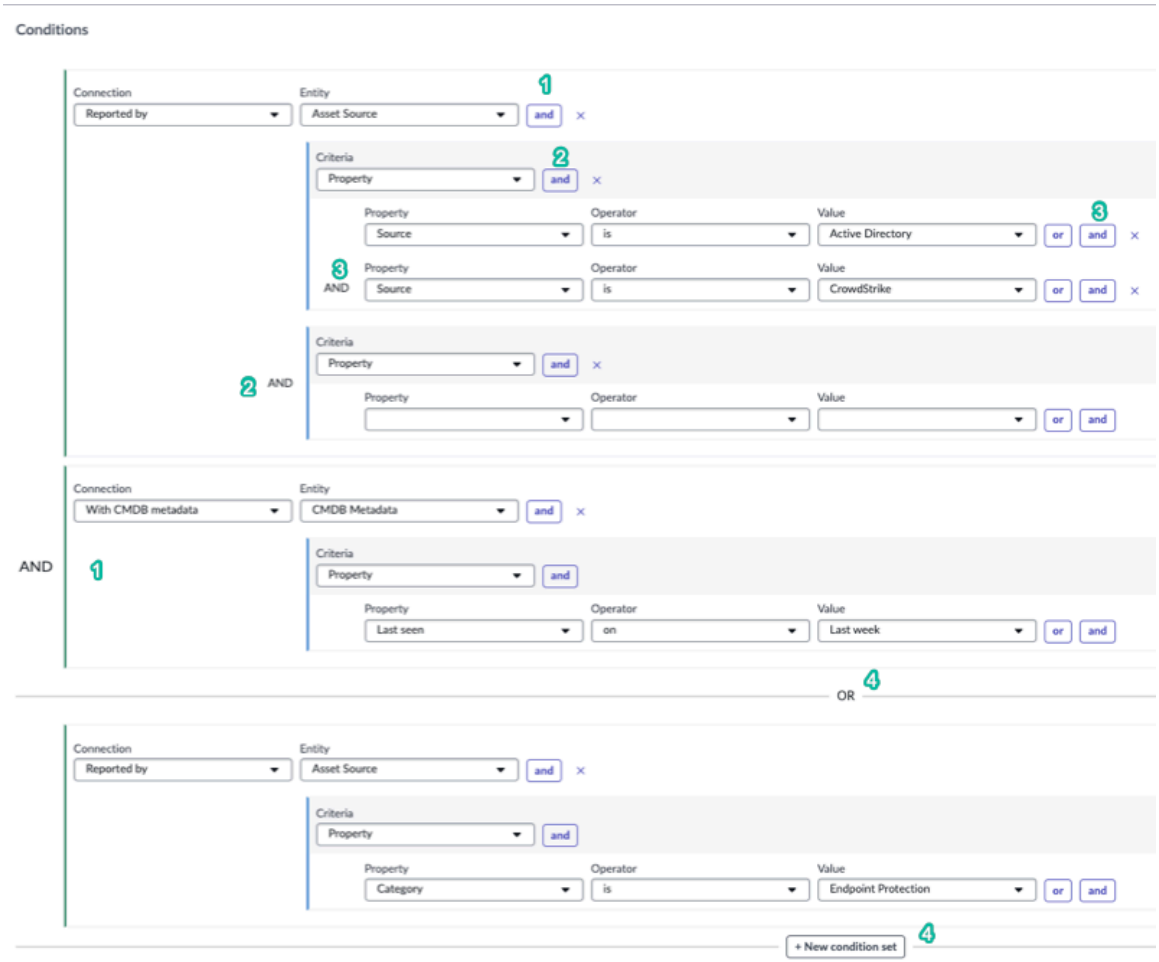
Mithilfe der Decorator-Elemente AND und OR im Bedingungsgenerator

Sie navigieren von den Asset-Typen der obersten Ebene für Hardware und Software zu ihren sekundären Entitäten, indem Sie den Bedingungsgenerator im Modul Richtlinien und Ergebnisse im Arbeitsbereich verwenden. Abhängig von Ihrer Auswahl werden Felder für Sie angezeigt, und Sie können Kriterien ändern oder hinzufügen.

Mit den AND-, OR-Decorator-Elementen im Bedingungsgenerator können Sie die Logik für die zurückgegebenen Daten einrichten, die für die Richtlinie zurückgegeben werden sollen.

Dekorateur	Beschreibung	Nummer, auf die im Bild verwiesen wird
Wählen Sie **AND** neben den obersten Feldern „Verbindung“ und „Entität“ aus, um eine neue Gruppe von Bedingungen anzuzeigen.	Fügt ein logisches UND zwischen den aktuellen Kriterien der Verbindungsentität und neuen Kriterien aus einer anderen Verbindungsentität hinzu.	1
Wählen Sie **AND** rechts neben einem Feld Kriterien oder Eigenschaft aus, um einen neuen Satz von Kriterien- und Eigenschaftsbedingungen zu erhalten.	Fügt ein logisches UND zwischen den aktuellen Kriterien der Verbindungsentität und einem neuen Kriterium unter derselben Verbindungsentität hinzu.	2
Wählen Sie **ODER/UND** rechts neben einem Eigenschaftsfeld aus, um einen neuen Satz von Eigenschaftsbedingungen zu erhalten.	Fügt ein logisches ODER/ UND zwischen der aktuellen Eigenschaft und einer neuen Eigenschaft aus denselben Verbindungsentitätskriterien hinzu.	3
Wählen Sie **+ Neuer Bedingungssatz aus,** um einen neuen Satz von Bedingungen zu erhalten.	Fügt ein logisches ODER zwischen dem Bedingungssatz aller aktuellen Kriterien und einem neuen Bedingungssatz hinzu.	4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Basisrichtlinien, Klonen und untergeordnete Richtlinien werden verwendet

Sie können mehrere Richtlinien verwenden, um Ihre Assets zu bewerten und eigene anwenderdefinierte Einblicke zu erstellen. Sie haben die folgenden Optionen, um anwenderdefinierte Richtlinien zu erstellen oder vorhandene Richtlinien schnell zu bearbeiten:

- Richtlinie klonen – Erstellt eine Kopie einer Richtlinie. Der Name der Richtlinie und ihre Bedingungen werden mit „Kopie“ im Titel angezeigt. Die Bedingungen werden angezeigt, und Sie können sie bearbeiten. Weitere Informationen finden Sie unter Bearbeiten Sie eine aktivierte Richtlinie in Sicherheitsstatus-Überwachung.
- Untergeordnete Richtlinie erstellen – Der Name der Richtlinie, mit der Sie gestartet haben, wird im neuen Datensatz als „Basisrichtlinie“ angezeigt. Die Bedingungen der Basisrichtlinie werden in der neuen Richtlinie geerbt, und ein neuer, leerer Bedingungssatz wird angezeigt. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.
- Ausschlussrichtlinien: Fügen Sie Ihren anwenderdefinierten Richtlinien Richtlinien hinzu, damit Asset-Ergebnisse aus den von Ihnen ausgewählten Richtlinien von Ihren Ergebnissen ausgeschlossen werden. Weitere Informationen finden Sie unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung.

Metadaten- und CMDB-Filterung

Für Ihre Sicherheitsteams kann es wichtig sein, Assets mit älterer Software zu überwachen. Sie können Richtlinienkriterien angeben, beginnend mit der Verbindung „Mit CMDB-Metadaten“ nach dem Hardware-Asset-Typ, um die unten aufgeführten allgemeinen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften einzubeziehen. Dies ist keine vollständige Liste. Um diese Metadaten zu sammeln, müssen die Eigenschaften über die CMDB-Metadatenverbindung verfügbar sein, die von Ihren Service Graph Connectors ausgefüllt wird.

- RAM
- Hostname
- Seriennummer
- BS-Domäne
- BS-Version
- Festplattenspeicher
- Zuletzt gesehen
- BS
- Zuerst gesehen
- CPU-Anzahl
- MAC-Hersteller
- NIC
- IP-Adresse
- Standort
- FQDN
- Netzmaske
- IP-Version
- Seriennummertyp
- BS-Service Pack

Ab v3.0 von Sicherheitsstatus-Überwachung:

Die Verbindung „Mit CMDB-Metadaten“ ermöglicht es Ihnen, die Eigenschaft „Hostname“ hinzuzufügen und den Operator für reguläre Ausdrücke für Übereinstimmungen zu verwenden, um reguläre Ausdrücke in Ihre Bedingungen für den Asset-Typ „Hardware“ einzugeben. Wenn Sie beispielsweise „LP“ eingeben, können Sie nach allen Laptops suchen, bei denen „LP“ das zweite und dritte Zeichen im Hostnamen ist.

„Zuerst gesehen“: Assets, die zum ersten Mal von einer beliebigen Quelle innerhalb des Zeitrahmens erkannt wurden, den Sie mit der Zeitstempeleigenschaft „Zuerst gesehen“ auswählen.

„Zuletzt gesehen“: Assets, die von einer beliebigen Quelle „Zuletzt gesehen innerhalb der letzten n Tage“ wurden. Geben Sie die Anzahl der Tage bis zu 30 als Wert ein. Geben Sie beispielsweise 3 als Wert ein, um Assets nach „letzter Anmeldung“ in Active Directory in den letzten drei Tagen zu überwachen.

Software-Asset-Typ: Suchen Sie nach Softwareherausgebern, oder verwenden Sie SGCs, die Sie installiert haben, um die gewünschten Softwaredaten und Metadaten zu importieren, wenn Sie mit der Verbindung „Mit Softwaredetails“ beginnen.

Für Hardware-Asset-Typen können Sie die Verbindung „Hat Modellinformationen“ mit der Verbindung „Mit CMDB-Metadaten“ für Geräte basierend auf bestimmten Modellen und Modellinformationen verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Hardware-Asset-Typen können Sie auch nach allen Assets suchen, die von einer Quelle gemeldet werden, z. B. Qualys, aber nicht von ServiceNow ITOM Discovery gemeldet werden.

Weitere Informationen zum Richtlinienschema Sicherheitsstatus-Überwachung finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

Ausnahmen bei der Anwendung Governance, Risk, and Compliance (GRC).

Eine Ausnahme für Integrated Risk Management (IRM) ist ein Asset mit einer genehmigten Ausnahme vom Produkt Governance, Risk, and Compliance (GRC). Sie haben die Möglichkeit, in einer Richtlinie eine Bedingung für eine Ausnahme hinzuzufügen, damit Sie diese Assets nicht überwachen und in Ihre Zählungen aufnehmen.

Beispielsweise können für einige Assets Ausnahmen für bestimmte Kontrollziele mit IRM genehmigt wurden. Um die zurückgegebenen Übereinstimmungen zu reduzieren, möchten Informationssicherheitsteams möglicherweise diese Assets von der Überwachung auf Sicherheitskontrollen mit IRM-Ausnahmen ausschließen, die bereits genehmigt wurden.

Wichtige Einblicke und konfigurierte Einblicke für Sicherheitsstatus-Überwachung

Wichtige und konfigurierte (anwenderdefinierte) Einblicke bieten Ihnen visuelle Berichte, die anhand der Bewertungskriterien erstellt und aktualisiert werden, die Ihren Assets entsprechen. Einblicke helfen Ihnen, Sicherheitskontrollmetriken in einem Dashboard zu überwachen.

Wichtige Einblicke

Die Kriterien, die für die Bewertungen Ihrer Assets verwendet werden, werden von den Richtlinien bereitgestellt, die in der Anwendung enthalten sind.

- Wichtige Einblicke verwenden die Richtlinien, die in der Anwendung enthalten sind.
- Konfigurierte Einblicke können mit den in der Anwendung enthaltenen Richtlinien, Ihren eigenen anwenderdefinierten Richtlinien oder einer Kombination aus beidem erstellt werden.

Auf der Startseite (Zielseite) im Arbeitsbereich für die Kontrolle des Sicherheitsstatus zeigt der Abschnitt „Wichtige Einblicke“ unter der Übersicht visuelle Berichte an. Diese werden anhand der in der Anwendung enthaltenen Richtlinien erstellt und aktualisiert. Diese Einblicke sind auch in der Anwendung enthalten und zeigen die folgenden Informationen an:

- Installierter Endpunktschutz-Agent: Gesamtzahl der Assets, die über Endpunktschutz verfügen oder nicht verfügen.
- Abdeckung verwalteter Geräte: Anzahl der verwalteten Assets im Vergleich zu den nicht verwalteten Assets.
- Abdeckung von Schwachstellenscan: Gesamtzahl der gescannten Assets im Vergleich zu den Assets, die nicht von einem Drittanbieter-Schwachstellenscanner auf bekannte Schwachstellen gescannt werden.
- Assets mit kritischen Schwachstellen: Anzahl der Assets aus der Gesamtzahl der Assets, die kritische Schwachstellen aufweisen.
- Angreifbare Elemente nach Relevanz: Gesamtzahl der angreifbaren Elemente, aufgeschlüsselt nach ihrem Schweregrad. Eine bekannte Schwachstelle, die mit einem Asset in Ihrer CMDB übereinstimmt, führt zu einem angreifbaren Element. Für diesen Einblick müssen Sie die Anwendung Vulnerability Response und mindestens eine Scanner-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration installieren: Qualys, Rapid7 oder Tenable Vulnerability Integration. Alle diese Anwendungen sind unter ServiceNow® Storeverfügbar.

- Top-3-Richtlinien nach Ergebnissen: Richtlinien, die die meisten Ergebnisse (Übereinstimmungen) für Ihre Assets zurückgeben.

Konfigurierte Einblicke

Sie können eigene Einblicke erstellen, wenn Sie weitere Informationen wünschen, die nicht in den Schlüsseleinblicken enthalten sind. Sie können diese konfigurierten Einblicke erstellen und vorhandene Richtlinien oder Ihre eigenen anwenderdefinierten Richtlinien für die Bewertung verwenden. Ihre konfigurierten Einblicke werden im Dashboard-Modul Konfigurierte Einblicke, dem zweiten Symbol von oben im Arbeitsbereich, angezeigt.

Die folgenden Arten von Einblicken können konfiguriert werden.

- Vergleichsdiagramm: Vergleichen Sie mithilfe von Balkendiagrammen Ergebnisse zwischen mehreren Richtlinien.
- Widget für die Anzahl der Richtlinienübereinstimmungen: Zeigen Sie die Anzahl der Geräte an, die mit einer Richtlinie übereinstimmen.
- Diagramm für prozentuale Richtlinienübereinstimmung: Zeigen Sie den Prozentsatz der Geräte an, die mit einer Richtlinie in einem Kreisdiagramm übereinstimmen. Sie können als Gesamt-Asset-Pool entweder alle von SPC überwachten Assets oder die Assets auswählen, die der Basisrichtlinie entsprechen, aus der die aktuell ausgewählte Richtlinie erstellt wird.
- Richtlinien-Trenddiagramm: Zeigen Sie die Trends von Assets an, die verschiedenen Richtlinien entsprechen.

Unter Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Überwachung finden Sie weitere Informationen zu den Schritten zum Erstellen eines konfigurierten Einblicks.

Gruppen

Sie müssen Gruppen erstellen oder Ihren konfigurierten Einblicken zuweisen, wenn Sie im Modul Benutzerdefinierter Einblickgenerator neue Datensätze erstellen. Mit Gruppen können Sie Ihre Berichte im Dashboard für konfigurierte Einblicke organisieren.

Einblicke können in Gruppen organisiert werden. Jede Gruppe kann 21 Widgets oder Einblicke haben.

Arbeitsbereich Sicherheitsstatus-Überwachung verwenden

Der Arbeitsbereich Sicherheitsstatus-Überwachung enthält die Module, die Sie zum Konfigurieren, Verwenden und Überwachen der importierten Daten zu Ihren Assets verwenden.

Rollen

SPC-Administratorgruppe

Benutzer in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, einschließlich Lizenzierungsinformationen. Granulare Rollen für diese Gruppe sind: [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin und sn_sec_spc_core.configure].

SPC-Analystengruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Granulare Rollen für diese Gruppe umfassen [pa_power_user und sn_sec_spc_core.analyst].

Schreibgeschützte SPC-Analystengruppe

Anwender in dieser Gruppe haben vollständigen Lesezugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Granulare Rollen für diese Gruppe sind [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read und cmdb_ms_user].

Unterstützende Anwendungsrollen

Die folgenden Rollen sind für die -Anwendungen erforderlich, die SSÜ und Sicherheitsstatus-Management für Assetsunterstützen.

- Konfigurations-Compliance Administrator [sn_vulc.admin]: Konfiguriert die Anwendung Konfigurations-Compliance, hat Einblick in alle Datensätze und kann Eigenschaften ändern. Weist Rollen in der Anwendung Konfigurations-Compliance zu.
- Vulnerability Response Administrator [sn_vulc.admin]: Konfiguriert die Anwendung Vulnerability Response und die Schwachstellenrisiko-Rechner.
- MID-Server [mid_server]: Konfiguriert einen MID-Server.

Die Module des Arbeitsbereichs

Um auf den Arbeitsbereich zuzugreifen, navigieren Sie zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** Die Homepage (Zielseite) wird angezeigt. Der Arbeitsbereich Sicherheitsstatus-Überwachung enthält die folgenden Module.

Module

Modul	Beschreibung
Startseite	Zeigen Sie Datenvisualisierungen und andere Informationen in den Abschnitten Übersicht, Wichtige Einblicke und Abdeckung wichtiger Anwendungsfälle an, um Ihre Assets zu überwachen. Mit den auf dieser Seite bereitgestellten Informationen können Sie der IT, IT- und Sicherheitsmanagern und anderen wichtigen Stakeholdern den Status Ihrer allgemeinen Sicherheitslage melden. Siehe Wichtige Einblicke und konfigurierte Einblicke für Sicherheitsstatus-Überwachung und Richtlinien für Sicherheitsstatus-Überwachung.
Konfigurierte Einblicke	Zeigen Sie die Datenvisualisierungen zu Ihren Assets an, die Sie erstellen, konfigurieren und aktivieren. Weitere Informationen finden Sie unter Wichtige Einblicke und konfigurierte Einblicke für Sicherheitsstatus-Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Module (Fortsetzung)

Modul	Beschreibung
Asset-Suche	Suchen Sie schnell nach Assets in Ihrer Umgebung basierend auf den von Ihnen festgelegten Bedingungen. Stellen Sie sicher, dass Sie Assets mit einer Reihe von Bedingungen finden können, bevor Sie diese Bedingungen für eine Richtlinie festlegen. Sie können diese Suchen einschränken, um eine Vorschau der Assets zu erhalten, die Ihren Suchkriterien entsprechen. Wenn Sie bereit sind, können Sie Ihre Bedingungen als Richtlinie speichern. Weitere Informationen finden Sie unter Erstellt eine Asset-Suche in Security Posture Control.
Richtlinien und Ergebnisse	Sie können Richtlinien erstellen, klonen, bearbeiten und aktivieren. Es gibt Richtlinien, die in der Anwendung enthalten sind, und Sie können eigene Richtlinien erstellen. Richtlinien prüfen Ihre Assets, um Übereinstimmungen für potenzielle Verstöße zu finden. Einblicke, Visualisierungen und Anwendungsfälle hängen von Richtlinien ab. Weitere Informationen finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung. Assets, die den Richtlinienbedingungen entsprechen, werden als Ergebnisse gemeldet und der Anwendung Konfigurations-Compliance zur Korrektur zugeordnet. Weitere Informationen finden Sie unter Zeigen Sie Ergebnisse für an Sicherheitsstatus-Überwachung.
Setup von Connectors und Anwendungsfällen	Aktivieren Sie, und zeigen Sie den Status der installierten Service Graph Connectors (SGC) und API-Integrationen an. Service Graph Connectors und API-Integrationen sind Quellen, die Sie für den Import von Daten zu Ihren Assets verwenden. Eine Vielzahl von (SGC) wird unterstützt und ist über ServiceNow® Storeverfügbar. Wichtige Anwendungsfälle einrichten und überwachen Anwendungsfälle sind verschiedene Szenarien, die Sie konfigurieren, um bestimmte Arten von Lücken bei der Toolabdeckung zu identifizieren. Jeder Anwendungsfall erfordert eine oder mehrere Richtlinien,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Module (Fortsetzung)

Modul	Beschreibung
	um Ihre Assets auf potenzielle Verstöße zu prüfen. Weitere Informationen finden Sie unter Anwendungsfälle, Richtlinienbeispiele und unterstützte Service Graph Connectors in Sicherheitsstatus-Überwachung.
Benutzerdefinierter Einblickgenerator	Erstellen Sie Ihre eigenen Datenvisualisierungen. Anwenderdefinierte Einblicke bieten visuelle Berichte, die anhand der Audit-Ergebnisse Ihrer Richtlinien und importierten Daten aktualisiert werden. Sobald Sie sie aktiviert haben, werden Ihre anwenderdefinierten Einblicke im Dashboard im Modul Konfigurierte Einblicke angezeigt. Mithilfe von Gruppen können Sie festlegen, wo Daten für einen Einblick im Dashboard angezeigt werden. Weitere Informationen finden Sie unter Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Überwachung.

Module des Arbeitsbereichs verwenden, um Lücken in der Toolabdeckung zu identifizieren

Um Lücken in Sicherheitstools zu identifizieren, müssen Sie die folgenden Schritte ausführen.

1. Richten Sie API-Verbindungen mit einem der Tools ein, die Sie in verschiedenen Kategorien verwenden. Sie können Service Graph Connectors für Produkte verwenden, die im ServiceNow Store für die erforderlichen API-Verbindungen verfügbar sind. Weitere Informationen zu den unterstützten Service Graph Connectors finden Sie unter Service Graph Connectors für Sicherheitsstatus-Überwachung und Service Graph Connectors. Unterstützte Service Graph Connectors sind im ServiceNow® Store mit separaten Abonnements verfügbar.
2. Führen Sie eine oder mehrere Asset-Suchen basierend auf bestimmten Kriterien durch, um einen Bestand zu erhalten.
3. Aktivieren Sie die in der Anwendung Security Posture Control enthaltenen Richtlinien. Sie können auch oder eigene Richtlinien erstellen und basierend auf den Ergebnissen Ihrer Asset-Suche aktivieren.
4. Erstellen und aktivieren Sie Ihre eigenen konfigurierten Einblicke, um Sie bei der Überwachung Ihrer Assets zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Unter Überwachung von Risikominderungssteuerungen mit Sicherheitsstatus-Überwachungerfahren Sie, welche Bedrohungen für Ihre Assets durch verfügbare Minderungskontrollen gemindert werden, je nachdem, wie verschiedene Sicherheitstools konfiguriert sind.
6. Richten Sie Regeln ein, um den Nachbesserungs-Workflow in der Anwendung Configuration Compliance zu automatisieren.

Das Identifizieren von Lücken in Sicherheitstools umfasst die folgenden Schritte:

1. Aktivieren Sie die mit der Anwendung Sicherheitsstatus-Überwachung gelieferten Richtlinien. Das Produkt Sicherheitsstatus-Überwachung findet Sicherheitstool-Lücken, indem es die folgenden Aufgaben ausführt:
   a. Identifiziert die Liste aller eindeutigen Assets, die von verschiedenen Service Graph Connectors in der CMDB ausgefüllt werden.
   b. Identifiziert Assets, die nicht von bestimmten Kategorien aus diesem Asset-Pool gemeldet werden, z. B. Endpunktschutz. Assets werden basierend auf der aktiven Richtlinie identifiziert, die ausgewertet wird.
   c. Assets, die von bestimmten Kategorien als nicht gemeldet identifiziert wurden, werden in der Anwendung Konfigurations-Compliance als „Ergebnisse“ oder „Testergebnisse“ gemeldet.
2. Weisen Sie „Ergebnisse“ mit der Anwendung „Konfigurations-Compliance“ automatisch verschiedenen Teams zur Korrektur zu.

Erstellen eigener Richtlinien

Unter Erstellen eigener Richtlinien in der Anwendung Sicherheitsstatus-Überwachung finden Sie weitere Informationen zum Erstellen eigener Richtlinien.

Unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung finden Sie weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

Beispielrichtlinien finden Sie unter Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Aktivieren Sie eine Richtlinie, die in der Anwendung Sicherheitsstatus-Überwachung enthalten ist

In der Anwendung enthaltene Richtlinien müssen aktiviert werden, bevor Sicherheitsstatus-Überwachung die Assets überwachen kann, die mit dieser Richtlinie übereinstimmen. Standardmäßig ist keine der in der Anwendung enthaltenen Richtlinien aktiviert.

Vorbereitungen

Sie müssen überprüfen, ob alle erforderlichen Voraussetzungen erfüllt sind, bevor Sie die in der Anwendung enthaltenen Richtlinien aktivieren.

- Stellen Sie sicher, dass die erforderlichen Service Graph Connectors aktiviert sind.
- Stellen Sie sicher, dass alle erforderlichen Anwendungen wie Vulnerability Response installiert und aktiviert sind, falls zutreffend.
- Weitere Informationen zu Richtlinien, die für die Überwachung von Ausgleichssteuerungen verwendet werden, finden Sie unter Steuerungen und Richtlinien zur Risikominderung in Sicherheitsstatus-Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Sie können die in der Anwendung enthaltenen Richtlinien nicht bearbeiten, aber Sie können mit den Funktionen **Richtlinie klonen** und **Untergeordnete Richtlinie erstellen neue Richtlinien basierend auf ihren Kriterien erstellen**. Diese Funktionen sind im Menü „Weitere Optionen“ verfügbar (drei vertikale Punkte).

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Alle**.

   Um zu bestimmen, ob eine Richtlinie aktiviert ist, überprüfen Sie ihren Status (wahr oder falsch) in der Spalte Aktiv.

2. Wählen Sie einen Richtliniendatensatz aus, um ihn zu öffnen.
3. Sie haben die folgenden Optionen für Richtliniendatensätze, die in der Anwendung enthalten sind:

Option	Beschreibung
Richtlinie aktivieren	Aktivieren Sie eine Richtlinie, wenn Sie Assets überwachen möchten, die den Richtlinienbedingungen entsprechen, und Ergebnisse generieren möchten. Wenn verfügbar, wählen Sie Richtlinie deaktivieren, um die Erstellung von Asset-Bewertungen und die Generierung von Ergebnissen für diese Richtlinie zu stoppen.
Ergebnisse konfigurieren	Wählen Sie im Modal **Ja** aus, um Ergebnisse für die Richtlinie zu generieren. Wählen Sie den Link **Zuweisungsregeln konfigurieren** aus, um Zuweisungsregeln in der Anwendung Configuration Compliance einzurichten, um Ergebnisse für Ihre Richtlinie zur Lösung zuzuweisen. **Hinweis:** Für Richtlinien, die Sie mit „Software“ als Asset-Typ erstellen, können Sie die Richtlinie speichern und anwenderdefinierte Einblicke erstellen, Sie können jedoch keine Ergebnisse aus dem Richtliniendatensatz konfigurieren.
Richtlinie klonen	Erstellen Sie eine neue Richtlinie mit allen Bedingungen aus der angezeigten Richtlinie als Ausgangspunkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Weitere Informationen finden Sie unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung.
Erstellen Sie eine untergeordnete Richtlinie	Erstellen Sie eine untergeordnete Richtlinie, die die Bedingungen der aktuellen Richtlinie erbt. Die aktuellen Richtlinienbedingungen werden im Feld „Basisrichtlinie“ des neuen Datensatzes angezeigt, und Sie fügen weitere Bedingungen hinzu.
Richtlinie deaktivieren (wird nur für aktivierte Richtlinien angezeigt)	Deaktivieren Sie eine aktive Richtlinie, wenn Sie nicht möchten, dass Assets anhand dieser Richtlinie überwacht oder bewertet werden. Diese Bearbeitungsoption ist nur bei aktivierten Richtliniendatensätzen sichtbar.
Ergebnisse anzeigen	Öffnen Sie eine neue Registerkarte, und zeigen Sie die übereinstimmenden Assets an, falls verfügbar. Ergebnisse werden auch als CTRs oder Testergebnisdatensätze für die Richtlinie bezeichnet.

Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung

Erstellen Sie Ihre eigenen anwenderdefinierten Richtlinien, um Assets hinsichtlich der Toolabdeckung und anderer Kombinationen mit hohem Risiko zu überwachen.

Vorbereitungen

Weitere Informationen zu den Schritten zum Erstellen einer Richtlinie finden Sie unter Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung. Die Beispiele führen Sie durch die Schritte, die erforderlich sind, um eine Basisrichtlinie zu erstellen, die Basisrichtlinie zum Erstellen einer untergeordneten Richtlinie zu verwenden und eine Richtlinie zu klonen.

Beispielrichtlinien finden Sie unter Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**.
2. Wählen Sie **Neue Richtlinie**aus.
3. Wählen Sie das Bleistiftsymbol neben dem Namen oben aus, um die Metadaten zu ändern.

Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Ein eindeutiger Name für Ihre Richtlinie.
Kritikalität	Wählen Sie eine aus der Liste aus.
Kurzbeschreibung	Eine eindeutige Beschreibung für Ihre Richtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Metadaten speichern**.
5. Wählen Sie für Asset type (Asset-Typ) aus der Liste aus.
6. **Wahlweise:** Wählen Sie keine, eine oder beide Optionen aus.

   (Optional) Die Felder Verbindung und Entität werden angezeigt.
7. Wählen Sie eine aus der Liste für das Feld Verbindung aus.
   Das Feld Zielentität wird basierend auf Ihrer Auswahl automatisch ausgefüllt. Ein neues Feld Kriterien wird zusammen mit den Feldern Eigenschaft, Operator und Wert angezeigt. Weitere Informationen zu Asset-Typen und zum Schema für Beziehungen finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.
8. Wählen Sie eine Eigenschaft aus der Liste aus.
9. Wählen Sie **Kategorie** oder **Quelle**aus.
10. Wählen Sie einen Operator aus, und geben Sie eine Connector-Kategorie ein, z. B. Endpunktverwaltung, oder einen Produktnamen (Quelle).
11. **Wahlweise:** Verwenden Sie den Bedingungsgenerator, und fügen Sie weitere Bedingungen oder Bedingungssätze hinzu.

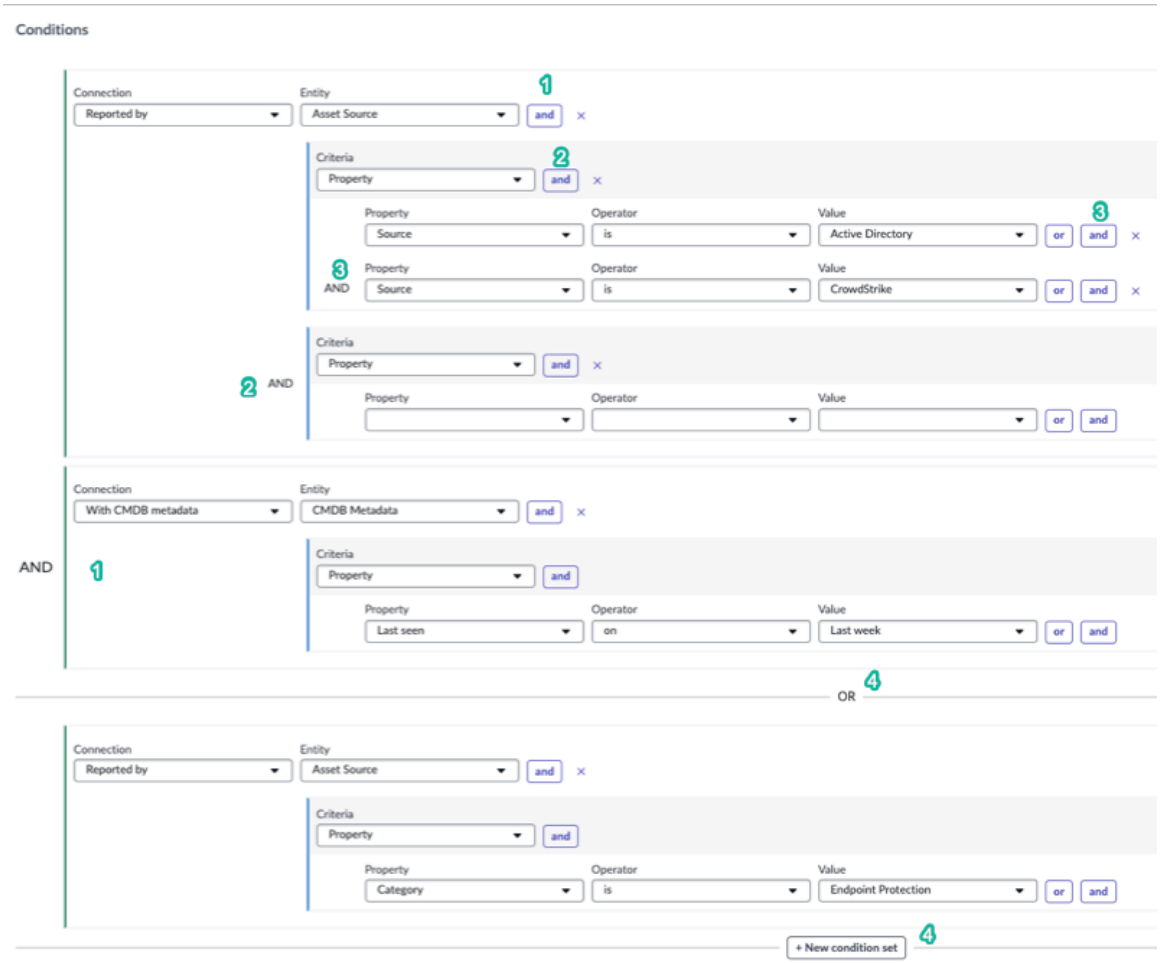
    (Optional) Mit dem Bedingungsgenerator navigieren Sie von den Asset-Typen der obersten Ebene für Hardware und Software zu den sekundären Entitäten. Abhängig von Ihrer Auswahl werden Felder für Sie angezeigt, und Sie können Kriterien ändern oder hinzufügen.

    Mit den AND-, OR-Decorator-Elementen im Bedingungsgenerator können Sie die Logik für die zurückgegebenen Daten einrichten, die für die Richtlinie zurückgegeben werden sollen. Weitere Informationen finden Sie in der folgenden Tabelle und Abbildung.

Dekorateur	Beschreibung	Nummer, auf die im Bild verwiesen wird
Wählen Sie **AND** neben den obersten Feldern „Verbindung“ und „Entität“ aus, um eine neue Gruppe von Bedingungen anzuzeigen.	Fügt ein logisches UND zwischen den aktuellen Kriterien der Verbindungsentität und neuen Kriterien aus einer anderen Verbindungsentität hinzu.	1
Wählen Sie **AND** rechts neben einem Feld Kriterien oder Eigenschaft aus, um einen neuen Satz von Kriterien- und Eigenschaftsbedingungen zu erhalten.	Fügt ein logisches UND zwischen den aktuellen Kriterien der Verbindungsentität und einem neuen Kriterium unter derselben Verbindungsentität hinzu.	2
Wählen Sie **ODER/UND** rechts neben einem Eigenschaftsfeld aus, um einen neuen Satz von Eigenschaftsbedingungen zu erhalten.	Fügt ein logisches ODER/ UND zwischen der aktuellen Eigenschaft und einer neuen Eigenschaft aus denselben Verbindungsentitätskriterien hinzu.	3
Wählen Sie **+ Neuer Bedingungssatz aus,**	Fügt ein logisches ODER zwischen dem Bedingungssatz aller aktuellen Kriterien und	4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dekorateur	Beschreibung	Nummer, auf die im Bild verwiesen wird
um einen neuen Satz von Bedingungen zu erhalten.	einem neuen Bedingungssatz hinzu.	



12. Wählen Sie **Richtlinie speichern** aus, nachdem Sie mit der Bearbeitung fertig sind.
Ihre Richtlinie ist gespeichert. Sie können sie jetzt aktivieren oder später zurückkehren, um sie zu aktivieren.
13. Wählen Sie im Menü mit weiteren Optionen neben **Richtlinie speichern**die Option Ergebnisse konfigurieren aus.
14. Füllen Sie die Felder aus.

Option	Beschreibung
Ergebnisse für diese Richtlinie generieren?	Wählen Sie **Ja** aus, um Ergebnisse für übereinstimmende Assets zu generieren. Nachdem die Daten importiert wurden, wählen Sie „Suchergebnisse anzeigen“ im Richtliniendatensatz aus. Wählen Sie **„Nein“**, wenn Sie keine Ergebnisse generieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Zuweisungsregeln konfigurieren	Wählen Sie den Link, um Zuweisungsregeln für die Zuweisung von Ergebnissen zur Korrektur in der Anwendung Configuration Compliance einzurichten. Die Tabelle [sn_vulc_assignment_rule_list] enthält eine Standardzuweisungsregel, die Sie in Configuration Compliance verwenden können.

15. Wählen Sie **Konfiguration speichern aus**.

Nachdem Sie eine Richtlinie gespeichert und aktiviert haben, wertet sie die importierten Daten aus dem geplanten Service Graph Connector bei der nächsten Ausführung aus. Wenn Sie die Daten im Dashboard „Konfigurierte Einblicke“ im Arbeitsbereich anzeigen möchten, müssen Sie im Modul Custom Insight Builder (Generator für anwenderdefinierte Einblicke) einen neuen Einblick erstellen. Nachdem Sie den konfigurierten Einblick aktiviert haben, werden die zugehörigen Daten im Dashboard „Konfigurierte Einblicke“ im -Arbeitsbereich angezeigt.

Bearbeiten Sie eine aktivierte Richtlinie in Sicherheitsstatus-Überwachung

Sie können aktivierte Richtlinien bearbeiten, um die Bedingungen besser an Ihre Assets anzupassen.

Vorbereitungen

Sie können die in der Anwendung enthaltenen Richtlinien nicht bearbeiten, aber Sie können sie klonen und untergeordnete Richtlinien daraus erstellen. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.

Wenn Sie Richtlinien bearbeiten und Ihre Änderungen veröffentlichen, werden Versionen nachverfolgt und Versionsnummern werden im Richtliniendatensatz und in den zugehörigen Testergebnissen angezeigt.

Bevor Sie eine aktivierte Richtlinie bearbeiten, können Sie sie deaktivieren, damit die Richtlinie Ihre Assets nicht weiter bewertet, während Sie sie bearbeiten.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**.
2. Wählen Sie einen Richtliniendatensatz aus, um ihn zu öffnen.
3. Wählen Sie **Richtlinie bearbeiten**aus.
   Wenn Sie die Bearbeitung zum ersten Mal durchführen, werden neben der aktiven **Schaltfläche Bearbeitungsmodus** beenden zwei deaktivierte Schaltflächen angezeigt: **Changes speichern** und **Changes veröffentlichen**. Wenn Sie diese Richtlinie zuvor bearbeitet und als Entwurf gespeichert haben, wird auch die Benachrichtigung Sie haben eine nicht veröffentlichte Bearbeitung angezeigt.
4. Nehmen Sie Ihre Änderungen vor, und wählen Sie eine aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Changes speichern	Speichern Sie Ihre Änderungen als Entwurf, und kehren Sie zum Bearbeitungsmodus zurück. Ihre Änderungen werden zu diesem Zeitpunkt nicht veröffentlicht. Sie können zur Richtlinie zurückkehren und die Bearbeitung später fortsetzen.
Changes veröffentlichen	Veröffentlichen Sie Ihre Änderungen als neue Version der Richtlinie und beenden Sie den Bearbeitungsmodus automatisch. Es kann einige Zeit dauern, bis die Ergebnisse in der neuen Version der Richtlinie auf der Schaltfläche Ergebnisse anzeigen in der Richtlinie angezeigt werden. Wenn Sie eine neue Version einer Richtlinie veröffentlichen, können Sie alle vorhandenen Ergebnisse für die von Ihnen geänderte Richtlinie schließen. Möglicherweise möchten Sie vorhandene Ergebnisse aus der ursprünglichen Richtlinie schließen, wenn Sie nur Ergebnisse für die geänderte Richtlinie anzeigen möchten. Wenn Sie an dieser Stelle abbrechen oder den Bearbeitungsmodus beenden, wird eine Meldung angezeigt, dass Sie eine unveröffentlichte Bearbeitung für diese Richtlinie haben. Wenn Sie die vorhandenen zugehörigen Testergebnisse (Ergebnisse) schließen, gehen die Status von Testergebnissen und Korrekturaufgaben gemäß den Statusübergangsprozessen der Anwendung Configuration Compliance über. Weitere Informationen finden Sie unter Testergebnis- und Statusübergänge für Korrekturaufgaben in der Anwendung Sicherheitsstatus-Überwachung ..
Versionsverlauf anzeigen	Bei veröffentlichten Änderungen werden die Versionen nachverfolgt, und Versionsnummern werden im Richtliniendatensatz und in den zugehörigen Testergebnissen angezeigt.
Bearbeitungsmodus beenden	Beenden Sie, ohne Ihre Änderungen zu speichern, oder speichern Sie Ihre Änderungen, und beenden Sie den Vorgang ohne Veröffentlichung. Wenn Sie Ihre Änderungen speichern und nicht veröffentlichen, müssen Sie Ihre neue Version

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	veröffentlichen, bevor Ergebnisse erstellt werden können.
Richtlinie deaktivieren (wird nur für aktivierte Richtlinien angezeigt)	Deaktivieren Sie eine aktive Richtlinie, wenn Sie nicht möchten, dass Assets anhand dieser Richtlinie überwacht oder bewertet werden. Diese Bearbeitungsoption ist nur für aktive Policendatensätze sichtbar.
Ergebnisse anzeigen	Öffnen Sie eine neue Registerkarte, und zeigen Sie die übereinstimmenden Assets an, falls verfügbar. Ergebnisse werden für die Richtlinie auch als CTRs oder Testergebnis-Datensätze bezeichnet.

5. Nachdem Sie die Richtlinie als Entwurf gespeichert und den Bearbeitungsmodus beendet haben, treffen Sie eine Auswahl aus den folgenden Optionen:

Option	Beschreibung
Richtlinie bearbeiten	Kehren Sie zum Bearbeitungsmodus zurück.
Richtlinie deaktivieren (wird nur für aktivierte Richtlinien angezeigt)	Deaktivieren Sie eine aktive Richtlinie, wenn Sie nicht möchten, dass Assets anhand dieser Richtlinie überwacht oder bewertet werden. Diese Option ist nur in aktiven Richtliniendatensätzen sichtbar.
Menü „Weitere Optionen“	
Ergebnisse konfigurieren	Wählen Sie im Modal **Ja** aus, um Ergebnisse für die Richtlinie zu generieren. Weitere Informationen finden Sie unter Zeigen Sie Ergebnisse für an Sicherheitsstatus-Überwachung.
Richtlinie klonen	Erstellen Sie eine Kopie des Richtliniendatensatzes. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.
Untergeordnete Richtlinie erstellen	Erstellen Sie eine neue Richtlinie, die diese Richtlinie als Basis verwendet. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.
Richtlinie löschen	Entfernen Sie den Richtliniendatensatz aus der Richtlinienliste.
Ergebnisse anzeigen	Öffnen Sie eine neue Registerkarte, und zeigen Sie die übereinstimmenden Assets an, falls verfügbar. Ergebnisse werden auch auf Testergebnisdatensätze (CTRs) für die Richtlinie verwiesen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Verknüpfte Datensätze anzeigen	Zeigen Sie für veröffentlichte Richtlinien anwenderdefinierte Einblicke an, falls verfügbar. Siehe Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Überwachung

Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung

Klonen Sie eine vorhandene Richtlinie, und fügen Sie ihr Bedingungen hinzu, um eine eigene anwenderdefinierte Richtlinie zu erstellen. Sie können auch untergeordnete Richtlinien aus vorhandenen Richtlinien erstellen.

Vorbereitungen

Sie können Richtlinien klonen, um eigene anwenderdefinierte Richtlinien zu erstellen. Sie können eine Richtlinie klonen oder eine untergeordnete Richtlinie erstellen, indem Sie eine beliebige Richtlinie als Basis verwenden, um die vorhandenen Richtlinien zu erweitern, ohne die Bedingungen erneut eingeben zu müssen. Alle Bedingungen in der Basisrichtlinie werden auch in der untergeordneten Richtlinie geerbt. Weitere Informationen finden Sie unter Richtlinie klonen für Sicherheitsstatus-Überwachung (Beispiel).

Sie können alle in der Anwendung enthaltenen Richtlinien klonen, aber Richtlinienübereinstimmungen werden nicht als wichtige Einblicke im Dashboard auf der Zielseite der Homepage angezeigt. Auf der Zielseite der -Homepage werden nur wichtige Einblicke für Richtlinien angezeigt, die in der Anwendung enthalten sind.

Nachdem Sie die von Ihnen erstellten Richtlinien geklont und aktiviert haben, müssen Sie im Modul Benutzerdefinierter Einblickgenerator im Arbeitsbereich (dem letzten Modul im Navigatorbereich) einen eigenen konfigurierten Einblicksdatensatz erstellen. Erst dann können Sie die Daten aus Ihren Richtlinien im Dashboard „Konfigurierte Einblicke“ (zweites Symbol von oben im Arbeitsbereich) anzeigen.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**.
2. Wählen Sie den Richtliniendatensatz aus, den Sie klonen möchten.
3. Wählen Sie eine aus dem Menü mit weiteren Optionen neben **Richtlinie aktivieren aus**.
4. **Wahlweise:** Wählen Sie **Basisrichtlinie** und anschließend eine Richtlinie als Basis für Ihre neue Richtlinie aus.

   (Optional) Sie können diese Option wählen, wenn Sie die Bedingungen einer vorhandenen Richtlinie als Ausgangspunkt für die neue Richtlinie erben möchten.
5. **Wahlweise:** Wählen Sie **Ausschlussrichtlinien** und anschließend Richtlinien aus, die bei den Ergebnissen dieser Richtlinie nicht berücksichtigt werden sollen.
   Alle Ergebnisse in Ihrer neuen Richtlinie, die mit ausgeschlossenen Richtlinien übereinstimmen, werden nicht in Ihre Ergebnisse einbezogen.
6. Bearbeiten Sie die Bedingungen für eine geklonte Richtlinie.
   Weitere Informationen zu den Beziehungen zwischen Asset und Verbindungsentität im Bedingungsgenerator finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung. Weitere Informationen zu den Decorator-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elementen im Bedingungsgenerator finden Sie unter Erstellen eigener Richtlinien in der Anwendung Sicherheitsstatus-Überwachung.

7. Bearbeiten und speichern Sie Ihre Richtlinie mit **Änderungen speichern**.
   Ihre Richtlinie wird in der Liste Alle im Listenmodul im -Arbeitsbereich angezeigt.
8. Um eine Richtlinie zu aktivieren, führen Sie die in Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachungbeschriebenen Schritte aus.
9. **Wahlweise:** Wählen Sie Richtlinie löschen, um eine Richtlinie zu löschen.
   Die Option zum Löschen wird für Richtlinien, die mit der Anwendung bereitgestellt werden, oder für Richtlinien, die Ergebnisse generiert haben, nicht unterstützt. Sie können Richtlinien nur mit Ergebnissen deaktivieren.

Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Überwachung

Sie können Ihre eigenen Einblicke erstellen. Konfigurierte Einblicke sind Einblicke, die Sie entweder mit vorhandenen Richtlinien oder mit Ihren eigenen anwenderdefinierten Richtlinien erstellen können.

Vorbereitungen

Sie müssen einen Einblicksdatensatz erstellen und aktivieren, bevor Sie Ihre Daten im Dashboard „Konfigurierte Einblicke“ anzeigen können. Im Dashboard-Modul „Konfigurierte Einblicke“ im -Arbeitsbereich können Sie bis zu sechs Einblicke und 21 Diagramme anzeigen.

Alle Richtlinien, die Sie für einen anwenderdefinierten Einblick verwenden, müssen aktiviert sein.

Für Richtlinien, die Sie mit „Software“ als Asset-Typ erstellen, können Sie die Richtlinie speichern und anwenderdefinierte Einblicke erstellen, Sie können jedoch keine Ergebnisse aus dem Richtliniendatensatz konfigurieren.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Benutzerdefinierter Einblickgenerator** (letztes Symbol im Arbeitsbereich).

   Auf dieser Zielseite gibt es drei Registerkarten:

   Aktiv

   Ihre aktivierten anwenderdefinierten Einblicke. Aktivierte anwenderdefinierte Einblicke werden auf der Zielseite „Konfigurierte Einblicke“ (zweites Symbol von oben im Arbeitsbereich) angezeigt.

   Inaktiv

   Ihre inaktiven anwenderdefinierten Einblicke. Deaktivierte Einblicke werden erst auf der Zielseite „Konfigurierte Einblicke“ angezeigt, wenn die Einblicke und die sie unterstützenden Richtlinien aktiviert sind.

   Alle

   Alle Ihre aktiven und inaktiven konfigurierten Einblicke.

2. Wählen Sie **Neuer Einblick** rechts auf der Seite aus, um einen neuen Datensatz zu erstellen.
3. Wählen Sie im Feld Typ einen Einblick aus der Auswahlliste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Vergleichsdiagramm	Vergleichen Sie die Anzahl der übereinstimmenden Assets für bis zu fünf Policen.
Widget für die Anzahl der Richtlinienübereinstimmungen	Die Gesamtzahl Ihrer Assets, die einer Police oder Policen entsprechen.
Diagramm für prozentuale Richtlinienübereinstimmung	Der Prozentsatz Ihrer gesamten Assets, die mit einer Police übereinstimmen oder nicht übereinstimmen.
Trenddiagramm für Richtlinienübereinstimmung	Verlaufstrend von Assets, die einer Police oder Policen entsprechen.

4. Wählen Sie eine Option aus.
   - Hardware-Asset
   - Software
5. Wählen Sie Gruppen für Ihren Einblick aus.
   Ein Einblick muss mindestens einer Gruppe angehören. Sie müssen Gruppen erstellen oder Ihren konfigurierten Einblicken zuweisen, wenn Sie im Modul Benutzerdefinierter Einblickgenerator neue Datensätze erstellen. Mit Gruppen können Sie Ihre Berichte im Dashboard für konfigurierte Einblicke organisieren.
6. Wählen Sie die Richtlinien und Einblicksbezeichnungen aus, die Sie für Ihre Einblicksdaten verwenden möchten.
7. Wählen Sie **Speichern**.
   Ihr Einblick wird auf der Registerkarte Inaktiver Einblick gespeichert.
8. Um Ihren neuen Einblick zu aktivieren, öffnen Sie den Datensatz in der Liste Inaktiv, und wählen Sie **Aktivieren**aus.
   Daten werden aus dem nächsten geplanten Import für die Service Graph Connectors gesammelt, die den Richtlinien des Einblicks zugeordnet sind, und Daten werden im Dashboard-Modul „Anwenderdefinierte Einblicke“ im -Arbeitsbereich angezeigt.

Zeigen Sie Ergebnisse für an Sicherheitsstatus-Überwachung

Sie können die Ergebnisse, die durch die Bewertung von Richtlinien in Sicherheitsstatus-Überwachung generiert wurden, im -Arbeitsbereich Sicherheitsstatus-Überwachung anzeigen.

Ergebnisse

Sie können Ergebnisse konfigurieren, die bei der Ausführung von Richtlinien generiert werden, sodass sie verschiedenen Teams zur Korrektur zugewiesen oder für die Berichterstellung verwendet werden können. Unter Aktivieren Sie eine Richtlinie, die in der Anwendung Sicherheitsstatus-Überwachung enthalten ist finden Sie weitere Informationen zum Generieren von Ergebnissen direkt aus Ihren Richtlinien.

Die Sicherheitsstatuskontrolle veröffentlicht diese Ergebnisse als „Testergebnisse“ im Konfigurations-Compliance-Modul. Alle administrativen Steuerungen in der Anwendung Configuration Compliance, die sich auf die Zuweisung, Gruppierung (Generierung von Korrekturaufgaben), Korrekturziele und Ausnahmen beziehen, werden für Ergebnisse unterstützt, die von der Sicherheitsstatus-Überwachung generiert werden.

Die für Ergebnisse verwendeten Bezeichnungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Toolabdeckung

Dieser Typ stellt eine Sicherheitstool-Abdeckungslücke dar. Dieser Ergebnistyp gilt für Richtlinien, die die Connector-Beziehungen „Gemeldet von“ und „Nicht gemeldet“ verwenden.

Internet-Gefahrenpotenzial

Dieser Typ stellt das Internet-Gefahrenpotenzial eines Cloud-Assets dar. Dieser Ergebnistyp gilt für Richtlinien, die die Beziehung oder Verbindung „Hat Port für Internet verfügbar gemacht“ verwenden.

Kombination mit hohem Risiko

Dieser Typ stellt ein Problem dar, dem mehr als ein Risikofaktor zugeordnet ist, z. B. Assets mit kritischen Schwachstellen und einem fehlenden Endpunktschutz-Agent.

Ausnahme bei Integrated Risk Management (IRM).

Dieser Typ stellt ein Asset mit einer genehmigten Ausnahme aus dem Produkt Governance, Risk, and Compliance (GRC) dar. Falls angegeben, werden diese Ausnahmen nicht in die Anzahl der Ergebnisse einbezogen.

Hat Schwachstelle

Dieser Typ stellt Assets mit zugehörigen angreifbaren Elementen (VITs) dar, die bekannte Schwachstellen aufweisen.

Sicherheitsstatusbezeichnungen werden generiert und an die Testergebnisse angehängt. Eine Bezeichnung eines geeigneten Typs, z. B. „Toolabdeckung“, wird den Testergebnissen automatisch basierend auf dem Richtlinientyp zugewiesen. Für Assets mit mehreren Bezeichnungen werden mehrere Bezeichnungen angezeigt.

Durch die Verwendung von Sicherheitsstatusbezeichnungen, die den Ergebnissen zugeordnet sind, können Sie Zuweisungsregeln in Configuration Compliance schreiben, um diese Probleme zur Korrektur an Teams weiterzuleiten. Sie können beispielsweise die Ergebnisse zur Toolabdeckung an ein IT-Betriebsteam und die Ergebnisse zur Internetexposition an ein Anwendungsteam senden.

Ort zum Anzeigen von Ergebnissen

Sie haben die folgenden Optionen, um die Ergebnisse anzuzeigen, die durch die Bewertung von Richtlinien generiert wurden.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

- Navigieren zu **Arbeitsbereich für Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Ergebnisse** > **Alle**
- Wählen Sie in einem Richtliniendatensatz **die Option Ergebnisse anzeigen aus**. In der Liste werden Gruppen von Ergebnissen angezeigt, die sie in allgemeine Kategorien einteilen, z. B. „Kombination mit hohem Risiko“, „Internetrisiko“ usw. Diese Gruppen sind jedoch keine formalen Gruppierungen, die zur Korrektur verwendet werden können. Sie müssen in Configuration Compliance Regeln zur Korrektur und Zuweisung von Ergebnissen einrichten.
- Wählen Sie in der Anwendung Configuration Compliance **Testergebnisse** aus, und filtern Sie die Datensätze nach **Quelle ist ServiceNow SPC**.

Dashboard

Im Arbeitsbereich für die Sicherheitsstatus-Überwachung werden auf der Startseite (Zielseite) diese Visualisierungen angezeigt:

Übersicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Assets: Anzahl der lokal und in der Cloud überwachten Assets.
- Ergebnisse nach Relevanz: Anzahl der kritischen Ergebnisse aus den gesamten Assets.
- Von den fünf wichtigsten Quellen überwachte Assets: Die fünf wichtigsten Service Graph Connectors, die über Assets berichten.
- Cloud-Accounts: Anzahl der von AWS und Azure überwachten Cloud-Accounts.
- Offene und geschlossene Ergebnisse: Vergleich von Datensätzen, die sich noch in Bearbeitung befinden oder auf eine Lösung warten, und solchen, die gelöst wurden.

Wichtige Einblicke

- Endpunktschutz-Agent installiert: Gesamtanzahl der Assets, die über Endpunktschutz verfügen oder nicht.
- Abdeckung verwalteter Geräte: Anzahl der verwalteten Assets im Vergleich zu den nicht verwalteten Assets.
- Abdeckung des Schwachstellen-Scans: Gesamtzahl der gescannten Assets im Vergleich zu der Anzahl, die nicht von einem Drittanbieter-Schwachstellenscanner auf bekannte Schwachstellen gescannt werden.
- Assets mit kritischen Schwachstellen: Anzahl der Assets aus der Gesamtzahl der Assets, die kritische Schwachstellen aufweisen.
- Angreifbare Elemente nach Relevanz: Gesamtzahl der angreifbaren Elemente, aufgeschlüsselt nach ihrem Schweregrad. Eine bekannte Schwachstelle, die mit einem Asset in Ihrer CMDB übereinstimmt, führt zu einem angreifbaren Element.
- Top-3-Richtlinien nach Ergebnissen: Richtlinien, die die meisten Ergebnisse (Übereinstimmungen) für Ihre Assets zurückgeben.

Abdeckung wichtiger Anwendungsfälle

Wählen Sie einen Anwendungsfall und dann **Hilfe bei Aktivierung** oder **Hilfe bei Verbesserung** aus, um anzuzeigen, welche Service Graph Connectors und Richtlinien für die wichtigsten Anwendungsfälle aktiviert werden sollten.

Testergebnis- und Statusübergänge für Korrekturaufgaben in der Anwendung Sicherheitsstatus-Überwachung .

Die Status von Ergebnissen (Konfigurationstestdatensätze) und den zugehörigen Korrekturaufgaben werden beeinflusst, wenn Sie Ihre Richtlinien in der Anwendung Security Posture Control ändern.

Statusübergangsszenarien zwischen Testergebnissen und Korrekturaufgaben

Mit einigen Ausnahmen werden die Status zwischen Ihren Ergebnissen (Testergebnissen) und den zugehörigen Korrekturaufgaben in der Sicherheitsstatuskontrolle im Allgemeinen auf die gleiche Weise übergehen wie zwischen Testergebnissen und Korrekturaufgaben in der Anwendung Konfigurations-Compliance. Wenn Sie jedoch Ihre Richtlinien in Security Posture Control ändern, wirken sich Ihre Änderungen auf die Statusübergänge bei Ihren Ergebnissen und den zugehörigen Korrekturaufgaben aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Tabellen veranschaulichen, wie sich die Status Ihrer Ergebnisse ändern, wenn Sie Ihre Richtlinien bearbeiten und eine neue Version veröffentlichen (bearbeiten) oder deaktivieren oder löschen.

Weitere Informationen zu Statusänderungen in Konfigurations-Compliancefinden Sie unter Testergebnis- und Statusübergänge für Korrekturaufgaben in der Anwendung Konfigurations-Compliance ..

Hinweis:
Ab v14.9 von Konfigurations-Compliancewurden die folgenden Begriffe umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie ab Version 14.9
Testergebnisgruppe	Korrekturaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Verbesserungen bei Richtlinien-Audits stellen sicher, dass stillgelegte Assets nicht anhand von aktivierten Richtlinien ausgewertet werden. Wenn der Status eines Assets von **Deaktiviert** zurück zu **Aktiv**wechselt, wird es in die nächste Richtlinienbewertung einbezogen.

Wenn eine Richtlinie ist …	Feldwerte in vorhandenen Ergebnisdatensätzen für …	Übergang zu …
Deaktiviert	Ergebnis	Ursprüngliche Werte beibehalten
	Status	Abgeschlossen
	Lösung	Veraltet

Wenn eine Richtlinie ist …	Feldwerte in vorhandenen Ergebnisdatensätzen für …	Übergang zu …
Bearbeitet mit der Option, alle vorhandenen Ergebnisse zu schließen	Ergebnis	Ursprüngliche Werte beibehalten
	Status	Abgeschlossen
	Lösung	Ergebnis ungültig

Wenn eine Richtlinie ist …	Feldwerte in vorhandenen Ergebnisdatensätzen für …	Übergang zu …
Mit der Option bearbeitet, alle vorhandenen Ergebnisse beizubehalten	Ergebnis	Gültige Testfälle (Bestanden) behalten ihre ursprünglichen Werte, und ungültige Testfälle (Fehlgeschlagen) werden geschlossen.
	Status	Abgeschlossen
	Lösung	Ergebnis ungültig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Richtlinie ist …	Feldwerte in vorhandenen Ergebnisdatensätzen für …	Übergang zu …
Gelöscht	Ergebnisse	Ursprüngliche Werte beibehalten
	Status	Abgeschlossen
	Lösung	Ergebnis ungültig

Erstellt eine Asset-Suche in Security Posture Control

Legen Sie Ihre Bedingungen fest, und suchen Sie nach Assets anhand bestimmter Service Graph Connector-Produkte oder nach Assets, deren bestimmte Daten von einem Connector gemeldet werden.

Vorbereitungen

Nehmen wir als Beispiel für eine Suche an, Sie möchten Ihre Assets mit Windows-Servern und einer bestimmten Version identifizieren, die Sie in den Metadatendetails CrowdStrike von finden.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Asset-Suche**.
2. Wählen Sie eine aus.
   Wählen Sie für dieses Beispiel **Hardware-Asset** als Asset-Typ aus.
3. **Wahlweise:** Wählen Sie **Basisrichtlinie** und **Ausschlussrichtlinien** aus, wenn Sie die Bedingungen einer vorhandenen Richtlinie als Start verwenden möchten und Assets ausschließen möchten, die vorhandenen Richtlinien entsprechen.
   Die von Ihnen ausgewählten Richtlinien werden angezeigt.
4. Wählen Sie **Mit Connector-Daten** für das Feld Verbindung aus.
5. Wählen Sie **CrowdStrike-Gerätedetails** für die Entität aus.
6. Wählen Sie für Eigenschaft, Operator und Wert **[Agent-Version][ist]** aus, und geben Sie die Version ein, z. B. **6.26.14003.0**.
7. Wählen Sie den Operator UND rechts neben dem Feld Entität mit CrowdStrike Gerätedetails als Wert für eine andere Bedingung aus.
8. Wählen Sie **Mit CMDB-Metadaten** für das Feld Verbindung aus.
   Das Feld Entität ist mit CMDB-Metadaten gefüllt.
9. Wählen Sie **Eigenschaft** für das Feld Kriterien aus.
10. Wählen Sie für Eigenschaft, Operator und Wert **[BS][enthält],** und geben Sie **Windows-Server**ein.
11. Wählen Sie **Assets anzeigen**aus.
    Nach einigen Minuten werden auf der Registerkarte Übereinstimmende Assets Ergebnisse angezeigt. Wenn Sie keine Übereinstimmungen sehen, können Sie Ihre Suche einschränken. Wenn Sie zufrieden sind, dass Sie die Bedingungen richtig festgelegt haben, können Sie die Suche als Richtlinie speichern und aktivieren. Wie andere Richtlinien durchsucht sie Ihre Assets kontinuierlich mit einem Hintergrundauftrag, nachdem Sie sie aktiviert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachung von Risikominderungssteuerungen mit Sicherheitsstatus-Überwachung

Im Arbeitsbereich Sicherheitsstatus-Überwachung (SSÜ) erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Steuerungen zur Risikominderung gemindert werden, je nach Konfiguration verschiedener Sicherheitstools.

Überwachung von Steuerungen zur Risikominderung

Die Anwendung Sicherheitsstatus-Überwachung konzentriert sich auf drei Kernproblembereiche:

- Asset-Bestand: Identifiziert alle Ihre Unternehmens-Assets, einschließlich nicht verwalteter oder unbekannter Assets.
- Abdeckung und Integrität von Sicherheitskontrollen – Identifizieren von Abdeckungslücken mit Ihren Sicherheitskontrollen
- Transparenz der Bedrohungsminderung: Identifiziert, welche Bedrohungen für Ihre Assets durch anwendbare Minderungssteuerungen gemindert werden.

Die Überwachung von Ausgleichssteuerungen beschreibt die Funktionen in Sicherheitsstatus-Überwachung, die unter die Transparenz der Bedrohungsminderung fallen. In diesem Zusammenhang listet MITRE-ATT&CK™ eine Reihe von verfügbaren Minderungen auf, die für verschiedene Techniken verwendet werden können. Einige Beispiele:

1. Webanwendungs-Firewall als Risikominderung für die Technik Initial **Anfänglicher Zugriff** > **Öffentlich zugängliche Anwendung Exploit**.
2. Exploit-Schutz als Risikominderung für Techniken wie **Ausführung** > **Schwachstelle für Client-Ausführung**.
3. Multifaktor-Authentifizierung als Risikominderung für die Technik **Berechtigungsausweitung** > **Account-Manipulation**.

Erforderliche Rollen:

- admin: Installiert Anwendungen aus dem ServiceNow® Store und aktiviert Plugins (ITOM Discovery).
- SSÜ Administratorgruppe und SSÜ Analystengruppe: Anwender in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt und den Arbeitsbereich.
- SSÜ Schreibgeschützte Analystengruppe: Anwender in dieser Gruppe haben vollständigen Lesezugriff auf alle Datensätze für das Produkt.

Mitigationssteuerungen, die Benutzer und Leistungen überwachen

Anwender

Anwender	Beschreibung
Cybersicherheitsteams, Sicherheitsanalysten und Manager	• Verschaffen Sie sich einen Überblick über alle Ihre Unternehmens-Assets, einschließlich nicht verwalteter oder unbekannter Assets. • Identifizieren Sie Abdeckungslücken bei Ihren Sicherheitskontrollen, toxische Kombinationen von Problemen wie kritische Schwachstellen und Internet-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung
	Gefahrenpotenzial für Ihre Assets sowie Abweichungen von Ihren internen Sicherheitsstandards. • Erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch Minderungskontrollen gemindert werden, die auf der Konfiguration der Sicherheitstools basieren.

Sicherheitsstatus-Überwachung und den Workflow zur Überwachung von Ausgleichssteuerungen

Sicherheitsstatus-Überwachung nutzt API-Integrationen mit Sicherheitstools wie Webanwendungs-Firewalls und Endpunktschutz-Tools, um zusätzliche Konfigurationsdaten zu Ihren Assets zu importieren und sie zu analysieren, um die entsprechenden Steuerungen zur Risikominderung für ein bestimmtes Asset zu identifizieren. Diese API-Integrationen sind getrennt von den von SSÜ unterstützten Service Graph Connector-Integrationen und importieren andere Daten. Sie konfigurieren diese API-Integrationen im -Arbeitsbereich SSÜ.

Service Graph Connector-Integrationen oder ITOM Discovery sind für die Überwachung von Ausgleichssteuerungen weiterhin erforderlich. Beispielsweise müssen sowohl der Service Graph Connector CrowdStrike als auch die von CrowdStrike unterstützte API-Integration SSÜ aktiviert werden, um zusätzliche Einblicke darüber zu importieren, welche Steuerungen zur Risikominderung durch die Endpunktschutzkonfiguration CrowdStrike aktiviert werden.

Steuerungen und Richtlinien zur Risikominderung in Sicherheitsstatus-Überwachung

Das Produkt Sicherheitsstatus-Überwachung enthält Richtlinien und Steuerungen zur Risikominderung, die Steuerungen zur Risikominderung für Ihre Enterprise-Assets erkennen können. Sie zeigen diese Richtlinien und Steuerungen im Arbeitsbereich Sicherheitsstatus-Überwachung an.

Richtlinien für ausgleichende Steuerungen

Die Anwendungen Sicherheitsstatus-Überwachung und Ausgleichssteuerungen sind erforderlich, um die Ausgleichssteuerungen und Richtlinien für Ausgleichssteuerungen in SSÜanzuzeigen. Beide Anwendungen sind im ServiceNow Store verfügbar.

Weitere Informationen zum Herunterladen und Installieren von Anwendungen aus ServiceNow® Storefinden Sie in den folgenden Themen.

- Laden Sie eine Anwendung zum ersten Mal von ServiceNow Store herunter
- Installieren Sie eine Security Operations -Integration

Um die Richtlinien für ausgleichende Steuerungen anzuzeigen, können Benutzer in der SPC-Administratorgruppe und in der SPC-Analystengruppe zu navigieren **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Alle** im Navigationsbereich des SSÜ -Arbeitsbereichs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Richtlinien für ausgleichende Steuerungen sind in der Anwendung enthalten und werden zusammen mit den anderen SSÜ -Richtlinien angezeigt:

- SEH-Überschreibung
- Häufchen-Spray
- CrowdStrike NULL-Seitenzuteilung
- CrowdStrike DEP erzwingen
- CrowdStrike ASLR erzwingen
- MicrosoftMicrosoft Azure Event Hubs Flow-Schutz für Defender-Steuerung
- MicrosoftMicrosoft Azure Event Hubs Defender Force ASLR
- MicrosoftMicrosoft Azure Event Hubs Obligatorische ASLR für Defender und ASLR von unten nach oben
- SentinelOne-Anwendungssteuerung
- SentinelOne-Datendateien
- Ausführbare SentinelOne-Dateien
- SentinelOne-Exploits
- SentinelOne-IDR
- SentinelOne – Interaktive Bedrohung erkennen
- SentinelOne erkennt seitliche Bewegung
- Statische SentinelOne-KI
- Statische SentinelOne-KI: verdächtig
- Potenziell unerwünschte SentinelOne-Anwendungen
- SentinelOne-Remote-Shell
- SentinelOne-Reputation

Ausgleichssteuerungen im -Arbeitsbereich anzeigen

Um die Liste der Verringerungssteuerungen anzuzeigen, können die SPC-Administratorgruppe und die SPC-Analystengruppe zu navigieren **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Steuerungen für Ausgleichsmaßnahmen** im Navigationsbereich des SSÜ -Arbeitsbereichs.

Die Liste der unterstützten Minderungssteuerungen enthält verschiedene Arten von Minderungen, die von SSÜ für Ihre Assets erkannt werden können. Wählen Sie einen Datensatz aus. Jede Verringerungssteuerung enthält die folgenden Informationen:

- Name: Name der Ausgleichssteuerung.
- Quellen: Quellen, die zum Importieren des Status dieser Verringerungssteuerung für ein bestimmtes Asset verwendet werden. Unterstützte Quellen für diese Integration sind die API-basierten Integrationen mit den Sicherheitstools CrowdStrike, MicrosoftMicrosoft Azure Event Hubs SCCM, SentinelOne und F5 BIG-IP.
- Kategorie: Kategorie der Verringerungssteuerung, z. B. Exploit Protection (EDR).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MITRE™ Techniken: MITRE-Techniken, für die diese Minderungssteuerung gilt.
- Richtlinien: SSÜ Im Produkt enthaltene Richtlinien, die verwendet werden, um das Vorhandensein dieser Minderungssteuerung zu identifizieren. Eine Ausgleichssteuerung erfordert möglicherweise mehr als eine Richtlinie.

Einige Verringerungssteuerungen erfordern eine Auswertung mit mehreren Richtlinien, während andere möglicherweise nur eine Richtlinie erfordern. Außerdem müssen für bestimmte Minderungssteuerungen alle Richtlinien übereinstimmen, für andere Steuerungen ist jedoch nur eine Richtlinie erforderlich, um zu bestimmen, ob der Status einer Minderungssteuerung für ein bestimmtes Asset aktiv ist.

Kategorien von Verringerungssteuerungen

Die folgenden Kategorien von Ausgleichssteuerungen werden derzeit mit SSÜunterstützt.

- Für Exploit Protection (EDR) erforderliche Steuerungen und Richtlinien zur Risikominderung.
- Für Exploit Protection (WAF) erforderliche Minderungssteuerungen und -richtlinien.

Für Exploit Protection (EDR) erforderliche Steuerungen und Richtlinien zur Risikominderung

Die Ausgleichssteuerungen und -richtlinien, die für die Überwachung von Exploit Protection Endpoint Detection and Response (EDR) erforderlich sind, sind im Produkt Sicherheitsstatus-Überwachung enthalten.

Exploit-Schutz (EDR)

Erforderliche Rolle: SSÜ Administratorgruppe und SSÜ Analystengruppe.

Diese Kategorie von Verringerungssteuerungen deckt Verringerungen ab, die für Ihre Assets in Form der Konfiguration des Endpunktschutz-Agents verfügbar sind. Dies gilt für Endpunktschutz-Agents wie CrowdStrike und MicrosoftMicrosoft Azure Event Hubs SCCM sowie die MicrosoftMicrosoft Azure Event Hubs Defender Mitigation Control Integration und SentineOne.

Einstellungen für die Exploit-Minderung wie „Randomization des Adressbereich-Layouts erzwingen“ und „DEP erzwingen“ können in Endpunktschutz-Tools wie CrowdStrikeaktiviert werden. SSÜ erkennt diese Konfiguration auf Geräten automatisch mithilfe der in der Anwendung enthaltenen Richtlinien und der API-Integration mit Endpunktschutz-Tools.

Voraussetzungen für die Erkennung von Exploit Protection (EDR) mit CrowdStrike

1. Vergewissern Sie sich, dass CrowdStrike Service Graph Connector aktiviert ist. Diese Anwendung ist im ServiceNow Store verfügbar. Die Installations- und Konfigurationsinformationen sind in der App-Liste enthalten. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die CrowdStrike -Integrationen für die Überwachung der Verringerungssteuerung.
2. Vergewissern Sie sich, dass die CrowdStrike -API-Integration im Sicherheitsstatus-Überwachung -Arbeitsbereich aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Steuerungen und Richtlinien zur Risikominderung in Exploit Protection (EDR) CrowdStrike

- CrowdStrike Exploit-Minderung – ASLR erzwingen
  - Quellen: CrowdStrike APIs
  - MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Berechtigungszugriff, Umgehung der Verteidigung, Eskalation von Berechtigungen, Seitliche Bewegung
  - MITRE Techniken, die von dieser Verringerung behandelt werden: Drive-by-Kompromittierung (Erstzugriff), Exploitation für Client-Ausführung (Ausführung), Schwachstelle für den Zugriff auf Anmeldeinformationen (Zugriff auf Anmeldeinformationen), Schwachstelle für die Umgehung der Verteidigung (Umgehung der Verteidigung), Ausnutzung der Eskalation der Berechtigung (Umgehung der Verteidigung), Schwachstelle bei Remote-Services (Lateral Mobility)
  - Richtlinien: Die Richtlinie CrowdStrike Force ASLR muss aktiviert sein, um diese Steuerung zur Risikoverringerung zu identifizieren. Sie können optional andere Richtlinien zur Minderungssteuerung aktivieren.
- CrowdStrike Exploit-Verringerung – DEP erzwingen
  - Quellen: CrowdStrike APIs
  - MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Berechtigungszugriff, Umgehung der Verteidigung, Eskalation von Berechtigungen, Seitliche Bewegung
  - MITRE Techniken, die von dieser Verringerung behandelt werden: Drive-by-Kompromittierung (Erstzugriff), Exploitation für Client-Ausführung (Ausführung), Schwachstelle für den Zugriff auf Anmeldeinformationen (Zugriff auf Anmeldeinformationen), Schwachstelle für die Umgehung der Verteidigung (Umgehung der Verteidigung), Ausnutzung der Eskalation der Berechtigung (Umgehung der Verteidigung), Schwachstelle bei Remote-Services (Lateral Mobility)
  - Richtlinien: Die Richtlinie CrowdStrike Force DEP muss aktiviert sein, um diese Steuerung zur Risikominderung zu identifizieren. Sie können optional andere Richtlinien zur Minderungssteuerung aktivieren.
- CrowdStrike Exploit-Verringerung – Heap-Spray-Vorzuteilung
  - Quellen: CrowdStrike APIs
  - MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Berechtigungszugriff, Umgehung der Verteidigung, Eskalation von Berechtigungen, Seitliche Bewegung
  - MITRE Techniken, die von dieser Verringerung behandelt werden: Drive-by-Kompromittierung (Erstzugriff), Exploitation für Client-Ausführung (Ausführung), Schwachstelle für den Zugriff auf Anmeldeinformationen (Zugriff auf Anmeldeinformationen), Schwachstelle für die Umgehung der Verteidigung (Umgehung der Verteidigung), Ausnutzung der Eskalation der Berechtigung (Umgehung der Verteidigung), Schwachstelle bei Remote-Services (Lateral Mobility)
  - Richtlinien: Die Richtlinie „Heap-Spray-Vorzuordnung“ muss aktiviert sein, um diese Steuerung zur Risikominderung zu identifizieren. Sie können optional andere Richtlinien zur Minderungssteuerung aktivieren.
- CrowdStrike Exploit-Verringerung – NULL-Seitenzuteilung
  - Quellen: CrowdStrike APIs
  - MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Berechtigungszugriff, Umgehung der Verteidigung, Eskalation von Berechtigungen, Seitliche Bewegung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MITRE Techniken, die von dieser Verringerung behandelt werden: Drive-by-Kompromittierung (Erstzugriff), Exploitation für Client-Ausführung (Ausführung), Schwachstelle für den Zugriff auf Anmeldeinformationen (Zugriff auf Anmeldeinformationen), Schwachstelle für die Umgehung der Verteidigung (Umgehung der Verteidigung), Ausnutzung der Eskalation der Berechtigung (Umgehung der Verteidigung), Schwachstelle bei Remote-Services (Lateral Mobility)
- Richtlinien: Die Richtlinie CrowdStrike „ NULL-Seitenzuteilung“ muss aktiviert sein, um diese Steuerung zur Risikoverringerung zu identifizieren. Sie können optional andere Richtlinien zur Minderungssteuerung aktivieren.

- CrowdStrike Exploit-Minderung – SEH-Überschreibung
  - Quellen: CrowdStrike APIs
  - MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Berechtigungszugriff, Umgehung der Verteidigung, Eskalation von Berechtigungen, Seitliche Bewegung
  - MITRE Techniken, die von dieser Verringerung behandelt werden: Drive-by-Kompromittierung (Erstzugriff), Exploitation für Client-Ausführung (Ausführung), Schwachstelle für den Zugriff auf Anmeldeinformationen (Zugriff auf Anmeldeinformationen), Schwachstelle für die Umgehung der Verteidigung (Umgehung der Verteidigung), Ausnutzung der Eskalation der Berechtigung (Umgehung der Verteidigung), Schwachstelle bei Remote-Services (Lateral Mobility)
  - Richtlinien: Mindestens die Richtlinie „CrowdStrike SEH Overwrite Protection“ muss aktiviert sein, um diese Steuerung zur Risikominderung zu identifizieren. Sie können optional andere Richtlinien zur Minderungssteuerung aktivieren.
- CrowdStrike Exploit-Verringerung – Alle Einstellungen Ein
  - Quellen: CrowdStrike APIs
  - MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Berechtigungszugriff, Umgehung der Verteidigung, Eskalation von Berechtigungen, Seitliche Bewegung
  - MITRE Techniken, die von dieser Verringerung behandelt werden: Drive-by-Kompromittierung (Erstzugriff), Exploitation für Client-Ausführung (Ausführung), Schwachstelle für den Zugriff auf Anmeldeinformationen (Zugriff auf Anmeldeinformationen), Schwachstelle für die Umgehung der Verteidigung (Umgehung der Verteidigung), Ausnutzung der Eskalation der Berechtigung (Umgehung der Verteidigung), Schwachstelle bei Remote-Services (Lateral Mobility)
  - Richtlinien: Alle folgenden Richtlinien müssen aktiviert sein, um diese Minderungssteuerung zu identifizieren: CrowdStrike Force ASLR, CrowdStrike Force DEP, Heap-Spray Pre-allocation, CrowdStrike NULL Page Allocation, and CrowdStrike SEH Overwrite Protection.

Voraussetzungen für die Erkennung von Exploit Protection (EDR) mit MicrosoftMicrosoft Azure Event Hubs SCCM und der MicrosoftMicrosoft Azure Event Hubs Integration für die Steuerungsminderungssteuerung von Defender

MicrosoftMicrosoft Azure Event Hubs SCCM-Anmeldeinformationen, die die Rolle „Skriptautoren“ enthalten. Die Rolle „Skriptautoren“ bietet die erforderlichen Berechtigungen zum Erstellen eines Skripts, das zum Importieren von Risikominderungsinformationen auf dem SCCM-Server erforderlich ist.

Weitere Informationen finden Sie unter Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Steuerungen und Richtlinien zur Risikominderung in Exploit Protection (EDR) mit Microsoft SCCM und der Integration der Microsoft Defender Mitigation Control:

- Defender – Exploit-Mitigation – CFG

  MicrosoftMicrosoft Azure Event Hubs Flow-Schutz für Defender-Steuerung.

- Defender – Exploit Mitigation – DEP

  MicrosoftMicrosoft Azure Event Hubs Verhinderung der Datenausführung mit Defender.

- Defender – Exploit-Verringerung – Obligatorische ASLR und Bottom-Up-ASLR

  MicrosoftMicrosoft Azure Event Hubs Defender Force ASLR.

- MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Berechtigungszugriff, Umgehung der Verteidigung, Eskalation von Berechtigungen, Seitliche Bewegung.
- MITRE Techniken, die von dieser Verringerung behandelt werden: Drive-by-Kompromittierung (Erstzugriff), Exploitation für Client-Ausführung (Ausführung), Schwachstelle für den Zugriff auf Anmeldeinformationen (Zugriff auf Anmeldeinformationen), Schwachstelle für die Umgehung der Verteidigung (Umgehung der Verteidigung), Ausnutzung der Eskalation der Berechtigung (Umgehung der Verteidigung), Ausnutzung von Remote-Services (Lateral Bewegung).

Voraussetzungen für die Erkennung von Exploit Protection (EDR) mit der SentinelOne Integration für die Verringerungssteuerung

1. Vergewissern Sie sich, dass SentinelOne Service Graph Connector aktiviert ist.

   Diese Anwendung ist im ServiceNow Store verfügbar. Die Installations- und Konfigurationsinformationen sind in der App-Liste enthalten. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie Service Graph Connector für SentinelOne und die SentinelOne-Integration für die Verringerungssteuerung.

2. Stellen Sie sicher, dass die SentinelOne-API-Integration im Arbeitsbereich für die Kontrolle des Sicherheitsstatus aktiviert ist.
3. Überprüfen Sie die in der Anwendung enthaltenen Richtlinien für SentinelOne-Minderungssteuerungen:
   - SentinelOne-Anwendungssteuerung
   - SentinelOne-Datendateien
   - Ausführbare SentinelOne-Dateien
   - SentinelOne-Exploits
   - SentinelOne-IDR
   - SentinelOne – Interaktive Bedrohung erkennen
   - SentinelOne erkennt seitliche Bewegung
   - Statische SentinelOne-KI
   - Statische SentinelOne-KI: verdächtig
   - Potenziell unerwünschte SentinelOne-Anwendungen
   - SentinelOne-Remote-Shell
   - SentinelOne-Reputation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie die CrowdStrike -Integrationen für die Überwachung der Verringerungssteuerung

CrowdStrike Service Graph Connector und API-Integrationen erfordern separate Konfigurationsschritte. Sie konfigurieren den CrowdStrike Service Graph Connector für den Import von Asset-Details. Konfigurieren Sie die CrowdStrike API-Integration für das Sammeln von Risikominderungsdaten zu den Assets, die von CrowdStrikeüberwacht werden.

Vorbereitungen

- Vergewissern Sie sich, dass Sie die Anwendungen zur Überwachung des Sicherheitsstatus und zur Überwachung der Verringerungssteuerungen in Ihrer Instanz installiert und aktiviert haben. Diese Anwendungen sind im ServiceNow Store verfügbar.
- Der CrowdStrike Service Graph Connector muss installiert und konfiguriert werden, bevor Sie die CrowdStrike API-Integration konfigurieren.

Erforderliche Rolle: „admin“ für die Installation von Plugins sowie „SPC-Administratorgruppe“ und „SPC-Analystengruppe“ für die Konfiguration von Integrationen im -Arbeitsbereich.

Prozedur

1. Gehen Sie folgendermaßen vor, um die CrowdStrike Service Graph Connector-Integration zu installieren und zu konfigurieren:

   Hinweis:
   Wenn Sie Service Graph Connector für CrowdStrikeinstalliert haben, fahren Sie mit Schritt 2 fort, um die CrowdStrike API-Integration zu konfigurieren.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“.**.

   b. Suchen Sie den Service Graph Connector für Endpunktschutz CrowdStrike.

   c. Wählen Sie den Link aus, der Sie zur App-Liste für den Service Graph Connector für CrowdStrike in ServiceNow® Storeführt.

   d. Befolgen Sie die Eingabeaufforderungen, um die Anwendung zu installieren.

   e. Laden Sie den Installationsleitfaden aus dem Abschnitt „Links und Dokumente zur Unterstützung“ in der App-Liste herunter, bevor Sie den Vorgang beenden, um bei der Konfiguration und Aktivierung zu helfen.

   f. Navigieren zu **CrowdStrike** > **Setup** in Ihrer Instanz.

   g. Befolgen Sie die Eingabeaufforderungen im geführten Setup, und lesen Sie die Dokumentation, um SGC zu konfigurieren und zu aktivieren.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**.

   Auf dieser Registerkarte werden die Quellen für die Verringerungssteuerungen (CrowdStrike, F5 BIG IP und SCCM) aufgelistet. Die Registerkarte wird nur im Arbeitsbereich angezeigt, wenn Sie die Anwendung „Überwachung der Verringerungssteuerungen“ installiert haben.

   Auf den Quellkarten können Sie den Status der Ausgleichsquelle (Aktiv oder Inaktiv) und die Anzahl der Ausgleichssteuerungen und der zugehörigen Richtlinien anzeigen, die von CrowdStrike (6) überwacht werden. Sie können die Nummer auswählen, um die Liste anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie die Spalte Aktiv in den Anzeigen Quellen, Aktiv. Dies zeigt an, dass die Quelle (CrowdStrike SGC) aktiv ist, Sie müssen jedoch die API-Integration CrowdStrike konfigurieren, bevor Sie Steuerungen zur Risikominderung überwachen können.

3. Wählen Sie **Weiter**.
4. Wählen Sie CrowdStrike in der Spalte Name aus.
5. Wählen Sie Bearbeiten aus, und füllen Sie die Felder aus.

Hinweis:
Geben Sie die gleichen CrowdStrike -Account-Informationen und Serverdetails für die API-Integration ein, die Sie für den CrowdStrike Service Graph Connector angegeben haben. Diese Informationen stellen sicher, dass Sie Verringerungsdaten importieren, die mit den Asset-Daten übereinstimmen, die Sie mit dem Service Graph Connector importiert haben.

Feld	Beschreibung
Name	Name der Instanz. Sie können diesen Namen ändern, um die Anmeldeinformationen zu speichern, ohne sie zu testen. Wenn Sie Felder unter dem Feld Name ändern, müssen Sie die Verbindung vor dem Speichern und Beenden testen.
Asset-Größenbeschränkung	Anzahl der überwachten Assets.
Client-ID	CrowdStrike – ID
Geheimer Clientschlüssel	CrowdStrike Geheimnis
API-URL	API-URL, z. B. https://api.rowdStrike.com

6. Wenn Sie bereit sind, wählen Sie **Verbindung testen**aus.
Bei erfolgreicher Verbindung wird eine Meldung angezeigt.
7. Wählen Sie **Speichern und beenden**.
8. Wählen Sie auf der Karte CrowdStrike auf der Registerkarte SPC-API-Integrationen **die Option Details anzeigen** aus. Beachten Sie, dass die Quelle und die API aktiviert sind und der Fortschrittsbalken für die Konfiguration abgeschlossen ist.
9. **Wahlweise:** Wenn der Test der Anmeldeinformationen nicht erfolgreich ist, können Sie **Zu vorherigen Anmeldeinformationen zurückkehren** auswählen, um zuvor validierte Anmeldeinformationen einzufügen.
10. Befolgen Sie diese Schritte, um die CrowdStrike -Integrationen auszuführen.

    a. Navigieren zu **CrowdStrike-Minderungssteuerung** > **Integrationen**.
    Es gibt drei Integrationen:

    - CrowdStrike Integration von Präventionsrichtlinien
    - CrowdStrike Integration von Gerätesteuerungsrichtlinien
    - CrowdStrike Asset Insight-Integration

    Die Integrationen sind verkettet und werden in einer bestimmten Reihenfolge ausgeführt. Der erfolgreiche Abschluss einer Integration initiiert die nächste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie in der Spalte „Name“ die Option CrowdStrike Integrationsrichtlinie aus, um die Integrationsausführungen zu initiieren.

c. Aktivieren Sie im Datensatz das Kontrollkästchen **Aktiv**, und wählen Sie **Jetzt ausführen**aus.

Sie können den Status der Integrationsausführung auf der Registerkarte Integrationsausführung in den Integrationsdatensätzen anzeigen.

Die Integration ist so geplant, dass sie standardmäßig täglich ausgeführt wird.

Die CrowdStrike Asset Insight Integration importiert nur Informationen zu Assets, die sich seit der letzten Integrationsausführung geändert haben. Die CrowdStrike Device Control Policy Integration und die CrowdStrike Prevention Policy Integration importieren alle Daten für jede Ausführung.

Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integration

Service Graph Connector for SCCM und die Microsoft Defender Mitigation Control Integration erfordern separate Konfigurationsschritte. Sie installieren und konfigurieren Service Graph Connector for SCCM, um Asset-Details zu importieren. Sie konfigurieren die Integration der Microsoft Defender-Minderungssteuerung, um Minderungsdaten für die Assets zu sammeln, die von Service Graph Connector for SCCM überwacht werden.

Vorbereitungen

Erforderliche Rollen:

- admin für die Installation und Aktivierung von Plugins
- SPC-Administratorgruppe und SPC-Analystengruppe für die Konfiguration von Integrationen im Arbeitsbereich
- Microsoft-SCCM-Anmeldeinformationen, die die Rolle „Skriptautoren“ enthalten. Die Rolle „Skriptautoren“ bietet die erforderlichen Berechtigungen zum Erstellen eines Skripts, das zum Importieren von Risikominderungsinformationen auf dem SCCM-Server erforderlich ist.

Hinweis:
Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Rolle „Skriptautoren“.

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein
Site	Lesen	Ja
SMS-Skripts	Erstellen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Löschen	Ja
SMS-Skripts	Ändern	Ja

- Microsoft-SCCM-Anmeldeinformationen, die die Rolle „Skriptgenehmiger“ enthalten. Das zum Importieren von Risikominderungsinformationen erstellte Skript muss in Ihrer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft-SCCM-Konsole durch einen Benutzer mit der Rolle „Skriptgenehmiger“ genehmigt werden.

Hinweis:
Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Skriptgenehmiger

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein
Site	Lesen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Genehmigen	Ja
SMS-Skripts	Ändern	Ja

Prozedur

1. Um die Integration von Service Graph Connector für Microsoft SCCM zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

   Hinweis:
   Wenn Sie die Integration von Service Graph Connector für Microsoft SCCM installiert haben, fahren Sie mit Schritt 2 fort, um die Integration von Microsoft Defender Mitigation Control zu konfigurieren.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“.**.
   b. Suchen Sie die Integration von Service Graph Connector für Microsoft SCCM.
   c. Wählen Sie den Link aus, der Sie zur App-Liste für die Anwendung in ServiceNow® Storeführt.
   d. Befolgen Sie die Eingabeaufforderungen, um die Anwendung zu installieren.
   e. Laden Sie den Installationsleitfaden aus dem Abschnitt „Links und Dokumente zur Unterstützung“ in der App-Liste herunter, bevor Sie den Vorgang beenden, um bei der Konfiguration und Aktivierung zu helfen.
   f. Navigieren zu **Setup** in Ihrer Instanz.
   g. Befolgen Sie die Eingabeaufforderungen im geführten Setup, und lesen Sie die Dokumentation, um SGC zu konfigurieren und zu aktivieren.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen** um die Microsoft Defender Integration für die Steuerung der Risikominderung zu konfigurieren.

   Auf dieser Registerkarte werden die Quellen für die Verringerungssteuerungen (CrowdStrike, F5 BIG IP und Defender) aufgelistet. Sie wird nur im -Arbeitsbereich angezeigt, wenn Sie die Anwendung „Überwachung der Steuerungen zur Verringerung“ installiert haben.

   Auf den Quellkarten können Sie den Status der Verringerungsquelle (Aktiv oder Inaktiv) anzeigen.

   Beachten Sie die Spalte Aktiv in den Anzeigen Quellen, Aktiv. Dies zeigt an, dass die Quelle (Service Graph Connector für Microsoft SCCM) zum Abrufen von Asset-Daten aktiv ist. Sie müssen jedoch die Microsoft Defender Mitigation Control-Integration konfigurieren, bevor Sie Risikominderungssteuerungen überwachen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Weiter**.
   Die Seite „SCCM-Konfiguration“ wird mit einem Link zur Microsoft SCCM-Verringerungssteuerungsinstanz angezeigt.
4. Wählen Sie den Instanzlink aus, der in der Spalte Name angegeben ist.
5. Füllen Sie die Felder für das Modal zur Konfiguration der SCCM-Anmeldeinformationen für Microsoft SCCM Integration Control aus.

Feld	Beschreibung
Name	Das Feld wird automatisch mit dem Instanznamen ausgefüllt.
Verbindung	Feld wird automatisch mit Verbindungsinformationen ausgefüllt.
Host	Hostname für den SCCM-Server innerhalb der Verbindungsinformationen im vorherigen Feld.
Anwendername	Anwendername für den Zugriff auf den SCCM-Server.
Passwort	Passwort für den Zugriff auf den SCCM-Server.
MID-Server	Wählen Sie einen von ServiceNow verwalteten MID-Server aus der Liste aus.
Validierungsstatus	Feld nach Validierungsversuch ausgefüllt. Wenn die Verbindung erfolgreich ist, lautet der Status der Integrationsinstanz **Gültig**.
SG-Connector-Verbindung	Wählen Sie eine Option für Aliasse für Verbindungen und Anmeldeinformationen aus der Liste für Service Graph Connector für Microsoft SCCM aus. Sie richten diese Verbindung während der Schritte des geführten Setups für Microsoft SCCM SGC ein.
Validierungsdetail	Details zum Validierungsversuch.

6. Wählen Sie **Anmeldeinformationen speichern und testen aus**.
   Eine gültige Antwort für eine erfolgreiche Verbindung ist erforderlich, um mit dem nächsten Schritt fortzufahren.
7. Wählen Sie **Weiter**.
   Es wird automatisch ein PowerShell-Skript erstellt, um Details zur Risikoverringerung abzurufen. Ein Modal mit der Option zum Validieren der Skriptgenehmigung wird angezeigt.
8. Um das Skript zu genehmigen, melden Sie sich mit der Rolle Skriptgenehmiger bei Ihrer Microsoft SCCM-Konsole an.

   In Ihrem SCCM-Konfigurationsmanager wurde ein PowerShell-Skript generiert, um Details zur Risikominderung abzurufen. Sie müssen sich mit den entsprechenden Anmeldeinformationen und einer Anwenderrolle mit der Berechtigung Skriptgenehmiger anmelden, um das Skript zu genehmigen. Nachdem er genehmigt wurde, können Sie ihn in Ihrer Now Platform-Instanz validieren.

9. Suchen Sie in Ihrer -Konsole nach dem Skript **[Servicenow Secops]: Get System Mitigations (ServiceNow Secops]: Get System Mitigations-Skript)**, und genehmigen Sie es.

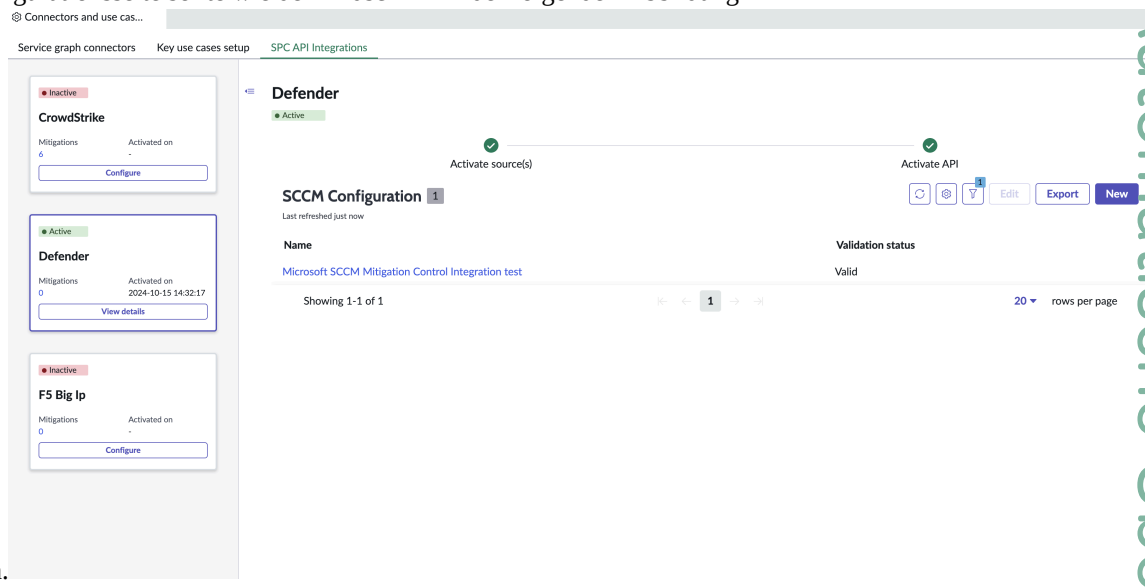
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Im SCCM-Konfigurationsmanager befindet sich der Abschnitt „Skript“ unter der Softwarebibliothek. Suchen Sie nach: [ServiceNow Secops]: Rufen Sie das Skript für Systemminderungen ab, um es zu genehmigen.

Dieses Skript bleibt im Status **Warten auf Genehmigung,** bis Sie es genehmigen.

Sie können das Skript in Ihrer Now Platform-Instanz validieren, ohne es wie oben beschrieben zu genehmigen. Es wird jedoch die Fehlermeldung Skript ist nicht genehmigt angezeigt.

10. Um die Genehmigung zu validieren, kehren Sie zu Ihrer Now Platform-Instanz zurück, und wählen Sie im modalen Fenster PowerShell-Skript genehmigen **die Option Skriptgenehmigung validieren aus**.
11. Wählen Sie **Fertig**.
    Die Konfigurationsseite sollte wie der Bildschirm in der folgenden Abbildung aussehen.



Erstellen Sie mehrere Instanzen für die Microsoft Defender Mitigation Control Integration

Sie können mehrere Instanzen für die Integration der Microsoft Defender-Minderungssteuerungen konfigurieren.

Vorbereitungen

Erforderliche Rollen:

- SPC-Administratorgruppe und SPC-Analystengruppe für die Konfiguration neuer Integrationsinstanzen im Arbeitsbereich
- Microsoft-SCCM-Anmeldeinformationen, die die Rolle „Skriptautoren“ enthalten. Die Rolle „Skriptautoren“ bietet die erforderlichen Berechtigungen zum Erstellen eines Skripts, das zum Importieren von Risikominderungsinformationen auf dem SCCM-Server erforderlich ist.

Hinweis:
Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Rolle „Skriptautoren“.

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Berechtigung	Status
Site	Lesen	Ja
SMS-Skripts	Erstellen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Löschen	Ja
SMS-Skripts	Ändern	Ja

- Microsoft-SCCM-Anmeldeinformationen, die die Rolle „Skriptgenehmiger“ enthalten. Das zum Importieren von Risikominderungsinformationen erstellte Skript muss in Ihrer Microsoft-SCCM-Konsole durch einen Benutzer mit der Rolle „Skriptgenehmiger“ genehmigt werden.

Hinweis:
Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Skriptgenehmiger

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein
Site	Lesen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Genehmigen	Ja
SMS-Skripts	Ändern	Ja

Prozedur

1. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**.
2. Wählen Sie **Neu**.
   Das Modal „Neue Defender-Instanz“ wird angezeigt.
3. Geben Sie einen Namen für Ihre neue Instanz ein, und wählen Sie **Instanz erstellen aus**.
   Die Seite „SPC-API-Integrationen“ wird mit der mit der Anwendung bereitgestellten Instanz und Ihrer neuen Instanz angezeigt.
4. Wählen Sie den Link für Ihre neue Instanz.
5. Füllen Sie die Felder im Dialogfeld für die Konfiguration der SCCM-Anmeldeinformationen für Ihre neue Instanz aus.

Feld	Beschreibung
Name	Das Feld wird automatisch mit dem Instanznamen ausgefüllt.
Verbindung	Erstellen Sie eine neue Verbindung. **a.** Wählen Sie **Verbindung und Alias erstellen** oben im Modal aus. **b.** Füllen Sie im Formular „Aliasse für Verbindungen und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Anmeldeinformationen“ die Pflichtfelder aus. ▪ **Name** : Eindeutiger Name ▪ **Typ** : Verbindung und Anmeldeinformationen ▪ **Verbindungstyp** : Standard **Hinweis:** Wählen Sie zu diesem Zeitpunkt nicht **Absenden** aus. **c.** Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle des grauen Headers, und wählen Sie **Speichern**aus. Die Seite wird aktualisiert. Zugehörige Links und Registerkarten werden nach dem Speichern unten auf der Seite angezeigt. **d.** Wählen Sie bei ausgewählter Registerkarte Verbindungen die Option **Neu** rechts neben der Registerkarte aus. Das Verbindungsformular wird angezeigt. Füllen Sie die Felder aus. ▪ **Name** : Eindeutiger Name ▪ Anmeldeinformationen: Wählen Sie das Suchsymbol. Suchen Sie die Windows-Anmeldeinformationen, und wählen Sie den Link. Füllen Sie die Felder im Formular „Windows-Anmeldeinformationen“ aus. ▪ **Name** : Eindeutiger Name ▪ Anwendername: Anwendername für die Anmeldeinformationen. Dies ist der Anwendername, auf den für das Feld Anwendername im Dialogfeld für die Konfiguration der SCCM-Anmeldeinformationen verwiesen wird, nachdem Sie es auf dieser Seite gespeichert haben. ▪ Passwort – Passwort für die Anmeldeinformationen. Dies ist das Passwort, das für das Passwortfeld im Dialogfeld für die Konfiguration der SCCM-Anmeldeinformationen referenziert wird, nachdem Sie es auf dieser Seite gespeichert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Host: Dies ist der Host für den SCCM-Server, auf den im Feld „Host“ im Dialogfeld „Konfiguration der SCCM-Anmeldeinformationen“ verwiesen wird, nachdem Sie ihn auf dieser Seite gespeichert haben. **e.** Aktivieren Sie das Kontrollkästchen **MID-Server verwenden**. Wählen Sie Spezifischer MID-Server für **MID-Auswahl** aus, und wählen Sie einen aus der Liste der MID-Server aus. **f.** Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle des grauen Headers, und wählen Sie **Speichern**aus. Dies sind die Anmeldeinformationen, die Sie im Verbindungsformular eingeben (siehe Schritt d).
Host	Dies ist der Host für den SCCM-Server, auf den im Feld Host verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Anwendername	Dies ist der Anwendername, auf den im Feld Anwendername verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Passwort	Dies ist das Passwort, auf das im Feld Passwort verwiesen wird, nachdem Sie es wie oben beschrieben auf der Verbindungsseite gespeichert haben.
MID-Server	Dies ist der MID-Server, auf den von den MID-Server-Feldern verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Validierungsstatus	Feld nach Validierungsversuch ausgefüllt. Wenn die Verbindung erfolgreich ist, lautet der Status der Integrationsinstanz **Gültig**.
SG-Connector-Verbindung	Wählen Sie eine Option für Aliasse für Verbindungen und Anmeldeinformationen aus der Liste für Service Graph Connector für Microsoft SCCM aus. Sie richten diese Verbindung während der Schritte des geführten Setups für Microsoft SCCM SGC ein.
Validierungsdetail	Details zum Validierungsversuch.

6. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**.
7. Wählen Sie den Link für Ihre neue Instanz.
8. Wählen Sie im modalen Fenster „Konfiguration der SCCM-Anmeldeinformationen“ die Verbindung aus der Liste aus, die Sie in Schritt 5 für das Feld Verbindung erstellt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie, dass die unten aufgeführten Felder automatisch basierend auf den Informationen ausgefüllt werden, die Sie für Ihre neue Verbindung eingegeben haben.

Host	Dies ist der Host für den SCCM-Server, auf den im Feld Host verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Anwendername	Dies ist der Anwendername, auf den im Feld Anwendername verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Passwort	Dies ist das Passwort, auf das im Feld Passwort verwiesen wird, nachdem Sie es wie oben beschrieben auf der Verbindungsseite gespeichert haben.
MID-Server	Dies ist der MID-Server, auf den von den MID-Server-Feldern verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Validierungsstatus	Feld nach Validierungsversuch ausgefüllt. Wenn die Verbindung erfolgreich ist, lautet der Status der Integrationsinstanz **Gültig**.
SG-Connector-Verbindung	Wählen Sie eine Aliasse für Verbindungen und Anmeldeinformationen aus der Liste aus.
Validierungsdetail	Details zum Validierungsversuch.

9. Wählen Sie **Anmeldeinformationen speichern und testen aus**.
   Eine gültige Antwort für eine erfolgreiche Verbindung ist erforderlich, um mit dem nächsten Schritt fortzufahren.
10. Wählen Sie **Weiter**.
    Das PowerShell-Skript wird wie in Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integrationbeschrieben erstellt. Führen Sie die Schritte in diesem Thema aus, um die Skripts für Ihre neuen Instanzen zu genehmigen.

Installieren und konfigurieren Sie Service Graph Connector für SentinelOne und die SentinelOne-Integration für die Verringerungssteuerung

Service Graph Connector für SentinelOne und die SentinelOne-Integration für die Integration zur Steuerung der Risikominderung erfordern separate Konfigurationsschritte. Sie installieren und konfigurieren Service Graph Connector für SentinelOne, um Asset-Details zu importieren. Sie konfigurieren die SentinelOne-Integration für die Integration der Steuerung zur Risikominderung, um Daten zur Risikominderung für die von Service Graph Connector für SentinelOneüberwachten Assets zu sammeln.

Vorbereitungen

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- admin für die Installation und Aktivierung von Plugins.
- SPC-Administratorgruppe und SPC-Analystengruppe für die Konfiguration von Integrationen im Arbeitsbereich.
- SentinelOne-Anmeldeinformationen.

Prozedur

1. Um die Service Graph Connector für SentinelOne -Integration zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

   Hinweis:
   Wenn Sie Service Graph Connector für SentinelOne installiert haben, fahren Sie mit Schritt 2 fort, um die SentinelOne-Integration für die Integration der Mitigationssteuerung zu konfigurieren.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“.**.
   b. Suchen Sie die Integration Service Graph Connector für SentinelOne.
   c. Wählen Sie den Link aus, der Sie zur App-Liste für die Anwendung in ServiceNow® Storeführt.
   d. Befolgen Sie die Eingabeaufforderungen, um die Anwendung zu installieren.
   e. Laden Sie den Installationsleitfaden aus dem Abschnitt „Links und Dokumente zur Unterstützung“ in der App-Liste herunter, bevor Sie den Vorgang beenden, um bei der Konfiguration und Aktivierung zu helfen.
   f. Navigieren zu **Setup** in Ihrer Instanz.
   g. Befolgen Sie die Eingabeaufforderungen im geführten Setup, und lesen Sie die Dokumentation, um SGC zu konfigurieren und zu aktivieren.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen** um die SentinelOne-Integration für die Integration der Steuerung zur Risikominderung zu konfigurieren.

   Auf dieser Registerkarte werden die Quellen für Ausgleichssteuerungen aufgelistet: CrowdStrike, F5 Big IP, Defender, SentinelOne. Die Registerkarte wird nur im Arbeitsbereich angezeigt, wenn Sie die Anwendung Überwachung der Steuerungen zur Risikominderung installiert haben.

   Auf den Quellkarten können Sie den Status der Verringerungsquelle (Aktiv oder Inaktiv) anzeigen.

   Beachten Sie die Spalte Aktiv in den Anzeigen Quellen, Aktiv. Dies zeigt an, dass die Quelle, in diesem Fall Service Graph Connector für SentinelOne, zum Abrufen von Asset-Daten aktiv ist. Sie müssen jedoch die SentinelOne-Integration für die Integration der Steuerung zur Risikominderung konfigurieren, bevor Sie die Steuerungen zur Risikominderung für die importierten Assets überwachen können.

3. Wählen Sie **Weiter**.
   Die SentinelOne-Konfigurationsseite wird mit einem Link zur Instanz „SentinelOne-Integration für Verringerungssteuerung“ angezeigt.
4. Wählen Sie den Instanzlink aus, der in der Spalte Name angegeben ist.
5. Füllen Sie die Felder für die SentinelOne-Integration für die Integration der Verringerungssteuerung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Geben Sie die gleichen SentinelOne-Account-Informationen und Serverdetails für die SentinelOne-Integration für die Integration der Mitigationssteuerung ein, die Sie für Service Graph Connector für SentinelOneangegeben haben. Diese Informationen stellen sicher, dass Sie Verringerungsdaten importieren, die mit den Asset-Daten übereinstimmen, die Sie mit dem Service Graph Connector importiert haben.

Wählen Sie das Stiftsymbol aus, wenn Sie die Felder bearbeiten müssen.

Feld	Beschreibung
Instanzname	Das Feld wird automatisch mit dem Instanznamen ausgefüllt.
API-Schlüssel	Feld wird automatisch mit den API-Schlüsselinformationen ausgefüllt.
API-URL	Hostname für den SentinelOne-Server, z. B.: https//usea1-na.sentinelone.net

6. Wählen Sie **Anmeldeinformationen speichern und testen aus**.
   Eine gültige Antwort für eine erfolgreiche Verbindung ist erforderlich, um mit dem nächsten Schritt fortzufahren.
7. Wählen Sie **Speichern und Beenden aus**.
8. Wählen Sie auf der SentinelOne-Karte auf der Registerkarte SPC-API-Integrationen **die Option Details anzeigen** aus.
   Beachten Sie, dass die Quelle und die API aktiviert sind und der Konfigurationsfortschrittsbalken abgeschlossen ist.
9. **Wahlweise:** Wählen Sie **„Zu vorherigen Anmeldeinformationen zurückkehren“** aus, um zuvor validierte Anmeldeinformationen einzufügen.
10. Führen Sie diese Schritte aus, um die SentinelOne-Asset-Importintegration auszuführen.

    a. Navigieren zu **SentinelOne-Verringerungssteuerung** > **Integrationen**.
    Es gibt eine Integration: SGC SentinelOne Asset Import.

    b. Wählen Sie in der Spalte „Name“ die **Option Integration der SentinelOne-Präventionsrichtlinie** aus, um die Integration zu initiieren.

    c. Aktivieren Sie im Datensatz das Kontrollkästchen **Aktiv**, und wählen Sie **Jetzt ausführen**aus.

    Sie können den Status der Integrationsausführung auf der Registerkarte **Integrationsausführung** in den Integrationsdatensätzen anzeigen.

    Die Integration ist so geplant, dass sie standardmäßig täglich ausgeführt wird.

    Die SentinelOne-Asset-Importintegration importiert nur Informationen zu Assets, die sich seit der letzten Integrationsausführung geändert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Exploit Protection (WAF) erforderliche Minderungssteuerungen und -richtlinien

Die für die Überwachung durch die Exploit Protection Web Application Firewall (WAF) erforderlichen Steuerungen und Richtlinien zur Risikominderung sind im SPC-Produkt enthalten.

Exploit-Schutz (WAF)

Diese Kategorie von Ausgleichssteuerungen umfasst Ausgleichsmaßnahmen, die in Form von Web Application Firewalls verfügbar sind. SPC erkennt Server, die hinter der Web Application Firewall (WAF) ausgeführt werden, indem die API-Integration mit WAF-Tools wie F5 BIG-IP (F5) und Netzwerk-Datenverkehrsdaten aus ITOM IP-basierter Discovery verwendet wird, falls erforderlich.

Erforderliche Rolle: SSÜ Administratorgruppe und SSÜ Analystengruppe.

Voraussetzungen für Exploit Protection (WAF) mit F5 BIG-IP

1. Stellen Sie sicher, dass Sie IP-basierte ITOM-Discovery in der Umgebung aktiviert ist, in der F5 BIG-IP F5 WAF und die zugehörigen Anwendungsserver eingerichtet sind.
2. Stellen Sie sicher, dass die API-Integration für F5 BIG-IP F5 im Arbeitsbereich Sicherheitsstatus-Überwachung aktiviert ist.

Steuerungen und Richtlinien zur Risikominderung in Exploit Protection (WAF)

F5 WAF-Schutz:

- Quellen: F5 und ITOM
- MITRE-Taktiken behandelt: Erster Zugriff
- Behandelte MITRE-Techniken: Exploit öffentlich zugänglicher Anwendung
- Richtlinien: Es sind keine Richtlinien erforderlich.

Konfigurieren Sie die F5 BIG-IP -Integrationen für die Überwachung der Verringerungssteuerung

Die Anwendung ITOM IP-basierte Discovery und die F5 BIG-IP API-Integrationen erfordern separate Konfigurationsschritte. Konfigurieren Sie die Anwendung ITOM IP-basierte Discovery, um Asset-Details zu importieren. Konfigurieren Sie die API-Integration F5 BIG-IP, um Risikominderungsdaten zu den Assets zu sammeln, die von ITOM IP-basierter Discovery überwacht werden.

Vorbereitungen

- Die IP-basierte ITOM-Discovery muss in der Umgebung, in der F5 BIG-IP und alle zugehörigen Anwendungsserver eingerichtet sind, ausgeführt werden.
- Für lokale Assets müssen Sie einen MID Server bereitstellen.
- Aktivieren Sie die Quelle (ITOM), um Daten zu den überwachten Assets zu sammeln.
- Aktivieren Sie die API-Integration, um Verringerungsdaten zu den Assets zu sammeln.

Erforderliche Rolle: admin für die Installation von Plugins und das Erstellen von Systemeigenschaften sowie SSÜ Administratorgruppe und SSÜ Analystengruppe für die Konfiguration von Integrationen im -Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um die Integration zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

   Hinweis:
   Wenn Sie ITOM installiert und aktiviert haben, fahren Sie mit Schritt 2 fort, um die F5 BIG-IP (F5)-API-Integration zu konfigurieren.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“.**.

   b. Wählen Sie die Karte F5 BIG-IP.

   c. Wählen Sie den Link **ITOM Plugin** aus, um das ITOM-Plugin zu aktivieren.

   d. Folgen Sie den Aufforderungen.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**.

   Auf dieser Registerkarte werden die Quellen für die Verringerungssteuerungen (CrowdStrike und F5 BIG IP sowie SCCM) aufgelistet. Die Registerkarte wird nur im Arbeitsbereich angezeigt, wenn Sie die Anwendung „Überwachung der Steuerungen zur Verringerung“ installiert haben.

   Auf den Quellkarten können Sie den Status der Verringerungsquelle (Aktiv oder Inaktiv)anzeigen.

3. Wählen Sie **Weiter**.

   Beachten Sie, dass die Quelle (ITOM) aktiv ist, Sie müssen jedoch die API-Integration F5 BIG-IP konfigurieren und aktivieren, bevor Sie Steuerungen zur Risikominderung überwachen können.

4. Wählen Sie F5 BIG-IP in der Spalte Name aus.

5. Wählen Sie Bearbeiten aus, und füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Instanz. Sie können diesen Namen ändern, um die Anmeldeinformationen zu speichern, ohne sie zu testen. Wenn Sie Felder unter dem Feld Name ändern, müssen Sie die Verbindung vor dem Speichern und Beenden testen.
Anwendername	F5 BIG-IP-Anwendername
Passwort	F5 BIG-IP Passwort.
MID-Server	Wählen Sie einen MID-Server aus der Liste aus.
API-URL	API-URL mit Port 8443, z. B. https://bigip.example.com:8443.

6. Wenn Sie bereit sind, wählen Sie **Verbindung testen**aus.
   Bei erfolgreicher Verbindung wird eine Meldung angezeigt.

   Wenn beim Testen der Verbindung während der Konfigurationsschritte der folgende Fehler auftritt, Sitzung enthält keine Zertifikate - Nicht vertrauenswürdig: Sitzung enthält

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

keine Zertifikate - Nicht vertrauenswürdig, legen Sie die folgenden Systemeigenschaften auf falschfest:

- com.glide.communications.httpclient.verify_hostname
- com.glide.communications.httpclient.verify_revoked_certificate

Ein Benutzer mit der Administratorrolle muss diese Systemeigenschaften im globalen Bereich erstellen, wenn sie nicht in der Tabelle „Systemeigenschaft“ [sys_properties] aufgeführt sind. Die Systemeigenschaften lauten Typ, Wahr/Falsch (Boolesch).

7. Wählen Sie **Speichern und beenden**.
8. Beachten Sie auf der Karte F5 BIG-IP auf der Registerkarte SPC-API-Integrationen, dass die Quelle und die API aktiviert sind und der Konfigurations-Fortschrittsbalken abgeschlossen ist.
9. **Wahlweise:** Wenn der Test der Anmeldeinformationen nicht erfolgreich ist, können Sie **Zu vorherigen Anmeldeinformationen zurückkehren** auswählen, um zuvor validierte Anmeldeinformationen einzufügen.
10. Führen Sie die folgenden Schritte aus, um die API-Integrationen auszuführen:

    a. Navigieren zu **F5-Steuerung zur Big IP-Minderung** > **Integrationen**

    Es gibt fünf Integrationen. Die Integrationen sind verkettet und werden in einer bestimmten Reihenfolge ausgeführt. Der erfolgreiche Abschluss einer Integration initiiert die nächste:

    - F5 BIG-IP-Geräteintegration
    - F5 BIG-IP-Richtlinienintegration
    - Signaturintegration für F5 Big IP-Angriff
    - Integration des virtuellen F5 Big IP-Servers
    - Integration von Mitgliedern des großen F5-IP-Pools

    b. Um die Integrationskette zu initiieren, wählen Sie in der Spalte „Name“ die **Option F5 BIG-IP-Geräteintegration** aus.

    c. Aktivieren Sie im Datensatz das Kontrollkästchen **Aktiv**, und wählen Sie **Jetzt ausführen**aus.

    d. Zeigen Sie den Status der Integrationsausführungen auf der Registerkarte Integrationsausführung in den Integrationsdatensätzen an.
    Die Integration ist so geplant, dass sie standardmäßig täglich ausgeführt wird.

Aktivieren Sie Richtlinien für Ausgleichssteuerungen, und zeigen Sie erkannte Ausgleiche an

Sie müssen Richtlinien aktivieren, um anzuzeigen, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen gemindert werden.

Vorbereitungen

Stellen Sie sicher, dass Sie Für Exploit Protection (EDR) erforderliche Steuerungen und Richtlinien zur Risikominderung überprüft und die in Installieren und konfigurieren Sie die CrowdStrike -Integrationen für die Überwachung der Verringerungssteuerung, Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integration und Konfigurieren Sie die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

F5 BIG-IP -Integrationen für die Überwachung der Verringerungssteuerungaufgeführten Anforderungen erfüllt haben.

Erforderliche Rolle: SPC-Administratorgruppe und SPC-Analystengruppe.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Alle**.
2. Aktivieren Sie die folgenden Richtlinien.
   - SEH-Überschreibung
   - Häufchen-Spray
   - CrowdStrike NULL-Seitenzuteilung
   - CrowdStrike DEP erzwingen
   - CrowdStrike ASLR erzwingen
   - MicrosoftMicrosoft Azure Event Hubs Flow-Schutz für Defender-Steuerung
   - MicrosoftMicrosoft Azure Event Hubs Defender Force ASLR
   - MicrosoftMicrosoft Azure Event Hubs Obligatorische ASLR für Defender und ASLR von unten nach oben
3. Führen Sie die folgenden Schritte aus, um Assets mit von der Sicherheitsstatuskontrolle erkannten Minderungen mit dem Widget „Assets mit MITRE-Minderungen“ im Dashboard anzuzeigen.
   a. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Startseite**.
   b. Überprüfen Sie im Abschnitt „Wichtige Einblicke“ das Widget „Assets mit MITRE-Minderungen“.
   c. Wählen Sie im Widget eine Verringerungskategorie, **Exploit Protection (EDR)** oder **Exploit Protection (WAF)**.
   d. Sie können die Liste der Assets mit Verringerungen anzeigen, die in dieser Verringerungskategorie erkannt wurden.
   e. Wählen Sie ein Asset aus.
   f. Wählen Sie die Registerkarte **Ausgleichssteuerungen** aus, um die Details der erkannten Ausgleichssteuerung anzuzeigen.
   g. Wählen Sie die Registerkarte **Verringerte angreifbare Elemente,** um die Liste der angreifbaren Elemente anzuzeigen, die durch diese Steuerung zur Risikoverringerung verringert wurden.

Hinweis:
Damit diese Registerkarte ausgefüllt wird, muss die Anwendung Vulnerability Response installiert und aktiviert sein.

Zuordnung von Ausgleichssteuerungen für angreifbare Elemente

Daten von Ausgleichssteuerungen werden angreifbaren Elementen zugeordnet. Sie können eine Liste der Minderungskontrollen anzeigen, die zum Mindern der Schwachstellen und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugrunde liegenden allgemeinen Schwachstellen und Risiken (Common Vulnerabilities and Exposures, CVEs) verwendet werden, die den angreifbaren Elementen zugeordnet sind.

Nach dem Identifizieren einer bestimmten Verringerungssteuerung für ein Asset identifiziert die Sicherheitsstatus-Überwachung automatisch alle angreifbaren Elemente, die durch diese Steuerung verringert werden. Beispielsweise werden alle angreifbaren Elemente mit CVEs, die Teil von Signaturen in Web Application Firewall-Richtlinien (WAF) sind, als verringerte angreifbare Elemente markiert. Diese Identifizierung kann für Schwachstellenmanagementteams nützlich sein, um sie dabei zu unterstützen, die Risikopunktzahlen für geminderte angreifbare Elemente automatisch zu reduzieren.

Tabelle der Risikominderungssteuerungen für angreifbare Elemente

Die Tabelle „Steuerungen für die Risikominderung für angreifbare Elemente“ [sn_vul_vulnerable_item_mitigation_control] wurde erstellt, um Daten für die Risikominderungssteuerung zu verringerten angreifbaren Elementen (VITs) zuzuordnen. In dieser Tabelle sind verringerte VITs und die erkannten Verringerungskontrollen aufgeführt, die zum Mindern der Schwachstellen und der zugrunde liegenden CVEs verwendet wurden, die den angreifbaren Elementen zugeordnet sind. Die verringerten CVE-Datensätze enthalten Verweise auf die für die Assets verwendete Verringerungssteuerung, z. B. Exploit Protection (EDR).

Beispieldaten sind in der folgenden Tabelle aufgeführt.

Daten zu Risikominderungssteuerungen für angreifbare Elemente

Ausgleichssteuerun ist vorhanden	Effektivität der Verringerungssteue	Erkannter Steuerungstyp für Risikominderung	CVEs gemindert	Angreifbares Element
Ja/Nein	Mittel	Exploit-Schutz (EDR)	CVE-2009-3373	VIT0018323

Öffnen Sie einen Steuerungsdatensatz für die Risikominderung (Erkannter Steuerungstyp für die Risikominderung) in der Tabelle, um Details dazu zu überprüfen, wie ein CVE und die zugehörige CWE-Schwachstelle (Common Weakness Enumeration) durch die einem Asset zugeordnete Steuerung zur Risikominderung gemindert werden. Der Minderungssteuerungsdatensatz enthält Details zu den geminderten CWEs, z. B. wie eine Minderungseinstellung in einer CWE angegebene Schwachstellen behebt.

Risikorechner und Risikorechnerregeln

Informationen zur Risikominderung können beim Einrichten angepasster Risikorechnerregeln zur Neuberechnung der Risikopunktzahlen für VITs verwendet werden, denen bestimmte Arten von Schwachstellen und Risikominderungssteuerungen zugeordnet sind. Für diese Beispielregel, die auf der vorherigen Tabelle basiert, berechnet der Standardrisikorechner eine Risikopunktzahl von 60 für VITs, die über den Steuerungstyp Exploit Protection (EDR) zur Risikominderung für erkannte Assets verfügen. Diese Berechnungspunktzahl ist auf das moderate Risiko zurückzuführen, das mit der Schwachstelle verbunden ist, wenn diese Minderung vorhanden ist.

Beispielregel für eine Risikorechnerregel mit den folgenden Bedingungen:

[Details zur Verringerungssteuerung] [ist nicht] [leer] UND [Details zur Verringerungssteuerung, erkannter Verringerungssteuerungstyp] [ist] [Exploit Protection (EDR)].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Werte:

[Risikopunktzahl][ist][60]

Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.

Anwendungsfälle, Richtlinienbeispiele und unterstützte Service Graph Connectors in Sicherheitsstatus-Überwachung

Anwendungsfälle sind verschiedene Szenarien, die Sie konfigurieren, um bestimmte Arten von Lücken bei der Toolabdeckung zu identifizieren. Jeder Anwendungsfall erfordert eine oder mehrere Richtlinien, um Ihre Assets auf potenzielle Verstöße zu prüfen. Sie können auch eigene Richtlinien definieren, um die Anforderungen für Ihre spezifischen internen Sicherheitsstandards zu erfüllen.

Anwendungsfälle

Die Anwendung Security Posture Control unterstützt verschiedene Anwendungsfälle, die in der Anwendung enthalten sind. Mithilfe von Anwendungsfällen können Sie bestimmte Arten von Lücken bei der Toolabdeckung in Ihren Assets, die Offenlegung von Cloud-Assets im Internet und Kombinationen mit Schwachstellen identifizieren. Die Richtlinien, die Sie für die unterstützten Anwendungsfälle benötigen, sind ebenfalls im Produkt enthalten.

Den Abdeckungsstatus für einige der wichtigsten Anwendungsfälle können Sie auf der Startseite (Zielseite) im Arbeitsbereich für die Kontrolle des Sicherheitsstatus unter anzeigen **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Startseite** im Homepage-Modul (Zielseite).

Alternativ können Sie die unterstützten Service Graph Connectors und den Abdeckungsstatus für einige der wichtigsten Anwendungsfälle auf den Registerkarten „Unterstützte Service Graph Connectors“ und „Setup für wichtige Anwendungsfälle“ unter anzeigen **Alle** > **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Setup von Connectors und Anwendungsfällen** (Zahnradsymbol).

Hinweis:

Auf der Registerkarte Wichtige Anwendungsfälle auf den Zielseiten der Homepage werden nicht alle möglichen Anwendungsfälle aufgelistet. Er stellt Ihnen einige wichtige Anwendungsfälle bereit, die Sie aktivieren, um Ihnen den Einstieg in die Bereitstellung des Security Posture Control-Produkts zu erleichtern.

Bevor Sie mit der Anwendung bereitgestellte Richtlinien für die unterstützten Anwendungsfälle aktivieren, müssen Sie die folgenden Aufgaben abgeschlossen haben.

- Sie haben alle in Installieren Sie die unterstützten Anwendungen für die Sicherheitsstatus-Überwachungbeschriebenen erforderlichen Anwendungen installiert und konfiguriert.
- Sie haben für jeden Anwendungsfall eine oder mehrere der folgenden Voraussetzungen erfüllt.

1. Sie verwenden derzeit oder installieren und aktivieren Service Graph Connectors für verschiedene Kategorien.

   Zu den Kategorien für die Anwendungsfälle gehören Service Graph Connectors, die Sie aktivieren müssen, um erste Einblicke zu erhalten, und Service Graph Connectors, die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie aktivieren können, um die Abdeckung der von der Sicherheitsstatus-Überwachung überwachten Assets zu verbessern.

2. Sie verwenden derzeit oder installieren und aktivieren die Anwendung Vulnerability Response.
3. Sie verwenden derzeit oder konfigurieren den Cloud-Account-Scan für Ihre AWS- und Azure-Accounts unter „Cloud Security Posture Management“.

Spezifische Anforderungen für jeden unterstützten Anwendungsfall werden in den folgenden Abschnitten beschrieben. Darüber hinaus müssen Sie eine oder mehrere der mit der Sicherheitsstatus-Überwachung gelieferten Richtlinien für einen Anwendungsfall aktivieren. Dieses Konzept wird auch in den folgenden Abschnitten behandelt.

Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien

Unter Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung erfahren Sie, wie Sie die Bedingungen einer Basisrichtlinie beim Erstellen anderer Richtlinien wiederverwenden können. Erstellen Sie in diesen Beispielen Basisrichtlinien, untergeordnete Richtlinien und das Klonen vorhandener Richtlinien. Anhand dieser Beispiele können Sie auch sehen, wie der Richtliniengenerator im Modul Richtlinien und Ergebnisse funktioniert.

Unterstützte Service Graph Connectors

Tabellen der unterstützten Service Graph Connectors, ihrer Toolkategorien und der Datentypen, die sie importieren, finden Sie in Unterstützte Hardware-Service Graph Connectors für Sicherheitsstatus-Überwachung und Unterstützte Softwareservice Graph Connectors für Sicherheitsstatus-Überwachung.

Sicherheitsstatus-Überwachung -Anwendungsfall: Erkennen von Assets mit fehlendem Endpunktschutz

Zum Erkennen von Assets ohne Endpunktschutz-Agent sind die folgenden Voraussetzungen erforderlich.

Abhängig von Ihrem Anwendungsfall können Sie festlegen, dass nur die erforderlichen Connectors aktiviert werden.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Endpunktschutz“.
2. Aktivieren Sie mindestens einen Service Graph Connector für EINE der folgenden Kategorien.
   a. Verzeichnisdienste (Microsoft Active Directory).
   b. Endpunktverwaltung: Microsoft Intune oder Jamf Device and Endpoint Management.
   c. Konfigurations- und Patchverwaltung: MicrosoftMicrosoft Azure Event Hubs SCCM oder IBM Bigfix.
   d. Cloud-Anbieter: Amazon AWS Cloud, Microsoft Azure, GCP.

> **Hinweis:**
> Wenn Cloud-Discovery aktiviert ist, sind diese Service Graph Connector-Produkte nicht erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von der Sicherheitsstatus-Überwachung gemeldet und überwacht werden.
   a. Netzwerksicherheit
   b. Infrastrukturüberwachung
   c. Netzwerk
   d. Überwachung der Anwendungsleistung

Nachdem Sie verifiziert haben, dass diese Voraussetzungen erfüllt sind, müssen Sie die folgende Richtlinie aktivieren: Assets ohne Endpunktschutz . Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

Sicherheitsstatus-Überwachung -Anwendungsfall: Erkennen von Assets, die von Schwachstellenbewertungstools übersehen wurden

Um Assets zu erkennen, die von Schwachstellenbewertungstools übersehen wurden, sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist. Abhängig von Ihrem Anwendungsfall können Sie festlegen, dass nur die erforderlichen Connectors aktiviert werden.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Schwachstellenbewertung“.
2. Aktivieren Sie mindestens einen Service Graph Connector für EINE der folgenden Kategorien.
   a. Verzeichnisdienste (Microsoft Active Directory).
   b. Endpunktverwaltung: Microsoft Intune oder Jamf Device and Endpoint Management.
   c. Konfigurations- und Patchverwaltung: MicrosoftMicrosoft Azure Event Hubs SCCM oder IBM Bigfix.
   d. Cloud-Anbieter: Amazon AWS Cloud, Microsoft Azure, GCP.

   Hinweis:
   Wenn Cloud-Discovery aktiviert ist, sind diese Service Graph Connector-Produkte nicht erforderlich.

3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von der Sicherheitsstatus-Überwachung gemeldet und überwacht werden.
   a. Netzwerksicherheit.
   b. Netzwerkfunktionen
   c. Infrastrukturüberwachung
   d. Überwachung der Anwendungsleistung

Nachdem Sie verifiziert haben, dass diese Voraussetzungen erfüllt sind, müssen Sie die folgende Richtlinie aktivieren: Assets werden nicht auf Schwachstellen gescannt. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsstatus-Überwachung Anwendungsfall: Erkennen nicht verwalteter Assets

Dieser Anwendungsfall umfasst zwei Teile: das Erkennen von Assets ohne Konfiguration und Patchverwaltungs-Agents.

Zum Erkennen von Assets ohne Konfigurations- und Patchverwaltungstools sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist.

Abhängig von Ihrem Anwendungsfall können Sie festlegen, dass nur die erforderlichen Connectors aktiviert werden.

1. Aktivieren Sie mindestens einen Service Graph Connector aus den Kategorien Konfiguration und Patch-Verwaltung.
2. Mindestens ein Service Graph Connector muss für EINE der folgenden Kategorien aktiviert sein.
   a. Verzeichnisdienste (Microsoft Active Directory).
   b. Endpunktschutz: CrowdStrike oder SentinelOne.
   c. Schwachstellenbewertung: Qualys, Rapid7oder Tenable.
   d. Konfigurations- und Patchverwaltung: MicrosoftMicrosoft Azure Event Hubs SCCM oder IBM Bigfix.
3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von der Sicherheitsstatus-Überwachung gemeldet und überwacht werden.
   a. Netzwerkfunktionen
   b. Infrastrukturüberwachung
   c. Netzwerksicherheit
   d. Überwachung der Anwendungsleistung

Nachdem Sie verifiziert haben, dass diese Voraussetzungen erfüllt sind, müssen Sie mindestens eine der folgenden Richtlinien aktivieren. Für jede Richtlinie, die mit „Cloud-Assets“ beginnt, müssen Service Graph Connectors in der Kategorie „Cloud-Anbieter“ aktiviert sein. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

- Für Assets fehlen Konfiguration und Patch-Management.
- Für Cloud-Assets fehlen Konfiguration und Patch-Verwaltung.

Sicherheitsstatus-Überwachung -Anwendungsfall: Erkennen von Assets ohne Endpunktverwaltungslösung

Zum Erkennen von Assets ohne Endpunktverwaltungslösung sind die folgenden Voraussetzungen erforderlich.

Abhängig von Ihrem Anwendungsfall können Sie festlegen, dass nur die erforderlichen Connectors aktiviert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Endpunktverwaltung“.
2. Mindestens ein Service Graph Connector muss für EINE der folgenden Kategorien aktiviert sein.
   a. Verzeichnisdienste (Microsoft Active Directory).
   b. Endpunktschutz: CrowdStrike oder SentinelOne.
   c. Schwachstellenbewertung: Qualys, Rapid7oder Tenable.
   d. Konfigurations- und Patchverwaltung: MicrosoftMicrosoft Azure Event Hubs SCCM oder IBM Bigfix.

Nachdem Sie verifiziert haben, dass diese Voraussetzungen erfüllt sind, müssen Sie die folgende Richtlinie aktivieren: Assets ohne Endpunktverwaltungslösung. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

Sicherheitsstatus-Überwachung Anwendungsfall: Erkennen von Assets mit Schwachstellen und Sicherheitstool-Abdeckungslücken

Sie können Assets mit kritischen Schwachstellen und fehlenden kritischen Sicherheitstools wie Endpunktschutz identifizieren, um diese Assets für die Korrektur zu priorisieren. Die Sicherheitsstatus-Überwachung liefert einige Richtlinien, die im Produkt enthalten sind, um diesen Anwendungsfall zu unterstützen.

Dieser Anwendungsfall erfordert, dass Sie die Anwendung Vulnerability Response und eine Integration mit mindestens einem Schwachstellenbewertungsprodukt wie Qualys, Rapid7oder Tenable installieren.

Die folgenden Richtlinien sind im Produkt Security Posture Control enthalten, um diesen Anwendungsfall für Assets mit kritischen Schwachstellen zu unterstützen, für die auch die Abdeckung durch Sicherheitstools fehlt.

1. Assets mit kritischen Schwachstellen und fehlendem Endpunktschutz.
2. Assets mit kritischen Schwachstellen und fehlender Konfiguration und fehlender Patchverwaltung.
3. Assets mit kritischen Schwachstellen und fehlender Endpunktverwaltung.

Sicherheitsstatus-Überwachung -Anwendungsfall: Erkennen des Internetrisikos von Cloud-Assets und Kombinationen mit hohem Risiko

Es ist wichtig, die potenzielle Gefährdung von Cloud-Assets (virtuelle Maschinen) im Internet auf verschiedenen Ports zu überwachen, um sicherzustellen, dass Schwachstellen in diesen Assets nicht remote ausgenutzt werden. Dieser Anwendungsfall hilft Ihnen, diese Assets zu identifizieren.

Mit der Sicherheitsstatus-Überwachung können Sie die Konfiguration von Cloud-Assets auswerten, um die Assets mit Internetverbindung zu identifizieren, d. h. welche Assets von überall im Internet erreichbar sind und über welche Ports sie verfügbar gemacht werden.

Die Sicherheitskontrolle kombiniert diese Einblicke mit Abdeckungslücken für Sicherheitstools und Schwachstellendaten von Drittanbieterscannern wie Qualys, Rapid7oder Tenable, um Kombinationen mit hohem Risiko zu identifizieren.

Derzeit unterstützt dieser Anwendungsfall AWS und erfordert die folgenden Voraussetzungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Service Graph Connector für AWS ist für dieselben AWS-Konten aktiviert, die Sie konfiguriert haben.
2. Sie haben eine oder mehrere der im Produkt enthaltenen Richtlinien unter Security Posture Control aktiviert.
   - Cloud-Assets mit SSH-Port 22 offen für das Internet.
   - Cloud-Assets mit für das Internet geöffnetem SSH-Port 22 und fehlendem Endpunktschutz.
   - Cloud-Assets mit HTTP-Port 80, die für das Internet geöffnet sind, und fehlendem Endpunktschutz.
   - Cloud-Assets mit kritischen Schwachstellen und SSH-Port 22 offen für das Internet (Erfordert Vulnerability Response).
   - Cloud-Assets mit kritischen Schwachstellen, fehlendem Endpunktschutz und offenem SSH-Port 22 für das Internet (Vulnerability Response erforderlich).
   - Cloud-Assets mit für das Internet geöffneten HTTP-Ports, kritischen Schwachstellen und fehlendem Endpunktschutz (erfordert Vulnerability Response).

Unterstützte Hardware-Service Graph Connectors für Sicherheitsstatus-Überwachung

Unterstützte Hardware-Service Graph Connectors mit CI-Klasse, Quelle (Produkt) und Toolkategorien. Diese Liste ist nicht vollständig und kann sich durch das Hinzufügen weiterer Produkte ändern.

Für die Discovery-Quelle für einen aufgeführten Connector stellt „SG“, „SGO“ oder „SGC“ dem Produktnamen für Produkte von Drittanbietern voran, z. B. SG-AWS, SGO-Datadog oder SGC-AD (Active Directory). Bei ServiceNow-Produkten stellen „SN“ oder „ServiceNow“ den Produktnamen voran, z. B. SNAssetManagement für ServiceNow Hardware Asset Management.

Nach der Installation können Sie die Connectors und ihre Kategorien in der Connector-Tabelle [sn_sec_spc_core_connector] in Ihrer Instanz anzeigen.

In der Tabelle [sn_sec_spc_core_asset_type_connector] können Sie Asset-Typen und ihre Zuordnung zu CI-Klassen und Connectors anzeigen.

Hardware-Service Graph Connectors

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_computer	Active Directory	Directory Services
Hardware-Asset	cmdb_ci_server	AppDynamics	Application Performance Monitoring
Hardware-Asset	cmdb_ci_server	Automox	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_computer	Automox	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_computer	BigFix	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_server	BigFix	Konfigurations- und Patchverwaltung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware-Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_printer	Cisco Merak	Netzwerk
Hardware-Asset	cmdb_ci_server	Cisco Merak	Netzwerk
Hardware-Asset	cmdb_ci_iot	Cisco Merak	Netzwerk
Hardware-Asset	cmdb_ci_hc_device	Cisco Merak	Netzwerk
Hardware-Asset	cmdb_ci_netgear	Cisco Merak	Netzwerk
Hardware-Asset	cmdb_ci_computer	Cisco Merak	Netzwerk
Hardware-Asset	cmdb_ci_server	CrowdStrike	Endpunktschutz
Hardware-Asset	cmdb_ci_server	Datadog	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	Dynatrace	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	Dynatrace	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_hc_device	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_server	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_iot	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_printer	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_iot	Forestout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_hc_device	Forestout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_computer	Forestout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_server	Forestout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_printer	Forestout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_server	Intune	Endpunktverwaltung
Hardware-Asset	cmdb_ci_computer	Intune	Endpunktverwaltung
Hardware-Asset	cmdb_ci_printer	Jamf Pro	Endpunktverwaltung
Hardware-Asset	cmdb_ci_server	Jamf Pro	Endpunktverwaltung
Hardware-Asset	cmdb_ci_computer	Jamf Pro	Endpunktverwaltung
Hardware-Asset	cmdb_ci_server	Landsweeper	IT Asset Management
Hardware-Asset	cmdb_ci_computer	Landsweeper	IT Asset Management
Hardware-Asset	cmdb_ci_printer	Landsweeper	IT Asset Management
Hardware-Asset	cmdb_ci_hc_device	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_printer	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_vm_instance	LogicMonitor	Infrastrukturüberwachung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware-Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_iot	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_computer	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_netgear	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	Microsoft Defender	Endpunktschutz
Hardware-Asset	cmdb_ci_server	New Relic	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	Nextthink	Digitale Mitarbeiter-Experience
Hardware-Asset	cmdb_ci_computer	Netskope	Verhinderung von Datenverlust
Hardware-Asset	cmdb_hardware_product_model	Netskope	Verhinderung von Datenverlust
Hardware-Asset	cmdb_ci_network_adapter	Netskope	Verhinderung von Datenverlust
Hardware-Asset	cmdb_software_instance	Netskope	Verhinderung von Datenverlust
Hardware-Asset	cmdb_sam_sw_install	Netskope	Verhinderung von Datenverlust
Hardware-Asset	sn_sec_sgc_netskop_client_attribute	Netskope	Verhinderung von Datenverlust
Hardware-Asset	cmdb_ci_server	Öffnen Sie Telemetrie	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	Puppet	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_server	Puppet	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_computer	Qualys-IDs	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_server	Qualys-IDs	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_vm_instance	Qualys-ServiceNow	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_server	Qualys-ServiceNow	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_hardware	Rapid7	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_computer	SCCM	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_server	SCCM	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_printer	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_iot	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	ScienceLogic	Infrastrukturüberwachung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware-Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_computer	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_hc_device	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_vm_instance	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_hardware	ServiceNow HAM	Hardware Asset Management
Hardware-Asset	cmdb_ci_hardware	ServiceNow ITOM Discovery	Discovery
Hardware-Asset	cmdb_ci_aws_datacenter	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_azure_datacenter	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_availability_zone	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_google_datacenter	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_cloud_service_account	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_cloud_subnet	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_compute_template	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_network	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_vm_instance	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_key_value	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_os_template	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_server	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_computer	SentinelOne	Endpunktschutz
Hardware-Asset	sn_sec_sgc_sntlone_asset_tags	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_ip_address	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_network_adapter	SentinelOne	Endpunktschutz
Hardware-Asset	sn_sec_sgc_sntlone_additional_attributes	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_server	Tanium-Asset	Endpunktverwaltung
Hardware-Asset	cmdb_ci_computer	Tanium-Asset	Endpunktverwaltung
Hardware-Asset	cmdb_ci_ups	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_industrial_sensor	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_cnc	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_hardware	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_netgear	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_industrial_actuator	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ip_switch	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_hub_network	Tenable	Schwachstellenbewertung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware-Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_security	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_server	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_rtu	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_ews	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_plc	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_control	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_dcs	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_storage_server	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_hmi	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_control_module	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_industrial_robot	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_historian	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_industrial_drive	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_iot	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ip_firewall	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_computer	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_unclassed_hardware	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ids_network	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ot_ied	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_printer	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_computer	VMware Workspace ONE UEM	Endpunktverwaltung
Hardware-Asset	cmdb_ci_server	VMware Workspace ONE UEM	Endpunktverwaltung
Hardware-Asset	cmdb_ci_printer	VMware Workspace ONE UEM	Endpunktverwaltung
Hardware-Asset	cmdb_ci_vm_instance	Assistent	Cloud Native Application Protection Platform
Hardware-Asset	cmdb_ci_server	Assistent	Cloud Native Application Protection Platform
Hardware-Asset	cmdb_ci_linux_server	Assistent	Cloud Native Application Protection Platform
Hardware-Asset	cmdb_ci_win_server	Assistent	Cloud Native Application Protection Platform

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Softwareservice Graph Connectors für Sicherheitsstatus-Überwachung

Unterstützte Softwareservice Graph Connectors mit CI-Klasse, Quelle (Produkt) und Toolkategorien. Diese Liste ist nicht vollständig und kann sich durch das Hinzufügen weiterer Produkte ändern.

Nach der Installation können Sie die Connectors und ihre Kategorien in der Connector-Tabelle [sn_sec_spc_core_connector] in Ihrer Instanz anzeigen.

In der Tabelle [sn_sec_spc_core_asset_type_connector] können Sie Asset-Typen und ihre Zuordnung zu CI-Klassen und Connectors anzeigen.

Softwareservice Graph Connectors

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Software	cmdb_ci_spkg	BigFix	Konfigurations- und Patchverwaltung
Software	cmdb_ci_spkg	Dynatrace	Application Performance Monitoring
Software	cmdb_ci_spkg	Forestout	Netzwerksicherheit
Software	cmdb_ci_spkg	Intune	Endpunktverwaltung
Software	cmdb_ci_spkg	Jamf Pro	Endpunktverwaltung
Software	cmdb_ci_spkg	New Relic	Application Performance Monitoring
Software	cmdb_ci_spkg	Nextthink	Digitale Mitarbeiter-Experience
Software	cmdb_ci_spkg	Netskope	Verhinderung von Datenverlust
Software	cmdb_ci_spkg	Qualys-ServiceNow	Schwachstellenbewertung
Software	cmdb_ci_spkg	SCCM	Konfigurations- und Patchverwaltung
Software	cmdb_ci_spkg	ServiceNow ITOM Discovery	Discovery
Software	cmdb_ci_spkg	Tanium-Asset	Endpunktverwaltung
Software	cmdb_ci_spkg	VMware Workspace ONE UEM	Endpunktverwaltung

Beispiele für Basisrichtlinien, untergeordnete Richtlinien und geklonte Richtlinien für Sicherheitsstatus-Überwachung

Sie können Ihre eigenen Basisrichtlinien erstellen, die über umfassende Bedingungen verfügen, die Sie als Ausgangspunkte für komplexere Richtlinien verwenden können.

Beispiele

Anhand der folgenden Beispiele erfahren Sie, wie Sie die Bedingungen einer Basisrichtlinie wiederverwenden können, wenn Sie andere Richtlinien erstellen, indem Sie untergeordnete

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinien erstellen oder vorhandene Richtlinien klonen. Anhand dieser Beispiele können Sie auch sehen, wie der Richtliniengenerator im Modul Richtlinien und Ergebnisse funktioniert.

Beginnen Sie mit dem ersten Beispiel, der Base-Richtlinie. In den anderen Beispielen wird die Basisrichtlinie als Ausgangspunkt verwendet.

Hinweis:
In diesen Beispielen wird der CrowdStrike Service Graph Connector als Service Graph Connector verwendet. Sie können jedoch jeden installierten Connector verwenden. In diesen Beispielen erstellen und aktivieren Sie die Richtlinien, um nach Asset-Übereinstimmungen zu suchen. Sie können diese Richtlinien jederzeit aus dem Modul Richtlinien und Ergebnisse entfernen, nachdem Sie sie aktiviert haben.

Basisrichtlinie für Sicherheitsstatus-Überwachung erstellen (Beispiel)

Beispiel für die Erstellung einer Basisrichtlinie, die Sie zum Erstellen anderer Richtlinien verwenden können.

Vorbereitungen
Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich für Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse**.
2. Wählen Sie **Neue Richtlinie**aus.
3. Wählen Sie das Stiftsymbol oben links aus, und füllen Sie im modalen Element „Metadaten bearbeiten“ die Felder aus.
4. Wählen Sie **Metadaten speichern**.
5. Wählen Sie im Bedingungsgenerator **Hardware-Asset** als Asset-Typ aus.

   Belassen Sie für diese Richtlinie die Optionen Basisrichtlinie und Ausschlussrichtlinien in ihren Standardeinstellungen (aus).
6. Wählen Sie für Verbindung die Option **Mit aggregierten Daten**aus.

   Für diese Richtlinie helfen Ihnen die aggregierten Daten, Assets in Ihrer CMDB zu finden, auf denen Windows 10 installiert ist. Beispielsweise können einige Datensätze geringfügige Abweichungen in der Art und Weise aufweisen, wie verschiedene Scanner „Windows 10“ melden. Aggregierte Daten stellen sicher, dass alle diese geringfügigen Variationen von „Windows 10“ mit dieser Richtlinie übereinstimmen.

   Die Felder Entität und Kriterien werden basierend auf Ihrer Auswahl im Feld Verbindung automatisch ausgefüllt.
7. Wählen Sie als Eigenschaft **OS**aus.
8. Für Werttyp in `Windows 10`.
9. Wählen Sie **Änderungen speichern**.
   Ihre Basisrichtlinie wird in der Liste Alle des Moduls Richtlinien und Ergebnisse angezeigt, ist jedoch nicht aktiviert.
10. Wählen Sie **Richtlinie aktivieren,** damit Ihre Basisrichtlinie alle Assets überwacht, die den Bedingungen der Richtlinie entsprechen, und Ergebnisse generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untergeordnete Richtlinie aus einer Basisrichtlinie für Sicherheitsstatus-Überwachung erstellen (Beispiel)

Ein Beispiel für das Erstellen einer untergeordneten Richtlinie mit den Bedingungen einer Basisrichtlinie.

Vorbereitungen

Diese untergeordnete Richtlinie erbt die Bedingungen einer Basisrichtlinie. Sie werden Ihrer untergeordneten Richtlinie weitere Bedingungen hinzufügen, damit Sie sich auf spezifischere Asset-Details konzentrieren können. Sie möchten eine neue Richtlinie zur Überwachung aller Ihrer Geräte, auf denen Windows 10 installiert ist und die vom Service Graph Connector CrowdStrike gemeldet werden, und Sie möchten alle Geräte ausschließen, die einer anderen Richtlinie entsprechen. In diesem Beispiel schließen Sie Assets, die für IRM-Ausnahmen (Integrated Risk Management) genehmigt wurden, aus Ihren Ergebnissen aus.

Hinweis:
Wenn Sie den Service Graph Connector CrowdStrike nicht installiert haben, können Sie einen verwenden, der installiert ist.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich für Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse**.
2. Suchen Sie in der Liste Aktiv nach Basisrichtlinie – Windows 10-Geräte, die Sie im ersten Beispiel erstellt haben, und wählen Sie sie aus, um den Datensatz zu öffnen.
3. Wählen Sie das Menü „Weitere Optionen“ (drei vertikale Punkte) und dann **Untergeordnete Richtlinie erstellen**aus.
   Eine neue Registerkarte wird geöffnet und mit einem neuen Datensatz sowie Basisrichtlinie – Windows 10-Geräte wird im Feld Basisrichtlinie angezeigt.
4. Wählen Sie das Stiftsymbol oben links aus, und füllen Sie im modalen Fenster Metadaten bearbeiten die Felder aus.
5. Wählen Sie **Metadaten speichern**.
6. Wählen Sie im Bedingungsgenerator **Hardware-Asset** als Asset-Typ aus.
7. Wählen Sie den Umschalter Basisrichtlinie.
8. Wählen Sie in der Liste die Richtlinie aus, die Sie für Beispiel 1, **Basisrichtlinie – Windows 10-Geräte** erstellt haben.

   Diese untergeordnete Richtlinie erbt automatisch die Bedingungen der Basisrichtlinie.
9. Wählen Sie den Umschalter Ausschlussrichtlinien.
10. Wählen Sie Assets mit genehmigter IRM-Ausnahme aus der Liste aus.

Hinweis:
Wenn Sie nicht über diese Richtlinie verfügen, können Sie eine andere Richtlinie aus der Liste auswählen, die Sie aus dieser Richtlinie ausschließen möchten.

Die Assets, die dieser Richtlinie entsprechen, werden von Ihrer untergeordneten Richtlinie ausgeschlossen. Beachten Sie, dass Sie weitere Richtlinien hinzufügen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

11. Wählen Sie **Gemeldet von aus**.
12. Wählen Sie **CrowdStrike** aus der Liste aus.
13. Wählen Sie **Änderungen speichern**.
    Ihre neue Richtlinie wird in der Liste „Alle“ des Moduls Richtlinien und Ergebnisse angezeigt, ist jedoch nicht aktiviert.
14. Wählen Sie **Richtlinie aktivieren,** damit Ihre Basisrichtlinie alle Assets überwacht, die den Bedingungen der Richtlinie entsprechen, und Ergebnisse generiert.

Richtlinie klonen für Sicherheitsstatus-Überwachung (Beispiel)

Beispiel für das Erstellen einer Richtlinie, die die Bedingungen aus einer anderen Richtlinie kopiert.

Vorbereitungen

Erstellen Sie eine Richtlinie, die die Bedingungen aus der in Beispiel 2 erstellten Richtlinie kopiert, damit Sie sie nicht erneut eingeben müssen. Sie werden diese Bedingungen klonen und der Kopie der von Ihnen erstellten untergeordneten Richtlinie weitere Bedingungen hinzufügen. In diesem Beispiel soll diese Richtlinie nach Geräten mit Windows 10 mit CrowdStrikesuchen und Assets mit IRM-Ausnahmen ausschließen, die in den letzten 7 Tagen nicht erkannt wurden.

Erforderliche Rolle: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich für Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse**.
2. Suchen Sie in der Liste Aktiv nach den untergeordneten Richtlinien – Windows -Geräte mit CrowdStrike, die Sie für das zweite Beispiel erstellt haben, und wählen Sie sie aus, um den Datensatz zu öffnen.
3. Wählen Sie das Menü „Weitere Optionen“ (drei vertikale Punkte) und anschließend **Richtlinie klonen**aus.
   Eine neue Registerkarte wird geöffnet, und der Richtlinienname wird in einem neuen Datensatz mit „Kopie“ im Titel angezeigt: Windows-Geräte mit CrowdStrike-Kopie.
4. Wählen Sie das Stiftsymbol oben links aus, und füllen Sie im modalen Fenster Metadaten bearbeiten die Felder aus.
5. Wählen Sie **Metadaten speichern**.
6. Wählen Sie rechts neben den ersten Feldern Verbindung und Entität den **AND-** Operator für neue Felder.
   Dadurch wird ein logisches UND zwischen den aktuellen Kriterien der Verbindungsentität und neuen Kriterien aus einer anderen Verbindungsentität hinzugefügt. In diesem Fall möchten Sie Connector-Daten für Assets angeben, die in den letzten 7 Tagen nicht von CrowdStrike erkannt wurden.
7. Wählen Sie für Verbindung die Option **Mit Connector-Daten**aus.
8. Wählen Sie für Entität **die Option CrowdStrike: CrowdStrike Device Details (CrowdStrike-Gerätedetails)**aus.
   Die eingereichten Kriterien werden basierend auf Ihrer Auswahl automatisch ausgefüllt.
9. Wählen Sie als Eigenschaft **Zuletzt gesehen um aus**.
10. Wählen Sie als Wert **Diese Woche**aus.
11. Wählen Sie **Änderungen speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Wählen Sie **Richtlinie aktivieren**.
    Sie können diese Richtlinien jederzeit aus dem Modul Richtlinien und Ergebnisse entfernen.

[store-future: BEGIN review]

Integration von Cloud Security Posture Management mit Amazon Web Services

Die von ServiceNow entwickelte CSPM-Anwendung (Cloud Security Posture Management) scannt Ihre Cloud-Umgebung kontinuierlich, um Nichteinhaltung oder Konfigurationsverstöße gegen Compliance-Frameworks wie CIS zu identifizieren.

Wichtige Begriffe und Konzepte

Derzeit unterstützt CSPM von ServiceNow CIS AWS Foundations Benchmark v1.4.0. Dieses Modul sammelt die Konfigurationsdaten von Cloud-Assets in Ihrer AWS-Umgebung direkt aus der Cloud, importiert sie in Ihre Now Platform-Instanz und prüft sie auf Compliance.

Region

Regionen beziehen sich auf ein geografisches Gebiet, das von Ihren AWS Cloud-Services unterstützt wird. Regionen haben Standardendpunkte, mit denen Sie auf die unterstützten Services für diese Region zugreifen können. Beispiele für Regionen sind VA oder Utah oder andere RECHENZENTREN-Standorte außerhalb der USA.

Ressource

Ressource ist ein Begriff, der in der AWS-Umgebung verwendet wird und die AWS-Assets und ihre Konfigurationseinstellungen beschreibt. Ressourcen sind die Services in Ihren AWS-Umgebungen. In Ihrer Instanz Now Platform von werden Ressourcen als Assets oder Configuration Items (CI) bezeichnet.

Center for Internet Security (CIS)

CIS ist eine Community-orientierte, Non-Profi-Organisation, die für die CIS Controls ® und CIS Benchmarks ™verantwortlich ist, weltweit anerkannte Prozesse zur Sicherung von IT-Systemen und Daten. Derzeit verwendet die CSPM-Anwendung ServiceNow die in CIS AWS Foundations 1.4.0 veröffentlichten Richtlinien, um die Compliance Ihrer Cloud-Assets zu überprüfen.

Richtlinie (Konfigurationsrichtlinien)

Richtlinien sind Governance-Richtlinien. In Now Platformwerden Richtlinien als Konfigurationsrichtlinien bezeichnet. Die von ServiceNow entwickelte Anwendung CSPM bietet Baseline-Konfigurationsrichtlinien, mit denen Sie Ihre Cloud-Umgebung anhand von Benchmark-Standards wie CIS bewerten können. Es gibt eine Eins-zu-eins-Zuordnung zwischen den Konfigurationsrichtlinien und den in den Compliance-Frameworks bereitgestellten Richtlinien.

Richtliniensatz (Konfigurationsrichtliniengruppen)

Richtliniensätze sind Gruppen von einzelnen Richtlinien. In Now Platformwerden Richtliniensätze als Konfigurationsrichtliniengruppen bezeichnet.

Cloud Security Posture Management

Richtlinien (**Konfigurationsrichtlinien**) und Richtliniensätze (**Konfigurationsrichtliniengruppen**) befinden sich im Modul **Cloud Security Posture Management,** das in Ihrer Instanz für diese Integration erstellt wurde.

Test

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tests sind Bibliotheken mit Datensätzen, in denen Scans Ihrer Assets organisiert werden. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets gesteuert werden sollte, um die Compliance zu erfüllen. Tests werden in der Anwendung Konfigurations-Compliance verwendet, um Assets zur Korrektur zu gruppieren.

Testergebnisse

Testergebnisse (Testergebnisse, Testergebnisse) werden in Ihrer Instanz erstellt, wenn bei einem Audit festgestellt wird, dass eine Ressource in Ihrer Cloud-Umgebung nicht konform ist. Testergebnisse werden in der Anwendung Konfigurations-Compliance in Ihrem Now Platformgespeichert. Diese Datensätze zeigen die Ergebnisse (Bestanden/Nicht bestanden) der Audits an, die für Ihre Ressourcen ausgeführt werden.

Testergebnisgruppen

Testergebnisgruppen helfen Ihnen, Testergebnisse in logischen Gruppen zu organisieren und Ihre Korrekturaufgaben zu priorisieren.

Erforderliche Now Platform-Rollen

Sicherheitsadministratoren mit der Rolle sn_vul.cspm_security_admin können dieses Produkt verwenden. Cloud-Account-Scans können auch von Benutzern mit der Rolle sn_vul.cspm_cloud_account_admin konfiguriert werden.

Eine vollständige Liste der erforderlichen Rollen für diese Integration finden Sie unter .

Workflow

- Die in der Anwendung enthaltenen Richtliniensätze (**Konfigurationsrichtliniengruppen**) definieren, welche Daten Sie importieren.
- Importierte Ressourcenkonfigurationsdaten werden in temporären Tabellen in Ihrer Instanz Now Platform gespeichert. Diese gespeicherten Daten werden dann auf Compliance mit den in CIS Amazon Web Services Foundations Benchmark v1.4.0 (CIS Amazon Web Services Foundations Benchmark v1.4.0) aufgeführten Richtlinien geprüft.
- Die Ergebnisse der Audits werden als Testergebnisse und Testergebnisgruppen in der Anwendung Konfigurations-Compliance in Ihrer -Plattforminstanz erstellt.
- Sie können Testergebnisse, Testergebnisgruppen und andere Konfigurations-Compliance -Daten in Dashboards und in Datensätzen in der Anwendung Konfigurations-Compliance anzeigen. Sicherheitsmanager, Schwachstellenmanager und Schwachstellenanalysten können diese Daten verwenden, um die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren, zu priorisieren und zu beheben.

Datensammlung

Zum Sammeln der AWS-Cloud-Konfigurationsdaten in Ihrer Umgebung rufen Sie die Cloud-API AWS über einen MID-Server von Ihrer Instanz Now Platform® auf. Sie rufen die Daten für die AWS-Ressourcen in Ihrer Enterprise-Umgebung ab. Die Daten in Ihren Ressourcen enthalten möglicherweise die folgenden Informationen, die Sie für Audits importieren können:

- Identity and Access Management (IAM)
- Speicher
- Protokollierung
- Überwachung
- Netzwerk

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für Nichteinhaltung von Sicherheit und Konfiguration in Ihren importierten Daten

Die folgende Liste enthält einige Beispiele für nicht konforme Ressourcen oder Abweichungen von ordnungsgemäßen Sicherheitspraktiken bei der Asset-Konfiguration:

- Suchen Sie nach S3-Buckets, die für die öffentliche Ansicht geöffnet sind.
- Suchen Sie nach S3-Buckets, die nicht verschlüsselt sind.
- IAM-Anwenderschlüssel werden nicht rotiert.
- Überprüfen Sie, ob der Zugriff auf VM-Images (virtueller Computer) bestimmter Lieferanten eingeschränkt ist.
- Überprüfen Sie, welche Ihrer IP-Adressen öffentlich sind.
- Überprüfen Sie, ob die Multifaktor-Authentifizierung (MFA) für S3-Buckets aktiviert ist.

Richtlinien und Benchmark-Standards

In CIS Amazon Web Services Foundations Benchmark v1.4.0 sind 58 Richtlinien definiert. 47 dieser Richtlinien sind in Ihrer Instanz als Teil dieser Anwendung codiert. Die 11 manuellen Richtlinien, die ebenfalls im Benchmark aufgeführt sind, werden von dieser Anwendung nicht unterstützt.

[End]
[store-future: BEGIN review]

Installieren und aktivieren Sie die Anwendung CSPM Innovation Lab für AWS

Die für diese Integration erforderlichen Anwendungen sind unter ServiceNow® Store verfügbar und werden unter dem Link Abhängigkeiten und Lizenzierung anzeigen auf der Seite mit der App-Liste aufgeführt. Einige Anwendungen haben Abhängigkeiten, die Sie separat herunterladen und installieren müssen.

Vorbereitungen
Erforderliche Rolle: admin zum Herunterladen, Installieren und Aktivieren aller -Anwendungen.

Der -Administrator weist die folgenden Rollen zu. Diese Now Platform® -Rollen sind für die Anwendung erforderlich.

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie in den folgenden Themen:

-
- Aktivieren Sie eine ServiceNow Store -Anwendung

Prozedur

1. Klicken Sie auf den Link, der in der E-Mail bereitgestellt wurde, um auf die Anwendungen für diese Integration im ServiceNow Storezuzugreifen.

   Um die Abhängigkeiten für eine Anwendung anzuzeigen, klicken Sie auf der Seite der Anwendung in ServiceNow Store**auf Abhängigkeiten und Lizenzierungsanforderungen anzeigen** unter Abhängigkeiten und Lizenzierung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Anwendung zur Verwaltung der Cloud-Sicherheitsposition finden Sie unter dem Link **Innovation Lab** von ServiceNow Store. Die anderen Anwendungen finden Sie unter **Apps und Lösungen**.

2. Installieren Sie die Anwendungen in der folgenden Reihenfolge.

Anwendung	App-Version und Abhängigkeits-Plugins
Plattformversion	San Diego vx.xx
Vulnerability Response (Abhängigkeiten)	v x.xx
Konfigurations-Compliance (Abhängigkeiten)	v x.xx
CMDB CI Class Models	Installieren Sie CMDB-CI-Klassenmodelle , Verzweigungsmaster
Security Support Common	Installieren Sie Security Support Common (Plugin-ID: com.snc.security_support.common) aus dem Repository , Verzweigungsfunktion/ EPIC1037528_native_cspm
Security Integration Framework	Installieren Sie das Security Integration Framework (Plugin-ID: com.snc.sec.int.framework) aus dem Repository , Verzweigungsfunktion/ EPIC1037528_native_cspm
Security Support Orchestration	Installieren Sie Security Support Orchestration (Plugin-ID: com.snc.secops.orchestration) aus dem Repository , Verzweigung „secops-dev“.
Vulnerability Response (Kernanwendung)	Installieren Sie Vulnerability Response (Plugin-ID: com.snc.vulnerability) aus dem Repository , Verzweigungsfunktion/EPIC1037528_native_cspm
Konfigurations-Compliance (Kernanwendung)	Installieren Sie Configuration Compliance (Plugin-ID: com.snc.vulc) aus dem Repository , Verzweigungsfunktion/EPIC1037528_native_cspm
Vulnerability Response und Configuration Compliance für Cloud	Installieren Sie Vulnerability Response und Configuration Compliance for Cloud (Plugin-ID: com.snc.vul_cloud) aus dem Repository , Verzweigung Scratch/STRY53500471_overview
Performance Analytics for Vulnerability Response	Installieren Sie Performance Analytics for Vulnerability Response (Plugin-ID: com.snc.vulnerability.analytics) aus dem Repository , Verzweigungsfunktion/ EPIC1037528_native_cspm
Installationsprogramm für das ServiceNow IntegrationHub Enterprise-Paket	Installationsprogramm für das ServiceNow IntegrationHub Enterprise-Paket installieren (Plugin-ID: com.glide.hub.integrations.enterprise)
Cloud Provisioning and Governance Core	Cloud Provisioning and Governance Core installieren (Plugin-ID: com.snc.cloud.core)
Cloud-Aktionsbibliothek	Installieren Sie die Cloud-Aktionsbibliothek (Plugin-ID: com.sn.itom.cal) aus dem Repository , Branch Master

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	App-Version und Abhängigkeits-Plugins
Governance für Cloud-Konfigurationen	Installieren Sie Governance für Cloud-Konfigurationen (Plugin-ID: com.sn.itom.ccg) , Verzweigungsmaster
Cloud Security Posture Management	Installieren Sie Cloud Security Posture Management (Plugin-ID: com.snc.secops.cspm) aus dem Repository , Verzweigung Scratch/Develop

3. Nachdem Sie die Anwendungen aus ServiceNow Storeheruntergeladen haben, navigieren Sie in Ihrer Instanz von Now Platform zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
4. Suchen Sie die in der vorherigen Tabelle aufgeführten Anwendungen, und klicken Sie auf **Installieren**, um sie zu aktivieren.
   Alle abhängigen Anwendungen, die zusammen mit einer Anwendung automatisch installiert werden, werden im Dialogfeld „Anwendungsinstallation“ angezeigt. Wenn Sie jedoch während der Installation aufgefordert werden, Abhängigkeits-Plugins zu installieren, befolgen Sie die bereitgestellten Eingabeaufforderungen. Stellen Sie sicher, dass alle in der vorherigen Tabelle aufgeführten Anwendungen und Abhängigkeiten installiert und aktiviert sind.

   Ein Dialogfeld wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.
5. Nachdem Sie die Anwendungen installiert und aktiviert haben, weisen Sie ihnen die folgenden Rollen zu, sofern sie noch nicht zugewiesen sind.

   Diese Rollen sind für verschiedene Workflow-Aktivitäten in der Integration erforderlich:

   - discovery_admin oder sn_cmmp.cloud_admin: Richtet die Cloud-Service-Accounts unter Now Platform für die entsprechenden AWS-Service-Accounts ein.
   - cspm_security_admin Diese Rolle erbt auch die folgenden Rollen:
     - sn_itom_ccg.governor - erstellt neue Richtlinien, Richtliniensätze und Sammler. Die Administratorrolle führt die Testrichtlinie aus und erstellt neue Entitäten, die vom Zeitplanungsadministrator verwendet werden.
     - sn_itom_ccg.operator: Der Operator Governance für Cloud-Konfigurationen testet die Richtlinien und überprüft die Ergebnisse. Der Operator korrigiert auch Testergebnisse und Testergebnisgruppen.
     - sn_itom_ccg.scheduling_admin - richtet Governance für Cloud-Konfigurationen für die AWS-Servicekonten ein. Erstellt Scan-Konfigurationen und Scan-Zeitpläne. Hat Zugriffsrechte für Scan-Ergebnisse, um importierte Entitäten und Richtlinien anzuzeigen.
   - cspm_cloud_account_admin Diese Rolle erbt auch die Rolle sn_itom_ccg.scheduling_admin.
   - mid_server: Konfiguriert einen MID-Server.
   - sn_vulc.admin: Konfiguriert die Anwendung Konfigurations-Compliance, hat Einblick in alle Datensätze und kann Eigenschaften ändern. Weist Rollen in der Anwendung Konfigurations-Compliance zu. Weitere Informationen zu Rollen in der Anwendung Konfigurations-Compliance finden Sie unter Mit Konfigurations-Compliance installierte Komponenten.
   - sn_vuln.admin: Konfiguriert die Anwendung Performance Analytics for Vulnerability Response.

   Führen Sie die folgenden Schritte aus, um einen Scan-Datensatz zum Scannen der Assets in Ihrer AWS-Umgebung zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Sofern noch nicht abgeschlossen, richten Sie AWS-Servicekonten und -Anmeldeinformationen sowie einen Alias für Anmeldeinformationen ein.
   Ein Benutzer mit der Rolle „discovery_admin“ oder „sn_cmmp.cloud_admin“ richtet die Servicekonten Amazon Web Services (AWS) ein. Weitere Informationen finden Sie unter . Diese Anmeldeinformationen werden in der Spalte Discovery-Anmeldeinformationen in den von Ihnen erstellten Cloud-Servicekonten-Datensätzen angezeigt.
7. Konfigurieren Sie Richtlinien mit der erforderlichen Berechtigungsebene, um Zugriff auf die AWS-Ressourcen für Cloud-Discovery und Cloud Provisioning and Governance zu gewähren.
   Fügen Sie das folgende JSON-Objekt in Ihren Anhang ein, um Ihre Berechtigungen zu erstellen. Kopieren Sie den Text, und nehmen Sie die erforderlichen Änderungen vor. Verwenden Sie diese Datei, um Ihre Richtlinienberechtigungen zu erstellen. Dies sind mindestens die Berechtigungen, die für diese Anwendung erforderlich sind. Weitere Informationen finden Sie unter .

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GenerateCredentialReport",
    "access-analyzer:ListAnalyzers",
    "iam:GetPolicyVersion",
    "iam:GetAccountPasswordPolicy",
    "iam:ListServerCertificates",
    "s3:GetBucketLogging",
    "cloudtrail:GetTrailStatus",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeRegions",
    "logs:DescribeMetricFilters",
    "cloudtrail:GetEventSelectors",
    "iam:ListVirtualMFADevices",
    "s3:GetEncryptionConfiguration",
    "kms:GetKeyRotationStatus",
    "iam:ListAttachedUserPolicies",
    "rds:DescribeDBInstances",
    "iam:GetCredentialReport",
    "ec2:DescribeNetworkAcls",
    "iam:ListPolicies",
    "sns:ListSubscriptionsByTopic",
    "iam:ListEntitiesForPolicy",
    "iam:ListUserPolicies",
    "s3:GetBucketVersioning",
    "config:DescribeConfigurationRecorderStatus",
    "cloudtrail:DescribeTrails",
    "ec2:DescribeSecurityGroups",
    "kms:ListKeys",
    "config:DescribeConfigurationRecorders",
    "ec2:DescribeVpcs",
    "cloudwatch:DescribeAlarms",
    "iam:GetLoginProfile",
    "iam:GetAccountSummary"
   ],
   "Resource": "*"
  }
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  ]
}
```

8. Ein Benutzer mit der Rolle sn_itom_ccg.scheduling_admin richtet in Governance für Cloud-Konfigurationen ein Cloud-Servicekonto mit den AWS-Anmeldeinformationen für die im vorherigen Schritt erstellten Servicekonten Amazon Web Services ein.

   Weitere Informationen zu den erforderlichen Schritten finden Sie unter .

9. Sofern noch nicht abgeschlossen, richtet ein Benutzer mit der Rolle „mid_server“ einen MID-Server Now Platform ein, um Ihre Instanz mit Ihren AWS-Konten zu verbinden.

   Weitere Informationen finden Sie unter .

10. Nachdem Sie den MID-Server eingerichtet haben, führt ein Benutzer mit der Eigenschaft sn_itom_ccg.scheduling_admin die DATACENTER-Discovery aus, um die DATACENTER mit den Servicekonten zu identifizieren.

    Weitere Informationen finden Sie unter .

Hinweis:
Wenn Sie die Tabelle im Cloud-Servicekonto nicht ausfüllen, wird die Integration nicht ordnungsgemäß ausgeführt.

11. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Gruppenregeln** und wählen Sie **Zuweisungsgruppe, Testregel,** um den Datensatz zu öffnen, und legen Sie das Feld Aktiv auf **wahr**fest.

    In Konfigurations-Compliance sind die in der Anwendung enthaltenen Gruppen- und Zuweisungsregeln standardmäßig deaktiviert. Ein Benutzer mit sn_vulc.admin aktiviert diese Regeln.

    Diese Regel gruppiert die während des Audits erstellten Testergebnisse. Alle Testergebnisse für eine bestimmte Richtlinie, deren Rückgabewert für das Testergebnis falsch ist, werden in einer Testergebnisgruppe gruppiert.

    Standardmäßig werden Testergebnisgruppen der Benutzergruppe „CI-Support“ zugewiesen. Diese Zuweisungsregel ist standardmäßig deaktiviert.

12. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Zuweisungsregeln** Öffnen Sie den Datensatz An CI-Supportgruppe zuweisen, und klicken Sie auf das Kontrollkästchen **Aktiv**, um ihn zu aktivieren.

    Diese Regel weist die Testergebnisgruppen Benutzern in der CI-Supportgruppe zu. Weisen Sie dieser Gruppe Anwender zu, die an diesen Testergebnissen arbeiten sollen.

    Dies ist eine Standardzuweisungsregel, die je nach internen Praktiken möglicherweise nicht für die Zuweisung von Cloud-Konfigurationsproblemen in Ihrer Organisation geeignet ist. Unter Umständen möchten Sie stattdessen eine Zuweisungsregel erstellen, die Ihren Anforderungen entspricht. Sie können Cloud-Account-Metadaten verwenden, indem Sie von der Testergebnistabelle aus durch die Tabelle „Erkanntes Element“ laufen, um Zuweisungsregeln zu definieren.

13. Navigieren zu **Performance Analytics** > **Datenerfasser** > **Aufträge** Suchen Sie nach den täglichen PA CC-Sammlungsaufträgen, und vergewissern Sie sich, dass diese Aufträge aktiviert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Audit-Ergebnisse in den Dashboards Performance Analytics for Vulnerability Response anzuzeigen, aktiviert ein Benutzer mit der Rolle sn_vuln.admin die Anwendung und aktiviert die Datensammler.

Sie haben das Setup für die Integration abgeschlossen. Sie sind bereit, einen Scan-Konfigurationsdatensatz in der CSPM-Anwendung zu erstellen.

[End]

[store-future: BEGIN review]

Cloud-Accounts mit der CSPM-Anwendung ServiceNow mit AWSscannen

In diesem Abschnitt wird beschrieben, wie Sie Sicherheitsscans für Ihre Cloud-Konten konfigurieren, um die Compliance Ihrer Ressourcen mit Benchmark-Frameworks zu überprüfen. Eine Beispielrichtlinie wird verwendet, um Ihnen diesen Prozess zu zeigen.

Vorbereitungen

Setup erforderlich: Dieses Beispiel beginnt mit der Erstellung eines Scan-Datensatzes. Wenn Sie die Informationen in Ihren Servicekonten für AWS einrichten oder überprüfen möchten, lesen Sie die Setup-Schritte unter .

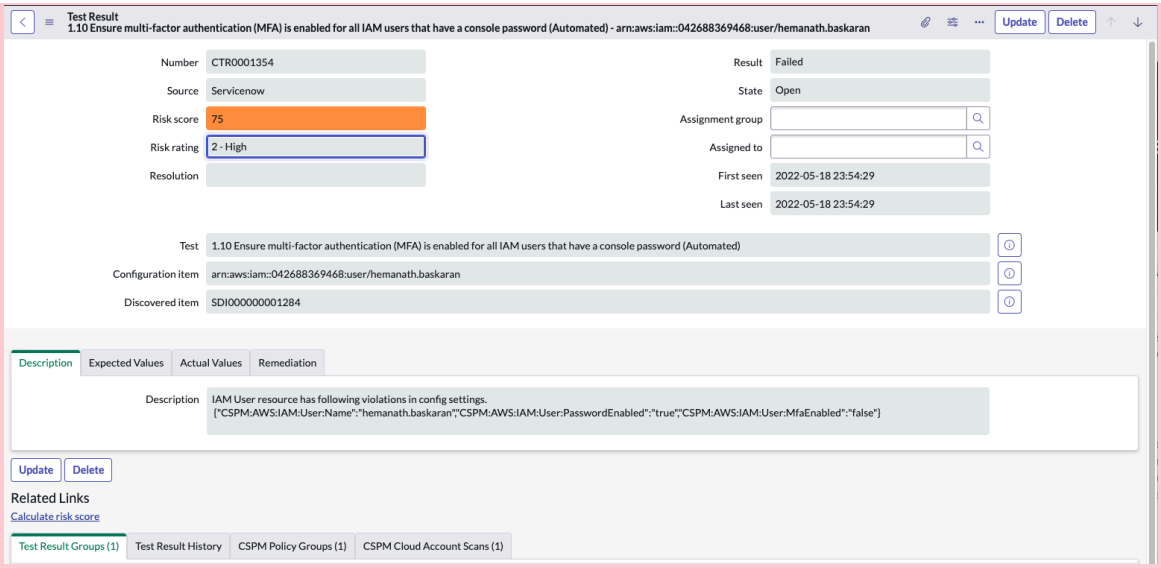
Erforderliche Rolle: sn_vul.cspm_cloud_account_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Administration** > **Cloud-Account-Scans** um einen Scan-Konfigurationsdatensatz in der CSPM-Anwendung zu erstellen.
   Die Seite „Richtlinienbewertungsregeln“ wird angezeigt.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.
   a. Geben Sie einen eindeutigen Namen für die Scan-Konfiguration ein.
   b. Geben Sie eine Kurzbeschreibung ein, um den Datensatz später zu finden.
   c. Wählen Sie **Cloud-Servicekonten** und dann die gewünschten Zielservicekonten aus.
      Dies sind die Datensätze, die Sie für Ihre AWS-Accounts erstellt und eingerichtet und in Governance für Cloud-Konfigurationeneingegeben haben.
4. Aktivieren Sie das Kontrollkästchen **Hintergrundscan**, um ihn zu aktivieren.
   Wenn die Prüfung stündlich ausgeführt werden soll, aktivieren Sie die Checkbox **Hintergrundprüfung**, um sie zu aktivieren. Wenn das Kontrollkästchen nicht aktiviert ist, müssen Sie die Prüfung bei Bedarf starten.
5. Um die verknüpften untergeordneten Accounts automatisch zu scannen, aktivieren Sie das Kontrollkästchen **Verknüpfte untergeordnete Accounts automatisch scannen**.
6. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse** > **Alle**.
   Die Liste der Testergebnisgruppen (CTR#), die aus dem Richtlinien-Audit erstellt wurden, wird angezeigt.

   Es werden Testergebnisdatensätze für Ihre nicht konformen Cloud-Ressourcen erstellt. Wenn Verstöße behoben werden, werden Testergebnisdatensätze geschlossen.
7. Öffnen Sie einen Datensatz, um die folgenden Daten anzuzeigen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Testfeld

Dieses Feld zeigt die Eins-zu-eins-Zuordnung zwischen der für das Audit verwendeten Richtlinie und dem Audit-Testdatensatz in Konfigurations-Compliancean. Klicken Sie, um eine Vorschau des Testdatensatzes anzuzeigen, ihn zu öffnen und die Zitate (also die autorisierende Quelle) anzuzeigen. In diesem Beispiel ist die autorisierende Quelle CIS AWS Foundations Benchmark v1.4.0, und der erwähnte Abschnitt, die Richtlinie, lautet 1.10. Jede Richtliniengruppe, zu der diese Richtlinie gehört, wird angezeigt. Eine Richtlinie kann in mehr als einer Richtliniengruppe enthalten sein. Außerdem wird die Anzahl der vom Audit generierten Testergebnisse angezeigt.

Feld „Konfigurationselement“

Diese Daten beziehen sich auf eine Ressource in AWS.

Feld „Erkanntes Element“.

Ein erkanntes Element in Ihrem Now Platform ist der AWS-Ressource zugeordnet. Alle über die AWS-Ressource importierten Cloud-Metadaten, z. B. Region, Cloud-Account und Ressourcentyp, werden im Datensatz „Erkanntes Element“ gespeichert.

Registerkarte „Testergebnisgruppen“.

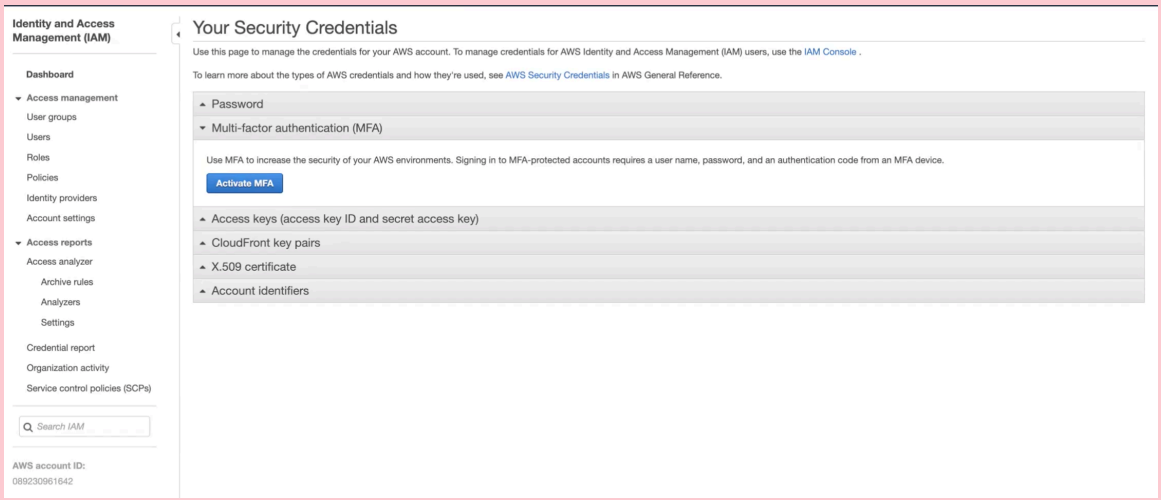
Standardmäßig gruppiert die Anwendung Konfigurations-Compliance die Testergebnisse in Testergebnisgruppen basierend auf einer falschen Rückgabe beim Audit. Für eine Ressource wird nur ein Datensatz pro Testergebnis erstellt, und er wird nach Datenimporten aktualisiert. Wenn die Konfigurationseinstellung für eine Ressource in Ihrer AWS-Umgebung zwischen den Scans geändert wird, wird der Datensatz in Ihrer Instanz Now Platform aktualisiert.

8. Um die importierten Daten zu überprüfen, können Sie zum AWS-Benutzerkonto zurückkehren.

In diesem Beispiel zeigt ein Scheck für diesen Account an, dass die Multifaktor-Authentifizierung nicht aktiviert ist (**MFA aktivieren**). Dieser Status entspricht den Sicherheitsdaten, die über die Ressourcen und Ressourcengruppen aus der Cloud importiert wurden. Nachdem Sie die Einstellung geändert haben und die Ressource konform ist, werden Ihre Änderungen im nächsten Datenimport übernommen. Im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

folgenden Beispiel muss MFA in AWS für diese Ressource aktiviert werden, bevor der zugehörige Testergebnisdatensatz geschlossen wird.



[End]

Zeigen Sie AWS CSPM-Audit-Daten in den Performance Analytics for Vulnerability Response -Dashboards an

Diese Integration umfasst Dashboards in der Anwendung Performance Analytics for Vulnerability Response.

Vorbereitungen

Erforderliche Rolle: pa_viewer

Prozedur

1. Um das Dashboard anzuzeigen, navigieren Sie zu **Konfigurations-Compliance** > **Übersicht**.

   Daten für die Dashboards werden täglich gesammelt. Um die Einstellungen zu ändern, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge**.

   Hinweis:
   Wenn Sie andere Schwachstellenintegrationen von Drittparteien ausführen, werden alle Ihre Schwachstellendaten und Audit-Ergebnisdaten zusammen in den Dashboard-Visualisierungen angezeigt. Sie können Ihre Filter festlegen, um die CSPM-Daten herauszufiltern.

   Das Dashboard enthält drei Registerkarten:

   - Asset-Kategorie
   - Korrektur
   - Genehmigungen

2. Klicken Sie auf eine Registerkarte, um die Daten anzuzeigen.
3. Die in den Daten enthaltenen autorisierenden Quellen werden unter den Datenvisualisierungen aufgelistet.

Erstellt eine anwenderdefinierte Richtlinie für AWS in CSPM

Erstellen Sie eine Richtlinie, um Ihre anwenderdefinierten Compliance-Standards zu implementieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Konfigurationsrichtlinien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular zur Erstellung von anwenderdefinierten CSPM-Richtlinien

Feld	Beschreibung		
Richtlinienname	Eindeutiger Name der Richtlinie.		
Beschreibung	Details der Richtlinie.		
Ressourcentyp			
Cloud-Provider	Cloud-Bereitstellungsplattform für die Richtlinie.		
Ressourcentyp	Typ der Ressource in der Cloud-Umgebung. Wenn der Ressourcentyp nicht vorhanden ist, erstellen Sie einen Ressourcentyp gemäß den Konventionen von AWS oder Azure.		
Richtlinienbedingung			
Typ			
Bedingung	Bedingung zum Erstellen eines Testergebnisses. Betrachten Sie die folgenden Szenarien.		
	Konfigurationsschlüssel vorhanden?	Ressourcentyp vorhanden?	Nächste Schritte
	Ja	Ja, Ressourcentyp und die Flows zum Abrufen der Metadaten sind vorhanden. Beispiel für einen Subflow: CSPM: Azure Subscription Resource Collector (CSPM: Azure-Abonnement-Ressourcensammler).	Geben Sie die Bedingungen für die Richtlinie an.
	Nein	Ja	**a.** Erstellen Sie einen Konfigurationsschlüssel. **b.** Erstellen Sie einen Ressourcensammler. **c.** Erstellen Sie einen Konfigurationssammler. **d.** Geben Sie die Bedingungen für die Richtlinie an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schweregrad	Schweregrad der Richtlinie.

4. Wählen Sie **Absenden** aus, um die anwenderdefinierte Richtlinie zu erstellen.

Cloud Security Posture Management mit Microsoft Azure

Die von ServiceNow® entwickelte CSPM-Anwendung (Cloud Security Posture Management) scannt Ihre Cloud-Umgebung kontinuierlich, um Nichteinhaltung oder Konfigurationsverstöße gegen Compliance-Frameworks wie CIS zu identifizieren.

Wichtige Begriffe und Konzepte

Diese von ServiceNow entwickelte CSPM-Integration unterstützt CIS Microsoft Azure. Die -Integration erfasst die Konfigurationsdaten von Cloud-Assets in Ihrer Microsoft Azure -Umgebung direkt aus der Cloud, importiert sie in Ihre Now Platform® -Instanz und prüft Ihre Assets auf Compliance.

Die folgenden Begriffe sollen Ihnen helfen, die Konzepte dieser CSPM-Integration zu verstehen. Weitere Informationen zu Azure-Produkten finden Sie unter Azure.com .

Region

Regionen beziehen sich auf geografische Bereiche, die von Ihren Microsoft Azure Cloud-Services unterstützt werden. Regionen haben Standardendpunkte, mit denen Sie auf die unterstützten Services für diese Region zugreifen können. Beispiele für Regionen sind VA oder Utah oder andere RECHENZENTREN-Standorte außerhalb der USA.

Ressource

„Ressource“ ist ein in der Umgebung Microsoft Azure verwendeter Begriff, der Microsoft Azure -Assets und ihre Konfigurationseinstellungen beschreibt. Ressourcen sind die Services in Ihren Microsoft Azure -Umgebungen. Virtuelle Maschinen, Speicherkonten, Web-Apps, Datenbanken und virtuelle Netzwerke sind Beispiele für gängige Ressourcen. In Ihrer Instanz Now Platform von werden Ressourcen als Assets oder Configuration Items (CI) bezeichnet.

Ressourcengruppen

Ressourcen in Ihren Microsoft Azure -Accounts können in Ressourcengruppen organisiert werden. Gruppen enthalten zugehörige Ressourcen für eine bestimmte Microsoft Azure -Lösung oder ein bestimmtes Produkt. Ressourcen in einer Ressourcengruppe können sich in verschiedenen Regionen befinden, und sie können in einer Region außerhalb der Gruppe selbst liegen. Die Ressourcengruppe speichert Metadaten zu ihren Ressourcen. Wenn Sie einen Speicherort für die Ressourcengruppe angeben, geben Sie an, wo diese Metadaten gespeichert werden. Aus Compliance-Gründen müssen Sie wissen, dass Ihre Daten in einer bestimmten Region gespeichert werden.

Center for Internet Security (CIS)

CIS ist eine Community-orientierte, Non-Profi-Organisation, die für die CIS Controls ® und CIS Benchmarks ™verantwortlich ist, weltweit anerkannte Prozesse zur Sicherung von IT-Systemen und Daten. Derzeit verwendet die CSPM-Anwendung ServiceNow die in Microsoft Azure (CIS Microsoft Azure Foundations Benchmark Version 1.4.0) veröffentlichten Richtlinien, um die Compliance Ihrer Cloud-Assets zu prüfen.

Automatisiert

Dieser Begriff bezieht sich auf die Empfehlungen, die sich aus einem Audit eines Assets oder einer technischen Steuerung ergeben, die vollständig automatisiert und durch einen Bestanden/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlgeschlagen-Status validiert werden können. Diese Integration unterstützt automatisierte Bewertungen.

Richtlinie (Konfigurationsrichtlinien)

Richtlinien sind Governance-Richtlinien. In Now Platformwerden Richtlinien als Konfigurationsrichtlinien bezeichnet. Die von ServiceNow entwickelte Anwendung CSPM bietet Baseline-Konfigurationsrichtlinien, mit denen Sie Ihre Cloud-Umgebung anhand von Benchmark-Standards wie CIS bewerten können. Es gibt eine Eins-zu-eins-Zuordnung zwischen den Konfigurationsrichtlinien und den in den Compliance-Frameworks bereitgestellten Richtlinien.

Richtliniensatz (Konfigurationsrichtliniengruppen)

Richtliniensätze sind Gruppen von einzelnen Richtlinien. In Now Platformwerden Richtliniensätze als Konfigurationsrichtliniengruppen bezeichnet.

Cloud Security Posture Management

Richtlinien (**Konfigurationsrichtlinien**) und Richtliniensätze (**Konfigurationsrichtliniengruppen**) befinden sich im Modul **Cloud Security Posture Management,** das in Ihrer Instanz für diese Integration erstellt wurde.

Test

Tests sind Deskriptordatensätze, die für Konfigurationsrichtlinien erstellt werden. Für jede Konfigurationsrichtlinie im CSPM-Modul wird automatisch ein entsprechender Konfigurationstest im Modul Konfigurations-Compliance erstellt. Konfigurationstests werden von den Testergebnissen referenziert, also von den Konfigurationsergebnissen des Scans, um den Test oder die Richtlinie zu identifizieren, die für eine bestimmte Cloud-Ressource ausgewertet wurde.

Testergebnisse

Testergebnisse (Testergebnisse, Testergebnisse) werden in Ihrer Instanz erstellt, wenn bei einem Audit festgestellt wird, dass eine Ressource in Ihrer Cloud-Umgebung nicht konform ist. Testergebnisse werden in der Anwendung Konfigurations-Compliance in Ihrem Now Platformgespeichert. Diese Datensätze zeigen die Ergebnisse (Bestanden/Nicht bestanden) der Audits an, die für Ihre Ressourcen ausgeführt werden.

Testergebnisgruppen

Testergebnisgruppen helfen Ihnen, Testergebnisse in logischen Gruppen zu organisieren und Ihre Korrekturaufgaben zu priorisieren.

Erforderliche Now Platform-Rollen

Sicherheitsadministratoren mit der Rolle sn_vul.cspm_security_admin können dieses Produkt verwenden. Cloud-Account-Scans können auch von Benutzern mit der Rolle sn_vul.cspm_cloud_account_admin konfiguriert werden.

Eine vollständige Liste der erforderlichen Rollen für diese Integration finden Sie unter .

Workflow

- Die in der Anwendung enthaltenen Richtliniensätze (**Konfigurationsrichtliniengruppen**) definieren, welche Daten Sie importieren.
- Importierte Ressourcenkonfigurationsdaten werden in temporären Tabellen in Ihrer Instanz Now Platform gespeichert. Diese gespeicherten Daten werden dann auf Compliance mit den in aufgeführten Richtlinien geprüft Microsoft Azure. . Es gibt 56 automatisierte Richtlinien, die von dieser Integration unterstützt werden. Die manuellen Richtlinien und neun der automatisierten Richtlinien werden nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Ergebnisse der Audits werden als Testergebnisse und Testergebnisgruppen in der Anwendung Konfigurations-Compliance in Ihrer -Plattforminstanz erstellt.
- Sie können Testergebnisse, Testergebnisgruppen und andere Konfigurations-Compliance -Daten in Dashboards und in Datensätzen in der Anwendung Konfigurations-Compliance anzeigen. Sicherheitsmanager, Schwachstellenmanager und Schwachstellenanalysten können diese Daten verwenden, um die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren, zu priorisieren und zu beheben.

Datensammlung

Um die Microsoft Azure Cloud-Konfigurationsdaten in Ihrer Umgebung zu sammeln, ruft ServiceNow die Microsoft Azure Cloud-API über einen MID-Server von Ihrer NOW Platform-Instanz auf. Die Konfigurationsdaten von Microsoft Azure-Ressourcen werden abgerufen, um Konfigurationsrichtlinien auszuwerten. Zu den Services oder Ressourcen, für die Konfigurationsdaten abgerufen werden, gehören:

- Identity and Access Management (IAM)
- Speicher
- Datenbankservices
- Protokollierung und Überwachung
- Netzwerk
- Virtuelle Maschinen
- Sicherheitsüberlegungen wie Schlüsselablaufdaten
- AppService

Beispiele für Nichteinhaltung von Sicherheit und Konfiguration in Ihren importierten Daten

Die folgende Liste enthält einige Beispiele für Konfigurationsrichtlinien, die für Cloud-Ressourcen Microsoft Azure ausgewertet wurden, um die nicht konformen Ressourcen zu identifizieren:

- Überprüfen Sie, ob die Zugriffsebene für Blob Storage auf „Privat“ festgelegt ist.
- Überprüfen Sie, ob der Blob Storage für kritische Daten verschlüsselt ist.
- Stellen Sie sicher, dass die Speicherzugriffsschlüssel regelmäßig neu generiert werden.
- Überprüfen Sie, ob der Endpunktschutz für alle virtuellen Computer (VM) installiert ist.
- Überprüfen Sie, ob der Standardzugriff für Speicherkonten auf „Verweigern“ festgelegt ist.
- Überprüfen Sie, ob „SSL-Verbindung erzwingen“ für den Standard-MySQL-Datenbankserver auf „Aktiviert“ festgelegt ist.

Richtlinien und Benchmark-Standards

In sind ungefähr 123 Richtlinien definiert Microsoft Azure. . 56 dieser Richtlinien oder Empfehlungen sind standardmäßig in der CSPM-Anwendung enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und aktivieren Sie die Anwendung CSPM Innovation Lab für Microsoft Azure

Die für diese Integration erforderlichen Anwendungen sind unter ServiceNow® Store verfügbar und werden unter dem Link Abhängigkeiten und Lizenzierung anzeigen auf der Seite mit der App-Liste aufgeführt. Einige Anwendungen haben Abhängigkeiten, die Sie separat herunterladen und installieren müssen.

Vorbereitungen

Erforderliche Rolle: admin zum Herunterladen, Installieren und Aktivieren aller -Anwendungen.

Der Administrator weist die in Schritt 5 aufgeführten Rollen Now Platform zu. Diese Rollen Now Platform® sind für die Anwendung erforderlich.

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie in den folgenden Themen:

Prozedur

1. Klicken Sie auf den Link, der in der E-Mail bereitgestellt wurde, um auf die Anwendungen für diese Integration im ServiceNow Storezuzugreifen.

   Um die Abhängigkeiten für eine Anwendung anzuzeigen, klicken Sie auf der Seite der Anwendung in ServiceNow Store**auf Abhängigkeiten und Lizenzierungsanforderungen anzeigen** unter Abhängigkeiten und Lizenzierung.

   Hinweis:
   Die Anwendung zur Verwaltung der Cloud-Sicherheitsposition für Microsoft Azure finden Sie unter dem **Innovation Lab-** Link von ServiceNow Store. Die anderen Anwendungen finden Sie unter **Apps und Lösungen**.

2. Installieren Sie die Anwendungen in der Reihenfolge, die in der folgenden Tabelle aufgeführt ist:
3. Nachdem Sie die Anwendungen aus ServiceNow Storeheruntergeladen haben, navigieren Sie in Ihrer Instanz von Now Platform zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**. Suchen Sie die Anwendungen, und aktivieren Sie sie in der in der Tabelle angegebenen Reihenfolge.
4. Klicken Sie auf **Installieren**, um sie zu aktivieren.

   Hinweis:
   Die Installation dieser Anwendungen kann 2 bis 3 Stunden dauern.

Anwendung	Installieren Sie die App-Version und die Abhängigkeits-Plugins
Plattformversion	San Diego, Tokyo
Vulnerability Response (Abhängigkeiten)	Plugin-ID: com.snc.vul_dep
Konfigurations-Compliance (Abhängigkeiten)	Plugin-ID: com.snc.vulc_dep
CMDB CI Class Models	CMDB-CI-Klassenmodelle installieren: com.sn_cmdb_ci_class – 1.39.0
Security Support Common	Plugin-ID: com.snc.security_support.common – 13.3.3
Security Integration Framework	Plugin-ID: com.snc.sec.int.framework – 13.2.2

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Installieren Sie die App-Version und die Abhängigkeits-Plugins
Security Support Orchestration	Plugin-ID: com.snc.secops.orchestration – 12.3.0
Vulnerability Response (Kernanwendung)	Plugin-ID: sn_vul – 17.0.2
Konfigurations-Compliance (Kernanwendung)	Plugin-ID: sn_vulc – 14.4.4
Performance Analytics for Vulnerability Response	Plugin-ID: com.snc.vulnerability.analytics – 12.4.4
Installationsprogramm für das ServiceNow IntegrationHub Enterprise-Paket	Plugin-ID: com.glide.hub.integrations.enterprise
Cloud Provisioning and Governance Core	Plugin-ID: com.snc.cloud.core
Cloud-Aktionsbibliothek	Plugin-ID: com.sn.itom.cal – 1.3.6
Governance für Cloud-Konfigurationen	Plugin-ID: com.sn.itom.ccg – 1.3.7
CCG-Inhaltspaket	Plugin-ID: com.sn.itom.ccg_cp – 1.3.7
Cloud Security Posture Management	Plugin-ID: com.snc.secops.condor – 1.1.1

Alle abhängigen Anwendungen, die zusammen mit einer Anwendung automatisch installiert werden, werden im Dialogfeld „Anwendungsinstallation“ angezeigt. Wenn Sie jedoch während der Installation aufgefordert werden, Abhängigkeits-Plugins zu installieren, befolgen Sie die bereitgestellten Eingabeaufforderungen.

Stellen Sie sicher, dass alle in der vorherigen Tabelle aufgeführten Anwendungen und Abhängigkeiten installiert und aktiviert sind, bevor Sie mit den nächsten Schritten fortfahren.

Ein Dialogfeld wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

5. Weisen Sie die folgenden Rollen zu, wenn sie noch nicht zugewiesen sind:
   Diese Rollen sind für verschiedene Workflow-Aktivitäten in der Integration erforderlich.
   - discovery_admin oder sn_cmmp.cloud_admin: Richtet die Cloud-Service-Accounts unter Now Platform für die entsprechenden Microsoft Azure -Service-Accounts ein.
   - cspm_security_admin Diese Rolle erbt auch die folgenden Rollen:
     - sn_itom_ccg.governor - erstellt Richtlinien, Richtliniensätze und Sammler. Die Administratorrolle führt die Testrichtlinie aus und erstellt Entitäten, die vom Zeitplanungsadministrator verwendet werden.
     - sn_itom_ccg.operator: Der Operator Governance für Cloud-Konfigurationen testet die Richtlinien und überprüft die Ergebnisse. Der Operator korrigiert auch Testergebnisse und Testergebnisgruppen.
     - sn_itom_ccg.scheduling_admin - richtet Governance für Cloud-Konfigurationen für die Accounts Microsoft Azure ein. Erstellt Scan-Konfigurationen und Scan-Zeitpläne. Hat Zugriffsrechte für Scan-Ergebnisse, um importierte Entitäten und Richtlinien anzuzeigen.
   - cspm_cloud_account_admin Diese Rolle erbt auch die Rolle sn_itom_ccg.scheduling_admin.
   - mid_server: Konfiguriert einen MID-Server.
   - sn_vulc.admin: Konfiguriert die Anwendung Konfigurations-Compliance, hat Einblick in alle Datensätze und kann Eigenschaften ändern. Weist Rollen in der Anwendung Konfigurations-Compliance zu. Weitere Informationen zu Rollen in der Anwendung

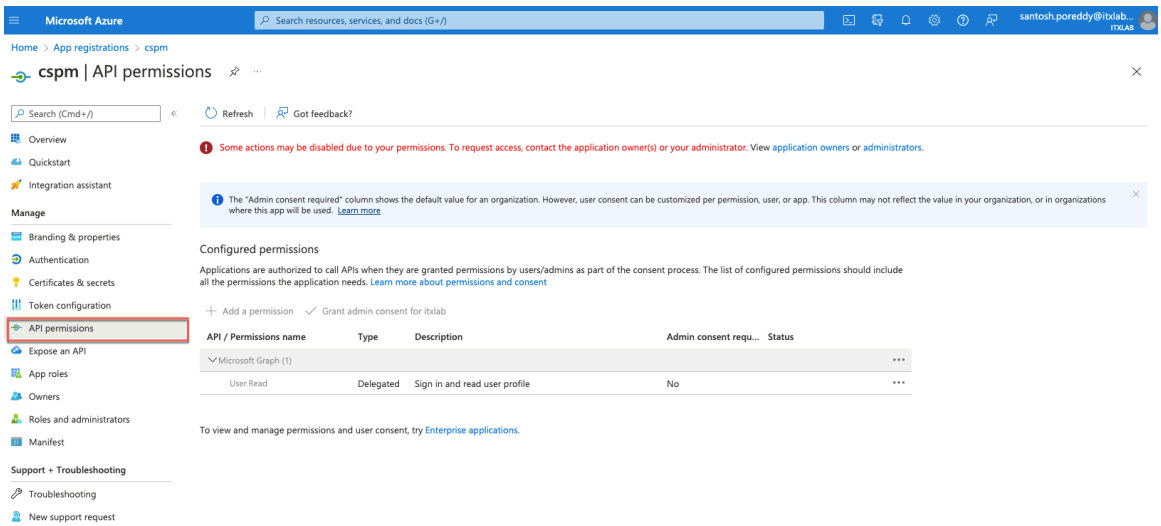
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance finden Sie unter Mit Konfigurations-Compliance installierte Komponenten.

- sn_vuln.admin: Konfiguriert die Anwendung Performance Analytics for Vulnerability Response.

Führen Sie die folgenden Schritte aus, um einen Scan-Datensatz zum Scannen der Assets in Ihrer Microsoft Azure -Umgebung zu erstellen.

6. Konfigurieren Sie in Ihrem Azure-Konto Richtlinien mit der erforderlichen Berechtigungsebene, um Zugriff auf die Ressourcen Microsoft Azure für Cloud-Discovery und Cloud Provisioning and Governance zu gewähren.
   Verwenden Sie die in der folgenden Abbildung gezeigte Seite, um Ihre Richtlinienberechtigungen zu erstellen. Diese Berechtigungen sind für diese Anwendung erforderlich.



In der Anwendung Konfigurations-Compliance sind die in der Anwendung enthaltenen Gruppen- und Zuweisungsregeln standardmäßig deaktiviert. Ein Benutzer mit sn_vulc.admin aktiviert diese Regeln.

7. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Gruppenregeln**.
8. Klicken Sie auf die **Regel Zuweisungsgruppe, Testregel,** um den Datensatz zu öffnen, und legen Sie das Feld Aktiv auf **wahr**fest.

   Diese Regel gruppiert die während des Audits erstellten Testergebnisse. Alle Testergebnisse für eine bestimmte Richtlinie, deren Rückgabewert für das Testergebnis falsch ist, werden in einer Testergebnisgruppe gruppiert.

   Standardmäßig werden Testergebnisgruppen der Benutzergruppe „CI-Support“ zugewiesen. Diese Zuweisungsregel ist standardmäßig deaktiviert.

9. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Zuweisungsregeln**.
10. Klicken Sie auf den Datensatz An CI-Supportgruppe zuweisen, um ihn zu öffnen, und klicken Sie auf das Kontrollkästchen **Aktiv**, um ihn zu aktivieren.

    Diese Regel weist die Testergebnisgruppen Benutzern in der CI-Supportgruppe zu. Weisen Sie dieser Gruppe Anwender zu, die an diesen Testergebnissen arbeiten sollen.

    Abhängig von Ihren internen Praktiken ist diese Standardzuweisungsregel möglicherweise nicht für die Zuweisung von Cloud-Konfigurationsproblemen in Ihrer Organisation nützlich. Unter Umständen möchten Sie stattdessen eine Zuweisungsregel erstellen, die Ihren Anforderungen entspricht. Sie können Cloud-Account-Metadaten verwenden, indem Sie von der Testergebnistabelle aus durch die Tabelle „Erkanntes Element“ laufen, um Zuweisungsregeln zu definieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Weitere Informationen zur Verwendung von Konfigurations-Compliancefinden Sie in der Konfigurations-Compliance -Dokumentation unter servicenow.com/docs.

11. Um die Audit-Ergebnisse in den Dashboards Performance Analytics for Vulnerability Response anzuzeigen, aktiviert ein Benutzer mit der Rolle sn_vuln.admin die Anwendung und aktiviert die Datensammler.
12. Navigieren zu **Performance Analytics** > **Datenerfasser** > **Aufträge** und suchen Sie die täglichen Sammleraufträge, um zu überprüfen, ob sie aktiviert sind.
    Sie haben das Setup für die Integration abgeschlossen. Sie sind bereit, Ihre Azure-Umgebung mit der CSPM-Anwendung zu scannen.

Cloud-Accounts werden mit der CSPM-Anwendung ServiceNow gescannt

In diesem Abschnitt wird beschrieben, wie Sie Sicherheitsscans für Ihre Cloud-Konten konfigurieren, um die Compliance Ihrer Ressourcen mit Benchmark-Frameworks zu überprüfen. Eine Beispielrichtlinie wird verwendet, um Ihnen diesen Prozess zu zeigen.

Vorbereitungen

Setup erforderlich: Dieses Beispiel beginnt mit der Erstellung eines Scan-Datensatzes. Wenn Sie die Informationen in Ihren Servicekonten für Microsoft Azureeinrichten oder überprüfen möchten, lesen Sie die Setup-Schritte in Installieren und aktivieren Sie die Anwendung CSPM Innovation Lab für Microsoft Azure.

Erforderliche Rolle: sn_vul.cspm_cloud_account_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Administration** > **Cloud-Account-Scans** um einen Scan-Konfigurationsdatensatz in der CSPM-Anwendung zu erstellen.
   Die Seite „Cloud-Account-Scan“ wird angezeigt.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.
   a. Geben Sie einen eindeutigen Namen für die Scan-Konfiguration ein.
   b. Geben Sie eine Kurzbeschreibung ein, um den Datensatz später zu finden.
   c. Wählen Sie **Cloud-Servicekonten** und dann die gewünschten Zielservicekonten aus.
   Sie haben diese Datensätze für Ihre Microsoft Azure -Accounts erstellt und in Governance für Cloud-Konfigurationeneingegeben.
4. Aktivieren Sie die Checkbox **Hintergrundprüfung**.
   Dadurch wird der Scan stündlich ausgeführt. Wenn das Kontrollkästchen nicht aktiviert ist, müssen Sie die Prüfung bei Bedarf starten.
5. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse** > **Alle**.
   Die Liste der Testergebnisgruppen (CTR#), die aus dem Richtlinien-Audit erstellt wurden, wird angezeigt.

   Es werden Testergebnisdatensätze für Ihre nicht konformen Cloud-Ressourcen erstellt. Wenn Verstöße behoben werden, werden Testergebnisdatensätze geschlossen.

6. Öffnen Sie einen Datensatz, um die folgenden Daten anzuzeigen:

   Testfeld

   Dieses Feld zeigt die Eins-zu-eins-Zuordnung zwischen der für das Audit verwendeten Richtlinie und dem Audit-Testdatensatz in Konfigurations-Compliancean. Klicken Sie,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um eine Vorschau des Testdatensatzes anzuzeigen, ihn zu öffnen und die Zitate (also die autorisierende Quelle) anzuzeigen. In diesem Beispiel ist die autorisierende Quelle Microsoft Azure (CIS Microsoft Azure Foundations Benchmark Version 1.4.0), und der Abschnitt, d. h. die Richtlinie, lautet 3.1.2. Stellen Sie sicher, dass „TLS-Mindestversion“ auf „Version 1.2“ festgelegt ist. (Automatisiert).

Jede Richtliniengruppe, zu der diese Richtlinie gehört, wird angezeigt. Eine Richtlinie kann in mehr als einer Richtliniengruppe enthalten sein. Außerdem wird die Anzahl der vom Audit generierten Testergebnisse angezeigt.

Feld „Konfigurationselement“

Diese Daten beziehen sich auf eine Ressource in Microsoft Azure.

Feld „Erkanntes Element“.

Ein erkanntes Element in Ihrem Now Platform ist der Ressource Microsoft Azure zugeordnet. Alle über die Ressource Microsoft Azure importierten Cloud-Metadaten, z. B. Region, Cloud-Account und Ressourcentyp, werden im Datensatz „Erkanntes Element“ gespeichert.

Registerkarte „Testergebnisgruppen“.

Standardmäßig gruppiert die Anwendung Konfigurations-Compliance die Testergebnisse in Testergebnisgruppen basierend auf einer falschen Rückgabe beim Audit. Für eine Ressource wird nur ein Datensatz pro Testergebnis erstellt, und er wird nach Datenimporten aktualisiert. Wenn die Konfigurationseinstellung für eine Ressource in Ihrer Microsoft Azure -Umgebung zwischen den Scans geändert wird, wird der Datensatz in Ihrer Instanz von Now Platform aktualisiert.

7. Um die importierten Daten zu überprüfen, können Sie zum Benutzerkonto Microsoft Azure zurückkehren.

In diesem Beispiel zeigt ein Häkchen bei diesem Account an, dass die minimale TLS-Version 1.0 ist. Dieser Status entspricht den Sicherheitsdaten, die über die Ressourcen und Ressourcengruppen aus der Cloud importiert wurden. Nachdem Sie die Einstellung geändert haben und die Ressource konform ist, werden Ihre Änderungen im nächsten Datenimport übernommen. Im folgenden Beispiel muss die TLS-Mindestversion für diese Ressource aktualisiert werden, bevor der zugehörige Testergebnisdatensatz geschlossen wird.

Zeigen Sie in den Performance Analytics für Vulnerability Response-Dashboards Azure CSPM-Auditdaten an

Diese Integration umfasst Dashboards in der Anwendung Performance Analytics for Vulnerability Response.

Vorbereitungen

Erforderliche Rolle: pa_viewer

Prozedur

1. Um das Dashboard anzuzeigen, navigieren Sie zu **Konfigurations-Compliance** > **Übersicht**.

Daten für die Dashboards werden täglich gesammelt. Um die Einstellungen zu ändern, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge**.

Hinweis:
Wenn Sie andere Schwachstellenintegrationen von Drittparteien ausführen, werden alle Ihre Schwachstellendaten und Audit-Ergebnisdaten zusammen in den Dashboard-Visualisierungen angezeigt. Sie können Ihre Filter festlegen, um die CSPM-Daten herauszufiltern.

Das Dashboard enthält drei Registerkarten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Asset-Kategorie
- Korrektur
- Genehmigungen

2. Klicken Sie auf eine Registerkarte, um die Daten anzuzeigen.
3. Die in den Daten enthaltenen autorisierenden Quellen werden unter den Datenvisualisierungen aufgelistet.

Erstellt eine anwenderdefinierte Richtlinie für Azure in CSPM

Erstellen Sie eine Richtlinie, um Ihre anwenderdefinierten Compliance-Standards zu implementieren.

Vorbereitungen

Erforderliche Rolle: sn_sec_cspm.cspm_security_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Konfigurationsrichtlinien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular zur Erstellung von anwenderdefinierten CSPM-Richtlinien

Feld	Beschreibung		
Richtlinienname	Eindeutiger Name der Richtlinie.		
Beschreibung	Details der Richtlinie.		
Ressourcentyp			
Cloud-Provider	Cloud-Bereitstellungsplattform für die Richtlinie.		
Ressourcentyp	Typ der Ressource in der Cloud-Umgebung. Wenn der Ressourcentyp nicht vorhanden ist, erstellen Sie einen Ressourcentyp gemäß den Konventionen von AWS oder Azure.		
Richtlinienbedingung			
Typ			
Bedingung	Bedingung zum Erstellen eines Testergebnisses. Betrachten Sie die folgenden Szenarien.		
	Konfigurationsschlüssel vorhanden?	Ressourcentyp vorhanden?	Nächste Schritte
	Ja	Ja, Ressourcentyp und die Flows zum Abrufen der Metadaten sind vorhanden. Beispiel für einen Subflow: CSPM: Azure Subscription Resource Collector (CSPM: Azure-Abonnement-Ressourcensammler).	Geben Sie die Bedingungen für die Richtlinie an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung		
	Nein	Ja	**a.** Erstellen Sie einen Konfigurationsschlüssel. **b.** Erstellen Sie einen Ressourcensammler. **c.** Erstellen Sie einen Konfigurationssammler. **d.** Geben Sie die Bedingungen für die Richtlinie an.
Schweregrad	Schweregrad der Richtlinie.		

4. Wählen Sie **Absenden** aus, um die anwenderdefinierte Richtlinie zu erstellen.

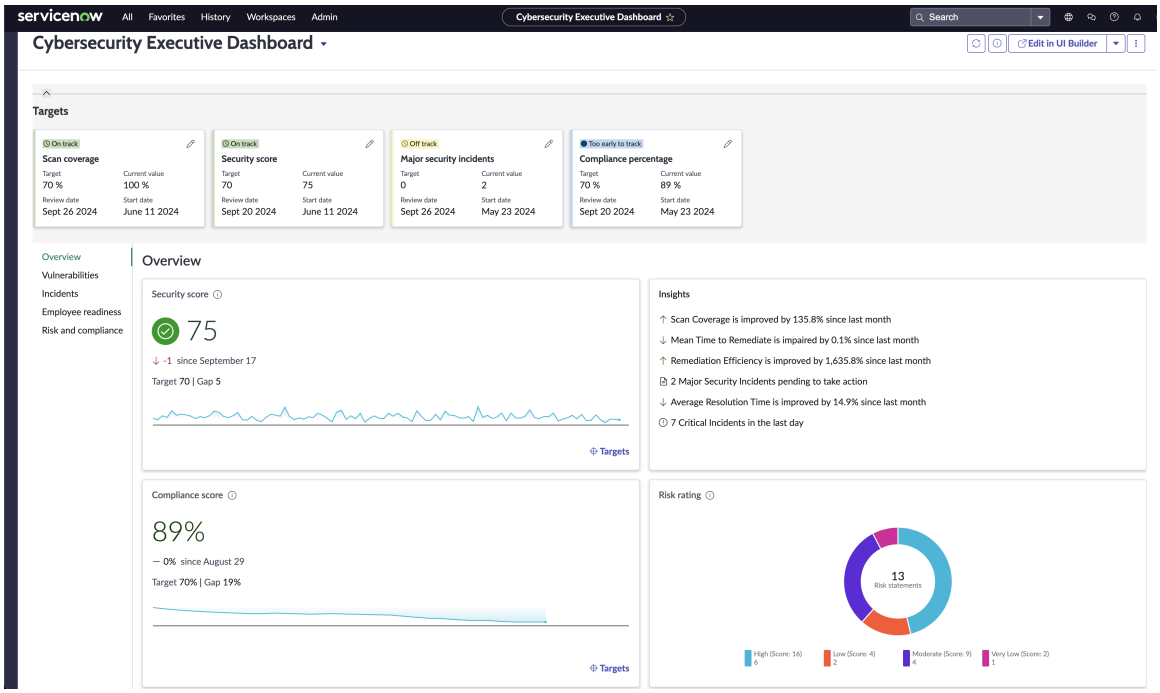
Cybersicherheits-Dashboard

Das Cybersecurity Executive Dashboard ist eine umfassende Lösung, die Chief Information Security Officers (CISOs) und Führungskräften im Bereich Cybersicherheit Einblick in die Sicherheitslage und die Sicherheitsinitiativen des Unternehmens verschafft. Das Dashboard fasst Daten aus verschiedenen Produkten innerhalb der Suite ServiceNow Security Operations Suite und Governance, Risk and Compliance (GRC) zusammen.

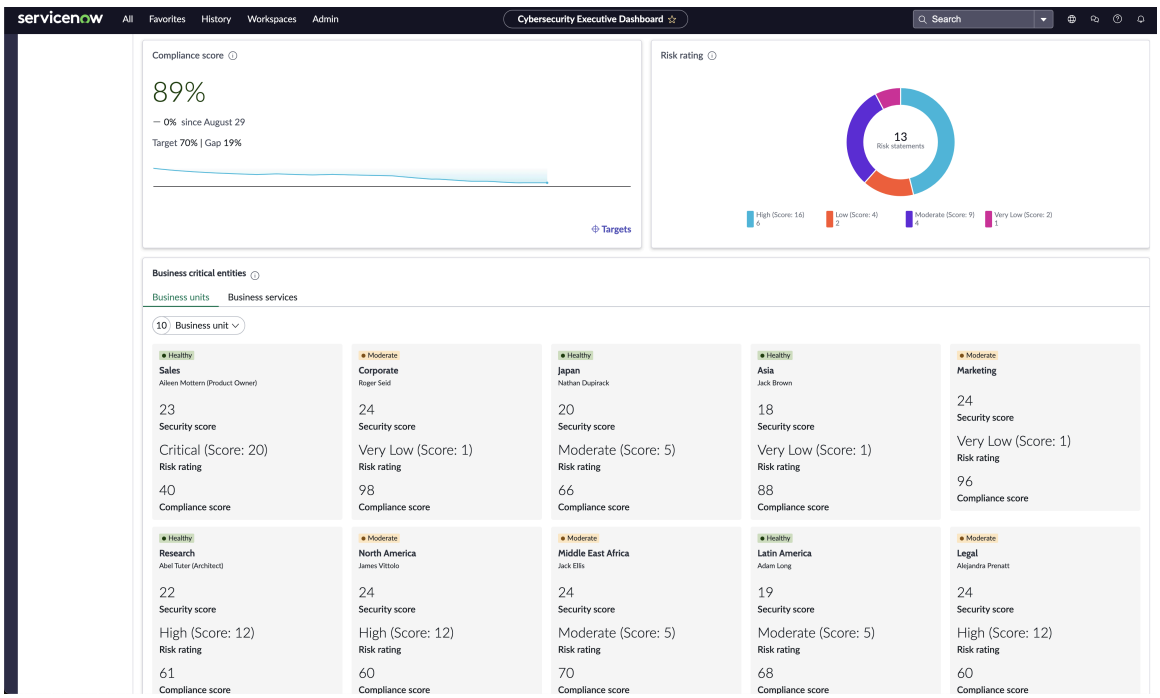
Das Dashboard bietet die folgenden Funktionen:

- Bewertung der Sicherheitslage im gesamten Unternehmen
- Sicherheits-, Risiko- und Compliance-Punktzahlen nach Geschäftsbereich
- Anpassbare Überwachung
- Einheitliche Ansicht der Sicherheitslandschaft einer Organisation
- Benchmarking
- Benutzerfreundliche Oberfläche
- Transparenz in Phishing-Simulationsmetriken von KnowBe4 und Microsoft Defender für Office 365

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Diese Funktionen ermöglichen eine proaktive Entscheidungsfindung durch schnellen Zugriff auf kritische Sicherheitsmetriken. Das macht sie zu einem unentbehrlichen Tool zur Verbesserung der allgemeinen Sicherheitsresilienz und -bereitschaft.



Erforderliche Now Platform-Rollen

- CISO (sn_bod.c iso) zum Anzeigen und Freigeben des Dashboards.
- sn_bod.c iso_admin zum Anzeigen, Freigeben des Dashboards und Konfigurieren von Gewichtungen für die Sicherheitslagenbewertung.
- GRC CISO-Benutzer (sn_grc_dashboards.grc_c iso_user), um Risiko- und Compliance-Berichte anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Greifen Sie auf das Cybersicherheits-Dashboard zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cybersicherheits-Dashboard** > **Cybersicherheits-Dashboard**.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Chief Information Security Officers (CISOs)	CISOs erhalten für ihre Organisationen Einblicke in Schwachstellenmanagement, Incident-Management, Sicherheitslage der Organisation, Phishing-Simulationsmetriken usw.

Datenvisualisierung

Hinweis:

Um mehr über ein Widget zu erfahren, wählen Sie das Informationssymbol ⓘ.

Ziele

Metriken	Typ	Beschreibung
Ziele	Prozentsatz	Zeigt das festgelegte Ziel für die Abdeckung durch eine Metrik an. Der Status der Ziele wird durch eine Farbcodierung angezeigt. Es werden alle Ziele angezeigt, deren Überprüfungsdatum entweder innerhalb der letzten 30 Tage liegt oder in der Zukunft liegt. Mit der Systemeigenschaft `sn_bod.show_targets_from` können Sie die Anzahl der Tage für die Anzeige von Zielen festlegen. Zusätzlich können diese Ziele bearbeitet werden. Weitere Informationen finden Sie unter Legen Sie Ziele fest.

Metriken	Typ	Beschreibung
Sicherheitspunktzahl	Einzelne Punktzahl	Gesamtpunktzahl der Sicherheitslage der Organisation

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Typ	Beschreibung
		unter Berücksichtigung von angreifbaren Elementen, Security Incidents, schwerwiegenden Security Incidents und Fehlkonfigurationen.
Einblicke	Hervorhebungen	Highlights des gesamten Dashboards.
Compliance-Bewertung	Einzelne Punktzahl	Stellt die Compliance-Situation des Unternehmens mithilfe der Compliance-Punktzahl bereit, die basierend auf dem Prozentsatz der konformen Steuerungen aus der Gesamtzahl der Steuerungen berechnet wird.
Risikopunktzahl	Einzelne Punktzahl	Gibt die Anzahl der Risikobeschreibungen basierend auf den Risikobewertungen an. Es hilft Unternehmen, die potenziellen Auswirkungen und Wahrscheinlichkeit verschiedener Risiken zu verstehen und diese Risiken zu priorisieren und zu verwalten.
Geschäftskritische Entitäten		
Geschäftsbereiche	Einzelne Punktzahl	Gesamtsicherheitspunktzahl der Geschäftsbereiche unter Berücksichtigung des Risikos im Zusammenhang mit Schwachstellen, Fehlkonfigurationen, Operational Technology(OT)-Schwachstellen, Security Incidents und schwerwiegenden Security Incidents. Die Integritätsbezeichnung der Geschäftsbereiche basiert nur auf der Sicherheitspunktzahl. Um zu sehen, wie diese Bezeichnungen zugewiesen werden, navigieren Sie zur Tabelle Risikopunktzahlgewichtungen [sn_sec_cmn_risk_score_weight_list.do], und suchen Sie nach einer Geschäftsentität. Bezeichnungen wie „In Ordnung“ werden basierend auf vordefinierten Wertbereichen zugewiesen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Typ	Beschreibung
		Beispielsweise wird eine Sicherheitspunktzahl zwischen 0 und 39 als fehlerfrei gekennzeichnet. Die Farbcodierung für diese Bezeichnungen ist in der Skripteinbindung UnifiedCISOutils angegeben. Sie können sowohl den Wertebereich als auch die Farben für die Bezeichnungen konfigurieren. Um zu sehen, wie die Namen des Geschäftsbereichs und der Geschäftsbereichsleiter zugewiesen sind, wechseln Sie zu **Alle** > **Organisation** > **Geschäftsbereiche**. **Hinweis:** Je nachdem, welche Plugins Sie aktiviert haben, können Sie auf die Compliance-Punktzahl, Risikopunktzahl und Sicherheitspunktzahl zugreifen. Um die Compliance- und Risikopunktzahlen anzuzeigen, müssen Sie die GRC-Plugins aktivieren. Um die Sicherheitspunktzahl anzuzeigen, müssen Sie die zugehörigen Plugins für Security Operations aktivieren. Weitere Informationen finden Sie im Abschnitt „Anwendungen für aktiv“.
Business-Services	Einzelne Punktzahl	Gesamtsicherheitspunktzahl der Business-Services unter Berücksichtigung des Risikos im Zusammenhang mit Schwachstellen, Fehlkonfigurationen, Operational Technology(OT)-Schwachstellen, Security Incidents und schwerwiegenden Security Incidents. Um zu sehen, wie diese Bezeichnungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Typ	Beschreibung
		zugewiesen werden, navigieren Sie zur Tabelle Risikopunktzahlgewichtungen [sn_sec_cmn_risk_score_weight_list.do], und suchen Sie nach einer Geschäftsentität. Bezeichnungen wie „fehlerfrei“, „mittel“ und „kritisch“ werden basierend auf vordefinierten Wertebereichen zugewiesen. Beispielsweise wird eine Sicherheitspunktzahl zwischen 0 und 39 als fehlerfrei gekennzeichnet. Die Farbcodierung für diese Bezeichnungen ist in der Skripteinbindung UnifiedCISOutils angegeben. Sie können sowohl den Wertebereich als auch die Farben für die Bezeichnungen konfigurieren. Um zu sehen, wie der Geschäftsbereich und der Geschäftsbereich-Leitername zugewiesen werden, wechseln Sie zu **Alle** > **Organisation** > **Geschäftsbereiche**. **Hinweis:** Je nachdem, welche Plugins Sie aktiviert haben, können Sie auf die Compliance-Punktzahl, Risikopunktzahl und Sicherheitspunktzahl zugreifen. Um die Compliance- und Risikopunktzahlen anzuzeigen, müssen Sie die GRC-Plugins aktivieren. Um die Sicherheitspunktzahl anzuzeigen, müssen Sie die zugehörigen Plugins für Security Operations aktivieren. Weitere Informationen finden Sie im Abschnitt „Anwendungen für aktiv“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen

Metriken	Typ	Beschreibung
Durchschnittliche Zeit bis zur Fehlerkorrektur (monatlich)	Liniendiagramm	Durchschnittliche Zeit, die in einem Monat für die Schließung von Schwachstellen und fehlgeschlagenen Testergebnissen für alle Assets (Hosts, Container und Anwendungen) benötigt wurde. Außerdem werden die folgenden Metriken bereitgestellt: • Ziel: Ziel, das in Tagen festgelegt wird, um die Schwachstellen zu beheben. • Abstand: Unterschied in Tagen zwischen der Ziel- und der tatsächlichen Zeit, die für die Korrektur der Schwachstellen benötigt wird. • Branchen-Benchmark: Durchschnitt der Metriken von Kollegen in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt Informationen zum Anzeigen der Benchmark-Punktzahlen finden Sie unter Benchmark-Punktzahlen aktivieren.
Durchschnittliches Alter aktiver Schwachstellen (monatlich)	Einzelne Punktzahl	Monatliches Durchschnittsalter aller drei Arten von angreifbaren Elementen. Sie bietet auch einen Vergleich des aktuellen Monatsalters mit dem Vormonat. Außerdem werden die folgenden Metriken bereitgestellt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

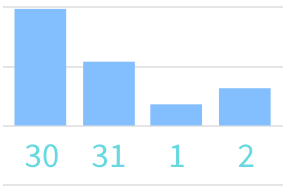
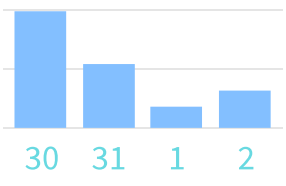
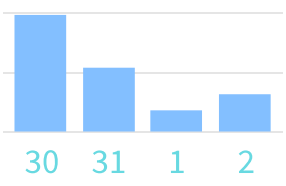
Schwachstellen (Fortsetzung)

Metriken	Typ	Beschreibung
		• Branchen-Benchmark: Durchschnitt der Metriken von Kollegen in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt • Ziel: Ziel, das in Tagen festgelegt wird, um die Schwachstellen zu beheben.
Effizienz der Fehlerbehebung (monatlich)	Einzelne Punktzahl	Prozentsatz der monatlich geschlossenen angreifbaren Elemente zu den monatlich aktiven angreifbaren Elementen. Außerdem werden die folgenden Metriken bereitgestellt: • Prozentuale Änderung gegenüber dem Vormonat. • Ziel: Ziel, das in Prozent festgelegt ist, um die Schwachstellen zu beheben. • Abstand: Abstand zwischen Ziel und aktueller Punktzahl. • Branchen-Benchmark: Durchschnitt der Metriken von Kollegen in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt
Durchschnittliches aktiver Schwachstellen nach Zuweisungsgruppe.	Mehrzeilig	Durchschnittliches Alter der aktiven Schwachstellen für jede Zuweisungsgruppe.
Schwachstellen nach Risikobewertung und Alter	Heatmap	Aufgliederung der aktiven Schwachstellen für Hosts, Container und Anwendungen nach Risikobewertung und Alter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen (Fortsetzung)

Metriken	Typ	Beschreibung
Einhaltung des Korrekturziels nach Zuweisungsgruppe	Vertikaler 	Verhältnis der Anzahl der innerhalb des Korrekturziels geschlossenen Schwachstellen und Fehlkonfigurationen zur Gesamtanzahl der geschlossenen Schwachstellen und Fehlkonfigurationen.
Scan-Abdeckung	Prozentsatz	Prozentsatz der in den letzten 90 Tagen gescannten Assets aller Assets im CMDB.
Assets gescannt im Vergleich zu ungescannt	Horizontale Leiste	Aufgliederung der in den letzten 90 Tagen gescannten Assets und der gesamten Assets in CMDB nach CI-Klasse
Assets gescannt	Horizontale Leiste	Assets, die in den letzten 90 Tagen auf Schwachstellen vs. Konfigurations-Compliance gescannt wurden.
Trend für aktive Funde der Stufen kritisch und hoch		Täglicher Trend von Schwachstellen und Fehlkonfigurationen mit Risikobewertung „Kritisch“ und „Hoch“.
Schwachstellen nach Asset-Kategorie und Risikobewertung	Vertikaler 	Aufgliederung der aktiven Schwachstellen und Fehlkonfigurationen nach Asset-Kategorie und Risikobewertung (kritisch, hoch und mittel).
Nach Grund und Zuweisungsgruppe zurückgestellte Funde	Vertikaler 	Aufgliederung der zurückgestellten aktiven Schwachstellen und Fehlkonfigurationen nach Zurückstellungsgrund und Zuweisungsgruppe.
Operative Technologien (OT)		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen (Fortsetzung)

Metriken	Typ	Beschreibung
Trend für aktive kritische und Schwachstellen mit hoher Anfälligkeit		Täglicher Trend der aktiven OT-Schwachstellen mit Risikobewertung „Kritisch“ und „Hoch“.
Durchschnittliche Zeit bis zur Fehlerkorrektur (monatlich)	Einzelne Punktzahl	Durchschnittliche Zeit, die zum Schließen von OT-Schwachstellen benötigt wird. Verhältnis des Gesamtalters der geschlossenen OT-Schwachstellen zur Gesamtzahl der OT-Schwachstellen. Außerdem werden die folgenden Metriken bereitgestellt: • Prozentuale Änderung gegenüber dem Vormonat. • Ziel: Ziel, das in Tagen festgelegt wird, um die Schwachstellen zu beheben. • Branchen-Benchmark: Durchschnitt der Metriken von Kollegen in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt Informationen zum Anzeigen der Benchmark-Punktzahlen finden Sie unter Benchmark-Punktzahlen aktivieren.
Schwachstellen nach Risikobewertung und Alter	Heatmap	Aufgliederung der aktiven OT-Schwachstellen nach Risikobewertung und Alter.
Durchschnittliches Alter aktiver Schwachstellen (monatlich)	Liniendiagramm	Monatliches Durchschnittsalter der angreifbaren OT-Elemente. Sie bietet auch einen Vergleich des aktuellen Monatsalters mit dem Vormonat.
Schwachstellen nach Status und Alter	Heatmap	Aufgliederung der aktiven OT-Schwachstellen nach Status und Alter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

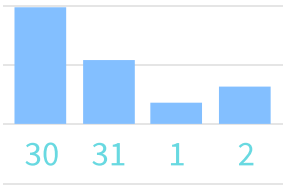
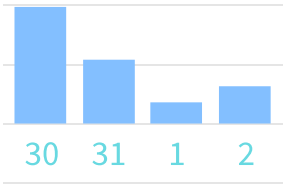
Incidents

Metriken	Typ	Beschreibung
Schwerwiegende Security Incidents	Einzelne Punktzahl	Anzahl der derzeit aktiven schwerwiegenden Security Incidents
Durchschnittliche Lösungszeit für Security Incidents (monatlich)	Einzelne Punktzahl	Monatliche durchschnittliche Lösungszeit für geschlossene Security Incidents in Tagen. Außerdem werden die folgenden Metriken bereitgestellt: • Prozentuale Änderung gegenüber dem Vormonat. • Ziel: Ziel in Tagen für die Korrektur der Security Incidents. • Lücke: Die Lücke zwischen den tatsächlichen Tagen, die für die Lösung benötigt werden, und dem für die Korrektur festgelegten Ziel. • Branchen-Benchmark: Durchschnitt der Metriken von Kollegen in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt
Durchschnittliche Zeit bis Beseitigung (monatlich)	Liniendiagramm	Monatliche durchschnittliche Lösung in Tagen zur Beseitigung von Security Incidents.
Durchschnittliche Zeit für Identifizierung (monatlich)	Einzelne Punktzahl	Monatliche durchschnittliche Lösung in Tagen zur Identifizierung der Security Incidents.
Durchschnittliche Zeit bis zur Eindämmung (monatlich)	Einzelne Punktzahl	Monatliche durchschnittliche Lösung in Tagen zur Eindämmung von Security Incidents.
Aktive Incidents nach Priorität und Kategorie	Heatmap	Anzahl der aktiven Security Incidents, kategorisiert nach Priorität und Kategorie

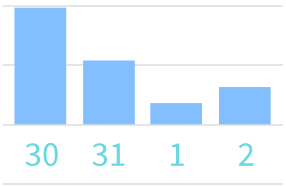
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incidents (Fortsetzung)

Metriken	Typ	Beschreibung
Trend geschlossener und offener Incidents	Vertikaler 	Aufgliederung geschlossener und offener Incidents.
Aktive Incidents nach Status	Vertikaler 	Aufgliederung aktiver Incidents basierend auf ihren Status.

Mitarbeiterbereitschaft

Metriken	Typ	Beschreibung
Übersicht über die monatliche Phishing-Simulation	Vertikaler 	Summe der Anwender, die in der Phishing-Simulation in den letzten sechs Monaten die Aktionen wie Öffnen, Klicken und Melden ausgeführt haben, zusammen mit der Summe der Gesamtanwender jeder Simulation.

Risiko und Compliance

Um die Widgets für Risiko und Compliance anzuzeigen, müssen Sie die GRC-Plugins aktivieren. Informationen zu GRC-Plugins finden Sie im Abschnitt Zu aktivierende Anwendungen. Informationen zu GRC-Widgets finden Sie unter Risiko- und Compliance-Dashboard für GRC: Metrics.

Indikatoren

Host-SLA: Geschlossen

Dieser Indikator wird täglich berechnet. Berücksichtigt das Gesamtalter aller Host-Schwachstellen, die am vorherigen Tag zum Zeitpunkt der Berechnung geschlossen wurden.

Container-SLA – Geschlossen

Dieser Indikator wird täglich berechnet. Berücksichtigt werden alle Container-Schwachstellen, die am vorherigen Tag zum Zeitpunkt der Berechnung geschlossen wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungs-SLA: Geschlossen

Dieser Indikator wird täglich berechnet. Er berücksichtigt das Gesamtalter aller Anwendungsschwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Testergebnis-SLA: Bestanden

Dieser Indikator wird täglich berechnet. Berücksichtigt werden alle Testergebnisschwachstellen, die am Vortag zum Zeitpunkt der Berechnung bestanden haben.

Host-SLA – Anzahl geschlossener

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Host-Schwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Container-SLA – Anzahl geschlossener

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Container-Schwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Anwendungs-SLA – Anzahl geschlossener

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Anwendungsschwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Testergebnis-SLA – Anzahl bestandener

Dieser Indikator wird täglich gemessen. Berücksichtigt die Anzahl aller Testergebnis-Schwachstellen, die am vorherigen Tag zum Zeitpunkt der Berechnung zuletzt bestanden wurden.

Gescannte Assets

Dieser Indikator wird täglich berechnet. Berücksichtigt wird die Summe der gescannten CIs aus der Tabelle sn_vul_analytics_scan_coverage_config, die die zuletzt innerhalb der letzten 90 Tage gescannten CIs für alle CMDB-CI-Klassen enthält.

Scannbare Assets

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Gesamt-CIs aus der Tabelle „sn_vul_analytics_scan_coverage_config“ für alle vorhandenen CMDB-CI-Klassen.

Angreifbare Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der aktiven angreifbaren Elemente zum Zeitpunkt der Berechnung.

Angreifbares Anwendungselement

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der aktiven angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung.

Angreifbares Container-Element

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der aktiven angreifbaren Container-Elemente zum Zeitpunkt der Berechnung.

Summiertes Alter der angreifbaren Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt das summierte Alter der aktiven angreifbaren Elemente zum Zeitpunkt der Berechnung.

Summiertes Alter der angreifbaren Anwendungselemente

Dieser Indikator wird täglich berechnet. Berücksichtigt das summierte Alter der aktiven angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung.

Offene angreifbare Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen angreifbaren Elemente zum Zeitpunkt der Berechnung.

Offene angreifbare Container-Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen angreifbaren Container-Elemente zum Zeitpunkt der Berechnung.

Offene angreifbare Anwendungselemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung.

Aktive Testergebnisse

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen Testergebnisse zum Zeitpunkt der Berechnung.

Zurückgestellte VITs

Dieser Indikator wird täglich berechnet. Verfügt über eine Indikatorquelle als angreifbares Host-Element.

Zurückgestellte AVITs

Dieser Indikator wird täglich berechnet. Er verfügt über eine Indikatorquelle als angreifbares Anwendungselement.

Zurückgestellte CVITs

Dieser Indikator wird täglich berechnet. Er verfügt über eine Indikatorquelle als angreifbares Container-Element.

Zurückgestellte Testergebnisse

Dieser Indikator wird täglich berechnet. Berücksichtigt werden Testergebnisse, die sich im Status „Zurückgestellt“ befanden.

Offene Konfigurationsprobleme – Testergebnisse

Dieser Indikator wird täglich berechnet. Er hat eine Indikatorquelle als Testergebnis für das Unified Vulnerability Response-Dashboard.

SI-Durchschnittliche Zeit bis zur Identifizierung

Dieser Indikator wird täglich berechnet. Berücksichtigt den Security Incident, bei dem die Definition von „Zeit zum Identifizieren“ zum Zeitpunkt der Berechnung ist.

SI – Durchschnittliche Dauer

Dieser Indikator wird täglich berechnet. Berücksichtigt den Security Incident, bei dem die Definition eine Incident-Statusdauer zum Zeitpunkt der Berechnung ist.

Anzahl der offenen schwerwiegenden Security Incidents

Dieser Indikator wird täglich berechnet. Er berücksichtigt offene schwerwiegende Security Incidents zum Zeitpunkt der Berechnung.

Anzahl der geschlossenen Security Incidents

Dieser Indikator wird täglich berechnet. Er berücksichtigt geschlossene Security Incidents zum Zeitpunkt der Berechnung.

Geschlossene angreifbare Anwendungselemente

Dieser Indikator wird täglich berechnet. Berücksichtigt geschlossene angreifbare Anwendungselemente zum Zeitpunkt der Berechnung.

Geschlossene angreifbare Container-Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt geschlossene angreifbare Container-Elemente zum Zeitpunkt der Berechnung.

Geschlossene angreifbare Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt geschlossene angreifbare Elemente zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für angreifbares Elemente abrufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Elemente zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für angreifbares Container-Element abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Container-Elemente zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für angreifbare Anwendungselemente abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Anwendungselemente zum Zeitpunkt der Berechnung.

Summierte Risikopunktzahl von VITs

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen von angreifbaren Elementen zum Zeitpunkt der Berechnung.

Summierte Risikopunktzahl von AVIs

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen von angreifbaren Anwendungselementen zum Zeitpunkt der Berechnung.

Summierte Risikopunktzahl von CVIs

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen von angreifbaren Containerelementen zum Zeitpunkt der Berechnung.

Summierte Risikopunktzahl der Fehlkonfigurationen

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen von Testergebnissen zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für SI-Incidents abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximalen Risikopunktzahlen von Security Incidents zum Zeitpunkt der Berechnung.

Max. Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximalen Risikopunktzahlen für eine Fehlkonfiguration von Testergebnissen zum Zeitpunkt der Berechnung.

Ruft die durchschnittliche Risikopunktzahl für Fehlkonfigurationstestergebnisse ab

Dieser Indikator wird täglich berechnet. Berücksichtigt die durchschnittlichen Risikopunktzahlen für eine Fehlkonfiguration von Testergebnissen zum Zeitpunkt der Berechnung.

Anzahl der offenen Security Incidents

Dieser Indikator wird täglich berechnet. Er berücksichtigt offene Security Incidents zum Zeitpunkt der Berechnung.

Phishing-Übersicht

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der Sicherheitssimulationsmetriken zum Zeitpunkt der Berechnung.

Aggregierte MTTR

Berechnet die durchschnittliche Zeit, die zum Schließen von Schwachstellen (Hosts, Container und Anwendungen) benötigt wurde, und die Zeit, die zum Schließen der Testergebnisse benötigt wurde, in Tagen. [[Host-SLA – Geschlossen]] + [[Anwendungs-SLA – Geschlossen]] + [[Container-SLA – Geschlossen]] + [[Testergebnis-SLA – Bestanden]]) / ([[Host-SLA – Anzahl geschlossener]] + [[Anwendungs-SLA – Anzahl geschlossener]] + [[Testergebnis-SLA – Anzahl bestandener]] + [[Container-SLA – Anzahl geschlossener]])

Aktuelle Scan-Abdeckung

Berechnet den Prozentsatz anhand des Verhältnisses zwischen der Anzahl der gescannten Elemente und der Gesamtanzahl der Elemente, die im selben Zeitraum gescannt werden konnten. var scannableItems = [[Gescannte Elemente]];var scannableItems = [[Scannbare Elemente]];var

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

res;if (scannedItems == 0)res = 0;elseres = scannableItems / scannableItems * 100;if (res > 100)res = 100;res;

Durchschnittliches Alter aktiver angreifbarer Elemente

Berechnet das durchschnittliche Alter aller aktiven angreifbaren Elemente (Hosts, Container und Anwendungen) in Tagen. ([[Summiertes Alter der angreifbaren Elemente]] + [[Summiertes Alter der angreifbaren Anwendungselemente]] + [[Summiertes Alter der angreifbaren Container-Elemente]])/([[Angreifbare Elemente]] + [[Angreifbare Anwendungselemente]] + [[Angreifbare Container-Elemente]])

Aktive VITs nach Alter und Risikobewertung

Berechnet die Gesamtanzahl aller aktiven angreifbaren Elemente (Hosts, Container und Anwendungen), kategorisiert nach Alter und Stufe der Risikobewertung. [[Offene angreifbare Elemente]] + [[Offene angreifbare Container-Elemente]] + [[Offene angreifbare Anwendungselemente]]

Zurückgestellte Probleme

Berechnet die Gesamtanzahl aller angreifbaren Elemente (Hosts, Container, Anwendungen und Testergebnisse) mit dem Status „Zurückgestellt“. [[Zurückgestellte VITs]] + [[Zurückgestellte AVITs]] + [[Zurückgestellte Testergebnisse]] + [[Zurückgestellte CVITs]]

Durchschnittliche Lösungszeit der geschlossenen Security Incidents

Berechnet die durchschnittliche Zeit, die zum Schließen der Security Incidents benötigt wurde, in Tagen. ([[Summierte Dauer der geschlossenen Security Incidents]]/[[Anzahl der geschlossenen Security Incidents]])/24

Sicherheitspunktzahl

Berechnet täglich die Gesamtsicherheitsbewertungen. Sie wird basierend auf der zusammengefassten Risikopunktzahl berechnet. varsecPostureRating = 100 – [[Sicherheitspunktzahl]]; Sek. PostureRating;

Sicherheitspunktzahl (Geschäftsbereiche)

Berechnet die endgültige Rollup-Risikopunktzahl, indem die Rollup-Risikopunktzahl von angreifbaren Elementen, Fehlkonfigurationen, Security Incidents und schwerwiegenden Security Incidents mit den jeweiligen Gewichtungen multipliziert wird, die aus der Rollup-Tabelle für die Sicherheitslage abgerufen werden. var numMajorIncidents = [[Anzahl offener schwerwiegender Security Incidents]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; sonst majorSIRiskScore = 0; rollUpRiskScore = ([[Rollup-Risikopunktzahl für Schwachstellen und Fehlkonfiguration]] * 20 + [[Rollup-Risikopunktzahl für OT-Schwachstelle]] * 20 + [[Maximale Risikopunktzahl für SI-Incidents abrufen]] * 20 + majorSIRiskScore * 40)/100 ; rollUpRisikoPunktzahl;

Sicherheitspunktzahl (Business-Services)

Berechnet die endgültige Rollup-Risikopunktzahl, indem die Rollup-Risikopunktzahl von angreifbaren Elementen, Fehlkonfigurationen, Security Incidents und schwerwiegenden Security Incidents mit den jeweiligen Gewichtungen multipliziert wird, die aus der Rollup-Tabelle für die Sicherheitslage abgerufen werden. var numMajorIncidents = [[Anzahl offener schwerwiegender Security Incidents – Services]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; sonst majorSIRiskScore = 0; rollUpRiskScore = ([[Rollup-Risikopunktzahl für Schwachstelle und Fehlkonfiguration – Services]] * 20 + [[Rollup-Risikopunktzahl für OT-Schwachstelle – Services]] * 20 + [[Maximale Risikopunktzahl für SI-Incidents abrufen – Services]] * 20 + majorSIRiskScore * 40)/100; rollUpRisikoPunktzahl;

Schwachstellen-Rollup-Risikopunktzahl

Berechnet die zusammengefasste Risikopunktzahl der Schwachstelle, indem die maximale Risikopunktzahl, die durchschnittliche Risikopunktzahl der angreifbaren Elemente und die Anzahl der angreifbaren Elemente mit ihren jeweiligen Gewichtungen multipliziert werden. Var maxRiskScore = 100; var count = [[Aktive VITs nach Alter und Risikobewertung]];

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Var countRiskScore; if (0 == Anzahl) countRiskScore = 0; Else if (Anzahl > 10.000) countRiskScore = maxRiskScore; Else if (Anzahl > 1000) countRiskScore = (maxRiskScore * 0,80); Else if (Anzahl > 100) countRiskScore = (maxRiskScore * 0,60); Else if (Anzahl > 10) countRiskScore = (maxRiskScore * 0,40); Else countRiskScore = (maxRiskScore * 0,20); var verulRiskScore = ([[Maximale Punktzahl für alle angreifbaren Elemente abrufen]] * 0 + [[Durchschnittliche Risikopunktzahl aller angreifbaren Elemente]] * 100 + countRiskScore * 0)/100; SchwachstellenRisikoPunktzahl

Maximale Risikopunktzahl von allen angreifbaren Elementen abrufen

Berechnet die zusammengefasste Risikopunktzahl der Schwachstelle, indem die maximale Risikopunktzahl, die durchschnittliche Risikopunktzahl der angreifbaren Elemente und die Anzahl der angreifbaren Elemente mit ihren jeweiligen Gewichtungen multipliziert werden. var maxScoreForVI = [[Maximale Risikopunktzahl für angreifbare Elemente abrufen]], maxScoreForCVI = [[Maximale Risikopunktzahl für angreifbares Container-Element abrufen]], maxScoreForAVI = [[Maximale Risikopunktzahl für angreifbare Anwendungselemente abrufen]], maxScore; if (maxScoreForVI >= maxScoreForCVI && maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI; Else if (maxScoreForCVI >= maxScoreForVI && maxScoreForCVI >= maxScoreForAVI) maxScore = maxScoreForCVI; sonst maxScore = maxScoreForAVI; maxScore;

Durchschnittliche Risikopunktzahlen aller angreifbaren Elemente

Berechnet die durchschnittliche Risikopunktzahl für alle angreifbaren Elemente (Hosts, Container und Anwendungen). var summedRiskScore = [[Summierte Risikopunktzahl von VITs]] + [[Summierte Risikopunktzahl von AVIs]] + [[Summierte Risikopunktzahl von CVIs]], avgRiskScore; var totalVulCount = [[Offene angreifbare Elemente]] + [[Offene angreifbare Anwendungselemente]] + [[Offene angreifbare Container-Elemente]]; if(sumedRiskScore == 0) avgRiskScore = 0; Else if(totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount; durchschn. Risikopunktzahl;

Fehlkonfiguration – Rollup-Risikopunktzahl

Berechnet die Rollup-Risikopunktzahl der Fehlkonfiguration anhand der Testergebnisse, die als Fehlgeschlagen, Fehler oder Unbekannt kategorisiert sind. Var maxRiskScore = 100; var count = [[Offene Konfigurationsprobleme – Testergebnisse]]; Var countRiskScore; if (0 == Anzahl) countRiskScore = 0; Else if (Anzahl > 10.000) countRiskScore = maxRiskScore; Else if (Anzahl > 1000) countRiskScore = (maxRiskScore * 0,80); Else if (Anzahl > 100) countRiskScore = (maxRiskScore * 0,60); Else if (Anzahl > 10) countRiskScore = (maxRiskScore * 0,40); Else countRiskScore = (maxRiskScore * 0,20); var missRiskScore = ([[Maximale Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen]] * 0 + [[[[Durchschn. Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen]] * 100 + countRiskScore * 0)/100; missRiskScore;

Durchschnittliche Zeit bis Beseitigung

Berechnet die durchschnittliche Zeit, die für die Beseitigung von Security Incidents benötigt wird, in Tagen [[SI – Durchschnittliche Dauer > Status des Security Incidents = Beseitigen]]/ 1440

Durchschnittliche Zeit für Identifizierung

Berechnet die durchschnittliche Zeit in Tagen, die für die Identifizierung von Security Incidents benötigt wird. [[SI – Durchschnittliche Zeit für Identifizierung]] / 1440

Durchschnittliche Zeit bis zur Eindämmung

Berechnet die durchschnittliche Zeit in Tagen, die benötigt wird, um Security Incidents einzudämmen. [[SI – Durchschnittliche Dauer > Security Incident-Status = Eindämmen]] / 1440

Einhaltung des Korrekturziels

Berechnet den monatlichen Prozentsatz der Einhaltung des Korrekturziels aus Testergebnissen, angreifbaren Elementen, angreifbaren Container-Elementen und angreifbaren Anwendungselementen. Die Zieleinhaltung wird durch die Anzahl der Elemente bestimmt, die das festgelegte Ziel erfüllt haben. ([[Testergebnis-SLA – Anzahl bestandener“ > Korrekturstatus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(einheitlich) = Ziel erfüllt]] + [[Container-SLA – Anzahl geschlossener > Korrekturstatus (einheitlich) = Ziel erfüllt]] + [[Anwendungs-SLA – Anzahl geschlossener > Korrekturstatus (einheitlich) = Ziel erfüllt]] + [[Host-SLA – Anzahl geschlossener > Korrekturstatus (einheitlich) = Ziel erfüllt]]) / ([[Testergebnis-SLA – Anzahl bestandener]] + [[Container-SLA – Anzahl geschlossener]] + [[Anwendungs-SLA – Anzahl geschlossener]] + [[Host-SLA – Anzahl geschlossener]]) * 100

Effizienz der monatlichen Fehlerbehebung (alle angreifbaren Elemente)

Berechnet den monatlichen Prozentsatz der geschlossenen angreifbaren Elemente, angreifbaren Container-Elemente und angreifbaren Anwendungselemente im Gegensatz zu den neu identifizierten Elementen. var closedItems = [[Host-SLA – Anzahl geschlossener]] + [[Container-SLA – Anzahl geschlossener]] + [[Anwendungs-SLA – Anzahl geschlossener]] + [[Testergebnis-SLA – Anzahl bestandener]];

var newItems = [[Host-VITs, die gestern geöffnet/erneut geöffnet wurden]] + [[Container-VITs, die gestern geöffnet/erneut geöffnet wurden]] + [[Anwendungs-VITs, die gestern geöffnet/erneut geöffnet wurden]] + [[Testergebnisse, die gestern geöffnet/erneut geöffnet wurden]];

var res = 0;if (closedItems == 0) res = 0;else if (newItems .=0)res = closedItems / newItems * 100;if (res > 1000) res = 1000; res;

Host-VITs, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Er berücksichtigt die angreifbaren Host-Elemente, die zuletzt am Vortag zum Zeitpunkt der Berechnung geöffnet wurden.

Anwendungs-VITs, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Er berücksichtigt die angreifbaren Anwendungselemente, die zuletzt am Vortag zum Zeitpunkt der Berechnung geöffnet wurden.

Container-VITs, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Berücksichtigt werden die angreifbaren Container-Elemente, die zuletzt am vorherigen Tag zum Zeitpunkt der Berechnung geöffnet wurden.

Testergebnisse, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Er berücksichtigt die Testergebnisse, die zuletzt am vorherigen Tag zum Zeitpunkt der Berechnung sichtbar waren.

Angreifbare OT-Elemente

Dieser Indikator wird täglich berechnet. Sie berücksichtigt aktive angreifbare OT-Elemente, die zum Zeitpunkt der Berechnung vorhanden sind.

Summierte Dauer der geschlossenen OT-Schwachstelle

Dieser Indikator wird täglich berechnet. Berücksichtigt das Gesamtalter aller OT-Schwachstellen, die am Tag der Berechnung geschlossen wurden.

Geschlossene angreifbare OT-Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die angreifbaren OT-Elemente, die am Tag der Berechnung geschlossen werden.

Durchschnittliches Alter der aktiven angreifbaren OT-Elemente

Berechnet das durchschnittliche Alter der angreifbaren OT-Elemente ([[Summiertes Alter der angreifbaren OT-Elemente]]/[[Angreifbare OT-Elemente]])

Aufgliederungen

- Geschäftsbereich
- Business-Services

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Risikobewertung
- Altersbereich
- Zuweisungsgruppe (einheitlich)
- Nachbesserungszielstatus (geschlossen)
- Asset-Klasse
- Asset-Kategorie
- Risikobewertung (einheitlich)
- Grund für Zurückstellung (einheitlich)
- Status des Security Incidents
- Priorität von Security Incident
- Kategorie von Security Incident
- Phishing-Ereignis
- Grund für Zurückstellung – Nicht geschlossen (einheitlich)

Zu aktivierende Anwendungen

Sie müssen die folgenden Anwendungen aktivieren, um die Punktzahl in den Widgets auszufüllen. Je nach verwendeter Anwendung müssen Sie die abhängigen Anwendungen aktivieren.

Bei Verwendung von	Aktivieren
Vulnerability Response	• Performance Analytics for Vulnerability Response • Gemeinsame Vulnerability Response-Komponenten • Vulnerability Response • Vulnerability Response und Configuration Compliance für Container • Konfigurations-Compliance
Operative Technologien	Vulnerability Response für operative Technologie
Phishing-Integrationen	• Security Simulation and Training Integration for SecOps • KnowBe4 Integration for SecOps • Integration von Microsoft Defender für Office365 für SecOps

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Verwendung von	Aktivieren
Security Incident Response	• Performance Analytics für Security Incident Response • Security Incident Response • Management schwerwiegender Sicherheits-Incidents
Governance, Risk und Compliance	• GRC: Allgemeine Dashboard-Elemente • GRC: Arbeitsbereich für Risikomanagement • GRC: Erweitertes Risikomanagement • GRC: Arbeitsbereich für Compliance-Management

Geplante Aufgaben für die Datensammlung

Die folgenden geplanten Aufgaben werden ausgeführt, um automatisch Punktzahlen für neue Daten zu sammeln.

Geplante Aufgabe	Häufigkeit	Beschreibung
Benchmark-Punktzahlen hochladen	Bei Bedarf	Sammelt Punktzahlen von der Instanz und postet sie an die zentrale Instanz. Die Benchmark-Algorithmen berechnen die besten Punktzahlen der Branche.
Benchmark-Punktzahlen herunterladen	Bei Bedarf	Lädt die Benchmark-Punktzahlen herunter. Sie ist in der Tabelle „Benchmark-Punktzahlen“ [sn_bm_client_score_list] verfügbar.

Benchmark-Punktzahlen aktivieren

Rufen Sie Benchmark-Punktzahlen ab, indem Sie Ihre Instanz bei der -Zentralinstanz ServiceNow registrieren. Letzterer verwaltet Informationen mehrerer Branchen, um die Benchmark-Punktzahl bereitzustellen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zu Benchmarking finden Sie unter Benchmarks overview .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um Ihre Instanz bei der Zentralinstanz zu registrieren, gehen Sie wie folgt vor:

   a. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.

   b. Wählen Sie die Systemeigenschaft *sn_bm_client.central_instance_url* aus.

   c. Geben Sie im Feld **Wert** die URL der zentralen Benchmark-Instanz ein.

   Hinweis:
   Wenn die Instanz bereitgestellt wird, werden Ihre Details automatisch an die Zentralinstanz übertragen.

   d. Wählen Sie im Widget **Aktivieren aus,** um zu validieren und eine Verbindung zur zentralen Instanz herzustellen.

2. Um Ihre Punktzahl in die zentrale Instanz hochzuladen, gehen Sie wie folgt vor:

   a. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**

   b. Wählen Sie die geplante Aufgabe *Upload the benchmark scores* aus.

   c. Wählen Sie **Aktualisieren**.
   Die Punktzahlen werden in die zentrale Instanz hochgeladen. Die regelmäßigen Aufgaben werden jedoch von der zentralen Instanz einmal im Monat ausgeführt, um die Punktzahlen in den Dashboard-Widgets zu aktualisieren.

3. Um die Punktzahl aus der zentralen Instanz herunterzuladen, gehen Sie wie folgt vor:

   a. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**

   b. Wählen Sie die geplante Aufgabe *Download the benchmark scores* aus.

   c. Wählen Sie **Jetzt ausführen**.
   Die Punktzahlen sind in der Tabelle Benchmark-Punktzahlen [sn_bm_client_score_list] verfügbar, die sich in den Dashboard-Widgets widerspiegelt.

Legen Sie Ziele fest

Legen Sie Ziele in Tagen fest, um Schwachstellen, Security Incidents und Fehlkonfigurationen zu beheben.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Wählen Sie im Widget **Ziele**, oder wählen Sie das Symbol **Ziele** auf der Seite „KPI-Details“.
2. Wählen Sie die Schaltfläche **Für alle aus**.
3. Geben Sie im Feld **Neuer Wert** die Anzahl der Tage ein, in denen das Ziel erreicht werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie das Zielstartdatum aus.
5. Wählen Sie das Zieldatum der Überprüfung aus.
6. Wählen Sie **Aktualisieren**.

Security Simulation and Training Integration for Security Operations

Verstärken Sie die Verteidigung Ihres Unternehmens gegen schwerwiegende Cybersicherheitsbedrohungen, indem Sie Phishing-Integrationen in das Cybersecurity Executive Dashboard integrieren. Die Phishing-Integrationen verbessern das Cybersicherheits-Dashboard durch die nahtlose Einbindung von Daten aus Phishing-Simulationstools von Drittanbietern wie KnowBe4 und Microsoft Defender for Office 365.

Die folgenden Integrationen erweitern die Fähigkeiten des Cybersicherheits-Dashboards für Führungskräfte und bieten eine einheitliche Perspektive auf das Sicherheitsniveau, die Bereitschaft der Mitarbeiter und die Anfälligkeit für Phishing-Angriffe Ihrer Organisation:

- KnowBe4-Integration
- Microsoft Defender für Office 365-Integration

Konfigurieren Sie die Knowbe4-Integration

Durch die Integration mit KnowBe4, einer führenden Schulungsplattform für Cybersicherheitsbewusstsein, erhalten Sie sofortige Einblicke in die Anfälligkeit Ihrer Mitarbeiter für Phishing-Angriffe. Durch die KnowBe4-Integration können Sie Trends und Verbesserungsbereiche in Ihren Schulungsprogrammen für Cybersicherheit identifizieren, die allgemeine Phishing-Resilienz überwachen und die Sicherheitsmaßnahmen Ihres Unternehmens proaktiv stärken.

Vorbereitungen

Erforderliche Rolle: sn_sec_phish.admin und sn_sec_phish_kb4.kb4_admin

Prozedur

1. Navigieren zu **Alle** > **KnowBe4-Integration** > **KnowBe4-Konfigurationen**.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Details aus:

Formular „KnowBe4-Konfiguration“.

Feld	Beschreibung
Integrationsinstanz	Name der Integrationsinstanz. Wählen Sie die Integrationsinstanz über das Suchsymbol aus.
Basis-URL	URL zur Integration mit KnowBe4.
API-Schlüssel	API-Schlüssel, der vom KnowBe4-Konto abgerufen wurde.
Seite	Seitennummer, von der Simulationen abgerufen werden sollen.
Seitengröße	Anzahl der Simulationen, die enthalten sein sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie **Neu** aus, wenn keine Integrationsinstanz verfügbar ist.

b. Füllen Sie im Formular die Details aus:

Formular „Integrationsinstanz".

Feld	Beschreibung
Name	Name für die Integrationsinstanz.
Anwendung	Name der Anwendung (KnowBe4 Integration for SecOps)
Integration	KnowBe4 ist der Standard.
Aktiv	Standardmäßig ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv.
Beschreibung	Kurze Beschreibung der Integrationsinstanz.

4. Wählen Sie **Absenden**.
5. Navigieren zu **Alle** > **Sicherheitssimulation und -training** > **Integrationen**.
6. Wählen Sie die Knowbe4-Integration aus.
7. Wählen Sie **Jetzt ausführen aus**, um KnowBe4 auszuführen und Daten aus diesem zu sammeln.

Konfigurieren Sie die Microsoft Defender-Integration für die Office 365-Integration

Durch die nahtlose Integration mit Microsoft Defender für Office 365 erhalten Sie wertvolle Einblicke in Phishing-Simulationsmetriken direkt im Cybersicherheits-Dashboard.

Vorbereitungen

Erforderliche Rolle: sn_sec_phish_msatk.ms_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Simulieren eines Phishing-Angriffs und zum Einrichten eines Mandanten finden Sie unter:

- Simulieren Sie einen Phishing-Angriff mit dem Angriffssimulationstraining
- Erste Schritte mit dem Angriffssimulationstraining
- Richten Sie einen Mandanten ein

Prozedur

1. Navigieren zu **Alle** > **Microsoft Attack-Integration** > **Microsoft Attack-Konfigurationen**.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Details aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Microsoft Attack-Konfiguration“.

Feld	Beschreibung
Integrationsinstanz	Name der Integrationsinstanz. Wählen Sie die Integrationsinstanz über das Suchsymbol aus.
Mandanten-ID	Mandanten-ID der im Microsoft Azure-Portal erstellten Anwendung.
Client-ID	Client-ID der im Microsoft Azure-Portal erstellten Anwendung.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der im Microsoft Azure-Portal erstellten Anwendung.
Lesezeichen	Datum, ab dem die Simulationen abgerufen werden müssen.
Token-URL	Basis-URL, von der aus das Token für den Zugriff auf die Microsoft Simulations-API erstellt wird.
Gesamte Simulations-URL	Basis-URL der Microsoft Simulations-API.

a. Wählen Sie **Neu** aus, wenn keine Integrationsinstanz verfügbar ist.

b. Füllen Sie im Formular die Details aus:

Formular „Integrationsinstanz“.

Feld	Beschreibung
Name	Name der Integrationsinstanz.
Anwendung	Name der Anwendung (Microsoft Defender für Office 365).
Integration	Drittpartei-Integrationsreferenz (Microsoft Attack-Integration).
Aktiv	Standardmäßig ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv.
Beschreibung	Kurze Beschreibung der Integrationsinstanz.

4. Wählen Sie **Absenden**.

5. Navigieren zu **Alle** > **Sicherheitssimulation und -training** > **Integrationen**.

6. Wählen Sie die Microsoft Attack-Integration aus.

7. Wählen Sie **Jetzt ausführen** aus, um die Ausführung auszuführen und Daten von Microsoft zu sammeln.

Risiko- und Compliance-Dashboard für GRC: Metrics

Das Dashboard für Risiko und Compliance bietet Compliance- und Risikoanwendern einen umfassenden Überblick über Risiko- und Complianceinformationen in einem einzigen Dashboard, das sie bei wichtigen Entscheidungen unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können von einem einheitlichen Cybersicherheits-Dashboard zum Risiko- und Compliance-Dashboard navigieren, um die Risiko- und Compliance-Metriken von Governance, Risk und Compliance -Anwendungen anzuzeigen.

Das Dashboard bietet Funktionen wie:

- Compliance-Übersicht
- Risikoübersicht
- Datenschutzübersicht
- Übersicht über die Geschäftskontinuität
- Drittpartei-Risiko
- Audit-Übersicht

Voraussetzungen für den Zugriff auf das Dashboard für Risiko und Compliance

Wichtig:
Sie müssen über primären Zugriff auf Cybersicherheits-Dashboard verfügen, um das Funktions-Plugin „Cybersecurity and Risk“ zu aktivieren, mit dem Sie auf das Dashboard „Risiko und Compliance“ zugreifen können.

Eine neue funktionale Domäne wird eingeführt, um Cybersicherheits- und Risikodaten zu trennen. Sie können das Plugin „Cybersicherheit und Risiko“ aktivieren, indem Sie die Schaltfläche UI-Aktion **aktivieren** auswählen. Standardmäßig ist diese funktionale Domäne inaktiv.

Erforderliche Now Platform-Rollen

Die Hauptbenutzerrolle GRC ist „sn_grc_dashboards.grc_c iso_user“. Sie kann die Berichte im Dashboard „Risiko und Compliance“ anzeigen. Diese Rolle enthält:

- sn_compliance.reader
- sn_risk.reader

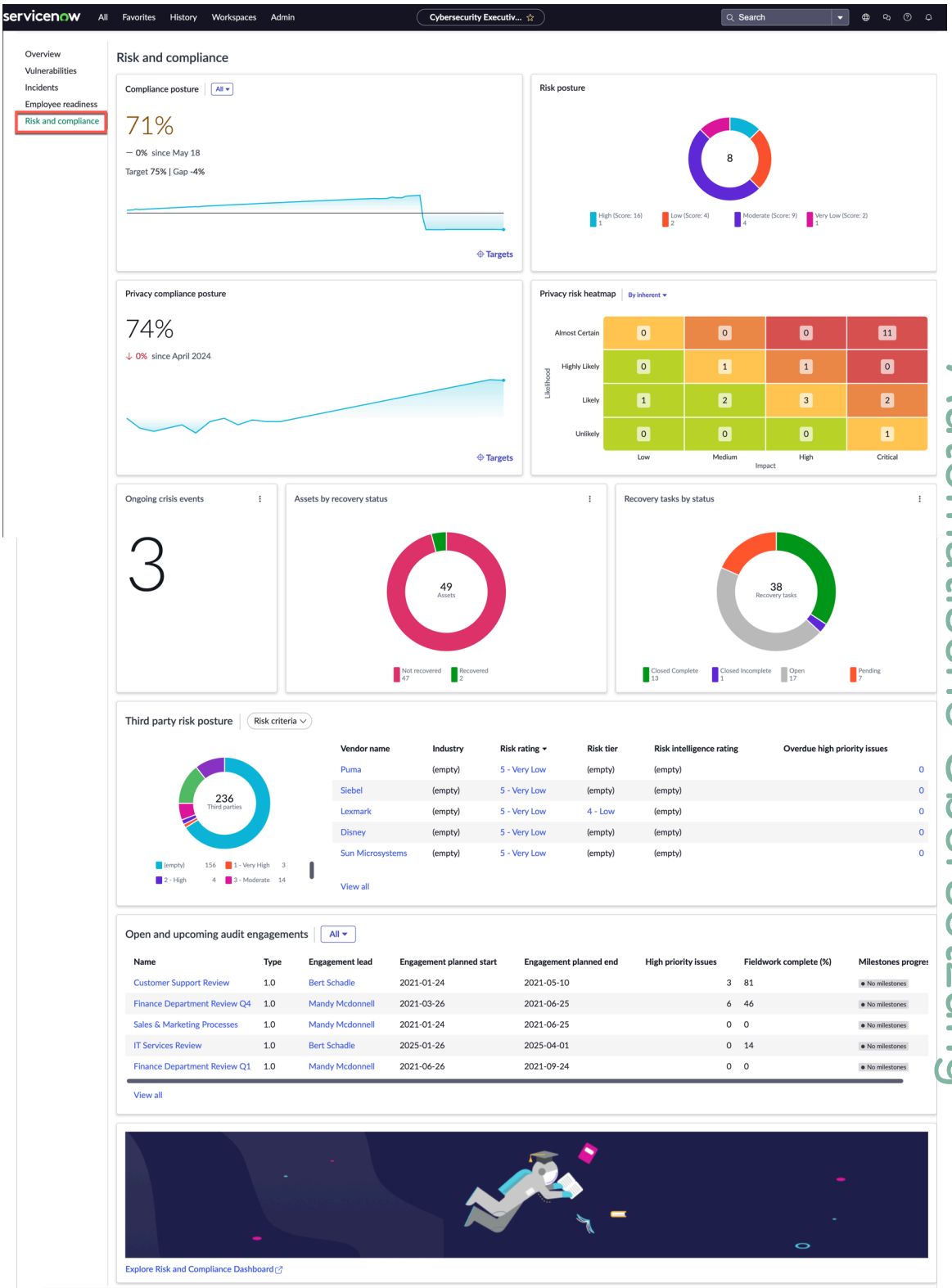
Hinweis:
Sie müssen jedoch über die Rolle sn_bod.cso verfügen, um sich beim Cybersicherheits-Dashboard anzumelden, es anzuzeigen und freizugeben. Von dort aus können Sie zum Risiko- und Compliance-Dashboard navigieren.

Greifen Sie auf das Dashboard für Risiko und Compliance zu

1. Um auf das Dashboard für Risiko und Compliance zuzugreifen, navigieren Sie zu **Alle** > **Cybersicherheits-Dashboard** > **Cybersicherheits-Dashboard**.
2. Wählen Sie in der Liste links im Dashboard die Option **Risiko- und Compliance** -Bezeichnung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einheitliches Cybersicherheits-Dashboard für Risiko- und Compliance-Metriken



Automatische Übersetzung

3. Um Ihre Daten zu visualisieren und die Berichte und Lösungen anzuzeigen, die im für den Benutzer entwickelten Dashboard verfügbar sind, wählen Sie die Bezeichnung Risiko- und Compliance-Dashboard erkundenaus.

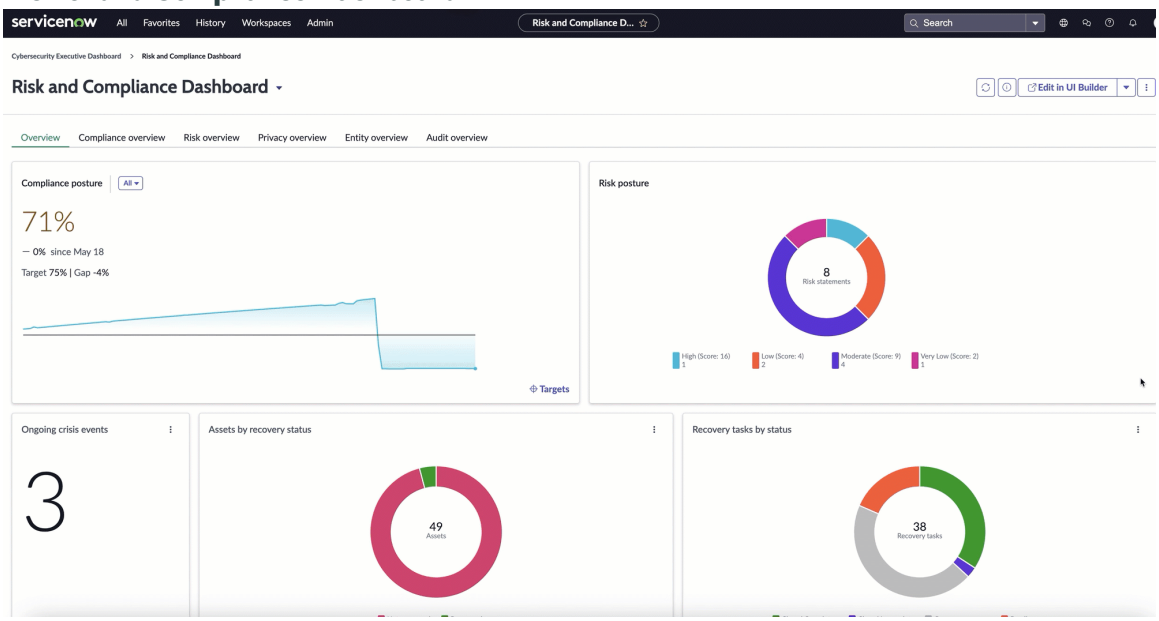
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte und Lösungen des Dashboards„Risiko und Compliance“.

Das Dashboard für Risiko und Compliance ist ein einheitliches Dashboard, das dem Chief Information Security Officer umfassende analytische Daten zu Berichten aus den wichtigsten GRC-Anwendungen bereitstellt, um die Compliance und die Risikosituation des Unternehmens zu verstehen. Das -Dashboard fasst Daten aus verschiedenen Produkten der Anwendungssuite ServiceNow GRC zusammen.

Hinweis:
Alle Berichte sind nur verfügbar, wenn die entsprechenden Arbeitsbereiche installiert sind.

Risiko- und Compliance-Dashboard



Erforderliche Now Platform-Rollen

Für Compliance-bezogene Berichte

Der Anwender muss über die Rollen sn_grc_dashboards.grc_c iso_user und sn_bod.c iso verfügen.

Für risikobezogene Berichte

Der Anwender muss über die Rollen sn_grc_dashboards.grc_c iso_user und sn_bod.c iso verfügen.

Für Berichte im Zusammenhang mit Business Continuity Management

Der Anwender muss über die Rollen sn_bcm.viewer und sn_bod.cso verfügen.

Für Berichte im Zusammenhang mit Drittparteirisiken

Der Anwender muss über die Rollen sn_vdr_risk_asmt.vendor_assessment_reviewer und sn_bod.c iso verfügen.

Für datenschutzbezogene Berichte

Der Anwender muss über die Rollen sn_privacy.analyst und sn_bod.c iso verfügen.

Für Audit-bezogene Berichte

Der Anwender muss über die Rollen sn_audit_ws.auditor und sn_bod.c iso verfügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Greifen Sie auf das Risiko- und Compliance-Dashboard zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cybersicherheits-Dashboard** > **Cybersicherheits-Dashboard**.

Indikatoren

Compliance-Situation

- Compliance-Prozentsatz: Formelindikator, der die Compliance-Situation darstellt.
- Alle Steuerungen: Automatisierter Indikator, der den Formelindikator unterstützt.
- Konforme Steuerungen: Automatisierter Indikator, der den Formelindikator unterstützt.

Compliance-Situation für Datenschutz

PA-Indikator: Prozentsatz der Compliance-Bewertung der Verarbeitungsaktivität.

Aufgliederungen

Funktionale Domäne

Berichte

Hinweis:
Alle Berichte sind nur verfügbar, wenn die entsprechenden Arbeitsbereiche installiert sind.

Registerkarte „Übersicht“

Titel	Typ	Quelltabelle	Beschreibung
Compliance-Situation	Liniendiagramm	Steuerung [sn_compliance_control]	Stellt den Compliance-Managern Cybersicherheit und Risiko sowie IT-Risiko- und Compliance-Situation basierend auf Datenanalysen bereit.
Risikosituation	Ringdiagramm	Die Quelltabellen lauten wie folgt: • Risiko [sn_risk_risk] • Detailliertes aggregiertes Risiko [sn_risk_advanced_risk_assessment_result] (Wenn die Anwendung Erweitertes Risikomanagement installiert und	Gibt die Risikoanzahl basierend auf den Risikoeinstufungen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Übersicht“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
		die erweiterte Risikobewertung aktiviert ist	
Laufende Krisenereignisse	Einzelne Punktzahl	Wiederherstellungsereignis [sn_recovery_event], bei dem der Ereignistyp „actual“ ist	Zeigt die Gesamtzahl der laufenden Krisenereignisse an, die weder genehmigt noch geschlossen wurden.
Assets nach Wiederherstellungsstatus	Ringdiagramm	Assets [sn_recovery_event_asset]	Stellt die Gesamtzahl der Assets für laufende Krisenereignisse gruppiert nach ihrem Wiederherstellungsstatus bereit, einschließlich Assets, die wiederhergestellt wurden und derer, bei denen dies nicht der Fall ist.
Wiederherstellungsaufgaben nach Status	Ringdiagramm	Wiederherstellungsaufgaben [sn_recovery_event_task]	Stellt den Status von Wiederherstellungsaufgaben in verschiedenen Status für laufende Krisenereignisse bereit.

Registerkarte „Compliance-Übersicht“.

Titel	Typ	Quelltabelle	Beschreibung
Regulatorische Dokumente	Ringdiagramm	Regulatorisches Dokument [sn_compliance_authority_document]	Stellt Daten von konformen und nicht konformen regulatorischen Dokumenten im Diagramm bereit. Die Liste enthält Details zu den regulatorischen Dokumenten, ihre einzelnen Compliance-Punktzahlen in Prozent, die Anzahl der Probleme mit hoher Priorität und die Ausnahmen mit hohem Risiko für die regulatorischen Dokumente sowie die Anzahl der konformen Fälle.
Richtlinien	Ringdiagramm	Richtlinie [sn_compliance_policy]	Gibt die Anzahl der konformen und nicht konformen Richtlinien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Compliance-Übersicht“. (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			im Diagramm an. Die Liste enthält Details zu den Richtlinien, ihre jeweilige Compliance-Punktzahl in Prozent, die Anzahl der Probleme mit hoher Priorität und Risikoausnahmen, die für jede Richtlinie ausgelöst wurden, und die Anzahl der konformen Fälle.

Registerkarte „Risikoübersicht“.

Titel	Typ	Quelltabelle	Beschreibung
Risikosituation	Ringdiagramm	Die Quelltabellen lauten wie folgt: • Risiko [sn_risk_risk] • Detailliertes zusammengefasstes Risiko [sn_risk_advanced_risk_assessment_result] (wenn die Anwendung Erweitertes Risikomanagement installiert ist und die erweiterte Risikobewertung aktiviert ist)	Gibt die Risikoanzahl basierend auf den Risikoeinstufungen an.
Risikosituation	Liste	GRC-Inhaltsstatus [sn_grc_content_reports]	Stellt die Risikobewertung für jedes Organisationsrisiko bereit, um die Gesamtergebnisse der Risikobewertung zu verstehen. Diese Bewertungen helfen Unternehmen, die potenziellen Auswirkungen und Wahrscheinlichkeit verschiedener Risiken zu verstehen und diese Risiken zu priorisieren und zu verwalten. Die Karte Risikostellung hebt außerdem die folgenden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Risikoübersicht“. (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			Informationen für jedes Risiko hervor: • **Risikobereitschaft**: Wert der Risikobereitschaft definiert. • **Probleme mit hoher Priorität**: Die Anzahl der Probleme mit Priorität ist als „Hoch“ definiert. • **Überfällige Risikoantwortaufgaben**: Anzahl der überfälligen Risikoantwortaufgaben. • **KRI-Verstoß in %**: Prozentsatz der Schlüsselrisikoindikatoren (Key Risk Indicators, KRI), die ihre vordefinierten Schwellenwerte oder Grenzwerte überschritten haben.
Risikostellung der Drittpartei	Ringdiagramm	Drittparteirisiken [sn_grc_dashboards_third_party_risk]	Gibt die Risikobewertung für jede Drittpartei an. Die Risikobewertung ist die Gesamtbewertung, die die Punktzahlen und Bewertungen aus allen Bewertungen berücksichtigt, die für eine Drittpartei oder einen Lieferanten durchgeführt wurden. Auf der Karte „Drittpartei-Risikostellung“ werden außerdem die folgenden Informationen für jede Drittpartei oder jeden Lieferanten hervorgehoben:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Risikoübersicht“. (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			• **Risikokriterien**: Gruppe von Risikodomänen (in anderen Plattformfunktionen manchmal auch als Risikobereiche bezeichnet), die für einen bestimmten Typ von Drittpartei gelten. • **Risikostufe**: Wert, der basierend auf den Antworten bestimmt wird, die nach Abschluss einer Bewertung des inhärenten Risikos (IRQ) gesammelt wurden. • **Risk Intelligence-Bewertung**: Aggregat aller von Risk Intelligence-Anbietern gesammelten Punktzahlen. • **Überfällige Risikoantwortaufgaben**: Anzahl der überfälligen Risikoantwortaufgaben.

Registerkarte „Datenschutzübersicht“.

Titel	Typ	Quelltabelle	Beschreibung
Compliance-Situation für Datenschutz	Linie	PA-Indikator: Prozentsatz der Compliance-Bewertung der Verarbeitungsaktivität [pa_indicators]	Gibt die Compliance-Situation nach Monat an und wird anhand der Compliance-Gesamtpunktzahl für alle Verarbeitungsaktivitäten dargestellt.
Überfällige Probleme hoher Priorität	Einzelne Punktzahl	Probleme [sn_grc_issue]	Bietet eine fokussierte Übersicht über alle überfälligen Datenschutzprobleme mit hoher Priorität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Datenschutzübersicht“. (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			Sie ermöglicht die schnelle Identifizierung und Lösung kritischer Aufgaben, um Compliance und Datenschutz sicherzustellen.
Heatmap für Datenschutzrisiken	Heatmap	Risikobewertungsmethode [sn_risk_advanced_risk_assessment_methodology]	Stellt die Bewertungsdaten für Datenschutzrisiken in Form einer Heatmap bereit. Datenschutzrisikobewertungen sind detaillierte Bewertungen, die durchgeführt werden, wenn die Kritikalitätspunktzahl hoch ist. Bewerten Sie jedes Risiko, das mit der Verarbeitungsaktivität verbunden ist, und kennen Sie die aggregierte Risikopunktzahl für die Verarbeitungsaktivität. Nachdem Sie die Datenschutzrisiken bewertet haben, können Sie die Datenschutzrisikosituation in der Risiko-Heatmap anzeigen.

Registerkarte „Entitätsübersicht“.

Titel	Typ	Quelltabelle	Beschreibung
Entitäten	Liste	Compliance-Status von Entitäten [sn_compliance_entities_reports]	Stellt die Zusammenfassung der Risiken bereit, die direkt mit der Entität verknüpft sind und zur Gesamtrisikobewertung der Entität beitragen. Die Liste zeigt auch die Compliance-Bewertung von Entitäten sowie Probleme mit hoher Priorität und Risikoausnahmen an, die aufgrund nicht konformer Steuerungen ausgelöst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Entitätsübersicht“. (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			werden, die der Entität zugeordnet sind.

Registerkarte „Audit-Übersicht“

Titel	Typ	Quelltabelle	Beschreibung
Offene und bevorstehende Audit-Interaktionen	Liste	Interaktion [sn_audit_engagement]	Stellt eine Liste offener und bevorstehender Audit-Interaktionen bereit. Die Liste enthält auch Details zum Interaktionsleiter für jedes regulatorische Dokument, die geplanten Start- und Enddaten jeder Interaktion, Probleme mit hoher Priorität, den Prozentsatz der abgeschlossenen Feldarbeit und die in Bearbeitung befindlichen Meilensteine.

Filter

Name	Typ	Beschreibung
Risikokriterium	Bericht	Je nachdem, welche Risikokriterien Sie auswählen, werden im Ringdiagramm und in der Liste die Drittparteien oder Lieferanten in diesen Risikobereichen angezeigt.

Threat Intelligence-Sicherheitszentrum

Die Plattform Threat Intelligence-Sicherheitszentrum (TISC) bietet eine Technologielösung für die Zusammenfassung, Verwaltung und Operationalisierung von Threat Intelligence.

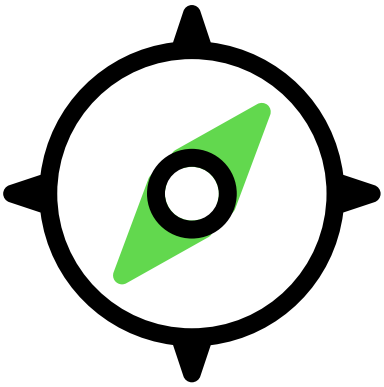
Erste Schritte

Klicken Sie auf eine Kachel, um zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

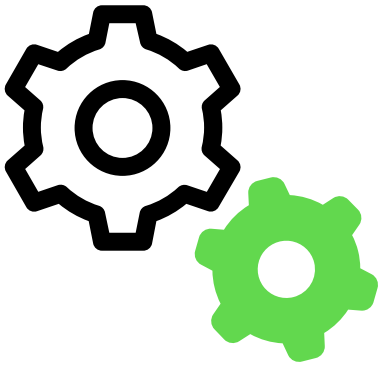
Automatische Übersetzung

Untersuchen



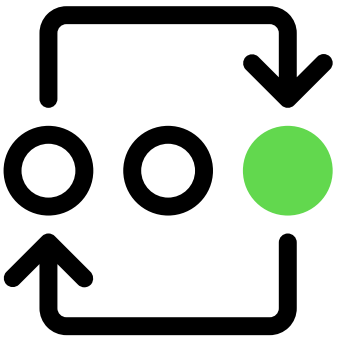
Erfahren Sie, wie das Threat Intelligence-Sicherheitszentrum Ihnen mit seinen wichtigsten Funktionen und Vorteilen helfen kann.

Konfigurieren



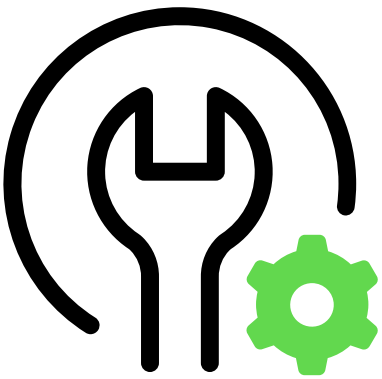
Richten Sie das Threat Intelligence-Sicherheitszentrum entsprechend Ihren spezifischen Anforderungen ein, und konfigurieren Sie es.

integrieren



Integrieren Sie in das Threat Intelligence-Sicherheitszentrum

Verwalten



Verwalten und passen Sie Ihr Threat Intelligence-Sicherheitszentrum an.

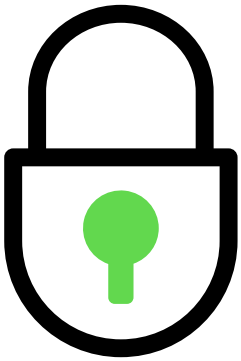
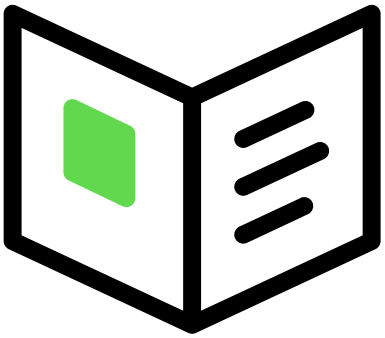
Verwenden

Verwalten Sie Ihre Threat Intelligence-Sicherheitszentrum-Bibliothek und -Objekte.

Berichtsvorlagen

Verwalten Sie Ihre Fallverwaltungsberichte, und passen Sie sie an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE ATT&CK-Repository	Archiv	Referenz
		
Verwalten Sie MITRE ATT&CK-Repository-Daten.	Verwalten Sie Datenarchivierungs- und -löschregeln.	Rufen Sie zusätzliche Informationen zum Threat Intelligence-Sicherheitszentrum ab.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Durch die Installation Threat Intelligence-Sicherheitszentrum von (sn_sec_tisc) werden alle abhängigen Anwendungen von ServiceNow Storeautomatisch installiert.

Weitere Ressourcen

Besuchen Sie das Security Incident Response Forum unter ServiceNow Community.

Problembehandlung und Hilfe

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Threat Intelligence-Sicherheitszentrum erkunden

Threat Intelligence-Sicherheitszentrum (TISC) ermöglicht Ihnen die Zusammenarbeit mit den Threat Intelligence-Teams und verfügt über mehrere Funktionen zum Sammeln und Verarbeiten verschiedener Threat Intelligence-Feeds sowie einen Arbeitsbereich zum Analysieren, Zusammenarbeiten, Bearbeiten und Freigeben der erforderlichen Informationen.

Sehen Sie sich eine Übersicht über die Anwendung Threat Intelligence-Sicherheitszentrum an.

https://player.vimeo.com/video/1020328039?h=33e58d6e14&badge=0&autopause=0&player_id=0&app_id=58479

Das Threat Intelligence-Sicherheitszentrum wird durch Funktionen zur Verwaltung der Datenerfassung und -verarbeitung wie DE-Duplizierung, Normalisierung und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenfassung, Analyse von Threat Intelligence und Verbreitung von Threat Intelligence sowie eines Arbeitsbereichs erweitert, der die Administrationsaufgaben bereitstellt.

Schlüsselfunktionen

Im Folgenden finden Sie die wichtigsten Funktionen des Threat Intelligence Security Center (TISC), die in den weiteren Abschnitten ausführlich erläutert werden:

- Datensammlung aus verschiedenen Quellen und in verschiedenen Formaten.
- Datenaggregation aus verschiedenen Feeds, einschließlich STIX, XML, JSON und OpenIOC.
- Ergänzungsfunktionen, einschließlich der Entfernung von falsch positiven Meldungen, der Konfidenz/Bewertung von Indikatoren, der Validierung von Indikatoren und des Hinzufügens von kontextbezogenen Informationen.
- Ein anwenderdefinierter Rechner für die Bedrohungsbewertung für eine differenzierte Bedrohungsbewertung.
- Integration interner Intelligenz aus VR, SIR, Assets, Services und CMDB.
- Bedrohungssuche mit Fallverwaltungs- und Aufgabenfunktionalitäten.
- Benutzerspezifische Dashboards, die auf die Persona der Bedrohungsinformationen zugeschnitten sind.
- Tools für die grafische Visualisierung zum Verständnis von Threat Intel-Daten.
- Ein dedizierter Threat Intel Analyst Workspace für optimierte Abläufe
- Korrelationsregeln zum automatischen Herstellen von Beziehungen zwischen erkennbaren Elementen.
- Das System kann alle erkennbaren Elemente automatisch aus den hochgeladenen Dateien identifizieren und extrahieren.
- Integration von Premium-Feeds zur Verbesserung der Bedrohungsinformationen
- Ermöglicht Benutzern die Zuordnung von MITRE ATT&CK-Informationen zu Datensätzen in der Threat Intelligence-Bibliothek und Fallverwaltung.
- Integration mit SIR- und Datenmigrationsfunktionen von Threat Intelligence zum Threat Intelligence-Sicherheitszentrum.

TISC-Schlüsselterminologie

Die nachfolgend definierten Begriffe werden im gesamten Threat Intelligence Security Center (TISC) verwendet.

Terminologiedefinitionen

Terminologie	Definition
Datenverarbeitung	Eine Threat Intelligence Platform (TIP) ist eine Technologielösung, die Threat Intelligence-Daten aus verschiedenen Quellen und Mustern sammelt, aggregiert und organisiert. Threat Intelligence sind die Daten, die gesammelt, verarbeitet und analysiert werden, um die Ziele und das Angriffsverhalten eines Bedrohungsakteurs zu verstehen.
Erkennbare Elemente	Erkennbare Elemente stellen zustandsbehaftete Eigenschaften (z. B. den MD5-Hash einer Datei oder den Wert eines Registrierungsschlüssels) oder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Terminologiedefinitionen (Fortsetzung)

Terminologie	Definition
	messbare Ereignisse (z. B. die Erstellung eines Registrierungsschlüssels oder das Löschen einer Datei) dar, die für den Betrieb von Computern und Netzwerken relevant sind . Weitere Informationen finden Sie unter Erkennbare Elemente.
Indikatoren	Indikatoren enthalten ein Muster, mit dem verdächtige oder böswillige Cyberaktivitäten erkannt werden können. Beispielsweise kann ein Indikator verwendet werden, um eine Reihe schädlicher Domänen darzustellen und die STIX-Mustersprache zu verwenden, um diese Domänen anzugeben. Die Indikator-SDO enthält eine einfache Textbeschreibung, die Kill Chain-Phasen, in denen das Verhalten erkannt wird, ein Zeitfenster, in dem der Indikator gültig oder nützlich ist, und eine erforderliche **Mustereigenschaft** zum Erfassen eines strukturierten Erkennungsmusters. Weitere Informationen finden Sie unter Indikatoren.
Objekte	Definiert den Satz von STIX Domain Objects (SDOs), die jeweils einem eindeutigen Konzept entsprechen, das häufig in Cyber Threat Intelligence (CTI) dargestellt wird. Mit SDOs und STIX-Beziehungsobjekten (STIX Relationship Objects, SROs) als Bausteine können Einzelpersonen umfassende und umfassende Cyberbedrohungsinformationen erstellen und teilen. Weitere Informationen finden Sie unter TISC-Bibliotheks-Repository.
Beziehungen	Eine Beziehung ist eine Verknüpfung zwischen zwei erkennbaren Elementen oder zwei SDOs oder einem erkennbaren Element und SDO, die beschreibt, wie die Objekte miteinander verknüpft sind. Beziehungen können mithilfe eines externen STIX-Beziehungsobjekts (STIX Relationship Object, SRO) oder in einigen Fällen durch bestimmte Eigenschaften dargestellt werden, die eine Bezeichnerreferenz speichern, die eine eingebettete Beziehung umfasst. Weitere Informationen finden Sie unter Beziehungsobjekte.

Domänentrennung und Threat Intelligence-Sicherheitszentrum

Domänentrennung wird für Threat Intelligence-Sicherheitszentrum unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Umfasst alle Aspekte des **Basis** -Supports.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

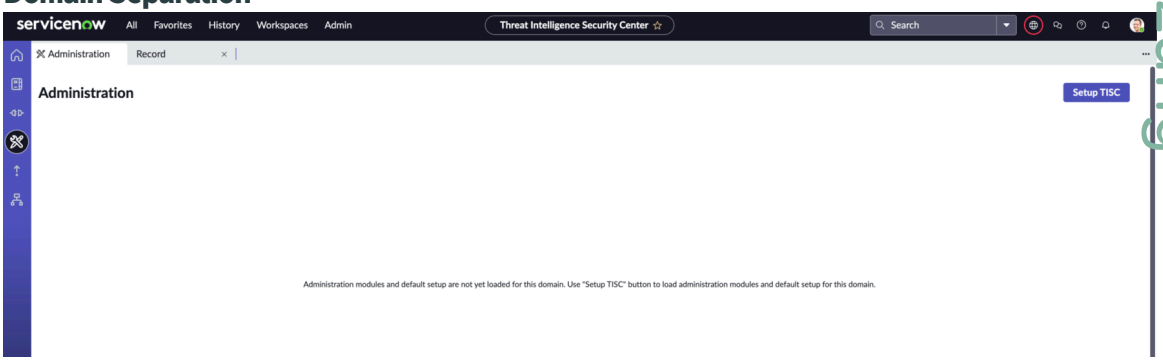
Übersicht

Domain Separation ist für alle Funktionen von Threat Intelligence-Sicherheitszentrumaktiviert.

So funktioniert Domain Separation in Threat Intelligence-Sicherheitszentrum

- Alle konfigurationsbezogenen Datensätze, die im Basissystem bereitgestellt werden, werden in der globalen Domäne bereitgestellt. Falls die Instanz domänengetrennt ist, wird Anwendern im **Administrationsmodul** des TISC-Arbeitsbereichs eine explizite Schaltfläche **„TISC einrichten“** angezeigt. Klicken Sie auf diese Schaltfläche, um die vom Basissystem bereitgestellten globalen Domänenkonfigurationen in die entsprechenden Domänen zu klonen.

Domain Separation



Hinweis:
Anwender sollten nur domänenspezifische Konfigurationsdatensätze aktivieren oder ändern und keine Konfigurationsdatensätze in der globalen Domäne aktivieren oder ändern.

- Im Basissystem werden einige Plattformbenachrichtigungsregeln (sysevent_email_action) bereitgestellt. Diese Benachrichtigungsregeln sollten in erforderliche Domänen geklont werden, und nur domänenspezifische Benachrichtigungsregeln müssen aktiviert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Navigieren Sie zu, um weitere Informationen zu den Regelbenachrichtigungen zu erhalten **Systembenachrichtigung** > **Benachrichtigungen** und filtern Sie nach allen globalen Domänenbenachrichtigungsregeln, die in den Tabellen mit dem Namen *„sn_sec_tisc“* definiert sind, um zu verstehen, wie Benutzer die im Basissystem bereitgestellten Basisbenachrichtigungsregeln identifizieren können.

- Alle erfassten Konfigurationen und Daten sind für jede Domäne spezifisch, was bedeutet, dass Anwender aus einer Domäne nicht auf Daten aus einer anderen Domäne zugreifen können.
- Konfigurieren Sie eine domänengetrennte Umgebung mit dieser Anwendung, indem Sie das Plugin „Domain Support – Domain Extensions Installer“ installieren.
- Für alle Anwendungstabellen des Basissystems werden Domänenspalten hinzugefügt.
- Mit der von der Plattform bereitgestellten Funktionalität verwalten die Mandantendomänen ihre eigenen Anwendungsdaten.
- Die Geschäftslogik und die Prozesse, die vom Instanzbesitzer domänengetrennt werden können, sind identisch mit dem, was die Plattform unterstützt.
- Die Geschäftslogik und die Prozesse, die von der Mandantendomäne verwaltet werden können, entsprechen denen, die von der Plattform unterstützt werden.
- Auf die Seite „Setup“ können Sie im Abschnitt Administration zugreifen. Klicken Sie auf den Link im Abschnitt „Administration“, um die Ansicht der Domänentrennung anzuzeigen.
- Eine detaillierte Anleitung zur Unterstützung der Domänentrennung für Widgets mithilfe von PA-Indikatoren (Performance Analytics) im TISC-Homepage-Dashboard finden Sie im KB-Artikel KB1647990 .

Domänengetrennte Tabellen

Alle Tabellen sind domänengetrennt.

Anwendungsfälle

Alle Funktionen dieser Anwendung sind domänengetrennt.

Zugehörige Informationen

Domänentrennung für Service Provider

Richten Sie das Threat Intelligence-Sicherheitszentrum ein

Bevor Sie Threat Intelligence-Sicherheitszentrumverwenden, müssen Sie es aus dem ServiceNow Store herunterladen.

Installierte Rollen

Lesen Sie sich die folgenden Informationen durch und vergewissern Sie sich, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben. Nachfolgend finden Sie die Liste der verschiedenen Benutzerpersonas, die für den Zugriff auf die und die Arbeit mit der Anwendung definiert sind:

- Threat Intelligence-Analyst (sn_sec_tisc.analyst)
- Threat Intelligence-Administrator (sn_sec_tisc.admin)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungen, die für TISC-Rollen gelten

Setup	Beschreibung
Weisen Sie die erforderlichen Rollen für Now Platform und Threat Intelligence Security Center zu, und überprüfen Sie sie.	Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich: • Als Administrator müssen Sie die Anwendung TISC aus dem Store ServiceNow installieren und die Rolle sn_sec_tisc.admin zuweisen. • Diese Rolle sn_sec_tisc.admin führt die folgenden Aufgaben aus: ◦ Konfiguriert die Datenquellen für die Erfassung der Daten. Weitere Informationen finden Sie unter Threat Intelligence-Feeds. ◦ Die Integrationen konfiguriert, die für die Anreicherung von Daten erkennbarer Elemente in TISC erforderlich sind Weitere Informationen finden Sie unter TISC-Ergänzungsintegrationen. ◦ Konfiguriert Datenimport-Genehmigungsrollen für den Import von Daten mit dem Import-Assistenten. Weitere Informationen finden Sie unter Arbeiten mit Datenimporten. ◦ Konfiguriert den Bedrohungsbewertungsrechner mit den erforderlichen Kriterien für die automatische Berechnung der Bedrohungsbewertung von erkennbaren Elementen. Weitere Informationen finden Sie unter Definieren Sie den Bedrohungsbewertungsrechner. ◦ Konfiguriert die erforderlichen Taxonomien und Taxonomiewerte. Weitere Informationen finden Sie unter Taxonomien werden erstellt. ◦ Konfigurieren Sie das für Ihre Organisation relevante MITRE ATT&CK-Repository. Weitere Informationen finden Sie unter MITRE-ATT&CK Repository. **Hinweis:** Als sn_sec_tisc.admin können Sie auch die Rolle sn_sec_tisc.analyst zuweisen. • Die Rolle sn_sec_tisc.analyst führt die folgenden Aufgaben aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungen, die für TISC-Rollen gelten (Fortsetzung)

Setup	Beschreibung
	○ Zeigt die Übersicht der Daten im System über die Produkt-Homepage an. Weitere Informationen finden Sie unter Zeigen Sie die Homepage des Threat Intelligence-Sicherheitszentrums an. ○ Importieren Sie Daten über die Schaltfläche „Import Intelligence“ auf der Seite „Bedrohungsbibliothek“ in das System. Weitere Informationen finden Sie unter Threat Intelligence-Sicherheitszentrum Bibliothek. ○ ▪ Durchsuchen Sie die in der Anwendung vorhandenen Daten mithilfe der Suche auf der Seite „Bedrohungsbibliothek“. ▪ Verwaltet die aus verschiedenen Quellen in der Bedrohungsbibliothek erfassten Daten. ▪ Führt verschiedene Ergänzungsaktionen für erkennbare Elemente durch. ▪ Erstellt und verwaltet Fälle. Weitere Informationen finden Sie unter Erstellen von Fällen mit der Workbench für Bedrohungsanalysten.

Abhängigkeits-Plugins

Plugin	Beschreibung
Die folgenden Anwendungen sind für die Installation dieser Anwendung erforderlich: • Komponenten des gemeinsamen Arbeitsbereichs für die Fallverwaltung für Security Cases [com.snc.escm.ws_commons]. • Threat Intelligence Support Common [com.snc.threat].	Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren.

Zeigen Sie die Homepage des Threat Intelligence-Sicherheitszentrums an

Verwenden Sie die TISC-Homepage, die die Zielseite ist, um die Daten im Zusammenhang mit Threat Intelligence zu visualisieren.

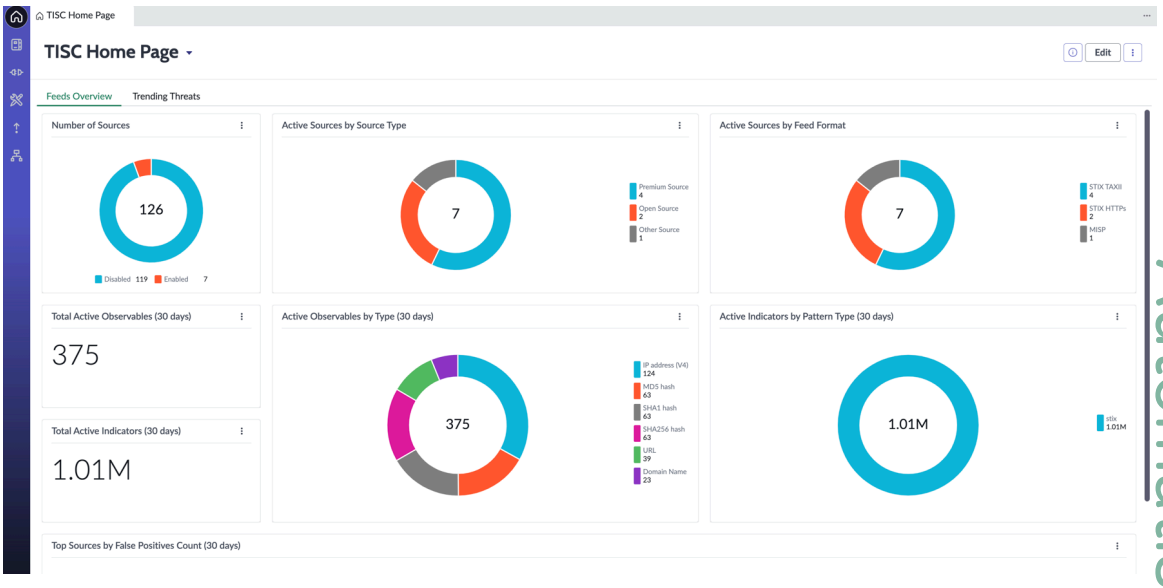
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
   Die TISC-Homepage wird angezeigt.



2. Zeigen Sie die TISC-Homepage mit verschiedenen Widget-Daten an.
   Die Homepage-Ansicht besteht aus zwei verschiedenen Registerkarten: **Feeds-Übersicht** und **Bedrohungstrends**. Der Inhalt auf der Homepage von stammt aus verschiedenen Quellen wie erkennbaren Elementen, Indikatoren und Daten-Feeds.

   a. **Feeds-Übersicht**: Diese Registerkarte bietet einen allgemeinen Überblick über verschiedene Quellen, aus denen die Daten erfasst werden, sowie über Quellen, die für die Datenerfassung konfiguriert sind.

Feeds-Übersicht

Widget-Name	Beschreibung	Aktion
Anzahl der Quellen	Zeigt die Anzahl der Quellen nach Status wie „Entwurf“, „Aktiviert“ und „Deaktiviert“ im System an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Aktive Quellen nach Quelltyp	Zeigt die Verteilung der aktiven Quellen nach Quelltyp an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Aktive Quellen nach Feed-Format	Zeigt die Anzahl der aktivierten Quellen nach Feed-Typ an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Gesamtzahl aktiver erkennbarer Elemente (30 Tage)	Zeigt die Top-10-Quellen nach Volumen der Intelligenzdatensätze an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget-Name	Beschreibung	Aktion
Aktive erkennbare Elemente nach Typ	Zeigt das höchste Gesamtvolumen der Aggregate erkennbarer Elemente an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.
Aktive Indikatoren nach Mustertyp	Zeigt das Gesamtvolumen der Indikatoraggregate nach Mustertyp an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.
Aktive Indikatoren insgesamt (30 Tage)	Zeigt das Gesamtvolumen der Indikatoraggregate an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.
Top-Quellen nach Anzahl der falsch positiven Ergebnisse (30 Tage)	Zeigt das Gesamtvolumen von falsch positiven erkennbaren Elementen an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.

b. **Bedrohungen im Trend**: Diese Registerkarte bietet eine allgemeine Übersicht über die Bedrohungen im Trend.

Feeds-Übersicht

Widget-Name	Beschreibung	Aktion
Aktuelle Berichte (Top 10)	Zeigt die Liste der Berichte und Links an – Top 10 nach Veröffentlichungsdatum geordnet.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Neueste RSS-Feeds (Top 10)	Zeigt die Liste der RSS-Feeds und Links an – Top 10 nach Veröffentlichungsdatum geordnet.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Aktive erkennbare Elemente nach Bedrohungsbewertungsbereich (30 Tage)	Zeigt die Anzahl der erkennbaren Elemente an, die in den letzten 30 Tagen erstellt wurden, verteilt nach Bedrohungsbewertungsbereichen.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.
Aktive erkennbare Elemente nach Reputation (30 Tage)	Zeigt die Anzahl der erkennbaren Elemente an, die in den letzten 30 Tagen erstellt wurden, verteilt nach Reputation.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.
Top-Tags (30 Tage)	Zeigt die Top-Tags der in den letzten 30 Tagen erstellten Datensätze basierend auf der Häufigkeit der Nutzung an.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.
Am meisten anvisierte Sektoren (30 Tage)	Zeigt die 10 besten Sektoren sortiert nach den gemeldeten	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget-Name	Beschreibung	Aktion
	Aktivitäten an, die in den letzten 30 Tagen erstellt wurden.	Widgets für den ausgewählten Filter in einer neuen Registerkarte geöffnet.

Integration von Threat Intelligence Security Center

Verwenden Sie diesen Abschnitt, um die Threat Intelligence-Sicherheitszentrum -Integrationen zu verstehen.

Der Abschnitt **„Integrationen“** enthält die folgenden Submodule.

Integrationen

Modulname	Beschreibung
Katalog	Alle verfügbaren Threat Intelligence-Feeds und Ergänzungsintegrationen werden hier als Kacheln/ Karten angezeigt. Die Anwender können in diesem Abschnitt keinen neuen Feed oder keine neue Integration erstellen.
Bedrohungsfeeds	Dieser Abschnitt enthält die Details, die sich nur auf Threat Intelligence-Feeds beziehen, und die Anwender können in diesem Abschnitt neue Threat Intelligence-Feeds konfigurieren.
Ergänzungsintegrationen	Dieser Abschnitt enthält nur die Details, die sich auf Ergänzungsintegrationen beziehen, und die Anwender können in diesem Abschnitt verfügbare Ergänzungsintegrationen konfigurieren. **Hinweis:** Der Abschnitt „Ergänzungsintegrationen“ ist nur sichtbar, wenn mindestens ein Plugin für die Ergänzungsintegration installiert ist.

Threat Intelligence-Sicherheitszentrum Katalog

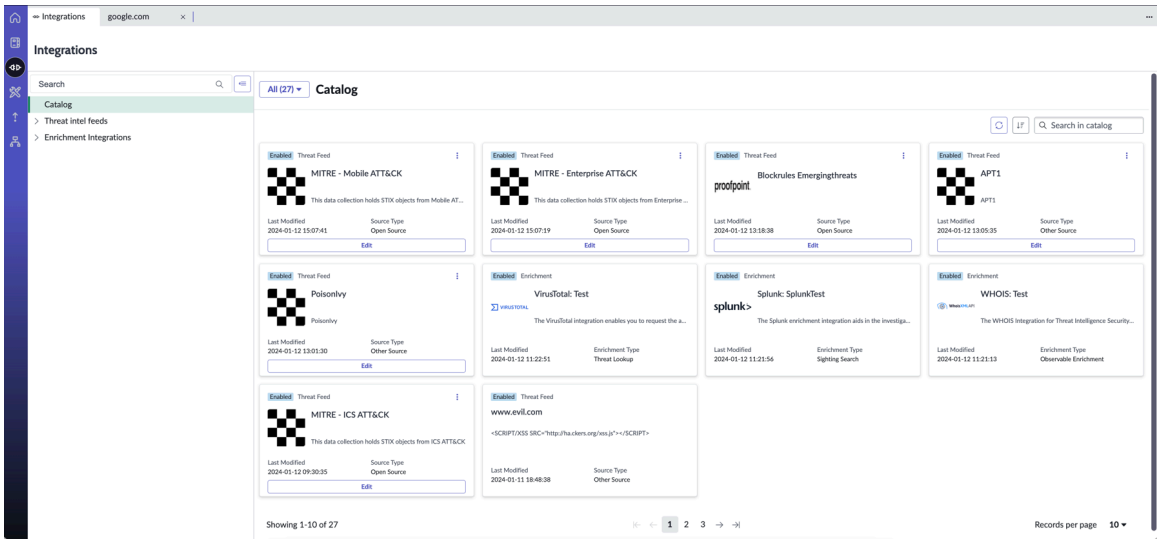
Der Katalog Threat Intelligence-Sicherheitszentrum ist eine kuratierte Liste von Threat Intelligence-Feeds und Ergänzungsintegrationen, die in der Anwendung verfügbar sind. Sie können sie nach dem Hinzufügen der erforderlichen Informationen aktivieren und den Feed so planen, dass Threat Intelligence-Daten automatisch mit einer festgelegten Häufigkeit erfasst werden.

Als sn_sec_tisc.admin können Sie auch die vorhandenen Quellkonfigurationen durchsuchen und bearbeiten, die Konfigurationen aktivieren oder deaktivieren und sie aus dem Katalog löschen. Jede neue Datenquelle wird dem Katalog hinzugefügt, der als neue Konfigurationskarte im Katalog angezeigt wird.

Erforderliche Rolle:

- sn_sec_tisc.admin (erstellen/aktualisieren)
- sn_sec_tisc.analyst (lesen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die Karten im Katalog unterscheiden sich durch die Bezeichnung, die sich oben auf der Karte befindet Bedrohungs-Feed/Ergänzung.

Aktionen in der Katalogansicht

In der Katalogansicht können Sie die folgenden Aktionen ausführen.

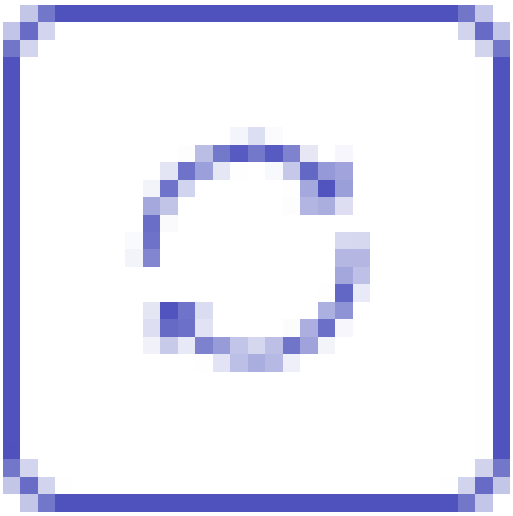
Aktionen in der Katalogansicht

Aktion	Beschreibung
Alle	Verwenden Sie dieses Dropdown-Menü, um Feeds und Integrationen basierend auf ihrem aktuellen Status zu filtern. Sie können basierend auf den folgenden Status filtern: • **Alle**: Zeigt alle Feeds und Integrationen auf der Seite an. Dies ist die Standardoption. • **Aktiviert**: Zeigt alle Feeds und Integrationen an, die sich im Status „Aktiviert“ befinden. • **Deaktiviert**: Zeigt alle Feeds und Integrationen an, die sich im Status „Deaktiviert“ befinden. • **Entwurf**: Zeigt alle Feeds und Integrationen an, die sich im Entwurfsstatus befinden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Katalogansicht (Fortsetzung)

Aktion	Beschreibung
	Diese Aktion verwenden, um den Katalog zu aktualisieren.
	Diese Aktion verwenden, um alle Feeds und Integrationen basierend auf den folgenden Kriterien zu sortieren: • **Zuletzt geändert (aktuell)** • **Zuletzt geändert (am ältesten)** • **Name A–Z** • **Name (Z–A)**
In Katalog suchen	Diese Aktion verwenden, um basierend auf dem Namen und der Beschreibung im Katalog nach Feeds/ Integrationen zu suchen.

Threat Intelligence-Feeds

Verwenden Sie Threat Intelligence-Feeds, um die Datenquelle des Threat Intelligence-Feeds hinzuzufügen, zu bearbeiten oder zu entfernen.

Die Datenquellen-Feeds sind im Threat Intel-Katalog im Abschnitt „Integrationen“ verfügbar.

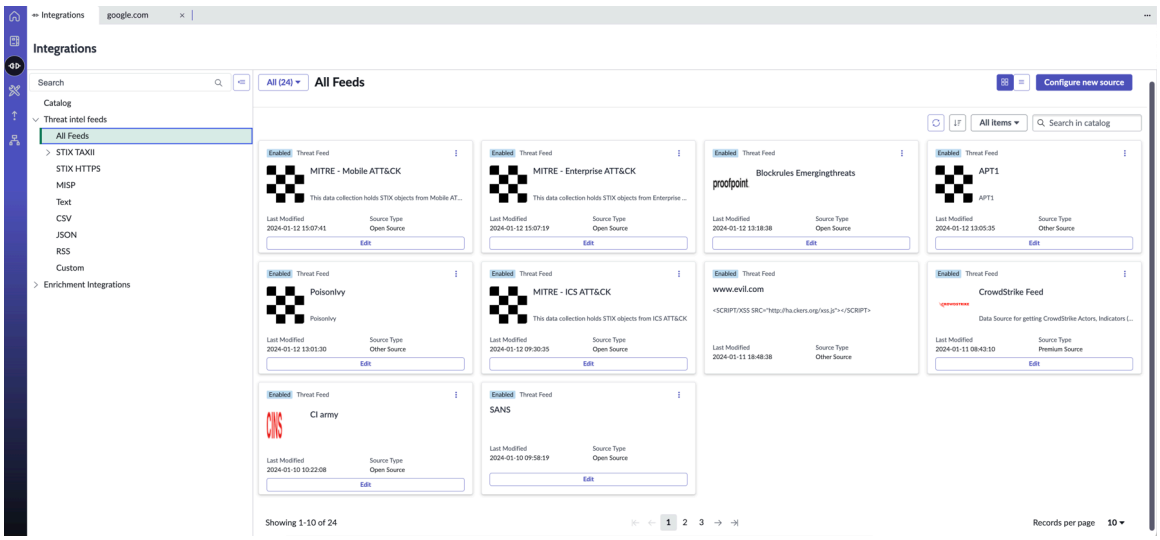
Der Katalog für Threat Intelligence-Feeds wird so erstellt, dass die verfügbaren Feed-Datenquellen in Form von Kacheln angezeigt werden. Er bietet die Möglichkeit zum Filtern, Suchen und Navigieren zu den Details der Quellkonfiguration sowie zum Ausführen verschiedener Aktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Feeds

Das Basissystem enthält eine Reihe von Karten für jeden der Feeds, die Sie aktivieren und verwenden können.

Die Feeds können angezeigt werden, indem Sie zu navigieren **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen** > **Bedrohungsinformationsfeeds** > **Alle Feeds**.



Aktionen in der Ansicht „Alle Feeds“.

Im Abschnitt „Alle Feeds“ können Sie die folgenden Aktionen ausführen.

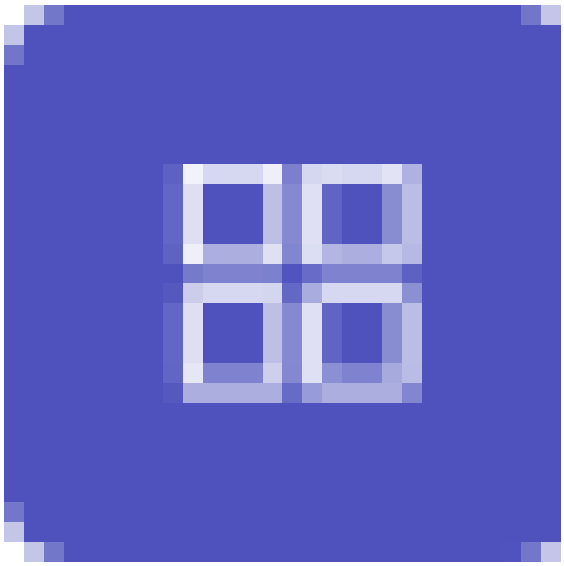
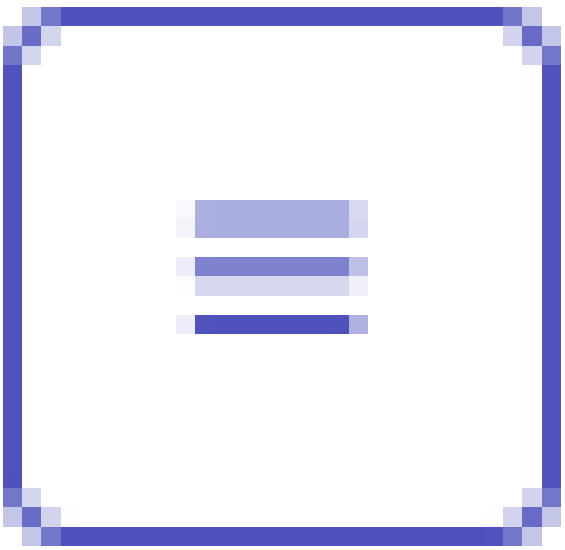
Aktionen in der Ansicht „Alle Integrationen“.

Aktion	Beschreibung
Alle	Verwenden Sie dieses Dropdown-Menü, um Feeds basierend auf ihrem aktuellen Status zu filtern. Sie können basierend auf den folgenden Status filtern: • **Alle**: Zeigt alle Feeds auf der Seite an. Dies ist die Standardoption. • **Aktiviert**: Zeigt alle Feeds an, die sich im Status „Aktiviert“ befinden. • **Deaktiviert**: Zeigt alle Feeds an, die sich im Status „Deaktiviert“ befinden. • **Entwurf**: Zeigt alle Feeds an, die sich im Entwurfsstatus befinden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

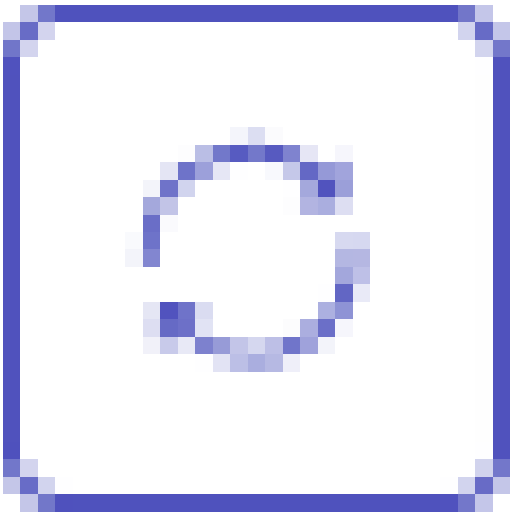
Aktionen in der Ansicht „Alle Integrationen“. (Fortsetzung)

Aktion	Beschreibung
	Diese Aktion verwenden, um alle Feeds in Form von Karten anzuzeigen.
	Diese Aktion verwenden, um alle Feeds in Form einer Listenansicht anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Ansicht „Alle Integrationen“. (Fortsetzung)

Aktion	Beschreibung
	Diese Aktion verwenden, um die Seite zu aktualisieren.
	Verwenden Sie diese Aktion, um alle Integrationen basierend auf den folgenden Kriterien zu sortieren: • **Zuletzt geändert (aktuell)** • **Zuletzt geändert (am ältesten)** • **Name A–Z** • **Name (Z–A)**
Alle Elemente	Diese Aktion verwenden, um die Kacheln für Threat Intelligence-Feeds nach Quelltyp oder Feed-Typ zu filtern und aufzulisten. **Quelltyp**: • Open Source • Andere Quelle • Premium-Quelle **Feed-Typ**: • CSV • Anwenderdefinierter Feed • JSON

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

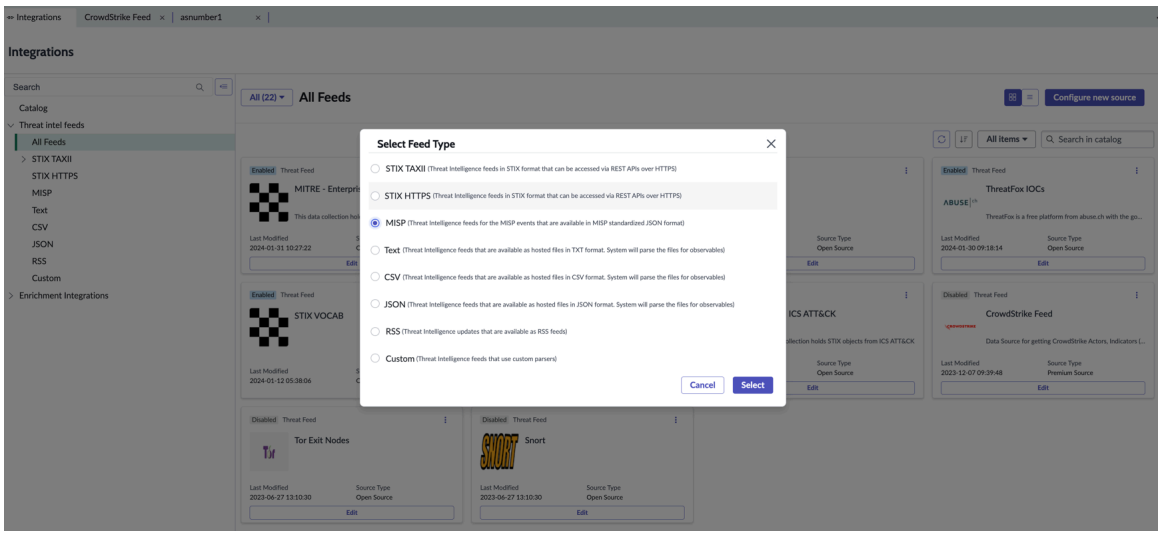
Aktionen in der Ansicht „Alle Integrationen“. (Fortsetzung)

Aktion	Beschreibung
	• MISP • RSS • STIX-HTTPS • Text
In Katalog suchen	Diese Aktion verwenden, um basierend auf dem Namen und der Beschreibung im Katalog nach Feeds zu suchen.

Konfigurieren Sie eine neue Datenquelle für Threat Intelligence-Feeds

Um eine neue Datenquelle für einen Threat Intelligence-Feed zu konfigurieren, gehen Sie wie folgt vor:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Auswahlvorgang **Bedrohungsinformationsfeeds** > **Alle Feeds**.
4. Klicken Sie auf **Neue Quelle konfigurieren**. Die verschiedenen Feed-Typen werden angezeigt.



5. Wählen Sie den entsprechenden Feed-Typ aus. Beispiel: MISP.
6. Klicken Sie auf **Auswählen**.
7. Füllen Sie die Felder des Formulars aus.

Neue Datenquelle erstellen

Feld	Beschreibung
Name	Geben Sie einen Namen für den Feed ein.
Beschreibung	Beschreibung des Feeds.
Feed-Typ	Der Feed-Typ. Beispiel: MISP.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standardmäßig wird dieser Wert basierend auf dem Feed-Typ angezeigt, den Sie im Katalog ausgewählt haben.
Logo	Hängen Sie das Logo des Quell-Feeds an.
Branche	Wählen Sie die Branchenkategorie aus, z. B. Luft- und Raumfahrt, Landwirtschaft usw., für die die Feed-Datenquelle gilt.
Quelltyp	Wählen Sie den Quelltyp aus der Liste der verfügbaren Quelltypen aus. Liste der verfügbaren Quellen: ○ Regierung ○ ISACs ○ Open Source ○ Premium-Quelle ○ Andere Quelle

Füllen Sie die Felder im Abschnitt Konfiguration entsprechend aus.

Konfiguration

Feld	Beschreibung
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für den Feed in Tagen ein. Zum Beispiel 180 Tage. **Hinweis:** Alle aus der Quelle erfassten Daten laufen 180 Tage nach der Erfassung ab.
Verwenden Sie die REST-Nachricht	Aktivieren Sie das Kontrollkästchen **REST-Nachricht verwenden,** wenn Sie die von Now Platformbereitgestellte REST-Nachrichten-/REST-Methoden-Funktion verwenden müssen. Wenn dieses Kontrollkästchen nicht aktiviert ist, verwendet die Anwendung den in **der REST-Endpunkt-URL** angegebenen Endpunkt, um die Daten aus dem Feed abzurufen. Weitere Informationen finden Sie unter Ausgehender REST-Webservice in der Dokumentation Now Platform. **Hinweis:** Die Felder „REST-Nachricht“ und „REST-Methode“ sind obligatorisch, wenn Sie die REST-Nachricht auswählen.
REST-Nachricht	Wählen Sie den REST-Nachrichtendatensatz aus der Liste der REST-Nachrichtendatensätze aus, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	bereits in der Instanz konfiguriert sind. Weitere Informationen finden Sie unter Ausgehender REST-Webservice in der Now Platform-Dokumentation. **Hinweis:** Wählen Sie diesen Wert aus, wenn Sie bestimmte Header anzeigen und die zugehörigen REST-Datensätze mit der REST-Nachrichtenoption definieren müssen.
REST-Methode	Wählen Sie die REST-Methode aus der Liste der verfügbaren REST-Methoden aus, die für die ausgewählte REST-Nachricht konfiguriert sind. Weitere Informationen finden Sie unter Ausgehender REST-Webservice in der Now Platform-Dokumentation.
Vertrauen	Legen Sie die Konfidenz für alle zutreffenden Datensätze fest, die über diesen spezifischen Feed erfasst werden. **Hinweis:** Legen Sie die Konfidenz für diese Quelle zwischen 0 und 100 fest.
REST-Endpunkt-URL	Geben Sie die REST-Endpunkt-URL ein, unter der die Daten von der Datenquelle gehostet werden.
Authentifizierung erforderlich	Aktivieren Sie dieses Kontrollkästchen, wenn für Ihre neue Datenquelle eine Authentifizierung erforderlich ist. **Hinweis:** Fügen Sie eine Anweisung hinzu, in der angegeben wird, dass dies nur gilt, wenn die REST-Endpunkt-URL zum Abrufen der Daten verwendet wird.
Authentifizierungstyp	Der Authentifizierungstyp für den Quell-Feed. Im Folgenden sind die Authentifizierungstypen aufgeführt, die im Basissystem für die Benutzer konfiguriert und bereitgestellt werden: ○ API-ID/API-Schlüssel ○ API-ID/API-Geheimnis ○ API-Schlüssel ○ API-Schlüssel/API-Geheimnis ○ API-Anwendername/API-Passwort/API-Schlüssel ○ Standardauthentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Der Authentifizierungstyp im Basissystem für den anwenderdefinierten Quell-Feed-Typ sind „Client-ID“ und „Geheimer Clientschlüssel“.
Header, die mit der Anforderung übergeben werden sollen	Alle Header, die mit den Anforderungen übergeben werden sollen, können in der Anforderungsheaderzuordnung angegeben werden. Der Header muss als Schlüssel-Wert-Paar angegeben werden, das durch einen Doppelpunkt (':') getrennt ist. Jedes Header-Schlüssel-Wert-Paar muss in einer neuen Zeile angegeben werden. Um Authentifizierungsparameter als Headerwerte bereitzustellen, schließen Sie die erforderliche Authentifizierungsbezeichnung in „${“ und „}$“ ein. Beispiel: x-api-key:${API-Schlüssel}$.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um ein anwenderdefiniertes Integrationsskript und ein Berichtsprozessorskript zu definieren. **Hinweis:** Wenn Sie dieses Kontrollkästchen aktivieren, werden die Felder **„Integrationsskript“** und **„Berichtsprozessor“** angezeigt, in denen Sie die anwenderdefinierten Skripts auswählen können.
Integrationsskript	Das Integrationsskript löst einen Aufruf an die REST-Endpunkt-URL aus und verwendet dazu die Authentifizierungsparameter und Header, wie sie im Feed konfiguriert sind. Anschließend ruft das Skript die Daten ab, die aus dem spezifischen Feed verfügbar sind. Im Basissystem sind die folgenden anwenderdefinierten Skripteinbindungen aufgeführt, die in der Anwendung für die Integrationsskripts bereitgestellt werden: ○ FeedDatasourceIntegrationBase ○ MITRESourceIntegration ○ RSSFeedDatasourceIntegration ○ SimpleFeedDatasourceIntegration ○ SimpleMISPFeedDatasourceIntegration Das standardmäßige Integrationsskript basiert auf dem von Ihnen ausgewählten Feed-Typ. Wenn Sie beispielsweise den Feed-Typ MISP auswählen, der ein Standardformat zum Verarbeiten und Abrufen der Daten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ist, lautet das Integrationsskript **SimpleFeedDatasourceIntegration**. **Hinweis:** Für die anwenderdefinierten Integrationsskripts können Sie eine Skripteinbindung erstellen, indem Sie **FeedDatasourceIntegrationBase** erweitern und die erforderlichen Methoden überschreiben.
Berichtsprozessor-Skript	Das Skript des Berichtsprozessors verarbeitet die Daten, die aus dem Feed abgerufen werden, mithilfe des Integrationsskripts. Im Basissystem sind die folgenden anwenderdefinierten Skripteinbindungen aufgeführt, die in der Anwendung für die Integrationsskripts bereitgestellt werden: ○ FeedDatasourceResponseProcessor ○ MITRECollectionDataProcessor ○ RSSFeedDatasourceResponseProcessor ○ SimpleFeedDatasourceResponseProcessor ○ SimpleMISPFeedDatasourceResponseProcessor ○ TAXIIV2CollectionDataProcessor Der standardmäßige Berichtsprozessor für STIX HTTPS ist **TAXIIV2CollectionDataProcessor**. Standardmäßig wird diese Option angezeigt, und Sie können keinen anderen Berichtsprozessor ändern oder auswählen.

Füllen Sie die Felder im Abschnitt „Zeitplanung“ entsprechend aus.

Zeitplanung

Feld	Beschreibung
Ausführen	Legen Sie die Häufigkeit fest, mit der Sie die Datensätze erfassen möchten. Der Feed wird basierend auf dem Intervall des geplanten Auftrags ausgeführt. Die verfügbaren Auftragsintervalle sind: ○ Täglich ○ Wöchentlich ○ Monatlich ○ In regelmäßigen Abständen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Einmal ○ Bei Bedarf ○ Geschäftskalender: Eintragsbeginn ○ Geschäftskalender: Eintragsende **Hinweis:** Standardmäßig ist die Häufigkeit auf Bei Bedarf festgelegt. Weitere Informationen finden Sie unter Geplante Aufgaben und Automatische Ausführung eines Skripts Ihrer Wahl .
Daten abrufen von	Startdatum, ab dem die Daten abgerufen werden müssen. In diesem Feld sollte die Zeit festgelegt werden, ab der die Daten aus der entsprechenden Quelle erfasst werden müssen. Sobald dieses Feld festgelegt ist, ruft die nächste Erfassungsausführung die Daten ab der konfigurierten Zeit ab, und nachfolgende Erfassungsausführungen rufen inkrementelle Daten ab. Beispiel: Quelle ist so geplant, dass die Daten stündlich erfasst werden. Der Anwender legt **„Daten abrufen von“** am 12. Januar um 9:30 Uhr auf 6:00 Uhr fest. Die Erfassung, die am 12. Januar um 10:00 Uhr ausgelöst wird, würde die Daten vom 12. Januar 6:00 Uhr bis zum 12. Januar 10:00 Uhr abrufen. Bei der nächsten Erfassung, die um 11:00 Uhr ausgelöst wird, werden nur die inkrementellen Daten vom 12. Januar, 10:00 Uhr, bis zum 12. Januar, 11:00 Uhr abgerufen. **Hinweis:** Dies bedeutet, dass die geplanten Ausführungen ab dem angegebenen Datum inkrementell Daten abrufen.

Tags

Feld	Beschreibung
Tags auswählen	Verwenden Sie die Tags, um Datensätze, die aus dieser Quelle im System erfasst werden, mit Anmerkungen zu versehen oder mit Tags zu versehen. Beginnen Sie mit der Eingabe des Tag-Namens in der **Suchleiste**, um die verfügbaren Tags in der Anwendung auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf **Hinzufügen**, um ihn der Quelle zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf die Aktion **Speichern**, um den Feed zu speichern und zu erstellen.

   Die angegebenen Details werden validiert, und standardmäßig ist der Feeds-Status deaktiviert.

9. (Optional) Klicken Sie auf die Aktion **Als Entwurf speichern,** um nur die Feedkonfigurationen als Entwurf zu speichern. Anwender können einen Feed nicht aktivieren, wenn er als Entwurf gespeichert ist.

   Wenn Sie sich bezüglich der Konfigurationsdetails nicht sicher sind, können Sie die Option **Als Entwurf speichern** verwenden. Nachdem Sie die Konfigurationsdetails abgerufen haben, können Sie die verbleibenden Informationen in die Entwurfsversion eintragen und sie erstellen.

10. Um den Feed zu aktivieren, klicken Sie auf **Aktivieren**.

    Der Feed wurde erfolgreich aktiviert. Sie können einen bestimmten Feed auch über das Menü **„Aktionen“** der erforderlichen Feed-Kachel auf der Seite **„Katalog“** oder **„Threat Intel Feeds“** aktivieren, deaktivieren oder löschen.

    Hinweis:
    Wenn die **Ausführungshäufigkeit** im Abschnitt **„Zeitplanung“** der Datenquellen-Formularseite auf **„Bei Bedarf“** festgelegt ist, wird bei jeder Aktivierung der Integration eine Meldung angezeigt, die die Benutzer darüber informiert, dass die Quelle jetzt erfolgreich aktiviert wurde. Sie müssen die Ausführungshäufigkeit ändern, damit die Quellkonfiguration Daten automatisch erfassen kann.

11. Klicken Sie auf **Aktivieren**, um den Datensatz zu aktivieren.

    Sobald der Datensatz der Feed-Datenquelle aktiviert ist, können Sie ihn ausführen, um die Integration auszuführen.

    Hinweis:
    Der Datenquelldatensatz erhält die Bezeichnung und wird als **aktiviert**angezeigt. Ebenso können Sie den Datenquellen-Feed deaktivieren, indem Sie auf die Schaltfläche **Deaktivieren** klicken.

12. Klicken Sie auf **Löschen,** um den Datensatz der Feed-Datenquelle zu löschen.
13. Wählen Sie den Abschnitt **Integrationsausführung** aus, um die Ausführungsdetails zu überprüfen.

Hinweis:
Das obige Verfahren zur Konfiguration von Feed-Datenquellen ist für alle anderen Feed-Datenquellentypen außer STIX TAXII identisch. Weitere Informationen zur Konfiguration von STIX TAXII finden Sie unter Konfigurieren Sie einen neuen TAXII-Feed.

Arten von Bedrohungsinformationenfeeds

Die folgenden Arten von Threat Intelligence-Feeds können konfiguriert und aktiviert werden:

Threat Intelligence-Feeds

Typ	Beschreibung
TAXII-Feeds	Feeds, die im Format STIX/TAXII-Sammlungen verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Feeds (Fortsetzung)

Typ	Beschreibung
STIX HTTPS	Threat Intelligence-Feeds im STIX-Format, auf die über REST APIs im HTTPS-Protokoll zugegriffen werden kann.
MISP	Feeds, die sich in den MISP-Format-Feeds befinden.
Text	Feeds, die als gehostete Dateien im Textformat verfügbar sind. **Hinweis:** Das System analysiert die Dateien im Hinblick darauf, ob URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert werden. Andere erkennbare Elemente werden nicht extrahiert.
CSV	Feeds, die als gehostete Dateien im CSV-Format verfügbar sind. **Hinweis:** Das System analysiert die Dateien im Hinblick darauf, ob URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert werden. Andere erkennbare Elemente werden nicht extrahiert.
JSON	Feeds, die als gehostete Dateien im JSON-Format verfügbar sind. **Hinweis:** Das System analysiert die Dateien im Hinblick darauf, ob URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert werden. Andere erkennbare Elemente werden nicht extrahiert.
RSS	Feeds, die im RSS-Format verfügbar sind. Die Anwendung speichert die Daten als RSS-Feed-Datensätze.
Anwenderdefiniert	Feeds, die mit anwenderdefinierten Parsern konfiguriert werden. **Hinweis:** Das System analysiert die Dateien im Hinblick darauf, ob URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert werden. Andere erkennbare Elemente werden nicht extrahiert.

Die nächsten Schritte im Verfahren finden Sie im entsprechenden Abschnitt zum Konfigurieren der einzelnen spezifischen Feed-Typen. Threat Intelligence-Feeds.

Zeigen Sie Threat Intel Feeds an

Dieser Abschnitt enthält die Bedrohungsinformationsfeeds, die im Basissystem konfiguriert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie STIX TAXII-Feeds an

Zeigen Sie die konfigurierten STIX TAXII-Feeds im Basissystem an.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Wählen Sie **STIX-TAXII**aus.
   In der folgenden Tabelle werden die MISP-Feeds im Basissystem beschrieben.

Bedrohungsfeed	Beschreibung	URL
Cyber-TAXII	Cyber Threat Intelligence eXchange (CTIX) ist eine Plattform, die die gemeinsame Nutzung von Cyberbedrohungsinformationen zwischen Unternehmen erleichtern soll.	https://threatfeed.cyware.com/ctixapi/ctix21/
RecordedZukünftiges TAXII	Recorded Future ist eine unabhängige Cloud-Plattform für Bedrohungsinformationen, mit der Unternehmen Bedrohungen in den Bereichen Cyber, Lieferkette, physische Bedrohungen und Betrug identifizieren und mindern können.	https://api.recordedfuture.com/taxii2
Pulsierendes TAXII	Pulsedive ist eine Threat Intelligence-Plattform, die Unternehmen eine breite Palette von Cyber Threat Intelligence-Services und -Tools bereitstellt.	https://pulsedive.com/taxii2/api/

4. Klicken Sie auf **Bearbeiten**, um den Feed zu bearbeiten.

Zeigen Sie STIX-HTTPS-Feeds an

Zeigen Sie die konfigurierten STIX-HTTP-Feeds im Basissystem an.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Wählen Sie **STIX HTTPs**aus.
   In der folgenden Tabelle werden die STIX-HTTPS-Feeds im Basissystem beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ThreatFeed	Beschreibung	URL
MITRE: Mobile ATT&CK	Diese Datensammlung enthält STIX-Objekte aus Mobile ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE: ICS ATT&CK	Diese Datensammlung enthält STIX-Objekte aus ICS ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE: Enterprise ATT&CK	Diese Datensammlung enthält STIX-Objekte aus Enterprise ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. Klicken Sie auf **Bearbeiten**, um den Feed zu bearbeiten und die erforderlichen Aktualisierungen vorzunehmen.

Zeigen Sie MISP-Feeds an

Zeigen Sie die MISP-Feeds an, die im Basissystem konfiguriert sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Wählen Sie **MISP**aus.
   In der folgenden Tabelle werden die MISP-Feeds im Basissystem beschrieben.

Bedrohungsfeed	Beschreibung	URL
Intel OSINT-Feed für DigitalSide Threat	Datenquelle zum Abrufen von Open Source Cyber Threat Intelligence-Informationen aus dem DigitalSide Threat-Intel OSINT-Feed, der hauptsächlich auf Malware-Analysen und gefährdeten URLs, IPs und Domänen basiert.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
URLhaus-IOCs	URLhaus ist ein Projekt von Missbrauch.ch mit dem Ziel, schädliche URLs freizugeben, die für die Verteilung von Malware verwendet werden.	https://urlhaus.abuse.ch/downloads/misp/manifest.json
Malware-Basar	MalwareBazaar ist ein Projekt von Missbrauch.ch mit dem Ziel, Malware-Beispiele für die Infosec-Community, AV-Anbieter und Threat Intelligence-Anbieter freizugeben.	https://bazaar.abuse.ch/downloads/misp/manifest.json

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungsfeed	Beschreibung	URL
ThreatFox IoCs	ThreatFox ist eine kostenlose Plattform vonuse.ch mit dem Ziel, mit Malware verbundene Kompromittierungsindikatoren (IoCs) für die Infosec-Community, AV-Lieferanten und Threat Intelligence-Anbieter freizugeben.	https://threatfox.abuse.ch/downloads/misp/manifest.json

4. Klicken Sie auf **Bearbeiten**, um den Feed zu bearbeiten.

Zeigen Sie Text-Feeds an

Zeigen Sie die Text-Feeds an, die im Basissystem konfiguriert sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Wählen Sie die Option **Text** aus.
   Im Folgenden sind die konfigurierten Text-Feeds im Basissystem aufgelistet.

Bedrohungsfeed	Beschreibung	URL
Haleys Brute-Force-IPs	Stellt eine nach IP-Adresse sortierte Liste der IP-Adressen der angreifenden Computer während der letzten 2 Jahre bereit	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Blockregeln für neu auftretende Bedrohungen	Emerging Threat (ET) Intelligence bietet umsetzbare Bedrohungsinformationsfeeds, um IPs zu identifizieren, die an verdächtigen und böswilligen Aktivitäten beteiligt sind.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Pop3-Nuug-Pop3-Entferner-Web	Liste der Hosts, die versucht haben, sich beim POI-Service unter bsdly.net anzumelden.	https://home.nuug.no/%7Epeter/pop3gropers.txt
Tor-Exit-Knoten	Tor-Exit-Knoten können verwendet werden, um Datenverkehr zu erkennen, der vom TOR-Netzwerk kommt.	https://www.dan.me.uk/torlist/?exit
Schwarze Liste für IP-Adresse von Talos Intelligence	Talos wurde durch den Zusammenschluss des Schwachstellen-Forschungsteams von SourceFire, der Cisco Threat Research and Communications-Gruppe und der Cisco Secure Applications Group gebildet.	https://www.talosintelligence.com/documents/ip-blacklist

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungsfeed	Beschreibung	URL
	Das kombinierte Fachwissen wird durch eine hochentwickelte Infrastruktur und die unübertroffene Datentelemetrie von Cisco unterstützt, die sich über Netzwerke, Endpunkte, Cloud-Umgebungen, virtuelle Systeme und den täglichen Web- und E-Mail-Datenverkehr erstreckt.	
SANS	ISC bietet Tausenden von Internetanwendern und Organisationen einen kostenlosen Analyse- und Warnungsservice.	https://isc.sans.edu/feeds/topips.txt
Schnaubend	Snort ist das weltweit führende Open Source Intrusion Prevention System (IPS). Snort IPS verwendet eine Reihe von Regeln, um schädliche Netzwerkaktivitäten zu definieren.	https://snort.org/downloads/ip-block-list
CI-Heer	Die CINS-Heerliste ist eine Teilmenge des Regelsatzes CINS Active Threat Intelligence und besteht aus IP-Adressen, die eines von zwei grundlegenden Kriterien erfüllen: 1) Der aktuelle Bewertungsfaktor für nicht autorisierte Pakete der IP ist sehr schlecht, oder 2) Die IP hat einen festgelegten ausgelöst Anzahl der „vertrauenswürdigen“ Warnungen für eine bestimmte Anzahl ihrer weltweit bereitgestellten Sentinels.	https://cinsscore.com/list/ci-badguys.txt
Proofpoint	Roh-IPs für die Firewall-Sperrlisten. Diese stammen von: Von Spamhaus (www.spamhaus.org) identifizierte Spam-Netze, von DShield (www.dShield.org) und Abuse.ch aufgelistete Top-Angreifer	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
Sperrliste Greensnow	GreenSnow ist ein Team, das aus den besten Spezialisten für Computersicherheit besteht. GreenSnow sammelt eine große Anzahl von IPs von verschiedenen Computern auf der ganzen Welt. GreenSnow ist für Angriffe jeder Art außer Spam mit SpamHaus.org vergleichbar.	https://blocklist.greensnow.co/greensnow.txt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungsfeed	Beschreibung	URL
CI-Heer	Die CINS-Heerliste ist eine Teilmenge des Regelsatzes CINS Active Threat Intelligence und besteht aus IP-Adressen, die eines von zwei grundlegenden Kriterien erfüllen: 1) Der aktuelle Bewertungsfaktor für nicht autorisierte Pakete der IP ist sehr schlecht, oder 2) Die IP hat einen festgelegten ausgelöst Anzahl der „vertrauenswürdigen“ Warnungen für eine bestimmte Anzahl ihrer weltweit bereitgestellten Sentinels.	https://cinsscore.com/list/ci-badguys.txt
Sperrliste	www.blocklist.de ist ein kostenlos und freiwillig bereitgestellter Dienst eines Betrugs-/Missbrauchsspezialisten, dessen Server häufig über SSH-, Mail-Login-, FTP-, Webserver- und andere Dienste angegriffen werden.	https://lists.blocklist.de/lists/all.txt
Tor-Exit-Knoten	Tor-Exit-Knoten können verwendet werden, um Datenverkehr zu erkennen, der vom TOR-Netzwerk kommt.	https://www.dan.me.uk/torlist/?exit
Botscout-BOT-IPs	BotScout verhindert, dass automatisierte Webskripts, die als „Bots“ bezeichnet werden, sich in Foren registrieren, Datenbanken belasten, Spam verbreiten und Formulare auf Websites missbrauchen.	http://botscout.com/last_caught_cache.txt
Datenebene VNC RFB	IP-Adressen, die als initiierende VNC-Remote-Framepuffersitzungen identifiziert wurden.	https://dataplane.org/signals/vncrfb.txt
Dataplane TELNET-Anmeldung	IP-Adressen, von denen angegeben wurde, dass der Anmeldeversuch über die TELNET-Passwortauthentifizierung erfolgt.	https://dataplane.org/signals/telnetlogin.txt
SSH-Passwortauthentifizierung für Dataplane	IP-Adressen, von denen erkannt wurde, dass der Anmeldeversuch über SSH-Passwortauthentifizierung erfolgt.	https://dataplane.org/signals/sshpwauth.txt
SSH-Clientverbindung für die Datenebene	IP-Adressen, von denen identifiziert wurde, dass sie SSH-Client-Protokollverhandlungen führen.	https://dataplane.org/signals/sshclient.txt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungsfeed	Beschreibung	URL
Blockregeln für neu auftretende Bedrohungen	Emerging Threat (ET) Intelligence bietet umsetzbare Bedrohungsinformationsfeeds, um IPs zu identifizieren, die an verdächtigen und böswilligen Aktivitäten beteiligt sind.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
SMTP-Begrüßung auf Ebene der Datenebene	IP-Adressen, die als SMTP-Clients identifiziert wurden, die nicht angeforderte HELO- oder EHLO-Befehle ausgeben.	https://dataplane.org/signals/smtpgreet.txt
Dataplane-SIP-Abfrage	IP-Adressen, die als sendende SIP-OPTIONEN-Abfragen identifiziert wurden.	https://dataplane.org/signals/sipquery.txt
Dataplane IP-Protokoll 41	IP-Adressen, die als offenes IPv4-Protokoll 41-Relais identifiziert wurden (z. B. IPv6 über IPv4).	https://dataplane.org/signals/proto41.txt
Dataplane-SIP-Einladung	IP-Adressen, die als sendende SIP INVITE-Vorgänge identifiziert wurden.	https://dataplane.org/signals/sipinvitation.txt
Dataplane DNS CH TXT version.bind	IP-Adressen, die als sendende DNS CH TXT VERSION.BIND-Abfragen identifiziert haben.	https://dataplane.org/signals/dnsversion.txt
Datenebene-DNS-TCP	IP-Adressen, von denen angegeben ist, dass sie DNS über TCP-Port 53-Abfragen senden.	https://dataplane.org/signals/dnstcp.txt
Dataplane-DNS-Rekursion IN BELIEBIG erwünscht	IP-Adressen, von denen identifiziert wurde, dass sie rekursive DNS IN ANY-Abfragen senden.	https://dataplane.org/signals/dnsrdany.txt
DNS-Rekursion auf Datenebene erwünscht	IP-Adressen, von denen identifiziert wurde, dass sie rekursive DNS-Abfragen senden.	https://dataplane.org/signals/dnsrd.txt
Phishing-Datenbank aus aktiven GitHub-Phishing-Links	Datenquelle zum Abrufen aktiver Phishing-Links aus der in GitHub verfügbaren Phishing-Datenbank.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-links-ACTIVE.txt
Phishing-Datenbank aus aktiven GitHub-Domänen	Datenquelle zum Abrufen aktiver Domänen aus der Phishing-Datenbank, die in GitHub verfügbar ist.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
Phishing-Datenbank aus GitHub – aktive IPs	Datenquelle zum Abrufen aktiver IPs aus der Phishing-Datenbank, die in GitHub verfügbar ist.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
Bots auf Sperrliste setzen	Alle IP-Adressen, von denen innerhalb der letzten 48 Stunden gemeldet wurde, dass sie Angriffe auf RFI-Angriffe, REG-Bots,	https://lists.blocklist.de/lists/bots.txt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungsfeed	Beschreibung	URL
	IRC-Bots oder SchlechteBots ausgeführt haben.	
Apache-Angriffe auf Blockliste setzen	Alle IP-Adressen, von denen innerhalb der letzten 48 Stunden gemeldet wurde, dass sie Angriffe auf den Service Apache, Apache-DDOS, RFI-Angriffe ausgeführt haben.	https://lists.blocklist.de/lists/apache.txt
Schwarze VoIP-Liste nach Scoped	Ruft die Liste der gesperrten IPs aus der schwarzen VoIP-Liste ab.	http://voipbl.org/update/?dm=bl
Sperrliste für Threatview-Domänen	Bösartige Domänen, die für Phishing/die Bereitstellung von Malware/Befehl und Steuerung identifiziert wurden.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
Threatview MD5-Hash-Sperrliste	MD5-Hashes von schädlichen Dateien oder im Zusammenhang mit Malware, Ransomware, Hack-Tools, Bots usw.	https://threatview.io/Downloads/MD5-HASH-ALL.txt
Sperrliste für Bedrohungsansichts-URLs	Bösartige URLs, die Malware, Phishing, Botnets und C2 bereitstellen.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Threatview-SHA-Datei-Hash-Sperrliste	SHA-Hashes von Dateien, die mit der Ausführung von Malware bekannt oder verknüpft sind.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
Threatview-IP-Sperrliste	Sperrliste für böswillige IPs für bekanntermaßen ungültige IP-Adressen.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Threatview C2-Jagd-Feed	Infrastruktur, die Befehls- und Steuerungsserver hostet, die während der proaktiven Suche nach Threatview.io gefunden wurden	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt
Threatview OSINT-Bedrohungs-Feed	Aus der OSINT-Quelle gesammelte böswillige Kompromittierungsindikatoren – Twitter und Einfügen.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

Automatische Übersetzung

4. Klicken Sie auf **Bearbeiten**, um den Feed zu bearbeiten.

CSV-Feeds anzeigen

Zeigen Sie die CSV-Feeds an, die im Basissystem konfiguriert sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **CSV**aus.
   In der folgenden Tabelle werden die CSV-Feeds im Basissystem erläutert.

ThreatFeed	Beschreibung	URL
Abuse.ch – Schwarze Liste für SSL-Zertifikate	Die schwarze Liste für SSL-Zertifikate (CSV) ist eine CSV-Datei, die den SHA1-Fingerabdruck aller SSL-Zertifikate enthält, die in SSLBL auf die schwarze Liste gesetzt wurden.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Botnet C2 IP Blacklist	Ein SSL-Zertifikat kann einem oder mehreren Servern zugeordnet werden (Kombination aus IP-Adresse und Port). SSLBL erfasst IP-Adressen, die mit einem SSL-Zertifikat ausgeführt werden, das auf SSLBL auf die schwarze Liste gesetzt wurde. Dies sind normalerweise Botnetz-Command&Control-Server (C&C). SSLBL veröffentlicht daher eine schwarze Liste mit diesen IPs, die zur Erkennung von Botnetz-C2-Datenverkehr von infizierten Computern in Richtung Internet verwendet werden können, die Ihr Netzwerk verlassen.	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
Phishing-Tank online	NA	https://data.phishtank.com/data/online-valid.csv

4. Klicken Sie auf **Bearbeiten**, um den Feed zu bearbeiten.

Anwenderdefinierten Feed anzeigen

Zeigen Sie den anwenderdefinierten Feed an, der im Basissystem enthalten ist.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Wählen Sie **Anwenderdefiniert**aus.
   In der folgenden Tabelle ist ein standardmäßig anwenderdefinierter Feed aufgeführt.

ThreatFeed	Beschreibung	URL
CrowdStrike-Feed	Quelle zum Abrufen von Daten von CrowdStrike-Akteuren,	https://api.crowdstrike.com

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ThreatFeed	Beschreibung	URL
	erkennbaren Elementen und Berichten.	

4. Klicken Sie auf **Bearbeiten**, um den Feed zu bearbeiten.

Zeigen Sie den Premium-Bedrohungsfeed für CrowdStrike an

Zeigen Sie den neu hinzugefügten Premium-Bedrohungsfeed für den anwenderdefinierten Feed-Typ an. Jeder Premium-Feed, der den Datenquellenmanager verwendet, erfordert Punktintegrationen.

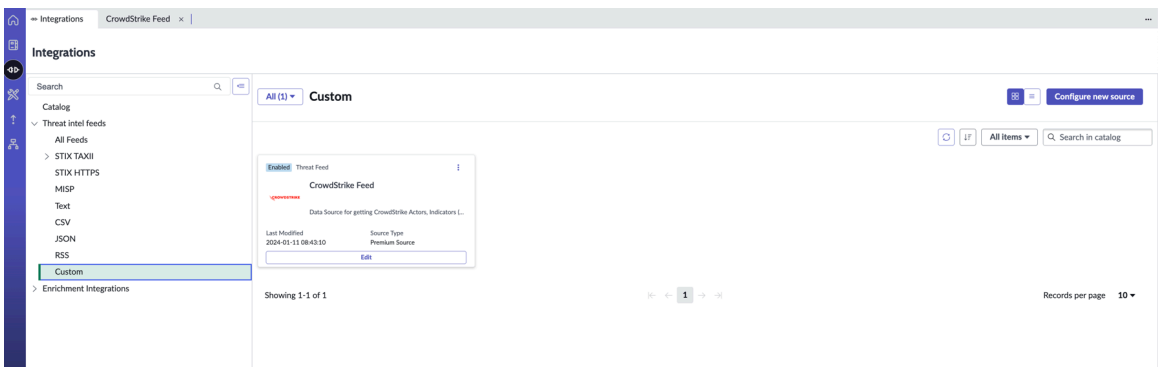
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Wählen Sie **Anwenderdefiniert**aus.
4. Klicken Sie auf die Karte **CrowdStrike Feed**.

Hinweis:
Standardmäßig ist der CrowdStrike-Feed deaktiviert. Sie müssen die Konfigurationen bearbeiten, um den Feed zu aktivieren.



5. Führen Sie einen Drilldown zum Abschnitt **„Konfigurationsdetails“** durch.
6. Geben Sie die **Basis-URL**,**Client-ID**und **den geheimen Clientschlüssel**ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

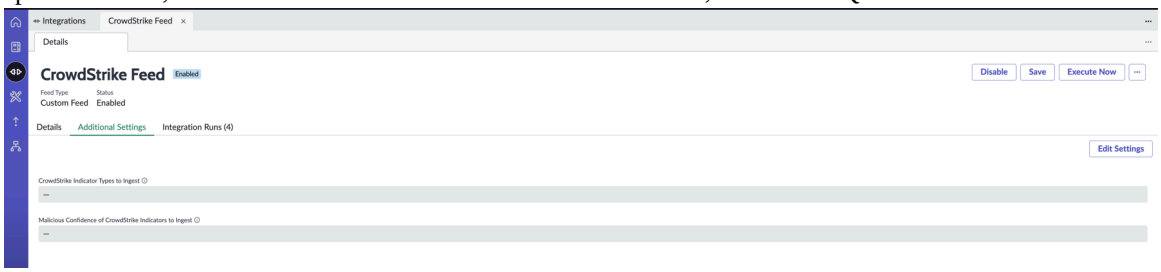
a. **Basis-URL**: Jede CrowdStrike-Cloud hat eine andere Basis-URL. Wenn Sie Anforderungen an die CrowdStrike-API stellen, verwenden Sie die Basis-URL, die der Cloud entspricht, in der CrowdStrike gehostet wird.

b. Sie müssen Ihre Client-ID und Ihren geheimen Clientschlüssel generieren, falls Sie keine haben. Weitere Informationen zur Client-ID und zum geheimen Clientschlüssel finden Sie im Abschnitt „Ihren ersten API-Client definieren“ .

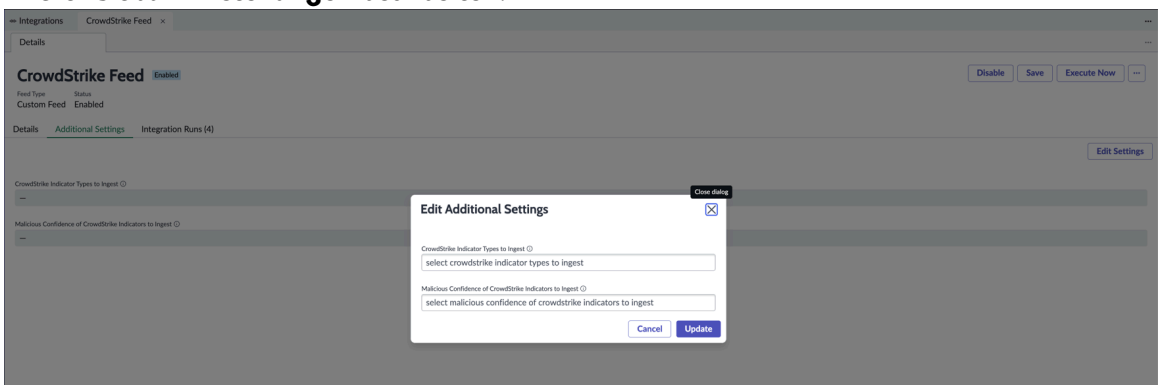
c. Rufen Sie die Client-ID und den geheimen Clientschlüssel von CrowdStrike für erforderliche Bereiche ab. Nachfolgend sind die Bereiche aufgeführt, die für die Client-ID und den geheimen Clientschlüssel aus Crowdstrike erforderlich sind:

- Indikatoren (Falcon Intelligence)
- Akteure (Falcon Intelligence)
- Berichte (Falcon Intelligence)

7. Navigieren Sie zu **Zusätzliche Einstellungen**, die für die Integration des CrowdStrike-Bedrohungsfeeds spezifisch sind, können zum Filtern von Daten verwendet werden, die aus der Quelle erfasst werden.

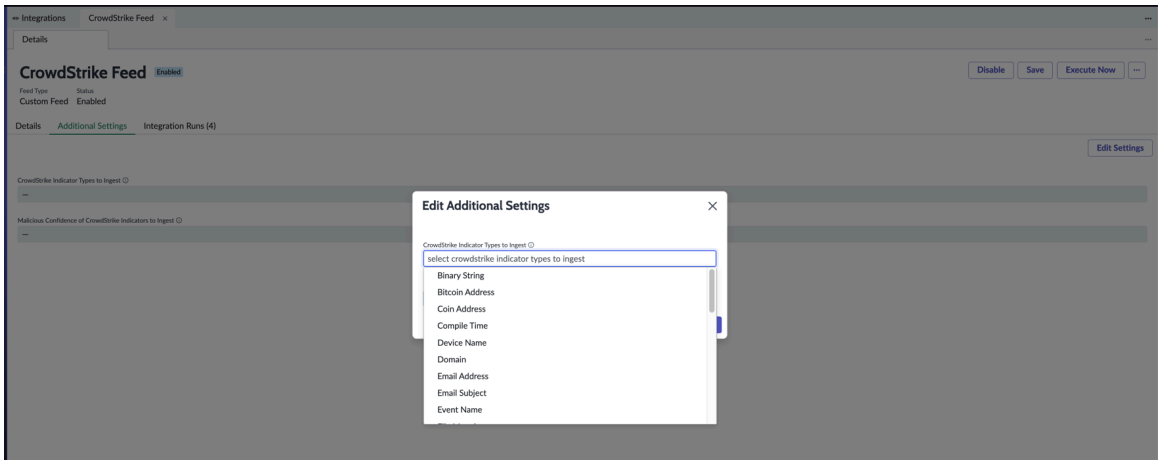


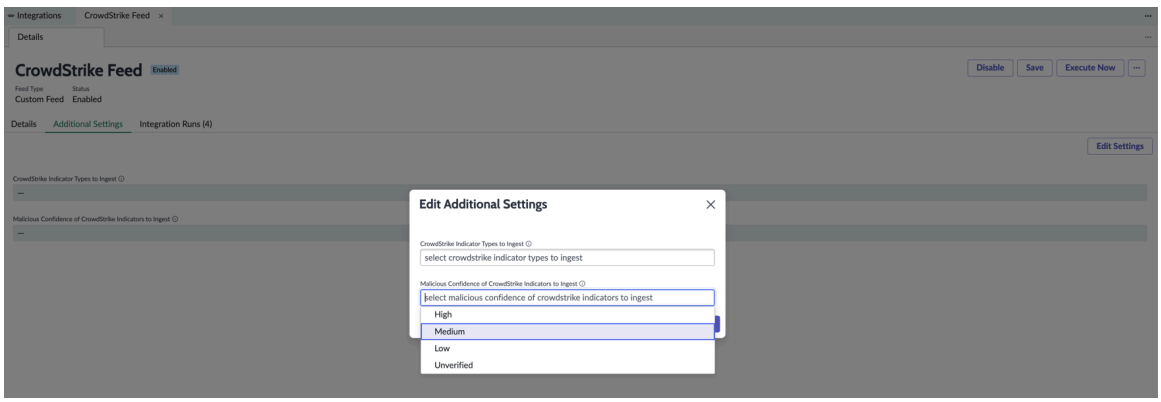
8. Klicken Sie auf **Einstellungen bearbeiten**.



9. Wählen Sie eine der Optionen aus: **Zu erfassende CrowdStrike-Indikatortypen** oder **Zu erfassende böswillige Konfidenz von CrowdStrike-Indikatoren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





Hinweis:

a. **Zu erfassende CrowdStrike-Indikatortypen**: Nur die ausgewählten Indikatortypen werden beim Abrufen der aktualisierten Indikatoren aus CrowdStrike erfasst (Indikatoren in CrowdStrike werden erkennbaren Elementen in TISC zugeordnet). Wenn dieses Feld leer gelassen wird, werden Indikatoren aller Typen erfasst.

b. **Böswilliges Vertrauen der zu erfassenden CrowdStrike-Indikatoren**: Nur der ausgewählte Indikator mit dem ausgewählten schädlichen Vertrauen wird beim Abrufen der aktualisierten Indikatoren von CrowdStrike erfasst (Indikatoren in CrowdStrike werden erkennbaren Elementen in TISC zugeordnet). Wenn leer gelassen, werden Indikatoren aller schädlichen Konfidenzen erfasst.

10. Wählen Sie die erforderlichen Werte für jede Option aus. Basierend darauf werden die übereinstimmenden Indikatoren erfasst.
11. Klicken Sie auf **Aktualisieren**.
12. Klicken Sie auf **Aktivieren**.

Hinweis:

Der Premium-Feed entspricht anderen Feeds bis auf die Antwort, die während der Konfiguration analysiert wird. Eine bestimmte Antwort wird in CrowdStrike analysiert, indem die Client-ID und der geheime Clientschlüssel hinzugefügt werden.

Welche Art von Daten wird von CrowdStrike abgerufen?

a. Indikatoren aus CrowdStrike, die nach der konfigurierten Erfassungszeit aktualisiert werden. Diese Indikatoren aus CrowdStrike werden dann erkennbaren Elementen in TISC zugeordnet. Nachfolgend sind die Indikatortypen aufgeführt, die in TISC erfasst werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- SHA256-Hash
- MD5-Hash
- SHA1-Hash
- URL
- Domäne
- IP-Adresse
- Mutex-Name
- Dateiname
- E-Mail-Adresse
- Anwendername
- IP-Adressblock

b. Bedrohungsakteure aus CrowdStrike, die nach der konfigurierten Erfassungszeit aktualisiert werden. Diese Akteure aus CrowdStrike werden in unserem System Bedrohungsakteur zugeordnet.

c. Berichte aus CrowdStrike, die nach der konfigurierten Erfassungszeit aktualisiert werden. Diese Berichte aus CrowdStrike werden den Bedrohungsberichten in unserem System zugeordnet.

d. Zusätzlich zu den oben genannten Entitäten rufen wir auch die folgenden Daten ab.

i. Bedrohungsakteure/-berichte/-indikatoren, die mit den oben erfassten Indikatoren zusammenhängen.

ii. Bedrohungsakteure/-indikatoren, die sich auf alle Berichte beziehen, die im Rahmen der aktuellen Erfassung erfasst werden.

Systemeigenschaften für CrowdStrike

Im Folgenden finden Sie die Systemeigenschaften für CrowdStrike.

1. sn_sec_tisc.rowdstrike_actor_batch_size: Gibt die Anzahl der Akteure an, die in einem einzelnen API-Aufruf abgerufen werden sollen. Hinweis: Gilt nur, wenn die Integration das erforderliche Element nicht im System findet.
   - Typ: Ganzzahl
   - Wert: 250
2. sn_sec_tisc.rowdstrike_api_limit: Anzahl der Datensätze, die gleichzeitig aus CrowdStrike abgerufen werden sollen. Je höher die Zahl, desto mehr Arbeitsspeicher wird für die Verarbeitung der Nutzlast verbraucht.
   - Typ: Ganzzahl
   - Wert: 1000
3. sn_sec_tisc.rowdstrike_indicator_batch_size: Gibt die Anzahl der Indikatoren an, die in einem einzelnen API-Aufruf abgerufen werden sollen. Hinweis: Gilt nur, wenn die Integration das erforderliche Element nicht im System findet.
   - Typ: Ganzzahl
   - Wert: 150
4. sn_sec_tisc.rowdstrike_offset_limit_total: Die zulässige Summe von Offset und Grenzwert aus der CrowdStrike-API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Typ: Ganzzahl
- Wert: 50.000

5. sn_sec_tisc.rowdstrike_report_batch_size: Gibt die Anzahl der Berichte an, die in einem einzelnen API-Aufruf abgerufen werden sollen. Hinweis: Gilt nur, wenn die Integration das erforderliche Element nicht im System findet.
   - Typ: Ganzzahl
   - Wert: 50

STIX TAXII verstehen

Der strukturierte Bedrohungsinformationsausdruck (STIX) ist eine Sprache und ein Serialisierungsformat, die zum Austausch von Cyberbedrohungsinformationen (CTI) verwendet werden. Trusted Automated Exchange of Intelligence Information (TAXII) ist ein Protokoll zum Austausch von Cyber Threat Intelligence (CTI) über HTTPS.

Mit STIX werden alle Aspekte von Verdächtigungen, Kompromittierungen und Zuschreibungen als Objekte und beschreibende Beziehungen dargestellt. STIX-Informationen können für einen Analysten visuell dargestellt oder als JSON gespeichert werden, um schnell maschinell lesbar zu sein.

Cyber Threat Intelligence (CTI) wurde beauftragt, eine Reihe von Informationsdarstellungen und Protokollen zu definieren, um die Notwendigkeit der Modellierung, Analyse und Freigabe von Cyberbedrohungsinformationen zu decken. Der Schwerpunkt von CTI liegt auf der Entwicklung und Standardisierung von STIX (Strukturierte Bedrohungsinformationen) und dem vertrauenswürdigen automatisierten Austausch von Indikatorinformationen (TAXII).

Konfigurieren Sie einen neuen TAXII-Feed

Sie können TAXII-Feeds für die Freigabe von STIX-formatierten Informationen verwalten. Jeder TAXII-Feed enthält eine oder mehrere TAXII-Sammlungen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**.
3. Auswahlvorgang **Bedrohungsinformationsfeeds** > **STIX-TAXII** > **TAXII-Feeds**.

   Hinweis:
   Konfigurieren Sie den TAXII-Feed so, dass er als Profil für alle darin enthaltenen TAXII-Sammlungen dient.

4. Klicken Sie auf **Neue Quelle konfigurieren**.
   Die Seite Neuen TAXII-Feed konfigurieren wird angezeigt.
5. Füllen Sie die Felder des Formulars aus.

Neue Datenquelle erstellen

Feld	Beschreibung
Name	Geben Sie einen Namen für den Feed ein.
Beschreibung	Beschreibung des Feeds.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelltyp	Der Typ der Quelle, z. B. Open Source, Premium-Quelle usw., die für den Feed bereitgestellt wurde. Die verfügbaren Quelltypen sind: ○ Regierung ○ ISACs ○ Open Source ○ Premium-Quelle ○ Andere Quelle
Logo	Hängen Sie das Logo des Quell-Feeds an.
Branche	Wählen Sie die Branchenkategorie aus, z. B. Luft- und Raumfahrt, Landwirtschaft usw., für die die Feed-Datenquelle gilt.

Füllen Sie die Felder im Abschnitt Konfiguration entsprechend aus.

Konfiguration

Feld	Beschreibung
TAXII-Version	Wählen Sie die TAXII-Version des zu konfigurierenden TAXII-Servers aus. Unterstützte Versionen sind 2.0 und 2.1.
Konfigurationstyp	Geben Sie einen Konfigurationstyp zum Abrufen von TAXII-Sammlungen an. Verfügbare Werte sind: ○ **Discovery-Service-URL**: Wählen Sie die Discovery-Service-URL, um Sammlungen von allen verfügbaren API-Stämmen innerhalb des Discovery-Service des TAXII-Servers abzurufen. ○ **API-Stamm-URL**: Wählen Sie die API-Stamm-URL, um Sammlungen vom spezifischen API-Stamm des TAXII-Servers abzurufen.
Authentifizierung	Wählen Sie die erforderliche Option aus der Dropdown-Liste aus, wenn die Authentifizierung erforderlich ist. Verfügbare Optionen: ○ **Keine**: Wählen Sie diese Option aus, wenn keine Authentifizierung erforderlich ist. ○ **Standard**: Wählen Sie diese Option aus, um Anwendernamen und Passwort anzugeben. ○ **API-Schlüssel**: Wählen Sie diese Option aus, um einen API-Schlüssel bereitzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **REST-Nachricht wählen**: Wählen Sie diese Option für jede andere Art der Authentifizierung aus. Die REST-Nachrichtenoptionen sind: ▪ **REST-Nachricht verwenden**: Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine REST-Nachricht zum Erstellen einer vorgefertigten REST-Nachricht benötigen. Wenn Sie nicht auswählen, wird der Wert im Endpunktfeld verwendet. Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Nachricht aus der Liste aus. ▪ **REST-Methode**: Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine REST-Methode benötigen. Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Methode aus der Liste aus. **Hinweis:** Die Felder REST-Nachricht und REST-Methode werden verfügbar, wenn die Option REST-Nachricht ausgewählt wird.
URL	Geben Sie entweder die URL des TAXII-Server-Discovery-Service oder die spezifische API-Stamm-URL basierend auf dem ausgewählten Konfigurationstyp ein.
Erweiterter Abschnitt	
Erweitert	Aktivieren Sie das Kontrollkästchen, um ein anderes Integrationsskript und einen anderen Berichtsprozessor auszuwählen. Stellen Sie sicher, dass die ausgewählten Skripts mit der ausgewählten TAXII-Version kompatibel sind. Basierend auf der TAXII-Version und Authentifizierung werden diese Skripts standardmäßig automatisch ausgefüllt.
Integrationsskript	Ruft einen Aufruf der REST-Endpunkt-URL-API unter Verwendung der Authentifizierungsparameter wie Authentifizierungstyp Anwendername/ Passwort/API-Schlüssel und der Header auf, die mit der Anforderung übergeben werden sollen. Anschließend ruft das Skript die erkennbaren Elemente oder STIX-Daten der Indikatoren ab, die für verfügbar sind spezifischen Feed

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die abgerufenen Daten sind nur die Rohdaten (es werden keine Datensätze erstellt), die an den Integrationsprozess angehängt werden und dann im Abschnitt **„Integrationsausführung“** angezeigt werden können. Im Basissystem sind die folgenden anwenderdefinierten Skripteinbindungen aufgeführt, die in der Anwendung für die Integrationsskripts bereitgestellt werden: ○ TAXIIV2_0QueryParamAPIKeyIntegrationScript ○ TAXIIV2_0BasicAuthIntegrationScript ○ TAXIIV2_1QueryParamAPIKeyIntegrationScript ○ TAXIIV2_1BasicAuthIntegrationScript Das standardmäßige Integrationsskript basiert auf dem von Ihnen ausgewählten Feed-Typ. Die Skripteinbindungen führen einen einfachen REST-Aufruf aus, speichern die Antwort als Anhang und geben den Anhang dann an den Prozessor zurück.
Berichtsprozessor-Skript	Der Berichtsprozessor löst einen Aufruf an die REST-Endpunkt-URL aus. Im Basissystem unten befinden sich die anwenderdefinierten Skripteinbindungen, die innerhalb der Anwendung für die Integrationsskripts **TAXIIV2CollectionDataProcessor**bereitgestellt werden.

Füllen Sie die Felder im Abschnitt „Zeitplanung“ entsprechend aus.

Zeitplanung

Feld	Beschreibung
Ausführungshäufigkeit von Sammlungen	Das Planungsintervall, das auf die TAXII-Erfassungsdatensätze angewendet wird. Die Ausführungshäufigkeit für eine TAXII-Sammlung kann in der Formularansicht der TAXII-Sammlung bei Bedarf geändert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Diese Einstellung wird standardmäßig auf alle abgerufenen TAXII-Sammlungen angewendet. Bei Bedarf besteht eine Option zum Überschreiben der Einstellung in TAXII-Sammlungen. Weitere Informationen finden Sie unter Geplante Aufgaben und Automatische Ausführung eines Skripts Ihrer Wahl.
Daten abrufen von	Startdatum, ab dem die Daten abgerufen werden müssen. In diesem Feld sollte die Zeit festgelegt werden, ab der die Daten aus der entsprechenden Quelle erfasst werden müssen. Sobald dieses Feld festgelegt ist, ruft die nächste Erfassungsausführung die Daten ab der konfigurierten Zeit ab, und nachfolgende Erfassungsausführungen rufen inkrementelle Daten ab. Beispiel: Quelle ist so geplant, dass die Daten stündlich erfasst werden. Der Anwender legt **„Daten abrufen von“** am 12. Januar um 9:30 Uhr auf 6:00 Uhr fest. Die Erfassung, die am 12. Januar um 10:00 Uhr ausgelöst wird, würde die Daten vom 12. Januar 6:00 Uhr bis zum 12. Januar 10:00 Uhr abrufen. Bei der nächsten Erfassung, die um 11:00 Uhr ausgelöst wird, werden nur die inkrementellen Daten vom 12. Januar, 10:00 Uhr, bis zum 12. Januar, 11:00 Uhr abgerufen. **Hinweis:** Dies bedeutet, dass die geplanten Ausführungen ab dem angegebenen Datum inkrementell Daten abrufen.

6. Klicken Sie **auf Verbindung validieren**
   Es wird eine Informationsmeldung angezeigt, dass die TAXII-Feed-Verbindung erfolgreich hergestellt wurde. Um die Sammlungen abzurufen, fahren Sie mit dem nächsten Schritt fort.
7. Klicken Sie **auf TAXII-Sammlungen abrufen**.

   Hinweis:
   Wenn Fehler auftreten, wird eine Fehlermeldung angezeigt, dass beim Abrufen von TAXII-Sammlungen ein Fehler aufgetreten ist. Weitere Details finden Sie in den Protokollen.

   Die TAXII-Sammlungen werden im Abschnitt TAXII-Sammlungen angezeigt und sind standardmäßig deaktiviert.
8. Aktivieren Sie die TAXII-Sammlungen, um die in diesen TAXII-Sammlungen verfügbaren STIX-Objekte abzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC-Integrationen

Dieser Abschnitt enthält Anweisungen zum Konfigurieren und Aktivieren der Threat Intelligence-Integrationen.

Ergänzung erkennbarer Elemente

Der WhoIs-Workflow „Erkennbares Element ergänzen“ bereichert ausgewählte erkennbare Elemente. Wenn die erkennbaren Elemente von einem Typ sind, der von der WhoisXML-API-Integration erkannt wird, werden die erkennbaren Elemente angereichert.

Hinweis:
Das Threat Intelligence-Sicherheitszentrum unterstützt die Ergänzung erkennbarer Elemente nur für die WHOIS-Integration.

Whois-Integration

Mit der Whois-Integration können Sie Whois-Suchen für Domänennamen und URLs übermitteln, um Kontext für erkennbare URL-Elemente zu erhalten und Bedrohungen besser zu bestimmen.

Konfigurieren und aktivieren Sie die Whois-Integration

Bevor Sie die Whois-Integration verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und über einen gültigen Account bei Whois verfügen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Die Plugins für die Integration erkennbarer Elemente mit Threat Intelligence-Sicherheitszentrum und Whois sind erforderlich.

Prozedur

1. Greifen Sie mit Ihrer -Instanz auf **Threat Intelligence-Sicherheitszentrum**zu.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.
3. Navigieren Sie nach Abschluss der Installation zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Ergänzung erkennbarer Elemente**.
6. Klicken Sie auf der **WHOIS-** Karte **auf Neue Ergänzung konfigurieren**, um **die WHOIS-** Integration zu konfigurieren.
7. Füllen Sie die Felder im Formular „Neue Ergänzung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: WHOIS.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: WHOIS.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein. Die Beschreibung für die WHOIS-Integration lautet beispielsweise: Die WHOIS-Integration für Threat Intelligence-Sicherheitszentrum ermöglicht es Anwendern, Whois-Suchen für Domänennamen und URLs zu übermitteln, um Kontext für erkennbare URL-Elemente zu erhalten und Bedrohungen besser zu bestimmen.

8. Führen Sie einen Drilldown zum Abschnitt **„Integrationskonfiguration“** durch.
9. Geben Sie den **API-Schlüssel** ein, den Sie von der WHOIS-Website erhalten haben, oder fügen Sie ihn ein.
10. Klicken Sie auf **Speichern**.
    Die Integrationsdetails werden validiert, und standardmäßig ist der Status der WHOIS-Integration deaktiviert.
11. Klicken Sie auf **Aktivieren**, um die WHOIS-Integration zu aktivieren.

Ergebnisse
Nach der Konfiguration kann WHOIS für die Durchführung von Ergänzungen erkennbarer Elemente im Threat Intelligence-Sicherheitszentrum ausgewählt werden.

Shodan-Integration

Shodan ist eine Suchmaschine, die Servicebannerinformationen von verbundenen Geräten auf der ganzen Welt analysiert.

Die Shodan-Integration führt eine Ergänzung der folgenden erkennbaren Elemente durch:

- IP-Adressen
- URLs
- Domänen

Konfigurieren und aktivieren Sie die Shodan-Integration

Bevor Sie die Shodan-Integration verwenden, müssen Sie sie aus dem Store ServiceNow herunterladen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Greifen Sie mit Ihrer -Instanz auf **Threat Intelligence-Sicherheitszentrum**zu.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.
3. Navigieren Sie nach Abschluss der Installation zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Ergänzung erkennbarer Elemente**.
6. Klicken Sie auf der **Shodan-** Karte **auf Neue Ergänzung konfigurieren**, um die Integration zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Füllen Sie die Felder im Formular „Neue Ergänzung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: Shodan.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden automatisch ausgefüllt, und standardmäßig ist dieses Feld schreibgeschützt. Beispiel: Shodan.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Ergänzung erkennbarer Elemente.
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein. Die Beschreibung für die Shodan-Integration lautet beispielsweise: Shodan hilft Ihnen, Bannerinformationen von verbundenen Geräten auf der ganzen Welt zu analysieren.

8. Führen Sie einen Drilldown zum Abschnitt **„Integrationskonfiguration“** durch.
9. Geben Sie den **API-Schlüssel** ein, den Sie im Shodan-Portal erworben haben, (oder fügen Sie ihn ein).
10. Klicken Sie auf **Speichern**.
    Die Integrationsdetails werden validiert, und standardmäßig ist der Status deaktiviert.
11. Klicken Sie auf **Aktivieren**, um die Integration zu aktivieren.

Sichtungssuche

In diesem Abschnitt werden die Integrationen TISC-Sichtungssuche und Elastic Search beschrieben.

Erste Schritte mit der Elasticsearch-Integration

Die Elasticsearch-Ergänzungsintegration durchsucht Ihre Protokolle und fügt Ihren erkennbaren Elementen relevante Sichtungsinformationen hinzu.

Konfigurieren und aktivieren Sie die Elasticsearch-Integration

Elasticsearch ist eine verteilte RESTful-Such- und Analyse-Engine, die sich problemlos in Security Operations integrieren lässt.

Vorbereitungen

Bevor Sie Elasticsearch verwenden können, müssen Sie es aus dem ServiceNow Store herunterladen.

Erforderliche Rolle: sn_sec_tisc.admin

- Das Plugin „Threat Intelligence Security Center“ muss installiert und aktiviert werden, bevor Sie die Elasticsearch-Integration verwenden können.
- Rufen Sie die Basis-URL der Elasticsearch-API, die Kibana-Basis-URL, den Anwendernamen und das Passwort in Ihrem Elasticsearch-Profil ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie mit Ihrer -Instanz auf **Threat Intelligence-Sicherheitszentrum**zu.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.
3. Navigieren Sie nach Abschluss der Installation zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Sichtungssuche**

Hinweis:
Die konfigurierten Integrationen werden als Reihe von Karten angezeigt.

6. Klicken Sie auf der Karte **Elasticsearchauf Neue Ergänzung konfigurieren**, um **die Elasticsearch-** Integration zu konfigurieren.
7. Füllen Sie die Felder im Formular „Neue Ergänzung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die Konfiguration der Sichtungssuche ein.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: Elasticsearch.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die Elasticsearch-Integration ein. Beispielsweise hilft die Elasticsearch-Ergänzungsintegration bei der Untersuchung eines erkennbaren Elements durch Unterstützung des Abfragens von Protokollen in Ihrer Elasticsearch-Bereitstellung.
Integrationskonfiguration	
Basis-URL der Elasticsearch-API	Die Basis-URL, die Sie von der Elasticsearch-Website erhalten haben.
Kibana-Basis-URL	Die Kibana-Basis-URL. [Optional] Links zu einer Kibana-Instanz, falls verfügbar.
Anwendername	Ihr Intel Elasticsearch-Anwendername.
Passwort	Ihr Intel Elasticsearch-Passwort.
Elasticsearch-Index	Der Elasticsearch-Index. Diese enthalten wiederum Dokumente, die für jeden Index eindeutig sind. Indizes werden durch Kleinbuchstaben identifiziert, die sich auf Aktionen beziehen, die durchgeführte Aktionen sind (z. B. Suchen und Löschen).
Feld „Datumsbereich“	Der Zeitstempel der Konfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der Anzahl der Zeilen der Rohdateneigenschaft in den Security Incident Response-Eigenschaften ab.
MID-Server	Wählen Sie Beliebig aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum Workflow-Editor.

8. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig ist der Status der Elasticsearch-Integration deaktiviert.
9. Klicken Sie auf **Aktivieren**, um die Elasticsearch-Integration zu aktivieren.

Ergebnisse
Nach der Konfiguration kann Elasticsearch für die Durchführung einer Sichtungssuche für erkennbare Elemente im Threat Intelligence-Sicherheitszentrum ausgewählt werden.

Erste Schritte mit der Splunk Search-Integration

Splunk-Software sucht, überwacht und analysiert maschinell generierte Big Data und lässt sich problemlos in Security Operations integrieren. Bevor Sie die Splunk-Sichtungssuche-Integration verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen.

Konfigurieren und aktivieren Sie die Splunk-Integration

Die Splunk-Ergänzungsintegration durchsucht Ihre Protokolle und fügt relevante Sichtungsinformationen hinzu.

Vorbereitungen
Bevor Sie die Splunk-Suche verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen.

Erforderliche Rolle: sn_sec_tisc.admin

- Das Plugin „Threat Intelligence Security Center“ muss installiert und aktiviert werden, bevor Sie die Splunk Search-Integration verwenden können.
- Rufen Sie Splunk ab, rufen Sie die Splunk-Suche ab und rufen Sie die API-Basis-URL, die Link-URL, den Anwendernamen und das Passwort von Ihrer Splunk-Instanz ab.

Prozedur

1. Greifen Sie mit Ihrer -Instanz auf **Threat Intelligence-Sicherheitszentrum**zu.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren Sie nach Abschluss der Installation zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Sichtungssuche**
   Die konfigurierten Integrationen werden als Reihe von Karten angezeigt.
6. Klicken Sie auf der Karte **Splunk-Sucheauf Neue Ergänzung konfigurieren**, um die Integration **von Splunk Search** zu konfigurieren.
7. Füllen Sie die Felder im Formular „Neue Ergänzung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die Konfiguration der Sichtungssuche ein.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: Splunk.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die Splunk-Integration ein. Beispiel: Die Splunk-Ergänzungsintegration hilft bei der Untersuchung eines erkennbaren Elements durch Unterstützung des Abfragens von Protokollen in Ihrer Splunk-Bereitstellung im Zusammenhang mit potenziell schädlichen Indikatoren.
Integrationskonfiguration	
Basis-URL der Splunk-API	Die Basis-URL, die Sie von der Splunk-Website erhalten haben.
Link-URL	[Optional] Die Link-URL, die auf die Splunk-Webschnittstelle verweist, falls verfügbar.
Anwendername	Ihr Intel Elasticsearch-Anwendername.
Passwort	Ihr Intel Elasticsearch-Passwort.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in die Ergebnisse der Sichtungssuche aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der Anzahl der Zeilen der Rohdateneigenschaft in den Security Incident Response-Eigenschaften ab.
Lokale Bereitstellung	In der bereitgestellten lokalen Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	Wählen Sie Beliebig aus, um einen beliebigen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden -Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum Workflow-Editor.

8. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig ist der Status der Splunk-Integration deaktiviert.
9. Klicken Sie auf **Aktivieren**, um die Splunk-Integration zu aktivieren.

Ergebnisse
Nach der Konfiguration kann Splunk für die Durchführung einer Sichtungssuche für erkennbare Elemente im Threat Intelligence-Sicherheitszentrum ausgewählt werden.

Bedrohungssuche

Der Workflow „Bedrohungssuche – VirusTotal und CrowdStrike Falcon Intelligence“ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn es sich bei den erkennbaren Elementen um einen von VirusTotal und CrowdStrike erkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

TISC VirusTotal-Integration

Mit der TISC VirusTotal-Integration können Sie die Analyse verdächtiger IP-Adressen, Dateien, Datei-Hashes und URL-Adressen anfordern, um Ihre Untersuchung zu unterstützen und festzustellen, ob sie böswillig sind.

Konfigurieren und aktivieren Sie die VirusTotal-Integration

Bevor Sie die VirusTotal-Integration verwenden können, müssen Sie sie von ServiceNow Storeherunterladen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Das Plugin „Threat Intelligence Security Center“ ist erforderlich, um die VirusTotal-Integration zu aktivieren.

Prozedur

1. Greifen Sie mit Ihrer -Instanz auf **Threat Intelligence-Sicherheitszentrum**zu.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.
3. Wenn die Installation abgeschlossen ist, rufen Sie VirusTotal auf, und rufen Sie den API-Schlüssel in Ihrem VirusTotal-Profil ab.
4. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
5. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**.
6. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Bedrohungssuche**
7. Klicken Sie auf **Neue Ergänzung konfigurieren**, um **die VirusTotal-** Integration zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Füllen Sie die Felder im Formular „Neue Ergänzung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: VirusTotal.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: VirusTotal.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein.

9. Führen Sie einen Drilldown zum Abschnitt **„Integrationskonfiguration“** durch.
10. Geben Sie den **API-Schlüssel** ein, den Sie auf der VirusTotal-Website erworben haben, (oder fügen Sie ihn ein).
11. Klicken Sie auf **Speichern**.
    Die Integrationsdetails werden validiert, und standardmäßig ist der Status der VirusTotal-Integration deaktiviert.
12. Klicken Sie auf **Aktivieren**, um die VirusTotal-Integration zu aktivieren.

Ergebnisse
Nach der Konfiguration kann VirusTotal für die Durchführung von Suchen nach erkennbaren Elementen im Threat Intelligence-Sicherheitszentrum ausgewählt werden.

TISC CrowdStrike Falcon Intelligence-Integration

CrowdStrike Falcon Intelligence bietet Cybersicherheitsinformationen, die sich problemlos in Security Operations integrieren lassen.

Hinweis:

Das Plugin „Threat Intelligence Security Center“ ist erforderlich, um die CrowdStrike Falcon Intelligence-Integration zu implementieren.

Konfigurieren und aktivieren Sie die CrowdStrike Falcon Intelligence-Integration

Bevor Sie CrowdStrike Falcon Intelligence verwenden können, müssen Sie es aus dem ServiceNow Store herunterladen und die entsprechende Client-ID und den geheimen Clientschlüssel hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

- Die Anwendung Threat Intelligence Security Center muss installiert und aktiviert sein.
- Rufen Sie die API-Client-ID und das API-Client-Geheimnis in Ihrem CrowdStrike Falcon Intelligence-Profil ab.
- Aktivieren Sie in den API-Bereichen des CrowdStrike Falcon Intelligence-Portals die Einstellung Lesen für Indikatoren (Falcon Intelligence).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie mit Ihrer -Instanz auf **Threat Intelligence-Sicherheitszentrum**zu.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.
3. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Bedrohungssuche**.
6. Klicken Sie auf **Neue Ergänzung konfigurieren**, um **die CrowdStrike Falcon Intelligence-**Integration zu konfigurieren.
7. Füllen Sie die Felder im Formular „Neue Ergänzung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: CrowdStrike Falcon Intelligence.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: CrowdStrike Falcon Intelligence.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein.
Integrationskonfiguration	
Client-ID	Die Client-ID, die Sie von CrowdStrike erhalten haben.
Geheimer Clientschlüssel	Der geheime Clientschlüssel, den Sie von CrowdStrike erhalten haben.

8. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig ist der Status der CrowdStrike Falcon Intelligence-Integration deaktiviert.
9. Klicken Sie auf **Aktivieren**, um die CrowdStrike Falcon Intelligence-Integration zu aktivieren.

Ergebnisse

Nach der Konfiguration kann CrowdStrike Falcon Intelligence für die Durchführung von Suchen nach erkennbaren Elementen im Threat Intelligence-Sicherheitszentrum ausgewählt werden.

TISC-Ergänzungsintegrationen

Das Basissystem Threat Intelligence-Sicherheitszentrum enthält keine vorkonfigurierten Integrationen. Dieser Abschnitt enthält Anweisungen zum Konfigurieren von ServiceNow und Drittanbieterintegrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Stellen Sie sicher, dass Sie die erforderlichen Integrationen von Drittanbieteranwendungen installiert haben. Sie können die erkennbaren Elemente, die Sichtungssuche und die Bedrohungssuchdetails nur für die installierten Drittanbieter-Apps anzeigen.

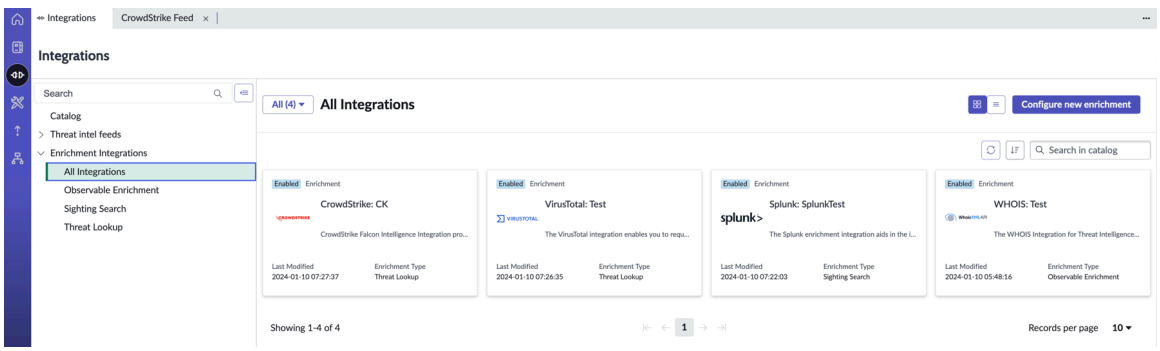
Alle Integrationskonfigurationen

Alle Integrationen sind separate Anwendungen, die installiert werden müssen. TISC unterstützt die Integration mit Drittanbietern. Alle installierten Integrationen können hier konfiguriert werden.

In diesem Abschnitt werden Karten für alle konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

Die Abschnitte jedes Ergänzungstyps sind nur sichtbar, wenn mindestens eine der entsprechenden Integrationen für diesen Ergänzungstyp installiert ist. Beispielsweise ist der Abschnitt **„Bedrohungssuche“** unter **„Ergänzungsintegrationen“** nur sichtbar, wenn mindestens eine Integration für die Bedrohungssuche installiert ist.

Die konfigurierten Integrationskarten können angezeigt werden, indem Sie zu navigieren **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**.



Aktionen in der Ansicht „Alle Integrationen“.

In der Ansicht „Alle Integrationen“ können Sie die folgenden Aktionen ausführen.

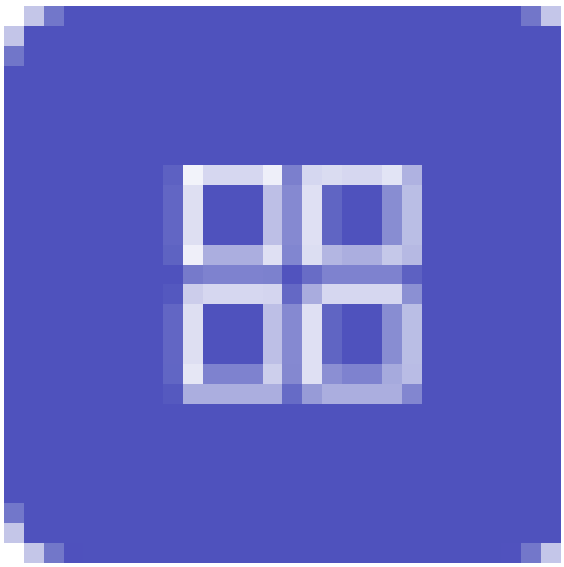
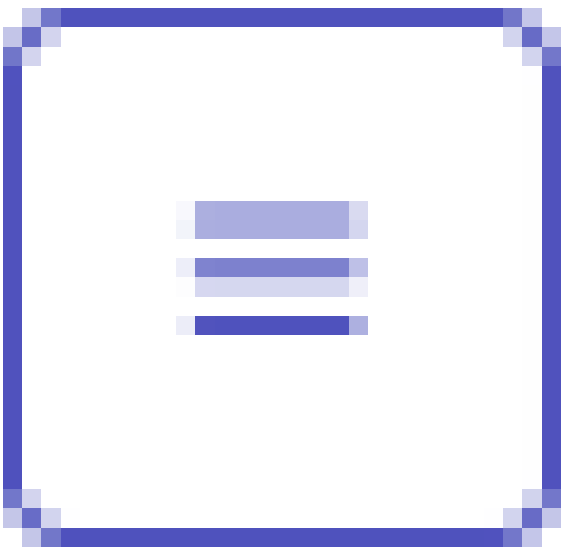
Aktionen in der Ansicht „Alle Integrationen“.

Aktion	Beschreibung
Alle	Verwenden Sie dieses Dropdown-Menü, um Integrationen basierend auf ihrem aktuellen Status zu filtern. Sie können basierend auf den folgenden Status filtern: • **Alle**: Zeigt alle Integrationen auf der Seite an. Dies ist die Standardoption. • **Aktiviert**: Zeigt alle Integrationen an, die sich im Status „Aktiviert“ befinden.

Automatische Übersetzung

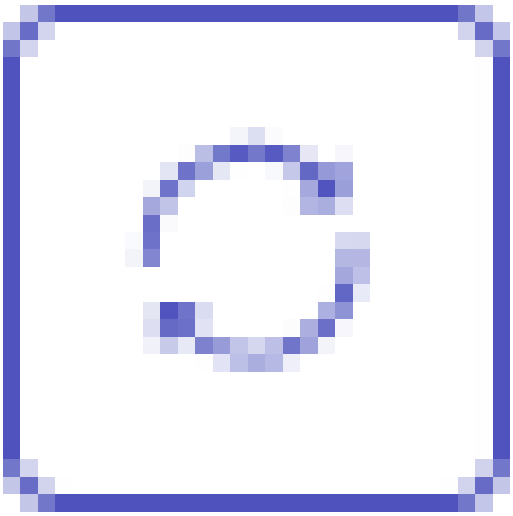
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Ansicht „Alle Integrationen“. (Fortsetzung)

Aktion	Beschreibung
	• **Deaktiviert**: Zeigt alle Integrationen an, die sich in einem deaktivierten Status befinden. • **Entwurf**: Zeigt alle Integrationen an, die sich im Entwurfsstatus befinden.
	Diese Aktion verwenden, um alle Integrationen in Form von Karten anzuzeigen.
	Diese Aktion verwenden, um alle Integrationen in Form von Listen anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Ansicht „Alle Integrationen“. (Fortsetzung)

Aktion	Beschreibung
	Diese Aktion verwenden, um die Seite „Alle Integrationen“ zu aktualisieren.
	Verwenden Sie diese Aktion, um alle Integrationen basierend auf den folgenden Kriterien zu sortieren: • **Zuletzt geändert (aktuell)** • **Zuletzt geändert (am ältesten)** • **Name A–Z** • **Name (Z–A)**
In Katalog suchen	Diese Aktion verwenden, um anhand des Namens und der Beschreibung im Katalog nach konfigurierten Integrationen zu suchen.

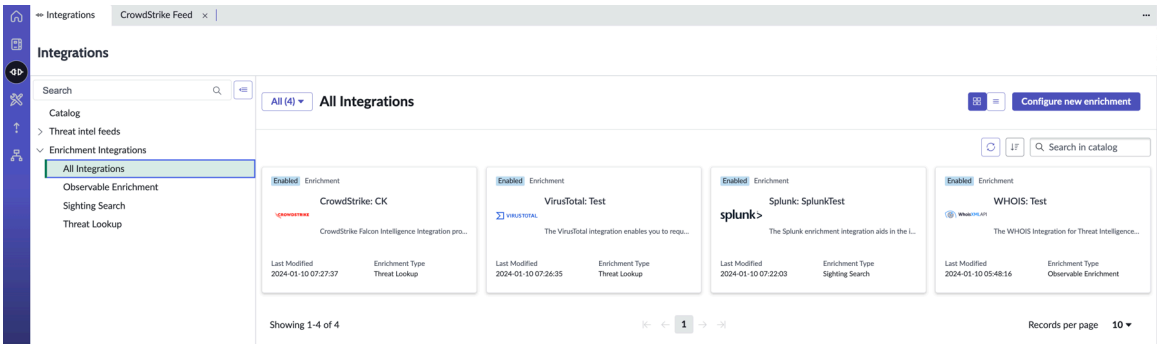
Automatische Übersetzung

Konfigurieren Sie eine neue Ergänzung in der Ansicht „Alle Integrationen“.

Sie können neue Ergänzungen in der Ansicht „Alle Integrationen“ oder direkt in den Abschnitten Ergänzung erkennbarer Elemente, Sichtungssuche bzw. Bedrohungssuche konfigurieren. Um die neue Ergänzung über die Ansicht „Alle Integrationen“ zu konfigurieren, führen Sie die folgenden Schritte aus.

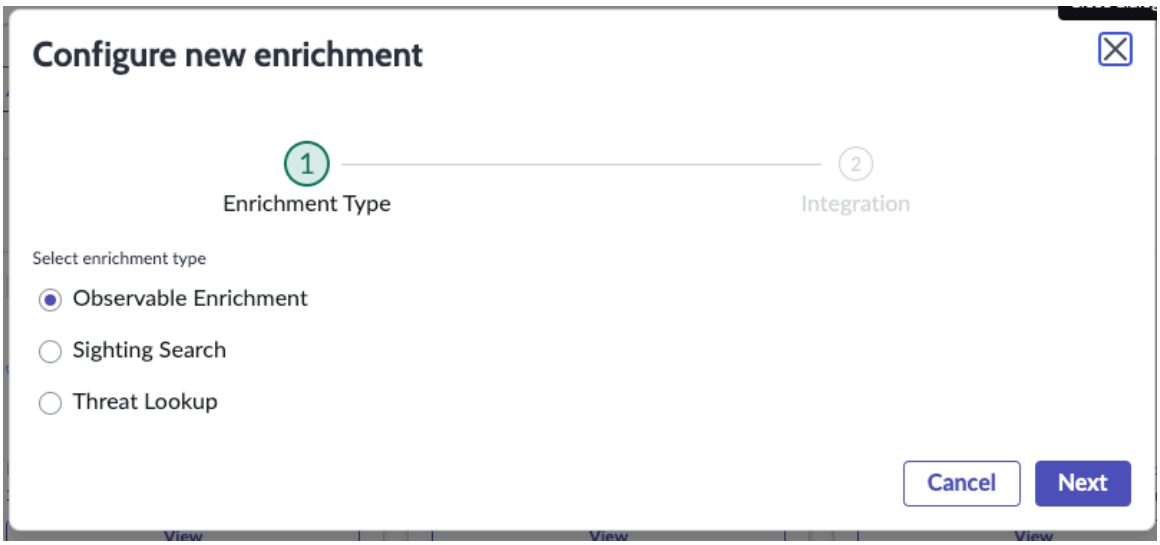
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**, und wählen Sie den Abschnitt **Alle Integrationen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf die Aktion **Neue Ergänzung konfigurieren**.

   Das Popup-Fenster „Neue Ergänzung konfigurieren“ wird mit drei Ergänzungstypen angezeigt: Ergänzung erkennbarer Elemente, Sichtungssuche oder Bedrohungssuche. Sie müssen auswählen, welche Art von Ergänzung Sie konfigurieren möchten.



4. Wählen Sie einen Ergänzungstyp aus, und klicken Sie auf **Weiter**.

   Dadurch gelangen Sie zum Popup-Fenster, das die verfügbaren Integrationen anzeigt. Sie müssen die Integration auswählen, die Sie konfigurieren möchten.

5. Wählen Sie eine Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Auswählen**.

   Dadurch gelangen Sie zur Seite „Neue Ergänzungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig bereits mit Details der ausgewählten Integration gefüllt. Beispiel: WHOIS-Integration.

6. Füllen Sie die Felder im Formular „Neue Integration erstellen“ aus.

Konfigurieren Sie das neue Formular zur Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: WHOIS1.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten sind standardmäßig vorab ausgefüllt. Beispiel: WHOIS.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Ergänzung erkennbarer Elemente. Die Details des ausgewählten Integrationstyps sind standardmäßig vorab ausgefüllt. Die folgenden Integrationstypen werden unterstützt: ○ Ergänzung erkennbarer Elemente ○ Sichtungssuche ○ Bedrohungssuche
Beschreibung	Geben Sie eine eindeutige Beschreibung für die neue Ergänzungsintegration ein.

7. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.

   Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Integrationen.

8. Klicken Sie auf die Aktion **Speichern**, um die Konfiguration der Ergänzungsintegration zu speichern und zu erstellen.

   Die angegebenen Details werden validiert, und standardmäßig ist der Status der Ergänzungsintegration deaktiviert.

9. (Optional) Klicken Sie auf die Aktion **Als Entwurf speichern,** um nur die Integrationskonfigurationen als Entwurf zu speichern. Anwender können eine Integration nicht aktivieren, wenn sie als Entwurf gespeichert ist

   Wenn Sie sich bezüglich der Konfigurationsdetails nicht sicher sind, können Sie die Option **Als Entwurf speichern** verwenden. Nachdem Sie die Konfigurationsdetails abgerufen haben, können Sie die verbleibenden Informationen in die Entwurfsversion eintragen und sie erstellen.

10. Zum Aktivieren der Ergänzungsintegration klicken Sie auf **Aktivieren**.

    Die Ergänzungsintegration wurde erfolgreich aktiviert.

11. Sie können eine bestimmte Ergänzungsintegration auch über das Menü „Aktionen“ der erforderlichen Integrationskachel auf der Seite „Katalog“ oder „Ergänzungsintegrationen“ aktivieren, deaktivieren oder löschen.

Konfigurieren Sie die Anreicherung erkennbarer Elemente

Sie können die Threat Intelligence-Anreicherung für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Welche Implementierungen ausgeführt werden, hängt von denen ab, die Sie aktiviert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Threat Intelligence-Sicherheitszentrum unterstützt ab sofort nur die Ergänzung erkennbarer Elemente für die WHOIS-Integration. Weitere Informationen finden Sie unter Konfigurieren und aktivieren Sie die Whois-Integration.

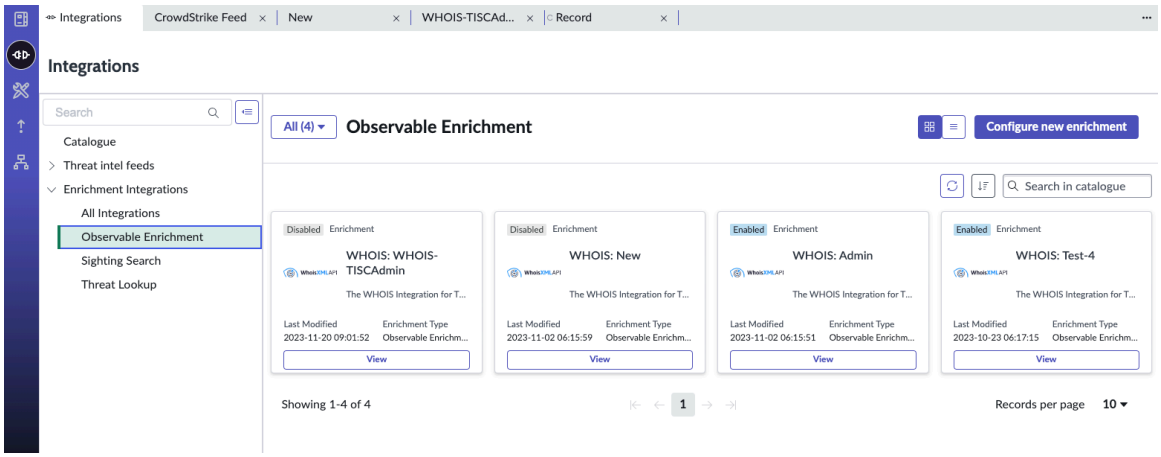
Hinweis:
Das Modul „Ergänzungsintegrationen“ wird nur angezeigt, wenn mindestens eine der Integrationen, die eine der Fähigkeiten unterstützen, in der Anwendung installiert ist.

Warum und wann dieser Vorgang ausgeführt wird

Der Abschnitt „Anreicherung erkennbarer Elemente“ enthält nur die Integrationen mit dem Integrationstyp Ergänzung erkennbarer Elemente. In diesem Abschnitt werden Karten für alle konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

Prozedur

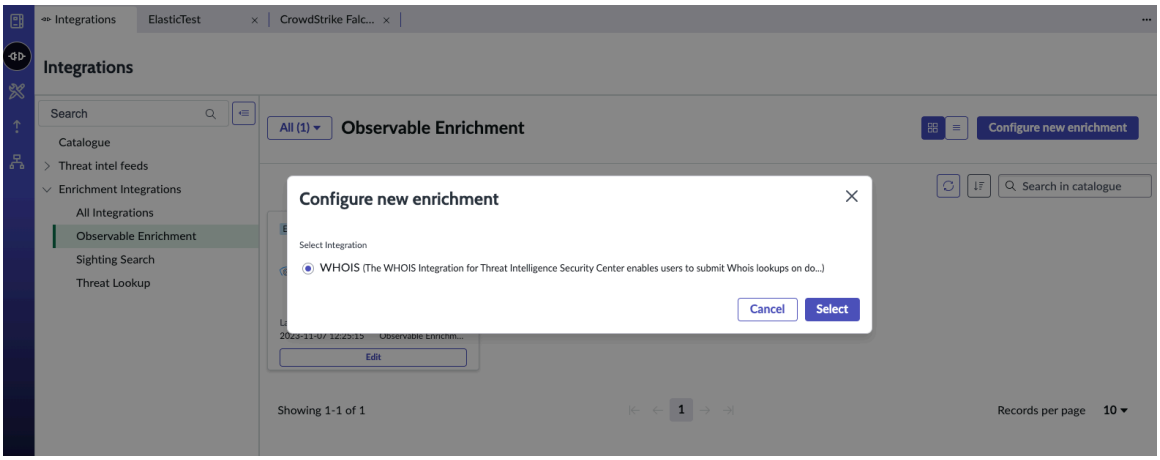
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**, und wählen Sie den Abschnitt **Anreicherung erkennbarer Elemente** aus.



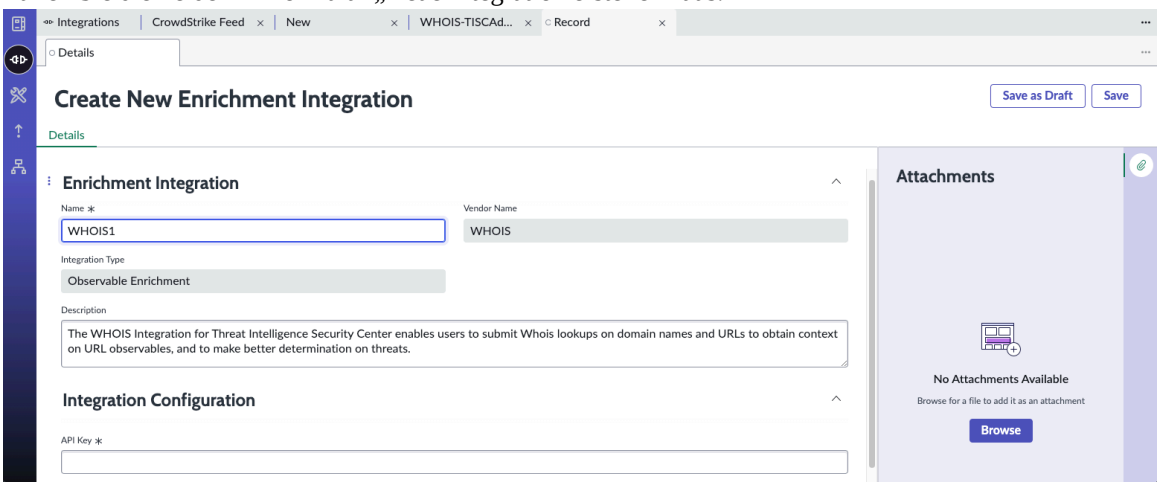
3. Klicken Sie auf die Aktion **Neue Ergänzung konfigurieren**.
   Dadurch gelangen Sie zum Popup-Fenster, das die verfügbaren Integrationen anzeigt. Sie müssen die Integration auswählen, die Sie konfigurieren möchten.
4. Wählen Sie eine Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Auswählen**.
   Dadurch gelangen Sie zur Seite „Neue Ergänzungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig bereits mit Details der ausgewählten Integration gefüllt. Beispiel: WHOIS-Integration.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder im Formular „Neue Integration erstellen“ aus.



6. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.
Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Apps.

7. Klicken Sie auf die Aktion **Speichern**, um die neue Konfiguration der Ergänzungsintegration zu speichern und zu erstellen.
Nachdem Sie auf die Aktion **Speichern** oder **Aktivieren** geklickt haben, wird die Integration anhand der angegebenen Integrationskonfigurationen validiert. Standardmäßig ist der Status der Ergänzungsintegration auf „deaktiviert“ festgelegt.

8. Klicken Sie auf die Aktion **Als Entwurf speichern,** um nur die an der Ergänzungskonfiguration vorgenommenen Aktualisierungen zu speichern und nicht zu erstellen.
Wenn Sie sich bezüglich der Konfigurationsdetails nicht sicher sind, können Sie die Option **Als Entwurf speichern** verwenden. Nachdem Sie die Konfigurationsdetails abgerufen haben, können Sie die verbleibenden Informationen in die Entwurfsversion eintragen und sie erstellen.

9. Zum Aktivieren der Ergänzungsintegration klicken Sie auf **Aktivieren**.
Die Ergänzungsintegration wurde erfolgreich aktiviert. Sie können eine bestimmte Ergänzungsintegration auch über das Menü „Aktionen“ der erforderlichen Integrationskachel auf der Seite „Katalog“ oder „Ergänzungsintegrationen“ aktivieren, deaktivieren oder löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Sichtungssuche

Sie können eine Sichtungssuche für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, wie oft die erkennbaren Elemente in Ihren Organisationsprotokollen gesehen wurden. Sie können eine Sichtungssuche für erkennbare Elemente innerhalb einer ausgewählten Anzahl von Tagen oder innerhalb eines Datumsbereichs durchführen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Das Modul „Ergänzungsintegrationen“ wird nur angezeigt, wenn mindestens eine der Integrationen, die eine der Fähigkeiten unterstützen, in der Anwendung installiert ist.

Threat Intelligence-Sicherheitszentrum unterstützt die Sichtungssuche nur für die folgenden Integrationen:

- Splunk-Suche
- ElasticSearch

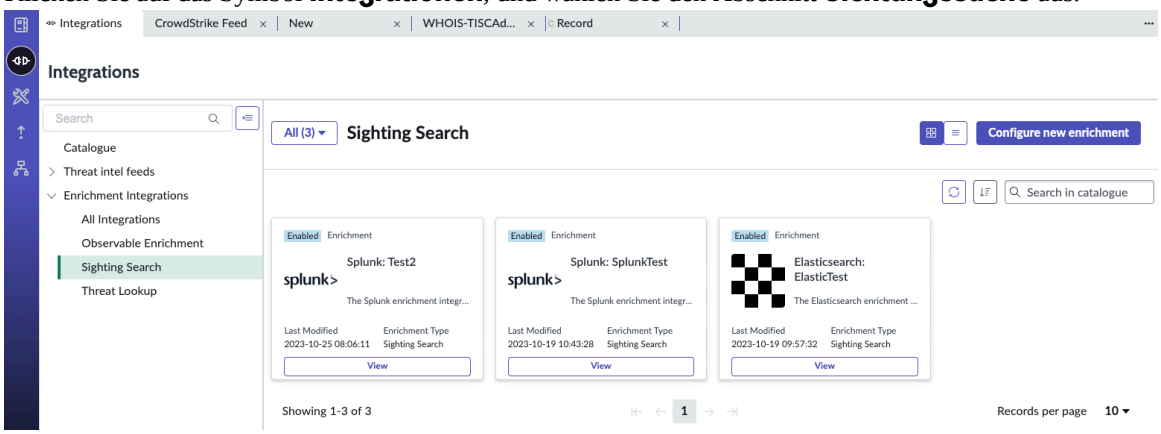
Warum und wann dieser Vorgang ausgeführt wird

Der Abschnitt „Sichtungssuche“ enthält nur Integrationen mit dem Integrationstyp „Sichtungssuche“.

In diesem Abschnitt werden Karten für alle konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

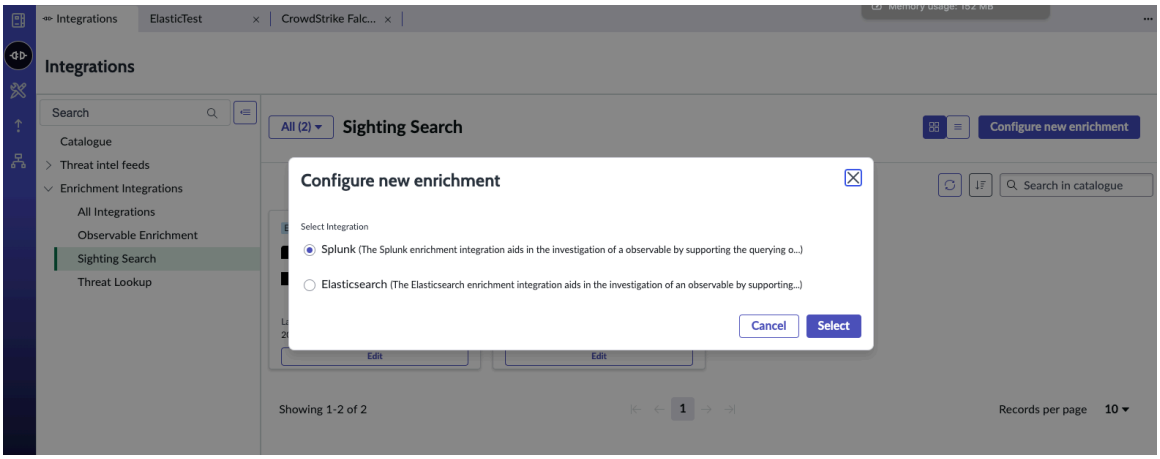
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**, und wählen Sie den Abschnitt **Sichtungssuche** aus.

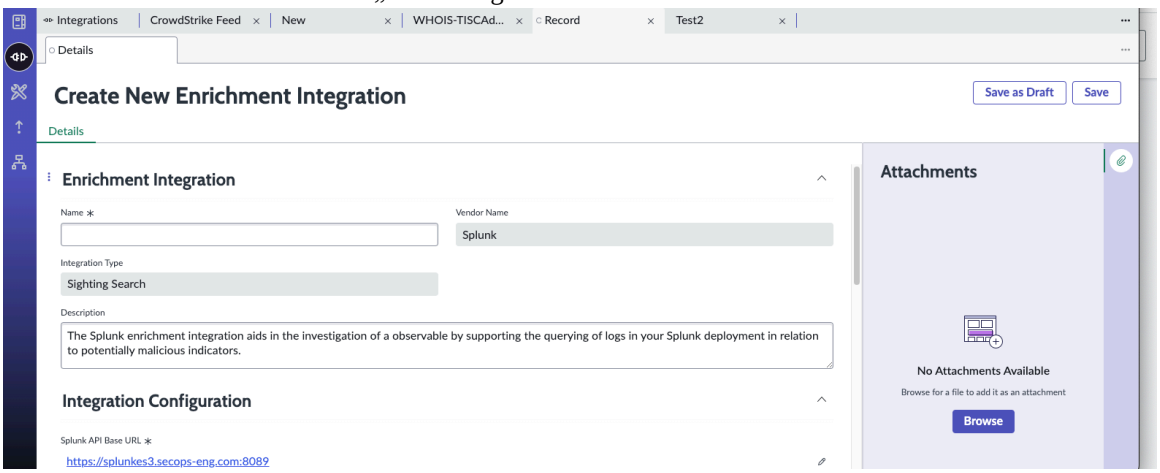


3. Klicken Sie auf die Aktion **Neue Ergänzung konfigurieren**.
   Dadurch gelangen Sie zum Popup-Fenster, das die verfügbaren Integrationen anzeigt. Sie müssen die Integration auswählen, die Sie konfigurieren möchten.
4. Wählen Sie eine Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Auswählen**.
   Dadurch gelangen Sie zur Seite „Neue Ergänzungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig bereits mit Details der ausgewählten Integration gefüllt. Beispiel: Splunk-Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder im Formular „Neue Integration erstellen“ aus.



6. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.
   Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Apps.

7. Klicken Sie auf die Aktion **Speichern**, um die neue Konfiguration der Ergänzungsintegration zu speichern und zu erstellen.
   Die angegebenen Details werden validiert, und standardmäßig ist der Status der Ergänzungsintegration deaktiviert.

8. Klicken Sie auf die Aktion **Als Entwurf speichern,** um nur die an der Ergänzungskonfiguration vorgenommenen Aktualisierungen zu speichern und nicht zu erstellen.
   Wenn Sie sich bezüglich der Konfigurationsdetails nicht sicher sind, können Sie die Option **Als Entwurf speichern** verwenden. Nachdem Sie die Konfigurationsdetails abgerufen haben, können Sie die verbleibenden Informationen in die Entwurfsversion eintragen und sie erstellen.

9. Zum Aktivieren der Ergänzungsintegration klicken Sie auf **Aktivieren**.
   Die Ergänzungsintegration wurde erfolgreich aktiviert. Sie können auch eine bestimmte Ergänzungsintegration aktivieren, indem Sie das Menü „Aktionen“ der erforderlichen Integrationskachel auf der Seite „Katalog“ oder „Alle Integrationen“ verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie Abfragen für die Sichtungssuche

Sie können Sichtungssuchkonfigurationen verwenden, um die Abfragen zu definieren, die verwendet werden, um die Verbreitung von erkennbaren Elementen in Ihrer Umgebung im Rahmen der Untersuchung von erkennbaren Elementen zu ermitteln.

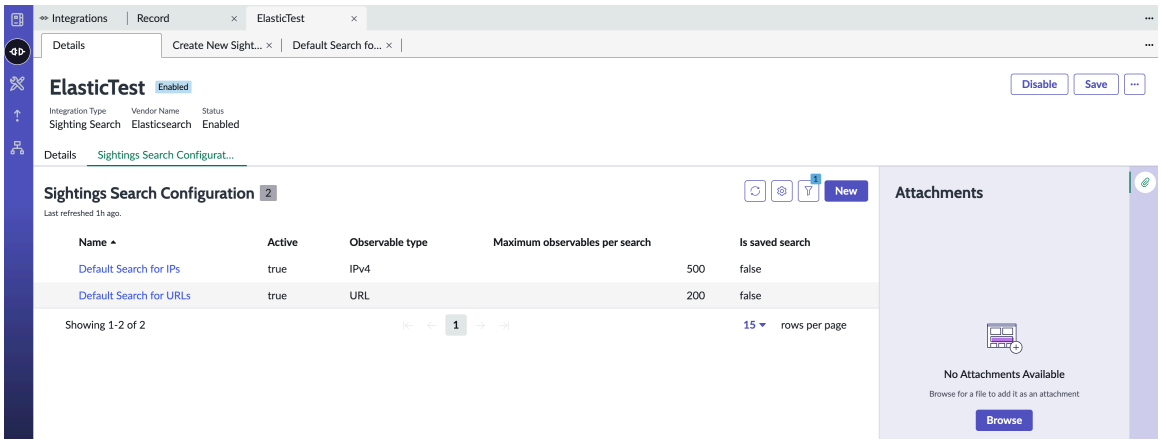
Zeigen Sie Abfragen für die Sichtungssuche an

Erforderliche Rolle: sn_sec_tisc.admin

Um die Konfigurationen für die Sichtungssuche anzuzeigen, gehen Sie wie folgt vor:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten**.
4. Wählen Sie die Registerkarte **Sichtungssuchkonfigurationen** aus.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.



5. Klicken Sie auf die erforderliche Sichtungssuche-Konfiguration, um die Details der Konfiguration anzuzeigen.
6. Um eine Testabfrage für die Sichtungssuche zu generieren, klicken Sie auf die Aktion **Testabfrage für Sichtungssuche generieren**.

   Hinweis:
   Die Aktion **„Testabfrage für Sichtungssuche generieren“** funktioniert nur, wenn Sie Abfrageparameter für die Sichtungssuche konfiguriert haben. Weitere Informationen finden Sie unter Sichtungssuchparameter werden verwendet.

7. Geben Sie im Popup-Fenster „Testabfrage für Sichtungssuche generieren“ mehrere erkennbare Elemente ein, oder fügen Sie sie mithilfe von Kommas, neuen Zeilen, Registerkarten oder Pipe-Trennzeichen ein, um eine Testabfrage zu generieren.
8. Klicken Sie auf **Generieren**, um die Testabfrage für die Sichtungssuche zu generieren.
9. Sie können auf der Registerkarte Sichtungssuchkonfigurationen auch die folgenden Aktionen ausführen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um die Liste der Sichtungssuchkonfigurationen zu aktualisieren, klicken Sie auf das Symbol .

b. Um eine Listenaktion für die Sichtungssuchkonfigurationen auszuführen, klicken Sie auf das Symbol .

Sie können die folgenden beiden Listenaktionen ausführen:

- **Spalten bearbeiten**: Sie können diese Aktion verwenden, um vorhandene Spalten hinzuzufügen oder zu entfernen und die Reihenfolge entsprechend Ihren Anforderungen zu ändern.
- **Breiten zurücksetzen**: Mit dieser Aktion können Sie die Breiten der Spalten zurücksetzen.

c. Um Konfigurationen für die Sichtungssuche basierend auf Bedingungen zu filtern, klicken Sie auf das Symbol .

Der Wert 1 gibt an, dass eine Bedingung für die Filterung verwendet wird.

Erstellen Sie Konfigurationen für die Sichtungssuche

Erforderliche Rolle: sn_sec_tisc.admin

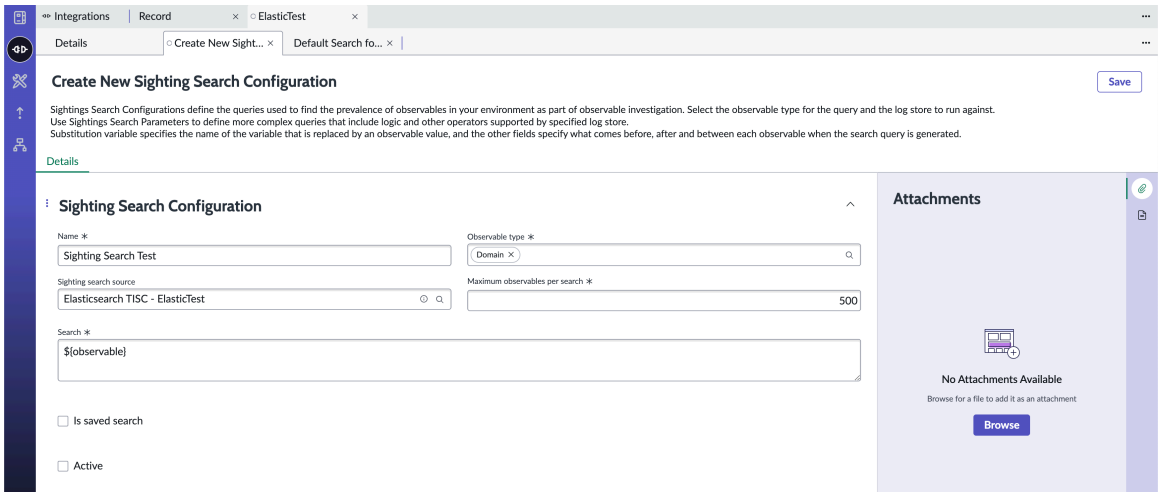
Maximum observables per search = "maximum number of observables that can be substituted in a single search query"
Search = "Search query that should be executed in sighting search source. Search query can contain substitution variables that would be substituted with observables of specific type as configured in sighting search parameters when sighting search query is formed"

Um eine Sichtungssuchkonfiguration zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten**.
4. Wählen Sie die Registerkarte **Sichtungssuchkonfigurationen** aus.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.
5. Zum Erstellen einer Sichtungssuchkonfiguration klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Füllen Sie die Felder im Formular aus.

Erstellen Sie eine Sichtungssuche-Konfiguration

Feld	Beschreibung
Name	Name für die Sichtungssuche-Konfiguration.
Erkennbarer Typ	Definiert den Typ der Kategorie des erkennbaren Elements.
Sichtungssuchquelle	Definiert die für die Integration konfigurierte Quelle.
Maximale erkennbare Elemente pro Suche	Die Anzahl der erkennbaren Elemente bevor die Suchabfrage in mehrere Abfragen aufgeteilt wird. Legen Sie diesen Wert für diese Integration auf 500 fest.
Suchen	Fügen Sie eine native Suchzeichenfolge hinzu, um eine Abfrage zu bilden. Beispiel: ${observable}.
Ist gespeicherte Suche	Führt eine gespeicherte Suche aus, d. h. das Feld Name muss mit dem Namen der gespeicherten Suche übereinstimmen.
Aktiv	Abfrage wird nur ausgeführt, wenn die Option „Aktiv“ ausgewählt ist.

7. Klicken Sie auf **Speichern**.

Sichtungssuchparameter werden verwendet

Sie können Sichtungssuchparameter verwenden, die komplexere Abfragen definieren, einschließlich Logik und anderer Operatoren, die vom angegebenen Protokollspeicher unterstützt werden.

Sichtungssuchparameter anzeigen

Erforderliche Rolle: sn_sec_tisc.admin

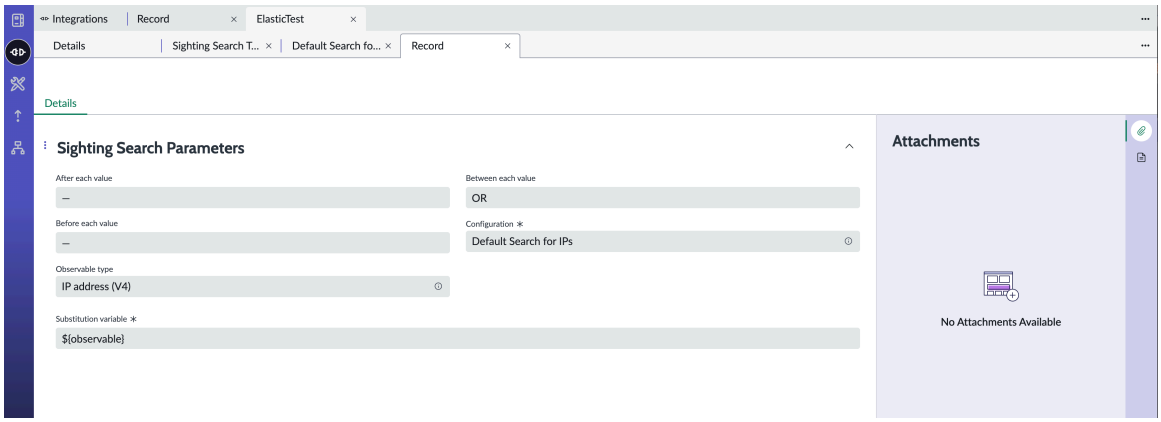
Um die Parameter für die Sichtungssuche anzuzeigen, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten**.
4. Wählen Sie die Registerkarte **Sichtungssuchkonfigurationen** aus.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.

5. Klicken Sie auf die erforderliche Sichtungssuche-Konfiguration, um die Details der Konfiguration anzuzeigen.



6. Wählen Sie die Registerkarte **Sichtungssuchparameter** aus.

   Sie können die Liste der Sichtungssuchparameter anzeigen.

7. Klicken Sie auf den erforderlichen Sichtungssuchparameter, um die Details des Parameters anzuzeigen.
8. Sie können auf der Registerkarte Sichtungssuchparameter auch die folgenden Aktionen ausführen:
   a. Um die Liste der Sichtungssuchparameter zu aktualisieren, klicken Sie auf das Symbol .
   b. Um eine Listenaktion für die Sichtungssuchparameter auszuführen, klicken Sie auf das Symbol .

      Spalten bearbeiten: Sie können diese Aktion verwenden, um vorhandene Spalten hinzuzufügen oder zu entfernen und die Reihenfolge entsprechend Ihren Anforderungen zu ändern.

   c. Um Sichtungssuchparameter basierend auf Bedingungen zu filtern, klicken Sie auf das Symbol .

      Der Wert 1 gibt an, dass eine Bedingung für die Filterung verwendet wird.

Sichtungssuchparameter erstellen

Beispiel für die Abfragegenerierung

```
Configured Query: ${Observable}

Observables Substitutes for Sightings search: Obs1 , Obs2
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

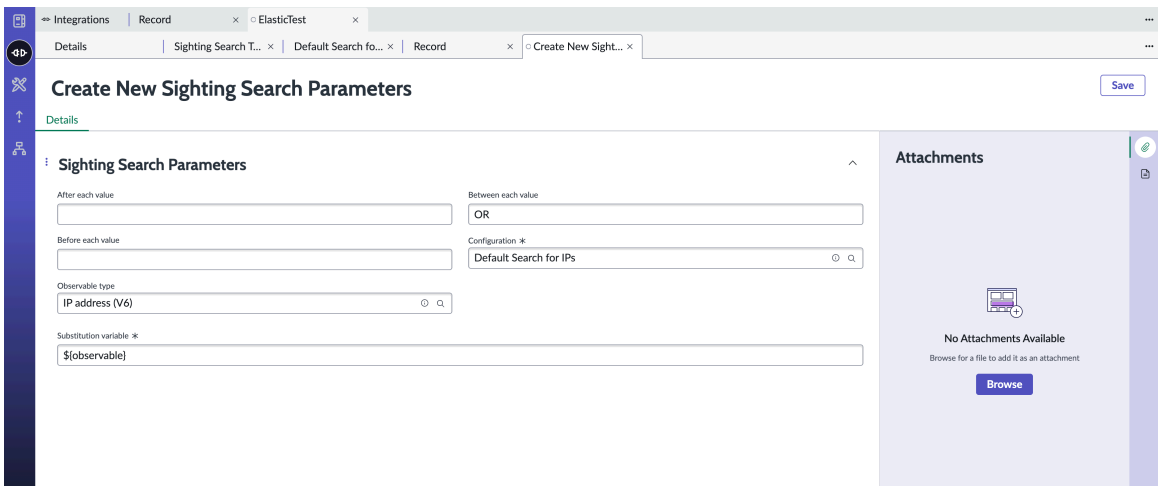
```
Query: {Before each Value}Obs1{After each Value}{Between each value}{Before each Value}Obs2{After each Value}

Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: “ip_address = 172.32.31.41 OR ip_address = 192.168.10.12”
```

Um einen Sichtungssuchparameter zu erstellen, gehen Sie wie folgt vor:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten**.
4. Wählen Sie die Registerkarte **Sichtungssuchkonfigurationen** aus.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.
5. Klicken Sie auf die erforderliche Sichtungssuche-Konfiguration, um die Details der Konfiguration anzuzeigen.
6. Wählen Sie die Registerkarte **Sichtungssuchparameter** aus.

   Sie können die Liste der Sichtungssuchparameter anzeigen.
7. Klicken Sie auf **Neu**, um einen Sichtungssuchparameter zu erstellen.



8. Füllen Sie die Felder im Formular aus.

Erstellen Sie einen Sichtungssuchparameter

Feld	Beschreibung
Nach jedem Wert	Der Sichtungssuchparameter nach jedem erkennbaren Element, wenn die Suchabfrage generiert wird.
Zwischen jedem Wert	Der Sichtungssuchparameter zwischen jedem erkennbaren Element, wenn die Suchabfrage generiert wird. Beispiel: ODER.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vor jedem Wert	Der Sichtungssuchparameter vor jedem erkennbaren Element, wenn die Suchabfrage generiert wird.
Konfiguration	Die Konfigurationsdetails des Suchparameters.
Erkennbarer Typ	Definiert den Typ der Kategorie des erkennbaren Elements.
Ersetzungsvariable	Gibt den Namen der Variablen an, die durch den Wert eines erkennbaren Elements ersetzt wird.

9. Klicken Sie auf **Speichern**.

Konfigurieren Sie die Bedrohungssuche

Sie können die Bedrohungssuche so konfigurieren, dass eine Suche nach ausgewählten erkennbaren Elementen durchgeführt wird. Wenn es sich bei den erkennbaren Elementen um einen von Threat Intelligence erkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben. Sie können eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen, um die Bösartigkeit eines erkennbaren Elements zu bestimmen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Das Modul „Ergänzungsintegrationen“ wird nur angezeigt, wenn mindestens eine der Integrationen, die eine der Fähigkeiten unterstützen, in der Anwendung installiert ist.

Threat Intelligence-Sicherheitszentrum unterstützt die Bedrohungssuche nur für die folgenden Integrationen:

- VirusTotal
- CrowdStrike Intelligence

Weitere Informationen finden Sie unter Bedrohungssuche.

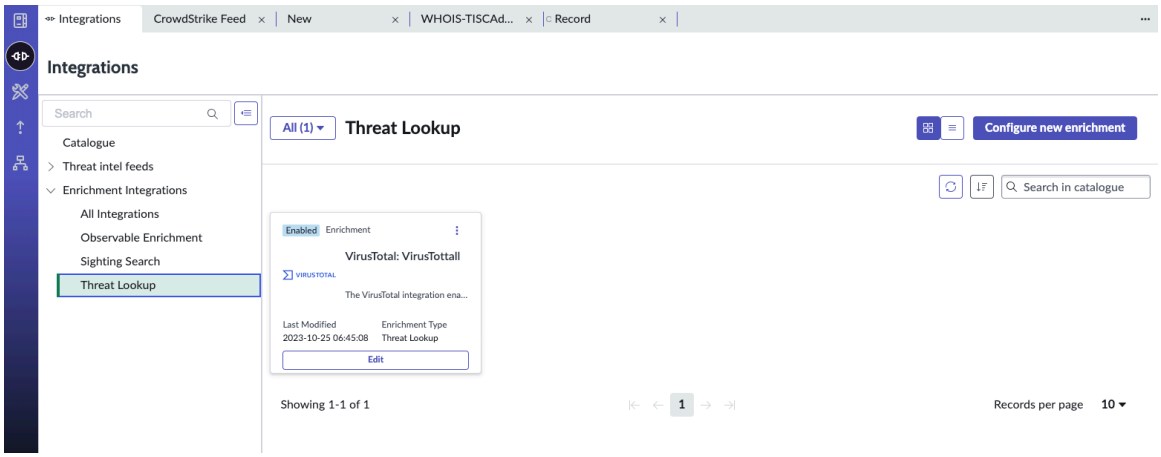
Warum und wann dieser Vorgang ausgeführt wird
Der Abschnitt „Bedrohungssuche“ enthält nur die Integrationen mit dem Integrationstyp „Bedrohungssuche“.

In diesem Abschnitt werden Karten für alle konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

Prozedur

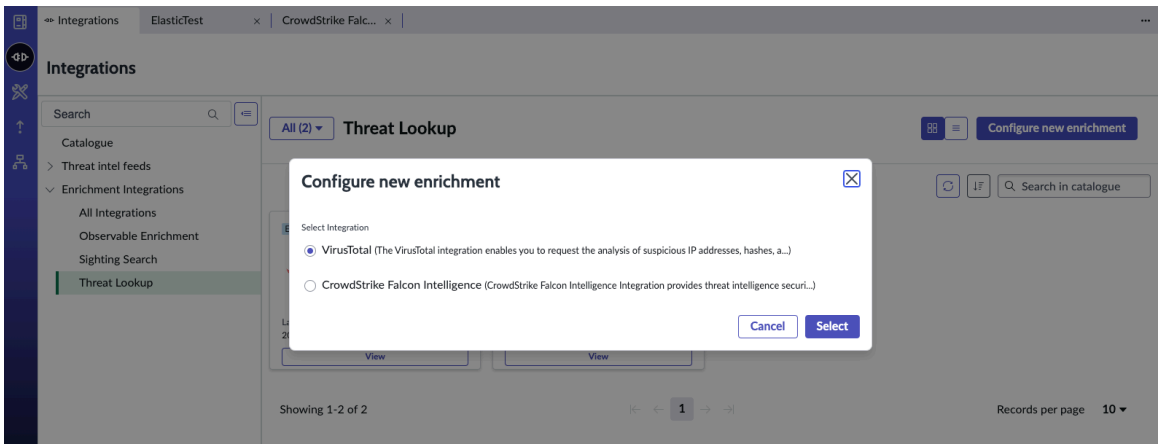
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Integrationen**, und wählen Sie den Abschnitt **„Bedrohungssuche“** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

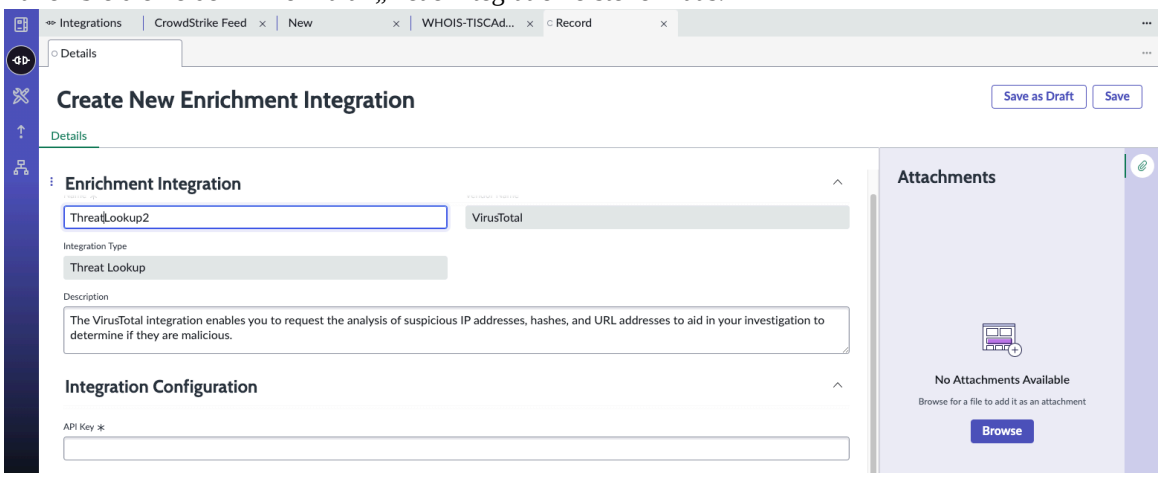


3. Klicken Sie auf die Aktion **Neue Ergänzung konfigurieren**.
   Dadurch gelangen Sie zum Popup-Fenster, das die verfügbaren Integrationen anzeigt. Sie müssen die Integration auswählen, die Sie konfigurieren möchten.

4. Wählen Sie und Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Auswählen**.
   Dadurch gelangen Sie zur Seite „Neue Ergänzungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig bereits mit Details der ausgewählten Integration gefüllt. Beispiel: VirusTotal-Integration.



5. Füllen Sie die Felder im Formular „Neue Integration erstellen“ aus.



6. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Apps.

7. Klicken Sie auf die Aktion **Speichern**, um die neue Konfiguration der Ergänzungsintegration zu speichern und zu erstellen.
   Die angegebenen Details werden validiert, und standardmäßig ist der Status der Ergänzungsintegration deaktiviert.
8. Klicken Sie auf die Aktion **Als Entwurf speichern,** um nur die an der Ergänzungskonfiguration vorgenommenen Aktualisierungen zu speichern und nicht zu erstellen.
   Wenn Sie sich bezüglich der Konfigurationsdetails nicht sicher sind, können Sie die Option **Als Entwurf speichern** verwenden. Nachdem Sie die Konfigurationsdetails abgerufen haben, können Sie die verbleibenden Informationen in die Entwurfsversion eintragen und sie erstellen.
9. Zum Aktivieren der Ergänzungsintegration klicken Sie auf **Aktivieren**.
   Die Ergänzungsintegration wurde erfolgreich aktiviert. Sie können eine bestimmte Ergänzungsintegration auch über das Menü „Aktionen“ der erforderlichen Integrationskachel auf der Seite „Katalog“ oder „Ergänzungsintegrationen“ aktivieren, deaktivieren oder löschen.

Zeigen Sie Reputationsrechner für die Bedrohungssuche an

Sie können den Rechner für Ergebnisse der Bedrohungssuche anzeigen, um die Ergebnisse erkennbarer Elemente für Ihre Integration zu berechnen.

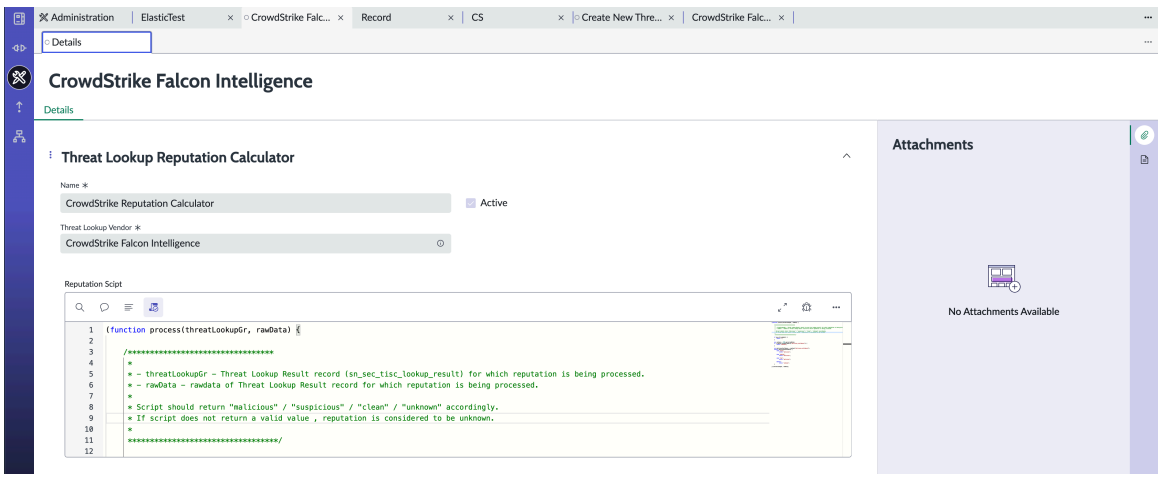
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Weitere Informationen zu den Reputationsrechnern der Bedrohungssuche finden Sie unter Verwaltung des Reputationsrechners der Bedrohungssuche.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Wählen Sie den Abschnitt **Rechner für Reputation der Bedrohungssuche** aus.
   Sie können die Liste der Reputationsrechner für die Bedrohungssuche anzeigen.
3. Klicken Sie auf den erforderlichen Reputationsrechner für die Bedrohungssuche, um die Details des Rechners anzuzeigen.



4. Im Abschnitt „Reputationsrechner für die Bedrohungssuche“ können Sie auch die folgenden Aktionen ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um die Liste der Reputationsrechner für die Bedrohungssuche zu aktualisieren, klicken Sie auf das Symbol .

b. Um eine Listenaktion für die Reputationsrechner der Bedrohungssuche auszuführen, klicken Sie auf das Symbol .

Sie können die folgenden beiden Listenaktionen ausführen:

- **Spalten bearbeiten**: Sie können diese Aktion verwenden, um vorhandene Spalten hinzuzufügen oder zu entfernen und die Reihenfolge entsprechend Ihren Anforderungen zu ändern.
- **Breiten zurücksetzen**: Mit dieser Aktion können Sie die Breiten der Spalten zurücksetzen.

c. Um die Reputationsrechner für die Bedrohungssuche basierend auf Bedingungen zu filtern, klicken Sie auf das Symbol .

Der Wert 1 gibt an, dass eine Bedingung für die Filterung verwendet wird.

TISC-Sicherheitstools – EDR

TISC Endpoint Detection and Response-Integrationen (EDR) konzentrieren sich auf die Identifizierung und Behebung von Sicherheitsbedrohungen auf Endpunktebene.

EDR-Netzwerklösungen prognostizieren neu auftretende Bedrohungen, verhindern sie und tragen zur Verbesserung des Sicherheitsstatus des gesamten Unternehmens bei.

Durch die Integration mit anderen Sicherheitstools wie EDR ermöglicht TISC die proaktive Bedrohungsüberwachung auf Endpunkten und verbessert dadurch den allgemeinen Sicherheitsstatus und die Resilienz gegenüber sich entwickelnden Bedrohungen.

Zugehörige Informationen

CrowdStrike Integration mit Falcon EDR

CrowdStrike Integration mit Falcon EDR

Die Integration mit CrowdStrike Falcon EDR ermöglicht eine kontinuierliche Überwachung und Echtzeitwarnung basierend auf den Informationen von TISC.

Diese Integration kann dazu beitragen, Sicherheitsabläufe zu optimieren und potenzielle Risiken für den Geschäftsbetrieb des Unternehmens zu reduzieren.

Konfigurieren Sie die Crowdstrike Falcon EDR-Integration

Bevor Sie die CrowdStrike Falcon EDR-Integration verwenden können, müssen Sie sie aus dem ServiceNow Store Store herunterladen und die entsprechende Client-ID und den geheimen Clientschlüssel hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Anwendung Threat Intelligence Security Center muss installiert und aktiviert sein.
- Rufen Sie die API-Client-ID und das API-Client-Geheimnis aus der Falcon-Konsole CrowdStrike ab.
- Aktivieren Sie in den API-Bereichen des Falcon-Portals CrowdStrike den **Lese- und Schreibzugriff für die IoC-Verwaltung**.

Prozedur

1. Greifen Sie mit Ihrer -Instanz auf **Threat Intelligence-Sicherheitszentrum**zu.
2. Laden Sie die -Integration aus dem herunter ServiceNow Store.
3. Auswahlvorgang **Integrationen** > **Sicherheitstools** > **EDR**.
4. Klicken Sie auf **Neues Sicherheitstool konfigurieren**, um CrowdStrike die Falcon EDR-Integration zu konfigurieren.
5. Wählen Sie die Option **CrowdStrike Falcon EDR** aus.
6. Füllen Sie die Felder im Formular „Neues Sicherheitstool konfigurieren“ aus.

Neue Ergänzungsintegration erstellen

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Sicherheitstool-Integration ein. Beispiel: CrowdStrike Falcon EDR.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: CrowdStrike Falcon EDR.
Beschreibung	Geben Sie die Beschreibung für die neue Sicherheitstool-Integration ein.
Integrationstyp	Option, die den Integrationstyp anzeigt.
Integrationskategorie	Option, mit der die Integrationskategorie angezeigt wird.
Integrationskonfiguration	
Basis-URL	Die Basis-URL ist die Basis-URL der CrowdStrike-API. Der Standardwert ist https://api.crowdstrike.com . Weitere Informationen finden Sie unter https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis#k9578c40
Client-ID	Die Client-ID, die Sie von CrowdStrikeerhalten haben. Weitere Informationen finden Sie unter https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .
Geheimer Clientschlüssel	Der geheime Clientschlüssel, den Sie von CrowdStrikeerhalten haben. Weitere Informationen finden Sie unter https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablaufzeitraum in Tagen für jede Art von erkennbaren Elementen	Der Ablaufzeitraum in Tagen, der für jede Art von erkennbarem Element gilt, wenn sie an CrowdStrike EDR gesendet werden. **Hinweis:** Diese Option ist ein Fallback-Ablaufzeitraum, wenn die Ablaufzeit nicht für einen bestimmten erkennbaren Elementtyp festgelegt ist.
Ablaufzeit erkennbarer IP-Elemente	Der Ablaufzeitraum in Tagen, der für den IP-Typ des erkennbaren Elements angewendet wird, wenn es an CrowdStrike EDR gesendet wird.
Ablaufzeit erkennbarer Elemente der Domäne	Der Ablaufzeitraum in Tagen, der für den Domänentyp des erkennbaren Elements gilt, wenn es an CrowdStrike EDR gesendet wird.
Ablaufzeit des erkennbaren Elements im Hash	Der Ablaufzeitraum in Tagen, der für den Hash-Typ des erkennbaren Elements angewendet wird, wenn er an CrowdStrike EDR gesendet wird.

7. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig ist der Status der CrowdStrike EDR-Integration deaktiviert.
8. Klicken Sie auf **Aktivieren**, um die CrowdStrike EDR-Integration zu aktivieren.

Hinweis:
Für CrowdStrike die Falcon EDR-Integration sind mehrere Konfigurationen zulässig.

Erkennbare Elemente an EDR senden

Erkennbare Elemente an das EDR-Sicherheitstool senden

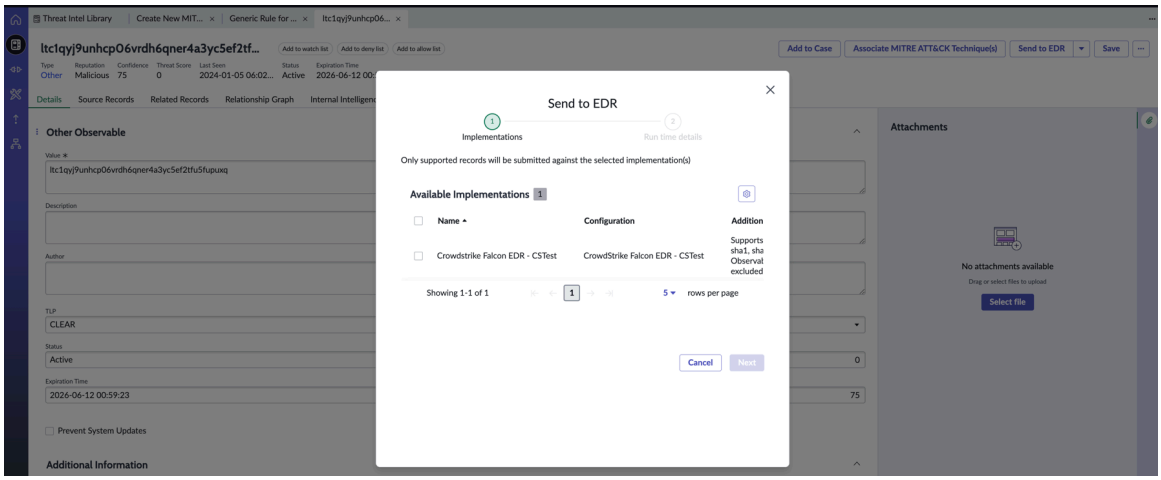
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

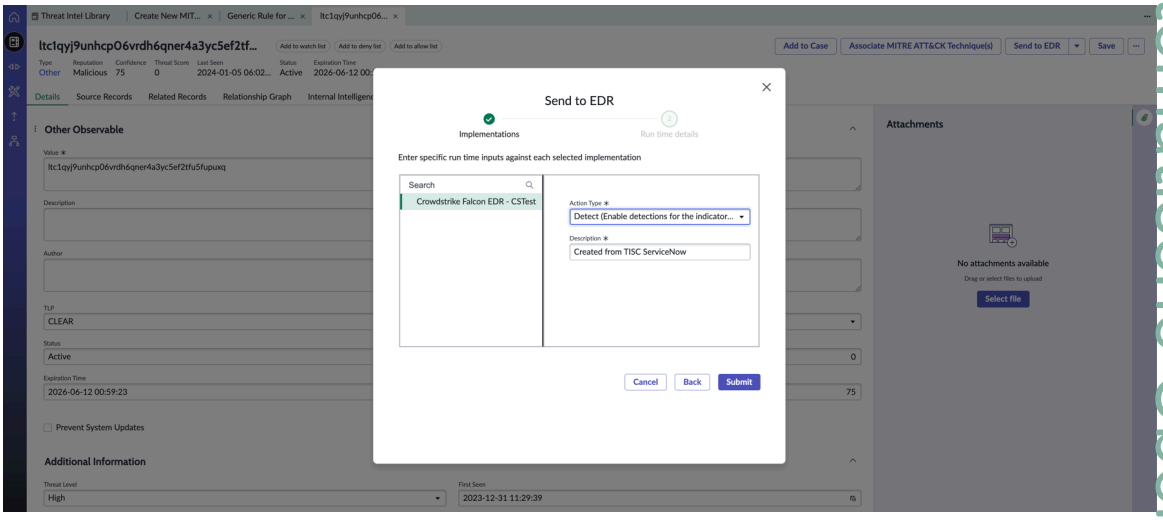
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Öffnen Sie einen beliebigen erkennbaren Datensatz.
5. Wählen Sie **An EDR senden aus**.
   Der modale Bildschirm „An EDR **-Implementierungen** senden“ wird angezeigt.
6. Wählen Sie die gewünschte Implementierung aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie die Laufzeitdetails wie **Aktionstyp** und **Beschreibung** der Implementierung aus.



Die verfügbaren Optionen für CrowdStrike während der Implementierungslaufzeit Details sind:

- **Keine Aktion (Indikator zur späteren Verwendung speichern, aber keine Aktion durchführen)**: In der Formularansicht des erkennbaren Elements ist der Bedrohungsschweregrad des erkennbaren Elements für CrowdStrike Falcon EDR optional.
- **Erkennen (Erkennungen für den Indikator im Bedrohungsschweregrad des Datensatzes aktivieren)**: In der Formularansicht des erkennbaren Elements ist der Bedrohungsschweregrad für CrowdStrike Falcon EDR obligatorisch. Der Bedrohungsschweregrad des erkennbaren Elements darf für das ausgewählte erkennbare Element nicht leer sein.

9. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ausgewählte Aktion wird ausgeführt, und es wird eine Informationsmeldung angezeigt, dass die Ausführung von „An EDR senden“ des erkennbaren Elements gestartet wurde.

Hinweis:

- Sobald die Ausführung initiiert oder abgeschlossen ist, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht.
- Die Aktion **„An EDR senden“** ist auch in der Liste der erkennbaren Elemente auf der Registerkarte **„Artefakte“** für einen Falldatensatz verfügbar. Weitere Informationen finden Sie unter Artefakte zu Fällen oder Fallaufgaben hinzufügen.

TISC-Sicherheitstools – Firewall

TISC-Sicherheitstools: Die Firewall verhindert den nicht autorisierten Zugriff auf das Netzwerk. Die Integration von Palo Alto mit TISC hilft beim Blockieren schädlicher IP-Adressen, URLs und Domänen mithilfe von EDL-Funktionen (External Dynamic List) mit ServiceNow Threat Intelligence-Daten.

Innerhalb von TISC verbessert durch die Integration mit anderen Sicherheitstools wie Palo Alto Networks die Netzwerksicherheit des gesamten Unternehmens.

Palo Alto Networks-Integration

Nach der Konfiguration der Palo Alto Networks-Integration kann der Bedrohungsanalyst der externen dynamischen Liste (External Dynamic List, EDL) schädliche IP-Adressen, URLs und Domänen hinzufügen oder diese Einträge aus der EDL entfernen, nachdem sie als nicht böswillig oder sauber bestätigt wurden.

Eine EDL ist eine Textdatei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihre Now Platform-Instanz, die der Palo Alto Networks-Firewall den Import von Objekten ermöglicht, die in der Liste enthalten sind, IP-Adressen, URLs und Domänen.

Erstellen Sie eine neue EDL für Palo Alto Networks

Erstellen Sie eine neue externe dynamische Liste (External Dynamic List, EDL) für Palo Alto Networks. Sobald Sie EDLs erstellt haben, können Sie mit der Erstellung von Einträgen für diese EDLs beginnen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Nachdem Sie die neu konfigurierte Palo Alto NGFW-Konfiguration gespeichert haben, navigieren Sie zum Abschnitt **EDLs**.
2. Klicken Sie auf **Neu**, um eine neue Externe Dynamische Liste (EDLs) zu erstellen.
3. Füllen Sie die Felder des Formulars aus.

Formular „Externe dynamische Liste für Palo Alto Networks-Firewall“.

Feld	Beschreibung
Name	Name der dynamischen Liste für Palo Alto Networks-Firewall.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erkennbarer Typ	Wählen Sie in der Auswahlliste einen erkennbaren Elementtyp aus, den diese EDL akzeptiert: IP (einschließlich CIDR), URL oder Domäne.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der EDL. 0 (Standardeinstellung) gibt an, dass der EDL-Eintrag nie abläuft. Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Es gibt keinen Höchstwert. Wenn Sie beispielsweise `30` Tage um den 1. November um 14:01 Uhr eingeben, läuft die EDL am 30. November um 14:01 Uhr ab. Alle Einträge in dieser EDL erben dann diesen Wert standardmäßig, es sei denn, Sie überschreiben den Wert auf Basis einzelner Einträge.
Change-Anforderungen erstellen	Dieses Kontrollkästchen ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in Ihrer Now Platform-Instanz zu erstellen, die an den EDL-Datensatz angehängt sind. Die Change-Anforderung wird verwendet, um die Abruf-URL für die EDL-Liste auf dem Palo Alto Networks Next-generation Firewall-Server zu konfigurieren. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch die Now Platform für Firewall-Richtlinien- oder Regeländerungen verwendet. Wenn Sie eine Anforderung erstellen, wird die EDL-Liste nach dem Schließen automatisch aktiviert.
Beschreibung	Beschreibung der dynamischen Liste der Palo Alto Networks-Firewalls. Der Name enthält im Allgemeinen die Typen von Websites und erkennbaren Elementen, die erwartet werden, dass sie sich in dieser EDL befinden. Sie können dieses Feld für weitere Details verwenden.
Change-Anforderung	Wenn das Kontrollkästchen Change-Anforderung erstellen aktiviert ist, wird die Nummer der Change-Anforderung in der Now Platform-Instanz angezeigt, sobald die EDL gespeichert wird. Wenn das Kontrollkästchen **Change-Anforderung erstellen** deaktiviert ist, wird dieses Feld nicht angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
IP-Adressen und Subnetzadressen in einem einzigen Eintrag zusammenfassen	Option zum Kombinieren von IP-Adressen und Subnetzadressen in einem einzigen Eintrag. Wenn Sie dieses Kontrollkästchen aktivieren und die IP des CIDR-Typs hinzugefügt wird, werden vorhandene Einträge, die in den CIDR-Bereich fallen, automatisch entfernt. Beispiel: Wenn in EDL ein Eintrag mit dem Wert 192.168.1.1 vorhanden ist und derselben EDL ein CIDR-Wert von 192.168.1.0/24 hinzugefügt wird, wird der ursprüngliche IP-Adresseintrag entfernt, da er in den CIDR-Bereich fällt des neuen Eintrags. **Hinweis:** Diese Option wird nur angezeigt, wenn Sie als **erkennbarer Elementtyp** IP auswählen.
EDL-Abruf-URL	Der URL-Link, den der Palo Alto Networks-Firewalladministrator für die Konfiguration in der Palo Alto Networks-Firewall verwendet, wird automatisch generiert und angezeigt.

4. Erstellen und fügen Sie nach Bedarf weitere EDLs hinzu.
   Die EDLs werden in der Liste „Externe dynamische Listen von Palo Alto Networks“ angezeigt.

Zugehörige Informationen

Palo Alto EDL-Genehmigungsregeln

Palo Alto EDL-Genehmigungsregeln

Mit Genehmigungsregeln können Benutzer den Genehmigungs-Workflow aktivieren, der zum Genehmigen oder Ablehnen der EDL-Einträge erforderlich ist.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
Der TISC-Administrator definiert diese Genehmigungsregeln, um die Einwilligung zu Genehmigungsanforderungen zu erteilen. Als TISC-Administrator können Sie hier auch mehrere Genehmigungsebenen definieren.

Prozedur

1. Nachdem Sie die neu konfigurierte Palo Alto NGFW-Konfiguration gespeichert haben, navigieren Sie zum Abschnitt **„EDL-Genehmigungsregeln“**.
2. Klicken Sie zum Erstellen einer neuen Genehmigungsregel **auf Neu**.
   Die folgenden Regeln sind die vorkonfigurierten Regeln im Basissystem für die Palo Alto NGFW-Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorkonfigurierte EDL-Genehmigungsregeln

Name	Beschreibung	EDL-Aktion
Genehmigungsregel zum Hinzufügen zu EDL	Mit dieser Genehmigungsregel können die Anwender den Genehmigungs-Workflow zum Hinzufügen von Einträgen zu EDL aktivieren.	Zu EDL hinzufügen
Genehmigungsregel zum Entfernen aus EDL	Mit dieser Genehmigungsregel können die Anwender den Genehmigungs-Workflow zum Entfernen von Einträgen aus EDL aktivieren.	Aus EDL entfernen

3. Füllen Sie die Felder im Formular entsprechend aus.

Neue EDL-Genehmigungsregeln erstellen

Feld	Beschreibung
Name	Name der Genehmigungsregel.
EDL-Aktion	Option zum Hinzufügen oder Entfernen des EDL-Eintrags.
EDLs	Wählen Sie die EDLs aus, für die eine Genehmigung erforderlich ist. Wenn Sie dieses Feld leer lassen, werden alle EDLs eingeschlossen.
Beschreibung	Geben Sie die Beschreibung für die Genehmigungsregel ein.
Anwender oder Gruppen mit erforderlicher Genehmigung auswählen	
Anwender	Wählen Sie die Anwender aus, für die eine Genehmigung erforderlich ist.
Gruppe(n)	Wählen Sie die Gruppen aus, für die eine Genehmigung erforderlich ist.
Den/die Genehmiger auswählen	
Anwender	Wählen Sie die Anwender zur Genehmigung aus.
Gruppe(n)	Wählen Sie die Gruppen zur Genehmigung aus.
Benachrichtigungen	
Anfordernde Person über Genehmigung benachrichtigen	Aktivieren Sie dieses Kontrollkästchen, um die anfordernde Person über die Genehmigung von EDLs zu benachrichtigen.
Anfordernde Person über Ablehnung benachrichtigen	Aktivieren Sie dieses Kontrollkästchen, um die anfordernde Person über die Ablehnung von EDLs zu benachrichtigen.

4. Klicken Sie auf **Speichern**, um die Genehmigungsregel zu validieren und zu speichern.

5. Klicken Sie auf **Aktivieren**, um die Genehmigungsregel zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennbare Elemente zu EDL hinzufügen

Fügen Sie der externen dynamischen Liste (EDLs) erkennbare Elemente wie IPs, Domänen und Hashes hinzu.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Öffnen Sie einen beliebigen erkennbaren Datensatz.
5. Klicken Sie **auf Zu EDL hinzufügen**.
   Der modale Bildschirm Zu EDL hinzufügen wird angezeigt.

Erkennbare Elemente aus EDL entfernen

Entfernen Sie erkennbare Elemente aus EDL.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Öffnen Sie einen beliebigen erkennbaren Datensatz.
5. Klicken Sie auf **Aus EDL entfernen**.
   Der modale Bildschirm „Remove from EDL“ (Aus EDL entfernen) wird angezeigt.

Genehmigen Sie EDL-Einträge für Palo Alto Networks

Das Genehmigen von EDL-Einträgen (External Dynamic List) ist Teil der Vorkonfiguration. Sie müssen die EDL-Einträge genehmigen, bevor die Einträge auf EDLs aktiviert werden, damit die Firewall den Eintrag abrufen und die Sicherheitsrichtlinie anwenden kann.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

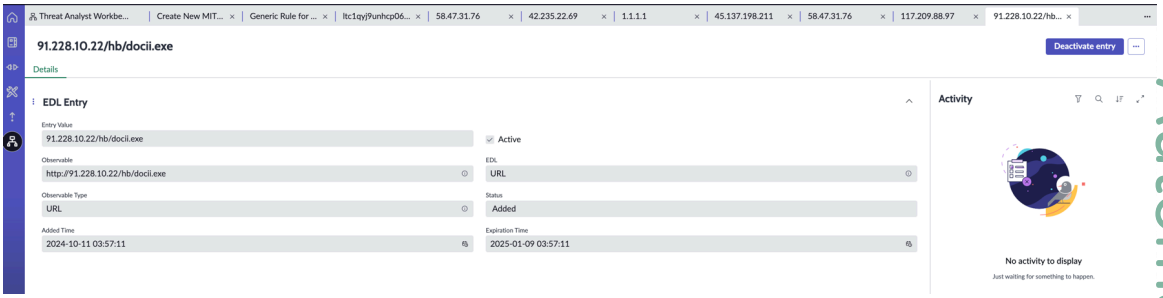
Warum und wann dieser Vorgang ausgeführt wird
Wenn der Genehmigungsprozess aktiviert ist, wird ein EDL-Eintrag in der EDL erst aktiviert oder deaktiviert, wenn er genehmigt wurde.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Analyst Workbench für Bedrohungen**.
2. Führen Sie einen Drilldown zum Abschnitt **„PAN NGFW“** durch, und wählen Sie den EDL-Datensatz zur Genehmigung aus.
3. Navigieren Sie zu **Meine Genehmigungen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie die zu genehmigenden EDL-Datensätze aus.
5. Klicken Sie auf **Genehmigen**.
6. Klicken Sie unter **Meine** Genehmigungsanforderungen auf ein Element in der Spalte **Status**, um es zu öffnen.
7. Wählen Sie die Option zum Genehmigen des EDL-Eintrags.
   Nachdem Sie den EDL-Eintrag genehmigt haben und er aktiviert ist, ruft Palo Alto Networks den EDL-Eintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, ist das erkennbare Element ab diesem Punkt blockiert. Beachten Sie, dass in der folgenden Abbildung das Kontrollkästchen **Aktiv** aktiviert ist, der Status Hinzugefügt lautet und in den Arbeitsnotizen angegeben ist, dass die Anforderung genehmigt wurde.



TISC-API-Referenzen

Die folgende Tabelle enthält die API-Endpunktreferenzen, die bei Anreicherungen hilfreich sind.

TISC-APIs

API	Beschreibung
TISC-API – POST /sn_sec_tisc/threat_intel_data/observables	Diese API ruft die Daten erkennbarer Elemente ab, einschließlich der Beziehungen zwischen erkennbaren Elementen und anderen zugehörigen Threat Intelligence-Daten.
TISC-API – POST /sn_sec_tisc/threat_intel_data/add_observables	Diese API fügt der Anwendung Threat Intelligence Security Center (TISC) gültige erkennbare Elemente hinzu, indem sie Quelldatensätze für erkennbare Elemente erstellt.

Weitere Informationen zu den TISC-API-Endpunkten finden Sie in der TISC-API im Abschnitt „REST API-Referenz“ zur API-Implementierung und zur Referenz unter servicenow.com/docs.

TISC-Add-on für Splunk-Übersicht

Das Threat Intelligence Security Center (TISC) für die App Splunk bietet eine Integration zwischen TISC und Splunk, mit der Benutzer die neuesten Bedrohungsinformationen nahtlos aus TISC in Splunk importieren können, um Warnungen zu überwachen und zu ergänzen. Benutzer können Indikatorsammlungen konfigurieren, Suchen durchführen und Dashboards verwenden, um Suchergebnisse und Indikatorsammlungen effektiv zu analysieren.

TISC integration with Splunk

Die Integration von Threat Intelligence-Sicherheitszentrum (TISC) und Splunk ermöglicht es Benutzern, relevante Daten erkennbarer Threat Intelligence-Elemente zu filtern und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in Splunkabzurufen. In Splunkkönnen Benutzer mit diesen Daten Sicherheitswarnungen generieren.

Erforderliche Rolle: Splunk-Administrator

Mit der TISC-Add-on-Anwendung können Sie das Intervall konfigurieren, in dem Sie erkennbare Elemente aus der TISC-Instanz ServiceNow abrufen können.

Dieses Intervall bestimmt, wie häufig die Anwendung Anforderungen an ServiceNow stellen und die Daten der erkennbaren Elemente abrufen kann. Außerdem können Sie Filter definieren und anwenden, um die erkennbaren Elemente anzugeben, die Sie aus der TISC-Instanz ServiceNow abrufen möchten.

Sobald die erkennbaren Elemente aus ServiceNowabgerufen wurden, werden die Daten der erkennbaren Elemente im KV Store (Schlüssel-Wert-Speicher) von Splunk gespeichert, und Sie können die Korrelationsregeln für den Satz der abgerufenen erkennbaren Elemente weiter schreiben.

Erstellen von Anwendern in ServiceNow TISC-Instanz

Sie können Benutzer in der TISC-Instanz ServiceNow mit jeder gültigen Benutzerrolle erstellen: sn_sec_tisc.api_obs_read_access.

Installieren Sie die TISC-Add-on-App in Splunk

Weitere Informationen finden Sie unter Einem Benutzer eine Rolle zuweisen .

Erforderliche Rolle: Splunk-Administrator.

1. Melden Sie sich bei **Splunk**an.
2. Navigieren zu **Apps** > **Apps verwalten** oder klicken Sie auf das Zahnradsymbol **Verwalten**.
3. Suchen Sie nach der App **Threat Intelligence Security Center for Splunk**, und installieren Sie sie.
4. Nach der Installation wird die Anwendung unter der Liste der Apps angezeigt.

TISC-Add-on wird in konfiguriert Splunk

Befolgen Sie die nachstehenden Schritte, um die Anwendung zu konfigurieren.

Vorbereitungen
Erforderliche Rolle: Splunk-Administrator

Warum und wann dieser Vorgang ausgeführt wird
Das folgende Verfahren beschreibt die Konfiguration des TISC-Add-ons in Splunk.

Prozedur

1. Suchen Sie in der linken Navigationsleiste nach der App **Threat Intelligence Security Center for Splunk**.
2. Klicken Sie in der Spalte **Aktionen** auf **Einrichten**.
   Die **Konfigurationsseite** wird angezeigt, und Sie können Ihr ServiceNow TISC-Konto einrichten.
3. Wählen Sie **Hinzufügen**.
4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Konten hinzufügen	
Name	Ein eindeutiger Name für den Account
Anwendername	Geben Sie den Anwendernamen für Ihren Account ServiceNow an. Sie können den gleichen Anwendernamen verwenden, der für die Anwender verwendet wird, die während der Rollenerstellung `sn_sec_tisc.api_obs_read_access` im obigen Schritt erstellt werden.
Passwort	Geben Sie das Account-Passwort ServiceNow an .
Instanz-URL	Geben Sie die URL-Adresse der Instanz ServiceNow an.

5. Klicken Sie auf **Hinzufügen**.
   Der Instanz-Account ServiceNow wird dem Splunkhinzugefügt.
6. Navigieren Sie zur Seite **„Eingaben“**, um Sammlungen zu erstellen und Ihre Dateneingaben für Ihren Account ServiceNow zu verwalten.
7. Klicken Sie auf **Neue Eingabe erstellen**.
   Das Dialogfeld **„Eingabe hinzufügen“** wird angezeigt, damit Sie die Eingaben Ihrem Account ServiceNow hinzufügen können.

   Sobald der Eingabesatz definiert ist, sendet die Anwendung die Informationen an die TISC-Instanz, um eine bestimmte Anzahl von erkennbaren Elementen abzurufen, die die Kriterien erfüllen.
8. Füllen Sie die Eingabedetails entsprechend aus.

Feld	Beschreibung
Name	Ein eindeutiger Name für Ihre Eingabe. Beispiel: Liste schädlicher IPs.
Account	Geben Sie den Anwendernamen für Ihren Account ServiceNow an. Sie können denselben Anwendernamen verwenden, der für die Anwender verwendet wird, die im obigen Schritt mit der Rolle `sn_sec_tisc.api_obs_read_access` erstellt wurden.
Intervall	Legen Sie das Zeitintervall in Sekunden fest, um die Daten von TISC abzurufen.
Ablaufzeitraum (in Tagen)	Option zum Festlegen des Ablaufzeitraums in Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Der Ablauf des Beispiels ist auf 30 Tage festgelegt. Wenn beispielsweise Daten an einem bestimmten Datum abgerufen werden, kann ein Satz von 10.000 Datensätzen abgerufen werden. Diese Datensätze werden im KV-Speicher (Key-Value) in Splunkgespeichert. Ab dem Erfassungsdatum werden die Datensätze 30 Tage lang aufbewahrt. Am 31. Tag werden sie automatisch aus dem KV-Speicher gelöscht.
Läuft nie ab	Wählen Sie diese Option aus, wenn die erfassten Datensätze nicht ablaufen sollen.
Filter	Definieren Sie die Bedingungen, auf deren Grundlage importierte Daten gefiltert werden sollen. Um die Filterbedingungen festzulegen, können Sie die Kriterien basierend auf den -Feldern wie Bedrohungsbewertung, Konfidenzniveau und Typ definieren. Für einfache Filterbedingungen können Sie diese Filteroption verwenden. Wenn die Filterbedingungen jedoch komplexer sind und erweiterte Filterung erforderlich ist, können Sie JSON-Filter hinzufügen. ○ Die zulässigen Ganzzahloperatoren sind: "=", "!=", ">", "<", ">=", "<=" ○ Die zulässigen Zeichenfolgenoperatoren sind: „=“, „!=", „IN“ **Nachfolgend finden Sie ein Beispiel für einen einfachen Filter**: {Sample filter format: Allowed Tokens: "threat_score", "confidence", "reputation", "type", "value". Allowed Integer Operators: "=", "!=", ">", "<", ">=", "<=". Allowed String Operators: "=", "!=", "IN". Example: reputation IN ("clean","suspicious","malicious") AND threat_score > 90 AND confidence > 90 AND type = "ip_v4_address"}
JSON	Mit JSON-basierten Filtern können Sie komplexere Bedingungen definieren. Der Status des JSON-Objekts muss aktiv sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Aktivieren Sie das Kontrollkästchen **JSON** -Filter, um zu erweiterten Filtern zu wechseln, bei denen JSON zum Anwenden von Filterbedingungen verwendet werden kann.

Beispiel für einen erweiterten Filter:

```
{"boolean_operator":"AND","filters":[{"field_name":"reputation","operator":"IN","field_value":"clean,suspicious,malicious"},{"field_name":"threat_score","operator":">","field_value":"90"},{"field_name":"confidence","operator":">","field_value":"90"},{"field_name":"type","operator":"=","field_value":"ip_v4_address"}]}
```

Hinweis:
Konten sind standardmäßig aktiv, aber Eingaben sind standardmäßig inaktiv. Sie müssen sie aktivieren, um mit dem Importieren der Daten zu beginnen. Informationen zu möglichen Filtern finden Sie im Abschnitt „Observable_filters“ in Fügt der Anwendung Threat Intelligence Security Center (TISC) Quelldatensätze erkennbarer Elemente hinzu .

9. Klicken Sie auf **Hinzufügen**, um die Eingaben hinzuzufügen.
10. Klicken Sie auf **Klonen** oder kopieren, um das vorhandene Konto zu kopieren und ein neues zu erstellen. Stellen Sie sicher, dass die Eingabe vor dem Klonen deaktiviert ist, um zu vermeiden, dass beim Importieren von Daten mit denselben Kriterien doppelte Einträge erstellt werden.
11. Sobald die Daten abgerufen wurden, werden die folgenden Informationen abgerufen und zusammen mit den aus TISC abgerufenen Datensätzen im KV-Speicher in Splunk gespeichert:

Feld	Beschreibung
Bedrohungsbewertung	Die Punktzahl, die die einem Datensatz zugeordnete Bedrohungsstufe angibt.
Vertrauen	Gibt das Konfidenzniveau an, das der Genauigkeit der Bedrohungsbewertung zugeordnet ist.
Ablaufzeitraum	Die Dauer, für die der Datensatz in der Anwendung gültig ist, bevor er abläuft.
Bedrohungsstufe	Gibt den Schweregrad der Bedrohung an.
Reputation	Gibt die Reputation der beteiligten Entität an.
Aktualisiert von	Stellt Informationen darüber bereit, wer den Datensatz zuletzt aktualisiert hat.
Updatezeit	Gibt den Zeitstempel der letzten Aktualisierung des Datensatzes an.
Erstellt um	Gibt die Datensatzerstellungszeit an.
Days_til_expiry	Gibt die Anzahl der Tage an, nach der der Datensatz aus dem KV-Speicher gelöscht wird.
Source_reported_score	Die Punktzahl der gemeldeten Quelle von TISC.
Sys_id	Sys-ID des Datensatzes, der über TISC kommt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedrohungsschweregrad	Gibt den Bedrohungsschweregrad des erkennbaren Elements an.
Wert	Wert des Datensatzes. Zum Beispiel IP, Hash usw.

Diese Felder sind zusammen mit allen anderen, die durch Ihre Kriterien definiert wurden, in Splunk verfügbar und können über die Registerkarte „Suchen“ angezeigt, durchsucht und analysiert werden.

Datenspeicherung in Splunk

In diesem Abschnitt wird beschrieben, wie TISC während der Integration Suchvorgänge innerhalb des Schlüssel-Wert-Speichers von Splunk für die Datenspeicherung verwendet. Es beschreibt, wie diese Suchen in Splunk konfiguriert und abgerufen werden.

Nachschlagen	Suchbeschreibung
`tisc_store_lookup`	Name der KV-Suche, die für die Suche in den eingehenden Datensätzen verwendet werden soll.
`tisc_kv_store`	Name des KV-Speichers, in dem sich die Daten befinden.
`inputlookup <lookup_name>" example : | inputlookup tisc_store_lookup`	Abfrage zum Suchen von Datensätzen im KV-Speicher.

TISC Microsoft Sentinel-Integration

Threat Intelligence-Sicherheitszentrum für Microsoft Sentinel bietet mehrere Funktionen, unter anderem das Importieren von erkennbaren Elementen aus TISC nach Sentinel, das Anreichern von Sentinel-Incidents mit Details zu zugehörigen erkennbaren Elementen und das Exportieren von erkennbaren Elementen aus Sentinel nach TISC.

Hinweis:
In Microsoft Sentinel werden erkennbare Elemente als Entitäten bezeichnet.

Voraussetzungen

Abhängigkeiten

Die Lösung **Threat Intelligence** von Microsoft Sentinel Content Hub muss installiert sein.

Rollen und Berechtigungen

Anwendung	Rollen und Berechtigungen	Beschreibung
Microsoft Sentinel-spezifische Rollen	1. Beitragender für Logik-App 2. Microsoft Sentinel-Beitragender	1. Zum Installieren der erforderlichen Playbooks auf Ressourcengruppenebene. 2. Interagieren Sie mit Microsoft Sentinel Playbooks.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen und Berechtigungen (Fortsetzung)

Anwendung	Rollen und Berechtigungen	Beschreibung
		Weitere Informationen finden Sie unter Rollen und Berechtigungen in Microsoft Sentinel.
Threat Intelligence-Sicherheitszentrum	sn_sec_tisc.api_azure_sentinel_solution	Der im anwenderdefinierten TISC-Connector konfigurierte Anwender muss über diese Rolle verfügen, um den Zugriff auf TISC-APIs zu ermöglichen.

TISC-Playbook-Vorlagen

In diesem Abschnitt werden die Playbook-Vorlagen beschrieben, die im Lieferumfang der TISC Sentinel-Lösung enthalten sind.

Playbook-Anwendungsfälle

In der folgenden Tabelle werden die verschiedenen Playbook-Anwendungsfälle beschrieben.

Anwendungsfall	Playbook	Beschreibung
Erkennbare Elemente werden von TISC nach Sentinel importiert	Batch_Indicator_Uploader	Bietet einen Batch-Mechanismus für den Export von erkennbaren Elementen aus TISC mithilfe der Upload Indicators-API von Microsoft Sentinel.
	Import_Observables_Batch	Aktiviert den geplanten Export von erkennbaren Elementen aus TISC.
Exportieren Sie Entitäten aus Sentinel nach TISC	Export_Incident_Entities	Exportiert alle Entitäten eines Sentinel-Incidents.
	Export_Hash_Entity	Exportieren Sie die Datei-Hash-Entitäten des Sentinel-Incidents.
	Export_Domain_Entity-Entitäten	Exportieren Sie Domänenentitäten des Sentinel-Incidents.
	Export_IP_Entity	Exportieren Sie IP-Entitäten des Sentinel-Incidents.
	Export_URL_Entity	Exportieren Sie URL-Entitäten des Sentinel-Incidents.
Sentinel-Incidents ergänzen	Incident_Enrichment	Aktiviert die Anreicherung von Sentinel-Incidents durch Abrufen von Details im Zusammenhang mit zugehörigen Entitäten und Veröffentlichen von Informationen in Form von Kommentaren zum Incident

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Alle Playbooks verwenden intern den TISC Custom Connector, um TISC-APIs zu verwenden.

Erstellen Sie Playbooks aus Vorlagen

1. Navigieren Sie zur Inhaltsseite der T**ISC-Lösung** aus dem **Inhalts-Hub im Sentinel-Arbeitsbereich**.
2. Gehen Sie für jedes auf der Inhaltsseite angezeigte Playbook wie folgt vor:
   a. Wählen Sie die Playbook-Vorlage aus. Ein Kontextbereich wird auf der rechten Seite des Bildschirms angezeigt. Klicken Sie auf **Konfiguration**.
   b. Lesen Sie die Beschreibung der Playbook-Vorlage, und gehen Sie die in der Beschreibung genannten Schritte **Voraussetzungen** und Schritte **nach der Bereitstellung** durch.
   c. Klicken Sie auf **Anwenderdefinierten Connector bereitstellen** (wenn Sie den anwenderdefinierten Connector noch nicht bereitgestellt haben).

      Fügen Sie auf der Seite **Bereitstellungskonfiguration** die **URL der ServiceNow-Instanz** hinzu.
   d. Klicken Sie auf **Playbook erstellen**. Sie gelangen zum Konfigurationsbildschirm für die Bereitstellung
   e. Im Konfigurationsbildschirm „Playbook erstellen“:
      - Wählen Sie die entsprechende Ressourcengruppe aus.
      - Ändern Sie den Playbook-Namen, oder verwenden Sie den Standardnamen.
      - Geben Sie den **Namen des anwenderdefinierten Connectors**(stellen Sie sicher, dass dieser mit dem Namen des Connectors übereinstimmt, den Sie im vorherigen Schritt bereitgestellt haben) im Abschnitt „Parameter“ an.
      - Klicken Sie auf **Überprüfen und erstellen**.

Konfigurieren Sie das Playbook „Import_Observables_Batch“.

Stellen Sie sicher, dass Sie das Playbook „Batch_Indicator_Uploader“ erstellen, bevor das Playbook „Import_Observables_Batch“ erstellt wird.

1. Navigieren zu **Logik-App-Designer** um das Playbook zu bearbeiten.
2. Aktualisieren Sie die Wiederholungszeit (in Stunden) nach Bedarf.
3. Aktualisieren Sie in der Komponente „TISC Custom Connector“ im Playbook die Parameter, die an die TISC-API gesendet werden.

Parametername	Beschreibung
Erkennbarer Typ	Nachfolgend sind die unterstützten Typen aufgeführt. Wählen Sie einen oder mehrere aus: ○ IP ○ Datei-Hash ○ Domäne ○ URL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Beschreibung
Bedrohungsbewertung	Geben Sie die Bedrohungsbewertung für erkennbare Elemente ein. Der Wert der Bedrohungsbewertung MUSS eine Zahl im Bereich von 0 bis 100 sein.
Vertrauen	Geben Sie die Konfidenz für erkennbare Elemente ein. Der Konfidenzwert muss eine Zahl im Bereich von 0 bis 100 sein.
Reputation	Nachfolgend sind die unterstützten Werte aufgeführt. Wählen Sie einen oder mehrere aus: ○ Clean ○ Böswillig ○ Verdächtig ○ Unbekannt
Bedrohungsschweregrad	Nachfolgend sind die unterstützten Schweregradstufen aufgeführt. Wählen Sie eine oder mehrere aus: ○ Kritisch ○ Hoch ○ Mittel ○ Niedrig
Bedrohungsstufe	Nachfolgend sind die unterstützten Bedrohungsstufen aufgeführt. Wählen Sie eine oder mehrere aus: ○ Hoch ○ Mittel ○ Niedrig
Zuletzt aktualisiertes Delta in Stunden	Die letzte Aktualisierungszeit (in Stunden) für erkennbare Elemente.

Konfigurieren Sie das Playbook „Export_Incident_Entities“.

Dieses Playbook verwendet die TISC-API zum Hinzufügen erkennbarer Elemente. Mit dem Logik-App-Designer können Sie die Parameter bearbeiten, die vom Playbook an die API gesendet werden. Weitere Informationen finden Sie unter TISC-API – POST /sn_sec_tisc/threat_intel_data/add_observables .

Sie können das gleiche Verfahren für alle unten aufgeführten Playbooks anwenden, die verschiedene Arten von Entitäten exportieren:

- Export_Hash_Entity
- Export_Domain_Entity
- Export_IP_Entity
- Export_URL_Entity

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für Incident_Enrichment konfigurieren

Dieses Playbook verwendet die TISC Observables API. Mit dem Logik-App-Designer können Sie die Parameter bearbeiten, die vom Playbook an die API gesendet werden. Weitere Informationen finden Sie unter TISC-API – POST /sn_sec_tisc/threat_intel_data/observables .

Führen Sie Playbooks aus

In der folgenden Tabelle wird beschrieben, wie Sie die folgenden Playbooks ausführen können.

Playbook	Aktion
Import_Observables_Batch	Dieses Playbook wird automatisch basierend auf der geplanten Zeit ausgeführt, die im Wiederholungsauslöser erwähnt wird.
Export_Incident_Entities	Wählen Sie bei einem Sentinel-Incident die Option aus **Incident-Aktionen** > **Führen Sie das Playbook aus** zur Ausführung.
Export_Hash_Entity	Wählen Sie bei einem Sentinel-Incident die Option aus **Datei-Hash-Entität** > **Führen Sie das Playbook aus** zur Ausführung.
Export_Domain_Entity	Wählen Sie bei einem Sentinel-Incident die Option aus **Domänenentität** > **Führen Sie das Playbook aus** zur Ausführung.
Export_IP_Entity	Wählen Sie bei einem Sentinel-Incident die Option aus **IP-Entität** > **Führen Sie das Playbook aus** zur Ausführung.
Export_URL_Entity	Wählen Sie bei einem Sentinel-Incident die Option aus **URL-Entität** > **Führen Sie das Playbook aus** zur Ausführung.
Incident_Enrichment	Wählen Sie bei einem Sentinel-Incident die Option aus **Incident-Aktionen** > **Führen Sie das Playbook aus** zur Ausführung.

TISC-Integration mit SIR Workspace

Die TISC-Integration mit SIR fügt den Kontext für die erkennbaren Elemente im Security Incident-Arbeitsbereich für Sicherheitsanalysten automatisch an. Alle neuen erkennbaren Elemente von SIR können zur weiteren Analyse durch das CTI-Team mithilfe der auf den Bildschirmen bereitgestellten UI-Aktionen an TISC gesendet werden.

Darüber hinaus können alle Ergänzungsergebnisse, die aus Integrationen erzeugt werden, die nur in SIR verfügbar sind, auch mit den im Arbeitsbereich bereitgestellten UI-Aktionen übertragen werden.

Administration

Verwenden Sie die linke Navigation, um zum Modul „Administration“ im Threat Intelligence-Sicherheitszentrum zu navigieren und die folgenden Module der TISC-Datenverwaltung anzuzeigen, um Filterregeln und Genehmigungsregeln festzulegen, die Bedrohungsbewertung zu definieren und Benachrichtigungen zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenverwaltung

Modul	Beschreibung
Regel-Engine	Dieser Abschnitt besteht aus den folgenden Regeln, die während der Datenverwaltung erforderlich sind: 1. **Genehmigungsregeln für Datenimporte**: Definieren Sie die Genehmigungsregeln, und integrieren Sie den Genehmigungs-Flow im Abschnitt „Import Intelligence“, nachdem Sie den Datenimport übermittelt haben. 2. **Eingehende Filterregeln**: Erstellen Sie Filterregeln, um die eingehenden Quelldatensatzdaten zu filtern. 3. **Regel zur Bedrohungsbewertung**: Passen Sie den Bedrohungsbewertungsrechner an, der den erkennbaren Elementen eine Bedrohungsbewertung zuweist.
Sicherheitskontrolllisten	Dieses Modul hilft Ihnen bei den Sicherheitskontrollen: 1. **Liste der zugelassenen Elemente** 2. **Sperrliste** 3. **Beobachtungsliste**
Taxonomien	Dieses Modul hilft Ihnen, Taxonomien für die Datenquellen-Datensätze zu erstellen.
Benachrichtigungen	Dieses Modul definiert, wie E-Mail-Benachrichtigungen verwaltet werden.
Vorlagen	Dieses Modul enthält einen Überblick über die Erstellung von Berichtsvorlagen in der Designzeit- und Laufzeit-Experience.

Genehmigungsregeln für Datenimporte definieren

Verwenden Sie diesen Abschnitt, um die Genehmigungsregeln zu definieren und den Genehmigungs-Flow nach dem Senden des Datenimports in den Abschnitt „Import Intelligence“ zu integrieren.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Administration**.
3. Gehe zu **Regel-Engine** > **Genehmigungsregeln für Datenimporte**.
4. Wählen Sie **Genehmigungsregel für Datenimporte aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Basissystem ist **die Genehmigungsregel für Datenimporte** die standardmäßige Genehmigungsregel, die bereitgestellt wird, damit Benutzer den Genehmigungsworkflow aktivieren können.

5. Geben Sie für die Abschnitte **Anwender oder Gruppen mit erforderlicher Genehmigung auswählen** und **Genehmiger auswählen** jeweils mindestens einen Anwendernamen oder eine Anwendergruppe ein.
6. Klicken Sie auf die Schaltfläche **Aktivieren**, um den Genehmigungs-Flow für die Datenimporte zu aktivieren.

Wenn diese Option aktiviert ist, befinden sich die Datenimporte in der Genehmigungswarteschlange, damit der Genehmiger die Datenverarbeitung genehmigen oder ablehnen kann. Der Genehmiger überprüft die vom Analysten vorgenommenen Änderungen und genehmigt dann die Datenimportanforderung oder lehnt sie ab.

Hinweis:
Eine E-Mail-Benachrichtigung wird an die Anwender oder Anwendergruppen gesendet, dass der Importauftrag verarbeitet und genehmigt oder abgelehnt wird.

Ablaufregeln definieren

Definieren Sie Ablaufregeln für verschiedene erkennbare Elemente oder eine Kombination aus verschiedenen Quellobjekten oder Indikatorquellen, die in TISC erstellt werden.

Vorbereitungen

Jede Quelle, die in der Anwendung erstellt wird, hat einen Ablaufzeitraum. Die Daten-Feeds verwenden Techniken wie einen zeitbasierten Ablaufzeitraum, um die Datenerfassung zu fördern. In TISC definieren die Ablaufregeln die Ablaufzeit für einen bestimmten Satz von Datenquellen oder Satz von Objekttypen oder Typen von erkennbaren Elementen.

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Ablaufregeln**.
   Die Seite Ablaufregeln wird angezeigt.
3. Klicken Sie auf **Neu**.
4. Klicken Sie auf **Aktivieren**, um die Ablaufregel zu aktivieren, nachdem Sie eine neue Regel erstellt haben. Wenn Sie die Ablaufregel nicht aktivieren, wird die Regel nicht auf den Quelldatensatz angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Sie eine Ablaufregel aktivieren, wird im Hintergrund eine Duplizierungsprüfung durchgeführt, um zu überprüfen, ob im System eine Duplikatregel mit derselben Kombination aus Datenquellen und Typ von Datensätzen vorhanden ist. Wenn dies der Fall ist, zeigt die Anwendung eine Informationsmeldung an, dass die Regel bereits die gleiche Kombination aus Datenquelle und Objektkategorie enthält und Sie die vorhandene Kombination ändern müssen, um die Regel zu aktivieren.
- Für die Anwender im Basissystem wird eine Beispiel-Ablaufregel bereitgestellt, und diese **Beispiel-Ablaufregel** für erkennbares Element befindet sich standardmäßig im Status „Deaktiviert“. Sie müssen die Regel aktivieren und aktivieren.

5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Löschen**, wenn Sie eine Ablaufregel löschen möchten.

Ablaufregeln für Quelldatensätze

Ablaufregeln sind im Grunde hilfreich, um die Ablaufzeit für die Quelldatensätze festzulegen. Der Aggregatdatensatz erbt die längste Ablaufzeit von den entsprechenden Quelldatensätzen.

Wie die Regeln angewendet werden

Example: Der Typ des eingehenden Quelldatensatzes ist Malware vom Datenquellentyp CrowdStrike

Regelbewertungsprozess basierend auf den Regeln, die für die Anwendung von Ablaufzeiten auf Quelldatensätze bereitgestellt werden:

1. **Alle aktivierten Regeln abrufen:** Die Anwendung überprüft zunächst alle derzeit aktivierten Regeln.
2. Suchen Sie nach einer bestimmten Regelkombination:

   Suchen Sie nach einer Regel, die speziell mit der folgenden Kombination übereinstimmt:

   - **Datenquellentyp**: CrowdStrike
   - **Typ der Datensätze**: Malware
3. **Priorität basierend auf den Übereinstimmungsregel-Kombinationen:**

   Wenn eine Regel vorhanden ist, bei der der Datenquellentyp **CrowdStrike** und der Datensatztyp **Malware**ist, hat diese Regel Vorrang. Die in dieser Regel angegebene Ablaufzeit wird angewendet.
4. **Fallback-Regeln:**

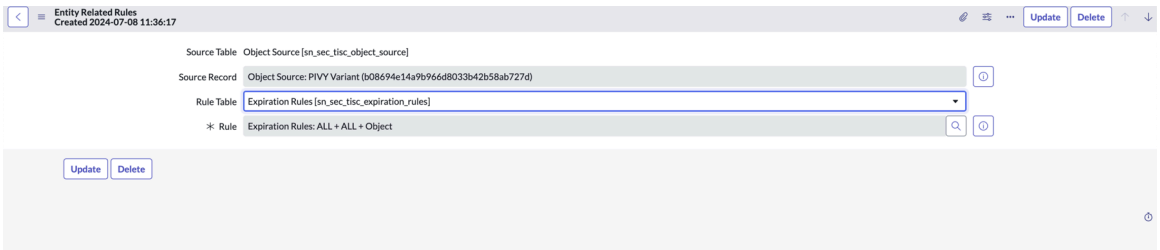
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn keine Regel mit der Kombination aus **CrowdStrike und Malware** übereinstimmt, sucht das System nach einer Regel, bei der der Datenquellentyp **CrowdStrike** und der Datensatztyp **Alle**ist.

b. Wenn immer noch keine Regel gefunden wird, wird nach einer Regel gesucht, bei der der Datenquellentyp **Alle** und der Datensatztyp **Malware**sind.

c. Wenn schließlich keine der oben genannten Regeln vorhanden ist, wird standardmäßig eine Regel verwendet, bei der sowohl der Datenquellentyp als auch der Datensatztyp **Alle**sind.

5. Wenn keine dieser Regeln im System vorhanden ist, wird keine Ablaufregel auf die Quelldatensätze angewendet. Navigieren Sie in diesem Fall zur folgenden Tabelle (im Screenshot), um die Kombination der Regeln zu überprüfen, die auf die Objekte angewendet wurden.



6. **Löschen von Datenquellen:**

   Angenommen, wenn eine Datenquelle, der die Ablaufregeln zugeordnet sind, gelöscht wird, kann das Löschen eingeschränkt oder nicht zulässig sein, bis diese Regeln behandelt werden. Dadurch wird sichergestellt, dass bei der Anwendung von Ablaufrichtlinien keine Inkonsistenzen auftreten.

Definieren von Filterregeln

Erstellen Sie Filterregeln, um alle Arten von Daten oder eingehenden Quelldatensatzdaten zu filtern. Mit dem Datenquellen-Manager werden mehrere Feeds wie STIX-Daten und RSS-Feeds konfiguriert. Um die Daten aus den konfigurierten Feeds zu filtern, müssen Sie bestimmte Filterregeln definieren.

Vorbereitungen

Wenn Sie eine Filterregel definieren, wird diese Regel nur auf den Satz von Quelldaten angewendet, auf den eine Regel zum Filtern von Datensätzen während der Datenerfassung und des Datenimports angewendet wird.

Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

Filterregeln werden erstellt und auf einen Quelldatensatz angewendet, um weitere Schritte zu verarbeiten. Das Basissystem bietet eine **Beispielfilterregel** für Benutzer mit einer vordefinierten Regel zum Filtern der erfassten erkennbaren Elemente, Indikatordaten oder Entitäten/Objekte.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Drilldown zu **Regel-Engine** > **Eingehende Filterregeln**.
3. Klicken Sie auf **Neu**, um Filterregeln zu definieren.
   Die Seite Neue eingehende Filterregeln erstellen wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die Felder des Formulars aus.

Definieren Sie Filterregeln

Feld	Beschreibung
Name	Name der neuen Filterregel.
Beschreibung	Kurzbeschreibung der Filterregel.
Bestellung	Die Priorität der Filterregel. Dieses Feld gibt die Reihenfolge an, in der die Filterregeln ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen. Die Filterregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw. Der Standardwert für die Filterregel des Basissystems ist 100.
Datenquellen	Wählen Sie den Datenquellentyp aus der Nachschlageliste aus.
Tabelle	Wählen Sie den Tabellentyp aus, für den Sie den Filter anwenden möchten. Beispiel: Quelle des erkennbaren Elements, Indikatorquelle und Objektquelle.
Filtertyp (nur wenn für Tabelle die Quelle erkennbarer Elemente ausgewählt ist)	Filtertypen enthalten zwei Optionen, auf deren Grundlage Sie den Filter anwenden können. ○ Basierend auf Bedingung filtern ○ Basierend auf Liste filtern
Filtertyp (Filter basierend auf Bedingung)	Filterbedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der Quelltabelle. Zum Beispiel haben Indikatorquelle und Objektquelle nur Filtertypen: Filter basierend auf Bedingung. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**. Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neuer Bedingungssatz**.
Filtertyp (Filter basierend auf Liste)	Wenn die eingehenden erkennbaren Elemente mit den Einträgen in der ausgewählten Liste übereinstimmen, wird gefiltert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Diese Filterregeln gelten nicht für Datenimporte mithilfe von Import Intelligence. Die verfügbaren Optionen sind Allow-Liste, Deny-Liste und Beobachtungsliste.

Sobald die Filterregel für die erfassten Daten aktiviert ist, kann das Ergebnis auf den folgenden Registerkarten als verschiedene gefilterte Datensätze angezeigt werden.

a. **Gefilterte Datensätze erkennbarer Elemente**: Filtert die Datensätze erkennbarer Elemente und listet sie auf.

b. **Gefilterte Indikatordatensätze**: Filtert die Indikatordatensätze und listet sie auf.

c. **Gefilterte Objektdatensätze**: Filtert die Objektdatensätze und listet sie auf.

Hinweis:
Um die Filterregeln basierend auf Tags anzuwenden, die den Quelldatensätzen hinzugefügt werden, wählen Sie die Option **TISC-Tags** im Generator für Filterbedingungen aus.

Rechner für anwenderdefinierte Bedrohungsbewertung in TISC

Mit dem anwenderdefinierten Bedrohungsbewertungsrechner können Sie einen Bedrohungsschweregrad eines erkennbaren Elements basierend auf den anwenderdefinierten Kriterien definieren und berechnen, wodurch eine transparente Intelligenzbewertung von erkennbaren Elementen ermöglicht wird. Die Bedrohungsbewertung wird für Datensätze erkennbarer Elemente automatisch berechnet.

Definieren Sie den Bedrohungsbewertungsrechner

Definieren Sie die Bedrohungsbewertung für die Datensätze erkennbarer Elemente, die basierend auf den anwenderdefinierten Parametern generiert werden. Das Basissystem wird mit einer Regel zur Bewertung von Bedrohungen bereitgestellt, die entsprechend angepasst und aktiviert werden kann.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Standardmäßig ist die Regel zur Bedrohungsbewertung inaktiv. Sie müssen die Regel aktivieren, um die Bewertung der erkennbaren Elemente anzuzeigen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Gehe zu **Regel der Bedrohungsbewertung**.
   Die Seite „Bedrohungsbewertungsrechner“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- In der Anwendung gibt es im Basissystem eine Bewertungsregel, die für Benutzer zum Anzeigen, Bearbeiten oder Ändern der Bedrohungsbewertung bereitgestellt wird. Der Benutzer kann jedoch weder eine neue Regel erstellen noch die vordefinierte Regel zur Bewertung von Bedrohungen löschen.
- Die Änderungen gelten für alle neuen erkennbaren Elemente oder Updates der erkennbaren Elemente ab diesem Zeitpunkt. Um historische Punktzahlen neu zu formulieren, sollte die Option „Neu berechnen“ verwendet werden.

3. Im Formular enthalten die folgenden Felder die vordefinierten Werte.

Bedrohungsbewertungsrechner

Feld	Beschreibung
Name	Name des Werts für die Bedrohungsbewertung. Beispiel: Bedrohungsbewertungsrechner.
Beschreibung	Beschreibung des Bedrohungsbewertungsdatensatzes. Beispiel: Berechnet die Bedrohungsbewertung basierend auf der gewichteten Summe der Punktzahlen vordefinierter Kriterien.
Gesamtgewichtung (gilt für den Kriteriengenerator)	Dieses Feld kann nicht bearbeitet werden und zeigt die vom System berechnete Gesamtgewichtung basierend auf der Gewichtung an, die den aktivierten Kriterien entspricht.
Bewertungskriterien	Gibt die Bewertungskriterien für ein erkennbares Element an. Im Folgenden sind die beiden verfügbaren Optionen zum Definieren der Kriterien für die Bedrohungsbewertung aufgeführt: ○ **Kriteriengenerator**: Verwenden Sie diese Option, um Kriterien hinzuzufügen, zu bearbeiten oder zu entfernen sowie Kriterien zu aktivieren und zu deaktivieren, die zur Berechnung der Bedrohungsbewertung beitragen, und stellen Sie sicher, dass die aggregierte Gesamtgewichtung 100 % beträgt. ○ **Skript verwenden (erweitert)**: Die Skripterstellungsfunktion ist eine erweiterte Funktion zum Erstellen eines anwenderdefinierten Skripts, das die Bedrohungsbewertung im Bereich von 0 bis 100 zurückgeben sollte.

Nachfolgend sind die verfügbaren Optionen zum Definieren der **Bewertungskriterien**aufgeführt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Kriteriengenerator
- Skript verwenden (erweitert)

Im Folgenden finden Sie das Verfahren für den Kriteriengenerator:

Hinweis:
Sie können die vorhandenen Kriterien bearbeiten oder ändern oder neue Kriterien hinzufügen.

a. Wählen Sie den Typ der Kriterien aus.
Beispiel: Neues Kriterium hinzufügen.

b. Wählen Sie die **Tabelle** aus, für die die Kriterien konfiguriert sind.
Die Liste der Werte in der Dropdown-Liste lautet „Erkennbare Elemente“, „Bedrohungsakteur“, „Kampagne“, „Standort“, „Identität“, „Schwachstelle“, „Bedrohungsereignis“, „Security Incident“ und „Aggregate“. Wenn Sie eine dieser Optionen aus der Dropdown-Liste auswählen, wird eine Bedingung angewendet. Diese Bedingung stellt sicher, dass nur Datensätze, die sich auf den ausgewählten Wert beziehen, angezeigt oder berechnet werden.

Hinweis:

- Wenn Erkennbares Element ausgewählt ist, wird die Bedingung auf den Datensatz des erkennbaren Elements angewendet, für den die Bedrohungsbewertung berechnet wird. Wenn die ausgewählte Tabelle kein erkennbares Element ist, wird die Bedingung nur angewendet, wenn sich die Datensätze auf das erkennbare Element beziehen, für das die Bedrohungsbewertung berechnet wird.
- Eine zusätzliche Tabelle „Aggregates“ wird hinzugefügt, um die Punktzahlen basierend auf der Anzahl der Beziehungen zu definieren, die den erkennbaren Elementen zugeordnet sind. Wählen Sie beispielsweise Tabelle: Aggregate und den Feldwert Bedrohungsakteure Dann für ein erkennbares Element aus. Wenn mehr als zwei Bedrohungsakteure vorhanden sind, legen Sie die Punktzahl fest, und wenden Sie die Bedingungen entsprechend an.
- Wenn Sie beispielsweise eine Punktzahl für einen oder mehrere Bedrohungsakteure festlegen möchten, die einem erkennbaren Element zugeordnet sind, wählen Sie das Feld No of Threat Actors (Anzahl der Bedrohungsakteure) aus, legen Sie die gewünschte Punktzahl fest, und wenden Sie die Bedingungen entsprechend an.

c. Wählen Sie das **Feld** aus der oben ausgewählten Tabelle aus.

d. Geben Sie die **Gewichtung** der Kriterien zwischen 0 und 100 ein.
Die Gesamtgewichtung aller Kriterien muss 100 % betragen.

e. Geben Sie den Namen und eine Kurzbeschreibung der Kriterien ein.

f. Aktivieren Sie das Kontrollkästchen **Bewertungskriterien aktivieren**, um die Bewertungskriterien zu aktivieren.

g. Definieren Sie die **Bedingungen**, und legen Sie die Punktzahl für die Bedingungen fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Sie können auch neue Bedingungen mit der Schaltfläche **Neue Bedingung** hinzufügen und die Bedingung mit dem Symbol **Kriterien löschen** löschen.

i. Klicken Sie auf **Hinzufügen**, um die konfigurierten Kriterien hinzuzufügen.

Hier sehen Sie ein Beispiel für das Definieren einer Bedingung für eine Bedrohungsbewertung:

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. Klicken Sie auf die Schaltfläche **Verlauf neu berechnen**, um die Bedrohungsbewertung neu zu berechnen. Wenn sich die Bedrohungsbewertungsregel ändert, müssen Sie die Bewertungsregel erneut auf die erkennbaren Elemente anwenden, für die die Bedrohungsbewertung bereits in der Vergangenheit berechnet wurde. Verwenden Sie die Schaltfläche **„Verlauf neu berechnen“,** um den Neuberechnungsauftrag auszulösen.

Hinweis:

- Es wird eine Bestätigungsmeldung angezeigt, in der Sie die Aktion ausführen können. Dies ist ein Prozess mit langer Laufzeit, der im Hintergrund ausgeführt wird. Sie können bis zum Abschluss des Prozesses keine Änderungen vornehmen. Möchten Sie diese Aktion wirklich ausführen?
- Für alle Aktualisierungsereignisse, die für erkennbare Elemente im Rahmen von **„Verlauf neu berechnen“**generiert werden, ist die Verarbeitung von Webhooks deaktiviert. Wenn Sie sie aktivieren möchten, ändern Sie die Systemeigenschaft `webhook_ignore_threat_score_reapply`.

5. Klicken Sie auf **OK**.

Wichtig:
Diese Aktion löst einen Auftrag mit langer Ausführungszeit aus, und das System lässt bis zum Abschluss des Auftrags keine weiteren Änderungen an der Regel zur Bewertung von Bedrohungen zu. Weitere Informationen zur Konfiguration von Hintergrundaufträgen finden Sie unter Framework für Vulnerability Response-Hintergrundaufträge konfigurieren .

Im Folgenden finden Sie das Skript **„Skript verwenden (erweitert)“** : Verwenden Sie dieses Skript, um ein anwenderdefiniertes Skript zu erstellen, das die Bedrohungsbewertung im Bereich von 0 bis 100 zurückgibt.

Das Feld „Erweitertes Skript“ wird automatisch mit einer Funktion ausgefüllt, die die Parameter **„current“** und **„aggregats“** übernimmt. Diese Funktion sollte die Bedrohungsbewertung im Bereich von 0 bis 100 zurückgeben.

Hier ist der Parameter current das GlideRecord-Objekt der Entität (des erkennbaren Elements), für die die Bedrohungsbewertung berechnet wird. Für die erkennbaren Elemente entspricht sie dem GlideRecord für die Tabelle sn_sec_tisc_observable.

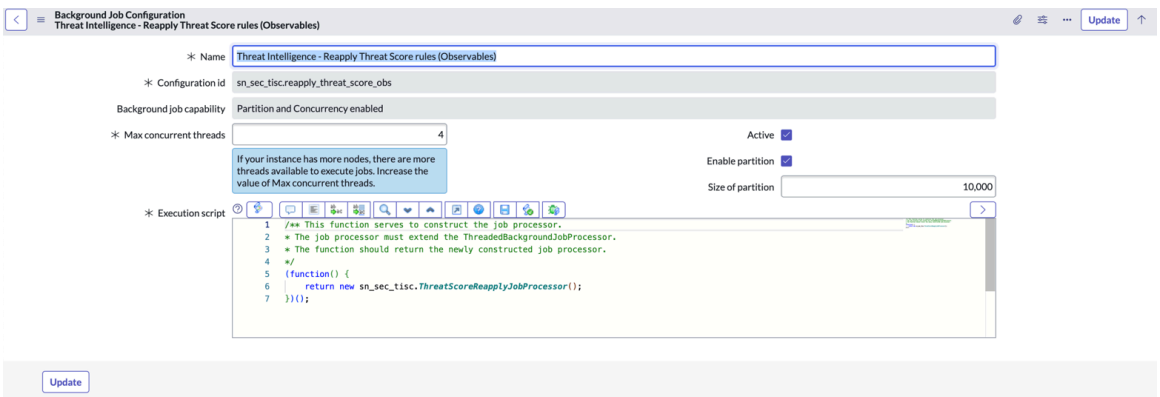
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Parameter „aggregats“ ist ein GlideRecord-Objekt des Tabellendatensatzes „sn_sec_tisc_aggregates“, das für den Zugriff auf die Datensatzanzahlen der verschiedenen zugeordneten Datensatztypen (z. B. Kampagnen oder Identitäten) für die Hauptentität (erkennbares Element) verwendet wird.

Beispielbeispiel für das Skript in der erweiterten Option:

```
answer = (function threatScoreCalculator(current, aggregates) {

   // return the threat score in the range of 0-100
   var threatSeverity = current.getValue("threat_severity");
   if(threatSeverity == "high")
    return 80;
   else {
      let associatedCampaigns = aggregates.getValue("num_of_campaigns");
      if(associatedCampaigns > 0)
         return 50;
   }
   return 0;

})(current, aggregates);
```

Zur Information sehen Sie unten einen Screenshot, der den Konfigurationsprozess des Hintergrundauftrags für die Bedrohungsbewertung zeigt.



Extraktionsregeln für MITRE ATT&CK-Technik

Extrahieren Sie MITRE-Techniken automatisch aus erkennbaren Elementen oder Objekten, die aus verschiedenen Datenquellen erfasst wurden, und extrahieren Sie MITRE-Techniken auch aus den Ergebnissen der Bedrohungssuche für den Datensatz erkennbarer Elemente.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Stellen Sie sicher, dass die MITRE ATT&CK-Repository-Daten in der von Ihnen verwendeten Instanz verfügbar sind. Wenn die Daten nicht verfügbar sind, führt die Anwendung die Extraktion nicht durch.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Gehe zu **Regel-Engine** > **Extraktionsregeln für MITRE ATT&CK-Technik**.
   Die Seite „Extraktionsregeln für MITRE ATT&CK-Technik“ wird angezeigt.
3. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **„Aktivieren“**, um die Extraktionsregel für MITRE ATT&CK-Technik zu aktivieren, nachdem Sie eine neue Regel erstellt haben.
   Wenn Sie die Extraktionsregel für MITRE ATT&CK-Technik nicht aktivieren, wird die Regel nicht auf den Datensatz angewendet.

Hinweis:

   a. Datenquellen: Wenn Sie die Extraktionsregel aktivieren, darf die Kombination aus Datenquellen und Integrationstyp mit keiner der vorhandenen aktivierten Extraktionsregeln übereinstimmen. Wenn dies der Fall ist, zeigt die Anwendung eine Fehlermeldung an, in der Sie aufgefordert werden, die vorhandenen Kombinationen zu ändern usw Aktivieren Sie die Regel.

   b. Bedrohungssuche: Wenn Sie die Extraktionsregel aktivieren, darf der Lieferantenname mit keiner der vorhandenen aktivierten Extraktionsregeln übereinstimmen. Wenn dies der Fall ist, zeigt die Anwendung eine Fehlermeldung an, in der Sie aufgefordert werden, den Lieferantennamen zu ändern und die Regel erneut zu aktivieren.

   c. Für die Anwender im Basissystem wird ein Beispiel für eine Extraktionsregel für die MITRE ATT&CK-Technik bereitgestellt. Diese Regeln befinden sich standardmäßig im Status „Deaktiviert“. Sie müssen die Regel aktivieren und aktivieren.

Feld	Beschreibung
Generische Regel für die Erfassung von Datenquellen	Dies ist eine generische Regel für die Erfassung aus allen Arten von Datenquellen, einschließlich Import Intelligence und manueller Erstellung.
Generische Regel für die Bedrohungssuche	Dies ist eine generische Regel für alle Integrationen der Bedrohungssuche.

5. Klicken Sie auf **Duplizieren**, um eine Kopie der Extraktionsregel zu erstellen.
6. Klicken Sie auf **Deaktivieren**, um die Extraktionsregel zu deaktivieren.

Hinweis:
Sobald sie deaktiviert ist, wird die Regel nicht mehr für die Extraktion von MITRE-Daten berücksichtigt.

7. Klicken Sie auf **Speichern**.
8. Klicken Sie **auf Löschen**, wenn Sie eine Extraktionsregel für MITRE ATT&CK-Technik löschen möchten.

Extraktionsmethode für MITRE ATT&CK-Technik

Die Extraktionsmethode für die MITRE ATT&CK-Technik beschreibt, wie die Extraktionsmethoden durchgeführt und die zugehörigen Techniken verifiziert werden.

1. Die Extraktionsregeln für Datenquellen (Bedrohungssuchen sind nicht anwendbar) werden verarbeitet, wenn ein Quelldatensatz für eine Entität (z. B. erkennbare Elementquelle oder Objektquelle) erstellt wird.
2. Die Regeln gelten für alle Felder im Datensatz der Entitätsquelle (außer Datum, Nummernfelder, Nutzungskategorie und Angriffsphasen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Die extrahierten MITRE-Techniken werden dem entsprechenden Entitätsdatensatz zugeordnet, und Sie zeigen die Datensätze in der zugehörigen Liste „MITRE-Techniken“ auf der Registerkarte **Zugehörige Datensätze** an.

Hinweis:
Die MITRE-Techniken werden zuerst extrahiert und dem Entitätsquelldatensatz zugeordnet. Anschließend werden die Technikzuordnungen dedupliziert und im übergeordneten Entitätsdatensatz zusammengefasst.

Zeigen Sie MITRE-Techniken an

1. Navigieren zu **Threat Intel-Bibliothek**beliebigen Entitätsdatensatz (erkennbares Element oder Objekt) mithilfe von.
2. Klicken Sie auf die Registerkarte **Zugehörige Datensätze**.
3. Wählen Sie **MITRE-Techniken** aus, und zeigen Sie die zugehörigen extrahierten Techniken an.
4. Klicken Sie auf die MITRE-Technik-ID, um den MITRE-Technikzuordnungsdatensatz anzuzeigen und darauf zuzugreifen. In der Spalte **„Quellen** “ werden alle Quellen angezeigt (ebenfalls durch Komma getrennt, wenn mindestens eine Quelle vorhanden ist), die dem Entitätsquelldatensatz zugeordnet sind, für den die MITRE-Extraktion durchgeführt wird.

Hinweis:
Wenn dieselben Taktik- und Technik-IDs aus mehreren Quellen extrahiert werden, wird nur ein Zuordnungsdatensatz für Taktik und Technik angezeigt, und in der Spalte **„Quellen** “ werden alle extrahierten Quellen angezeigt.

5. Zur Problembehandlung können Sie die MITRE-Extraktionsregel anzeigen, die für die Extraktion der Taktik- und Technikzuordnungen verantwortlich war, indem Sie zu **Technik Quellbeziehungen**navigieren.

Hinweis:
Achten Sie darauf, die Spalte **„Extraktionsregel“** über das Symbol **„Listenaktionen“** hinzuzufügen, falls die Spalte „Extraktionsregel“ nicht angezeigt wird.

Die Extraktionsregeln für Bedrohungssuchen werden immer dann verarbeitet, wenn der Datensatz für das Bedrohungssuchergebnis für ein erkennbares Element erstellt wird, für das die Aktion **„Bedrohungssuche ausführen“** ausgelöst wird. Die Extraktion wird nur für die Nutzlast der Rohdaten (Feld „raw_data“) durchgeführt, die im Ergebnis der Bedrohungssuche verfügbar ist Datensatz

Hinweis:

- Wenn in der extrahierten Entitätsquelle (erkennbares Element oder Objekt) oder im Bedrohungssuchergebnis für eine MITRE ATT&CK-Technik keine Taktik-ID vorhanden ist, werden die Technikzuordnungen für alle Taktiken erstellt, die der entsprechenden Technik im MITRE-Repository zugeordnet sind.
- Wenn in der extrahierten Entitätsquelle (erkennbares Element oder Objekt) oder im Bedrohungssuchergebnis für eine MITRE ATT&CK-Technik eine Taktik-ID vorhanden ist, werden die Technikzuordnungen ausdrücklich nur für alle extrahierten Taktiken erstellt, die der entsprechenden Technik zugeordnet sind im MITRE-Repository.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitskontrolllisten definieren

Verwenden Sie diese Funktion, um erkennbare Elemente in einem Massenvorgang hinzuzufügen oder zu entfernen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Gehe zu **Sicherheitskontrolllisten**.
   Sie können beispielsweise erkennbare Elemente zur Zulassungsliste hinzufügen und dann zur Option „Zulassungsliste“ wechseln.
3. Wählen Sie **Allow-Liste**aus.
4. Wählen Sie den Typ der erkennbaren Elemente wie IP-Adresse, Datei usw. aus, um sie der Allow-Liste hinzuzufügen.
5. Klicken Sie auf **Hinzufügen**.
   Die **Liste „Erkennbare Elemente auswählen für zulässig“** wird angezeigt.
6. Wählen Sie alle erkennbaren Elemente aus, die der Allow-Liste hinzugefügt werden müssen.
7. Klicken Sie auf **Zur Allow-Liste hinzufügen**.
   Die ausgewählten erkennbaren Elemente werden hinzugefügt.
8. Wählen Sie in ähnlicher Weise **Zu Verweigerungsliste hinzufügen,** um die erkennbaren Elemente der Liste „Entfernt“ hinzuzufügen.
9. Wählen Sie **Zur Beobachtungsliste hinzufügen**, um die erkennbaren Elemente zur Beobachtungsliste hinzuzufügen.

   Hinweis:
   Sie können die erkennbaren Elemente direkt über die Ansichtsseite des Formulars „Erkennbare Elemente“, die über dem Formularbanner verfügbar ist, der Zulassungsliste, der Deny-Liste oder der Beobachtungsliste hinzufügen.

10. Navigieren Sie zur Überprüfung zu **Threat Intel Library (Threat Intel Library**).
11. Wählen Sie den Typ des erkennbaren Elements aus, das der Allow-Liste hinzugefügt wurde.
    Das erkennbare Element wird als zur Allow-Liste hinzugefügt angezeigt.

    Hinweis:
    Allow-Liste und Deny-Liste schließen sich gegenseitig aus, und das System stellt automatisch sicher, dass ein erkennbares Element in der Allow-Liste nicht Teil der Deny-Liste ist und umgekehrt.

Taxonomien werden erstellt

Erstellen Sie Taxonomien für die Datenquellen-Datensätze.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Taxonomien**.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie den **Namen**ein.
4. Aktivieren oder deaktivieren Sie den **Taxonomiestatus** mithilfe der Formularaktionen Aktivieren oder Deaktivieren.

   Hinweis:
   Deaktivierte Taxonomien sind nicht für die Auswahl von Datensätzen verfügbar, für die Taxonomien anwendbar sind.

5. Wechseln Sie zum Abschnitt **„Taxonomiewerte“**, um Taxonomiewerte hinzuzufügen.
6. Klicken Sie auf **Neu**, um eine neue Formularansicht für den Taxonomiewert zu öffnen, und geben Sie die **Taxonomie** und **den Wert**ein.
7. Klicken Sie auf **Speichern**.
8. Navigieren Sie beispielsweise zu **Threat Intel-Bibliothek** > **Erkennbare Elemente** um die Taxonomien für den Datensatz erkennbarer Elemente zu überprüfen.
9. Navigieren Sie auf einer beliebigen Formularseite für erkennbare Elemente zum Abschnitt **„Tags und Taxonomien“,** und wählen Sie die neu erstellte Taxonomie aus.

   Hinweis:
   Sie können Tags und Taxonomien auch aus der Listenansicht der Threat Intel-Bibliothek hinzufügen.

Importieren Sie Taxonomien in einem Massenvorgang

Importieren Sie die Taxonomiedatensätze.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Taxonomien mit den Daten aus der Tabellenkalkulation importieren. Auf diese Weise können Sie mehrere Datensätze massenweise importieren.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Taxonomien**.
2. Wählen Sie die Schaltfläche **Importieren** aus.
   Diese Aktion öffnet eine Aktion zum Importieren der Datendatei im XLSX- oder CSV-Format. können Sie auch die Beispieldatei herunterladen, um das zu importierende Format zu verstehen. Das Dateiformat enthält zwei Werte, einschließlich Taxonomie und Taxonomiewert.
3. Klicken Sie auf den Link **Datei hinzufügen**.
4. Wählen Sie die Datei aus und **laden Sie sie hoch**.
5. Klicken Sie auf **Erledigt**.
   Eine Bestätigungsmeldung zeigt an, dass die Daten aus der angehängten Datei erfolgreich importiert wurden. Sie können auf den Link klicken, um die Importzusammenfassung anzuzeigen. Durch Klicken auf den Link wird der Datensatz in einer neuen Registerkarte geöffnet. Sie können die Anzahl der erstellten Taxonomien und Taxonomiewerte anzeigen. Wenn Fehler protokolliert werden, werden sie im Abschnitt „Importfehler“ protokolliert.

   Hinweis:
   Standardmäßig werden alle diese Taxonomien und Taxonomiewerte mit dem Status Aktiviert erstellt. Wenn Sie deaktivieren möchten, können Sie dies jederzeit in der Listenansicht tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Auf der Seite **„Taxonomien“** können Sie auf einen beliebigen Datensatz klicken. Mit dieser Aktion werden die Taxonomiewerte als separate Registerkarte angezeigt. Außerdem können Sie die beiden Taxonomiewerte sehen, die erfolgreich importiert wurden. Diese Taxonomiewerte befinden sich im Status „Aktiviert“.
7. Um einen der Taxonomieimporte anzuzeigen, können Sie außerdem jederzeit zum Abschnitt „ **Importe“** navigieren. Die importierten Taxonomien werden im Abschnitt **„Taxonomieimporte“** angezeigt.
8. Klicken Sie auf **Alle Importe**, um alle Taxonomieimporte anzuzeigen, die von verschiedenen Benutzern in der Anwendung erstellt wurden.
9. Klicken Sie auf **Meine Importe**, um die Taxonomieimporte für den aktuell angemeldeten Benutzer anzuzeigen.

Verwaltung des Reputationsrechners der Bedrohungssuche

Sie können den Rechner für Ergebnisse der Bedrohungssuche verwenden, um die Ergebnisse erkennbarer Elemente basierend auf den Antworten zu berechnen, die Sie vom Bedrohungssuche-Anbieter erhalten haben.

Sie können einen Rechner für Ergebnisse der Bedrohungssuche für Ihre Integration erstellen und ein Skript verwenden, um zu bestimmen, wie die verschiedenen Ergebnisse erkennbarer Elemente identifiziert werden sollen. Der Rechner für Ergebnisse der Bedrohungssuche enthält ein Beispielskript, das im Basissystem enthalten ist und das Sie verwenden können, um die Ergebnisse erkennbarer Elemente zu identifizieren. Alternativ können Sie dieses Skript entsprechend Ihren Anforderungen ändern.

Bei Drittanbieterintegrationen, die die berechneten Ergebnisse bereitstellen, ordnet der Rechner für Ergebnisse der Bedrohungssuche die Ergebnisse unterstützten Ergebnissen im Basissystem zu.

Rollup der Ergebnisse der Bedrohungssuche

Wenn Sie mehrere Ergebnisse der Bedrohungssuche für ein erkennbares Element von den verschiedenen Integrationsanbietern haben, werden die aktuellen Ergebnisse der Bedrohungssuche von allen Anbietern berücksichtigt, und die Gesamtergebnisse der erkennbaren Elemente werden wie folgt gekennzeichnet:

Rollup der Ergebnisse der Bedrohungssuche

Neuestes Ergebnis erkennbarer Elemente	Gesamtergebnis erkennbarer Elemente
Böswillig	Wenn einer der Integrationslieferanten das erkennbare Element als böswillig meldet, wird der gesamte Fund des erkennbaren Elements als böswillig gekennzeichnet.
Verdächtig	Wenn keiner der Integrationsanbieter das erkennbare Element als schädlich meldet, meldet einer von ihnen es als verdächtig. Anschließend wird der gesamte Fund des erkennbaren Elements als verdächtig markiert.
Clean	Wenn alle Integrationslieferanten das erkennbare Element als „Sauber“ melden, wird das gesamte Ergebnis des erkennbaren Elements als „Sauber“ markiert.
Unbekannt	Wenn keiner der Integrationslieferanten das erkennbare Element als schädlich oder verdächtig und einer von ihnen als unbekannt meldet, wird der Gesamtbefund des erkennbaren Elements als unbekannt markiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Reputationsrechner für die Bedrohungssuche an

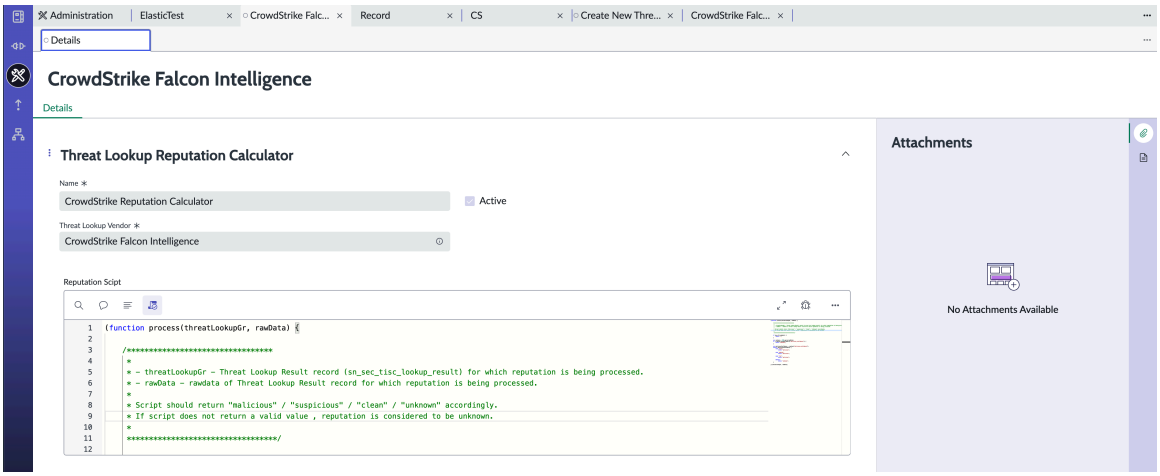
Sie können den Rechner für Ergebnisse der Bedrohungssuche anzeigen, um zu bestimmen, wie die Reputation des erkennbaren Elements basierend auf der Antwort eines bestimmten Anbieters der Bedrohungssuche berechnet wird.

Erforderliche Rolle: sn_sec_tisc.admin

Um den Reputationsrechner der Bedrohungssuche anzuzeigen, gehen Sie wie folgt vor:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Wählen Sie den Abschnitt **Rechner für Reputation der Bedrohungssuche** aus.

   Sie können die Liste der Reputationsrechner für die Bedrohungssuche anzeigen.
3. Klicken Sie auf den erforderlichen Reputationsrechner für die Bedrohungssuche, um die Details des Rechners anzuzeigen.



Erstellen Sie den Reputationsrechner für die Bedrohungssuche

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Pro Bedrohungssuche-Anbieter kann zu jedem Zeitpunkt nur ein Rechner für die Bedrohungssuche aktiv sein.

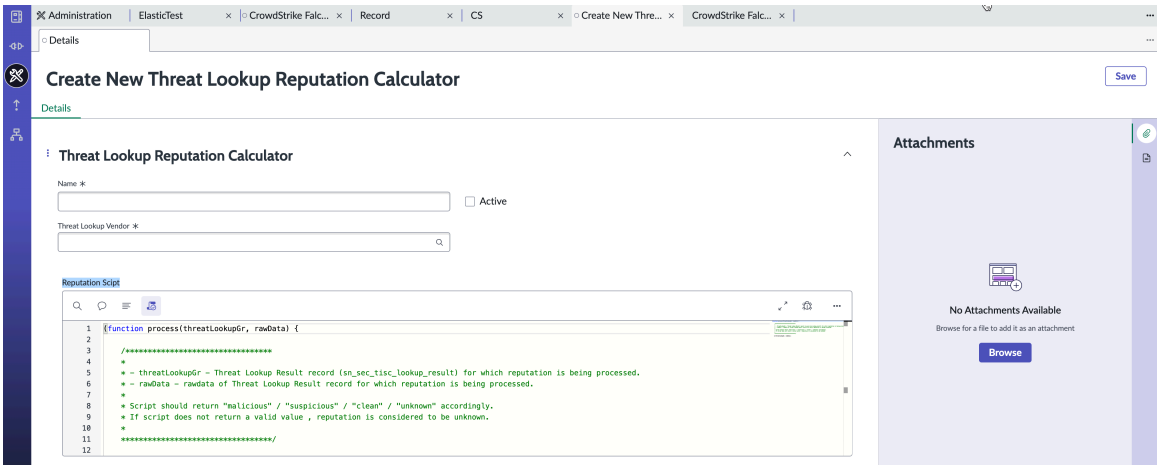
Um einen Reputationsrechner für die Bedrohungssuche zu erstellen, gehen Sie wie folgt vor:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Wählen Sie den Abschnitt **Rechner für Reputation der Bedrohungssuche** aus.

   Sie können die Liste der Reputationsrechner für die Bedrohungssuche anzeigen.
3. Klicken Sie auf **Neu**, um einen Reputationsrechner für die Bedrohungssuche zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Felder im Formular aus.

Erstellen Sie einenReputationsrechner für dieBedrohungssuche

Feld	Beschreibung
Name	Name für den Reputationsrechner der Bedrohungssuche.
Aktiv	Die Berechnung der Bedrohungssuche wird nur ausgeführt, wenn die Option „Aktiv“ ausgewählt ist.
Bedrohungssuche-Anbieter	Name des Anbieters der Bedrohungssuche. Beispiel: CrowdStrike Falcon Intelligence.
Reputationsskript	Skript-Editor, um festzulegen, wie die verschiedenen Ergebnisse erkennbarer Elemente identifiziert werden sollen. Jede Integration der Bedrohungssuche verfügt über ein Basisskript zur Berechnung der Reputation der Bedrohungssuche.

5. Klicken Sie auf **Speichern**.

Verwalten Sie E-Mail-Benachrichtigungen

Verwenden Sie ServiceNow Benachrichtigungen, um E-Mail-Benachrichtigungen für das System zu erstellen und zu verwalten und E-Mail-Protokolle anzuzeigen.

E-Mail-Benachrichtigungen

Verwenden Sie E-Mail-Benachrichtigungen, um ausgewählten Anwendern E-Mail-Benachrichtigungen zu bestimmten Aufgaben in der Anwendung zu senden, z. B. Aktualisierungen von erkennbaren Elementen/Indikatoren/verschiedenen anderen Objekten.

Erforderliche Rolle: Administrator

Hinweis:
Als Systemadministrator können Sie die Details der E-Mail-Benachrichtigungsregel in der klassischen Ansicht der Anwendung anzeigen, erstellen oder bearbeiten.

Threat Intelligence-Sicherheitszentrum bietet regelgesteuerte E-Mail-Benachrichtigungen, die an einzelne E-Mail-Adressen oder eine Liste von E-Mail-Adressen gesendet werden. Normalerweise werden Informationen zur Verbreitung von Bedrohungsinformationen an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

interne Benutzer in Form von E-Mails gesendet. Der Prozess beinhaltet die Bereitstellung der Threat Intelligence-Daten an Benutzer gemäß dem angegebenen Format und den angegebenen Zeitachsen.

Mit E-Mail-Benachrichtigungen können Administratoren Folgendes angeben:

- Wann die Benachrichtigung gesendet wird
- Wer die Benachrichtigung erhält
- Welchen Inhalt die Benachrichtigung hat

Hinweis:
Wenn Sie Änderungen vornehmen möchten, müssen Sie konfigurieren, an wen die E-Mail gesendet werden soll, indem Sie die Basissystemregeln entsprechend Ihren Anforderungen ändern.

Weitere Informationen finden Sie im Abschnitt E-Mail-Benachrichtigung erstellen in der Dokumentation Verwaltung der Now Platform.

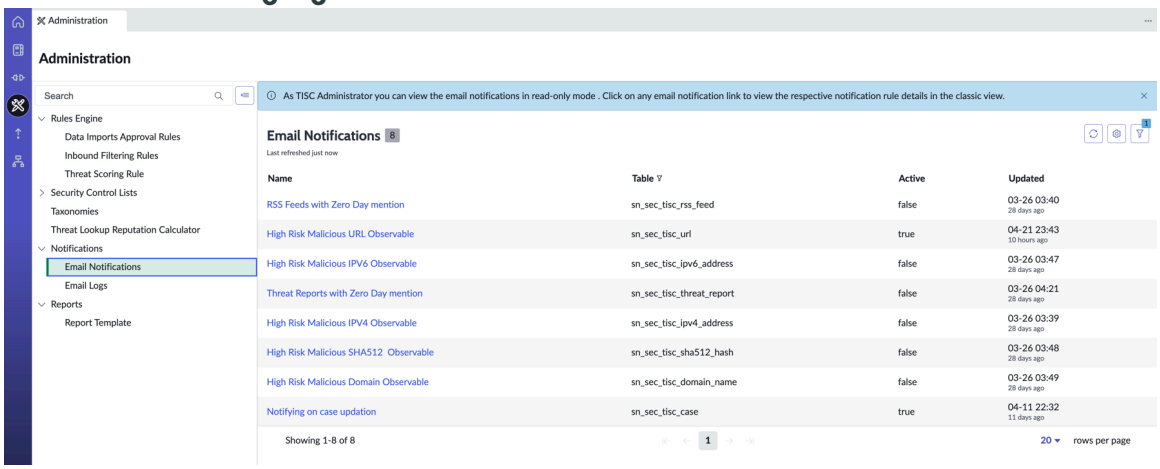
In der folgenden Tabelle sind die im Basissystem bereitgestellten E-Mail-Benachrichtigungsregeln aufgeführt.

E-Mail-Benachrichtigungen

Name	Tabelle
RSS-Feeds mit Zero Day-Erwähnung	sn_sec_tisc_rss_feed
Erkennbares Element der schädlichen URL mit hohem Risiko	sn_sec_tisc_url
Bösartiges erkennbares IPV6-Element mit hohem Risiko	sn_sec_tisc_ipv6_address
Bedrohungsberichte mit Zero Day-Erwähnung	sn_sec_tisc_threat_report
Bösartiges erkennbares IPv4-Element mit hohem Risiko	sn_sec_tisc_ipv4_address
Bösartiges SHA512-Erkennbares Element mit hohem Risiko	sn_sec_tisc_sha512_hash
Erkennbares Element der böswilligen Domäne mit hohem Risiko	sn_sec_tisc_domain_name
Benachrichtigung bei Fallaktualisierung	sn_sec_tisc_case

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Benachrichtigungen



Hinweis:
Durch Klicken auf die einzelnen E-Mail-Benachrichtigungen gelangen Sie zur klassischen Anwenderoberfläche, sodass Sie die erforderlichen Aktionen ausführen können, z. B. Anzeigen, Bearbeiten oder Erstellen der Benachrichtigungen.

E-Mail-Protokolle

Dieser Abschnitt bietet TISC-Administratoren eine übersichtliche Übersicht über die E-Mails, die mithilfe der konfigurierten E-Mail-Benachrichtigungsregeln gesendet werden.

E-Mail-Benachrichtigungen und Protokolle

TISC bietet verschiedene Bereiche für den Zugriff auf E-Mail-Benachrichtigungen und Protokolle basierend auf verschiedenen Personas.

Hinweis:

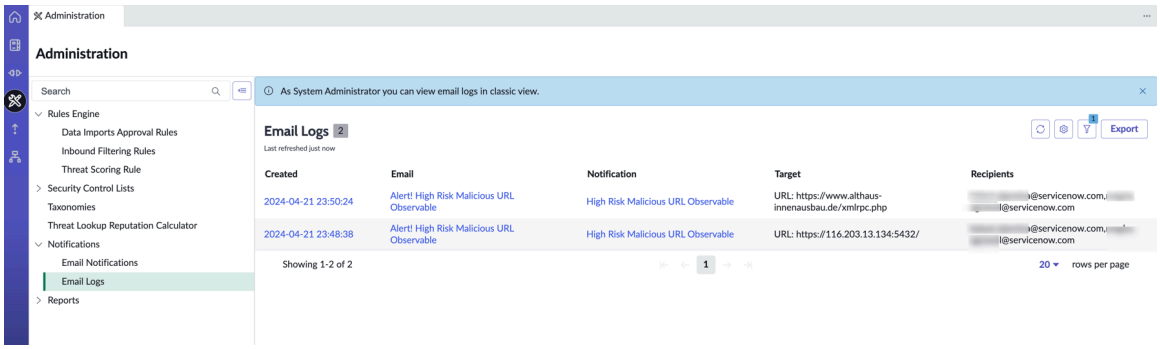
Persona	Zugriffsebenen
TISC-Administrator (sn_sec_tisc.admin)	Als sn_sec_tisc.admin können Sie nur die E-Mail-Benachrichtigungen anzeigen, die für TISC konfiguriert sind. **Hinweis:** Klicken Sie auf die Hyperlinks der E-Mail-Protokolle, um zur klassischen Anwenderoberfläche zu navigieren und diese Benachrichtigungen anzuzeigen.
Systemadministrator (admin)	Als Administrator können Sie Benachrichtigungen in der klassischen Anwenderoberfläche erstellen, anzeigen und bearbeiten. **Hinweis:** Klicken Sie auf die Hyperlinks der E-Mail-Protokolle, um zur klassischen Anwenderoberfläche zu navigieren und diese Benachrichtigungen anzuzeigen und zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sowohl der TISC-Administrator als auch der Systemadministrator können die Filter verwenden und nach den E-Mail-Protokollen suchen.

E-Mail-Protokolle



Berichtsvorlagen

Definiert die Möglichkeit, die Berichtsvorlagen, die innerhalb der Gruppe von Benutzern geteilt werden können, wiederzuverwenden, um Berichte schnell und konsistent zu generieren.

Verwenden Sie diese Funktion, um verschiedene Arten von Berichtsvorlagen zu erstellen, die auf Fälle angewendet werden können, die den Status laufender Untersuchungen in Bezug auf eine Bedrohung für Ihre Organisation bereitstellen und bei der Generierung entsprechender Berichte helfen.

In diesem Abschnitt wird erläutert, wie das CTI-Reporting auf Fallebene implementiert wird. Außerdem erhalten Sie Einblicke in Administrator- (Vorlagendesign) und Analysten- (Laufzeit) Experiences.

Sie können der Berichtsvorlage anwenderdefinierte Formularfelder für Fallaufgaben oder zugehörige Listen hinzufügen, die punktweise durchlaufbar sind. Darüber hinaus können Sie den Bericht mithilfe verschiedener Berichtselemente entsprechend Ihren Anforderungen formatieren und konfigurieren.

Erforderliche Rolle: sn_sec_tisc.admin

In der folgenden Tabelle werden einige Berichtsvorlagen erläutert, die im Basissystem bereitgestellt werden.

Berichtsvorlage

Name	Beschreibung
Fallstatusbericht – Profil des Bedrohungsakteurs	Der Bericht bietet einen Status über die laufende Falluntersuchung im Zusammenhang mit einem Bedrohungsakteur, der versucht, den Kontext und die Relevanz der Bedrohung für die Organisation, das Verhalten des Angreifers und die potenziellen Ziele, die IoC-Anreicherung, die zugehörigen Malware und Tools, die beobachteten TTPs und den Unterschied zu zu verstehen bestehende TTPs – neue Nettofähigkeiten, geringfügige Änderungen usw.
Kurzübersicht	Der Bericht soll leitende Entscheidungsträger über ein bestimmtes Risiko informieren. Der Schwerpunkt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichtsvorlage (Fortsetzung)

Name	Beschreibung
	liegt auf Zielgruppen von Führungskräften, und bei der Unterstützung strategischer Probleme wird das Warum und Wie und nicht das Was und Wann erläutert. Technische Details und Anhänge zur Unterstützung von langen, erzählenden Texten werden in diesen Bericht nicht aufgenommen.
Zusammenfassung nach Untersuchung – Profil des Bedrohungsakteurs	Der Bericht soll dem Unternehmen Kontext und Relevanz der Bedrohung bieten. Angreiferverhalten und potenzielle Ziele IoC-Ergänzung Zugehörige Malware und Tools; Beobachtete TTPs; Unterschied zu vorhandenen TTPs – neue Nettofähigkeiten, geringfügige Änderungen usw.

Hinweis:
Standardmäßig befinden sich diese Berichte im Status „Veröffentlicht“ und befinden sich im schreibgeschützten Modus. Da sich die Berichtsvorlagen im schreibgeschützten Modus befinden, können die Anwender keine Änderungen an den Vorlagen vornehmen, und die Analysten können die Berichte nicht generieren, da die Berichtsvorlagen deaktiviert sind.

Erstellen Sie eine neue Berichtsvorlage

Erstellen Sie eine neue Fallberichtsvorlage, die den Geschäftsanforderungen Ihrer Organisation entspricht.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Berichte** > **Berichtsvorlage**.
   In diesem Abschnitt werden die im Basissystem verfügbaren Vorlagen und die veröffentlichten Vorlagen angezeigt. Sie können jede gewünschte Vorlage für die Arbeit mit den Berichten auswählen.

   Hinweis:
   In diesem Abschnitt können Sie bei Bedarf auch die Vorlagen löschen.

3. Klicken Sie auf **Neu**.
4. Geben Sie den Namen und die Beschreibung der Vorlage ein.
5. Klicken Sie auf **Speichern**.
   Der Abschnitt „Vorlageninhalt“ wird angezeigt.

   Hinweis:
   Wenn Sie eine neue Berichtsvorlage erstellen, befindet sich die Vorlage im Entwurfsstatus. Dies bedeutet, dass die Vorlagenerstellung in Arbeit ist und andere Anwender die Berichtsvorlage erst anzeigen können, wenn sie abgeschlossen ist.

6. Erweitern Sie den **Vorlageninhalt**, um die gewünschten Felder in den Vorlagentext einzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Mit der Vorlage, die Sie bearbeiten, können Sie den Vorlagentext definieren und die erforderlichen Variablen auswählen, um sie dem Abschnitt des Vorlageneditors hinzuzufügen. Die Vorlagen werden mit dem Rich-Text-Editor (RTE) unterstützt, sodass Sie verschiedene verfügbare Funktionen wie Einrückung, Schriftgröße, Tabellen erstellen, Bilder hinzufügen und verschiedene andere Formatierungsfunktionen steuern können.
- Sie können auch Bilder in Ihre Berichtsvorlagen einfügen. Dazu müssen Sie das Bild kopieren und direkt in die Vorlage einfügen. Wenn Sie ein Bild hinzufügen, wird dieses Bild als Anhang hochgeladen.
- Sie können ein Bild mit bis zu 698 Pixeln hochladen oder anhängen. Wenn das Bild größer als die definierte Größe ist, wird es automatisch an die Originalgröße angepasst. Diese Einschränkung der Pixelgröße trägt dazu bei, dass die PDF-Berichtsgenerierung im richtigen Format angezeigt wird, und die Bilder werden im Bericht nicht abgeschnitten.

7. Fügen Sie die erforderlichen Elemente des Falls hinzu.
8. Klicken Sie **auf Inhalt speichern**, um den Inhalt Ihrer neuen Berichtsvorlage zu speichern.
9. Klicken Sie auf **Vorschau**, um eine Vorschau Ihres Berichtsformats anzuzeigen und zu sehen, wie ein Bericht generiert wird, wenn Sie einen Fallbericht generieren.

Hinweis:

- **Fallfelder**: Wenn Sie Ihre Berichtsvorlage(n) ändern, können Sie eine Vorschau der der Vorlage hinzugefügten Inhalte anzeigen. Wenn Sie beispielsweise einen Fallbericht generieren und ein Feld mit der Bezeichnung „Kurzbeschreibung“ hinzufügen möchten, können Sie dieses Feld aus den Fallfeldern auswählen. Anschließend wird dieses Feld als Variable in der Berichtsvorlage hinzugefügt. Wenn ein Bericht für den Analysten generiert wird, wird die Kurzbeschreibung des Falls im Bericht angezeigt.
- **Datensätze**: In der Berichtsvorlage können Sie auch die zugehörigen Datensätze dieses bestimmten Falls hinzufügen, die als Artefakte des Falls angezeigt werden. Wenn Sie beispielsweise schädliche erkennbare Elemente im Bericht aus den zugehörigen Listen erkennbarer Elemente anzeigen möchten, können Sie diese Ihrer Berichtsvorlage hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt
- **Skripts**: Wenn Sie das Datum und die Uhrzeit des Berichts anzeigen möchten, können Sie Ihrer Berichtsvorlage das Skript **„Aktuelles Datum/Uhrzeit“** hinzufügen. Dadurch werden das Datum und die Uhrzeit der Berichterstellung hinzugefügt.
- **MITRE ATT&CK**: Hiermit werden die Techniken angezeigt, die der MITRE-Karte in Ihrem Bericht zugeordnet sind.

Nachdem Sie Ihrer Berichtsvorlage alle erforderlichen fallbezogenen Felder hinzugefügt haben, müssen Sie Ihre Berichtsvorlage veröffentlichen.

10. Klicken Sie **auf Veröffentlichen**, um die Vorlage zu veröffentlichen.
Ob Sie die Berichtsvorlage veröffentlichen möchten oder nicht wird eine Bestätigungsmeldung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie eine Berichtsvorlage veröffentlichen, wird diese Vorlage für alle Anwender aktiviert. Falls er veraltet ist und Sie die Anzeige des Berichts für die Anwender einschränken möchten, können Sie den veröffentlichten Bericht deaktivieren. Dies bedeutet, dass die Berichtsvorlage für die Anwender ausgeblendet wird. Sie müssen den veröffentlichten Bericht erneut aktivieren, damit die Anwender ihn anzeigen und verwenden können, bis er für die Anzeige ausgeblendet wird.

11. Klicken Sie auf **Löschen**, um die Berichtsvorlage zu löschen, falls Sie sie nicht mehr verwenden möchten. Wenn Sie Ihre Berichtsvorlage umbenennen möchten, klicken Sie auf **Bearbeiten**, und ändern Sie die gewünschten Felder.

Systemeigenschaften für Berichte

Im Folgenden werden die Systemeigenschaften für Berichte erläutert.

Eigenschaft	Beschreibung	Wert
sn_sec_reporting.max_list_columns_allowed	Anzahl der Spalten beschränken, die beim Rendern von Listen in PDF-Berichten hinzugefügt werden können. Dadurch werden die Spalten vom Anfang der Ansicht bis zum zulässigen Grenzwert verwendet.	5
sn_sec_reporting.report_default_style_object	Verwenden Sie diese Eigenschaft, um die CSS von freien Formfeldern, dem linken Bereich und der Berichtslisten zu steuern.	(JSON-Objekt)
sn_sec_reporting.load_all_records	Lädt alle Datensätze für die Listen im Bericht, die aus einer Vorlage erstellt wurden. „true“ – lädt alle Datensätze; und „false“ – lädt eine bestimmte Anzahl von Datensätzen, die durch die Eigenschaft „sn_sec_reporting.reporting_list_records_count“ definiert sind.	falsch
sn_sec_reporting.reporting_list_records_count	Lädt eine bestimmte Anzahl von Datensätzen im Berichtseditor.	20
sn_sec_tisc.sn_sec_tisc_case.defang_secured_urls	Steuert, ob URLs aus Listen entsperrt werden oder nicht.	wahr
sn_sec_tisc.show_all_task_reporting	Bei „true“ werden alle Taktiken (einschließlich der Taktiken, denen keine Techniken mit dem Fall zugeordnet sind) für die im Bericht gerenderten MITRE-Listen angezeigt.	falsch
sn_sec_tisc.reporting_email_template	Sys-ID der E-Mail-Client-Vorlage für die Falltabelle (sn_sec_tisc_case), die in der Berichtfreigabe verwendet wird.	b55e22c54324021060eee0ea78b8f2df

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Wert
sn_sec_tisc.sn_sec_tisc_case.excluded_fields	Ausgeschlossene Felder des Falls in den Menüoptionen des Berichts/ der Vorlage zum Ersetzen eines Felds.	(Liste aller ausgeschlossenen Fallfelder
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_header	Diese Eigenschaft wird verwendet, um den entsprechenden UI-Nachrichtendatensatz für die Fallfeldbezeichnung in den Menüoptionen für Berichte/ Vorlagen abzurufen.	sn_sec_tisc_case_reporting_ctx_menu_field_header

Bearbeiten Sie eine veröffentlichte Berichtsvorlage

Bearbeiten Sie die Berichtsvorlagen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > > **Administration**.
2. Auswahlvorgang **Berichte** > **Berichtsvorlage**.
3. Wählen Sie die gewünschte Berichtsvorlage aus.
4. Klicken Sie auf die Schaltfläche **Bearbeiten**, die in der Berichtsvorlage angezeigt wird.

Hinweis:

In einer Bestätigungsmeldung wird Folgendes angezeigt: Sie bearbeiten eine veröffentlichte Vorlage und müssen die Vorlage erneut veröffentlichen, um sie unter Fallberichte verfügbar zu machen. Möchten Sie die Bearbeitung fortsetzen? was bedeutet, dass Sie die bearbeitete Vorlage erneut veröffentlichen müssen, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. Klicken Sie im Bestätigungsdialogfeld **auf Bearbeiten**.
6. Nehmen Sie die erforderlichen Änderungen vor, indem Sie die erforderlichen Inhaltsfelder oder die zugehörige Liste hinzufügen.
7. Klicken Sie auf **Inhalt speichern**.
8. Klicken Sie auf die Schaltfläche **Veröffentlichen**, um die Änderungen zu veröffentlichen.

Hinweis:

a. Sie können den Inhalt der Berichtsvorlage auch in der Vorschau anzeigen, bevor Sie die Berichtsvorlage veröffentlichen.
b. Es wird eine Bestätigungsmeldung angezeigt: Möchten Sie diese Vorlage wirklich veröffentlichen? Klicken Sie **auf Veröffentlichen,** um mit der Veröffentlichung der Berichtsvorlage fortzufahren.
c. Wenn Sie die Berichtsvorlage löschen möchten, können Sie auf **„Löschen“** klicken, um die Berichtsvorlage zu löschen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Duplizieren Sie eine Berichtsvorlage

Duplizieren Sie eine Berichtsvorlage. Wenn Sie inkrementelle Aktualisierungen hinzufügen möchten, können Sie eine Kopie der Berichtsvorlage erstellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > > **Administration**.
2. Auswahlvorgang **Berichte** > **Berichtsvorlage**.
3. Wählen Sie die Vorlage aus.
4. Klicken Sie auf **Duplikat**.
   Der Inhalt der ausgewählten Vorlage wird dupliziert, und eine Kopie dieser Vorlage wird angezeigt. Die Vorlage geht wieder in den Status Entwurf über. Sie können den Inhalt anpassen und die Vorlage dann nach Bedarf umbenennen.
5. Bearbeiten oder ändern Sie den Inhalt der kopierten Vorlage.

Hinweis:
Sie können die Berichtsvorlagen auch löschen, wenn Sie sie nicht mehr benötigen, und neue Vorlagen erstellen.

Arbeiten mit Webhooks

Ein Webhook ist eine HTTP-Anforderung, die von einem Ereignis im Quellsystem (TISC) ausgelöst und mit einer Nutzlast von Ereignisdaten an ein Zielsystem gesendet wird (in dem die Endpunkt-URL vorhanden ist).

Diese Webhooks in Threat Intelligence-Sicherheitszentrum sind nützlich, um die Zielanwendung zu benachrichtigen, wenn das -Ereignis auftritt.

In TISC können Sie:

- Konfigurieren Sie Webhooks
- Auslöser verwalten
- Wiederholungsmechanismus
- Validierung durchführen
- Abonnements verwalten

Systemeigenschaften für Webhooks

Die Systemeigenschaften für Webhooks werden unten erläutert.

Eigenschaftsname	Beschreibung	Typ	Wert
sn_sec_tisc.webhook_ignore_threat_score_reapply	Ignorieren Sie Webhook-Ereignisse, die durch den Verlauf der Neuberechnung der Bedrohungsbewertung ausgelöst werden.	Wahr/Falsch	wahr
sn_sec_tisc.webhook_max_event_batch_size	Maximale Anzahl von Ereignissen, die als	Ganzzahl	1000

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung	Typ	Wert
	Teil einer Webhook-Anforderung gesendet werden sollen. Die Batchgröße wird auf 2.000 beschränkt, auch wenn in dieser Eigenschaft ein höherer Wert festgelegt ist.		
sn_sec_tisc.webhook_retry_count	Anzahl der Wiederholungen einer fehlgeschlagenen Anforderung, bevor sie als Fehler markiert und mit dem nächsten Ereignis-Batch fortgefahren wird. Die Wiederholungsanzahl wird auf 10 beschränkt, auch wenn in dieser Eigenschaft eine höhere Zahl festgelegt ist.	Ganzzahl	5
sn_sec_tisc.webhook_retry_interval	Anzahl der zu wartenden Sekunden, bevor ein fehlgeschlagener Batch erneut versucht wird. Dies wird basierend auf der Anzahl der Wiederholungen exponentiell erhöht. Beispiel: Wenn „retry_count“ auf „3“ und „retry_interval“ auf „30“ festgelegt ist, werden Wiederholungen nach 30, 60 und 120 Sekunden ausgelöst. Das anfängliche Wiederholungsintervall wird auf 300 Sekunden begrenzt, auch wenn in dieser Eigenschaft ein höherer Wert festgelegt ist.	Ganzzahl	30

Automatische Übersetzung

Konfigurieren Sie Webhooks

Konfigurieren Sie einen Webhook, um Ereignisse im Threat Intelligence-Sicherheitszentrum zu abonnieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
TISC-Webhooks bieten die Möglichkeit zur Integration in Sicherheitstools wie SIEM. Benutzer können dann verschiedene Ereignisse abonnieren, die sich auf verschiedene Artefakte beziehen, z. B. erkennbare Elemente oder Indikatoren, Malware oder Bedrohungsakteure. TISC benachrichtigt Sicherheitstools (z. B. SIEM), wenn eine neue Threat Intelligence verfügbar ist oder vorhandene Threat Intelligence-Daten in TISC aktualisiert oder gelöscht werden.

Beispiel: Wenn in Threat Intelligence ein neues erkennbares Element hinzugefügt wird, wird eine Nutzlastanforderung an die Webhook-URL-Konfiguration gesendet. Diese Nutzlastanforderung sammelt normalerweise die Informationen der erkennbaren Elemente und stellt sie als zusätzliche Informationen für Sicherheitstools (z. B. SIEM) bereit.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Webhook-Konfigurationen** > **Webhooks**.
   Die Seite „Webhooks“ wird angezeigt.
3. Klicken Sie auf **Neu**.
4. Klicken Sie auf **Validieren und speichern**.
   Falls Ihre Konfigurationsdetails falsch sind, validiert das System automatisch die Verbindung, wenn die Konfigurationsdetails geändert werden. Anschließend zeigt die Anwendung eine Warnmeldung an, dass die Validierung des Webhook fehlgeschlagen ist und Sie die Konfigurationsdetails überprüfen und entsprechend ändern müssen .

Hinweis:

- Zur Validierung des Webhooks wird eine leere Anforderungsnutzlast an den Endpunkt gesendet, und der Anwender muss sicherstellen, dass der Endpunkt einen erfolgreichen Antwortcode (200) sendet, wenn die leere Anforderung an den konfigurierten Webhook-Endpunkt übergeben wird.
- Standardmäßig weist jeder erstellte Webhook den Status „Deaktiviert“ auf. Sie müssen den Webhook aktivieren und aktivieren. Im Basissystem wird ein Beispiel-Webhook als Referenz für die Benutzer bereitgestellt.

Abonnieren Sie Auslöser

Zeigen Sie die Liste aller abonnierten Webhook-Auslöser für den aktuellen Webhook an.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Webhook-Konfigurationen** > **Webhooks**.
   Die Seite „Webhooks“ wird angezeigt.
3. Wählen Sie den Webhook aus.
   Der Abschnitt Abonnierte Auslöser wird angezeigt.
4. Klicken Sie im Abschnitt Abonnierter Auslöser auf die Schaltfläche **Abonnieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Listenansicht zeigt alle aktivierten Webhook-Auslöser in der Instanz.

5. Wählen Sie die gewünschten Webhook-Auslöser aus, und klicken Sie im Dialogfeld „Webhook-Auslöser“ **auf Abonnieren**.
   Es wird eine Bestätigungsmeldung angezeigt, dass der Webhook die ausgewählten Auslöser erfolgreich abonniert hat. Von hier aus können Sie auch direkt einen neuen Auslöser erstellen und den Webhook abonnieren.

Hinweis:
Sie können das Abonnement des Webhooks auch von den ausgewählten Auslösern **abbestellen**.

Zeigen Sie Webhook-Fehlerprotokolle an

Verwenden Sie diesen Abschnitt mit Fehlerprotokollen, um alle Audit-Einträge anzuzeigen, die im Status für einen bestimmten Webhook als Fehler markiert sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
Die Audit-Protokolle ermöglichen es den Anwendern, weitere Untersuchungen durchzuführen, die Ausführung zu debuggen und die Ursache des Ausführungsfehlers zu identifizieren.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Webhook-Konfigurationen** > **Webhooks**.
   Die Seite „Webhooks“ wird angezeigt.
3. Wählen Sie den Webhook aus.
4. Navigieren Sie zu **Fehlerprotokolle**.
5. Zeigen Sie die Fehlerprotokolle an.
   In der Listenansicht werden alle Fehlerprotokolle eines bestimmten Webhooks angezeigt.
6. Wechseln Sie zur **Batch** -Spalte.
7. Klicken Sie auf eine beliebige **Batch-ID**.

Hinweis:
Jedes Fehlerprotokoll ist einem Batch zugeordnet. Mit der Batch-ID (in der Spalte Batch) können Sie den zugehörigen Batch-Datensatz anzeigen. Klicken Sie auf eine der Batch-IDs. Diese wird auf einer separaten Registerkarte geöffnet. Jede Batch-ID enthält die Webhook-Batch-Nummer, die Fehlermeldung, den Antwortstatuscode, die Anzahl der Wiederholungen, die tatsächlichen Nutzlastdaten und die Liste der Ereignisse, die an den Webhook gesendet werden.

8. Klicken Sie auf **„Batch wiederholen“**, um die fehlgeschlagenen Batches zu wiederholen.
   Wenn Sie auf diese Schaltfläche klicken, wird eine Anforderungsnutzlast (dieser bestimmten Batch-Informationen) an den konfigurierten Webhook-Endpunkt gesendet.

Hinweis:
Diese Aktion ist nur für die Batch-Datensätze verfügbar, bei denen Ausführungsfehler aufgetreten sind oder die erfolgreich abgeschlossen wurden. Die Datensätze mit dem Status „Wiederholen“ werden automatisch wiederholt.

Webhook-Batch anzeigen

Für jede Webhook-Ausführung wird ein Webhook-Batch-Datensatz erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Um die Anzahl der API-Aufrufe zu reduzieren, die an die Webhook-Endpunkte gesendet werden, wird die Stapelverarbeitung von Ereignissen in Webhooks implementiert. Wenn für jeden Webhook mehrere Ereignisse fast gleichzeitig ausgelöst werden, werden alle diese Ereignisse als Teil derselben Anforderung an den Webhook-Endpunkt gesendet.

Prozedur
1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Webhook-Konfigurationen** > **Webhooks**.
   Die Seite „Webhooks“ wird angezeigt.
3. Wählen Sie den Webhook aus.
4. Navigieren Sie zu **Fehlerprotokolle**.
5. Zeigen Sie die Fehlerprotokolle an.
   In der Listenansicht werden alle Fehlerprotokolle eines bestimmten Webhooks angezeigt.
6. Wechseln Sie zur **Batch** -Spalte.
7. Klicken Sie auf eine beliebige **Batch-ID**.
   Die Seite „Webhook Batch“ wird angezeigt.

Hinweis:
Alle Batches werden in der Tabelle `sn_sec_tisc_webhook_batch`gespeichert.

Nachfolgend finden Sie das Beispiel für ein Nutzlastformat, das der Webhook-Endpunkt empfängt:


```
{
  "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
  "events": [
    {
      "record": "Observable",
      "record_fields": {
        "is_false_positive": "false",
        "reputation": "malicious",
        "sys_updated_on": "2024-07-22T14:31:26.000Z",
        "type": "url",
        "sys_updated_by": "admin",
        "sys_created_on": "2024-07-04T06:45:20.000Z",
        "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
        "is_defanged": "false",
        "sys_created_by": "SecCommon.System",
        "tags": "Enriched",
        "taxonomies": "T1: V1",
        "domain": "urlhaus.abuse.ch",
        "status": "active",
        "source_count": "1",
        "threat_score": "20",
        "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
        "value": "https://urlhaus.abuse.ch/url/2578255/",
        "confidence": "89",
        "expiration_time": "2025-10-07T07:13:18.000Z",
        "tlp": "CLEAR"
      },
```


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "trigger": {
          "name": "Observable Update",
          "type": "UPDATE",
          "trigger_time": "2024-07-22T14:31:26.000Z",
          "trigger_fields": [
            {
              "field_name": "reputation",
              "previous_value": null,
              "current_value": "malicious"
            }
          ]
        }
      },
      {
        "record": "Observable",
        "record_fields": {
          "is_false_positive": "false",
          "reputation": "malicious",
          "sys_updated_on": "2024-07-22T14:31:19.000Z",
          "type": "url",
          "sys_updated_by": "admin",
          "sys_created_on": "2024-07-04T06:45:20.000Z",
          "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
          "is_defanged": "false",
          "sys_created_by": "SecCommon.System",
          "tags": "Enriched",
          "taxonomies": "T1: V1",
          "domain": "urlhaus.abuse.ch",
          "status": "active",
          "source_count": "1",
          "threat_score": "20",
          "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
          "value": "https://urlhaus.abuse.ch/url/2578264/",
          "confidence": "89",
          "expiration_time": "2025-10-07T07:13:18.000Z",
          "tlp": "CLEAR"
        },
        "trigger": {
          "name": "Observable Update",
          "type": "UPDATE",
          "trigger_time": "2024-07-22T14:31:19.000Z",
          "trigger_fields": [
            {
              "field_name": "reputation",
              "previous_value": null,
              "current_value": "malicious"
            }
          ]
        }
      }
    ]
}
```


Die folgende Tabelle enthält die Batch-Nutzlaststruktur und ihre Attribute, die als Webhook-Nutzlast an die Anwender gesendet werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter in der Batch-Nutzlast	Typ	Beschreibung
batch_id	Zeichenfolge	Gibt den eindeutigen Bezeichner für einen Batch an.
Ereignisse	Array von Objekten	Enthält ein Array von Ereignissen, die als Teil dieses Webhooks ausgelöst werden. Jedes Ereignis enthält den Snapshot der Feldwerte zum Zeitpunkt der Ereignisgenerierung und enthält auch die Auslöserinformationen. **Hinweis:** Weitere Informationen zum Anzeigen der Parameter im Ereignisobjekt finden Sie unter Webhook-Auslöser.

Hinweis:

8. Klicken Sie auf die Schaltfläche **„Batch wiederholen“**, um den fehlgeschlagenen Batch zu wiederholen.

Hinweis:
Sie können den Wiederholungsbatch auch für die abgeschlossenen Batches auslösen.

Webhook-Auslöser

Webhook-Auslöser werden verwendet, um die Threat Intelligence-Entitäten zu filtern, die für Ereignisänderungen wie Erstellen, Aktualisieren und Löschen nachverfolgt werden müssen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Webhook-Konfigurationen** > **Wiederholungen**.
   Die Seite „Webhooks-Auslöser“ wird angezeigt.
3. Klicken Sie auf **Neu**.
4. Klicken Sie auf **Speichern**.
   Standardmäßig wird der Auslöser im Status „deaktiviert“ erstellt.
5. Klicken Sie auf **„Aktivieren“**, um den Auslöser zu aktivieren. Dieser Auslöser steht dann den Webhooks zum Abonnieren zur Verfügung.

Hinweis:
Klicken Sie auf **Deaktivieren**, um den aktivierten Auslöser zu deaktivieren. Durch die Deaktivierung werden alle zugehörigen Webhooks von diesem Auslöser abgemeldet.

6. Klicken Sie auf **Beispielnutzlast anzeigen,** um den Datensatz auszuwählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die Beispielnutzlast dieses bestimmten Webhook-Auslösers an. Basierend auf der ausgewählten Tabelle werden die Datensätze aus der angegebenen Tabelle in der Dropdown-Liste **„Datensatz auswählen“** gefüllt. Wählen Sie den Datensatz aus, um die Beispielnutzlast anzuzeigen. Die Beispielnutzlast wird im JSON-Format angezeigt. Die Felder in der Nutzlast sind unten aufgeführt.

7. Wählen Sie den Typ des Datensatzes aus der Dropdown-Liste aus.
   Die Nutzlast wird basierend auf dem ausgewählten Datensatz automatisch geändert.


```
{
   "record": "Observable",
   "record_fields": {
      "additional_context": "This could be a potential malicious IP. ",
      "attack_phases": "Lockheed Martin: Command and Control",
      "author": "Anomali",
      "confidence": "50",
      "description": "This could be a potential malicious IP. ",
      "expiration_time": "2024-12-01T00:00:00.000Z",
      "first_observed": "2024-01-01T00:00:00.000Z",
      "first_seen": "2024-01-01T00:00:00.000Z",
      "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
      "is_defanged": "false",
      "is_false_positive": "false",
      "last_observed": "2024-01-01T00:00:00.000Z",
      "last_seen": "2024-01-01T00:00:00.000Z",
      "reputation": "suspicious",
      "source_count": "1",
      "status": "active",
      "sys_created_by": "SecCommon.System",
      "sys_created_on": "2024-06-04T00:00:00.000Z",
      "sys_id": "30526b0a436a02102164e0ea78b8f210",
      "sys_updated_by": "system",
      "sys_updated_on": "2024-06-15T00:00:00.000Z",
      "tags": "critical",
      "taxonomies": "MITRE: T121",
      "threat_level": "medium",
      "threat_score": "24",
      "threat_severity": "medium",
      "tlp": "CLEAR",
      "type": "ip_v4_address",
      "usage_categories": "APT",
      "value": "116.98.170.70"
   },
   "trigger": {
      "name": "Observable Update",
      "type": "UPDATE",
      "trigger_time": "2024-07-26T07:27:29.000Z",
      "trigger_fields": [
         {
            "field_name": "confidence",
            "previous_value": "30",
            "current_value": "50"
         }
      ]
   }
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der Parameter in der Auslösernutzlast

Parameter in der Nutzlast des Auslösers	Typ	Beschreibung
record	Zeichenfolge	Gibt den Datensatztyp an, z. B. erkennbares Element oder Indikator.
record_fields	Objekt	Gibt den Snapshot der Datensatzfelder an, wenn das Ereignis generiert wird. Eine Liste der unterstützten Felder finden Sie in der Tabelle im folgenden Abschnitt.
Auslöser	Objekt	Gibt die übereinstimmenden Auslöserinformationen an.
trigger.name	Zeichenfolge	Gibt den Namen des Auslösers an
trigger.type	Zeichenfolge	Gibt den Typ des Auslösers an. Gültige Werte sind CREATE, UPDATE, DELETE.
trigger.trigger_time	Datum (im ISO-Format mit UTC-Zeitzone)	Gibt die Zeit an, zu der das Ereignis im Datensatz aufgetreten ist.
trigger_fields	Array von Objekten	Dies ist nur für den Auslösertyp UPDATE verfügbar. Gibt die Liste der Auslöserfelder an, die im Rahmen des aufgetretenen Ereignisses geändert wurden. Die Parameter in **trigger_fields** sind: ○ **field_name**: gibt den Feldnamen an, der geändert wurde ○ **previous_value**: liefert den vorherigen Wert des Felds ○ **current_value**: liefert den aktuellen Wert des Felds

Liste der unterstützten Felder für Erstellungs- und Aktualisierungsauslöser

Tabelle	Spaltenname	Spaltenbezeichnung
Kampagne	Aliasse	Aliase
Kampagne	description	Beschreibung
Kampagne	first_seen	Erstmals aufgetreten
Kampagne	last_seen	Zuletzt aufgetreten
Kampagne	name	Name
Kampagne	Ziel	Ziel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Spaltenname	Spaltenbezeichnung
Indikator	additional_context	Zusätzlicher Kontext
Indikator	„attach_phases“	Angriffsphasen
Indikator	Autor	Autor
Indikator	confidence	Vertrauen
Indikator	description	Beschreibung
Indikator	Ablaufzeit	Ablaufzeit
Indikator	first_detected	Zuerst erkannt
Indikator	first_observed	Zuerst beobachtet
Indikator	first_seen	Erstmals aufgetreten
Indikator	id	ID
Indikator	indicator_types	Indikatortypen
Indikator	ioc_classification	IoC-Klassifizierung
Indikator	last_observed	Zuletzt beobachtet
Indikator	last_seen	Zuletzt aufgetreten
Indikator	name	Name
Indikator	pattern	Muster
Indikator	Pattern_Type	Mustertyp
Indikator	Pattern_Version	Musterversion
Indikator	Plattformen	Plattformen
Indikator	widerrufen	Widerrufen
Indikator	source_count	Anzahl der Quellen
Indikator	spec_version	Spezifikationsversion
Indikator	status	Status
Indikator	tags	TISC-Tags
Indikator	Taxonomien	Taxonomien
Indikator	Threat_level	Bedrohungsstufe
Indikator	Threat_severity	Bedrohungsschweregrad
Indikator	tLP	TLP
Indikator	„usage_categories“	Nutzungskategorien
Indikator	valid_from	Gültig ab
Indikator	valid_until	Gültig bis
Malware	Aliasse	Aliase
Malware	„attach_phases“	Angriffsphasen
Malware	description	Beschreibung
Malware	executable_process_architectures	Prozessarchitekturen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Spaltenname	Spaltenbezeichnung
Malware	first_seen	Erstmals aufgetreten
Malware	Implementation_languages	Implementierungssprachen
Malware	is_family	Ist Familie
Malware	last_seen	Zuletzt aufgetreten
Malware	Malware_capabilities	Malware-Fähigkeiten
Malware	Malware_types	Schadsoftwaretypen
Malware	name	Name
Objekt (gemeinsame Objektfelder)	additional_context	Zusätzlicher Kontext
Objekt (gemeinsame Objektfelder)	confidence	Vertrauen
Objekt (gemeinsame Objektfelder)	Ablaufzeit	Ablaufzeit
Objekt (gemeinsame Objektfelder)	id	ID
Objekt (gemeinsame Objektfelder)	widerrufen	Widerrufen
Objekt (gemeinsame Objektfelder)	source_count	Anzahl der Quellen
Objekt (gemeinsame Objektfelder)	spec_version	Spezifikationsversion
Objekt (gemeinsame Objektfelder)	status	Status
Objekt (gemeinsame Objektfelder)	tags	TISC-Tags
Objekt (gemeinsame Objektfelder)	Taxonomien	Taxonomien
Objekt (gemeinsame Objektfelder)	Threat_level	Bedrohungsstufe
Objekt (gemeinsame Objektfelder)	Threat_severity	Bedrohungsschweregrad
Objekt (gemeinsame Objektfelder)	tLP	TLP
Erkennbares Element	additional_context	Zusätzlicher Kontext
Erkennbares Element	„attach_phases“	Angriffsphasen
Erkennbares Element	Autor	Autor
Erkennbares Element	confidence	Vertrauen
Erkennbares Element	description	Beschreibung
Erkennbares Element	Ablaufzeit	Ablaufzeit
Erkennbares Element	first_observed	Zuerst beobachtet
Erkennbares Element	first_seen	Erstmals aufgetreten
Erkennbares Element	id	ID
Erkennbares Element	is_defanged	Ist entsperrt
Erkennbares Element	is_false_positive	Ist falsch positiv
Erkennbares Element	last_observed	Zuletzt beobachtet
Erkennbares Element	last_seen	Zuletzt aufgetreten
Erkennbares Element	Ruf	Reputation
Erkennbares Element	source_count	Anzahl der Quellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Spaltenname	Spaltenbezeichnung
Erkennbares Element	status	Status
Erkennbares Element	tags	TISC-Tags
Erkennbares Element	Taxonomien	Taxonomien
Erkennbares Element	Threat_level	Bedrohungsstufe
Erkennbares Element	Threat_score	Bedrohungsbewertung
Erkennbares Element	Threat_severity	Bedrohungsschweregrad
Erkennbares Element	tLP	TLP
Erkennbares Element	Typ	Typ
Erkennbares Element	„usage_categories“	Nutzungskategorien
Erkennbares Element	Wert	Wert
Bedrohungsakteur	Aliasse	Aliase
Bedrohungsakteur	description	Beschreibung
Bedrohungsakteur	first_seen	Erstmals aufgetreten
Bedrohungsakteur	goals	Ziele
Bedrohungsakteur	last_seen	Zuletzt aufgetreten
Bedrohungsakteur	name	Name
Bedrohungsakteur	personal_motivations	Persönliche Motivationen
Bedrohungsakteur	primary_motivation	Primäre Motivation
Bedrohungsakteur	resource_level	Ressourcenebene
Bedrohungsakteur	sekundäre_Motivationen	Sekundäre Motivationen
Bedrohungsakteur	Ausgereiftheit	Ausgereiftheit
Bedrohungsakteur	Threat_actor_roles	Bedrohungsakteurrollen
Bedrohungsakteur	Threat_actor_types	Bedrohungsakteurtypen
Bedrohungsbericht	description	Beschreibung
Bedrohungsbericht	name	Name
Bedrohungsbericht	Veröffentlicht	Veröffentlicht
Bedrohungsbericht	report_types	Berichtstypen
Schwachstelle	impacted_software	Betroffene Software
Schwachstelle	description	Beschreibung
Schwachstelle	Exploitation_status	Nutzungsstatus
Schwachstelle	Exploit_existiert	Exploit vorhanden
Schwachstelle	name	Name
Schwachstelle	Veröffentlicht	Veröffentlicht
Schwachstelle	record_last_modified	Datensatz zuletzt geändert
Schwachstelle	Schweregrad	Schweregrad

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachfolgend finden Sie die Liste der anwendbaren Systemfelder, die für jede Entität gelten und in der Webhook-Auslösernutzlast für die Auslöser „Erstellen“ und „Aktualisieren“ unterstützt werden.

- sys_id (Sys-ID)
- sys_created_on (Erstellt)
- sys_created_by (Erstellt von)
- sys_updated_on (Aktualisiert)
- sys_updated_by (Aktualisiert von)

Hinweis:
Beim Löschen wird nur sys_id (Sys-ID) als Teil der Nutzlast an die Webhook-Endpunkt-URL gesendet, und andere Systemfelder werden nicht unterstützt.

Liste der unterstützten Felder für Löschauslöser

Tabelle	Spaltenname	Spaltenbezeichnung
Erkennbares Element	Typ	Typ
Erkennbares Element	Wert	Wert
Indikator	name	Name
Indikator	pattern	Muster
Indikator	Pattern_Type	Mustertyp
Indikator	valid_from	Gültig ab
Kampagne	name	Name
Malware	is_family	Ist Familie
Malware	name	Name
Bedrohungsakteur	name	Name
Bedrohungsbericht	name	Name
Bedrohungsbericht	Veröffentlicht	Veröffentlicht
Schwachstelle	name	Name
Schwachstelle	Schweregrad	Schweregrad

Arbeiten mit automatisierten Flows

Verwenden Sie diese definierten Schritte, um zu erfahren, wie Sie die automatisierten Flows in TISC und ihre Fähigkeiten verwenden können.

Erstellen Sie Flows, die mit TISC-Rollen ausgeführt werden. In TISC werden Flows für Folgendes erstellt:

- Automatisierte IoC-Ergänzung
- Analysieren, bewerten und verbreiten Sie IoCs im Zusammenhang mit Bedrohungen
- Analysieren, bewerten Sie die mit der Bedrohung verbundenen IoCs, und erstellen Sie einen Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unterstützung für Schwachstellenmanagement.
- Zero-Day-Schwachstellen-Nachverfolgung.

Hinweis:
Alle Flows sind Vorlagen, die im Entwurfsstatus geliefert werden, damit die Anwender sie entsprechend ihren eigenen Anforderungen anpassen oder kopieren können.

Wiederverwendbare Aktionen

Flow-Aktion	Beschreibung
Tag zu Entität hinzufügen	Tag wird einer Entität hinzugefügt, die dies unterstützt (erkennbares Element/Indikator/Objekt).
Tag aus Entität entfernen	Tag wird zu einer Entität entfernt, die es unterstützt (erkennbares Element/Indikator/Objekt).
Überprüfen, ob die IP-Adresse im CIDR-Bereich vorhanden ist	Es wird überprüft, ob sich eine IP-Adresse innerhalb eines CIDR-Bereichs befindet.
Überprüfen, ob die IP-Adresse im Bereich vorhanden ist	Es wird überprüft, ob eine IP-Adresse zwischen dem Ausgangsbereich und dem Zielbereich liegt.

Automatisierte IoC-Ergänzung

Erfahren Sie, wie Sie die Anreicherung von IoCs mithilfe von Flows automatisieren, wenn sie ein bestimmtes Kriterium erfüllen.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Automatisieren Sie die Anreicherung von IoC-Auslösern nur dann, wenn:

- Der Typ des erkennbaren Elements ist ein Domänenname, eine IPv4-Adresse oder eine IPv6-Adresse.
- Das erkennbare Element befindet sich im Status „Verarbeitet“.
- Das erkennbare Element enthält nicht die Tags angereichert oder Ergänzung überspringen.

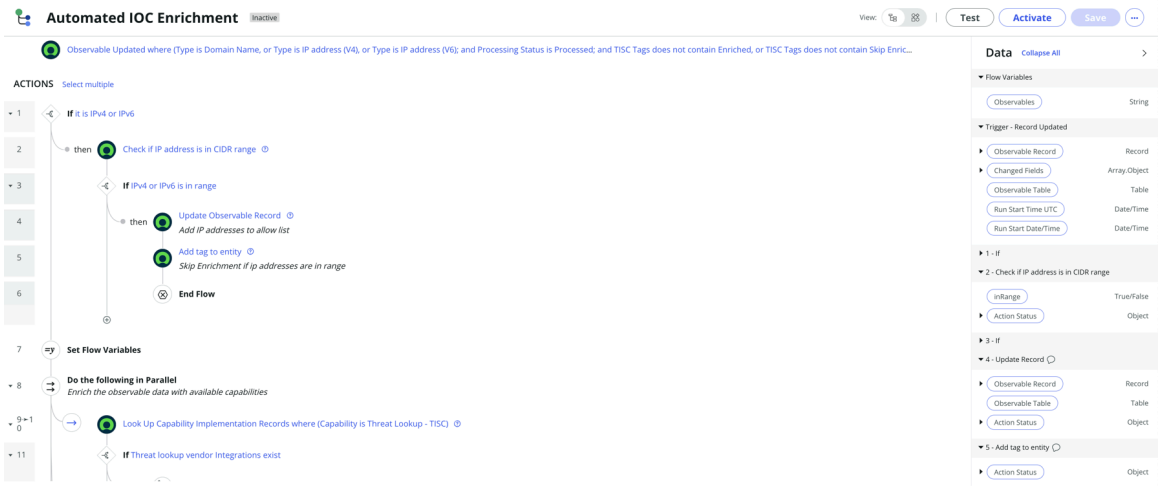
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Automatisierte Flows**.
3. Wählen Sie den Link Aktion **„Automatisierte IoC-Ergänzung“** aus, um die entsprechenden Regeldetails im Flow Designer anzuzeigen.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

```
Observable Updated where (Type is Domain Name, or Type is IP address (V4), or Type is IP address (V6); and Processing Status is Processed; and TISC Tags does not contain Enriched, or TISC Tags does not contain Skip Enrichment, or TISC Tags does not contain Potential New Threat)
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wenn das erkennbare Element eine IPv4- oder IPv6-Adresse ist und innerhalb eines zulässigen CIDR-Bereichs liegt, gilt:**
   a. Fügen Sie das erkennbare Element der Allow-Liste hinzu.
   b. Aktualisieren Sie die Tags der erkennbaren Elemente auf Ergänzung überspringen.
   c. Beenden Sie den Flow für dieses erkennbare Element.
6. **Andernfalls können Sie die Daten des erkennbaren Elements mit verfügbaren Funktionen ergänzen:**
   a. Führen Sie eine Bedrohungs- und Sichtungssuche durch, um zusätzliche Informationen zum erkennbaren Element zu sammeln.
   b. Erkennbares Element mit angereicherten Daten aktualisieren
   c. Fügen Sie ein Tag **„Ergänzt“** hinzu, um anzugeben, dass die IoC verarbeitet wurde.
7. **Wenn erkennbare Elemente sauber sind, gilt Folgendes:**
   a. Erkennbares Element als falsch positiv und inaktiv markieren.
8. **Andernfalls, wenn die Reputation des erkennbaren Elements unbekannt ist**
   a. Fügen Sie die Tags **„Nicht potenzielle Bedrohung“ und „Ergänzt“** hinzu, um anzugeben, dass es sich nicht um eine Bedrohung handelt.



Analysieren, bewerten und verbreiten Sie erkennbare Elemente

Erfahren Sie, wie erkennbare Elemente im Zusammenhang mit Bedrohungen analysiert und verbreitet werden.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Ergänzung der Sichtungssuche angefordert wird, werden keine Sichtungen zurückgegeben.

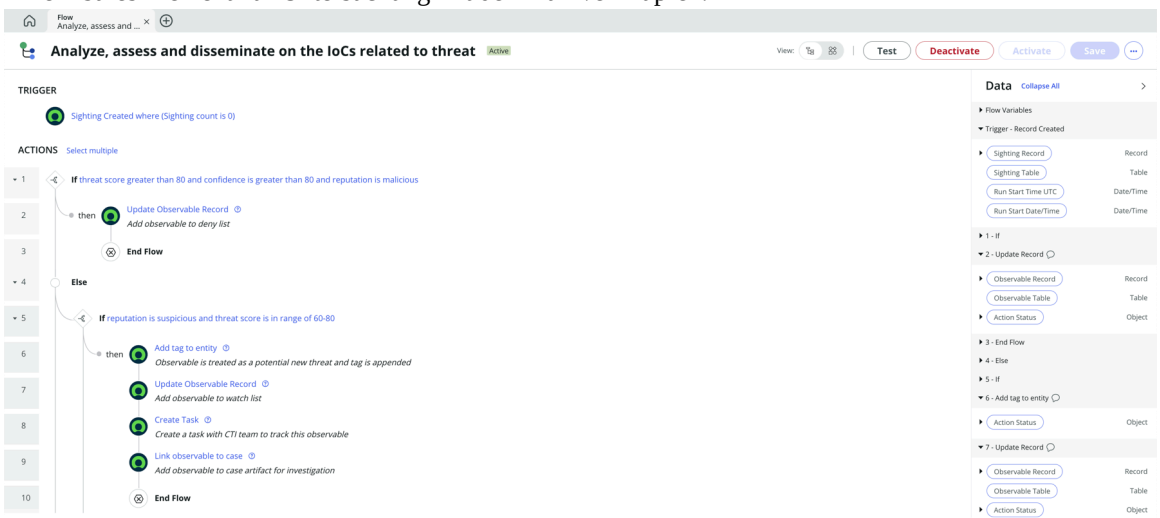
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Automatisierte Flows**.
3. Wählen Sie **unter „IoCs im Zusammenhang mit Bedrohungsaktionen“ die Option Analysieren, bewerten und verbreiten aus,** um die entsprechenden Regeldetails im Flow Designer anzuzeigen.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   Sighting Created where (Sighting count is 0)

5. **Das erkennbare Element weist eine Bedrohungsbewertung über 80, ein Vertrauen über 80 und einen böswilligen Ruf auf:**
   a. Fügen Sie das erkennbare Element der Deny-Liste hinzu.
   b. Beenden Sie den Flow für dieses erkennbare Element.
6. **Andernfalls ist die Reputation des erkennbaren Elements verdächtig, und die Bedrohungsbewertung liegt im Bereich von 60 bis 80:**
   a. Fügen Sie ein Tag mit der Bezeichnung „Potenzielle neue Bedrohung“ hinzu.
   b. Fügen Sie das erkennbare Element der Beobachtungsliste hinzu.
   c. Erstellen Sie eine Fallaufgabe mit dem CTI-Team, um dieses erkennbare Element nachzuverfolgen und weiter zu analysieren.
   d. Erkennbares Element zur Untersuchung mit dem Fall verknüpfen.



Analysieren und bewerten Sie Bedrohungs-IoCs

Erfahren Sie, wie Sie IoCs analysieren, die eine Bedrohung darstellen und das Security Incident-Team benachrichtigen.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wann immer eine Ergänzung einer Sichtungssuche angefordert wird:

- wenn das erkennbare Element gesehen wurde (Anzahl > 0) und
- Die Reputation des erkennbaren Elements ist böswillig und
- Die Bedrohungspunktzahl des erkennbaren Elements ist > 80 und
- Konfidenz erkennbarer Elemente > 80

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Automatisierte Flows**.
3. Wählen Sie **Analysieren, bewerten Sie die mit der Bedrohung verbundenen IoCs, und erstellen Sie den Link Incident-** Aktion, um die entsprechenden Regeldetails im Flow Designer anzuzeigen.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

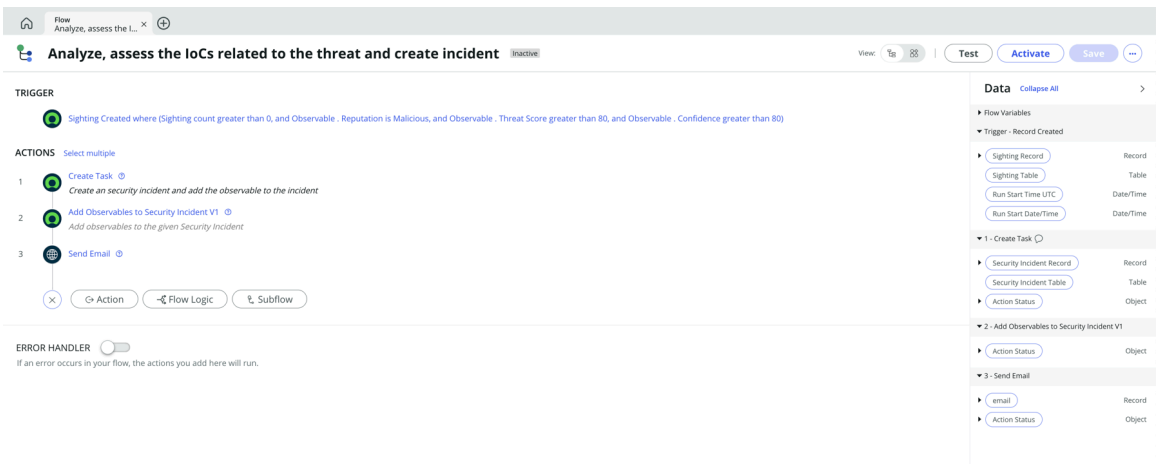
   Sighting Created where (Sighting count greater than 0, and Observable. Reputation is Malicious, and Observable. Threat Score greater than 80, and Observable. Confidence greater than 80)

5. **Wenn Sichtung erstellt wurde (Sichtungsanzahl größer als 0 und erkennbares Element. Die Reputation ist böswillig und erkennbar. Bedrohungsbewertung größer als 80 und erkennbares Element. Konfidenz höher als 80), dann:**

   a. Erstellen Sie einen Security Incident, und fügen Sie das erkennbare Element zum Incident hinzu.

   b. Erkennbare Elemente zu Security Incident hinzufügen V1.

   c. Senden Sie eine E-Mail-Kommunikation.



Unterstützung für Schwachstellenmanagement

Erfahren Sie, wie eine neue Schwachstelle in TISC mit einer zugehörigen Schwachstelle in VR erstellt wird.

Vorbereitungen

Erforderliche Rolle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Wenn in TISC eine neue Schwachstelle erstellt wird und in VR eine zugehörige Schwachstelle vorhanden ist.

- Wenn die Punktzahl für VR-Schwachstelle(v2) > 8 ODER die Punktzahl für VR-Schwachstelle(v3) > 8 ist.
- Gesamtzahl der ihr zugeordneten VIs ist größer als 0.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Automatisierte Flows**.
3. Wählen Sie den Aktionslink **Support für Schwachstellenmanagement,** um die entsprechenden Regeldetails im Flow Designer anzuzeigen.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   When new vulnerability is created in TISC and there is a related vulnerability in VR.

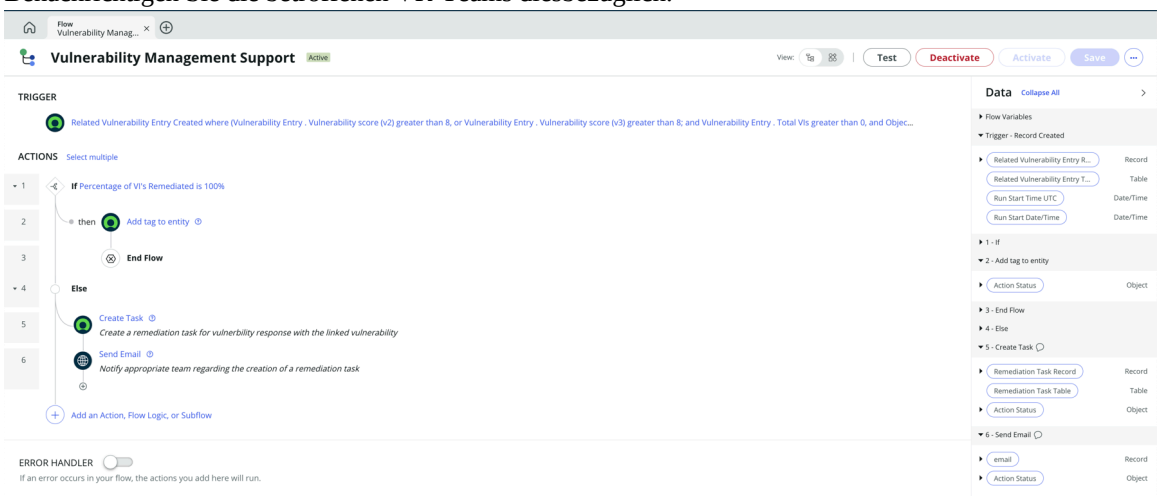
5. **Wenn der Prozentsatz der insgesamt korrigierten AEs, die dieser Schwachstelle zugeordnet sind, 100 % beträgt, gilt:**

   a. Fügen Sie dem erkennbaren Element ein Tag mit der Bezeichnung „Nachgebessert“ hinzu.

6. **Andernfalls können Sie die Daten des erkennbaren Elements mit verfügbaren Funktionen ergänzen:**

   a. Erstellen Sie eine Korrekturaufgabe für VR.

   b. Benachrichtigen Sie die betroffenen VR-Teams diesbezüglich.



Zero-Day-Schwachstellen-Nachverfolgung

Erfahren Sie, wie Sie im System eingehende RSS-Feeds analysieren.

Vorbereitungen

Erforderliche Rolle:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Immer wenn ein neuer RSS-Feed im System erstellt wird, in dem „Zero Day“ entweder im Titel oder in der Beschreibung erwähnt wird.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**.
2. Auswahlvorgang **Automatisierte Flows**.
3. Wählen Sie den Link **Zero-Day-Schwachstellennachverfolgung,** um die entsprechenden Regeldetails im Flow Designer anzuzeigen.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   RSS Feed Created where (Title contains zero day, or Description contains zero day, or Title contains zero_day, or Description contains zero_day, or Title contains zero-day, or Description contains zero-day)

5. **Wenn das erkennbare Element eine IPv4- oder IPv6-Adresse ist und innerhalb eines zulässigen CIDR-Bereichs liegt, gilt:**
   a. Erstellt einen Fall für das TISC-Team zusammen mit einer Korrekturaufgabe für das VR-Team.
   b. Benachrichtigen Sie die betroffenen TISC-Teams und VR-Teams.

Tabellen für automatisierte Flows

Die folgenden Tabellen helfen Ihnen, die Beziehungstabellen zwischen Entitäten und Ergänzungstabellen zu verstehen, die in automatisierten Flows verwendet werden.

Beziehungstabellen zwischen Entitäten

Tabelle	Entität
Zugehöriges erkennbares Element des Indikators	sn_sec_tisc_m2m_indicator_observable
Zugehöriger Indikator	sn_sec_tisc_m2m_indicator
Zugehöriges erkennbares Element	sn_sec_tisc_m2m_observable
Objekt-Objekt-Beziehung	sn_sec_tisc_m2m_object
Zugehöriges Indikatorobjekt	sn_sec_tisc_m2m_object_indicator
Beziehung von Objekt und erkennbarem Element	sn_sec_tisc_m2m_object_observable

Ergänzungstabelle

Tabelle	Entität
Bedrohungssuche – Ergebnisse	sn_sec_tisc_lookup_result
Sichtungen	sn_sec_tisc_sighting
Ergänzung eines erkennbaren Elements – Ergebnisse	sn_sec_tisc_observable_enrichment_result

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeiten mit Datenimporten

Mit Datenimporten können Sie alle Datensätze anzeigen, die für den Importauftrag verarbeitet werden, und die Importaufträge auflisten, die auf Genehmigungen warten.

Alle Importe werden angezeigt

Verwenden Sie diesen Abschnitt, um alle importierten Datensätze anzuzeigen, die in der Listenansicht für alle Anwender angezeigt werden.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**.
2. Auswahlvorgang **Datenimporte** > **Alle Importe**
   Auf dieser Seite werden alle Datensätze angezeigt, die für den Importauftrag verarbeitet werden.
3. Öffnen Sie einen beliebigen Datensatz, um den Status des Importvorgangs anzuzeigen.

Hinweis:
Sie können auch auf **Neuer Import** klicken, um einen neuen Importdatensatz zu erstellen. Nachdem Sie auf diese Schaltfläche geklickt haben, werden Sie von der Anwendung zur Seite **„Import Intelligence“** weitergeleitet. Weitere Informationen zum Erstellen neuer Datensätze finden Sie im Abschnitt Importieren Sie Threat Intelligence, und fahren Sie mit dem jeweiligen Importtyp fort.

Meine Importe werden angezeigt

Verwenden Sie diesen Abschnitt, um die Importdatensätze anzuzeigen, die vom angemeldeten Benutzer erstellt wurden.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**.
2. Auswahlvorgang **Datenimporte** > **Meine Importe**
   Auf dieser Seite werden alle Datensätze angezeigt, die diese Datensätze importieren und die für die weitere Verarbeitung für den Importauftrag kategorisiert sind.
3. Öffnen Sie einen beliebigen Datensatz, um den Status des Importvorgangs anzuzeigen.

Hinweis:
Sie können auch auf **Neuer Import** klicken, um einen neuen Importdatensatz zu erstellen. Nachdem Sie auf diese Schaltfläche geklickt haben, werden Sie von der Anwendung zur Seite **„Import Intelligence“** weitergeleitet. Weitere Informationen zum Erstellen neuer Datensätze finden Sie im Abschnitt Importieren Sie Threat Intelligence, und fahren Sie mit dem jeweiligen Importtyp fort.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Zeigen Sie die Zusammenfassung der importierten Datensätze an.

Hinweis:
Falls einer der Importaufträge nicht übermittelt wird, können Sie die Datensätze zur weiteren Verarbeitung und zur Genehmigung **senden**. Wenn für diesen bestimmten Importauftrag keine Genehmigung erforderlich ist, werden diese Datensätze automatisch verarbeitet.

Meine Genehmigungen werden angezeigt

Verwenden Sie diesen Abschnitt, um die Datensätze des Importauftrags zu überprüfen und zu genehmigen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**.
2. Auswahlvorgang **Datenimporte** > **Meine Genehmigungen**
   Auf dieser Seite werden alle Importdatensätze angezeigt, die auf die Genehmigung durch den angemeldeten Anwender warten.
3. Öffnen Sie einen beliebigen Datensatz, um den Importdatensatz zu genehmigen oder abzulehnen.
4. Klicken Sie auf **Genehmigen**, um den Datensatz des Importauftrags zu genehmigen.
   Das Dialogfeld **„Import genehmigen“** wird angezeigt, und es wird eine Bestätigungsmeldung angezeigt, ob die ausgewählten Importe genehmigt werden sollen.

Hinweis:
Eine E-Mail-Benachrichtigung wird an die entsprechenden Anwender gesendet, dass der Importauftrag, der in Bearbeitung war, jetzt genehmigt ist. Weitere Informationen zum Genehmigen von Regeln finden Sie unter Genehmigungsregeln für Datenimporte definieren.

5. Wählen Sie im Dialogfeld **Genehmigen** aus.
   Eine E-Mail-Benachrichtigung wird an den Benutzer gesendet, der den Importauftrag erstellt hat, und der Importauftrag, der in Bearbeitung war, wird jetzt genehmigt.
6. Klicken Sie auf **Ablehnen**, um einen Datensatz abzulehnen.

Hinweis:
- Sie können den abgelehnten Importauftrag überprüfen und erneut übermitteln. Denken Sie daran, Anmerkungen zur Ablehnung hinzuzufügen.
- Eine E-Mail-Benachrichtigung wird an den Benutzer gesendet, der den Importauftrag erstellt hat, wenn der in Bearbeitung befindliche Importauftrag abgelehnt wird.
- Eine E-Mail-Benachrichtigung wird an die Genehmiger gesendet, in denen die Genehmigung angefordert wird.

Importieren Sie Threat Intelligence

Verwenden Sie diese Funktion, um die Threat Intelligence-Daten manuell zum Repository hinzuzufügen oder zu importieren.

Die folgenden Importformate werden im Intelligenzdaten-Importprozess unterstützt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aus strukturierter Datei importieren
2. Import aus Standardformat
3. Import aus Rohtext
4. Aus Datei (unstrukturiert) importieren

Importieren Sie Daten mithilfe einer strukturierten Datei

Laden Sie die strukturierten Daten in den unterstützten Dateiformaten wie CSV, XLSX oder XLS hoch.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie auf **Intelligenz importieren**.
3. Klicken Sie auf **Aus strukturierter Dateikarte importieren**.

> **Wichtig:**
> Beim Importieren von Threat Intelligence-Daten in unterstützten Dateiformaten wie TXT, CSV, STIX 2.x JSON, MISP JSON oder strukturierte Datei ist die Dateigröße auf 5 MB beschränkt. Die Zeichenbeschränkung für Rohtext ist auf 10.000 beschränkt.

4. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Option wählen	Wählen Sie die erforderliche Option aus der Dropdown-Liste aus, z. B. Erkennbare Elemente oder Indikatoren. ○ **Erkennbare Elemente**: Wählen Sie die zu importierenden Daten erkennbarer Elemente aus. **Hinweis:** Wählen Sie diese Option aus, wenn Sie Daten von erkennbaren Elementen importieren. Ändern Sie auch nicht die Spalten-Header in der Datei. „Wert“ und „Typ“ sind Pflichtfelder, die anderen Felder sind optional. Geben Sie außerdem Datum/Uhrzeit im Format JJJJ-MM-DDThh:mm:ssZ ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Indikatoren**: Wählen Sie die zu importierenden Indikatordaten aus. **Hinweis:** Wählen Sie diese Option aus, wenn Sie Indikatordaten importieren. Ändern Sie auch nicht die Spalten-Header in der Datei. „Muster“, „Mustertyp“ und „Gültig ab“ sind Pflichtfelder für Indikatoren. Die Felder „Gültig ab“ sind optional. Geben Sie außerdem Datum/Uhrzeit im Format JJJJ-MM-DDThh:mm:ssZ ein.
Beispieldatei für Indikatoren in der Vorschau anzeigen und herunterladen	Verwenden Sie diesen Link, um die Beispieldatei über den Vorschaulink herunterzuladen und die strukturierten Daten in einem kompatiblen Dateiformat wie CSV, XLS oder XLSX hochzuladen. **Hinweis:** Die Spaltenheader müssen genau mit den Headern übereinstimmen. Die Felder „Wert“ und „Typ“ sind für jedes erkennbare Element in der Datei erforderlich. Die verbleibenden Felder sind optional, wobei „Zuerst gesehen“ und „Zuletzt gesehen“ in Zahlen angegeben werden müssen und die Epochenzeit in Millisekunden angegeben ist.
Datei hochladen	Klicken Sie auf diesen Link, um die Dateidaten im empfohlenen Strukturdateiformat hochzuladen. **Hinweis:** Sie können jeweils nur eine Datei hochladen. Um eine neue Datei hinzuzufügen, müssen Sie die vorhandene entfernen und eine neue Datei hinzufügen.
Legen Sie Definitionen fest	
TLP	Wählen Sie in der Dropdown-Liste den Indikator Traffic Light Protocol (TLP) aus, der auf die importierten Datensätze angewendet werden soll. TLP ist in TISC mit verschiedenen Farben gekennzeichnet, um sicherzustellen, dass die vertraulichen Daten für die vorgesehenen Anwender freigegeben werden. ○ CLEAR: Informationen können ohne Einschränkung geteilt werden. ○ ROT ○ GELB+STRIKT

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ GELB ○ GRÜN
Konfidenz (0-100)	Legen Sie den Konfidenzwert für die importierten Datensätze zwischen 0 und 100 fest.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für die importierten Datensätze ein. **Hinweis:** Das ist ein Pflichtfeld.
Tags	
Tags hinzufügen	Verwenden Sie die Tags, um Datensätze, die aus dieser Quelle im System erfasst wurden, mit Anmerkungen zu versehen oder mit Tags zu versehen. Beginnen Sie mit der Eingabe des Tag-Namens in der **Suchleiste**, um die verfügbaren Tags im System auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf **Hinzufügen**, um ihn der Quelle zuzuweisen.
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Bedrohungsinformationsdatensätzen zugewiesen werden. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien werden erstellt. **Hinweis:** Die Optionen für den Taxonomiewert ändern sich je nach ausgewählter Taxonomie.
Quellwert überschreiben	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Quellwerte für TLP, Konfidenz, Ablauf, Tags und Taxonomien mit den konfigurierten Werten überschreiben möchten. Wenn Sie dieses Kontrollkästchen nicht aktivieren, werden die konfigurierten Werte angewendet, sofern sie nicht leer sind.

5. Klicken Sie auf **Next (Weiter)**.
6. Überprüfen Sie die Daten, bevor Sie sie zur Verarbeitung senden.

Hinweis:
Die Überprüfung von importierten Datensätzen wird für die STIX-Option nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie **auf Weiter**geklickt haben, sehen Sie die Zusammenfassung aller Informationen, die der Anwender im obigen Abschnitt angegeben hat. Der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

Der Benutzer kann jede Art von Aktivität ausführen, und mehrere Benutzer können über den Kommentarbereich, der im rechten Kontextmenü verfügbar ist, zusammenarbeiten. Die Liste der importierten Datensätze wird gerendert, sobald die gesamte Datei oder der Rohtext verarbeitet wurde. Die Importverarbeitung für große Dateien dauert länger. Während der Verarbeitung können Sie den Status überprüfen, überprüfen und auch über die Importdatensatzseite übermitteln.

Hinweis:
Datensätze, die die Validierungen nicht bestehen, werden beim Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und absenden“ zur weiteren Verarbeitung angezeigt.

7. Klicken Sie auf **Updatetyp**, und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
8. Klicken Sie auf **Löschen,** um einen beliebigen Typ der importierten Datensätze zu löschen.
9. Klicken Sie auf **Absenden**.

Hinweis:
Nachdem Sie den Importdatensatz gesendet haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht benötigt, durchläuft der Datensatz den automatischen Genehmigungsprozess, und der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

10. Klicken Sie auf **Status anzeigen**, um den Status des Importdatensatzes anzuzeigen, oder klicken Sie auf **Fertig**.
    Der Datensatz zeigt den Status „Verarbeitet“ an, sobald die Daten zur Verarbeitung importiert wurden.
11. Klicken Sie auf **Abbrechen**, um den Importvorgang abzubrechen.
12. Klicken Sie auf **Zurück**, um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

Importieren Sie Daten im Standardformat

Laden Sie die Standarddaten in den unterstützten Dateiformaten wie STIX 2.x JSON, MISP JSON hoch.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie auf **Intelligenz importieren**.
3. Klicken Sie auf **Aus Standarddateikarte importieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Beim Importieren von Threat Intelligence-Daten in unterstützten Dateiformaten wie TXT, CSV, STIX 2.x JSON, MISP JSON oder strukturierte Datei ist die Dateigröße auf 5 MB beschränkt. Die Zeichenbeschränkung für Rohtext ist auf 10.000 beschränkt.

4. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Dateiformat	Wählen Sie die erforderliche Option aus der Dropdown-Liste aus, z. B. STIX 2.x JSON oder MISP JSON. ○ **STIX 2.x JSON**: Wählen Sie das zu importierende Format in STIX 2.x JSON aus. ○ **MISP JSON**: Wählen Sie das zu importierende Format im MISP-JSON-Format aus.
Datei hochladen	Klicken Sie auf diesen Link, um die Daten im Standarddateiformat hochzuladen.
Legen Sie Definitionen fest	
TLP	Wählen Sie den TLP-Indikator aus der Dropdown-Liste aus, der für die importierten Datensätze angewendet werden soll.
Konfidenz (0-100)	Definieren Sie den Konfidenzwert.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für die importierten Datensätze ein. **Hinweis:** Das ist ein Pflichtfeld.
Tags hinzufügen	Verwenden Sie die Tags, um Datensätze, die aus dieser Quelle im System erfasst wurden, mit Anmerkungen zu versehen oder mit Tags zu versehen. Beginnen Sie mit der Eingabe des Tag-Namens in der Suchleiste, um die verfügbaren Tags im System auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf Hinzufügen, um ihn der Quelle zuzuweisen.
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Bedrohungsinformationsdatensätzen zugewiesen werden. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien werden erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wählen Sie Taxonomiewerte aus	Gibt die Taxonomiewerte an, die der Taxonomie zugeordnet sind.
Quellwert überschreiben	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Quellwerte für TLP, Konfidenz, Ablauf, Tags und Taxonomien von den konfigurierten Werten überschreiben möchten. Wenn Sie dieses Kontrollkästchen nicht aktivieren, werden die Standardwerte angewendet.

5. Klicken Sie auf **Next (Weiter)**.
6. Überprüfen Sie die Daten, bevor Sie sie zur Verarbeitung senden.

Hinweis:
Die Überprüfung von importierten Datensätzen wird für die STIX-Option nicht unterstützt.

Nachdem Sie **auf Weiter**geklickt haben, sehen Sie die Zusammenfassung aller Informationen, die der Anwender im obigen Abschnitt angegeben hat. Der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

Der Benutzer kann jede Art von Aktivität ausführen, und mehrere Benutzer können über den Kommentarbereich, der im rechten Kontextmenü verfügbar ist, zusammenarbeiten.

Hinweis:
Datensätze, die die Validierungen nicht bestehen, werden beim Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und absenden“ zur weiteren Verarbeitung angezeigt.

7. Klicken Sie auf **Updatetyp**, und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
8. Klicken Sie auf **Löschen,** um einen beliebigen Typ der importierten Datensätze zu löschen.
9. Klicken Sie auf **Absenden**.

Hinweis:

Nachdem Sie den Importdatensatz gesendet haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht benötigt, durchläuft der Datensatz den automatischen Genehmigungsprozess, und der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

10. Klicken Sie auf **Status anzeigen,** um den Status des Datensatzes anzuzeigen, oder klicken Sie auf **Fertig**. Der Datensatz zeigt den Status „Verarbeitet“ an, sobald er verarbeitet wurde.
11. Klicken Sie auf **Abbrechen**, um den Importvorgang abzubrechen.
12. Klicken Sie auf **Zurück**, um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

Importieren Sie Daten mit Rohtext

Importieren Sie die Daten der erkennbaren Elemente durch Kopieren und Einfügen von Rohtext oder durch Eingabe des Freitexts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie auf **Intelligenz importieren**.

Wichtig:

- Alle entsperrenden Zeichen werden im Rahmen der Analyse und Extraktion von erkennbaren Elementen bereinigt.
- Für diese Option zum Einfügen von Text werden nur URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert. Andere erkennbare Elemente werden nicht für den Datenimport extrahiert. Im Falle von erkennbaren Elementen wie Registrierung oder Verzeichnistypen werden diese Typen erkennbar vom Import übersprungen werden.

3. Klicken Sie auf **Aus Rohtextkarte importieren**.

Wichtig:
Beim Importieren der Threat Intelligence-Daten im Rohtextformat sind die Zeichen auf 10.000 beschränkt. Die Rohtextoption kann als Problemumgehung verwendet werden, um die erkennbaren Elemente aus der PDF-Datei zu extrahieren.

4. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Textfeld für Rohdaten	Geben Sie den Rohtext hier in dieses Textfeld ein, oder kopieren Sie ihn und fügen Sie ihn ein. **Hinweis:** Sie können nur Rohtext mit maximal 10.000 Zeichen eingeben oder einfügen.
Legen Sie Definitionen fest	
TLP	Wählen Sie den TLP-Indikator aus der Dropdown-Liste aus, der für die importierten Datensätze angewendet werden soll.
Konfidenz (0-100)	Definieren Sie den Konfidenzwert.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für die importierten Datensätze ein. **Hinweis:** Das ist ein Pflichtfeld.
Tags hinzufügen	Verwenden Sie die Tags, um Datensätze, die aus dieser Quelle im System erfasst wurden, mit Anmerkungen zu versehen oder mit Tags zu versehen. Beginnen Sie mit der Eingabe des Tag-Namens in der Suchleiste, um die verfügbaren Tags

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	im System auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf Hinzufügen, um ihn der Quelle zuzuweisen.
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Bedrohungsinformationsdatensätzen zugewiesen werden. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien werden erstellt.

5. Klicken Sie auf **Next (Weiter)**.
6. Überprüfen Sie die Daten, bevor Sie sie zur Verarbeitung senden.

   Nachdem Sie **auf Weiter**geklickt haben, sehen Sie die Zusammenfassung aller Informationen, die der Anwender im obigen Abschnitt angegeben hat. Der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

   Der Benutzer kann jede Art von Aktivität ausführen, und mehrere Benutzer können über den Kommentarbereich, der im rechten Kontextmenü verfügbar ist, zusammenarbeiten.

   Hinweis:
   Datensätze, die die Validierungen nicht bestehen, werden beim Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und absenden“ zur weiteren Verarbeitung angezeigt.

7. Klicken Sie auf **Updatetyp**, und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
8. Klicken Sie auf **Löschen,** um einen beliebigen Typ der importierten Datensätze zu löschen.
9. Klicken Sie auf **Absenden**.

   Hinweis:
   Nachdem Sie den Importdatensatz gesendet haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht benötigt, durchläuft der Datensatz den automatischen Genehmigungsprozess, und der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

10. Klicken Sie auf **Status anzeigen,** um den Status des Datensatzes anzuzeigen, oder klicken Sie auf **Fertig**. Der Datensatz zeigt den Status „Verarbeitet“ an, sobald er verarbeitet wurde.
11. Klicken Sie auf **Abbrechen**, um den Importvorgang abzubrechen.
12. Klicken Sie auf **Zurück**, um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie Daten im unstrukturierten Dateiformat

Laden Sie die Daten in einem unstrukturierten Format hoch, das von Dateiformaten wie TXT, CSV, JSON, XLS und XLSX unterstützt wird.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie auf **Intelligenz importieren**.

Wichtig:

- Alle entsperrenden Zeichen werden im Rahmen der Analyse und Extraktion von erkennbaren Elementen bereinigt.
- Für diese unstrukturierte Dateiformatoption werden nur URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert. Andere erkennbare Elemente werden nicht für den Datenimport extrahiert. Im Falle eines solchen erkennbaren Elementtyps wie Registrierung, Verzeichnistypen usw wird beim Importieren von übersprungen.

3. Klicken Sie auf **Aus Datei importieren (unstrukturiert)** Karte.

Hinweis:
Beim Importieren von Threat Intelligence-Daten in unterstützten Dateiformaten wie TXT, CSV, STIX 2.x JSON, MISP JSON oder strukturierte Datei ist die Dateigröße auf 5 MB beschränkt.

4. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Datei hochladen	Klicken Sie auf diesen Link, um die Daten im Standarddateiformat hochzuladen.
Legen Sie Definitionen fest	
TLP	Wählen Sie den TLP-Indikator aus der Dropdown-Liste aus, der für die importierten Datensätze angewendet werden soll.
Konfidenz (0-100)	Definieren Sie den Konfidenzwert.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum der zugeordneten erkennbaren Elemente ein. **Hinweis:** Das ist ein Pflichtfeld.
Tags hinzufügen	Verwenden Sie die Tags, um Datensätze, die aus dieser Quelle im System erfasst wurden, mit Anmerkungen zu versehen oder mit Tags zu versehen. Beginnen Sie mit der Eingabe des Tag-Namens in der Suchleiste, um die verfügbaren Tags im System auszuwählen, oder geben Sie einen neuen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Tag-Namen ein, und klicken Sie auf Hinzufügen, um ihn der Quelle zuzuweisen.
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Bedrohungsinformationsdatensätzen zugewiesen werden. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien werden erstellt.

5. Überprüfen Sie die Daten, bevor Sie sie zur Verarbeitung senden.

   Nachdem Sie **auf Weiter**geklickt haben, sehen Sie die Zusammenfassung aller Informationen, die der Anwender im obigen Abschnitt angegeben hat. Der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

   Der Benutzer kann jede Art von Aktivität ausführen, und mehrere Benutzer können über den Kommentarbereich, der im rechten Kontextmenü verfügbar ist, zusammenarbeiten.

   Hinweis:
   Die unterstützten Formate für den Datenimport sind TXT, CSV, JSON und XLS. Datensätze, die die Validierungen nicht bestehen, werden beim Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und absenden“ zur Verarbeitung angezeigt.

6. Klicken Sie auf **Updatetyp**, und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
7. Klicken Sie auf **Löschen,** um einen beliebigen Typ der importierten Datensätze zu löschen.
8. Klicken Sie auf **Absenden**.

   Hinweis:
   Nachdem Sie den Importdatensatz gesendet haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht benötigt, durchläuft der Datensatz den automatischen Genehmigungsprozess, und der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

9. Klicken Sie auf **Status anzeigen,** um den Status des Datensatzes anzuzeigen, oder klicken Sie auf **Fertig**. Der Datensatz zeigt den Status „Verarbeitet“ an, sobald die Übermittlung erfolgreich war.
10. Klicken Sie auf **Abbrechen**, um den Importvorgang abzubrechen.
11. Klicken Sie auf **Zurück**, um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

Analyst Workbench für Bedrohungen

Die Seite „Workbench für Bedrohungsanalysten“ besteht aus Fällen und Fallaufgaben, die sich unter Bedrohungsanalysten und ihrem Team befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die **Fallverwaltungsfunktion**, um die Bedrohungsuntersuchungen und Analyseaktivitäten zu erstellen und nachzuverfolgen.

Während der Bedrohungsuntersuchungen erfassen die Analysten die Daten aus internen Intelligenzdatensätzen wie erkennbaren Elementen, Bedrohungsakteuren, Kampagnen usw.

Workbench – Übersicht

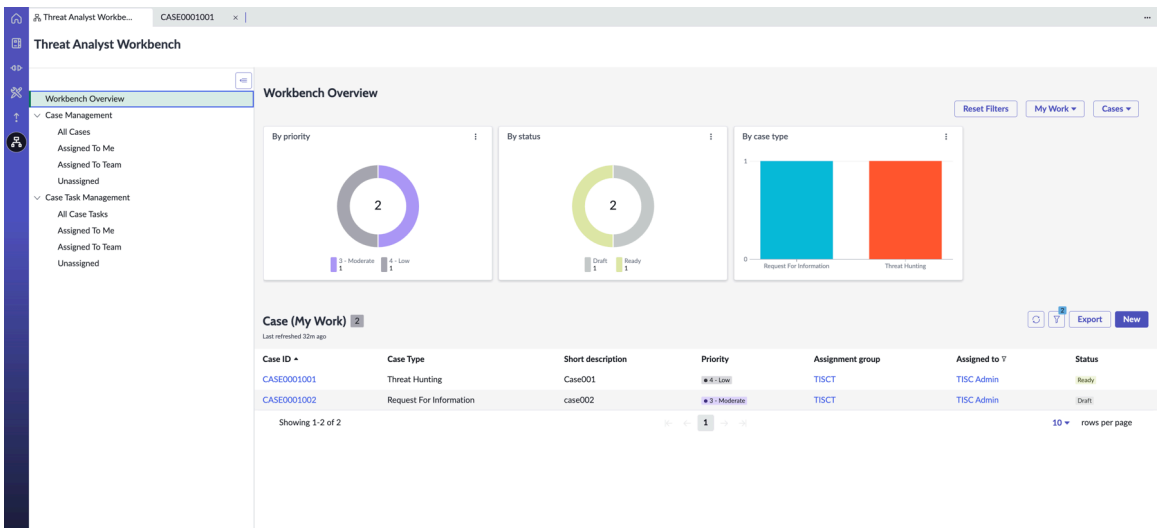
Die Seite „Workbench-Übersicht“ besteht aus den Fallaufgaben und Fällen, die sich unter Bedrohungsanalysten und ihrem Team befinden.

In der Übersicht werden alle offenen Fälle und deren Status aufgelistet. Dies hilft den Analysten, ihre Arbeitsauslastung zu verwalten und ihre Untersuchungen zu priorisieren.

Erforderliche Rolle: sn_sec_tisc.analyst, sn_sec_tisc.admin

Nachdem der Fall erstellt wurde, weisen die Analysten die Fallaufgaben anderen Analysten oder Teams zur weiteren Untersuchung zu und arbeiten auch mit ihnen zusammen, um Informationen und Einblicke auszutauschen.

Unter jedem Filter sind verschiedene Widgets vorhanden, die nach Priorität, Status und Falltyp gruppiert sind und sich in den Warteschlangen der Bedrohungsanalysten und in der Warteschlange des Bedrohungsanalystenteams befinden.



Wenn Filter auf die Widgets angewendet werden, wird die untere Hälfte der Übersichtsseite mit den entsprechenden Fällen oder Fallaufgaben gefüllt, die als Listenelemente dargestellt werden. Klicken Sie auf **„Filter zurücksetzen“**, um die angewendeten Filter zu entfernen und die ursprüngliche Ansicht wiederherzustellen.

Auf dieser Seite können Bedrohungsanalysten und Administratoren ihre Arbeit, die Arbeit von Teams und nicht zugewiesene Arbeit anzeigen. Sie können zur Dropdown-Liste navigieren. Verfügbare Optionen:

- Meine Arbeit: Wählen Sie diese Option, um die Ihnen zugewiesene Arbeit anzuzeigen.
- Arbeit meines Teams: Wählen Sie diese Option, um die Arbeit Ihres Teams anzuzeigen, die allen Gruppen zugewiesen ist, denen Sie angehören.
- Nicht zugewiesene Arbeit: Wählen Sie diese Option aus, um den nicht zugewiesenen Fall oder die Fallaufgabe anzuzeigen. Um den Fall oder die Fallaufgabe zuzuweisen, müssen Sie zur Formularansicht wechseln und den/die Anwender oder die Anwendergruppe(n) dem Fall und den Fallaufgaben zuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Fälle und Fallaufgaben, die Ihnen zugewiesen sind, auch direkt in der Workbench-Übersicht anzeigen. Standardmäßig wird die Fallansicht angezeigt. Sie können die Dropdownliste verwenden und die Fallaufgaben auswählen, wenn Sie die Fallaufgaben nach Priorität und Status anzeigen möchten.

Erstellen von Fällen mit der Workbench für Bedrohungsanalysten

Fälle werden verwendet, um Informationen über eine Kampagne oder einen Bedrohungsakteur nachzuverfolgen, die bzw. der Ihre Organisation bedrohen. Nachdem ein Fall erstellt wurde, können Sie Artefakte hinzufügen, mit denen Sie alle zugehörigen Informationen aus einem einzelnen Fall oder einer Fallaufgabe überprüfen und analysieren können.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst, sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallmanagement** > **Alle Fälle**.
   Alle Fälle werden angezeigt.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder entsprechend aus.

Neuen Fall erstellen

Feld	Beschreibung
Fall-ID	Ein eindeutiger Bezeichner für den Fall. Dies ist die vom System generierte ID.
Kurzbeschreibung	Zusammenfassung der Anforderung oder des Problems, die bzw. das untersucht wird, oder eine Kurzbeschreibung.
Beschreibung	Eine detaillierte Beschreibung mit allen relevanten Informationen zum Fall, z. B. Hintergrund, erforderliche Analyse, erwartete Ergebnisse.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus. Die möglichen Optionen für die Untersuchung sind: ○ Bedrohungssuche ○ Informationsanforderung ○ Schwachstellenmanagement-Fall ○ Compliance-Fall ○ Fall vom Typ „Reaktion auf Incidents“ ○ Zusammenarbeitsfall ○ Andere
Priorität	Eine Bewertung des Schweregrads der Anforderung oder des Problems.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuweisungsgruppe	Die zugewiesene Gruppe, die für die Bearbeitung des Falls verantwortlich ist.
Status	Der aktuelle Status des Falls.
Zugewiesen an	Der für die Bearbeitung eines Falls verantwortliche Analyst
Fälligkeitsdatum	Datum und Uhrzeit, zu der die Aufgabe abgeschlossen oder geschlossen werden soll.
Beitragende	Die Liste der Beauftragten, die aus Aufgaben zusammengefasst wurden und die hinzugefügt werden können.
TLP	Eindeutiger Wert, der die Vertraulichkeitseinstellung für Daten pro TLP angibt.
Beobachtungsliste	Wenn ein Benutzer der Beobachtungsliste hinzugefügt wird, erhält er E-Mail-Benachrichtigungen über Änderungen an Status und Priorität.
Beschränkung erzwingen	Aktivieren Sie dieses Kontrollkästchen, um Mitglieder der zulässigen Gruppe und zulässige Mitglieder zu ändern. Weitere Informationen finden Sie unter Erzwungene Einschränkungen für Fall/Fälle.

6. Füllen Sie die Felder im Abschnitt „Einblicke“ entsprechend aus.

Einblicke

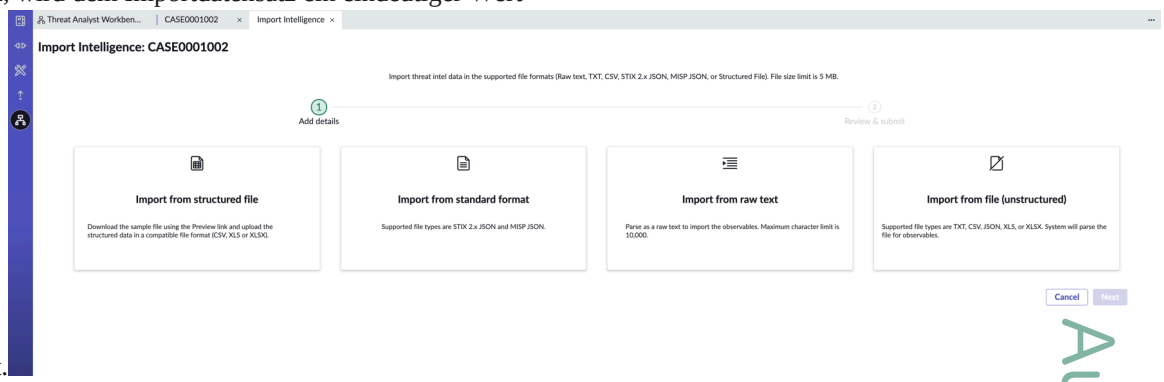
Feld	Beschreibung
Notizen	Alle zusätzlichen Hinweise im Zusammenhang mit der Bedrohungsuntersuchung.
Empfehlungen oder Aktionen	Alle Empfehlungen oder Aktionen im Zusammenhang mit der Bedrohungsuntersuchung.
Analyse und Ergebnisse	Geben Sie die Analysen und Ergebnisse im Zusammenhang mit der Bedrohungsuntersuchung ein.
Abschlusszusammenfassung	Fügen Sie die Abschlusszusammenfassung der Ergebnisse hinzu.

7. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem der Datensatz gespeichert wurde, können Sie auf die Registerkarte **„Import Intelligence“** klicken, um die Bedrohungsdaten mithilfe der Funktion **„Intelligence importieren“** zu importieren.

Hinweis:
Wenn Sie Daten aus der Fallverwaltung importieren und verarbeiten, wird dem Importdatensatz ein eindeutiger Wert zugeordnet.



Erzwungene Einschränkungen für Fall/Fälle

Verwenden Sie diese Funktion, um einen Fall einzuschränken und eine Liste der Gruppen und Anwender bereitzustellen, die darauf zugreifen können.

Erforderliche Rolle:

- sn_sec_tisc.analyst
- sn_sec_tisc_admin
- sn_sec_tisc.restriction_access_manager

Wichtige Überlegungen

1. Schränken Sie einen Fall ein, und stellen Sie eine Liste der Gruppen/Anwender bereit, die darauf zugreifen können.
2. Aktivieren Sie das Feld „Beschränkung erzwingen“ auf der Fallformularseite.
3. Ändern Sie die Mitglieder der zulässigen Gruppe und zulässige Mitglieder.
4. Sobald ein Fall als eingeschränkt markiert ist, können nur Mitglieder zulässiger Gruppen, Mitglieder der Liste zulässiger Anwender und Anwender mit der Rolle „sn_sec_tisc.admin“ auf diesen Fall zugreifen.
5. Gewähren Sie dem Analysten (sn_sec_tisc.restriction_access_manager mit dieser Rolle) Zugriff, der auf das Feld „Beschränkung erzwingen“ zugreifen muss.
6. Ein vorhandener assigned_to-Analyst und ein Analyst, der dies als eingeschränkt markiert hat, verlieren ebenfalls den Zugriff, wenn sie nicht zu den zulässigen Gruppen oder Mitgliedern hinzugefügt werden.
7. Die Einschränkung von Fällen innerhalb des CTI-Teams wird pro Fall implementiert. Zulässige Mitglieder können auf eingeschränkte Fälle zugreifen, wenn sie sich in der Zulassungsliste befinden. Wenn Sie sie in eine der zulässigen Fälle aufnehmen, bedeutet dies nicht, dass sie auf alle anderen eingeschränkten Fälle zugreifen können.
8. Wenn der Fall als eingeschränkt markiert ist und „Zulässige Mitglieder“ oder „Zulässige Gruppe“ leer gelassen wird, kann nur „sn_sec_tisc.admin“ auf diese eingeschränkten Fälle zugreifen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Nur die Gruppen, denen die Rolle „Analyst“ (sn_sec_tisc.analyst) zugewiesen ist, sind in der Liste der zulässigen Mitglieder und Gruppen zulässig.

Hinweis:
Wenn ein Fall als eingeschränkt gekennzeichnet ist, wird eine Arbeitsnotiz veröffentlicht.

Zugriffssteuerungen für einen Fall

Lassen Sie spezifische Zugriffssteuerungen für einen Fall zu.

In der folgenden Tabelle werden die Rollen und Zugriffssteuerungen beschrieben.

Rolle	Zugriff	Beschreibung
sn_sec_tisc.restriction_access_manager	Lesezugriff	Hier hinzugefügte externe Anwender erhalten Zugriff auf das Fallformular, können jedoch keine Felder im Fall bearbeiten oder Aktionen ausführen.
	Privilegierter Zugriff	Hier hinzugefügte externe Anwender erhalten Zugriff auf die Bearbeitung aller Felder im Fallformular, dürfen jedoch keine Orchestrierungen ausführen.
sn_sec_tisc.spezial_access_read_manager	Lesezugriff	Hier hinzugefügte externe Anwender erhalten Zugriff auf das Fallformular, können jedoch keine Felder im Fall bearbeiten oder Aktionen ausführen.
sn_sec_tisc.spezial_access_write_manager	Privilegierter Zugriff	Hier hinzugefügte externe Anwender erhalten Zugriff auf die Bearbeitung aller Felder im Fallformular, dürfen jedoch keine Orchestrierungen ausführen.

Externer Anwenderzugriff für Fallaufgaben

In diesem Abschnitt wird der externe Anwenderzugriff für Fallaufgaben beschrieben.

Zuweisung von Fallaufgaben an externe Benutzer

Fallaufgaben werden Anwendern mit der externen Rolle zugewiesen, auch wenn sie keinen Zugriff auf die Rolle „sn_sec_tisc.analyst“ haben.

1. Jeder externe Anwender, dem eine Fallaufgabe zugewiesen ist, kann das Fallaufgabenmodul nur anzeigen und verfügt über die Berechtigung, die Fallaufgabe zu bearbeiten.
2. Der externe Anwender kann nur die Fallaufgaben anzeigen, die ihm oder den Gruppen, denen er angehört, zugewiesen sind.
3. Der externe Anwender sollte in der Lage sein, die Aufgabe innerhalb der Gruppe, der er angehört, neu zuzuweisen.

Ordnen Sie MITRE-Techniken einem Fall zu

Ordnen Sie einem Fall eine oder mehrere MITRE-Techniken zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallmanagement** > **Alle Fälle**.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Klicken Sie auf die Schaltfläche **MITRE-Technik zuordnen**.
6. Klicken Sie auf **„Matrix hinzufügen“**, um die MITRE-Technik zuzuordnen.
   Das Dialogfeld **„MITRE-Technik zu Fall zuordnen“** wird angezeigt.
7. Wählen Sie die **Matrix**aus.
   Alle aktivierten Matrizen werden angezeigt, damit Sie die Matrix auswählen können.
8. Wählen Sie die Taktik aus den Dropdown-Listen aus.
   Alle einer Matrix zugeordneten Taktiken werden angezeigt.

   Hinweis:
   Wenn Sie weitere Taktiken hinzufügen möchten, klicken Sie auf **Taktik hinzufügen**. Die zuvor ausgewählten Taktiken werden nicht mehr in der Dropdown-Liste angezeigt, wenn Sie eine neue Taktik hinzufügen.

9. Wählen Sie die **Technik**aus.
   Alle Techniken, die der ausgewählten Taktik zugeordnet sind, werden angezeigt. Wenn Sie weitere Taktiken hinzufügen, können Sie die zugehörigen Techniken für diese ausgewählte Taktik auswählen.
10. Klicken Sie auf **Speichern**.
    Wenn Sie die gesamten zugeordneten Matrixdaten löschen möchten, klicken Sie auf **„Matrix löschen“**. Mit dieser Aktion werden nur die zugeordneten Matrixdaten entfernt, die Matrix verbleibt jedoch im MITRE ATT&CK-Repository.

    Der zugehörige Matrixdatensatz wird unter dem Abschnitt MITRE ATT&CK-Karte angezeigt. In der Kartenansicht:

    Hinweis:
    In der Dropdown-Liste „Matrix“ können Sie zwischen mehreren Matrizen wechseln.

    a. In der ersten Zeile der Kartenansicht werden alle Taktiken angezeigt, die der aktuell ausgewählten Matrix zugeordnet sind.
    b. Jede Taktikkarte zeigt den Namen der Taktik und die Anzahl der Techniken an, die dem aktuellen Falldatensatz zugeordnet sind.
    c. Alle Techniken, die diesem Fall zugeordnet sind, werden vertikal unter jeder Taktik angezeigt. Sie können auf jede Technik klicken, um die Technikformularansicht anzuzeigen.
11. Klicken Sie auf **„ID anzeigen“,** um die IDs für alle zugehörigen Techniken anzuzeigen.

    Hinweis:
    Auf jeder Technikkarte werden der Name und die ID der Technik nur angezeigt, wenn **ID anzeigen** aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Klicken Sie auf **Aktualisieren**, um die Kartenansicht zu aktualisieren.
    Sie können den Zeitstempel der letzten Aktualisierung für die ausgewählte Matrix anzeigen.

Hinweis:
Klicken Sie auf das Symbol zum Ausklappen, um die zugehörige Matrixkarte auszuklappen und auf einer neuen Registerkarte anzuzeigen.

Rollup von MITRE-Technikzuordnungen durchführen

Führen Sie einen Rollup von MITRE-Technikzuordnungen von erkennbaren Elementen, Indikatoren, Objekten und Security Incidents durch, die mit einem Falldatensatz verknüpft sind oder nicht.

Vorbereitungen

Hinweis:

- Beim Rollup von MITRE-Technikzuordnungen für Security Incidents werden die der MITRE-Technik zugeordneten Daten aus Security Incidents für die Fallverwaltung in TISC zusammengefasst.
- Standardmäßig ist diese Eigenschaft „sn_sec_tisc.auto_rollup_mitre_data“ für MITRE-Techniken aktiviert, um automatisch ein Rollup zu Fällen aus den zugeordneten Objekten oder Security Incidents durchzuführen.
- Wenn Sie bei Bedarf ein Rollup von MITRE-Technikzuordnungen durchführen möchten, navigieren Sie zu den weiteren Aktionen in der **Fallformularansicht,** und wählen Sie die Option **Rollup für MITRE-Techniken durchführen aus**. Dieser Vorgang wird asynchron ausgeführt, und Sie können den Abschnitt **„Aktivitätenstrom“** auf Aktualisierungen für die Rollup-Aktivität überprüfen.

Erforderliche Rolle: sn_sec_tisc.analyst

Warum und wann dieser Vorgang ausgeführt wird

- Wenn eine Entität wie ein erkennbares Element oder ein Indikator mit einem Fall verknüpft ist, werden alle MITRE-Technikzuordnungen, die für diese Entität vorhanden sind, automatisch für den Fall zusammengefasst.
- Wenn die Verknüpfung einer Entität (z. B. eines erkennbaren Elements oder eines Indikators) aufgehoben und aus dem Fall entfernt wird, werden alle MITRE-Technikzuordnungen, für die ein Rollup aus dem Fall durchgeführt wird und für diese Entität vorhanden sind, automatisch entfernt und für den Fall zusammengefasst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallmanagement** > **Alle Fälle**.
   Alle Fälle werden angezeigt.
4. Öffnen Sie einen beliebigen Fall.
5. Wechseln Sie zur Registerkarte **Artefakte**.
6. Wählen Sie in der zugehörigen Liste der Artefakte **Observables (** Erkennbare Elemente) aus.
7. Wählen Sie die Schaltfläche **Link** aus.
8. Wählen Sie die erkennbaren Elemente aus, die Sie mit dem Fall verknüpfen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie auf **Link**, um die erkennbaren Elemente zu verknüpfen.
   Nachdem Sie die erkennbaren Elemente mit einem Fall verknüpft haben, werden die MITRE-Techniken, die diesem bestimmten erkennbaren Element zugeordnet sind, automatisch zusammengefasst, und die Listenanzahl der MITRE-Techniken im Abschnitt „Artefakte“ wird automatisch aktualisiert.
10. Klicken Sie **auf Verknüpfung aufheben**, um die Verknüpfung der erkennbaren Elemente mit dem Fall aufzuheben.
    Nachdem Sie die Verknüpfung der erkennbaren Elemente mit einem Fall aufgehoben haben, werden die diesem bestimmten erkennbaren Element zugeordneten MITRE-Techniken automatisch entfernt, und die Anzahl der MITRE-Technikenliste im Abschnitt „Artefakte“ wird automatisch aktualisiert.

Erstellen Sie eine Fallaufgabe mit der Workbench für Bedrohungsanalysten

Erstellen Sie Fallaufgaben, die dem Fall/den Fällen zugeordnet werden.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst, sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallaufgabenmanagement** > **Alle Fallaufgaben**.
   Alle Fallaufgaben werden angezeigt.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder entsprechend aus.

Neue Fallaufgabe erstellen

Feld	Beschreibung
Aufgaben-ID	Ein eindeutiger Bezeichner für die Fallaufgabe. Dies ist die vom System generierte ID.
Kurzbeschreibung	Zusammenfassung der Anforderung oder des Problems, die bzw. das untersucht wird, oder eine Kurzbeschreibung.
Beschreibung	Eine detaillierte Beschreibung mit allen relevanten Informationen zur Fallaufgabe, z. B. Hintergrund, erforderliche Analyse, erwartete Ergebnisse.
ID des übergeordneten Falls	Wählen Sie die übergeordnete Fall-ID aus der Suche aus.
Priorität	Eine Bewertung des Schweregrads der Anforderung oder des Problems.
Zuweisungsgruppe	Die zugewiesene Gruppe, die für die Bearbeitung der Fallaufgabe verantwortlich ist.
Status	Der aktuelle Status der Fallaufgabe.
Zugewiesen an	Der für die Bearbeitung einer Fallaufgabe verantwortliche Analyst
Fälligkeitsdatum	Zeitpunkt (Datum und Uhrzeit), zu dem die Fallaufgabe abgeschlossen oder geschlossen werden soll

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
TLP	Eindeutiger Wert, der die Vertraulichkeitseinstellung für Daten pro TLP angibt.
Beschränkung erzwingen	Aktivieren Sie als sn_sec_tisc_admin dieses Kontrollkästchen, um Mitglieder der zulässigen Gruppe und zulässige Mitglieder zu ändern. Weitere Informationen finden Sie unter Erzwungene Einschränkungen für Fall/Fälle.

6. Füllen Sie die Felder im Abschnitt „Einblicke“ entsprechend aus.

Einblicke

Feld	Beschreibung
Notizen	Alle zusätzlichen Hinweise im Zusammenhang mit der Bedrohungsuntersuchung.
Abschluss	Fügen Sie die Abschlusszusammenfassung der Ergebnisse hinzu.

7. Klicken Sie auf **Speichern**.
   Ihre Fallaufgabe wird Ihrem Fall zugeordnet.

Hinweis:
Nachdem Sie die Fallaufgabe gespeichert haben, können Sie ihr Tags und Taxonomien hinzufügen. Weitere Informationen finden Sie unter Taxonomien werden erstellt.

Artefakte zu Fällen oder Fallaufgaben hinzufügen

Nachdem Sie einen Fall erstellt haben, können Sie Artefakte wie Security Incidents, CIs und Kompromittierungsindikatoren anzeigen oder dem Fall hinzufügen. Diese Artefakte dienen als Hinweise zur Lösung des Falls.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis:
Artefakte sind nur für die vorhandenen Fälle verfügbar. Für erkennbare Elemente und Indikatoren können die Artefakte auch über die Schaltfläche „Import Intelligence“ aus dem Importauftrag hinzugefügt oder einem Fall zugeordnet werden. Weitere Informationen zum Importieren finden Sie unter Importieren Sie Threat Intelligence

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallmanagement** > **Alle Fälle**.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen Fall oder eine Fallaufgabe aus.
5. Wechseln Sie zur Registerkarte **Artefakte**.
   Die zugeordneten Artefakte werden als zugehörige Listen für diesen bestimmten Fall oder diese Fallaufgabe angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verknüpfen Sie die Datensätze mit dem Fall oder der Fallaufgabe, oder heben Sie die Verknüpfung auf.

Hinweis:
Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen

Die folgende Tabelle enthält die zugehörigen Listen der Artefakte, die sich auf die Fälle oder Fallaufgaben beziehen:

Zugehörige Datensätze

Zugehörige Liste	Beschreibung
MITRE-Techniken	Liste der MITRE-Techniken im Zusammenhang mit den Fällen. MITRE-Techniken zeigt auch alle zugehörigen Techniken in einem Fall an.
Erkennbares Element	Liste der erkennbaren Elemente im Zusammenhang mit diesen Fällen oder Fallaufgaben.
Indikatoren	Liste der Indikatoren, die sich auf diese Fälle oder Fallaufgaben beziehen.
Angriffsmuster	Liste der Angriffsmuster, die sich auf diese Fälle oder Fallaufgaben beziehen.
Kampagnen	Listen Sie die Kampagnen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Vorgehensweisen	Listen Sie die Aktionen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Datenkomponenten	Liste der Datenkomponenten, die sich auf diese Fälle oder Fallaufgaben beziehen
Bedrohungsgruppierungen	Listen Sie die Bedrohungsgruppierungen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Identitäten	Listen Sie die Identitäten auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Infrastruktur	Listen Sie die Infrastruktur auf, z. B. Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die sich auf diese Fälle oder Fallaufgaben beziehen.
Angriffssätze	Liste der Angriffssätze, z. B. eine Reihe von Angreiferverhalten und Ressourcen mit allgemeinen Eigenschaften, die sich auf diese Fälle oder Fallaufgaben beziehen.
Standorte	Liste der Standortdatensätze, die sich auf diese Fälle oder Fallaufgaben beziehen.
Malware	Liste der Malware-Quelldatensätze, die sich auf diese Fälle oder Fallaufgaben beziehen.
Markierungsdefinitionen	Listen Sie die Markierungsdefinitionen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Bedrohungshinweise	Listen Sie die Markierungsdefinitionen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Beobachtete Daten	Listen Sie die beobachteten Daten auf, die sich auf diese Fälle oder Fallaufgaben beziehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Bedrohungsmeinungen	Liste der Bedrohungsmeinungen, die sich auf diese Fälle oder Fallaufgaben beziehen.
Bedrohungsberichte	Liste der Bedrohungsberichte, die sich auf diese Fälle oder Fallaufgaben beziehen.
Sichtungen	Liste der Sichtungen, die sich auf diese Fälle oder Fallaufgaben beziehen
Bedrohungsakteure	Liste der Bedrohungsakteure, die mit diesen Fällen oder Fallaufgaben zusammenhängen.
Tools	Listen Sie die Tools auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Schwachstellen	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die über eine übereinstimmende IP-Adresse verfügen und sich auf diese Fälle oder Fallaufgaben beziehen.
Verwandte Fälle	Listet die zugehörigen Fälle auf.
Zugehöriger Fall – Aufgaben	Listet die zugehörigen Fallaufgaben auf.
Security Incidents	Listet die Security Incidents auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Betroffene Konfigurationselemente	Liste der betroffenen Konfigurationselemente, die sich auf diese Fälle oder Fallaufgaben beziehen.
Betroffene Services	Listet die betroffenen Services auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Betroffene Assets	Listen Sie die betroffenen Assets auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Schwachstelleneinträge	Liste der Schwachstelleneinträge, die sich auf diese Fälle oder Fallaufgaben beziehen.

Führen Sie Ergänzungsaktionen innerhalb eines Falls aus

Verwenden Sie diesen Abschnitt, um zu verstehen, wie Ergänzungsaktionen für Fälle ausgeführt werden.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

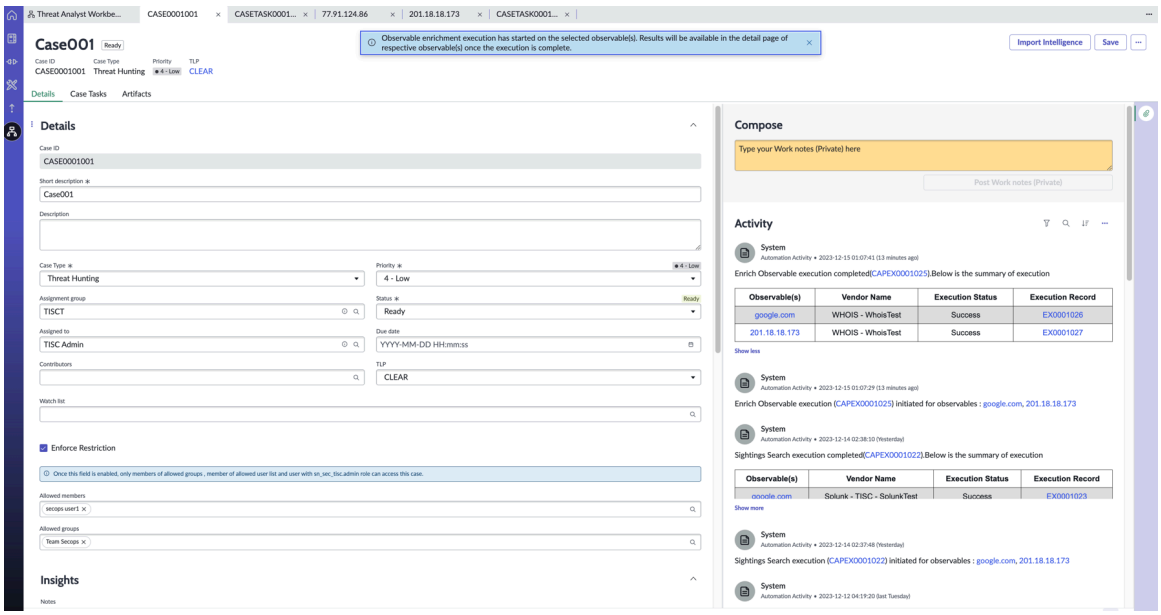
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallmanagement** > **Alle Fälle**.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen Fall oder eine Fallaufgabe aus.
5. Wechseln Sie zur Registerkarte **Artefakte**.
6. Wählen Sie die zugehörige Liste „Erkennbare Elemente“ aus.
7. Wählen Sie ein oder mehrere erkennbare Elemente aus.
8. Klicken Sie in der Dropdown-Liste auf eine beliebige Ergänzungsaktion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie die verfügbare(n) Implementierung(en) aus.
10. Klicken Sie auf **Absenden**.
    Beispiel: Bedrohungssuche ausführen. Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsmeldung angezeigt, dass die Ausführung der Ergänzung erkennbarer Elemente für für das/die ausgewählte(n) erkennbare(n) Element(en) gestartet wurde. Ergebnisse sind auf der Detailseite des jeweiligen erkennbaren Elements verfügbar, sobald die Ausführung abgeschlossen ist.

Hinweis:
Sobald die Ausführung initiiert oder abgeschlossen ist, wird im Aktivitätenstrom der Formularansicht eine Arbeitsnotiz veröffentlicht.



Fallberichte anzeigen

Verwenden Sie die Funktion „Fallberichte“, um Berichte zu den Fällen zu generieren. Diese Berichte umfassen einen Nachuntersuchungsbericht oder einen Zusammenfassungsbericht.

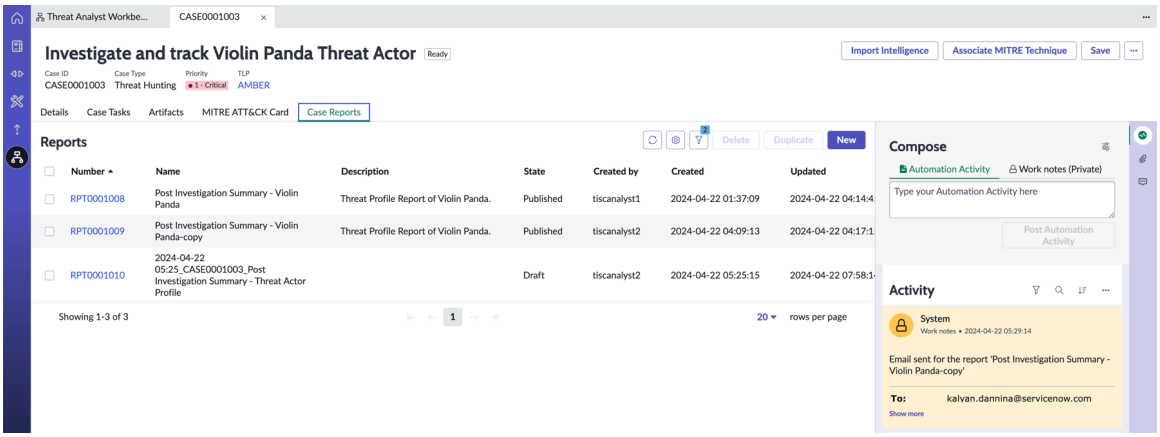
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

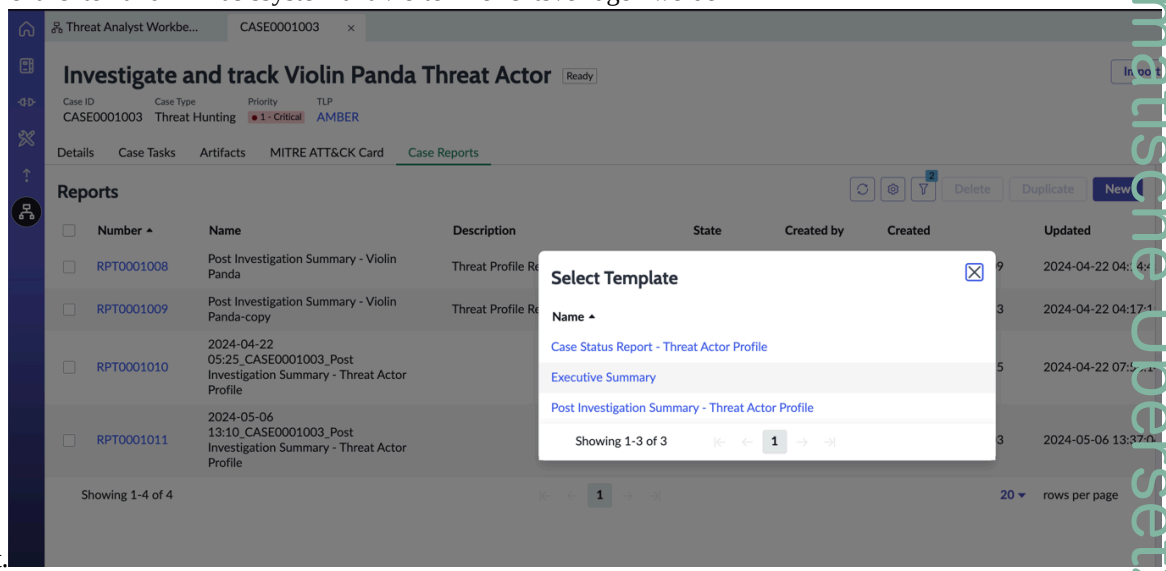
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallmanagement** > **Alle Fälle**.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Wechseln Sie zu **Fallberichte**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Sie können die Berichte aus der Liste löschen, Duplikate der vorhandenen Berichte erstellen und Ihren eigenen Bericht anpassen.

6. Klicken Sie auf **Neu**.
   Die veröffentlichten und im Basissystem aktivierten Berichtsvorlagen werden angezeigt.



7. Wählen Sie die gewünschte Berichtsvorlage aus.
   Die ausgewählte Berichtsvorlage für den Berichtstyp wird generiert. Auch hier kann der Bericht nach seiner Veröffentlichung von einer größeren Gruppe von Anwendern angezeigt werden. Wenn sich der Bericht jedoch im Entwurfsstatus befindet, ist er für die Anwender ausgeblendet. Als Analyst können Sie nur die veröffentlichten Berichte, nicht jedoch die Berichte im Entwurfsstatus anzeigen.

Hinweis:

- Wenn Sie weitere Felder hinzufügen möchten, wählen Sie die Felder aus, und fügen Sie sie direkt in Ihrem Fallbericht hinzu.
- Wenn Sie eine zugehörige Liste hinzufügen möchten, z. B. eine Liste von erkennbaren Elementen, wählen Sie Observables (Erkennbare Elemente). Alle erkennbaren Elemente, die diesem bestimmten Fall zugeordnet sind, werden aufgelistet. Wählen Sie mindestens ein erkennbares Element aus, und klicken Sie auf **„Hinzufügen“**. Sie können auch das erforderliche erkennbare Element herausfiltern und Ihrem Fall hinzufügen.

8. Klicken Sie auf **Inhalt speichern,** um den Inhalt Ihres Berichts zu speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie **auf Vorschau,** um eine Vorschau des Berichts anzuzeigen.

   Hinweis:
   Sie können dann wie folgt vorgehen:

   - **Maximieren Sie** das Berichtsfenster.
   - **Laden Sie** den Bericht über **das Download** -Symbol herunter.
   - Popouten Sie den Bericht auf einer neuen Registerkarte, falls die Höhe oder Größe des Berichts geändert wird, um eine bessere Anzeige-Experience zu bieten.
   - **Bearbeiten Sie** den Berichtsnamen und die Berichtsbeschreibung.
   - **Veröffentlichen Sie** den Bericht.

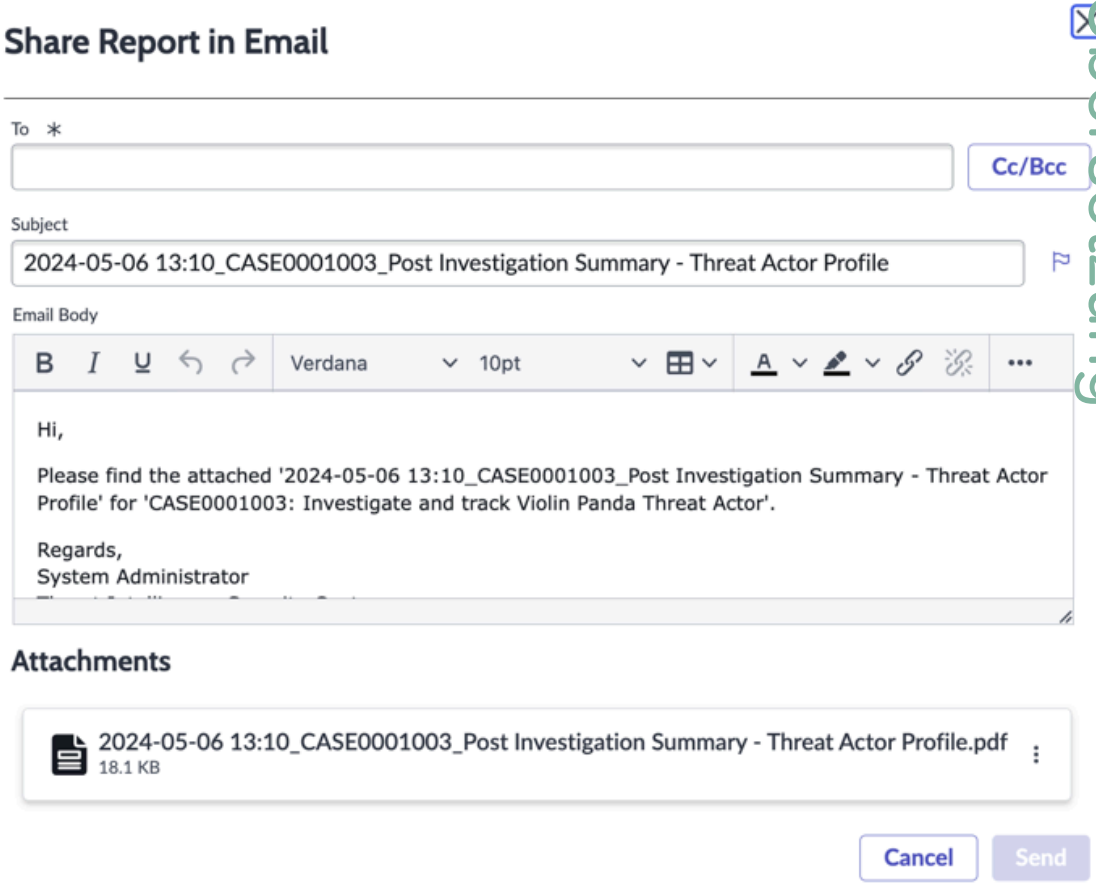
10. Klicken Sie auf die Schaltfläche **Inhalt bearbeiten**, um den Bericht erneut zu veröffentlichen.

    Hinweis:
    Es wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, den Bericht freizugeben:

    Sie müssen den Bericht erneut veröffentlichen, nachdem Sie Changes vorgenommen haben, damit Sie den Bericht herunterladen oder freigeben können. Möchten Sie die Bearbeitung trotzdem fortsetzen?

11. Klicken Sie auf **Bearbeiten**.
    Wenn Sie den Bericht bearbeiten möchten, können Sie mit der Bearbeitung des Berichts wie erläutert fortfahren oder den Bericht veröffentlichen. Nach der Veröffentlichung ist der Bericht schreibgeschützt.

12. Klicken Sie auf **„Bericht in E-Mail freigeben",** um den Bericht freizugeben.
    Bei der Freigabe des Berichts wird der generierte PDF-Bericht als Anhang an die E-Mail



angehängt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Fügen Sie die erforderlichen E-Mail-Felder hinzu, z. B. An (für den Sie den Bericht freigeben möchten), CC und BCC
14. Markieren Sie die E-Mail bei Bedarf als wichtig.
15. Klicken Sie auf **Senden**.
    Der Bericht wird für die größere Gruppe von Anwendern freigegeben.

Sichere Dateianhänge hochladen

In diesem Abschnitt erfahren Sie, wie Sie die sicheren Dateianhänge in den Fall/die Fälle hochladen.

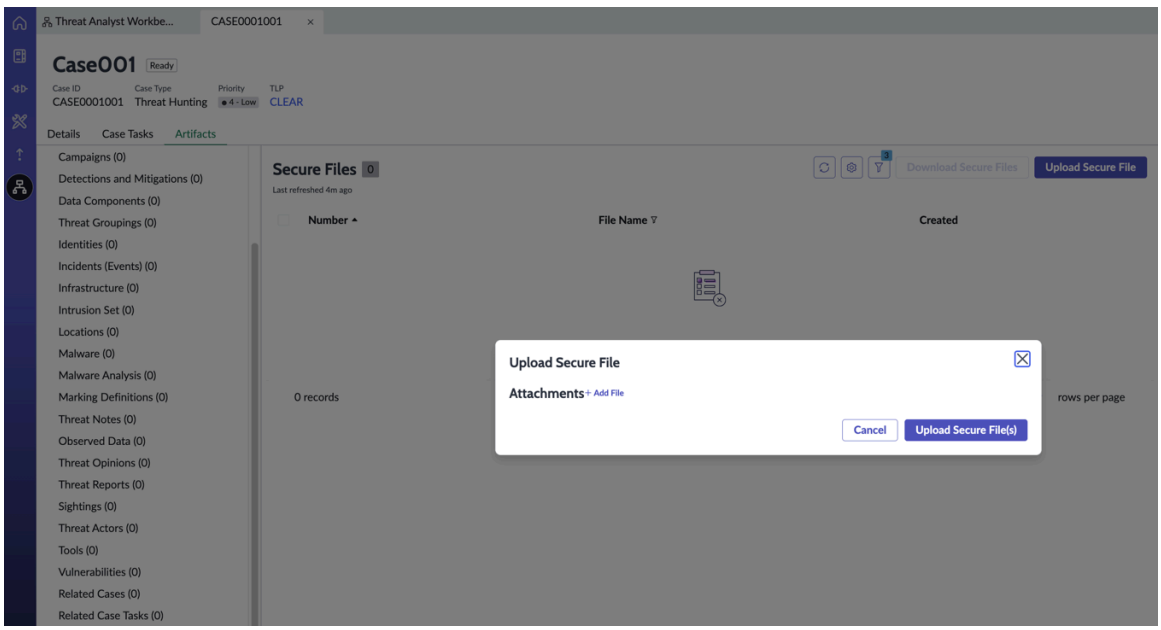
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc_secure_file_access, sn_sec_tiscadmin

Hinweis:
Die zugehörigen Listen für „Sichere Dateien“ werden nur angezeigt, wenn Sie über die Anwenderrolle sn_sec_tisc.secure_file_access verfügen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Fallmanagement** > **Alle Fälle**.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Gehe zu **Artefakte** > **Sichere Dateien** zugehörige Listen.
6. Klicken Sie auf die Schaltfläche **Sichere Datei hochladen**.
7. Klicken Sie auf **Datei hinzufügen**, um die Anhänge hinzuzufügen.
8. Wählen Sie die Dateien aus, und klicken Sie auf die Schaltfläche **Sichere Datei(en) hochladen**.
   Die Dateianhänge werden hochgeladen.



9. Klicken Sie auf **Sichere Dateien herunterladen**, um die Anhänge herunterzuladen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anhänge sind im ZIP-Format verfügbar.

10. Alternativ können Sie die Datei herunterladen, indem Sie zur Detailseite des sicheren Dateidatensatzes navigieren.

Hinweis:

- Alle sicheren Anhänge werden mit dem Key Management Framework (KMF) verschlüsselt und im System gespeichert. Weitere Informationen finden Sie unter Anhangsverschlüsselung .
- Wenn Benutzer ein Abonnement für *ServiceNow IntegrationHub* **Professional Pack Installer**haben, werden sichere Dateien im ZIP-Format komprimiert und außerdem verschlüsselt und gespeichert

Threat Intelligence-Sicherheitszentrum Bibliothek

Eine Bedrohungsbibliothek wird als eine Gruppe von organisierten Objekten und Entitäten definiert, die Organisationen mit strukturierten und unstrukturierten Sicherheitsbedrohungsinformationen bereitstellen.

Die Bedrohungsinformationen sind in Form von Feeds verfügbar. Die Feeds liefern Ihnen wertvolle Bedrohungsdaten aus Quellen wie STIX, MISP usw., in denen Threat Intelligence-Entitäten aufgelistet sind.

In der Bibliothek des Threat Intelligence-Sicherheitszentrums wird erläutert, wie Sie die Daten durchsuchen, indem Sie grundlegende und erweiterte Suchen und Filterregeln durchführen, den Import-Assistenten aufrufen, manuell Threat Intelligence-Datensätze hinzufügen und die erforderlichen Aktionen ausführen, z. B. Hinzufügen zur Zulassungsliste, zur Deny-Liste und zur Beobachtungsliste .

Die Detailansicht bietet Einblicke in die Intelligenzdatensätze, und in Listenansichten können Sie Schnellaktionen für einen oder mehrere Datensätze ausführen.

Datenmodell verstehen

Das Datenmodell und die Architektur des Moduls „Threat Intelligence Security Center“ sind so konzipiert, dass die Funktionen der Threat Intelligence-Plattform und verschiedene Sicherheitsansichten unterstützt werden, die detaillierte Daten für Bedrohungsanalysten bereitstellen.

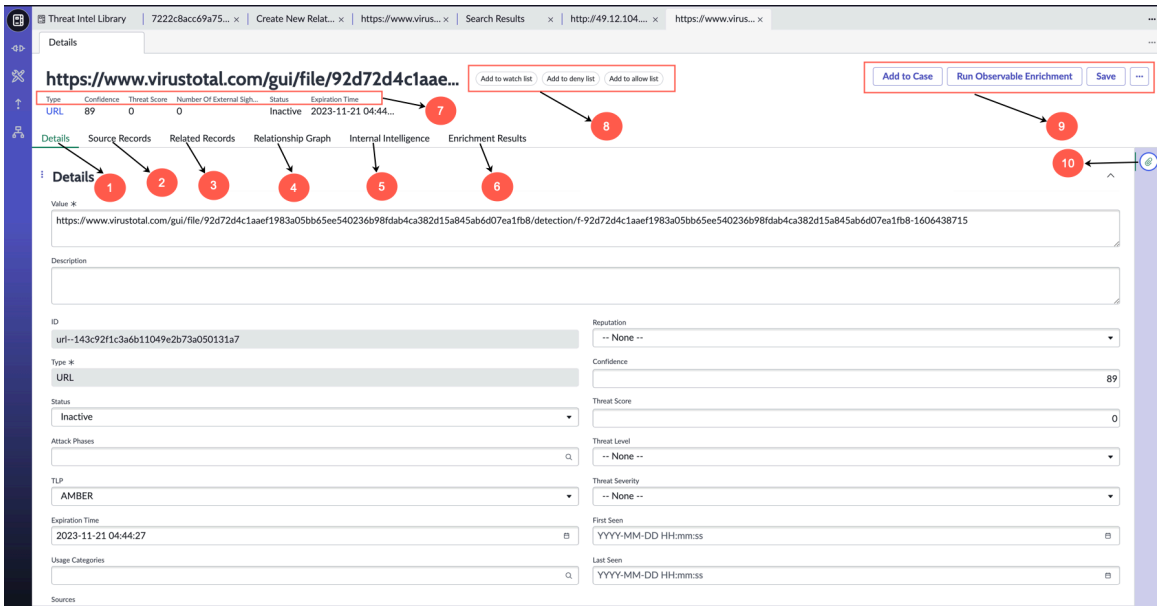
Das Datenmodell verfügt über die Datenstrukturen, die im Threat Intelligence-Repository als Objekte dargestellt werden.

TISC Formularansicht „Bibliotheksobjekte“.

Die Homepage für Threat Intelligence-Sicherheitszentrum -Objekte besteht aus den folgenden Funktionen.

Verwenden Sie, oder navigieren Sie zu diesen folgenden Abschnitten, um mehr über die einzelnen SDOs im Detail zu erfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



TISC Formularansicht „Bibliotheksobjekte“.

Bestellung	Menü/Registerkarte	Beschreibung
1	Registerkarte **Details**	Verwenden Sie diesen Abschnitt, um die SDOs in der Formularansicht anzuzeigen oder zu bearbeiten.
2	Registerkarte**„Quelldatensätze “**.	Quelldatensätze tragen zu einem aggregierten Datensatz bei, wie in der Formularansicht angezeigt. Diese Quelldatensätze werden automatisch aus Feeds erstellt oder manuell vom Anwender erstellt.
3	Registerkarte **Zugehörige Datensätze**	Listet alle zugehörigen Datensätze auf, die dem SDO zugeordnet sind.
4	Registerkarte**„Beziehungsdiagramm “**.	Visuelle Darstellung der zugehörigen Objekte.
5	Registerkarte**„Interne Intelligenz“.**	Listet die internen Intelligenzdatensätze der zugeordneten Objekte auf.
6	Registerkarte**„Ergänzungsergebnisse “**.	Listet die Ergänzungsintegrationen auf, die den Objekten zugeordnet sind.
7	**Formularbanner**	Dies ist ein schreibgeschützter Abschnitt, der die wichtigsten Felder wie Typ, Konfidenz, Bedrohungsbewertung, Anzahl der Sichtungen, Status und Ablaufzeit enthält.
8	**UI-Aktionen für Formularbanner**	Dies sind die Sicherheitskontrolllisten, auf die Sie klicken können, wenn sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC Formularansicht „Bibliotheksobjekte“. (Fortsetzung)

Bestellung	Menü/Registerkarte	Beschreibung
		basierend auf den erkennbaren Elementen zur Allow-Liste hinzugefügt, aus der Allow-Liste entfernt (Deny-Liste) oder zur Beobachtungsliste hinzugefügt werden sollen. Klicken Sie, um: • Zur Beobachtungsliste hinzufügen • Zur Deny-Liste hinzufügen • Zur Allow-Liste hinzufügen **Hinweis:** Die Formularaktionen gelten nur für erkennbare Elemente.
9	**Formular-UI-Aktionen**	Die für Formulare verfügbaren UI-Aktionen sind: 1. **Dem Fall hinzufügen**: Fügt die Objekte dem Fall hinzu. 2. **Ergänzung erkennbarer Elemente ausführen**: Führt die Ergänzungen für die ausgewählten Objekte aus. 3. **Speichern**: Speichern Sie den Datensatz. 4. **Löschen**: Löscht den Datensatz.
10	**Rechtes Kontextmenü**	Bietet einfachen Zugriff auf Schnellsteuerungen wie Anhänge, Notizen usw., basierend auf den Aufgaben, die diesem Objekt zugeordnet sind. Diese Option ist auf den verbleibenden beiden Registerkarten verfügbar, auf die der Bedrohungsanalyst bei Bedarf zugreifen kann. Über das Kontextmenü können Sie ganz einfach zu folgenden Aufgaben navigieren: 1. **Anhänge**: Hängen Sie beliebige Dateien an, die sich auf die Objekte beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC Formularansicht „Bibliotheksobjekte“. (Fortsetzung)

Bestellung	Menü/Registerkarte	Beschreibung
		Hinweis: Wenn Sie ein neues erkennbares Element, Indikatoren oder andere Objekte erstellen oder die vorhandenen Objekte anzeigen, wird der Bereich **Anhänge** standardmäßig in der entsprechenden Formularansicht angezeigt. Sie können entweder auf das Symbol **Anhänge** im rechten Kontextmenü klicken oder zu wechseln **Einstellungen** > **Arbeitsbereiche** und deaktivieren Sie **Sidebar anzeigen**. Weitere Informationen finden Sie unter Einstellungen für Next Experience-Arbeitsbereich konfigurieren . 2. **Einblicke**: Fügen Sie zusätzliche Informationen zu den erkennbaren Elementen oder Indikatoren hinzu, die diesem Objekt zugeordnet sind.
NA	**Im Navigator suchen**	Verwenden Sie diese Suchfunktion, um nach verschiedenen Objekten in der Threat Intel (TI)-Bibliothek zu suchen. Sie können beispielsweise nach allen Datensätzen erkennbarer Elemente im TI-Bibliotheksmodul suchen.
NA	**In Bedrohungsinformationenbibliothek suchen**	Verwenden Sie diese Suchfunktion, um basierend auf Ihren Suchkriterien in mehreren Quellen nach den Quelldatensätzen zu suchen. Die Ergebnisse werden auf einer separaten Registerkarte **Suchergebnisse** angezeigt. Wenn Sie beispielsweise bei der IP-Adresse 104.227.137.35 die Datensätze durchsuchen müssen,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC Formularansicht „Bibliotheksobjekte“. (Fortsetzung)

Bestellung	Menü/Registerkarte	Beschreibung
		geben Sie 104.* ein. Dann werden die Datensätze durch die Suche eingegrenzt und die Datensätze, die die IP-Adresse beginnend mit 104 enthalten, werden auf der separaten Registerkarte **Suchergebnisse** angezeigt. • Sie können auch die vorhandenen Suchbegriffe in den Suchkriterien auf derselben Seite Suchergebnisse ändern, ohne zur Seite „Bedrohungsbibliothek“ zurückzukehren. • Auf ähnliche Weise können Sie auch anhand des Namens und der Beschreibung eines bestimmten Datensatzes suchen. • Sobald die Datensätze gefiltert und aufgelistet sind, können Sie auf die Listenansicht klicken, um zum entsprechenden Datensatz auf einer neuen Registerkarte zu gelangen.

TISC-Bibliotheks-Repository

Das IoC-Repository enthält STIX-Objekte. Jedes dieser Objekte enthält eine bestimmte Information.

Erkennbare Elemente

Erkennbare Elemente stellen zustandsbehaftete Eigenschaften (z. B. den MD5-Hash einer Datei oder den Wert eines Registrierungsschlüssels) oder messbare Ereignisse (z. B. die Erstellung eines Registrierungsschlüssels oder das Löschen einer Datei) dar, die für den Betrieb von Computern und Netzwerken relevant sind .

Im Folgenden finden Sie die Arten von erkennbaren Elementen, die in der Anwendung verfügbar sind:

- Artefakt
- AS-Nummer
- Verzeichnis
- Domänenname
- E-Mail-Adresse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- E-Mail-Nachricht
- E-Mail-Betreff
- Datei
- IPv4-Adresse
- IPv4-CIDR
- IPv6-Adresse
- IPv6-CIDR
- MAC-Adresse
- MD5-Hash
- Mutex-Name
- Netzwerk
- Sonstiges erkennbares Element
- Prozess
- SHA1-Hash
- SHA256-Hash
- SHA512-Hash
- Software
- URL
- Anwenderaccount
- Windows-Registrierungsschlüssel
- X.509-Zertifikat

Definieren Sie ein erkennbares Element

Erkennbare Elemente können aus der geplanten Feed-Erfassung oder dem Import-Assistenten abgerufen werden. Sie können jedoch bei Bedarf erkennbare Elemente erstellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie den **Typ des erkennbaren Elements**aus.
   Das Formular zum Erstellen eines neuen erkennbaren Elementdatensatzes wird angezeigt.

   Hinweis:
   Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie ein neues erkennbares Element erstellen oder die vorhandenen erkennbaren Elemente anzeigen, wird der Bereich **Anhänge** standardmäßig in der Formularansicht angezeigt. Sie können entweder auf das Symbol Anhänge im rechten Kontextmenü klicken oder zu wechseln **Einstellungen** > **Arbeitsbereiche** und deaktivieren Sie **Sidebar anzeigen**. Weitere Informationen finden Sie unter Einstellungen für Next Experience-Arbeitsbereich konfigurieren .

Abschnitt „Details“

Feld	Beschreibung
Wert	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.
Beschreibung	Beschreibung des Datensatzes des erkennbaren Elements.
Autor	Geben Sie den Namen ein.
Typ	Der Klassifizierungstyp des erkennbaren Elements, z. B. IP-Adresse, Domänenname, Artefakt, Verzeichnis, Datei oder Hash. Standardmäßig wird dies angezeigt, wenn Sie den neuen Datensatz auswählen.
Status	Der aktive oder inaktive Status des erkennbaren Elements.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
TLP	Eindeutiger Wert, der die Vertraulichkeitseinstellung für Daten pro TLP angibt.
Reputation	Gibt die schädliche Reputation des erkennbaren Elements an.
Status	Geben Sie den Status des erkennbaren Elements ein, ob aktiv oder inaktiv.
Bedrohungsbewertung	Gibt die Bedrohungsbewertung für dieses erkennbare Element an.
Ablaufzeit	Gibt die Ablaufzeit des Datensatzes des erkennbaren Elements an.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Vertrauen	Geben Sie die Konfidenz für diesen Datensatz eines erkennbaren Elements ein. Die Konfidenzeigenschaft gibt das Vertrauen des Erstellers in die Richtigkeit seiner Daten an. Der Konfidenzwert muss eine Zahl im Bereich von 0 bis 100 sein.
Systemupdates verhindern	Wenn Sie diese Kennzeichnung auf „wahr“ festlegen, kann das System die Werte von Feldern im Datensatz nicht überschreiben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ist falsch positiv	Eine boolesche Kennzeichnung, die angibt, ob das erkennbare Element als falsch positiv identifiziert wurde.

Attribute

Feld	Beschreibung
Auflösung	Gibt eine Liste von Verweisen auf eine oder mehrere IP-Adressen oder Domänennamen an, in die der Domänenname auflöst.
Ist FQDN	Ein vollqualifizierter Domänenname (FQDN) ist die vollständige Adresse eines Internethosts oder Computers. Es stellt seinen genauen Speicherort innerhalb des Domain Name System (DNS) bereit, indem der Hostname, der Domänenname und die Domäne der obersten Ebene (TLD) angegeben werden.

Zusätzliche Informationen

Feld	Beschreibung
Bedrohungsstufe	Gibt die Bedrohungsstufe des Datensatzes des erkennbaren Elements an.
Erstmals aufgetreten	Der Zeitpunkt, zu dem dieser erkennbare Datensatz zum ersten Mal bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Bedrohungsschweregrad	Gibt den Bedrohungsschweregrad für den Datensatz des erkennbaren Elements an.
Zuletzt aufgetreten	Die Uhrzeit, zu der dieser Datensatz des erkennbaren Elements zuletzt bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Nutzungskategorien	Kategorien, unter die das erkennbare Element fällt, z. B. Botnet oder Phishing.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext hinzu.
Quellen	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.

Wichtig:
Quelle – Gemeldete Punktzahl: Dieses Feld enthält den aggregierten Wert der Bedrohungspunktzahlen, die von den Quellen gemeldet werden, aus denen das erkennbare Element erfasst wird. Um dieses Feld im Datensatzformular des erkennbaren Elements anzuzeigen, müssen Sie es manuell hinzufügen, da es standardmäßig nicht verfügbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute

Feld	Beschreibung
Auflösung	Gibt eine Liste von Verweisen auf eine oder mehrere IP-Adressen oder Domänennamen an, in die der Domänenname auflöst.
Ist FQDN	Ein vollqualifizierter Domänenname (FQDN) ist die vollständige Adresse eines Internethosts oder Computers. Es stellt seinen genauen Speicherort innerhalb des Domain Name System (DNS) bereit, indem der Hostname, der Domänenname und die Domäne der obersten Ebene (TLD) angegeben werden.

Hinweis:
Die Attribute **„Löst in“** und **„Ist FQDN“** gelten nur für den Typ **„Domänenname“** von erkennbaren Elementen.

Typattribute für erkennbares Element

Attributname	Attributtypen
Artefakt	○ Entschlüsselungsschlüssel ○ Verschlüsselungsalgorithmus ○ MD5-Hash ○ MIME-Typ ○ SHA1-Hash ○ SHA256-Hash ○ SHA512-Hash ○ URL
AS-Nummer	○ Name ○ RIR
Verzeichnis	○ Verzeichniserstellungszeit ○ Zeit des letzten Zugriffs auf das Verzeichnis ○ Zeit der letzten Bearbeitung des Verzeichnisses ○ Codierter Pfad
Domänenname	○ Ist FQDN ○ Auflösung
E-Mail-Adresse	○ Anzeigename ○ E-Mail-Hauptteil ○ E-Mail-Empfänger Bcc

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
	○ E-Mail-Empfänger CC ○ E-Mail-Empfänger an ○ E-Mail-Absender ○ E-Mail-Betreff ○ Sendedatum
Datei	○ Zusätzliche Informationen ○ Codierter Dateiname ○ Zeitpunkt der Dateierstellung ○ Zeitpunkt des letzten Dateizugriffs ○ Zeitpunkt der letzten Änderung ○ Magische Zahl des Dateinamens ○ MD5-Hash ○ MIME-Typ ○ SHA1-Hash ○ SHA256-Hash ○ SHA512-Hash
IPv4-Adresse	○ AS-Nummer ○ MAC-Adresse
IPv4-CIDR	○ AS-Nummer ○ MAC-Adresse
IPv6-Adresse	○ AS-Nummer ○ MAC-Adresse
IPv6-CIDR	○ AS-Nummer ○ MAC-Adresse
Netzwerk	○ Ziel-Bytes ○ Anzahl der Zielpakete ○ Ziel-Port ○ Endzeit ○ Länge des HTTP-Nachrichtentexts ○ HTTP-Anforderungsheader ○ HTTP-Anforderungsmethode ○ HTTP-Anforderungswert ○ HTTP-Anforderungsversion ○ ICMP-Code-Byte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
	○ ICMP-Typ-Byte ○ Ist Netzwerk aktiv ○ Socket-Blockierung ○ Socket-Zuhörvorgang ○ Netzwerkprotokolle ○ Socket-Adressenfamilie ○ Socket-Deskriptor ○ Socket-Handle ○ Socket-Optionen ○ Socket-Typ – Byte-Anzahl der Quelle ○ Anzahl der Quellpakete ○ Quell-Port ○ Startzeit ○ TCP-Ziel-Kennzeichnungen ○ TCP-Quell-Kennzeichnungen
Prozess	○ ASLR aktiviert ○ Befehlszeile ○ Aktuelles Arbeitsverzeichnis (Current Working Directory, CWD) ○ DEP aktiviert ○ Umgebungsvariablen ○ Ausgeblendet ○ Besitzer-SID ○ Prozess-ID ○ Priorität ○ Verarbeitungszeit des Prozesses ○ Servicebeschreibungen ○ Anzeigename für Service ○ Name der Servicegruppe ○ Servicename ○ Servicestarttyp ○ Servicestatus des Servicestatus ○ Startinformation ○ Windows-Integritätsstufe ○ Fenstertitel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
Software	○ Common Platform Enumeration (CPE) ○ Unterstützte Sprachen ○ Softwareidentifizierung (SWID) ○ Lieferantenversion
Anwenderaccount	○ Account-Erstellungszeit ○ Account-Ablaufzeit ○ Account-Anmeldung ○ Kontotyp ○ Zusätzliche Informationen ○ Kann Berechtigungen eskalieren ○ Zeit der letzten Änderung der Anmeldeinformationen ○ Anzeigename ○ Zeit der ersten Anmeldung ○ Ist Account deaktiviert ○ Ist berechtigt ○ Ist Serviceaccount ○ Zeitpunkt der letzten Anmeldung ○ Anwender-ID
Windows-Registrierungsschlüssel	○ Schlüssel geändert ○ Wert der Zeitregistrierung ○ Anzahl der Unterschlüssel
X.509-Zertifikat	○ Zusätzliche Informationen ○ Bezeichner des regulatorischen Schlüssels ○ Grundlegende Einschränkungen ○ Zertifizierungsrichtlinien ○ CRL-Verteilungspunkte ○ Erweiterte Schlüsselnutzung ○ Beliebige Richtlinie sperren ○ Bearbeiter ○ Alternativer Ausstellername ○ Ist selbstsigniert ○ Schlüsselnutzung ○ Nameneinschränkungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
	○ Richtlinieneinschränkungen ○ Richtlinienzuordnungen ○ Nutzung des privaten Schlüssels gültig ab ○ Nutzung des privaten Schlüssels gültig bis ○ Signaturalgorithmus ○ Betreff ○ Alternativer Antragstellername ○ Attribute des Betreffverzeichnisses ○ Antragstellerschlüssel-Bezeichner ○ Algorithmus des Antragstellers des öffentlichen Schlüssels ○ Exponent des Antragstellers des öffentlichen Schlüssels ○ Modulo des öffentlichen Schlüssels des Antragstellers ○ Gültig ab ○ Gültig bis ○ Version

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für einen Datensatz eines erkennbaren Elements hinzu.

5. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
6. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tags auswählen	Wählen Sie die Tags aus, die einem erkennbaren Element zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie die Taxonomie aus, die einem erkennbaren Element zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie die Taxonomiewerte hinzu, die einem erkennbaren Element zugeordnet sind.

Quelldatensätze

Feld	Beschreibung
Die Details der Quelldatensätze für ein erkennbares Element werden angezeigt, falls vorhanden.	

Nächste Maßnahme

Die folgende Tabelle listet die zugehörigen Datensätze auf, die sich auf die erkennbaren Elemente beziehen:

Zugehörige Datensätze

Zugehörige Liste	Beschreibung
Erkennbares Element	Liste der erkennbaren Elemente, die sich auf dieses erkennbare Element beziehen. **Hinweis:** Dieser Abschnitt enthält auch die potenziellen Beziehungen zwischen zwei erkennbaren Elementen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehung zwischen erkennbarem und potenziellem erkennbarem Element, und unter Definieren Sie Beziehungen zwischen erkennbaren Elementen und erkennbaren Elementen finden Sie die bestätigten Beziehungen zwischen den beiden erkennbaren Elementen.
Indikatoren	Liste der Indikatoren, die sich auf dieses erkennbare Element beziehen.
Angriffsmuster	Liste der Angriffsmuster, die sich auf dieses erkennbare Element beziehen.
Kampagnen	Listen Sie die Kampagnen auf, die sich auf dieses erkennbare Element beziehen.
Infrastruktur	Listen Sie die Infrastruktur auf, z. B. Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die sich auf dieses erkennbare Element beziehen.
Angriffssätze	Liste der Angriffssätze, z. B. eine Reihe von Angreiferverhaltensweisen und Ressourcen mit allgemeinen Eigenschaften, die sich auf dieses erkennbare Element beziehen.
Malware	Liste der Malware-Quelldatensätze, die sich auf dieses erkennbare Element beziehen.
Bedrohungsakteure	Liste der Bedrohungsakteure, die mit diesem erkennbaren Element verbunden sind.
Bedrohungsereignisse	Listet die Bedrohungsereignisse auf, die sich auf dieses erkennbare Element beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Zugehörige Liste	Beschreibung
Schwachstellen	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die über eine übereinstimmende IP-Adresse verfügen, die mit diesem erkennbaren Element verknüpft ist.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Außerdem können Sie im Abschnitt **„Zugehörige Datensätze“** die Beziehungen zwischen zwei erkennbaren Elementen mithilfe des Abschnitts **„Potenzielle Beziehungen“** bestätigen, der in der Formularansicht „ **Erkennbare Elemente** “ verfügbar ist. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
3. Sie können erkennbare Elemente zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.
4. Sie können auch Ergänzungsaktionen für erkennbare Elemente ausführen. Weitere Informationen finden Sie unter Führen Sie Ergänzungsaktionen innerhalb eines Falls aus.

Quelldatensätze für erkennbare Elemente

Die Quelldatensätze tragen zu einem zusammengefassten Datensatz bei, wie in der Formularansicht angezeigt. Diese Quelldatensätze werden automatisch aus Feeds erstellt oder manuell vom Anwender erstellt.

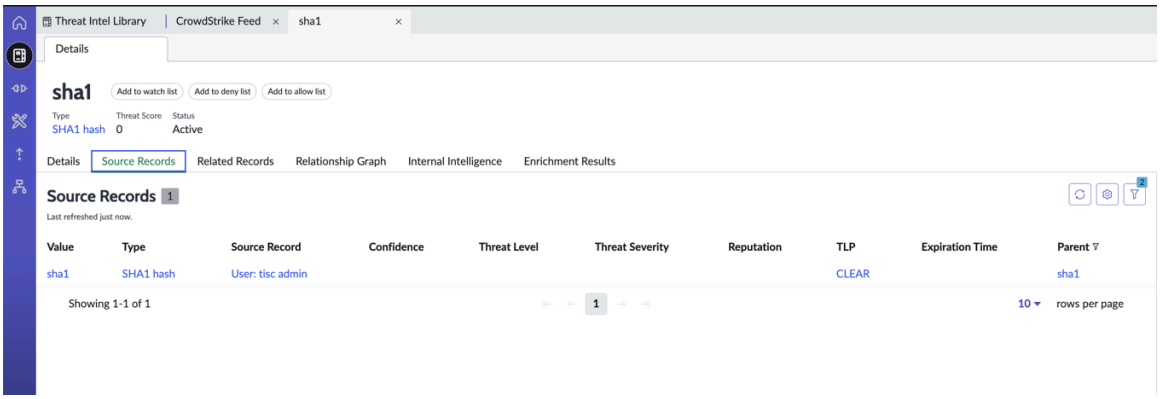
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Wählen Sie mindestens ein erkennbares Element aus.
5. Navigieren Sie zu **Quelldatensätze**.
   Die Quelldatensätze zu einem aggregierten Datensatz werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Zeigen Sie die Datensätze an.

Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen

Verknüpfen Sie die zugehörigen Datensätze, die sich auf die entsprechenden Bedrohungsinformationsobjekte beziehen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
2. Wählen Sie als Beispiel einen beliebigen Datensatz eines erkennbaren Elements aus.
3. Wechseln Sie zum Abschnitt **Zugehörige Datensätze**.
4. Wählen Sie einen beliebigen zugehörigen Datensatz aus.
5. Klicken Sie auf **Link**.
   Das Dialogfeld „Objekte verknüpfen“ wird angezeigt.
6. Wählen Sie die Objekte aus der Liste aus, und klicken Sie auf die Schaltfläche **Link**.
   Die einem erkennbaren Elementdatensatz zugeordneten Objekte werden verknüpft und in der Listenansicht „Zugehörige Datensätze“ angezeigt.
7. Klicken Sie auf **Speichern**.
   Klicken Sie auf die Schaltfläche **Verknüpfung aufheben**, um die Verknüpfung der Objekte aufzuheben

Daten zu erkennbaren Elementen abrufen

Rufen Sie die Daten der zugehörigen Datensätze erkennbarer Elemente ab.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zu **Erkennbare Elemente**.
   Die zugehörigen erkennbaren Elemente, die diesem ausgewählten Objekt zugeordnet sind, werden angezeigt.
4. Wählen Sie einen beliebigen erkennbaren Datensatz aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn den angegebenen erkennbaren Elementen CVEs zugeordnet sind, können Sie die zugehörigen Daten zu Schwachstellen automatisch über die bereitgestellte Schaltfläche abrufen. Diese zugeordneten Datensätze werden im Abschnitt „Geschäftskontext“ der Schwachstellen angezeigt.

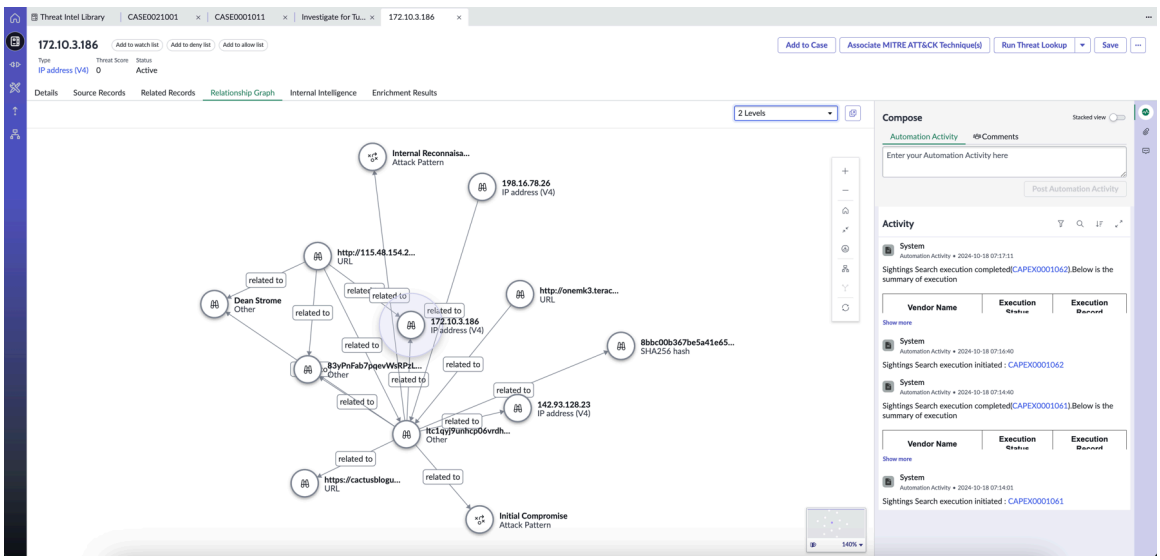
5. Gehe zu **Interne Intelligenz** > **Angreifbare Einträge**.
   Die zugeordneten CVEs-Datensätze für die erkennbaren Elemente werden angezeigt.
6. Wählen Sie ein beliebiges CVE aus, und klicken Sie auf die Schaltfläche **Vulnerability-bezogene Daten abrufen**.

Hinweis:

- In einer Informationsnachricht wird angezeigt, dass diesem spezifischen Schwachstellenobjekt keine angreifbaren Einträge zugeordnet sind. Sie müssen die Objekte mit den angreifbaren Einträgen verknüpfen, um die Daten abzurufen. Weitere Informationen zum Verknüpfen von Datensätzen und Ausführen der geplanten Aufgabe zum Abrufen der Daten finden Sie unter Rufen Sie Schwachstellendaten ab. Weitere Informationen zu geplanten Aufgaben finden Sie unter Geplante Aufgaben .
- Diese Schaltfläche löst eine geplante Hintergrundaufgabe aus, und die Details zur Initiierung und Ausführung des Auftrags werden im Abschnitt „Aktivitätenstrom“ angezeigt. Beispiel: Wenn der -Auftrag ausgelöst wird, zeigt der Aktivitätenstrom eine Aktivität an: Das Abrufen der zugehörigen Daten mit den Einträgen angreifbarer Elemente wurde gestartet. Die geplante Hintergrundaufgabe sucht kontinuierlich nach erkennbaren Elementen, denen ein angreifbarer Eintrag zugeordnet ist, und wird automatisch ausgeführt. Diese geplante Aufgabe wird jede Stunde ausgeführt. Falls die Datensätze nicht abgerufen werden, können Sie die Datensätze manuell verknüpfen und die Daten abrufen.

Details in Visualizer anzeigen

Mit der Visualisierung können Sie die Beziehungen zwischen Objekten, erkennbaren Elementen und Indikatoren anzeigen, die Kontext für weitere Untersuchungen bieten. In der Visualisierung werden Farben und Symbole verwendet, um verschiedene Informationen zu den Objekten darzustellen.



Sie können dann wie folgt vorgehen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zoomen Sie auf ein beliebiges Objekt, passen Sie es an den Bildschirm an, ziehen Sie die Knoten, oder heften Sie sie an, um den Fokus auf eine bestimmte Beziehung zu legen.
- Klicken Sie auf ein beliebiges Objekt, um den Detailbereich zu öffnen. Im Detailbereich erfahren Sie mehr über die dem Objekt zugeordneten Informationen. Sie können die Knoteneigenschaften wie Objekt, Objektname, Beschreibung und Quellen anzeigen. Standardmäßig wird der Detailabschnitt jedes Diagrammknotens nicht angezeigt, und Sie müssen auf jeden Knoten im Diagramm klicken, um die Details des ausgewählten Knotens anzuzeigen.

Hinweis:
Die Visualisierung ist für alle STIX Domain Objects (SDOs) mit Ausnahme der Observed Data-Objekte verfügbar. Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Visualisierung zu aktualisieren.

- Sie können auch auf das Popout-Symbol klicken, um das Diagramm in einem viel größeren Fenster anzuzeigen.

Arbeiten mit Datensätzen interner Intelligenz

Verwenden Sie diese Funktion, um mit den internen Intelligenzdaten zu arbeiten, die vom Configuration Database Management System (CMDB) im Threat Intelligence-Sicherheitszentrum erfasst werden.

Interne Intelligenzdatensätze anzeigen

Zeigen Sie die Datensätze für interne Intelligenz an, die von CMDB, Security Incident Response (SIR) und Vulnerability Response (VR) gesammelt wurden.

Vorbereitungen

Der Abschnitt „Interne Intelligenz“ bietet den Kontext aus anderen Anwendungen der Plattform wie SIR, VR und CMDB, um den Analysten eine breitere Perspektive der Bedrohung zu bieten.

Erforderliche Rolle: sn_sec_tisc.analyst

Hinweis:
Die Registerkarte „Interne Intelligenz“ ist nur für erkennbare Elemente und Schwachstellenobjekte sichtbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
2. Wählen Sie einen beliebigen Datensatz eines erkennbaren Elements aus.
3. Wechseln Sie zur Registerkarte **Interne Intelligenz**.
   Der Abschnitt „Interne Intelligenz“ besteht aus drei Unterabschnitten wie „Security Incident Response“, „Geschäftskontext“ und „Vulnerability Response“.

Hinweis:
Sie müssen die entsprechenden Anwendungen auf Ihrer Instanz installiert haben, damit diese Abschnitte auf der Registerkarte **„Internal Intelligence“** aufgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. **Security Incident Response**: Zeigt alle Incidents an, die mit den zugehörigen erkennbaren Elementen und angreifbaren Elementen verknüpft sind.

> **Hinweis:**
> Der Wert für erkennbare Elemente muss zwischen dem SIR-Incident und auch innerhalb von TISC übereinstimmen. Nur dann werden die zugehörigen erkennbaren Elemente oder Indikatoren im Abschnitt „Reaktion auf Security Incidents“ aufgeführt. Sie können die Datensätze auch verknüpfen und die Verknüpfung aufheben, indem Sie in den Quellsystemen nach Datensätzen suchen. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.

   - Wählen Sie einen beliebigen Datensatz aus, um im Quellsystem zu navigieren und die Details anzuzeigen. Beispiel: Zugeordnete erkennbare Elemente in Security Incident Response, um die Datensätze der zugehörigen erkennbaren Elemente abzurufen.
   - Im Rahmen des aktuellen Release können Sie die folgenden Intelligenzdaten aus den Quelldatensätzen (SIR) abrufen:
     - Zugehörige erkennbare Elemente
     - Angreifbare Elemente

b. **Geschäftskontext**: Zeigt die betroffenen Anwender und alle anderen Configuration Items an. Im Rahmen des aktuellen Release können Sie die folgenden Intelligenzdaten aus den Quelldatensätzen (Geschäftskontext) abrufen:
   - Konfigurationselemente
   - Betroffene Services
   - Betroffene Assets

c. **Vulnerability Response**: Zeigt die Schwachstellen-Intelligenzdaten an.

   Schwachstelleneinträge: Diese Option entspricht den Schwachstellen und ruft die zugehörigen Datensätze ab.

Führen Sie Ergänzungsaktionen über das erkennbare Element aus

Verwenden Sie diesen Abschnitt, um zu verstehen, wie Ergänzungsaktionen für erkennbare Elemente und andere Objekte ausgeführt werden.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Klicken Sie über die Schaltfläche „Teilen“ auf eine beliebige Ergänzungsaktion.
5. Wählen Sie die verfügbare(n) Implementierung(en) aus.
6. Klicken Sie auf **Absenden**.
   Beispiel: Bedrohungssuche ausführen. Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsmeldung angezeigt, dass die Ausführung der Ergänzung erkennbarer Elemente für für das/die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ausgewählte(n) erkennbare(n) Element(en) gestartet wurde. Ergebnisse sind auf der Detailseite des jeweiligen erkennbaren Elements verfügbar, sobald die Ausführung abgeschlossen ist.

Hinweis:
Sobald die Ausführung initiiert oder abgeschlossen ist, wird im Aktivitätenstrom der Formularansicht eine Arbeitsnotiz veröffentlicht.

Dem Fall hinzufügen

Fügen Sie dem Fall erkennbare Elemente, Indikatoren oder andere Objekte hinzu.

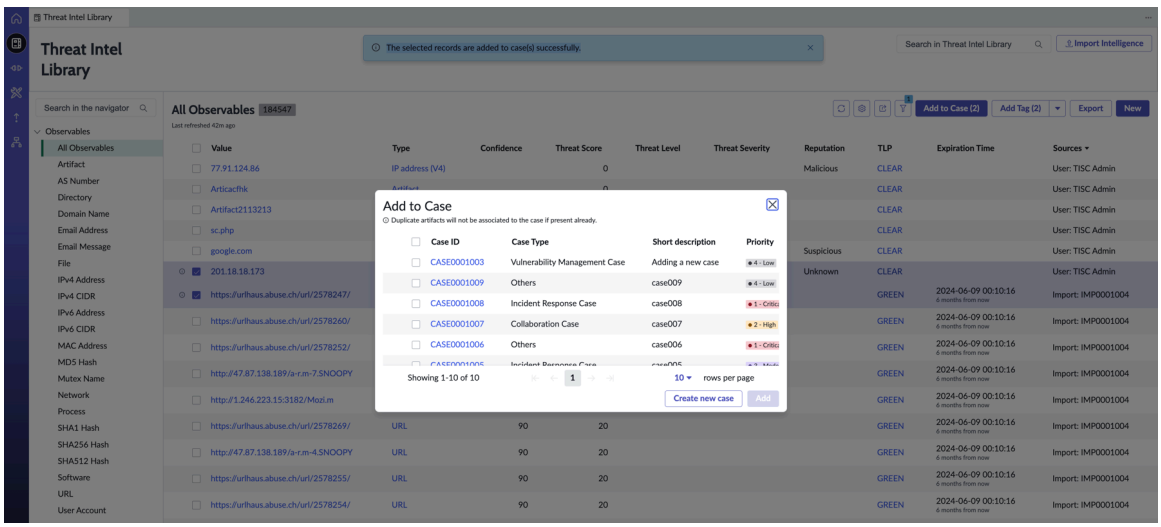
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Im Folgenden finden Sie das Verfahren zum Hinzufügen eines Falls zu einem Datensatz eines erkennbaren Elements.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
2. Wählen Sie das/die erkennbare(n) Element(e) aus.
3. Klicken Sie **auf die Schaltfläche Zu Fall hinzufügen**.
   Dadurch werden nur die Fälle angezeigt, bei denen der Datensatz noch nicht zugeordnet ist.



4. Überprüfen Sie, ob Sie den Datensatz den vorhandenen Fällen hinzufügen möchten, und wählen Sie in diesem Fall den vorhandenen Fall aus. Andernfalls klicken Sie auf **Neuen Fall erstellen**.
   Erstellen Sie einen neuen Fall, indem Sie die folgenden Informationen eingeben.

Neuen Fall erstellen

Feld	Beschreibung
Fall-ID	Ein eindeutiger Bezeichner für den Fall. Dies ist die vom System generierte ID.
Kurzbeschreibung	Zusammenfassung der Anforderung oder des Problems, die bzw. das untersucht wird, oder eine Kurzbeschreibung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Falltyp	Wählen Sie den Typ des untersuchten Falls aus. Die möglichen Optionen für die Untersuchung sind: ○ Bedrohungssuche ○ Informationsanforderung ○ Schwachstellenmanagement-Fall ○ Compliance-Fall ○ Fall vom Typ „Reaktion auf Incidents“ ○ Zusammenarbeitsfall ○ Andere
Priorität	Eine Bewertung des Schweregrads der Anforderung oder des Problems.
Zuweisungsgruppe	Die zugewiesene Gruppe, die für die Bearbeitung des Falls verantwortlich ist.
Zugewiesen an	Der für die Bearbeitung eines Falls verantwortliche Analyst

5. Klicken Sie auf **Erstellen**, wenn Sie einen neuen Fall erstellen.

> **Hinweis:**
> Der neue Fall wird der vorhandenen Fallliste hinzugefügt.

6. Wählen Sie die neu hinzugefügten Fälle aus.
7. Klicken Sie auf **Hinzufügen**.
   Eine Informationsmeldung wird angezeigt, dass die ausgewählten Datensätze erfolgreich dem Fall/den Fällen hinzugefügt wurden.

Führen Sie Ergänzungsvorgänge in TISC aus

In der folgenden Tabelle werden die Interaktionen beschrieben, die an der Ausführung verschiedener Ergänzungsvorgänge von TISC beteiligt sind.

Modale TISC-Bildschirme

Fähigkeit	Interaktionen mit UX-Frameworks	Integrationen unterstützt
Bedrohungssuche durchführen	Auf Bildschirm 1 – Implementierung(en) auswählen und übermitteln. Es gibt keine allgemeinen oder Implementierungsspezifischen Eingaben, die für	• Viren insgesamt • CrowdStrike Falcon Intelligence

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fähigkeit	Interaktionen mit UX-Frameworks	Integrationen unterstützt
	die Ausführung der Bedrohungssuche gelten.	
Sichtungssuche ausführen	Bildschirm 1 – Implementierungen auswählen und Bildschirm 2 – Allgemeine Eingaben sind anwendbar. Die Sichtungssuche verwendet Datum und Uhrzeit (Häufigkeit) als allgemeine Eingaben für mehrere Implementierungen von Splunk und anderen Integrationen.	• Elasticsearch • Splunk-Sichtung
Anreicherung erkennbarer Elemente durchführen	Nur Bildschirm 1 – Wählen Sie Implementierungen aus. Es gibt keine allgemeinen oder Implementierungsspezifischen Eingaben, die für die Ausführung der Anreicherung erkennbarer Elemente gelten.	• WHOIS • Shodan

Bedrohungssuche durchführen

Wählen Sie je nach Bedarf eine oder mehrere Implementierungen aus, um die Bedrohungssuche für erkennbare Elemente auszuführen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

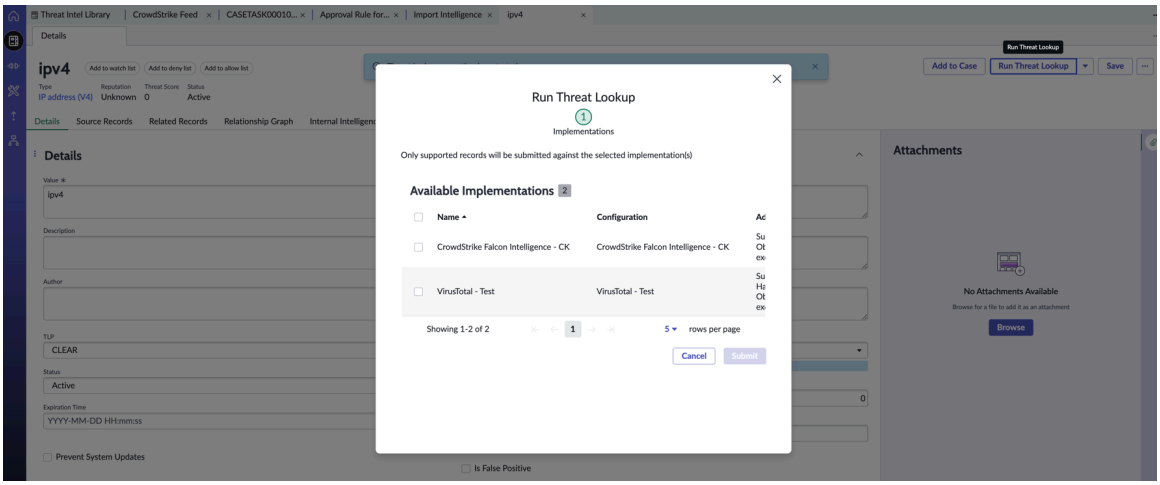
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Öffnen Sie einen beliebigen erkennbaren Datensatz.
5. Klicken Sie auf **Bedrohungssuche ausführen**.
   Der modale Bildschirm „Bedrohungssuche **– Implementierungen auswählen“** wird angezeigt.

   Hinweis:
   Mit Bedrohungssuche ausführen werden die Threat Intelligence-Suchen durchgeführt, um zu bestimmen, ob die erkennbaren Elemente bekannten Bedrohungen zugeordnet sind.

6. Wählen Sie die erforderliche(n) Implementierung(en) aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.
   Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsmeldung angezeigt, dass die Ausführung der Bedrohungssuche gestartet wurde.

Hinweis:

- Sobald die Ausführung initiiert oder abgeschlossen ist, wird im Aktivitätenstrom der Formularansicht eine Arbeitsnotiz veröffentlicht.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse finden Sie auf der Registerkarte **Ergänzungsergebnisse** der entsprechenden Detailseite für erkennbare Elemente im TISC-Arbeitsbereich.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse können anhand des Felds **Quelle** der Ergänzungsergebnistabelle identifiziert werden.

Sichtungssuche ausführen

Führt die zugehörige Integration „Sichtungssuche ausführen“ durch.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Wählen Sie zum Ausführen dieser Aktion die Implementierung aus, und fügen Sie allgemeine Laufzeiteingaben hinzu, die für alle ausgewählten Implementierungen gelten.

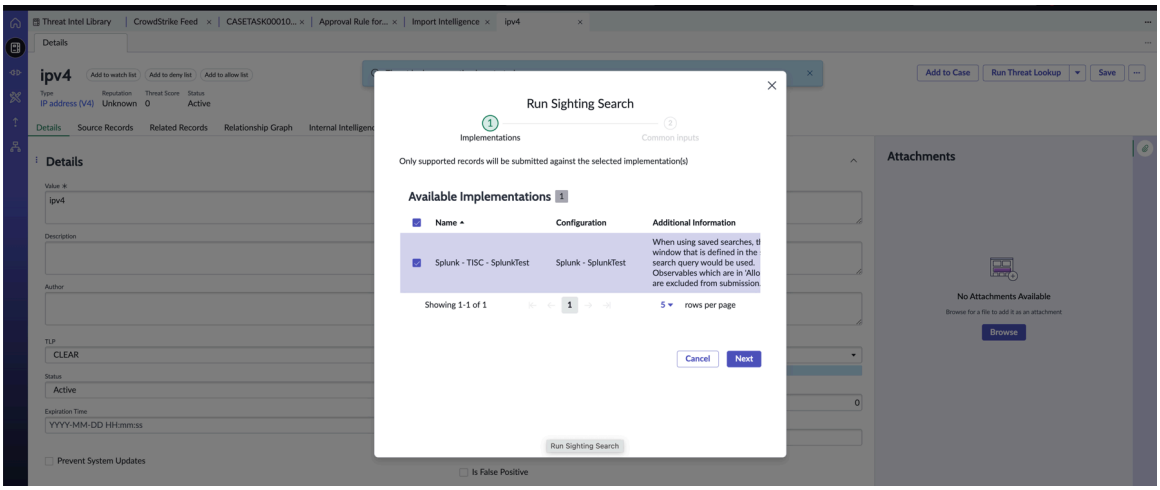
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Öffnen Sie einen beliebigen erkennbaren Datensatz.
5. Klicken Sie auf **Sichtungssuche ausführen**.
   Der modale Bildschirm „Sichtungssuche **– Implementierungen auswählen“** wird angezeigt.

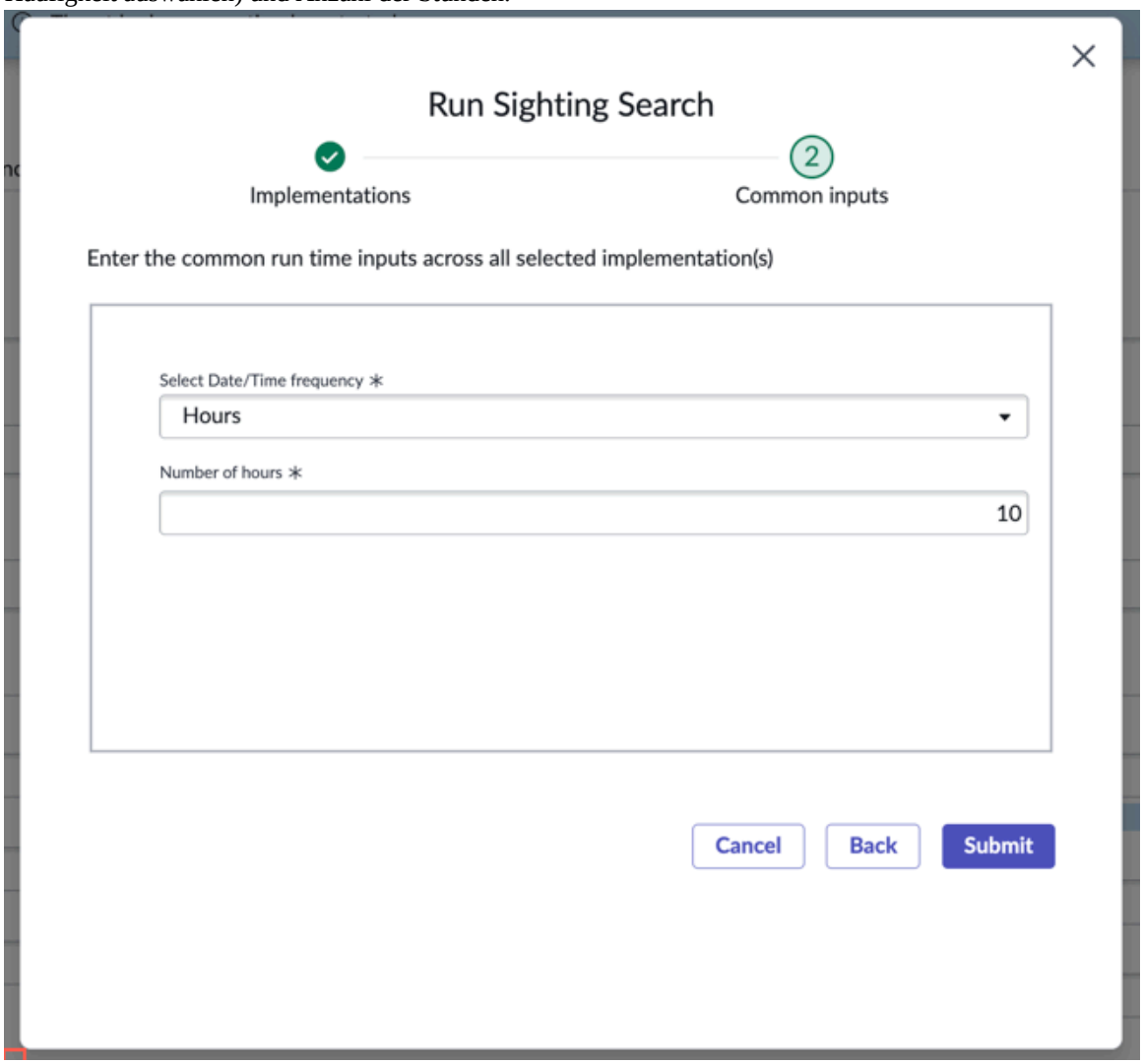
Hinweis:
Mit Sichtungssuche ausführen werden Threat Intelligence-Suchen durchgeführt, um zu bestimmen, ob die erkennbaren Elemente bekannten Bedrohungen zugeordnet sind.

6. Wählen Sie die erforderliche(n) Implementierung(en) aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie den allgemeinen Laufzeit-Eingabewert aus, z. B. Select Date/Time-Häufigkeit (Datum/Uhrzeit-Häufigkeit auswählen) und Anzahl der Stunden.



9. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsmeldung angezeigt, dass die Ausführung von „Sichtungssuche ausführen“ gestartet wurde.

Hinweis:

- Sobald die Ausführung initiiert oder abgeschlossen ist, wird im Aktivitätenstrom der Formularansicht eine Arbeitsnotiz veröffentlicht.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse finden Sie auf der Registerkarte **Ergänzungsergebnisse** der entsprechenden Detailseite für erkennbare Elemente im TISC-Arbeitsbereich.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse können anhand des Felds **Quelle** der Ergänzungsergebnistabelle identifiziert werden.

Anreicherung erkennbarer Elemente durchführen

Wählen Sie je nach Bedarf eine oder mehrere Implementierungen aus, um die Bedrohungssuche für erkennbare Elemente auszuführen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

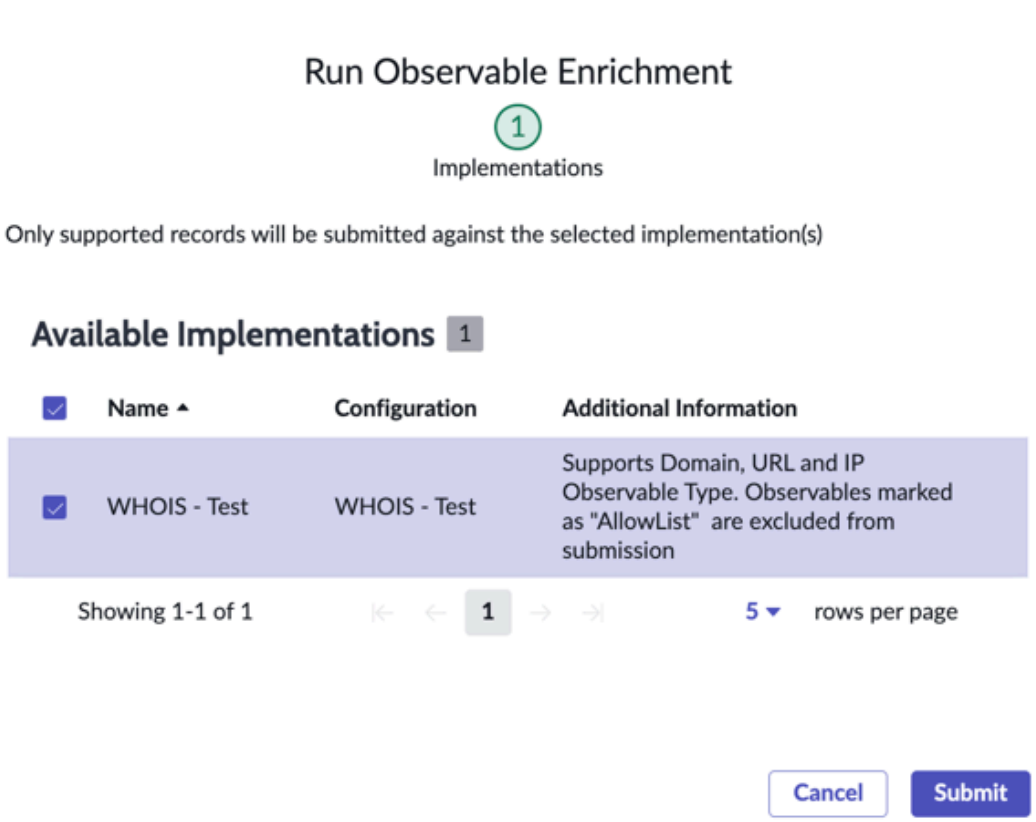
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie auf das Symbol **„Workbench für Bedrohungsanalysten“**.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
4. Öffnen Sie einen beliebigen erkennbaren Datensatz.
5. Klicken Sie auf **Anreicherung erkennbarer Elemente ausführen**.
   Der modale Bildschirm „Anreicherung erkennbarer Elemente **ausführen – Implementierungen auswählen“** wird angezeigt.

   Hinweis:
   Nur unterstützte Datensätze werden für die ausgewählte(n) Implementierung(en) übermittelt.

6. Wählen Sie die erforderliche(n) Implementierung(en) (z. B. WHOIS) aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.
Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsmeldung angezeigt, dass die Ausführung der Bedrohungssuche gestartet wurde.

Hinweis:

- Sobald die Ausführung initiiert oder abgeschlossen ist, wird im Aktivitätenstrom der Formularansicht eine Arbeitsnotiz veröffentlicht.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse finden Sie auf der Registerkarte **Ergänzungsergebnisse** der entsprechenden Detailseite für erkennbare Elemente im TISC-Arbeitsbereich.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse können anhand des Felds **Quelle** der Ergänzungsergebnistabelle identifiziert werden.

Datenanreicherungs-Ergebnisse anzeigen

Zeigen Sie erkennbare Elemente, Indikatoren und verschiedene Ergänzungsergebnisse für Objekte an.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**.
2. Wählen Sie einen beliebigen Datensatz eines erkennbaren Elements aus.
3. Wechseln Sie zur Registerkarte **Ergänzungsergebnisse**.
   Unter Ergänzungsergebnisse werden die Ergänzungsergebnisse der TISC-Integrationen angezeigt.

Ergänzungsname	Beschreibung
Bedrohungssuche – Ergebnisse	Listet alle zugehörigen Ergebnisse der Bedrohungssuche für ein erkennbares Element auf.
Sichtungen	Listet alle zugehörigen Sichtungen für ein erkennbares Element auf.
Erkennbare Elemente – Datenanreicherungs-Ergebnisse	Listet alle zugehörigen Datenanreicherungs-Ergebnisse erkennbarer Elemente für ein erkennbares Element auf.

Indikatoren

Indikatoren sind Artefakte, die in einem Netzwerk oder Betriebssystem beobachtet werden und wahrscheinlich einen Angriff anzeigen. Typische IoCs sind Virussignaturen und IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen.

Definieren Sie einen Indikator

Definieren Sie einen Indikator.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Indikatoren**.
2. Wählen Sie **Indikator**aus.
3. Klicken Sie auf **Neu**.

> **Hinweis:**
> Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

4. Füllen Sie die Felder des Formulars aus.

Abschnitt „Details“

Feld	Beschreibung
ID	Eindeutige ID des Indikators.
Beschreibung	Beschreibung des Indikators.
Name	Name des Indikators.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Muster	Das Erkennungsmuster für diesen Indikator kann als STIX-Muster ausgedrückt werden.
Mustertyp	Die in diesem Indikator verwendete Mustersprache.
Musterversion	Die Version der Mustersprache, die für die Daten in der Mustereigenschaft verwendet wird. Sie muss mit dem Typ der Musterdaten übereinstimmen, die in der Mustereigenschaft enthalten sind.
Gültig ab	Der Zeitpunkt, ab dem dieser Indikator als gültiger Indikator für das Verhalten betrachtet wird, mit dem er zusammenhängt oder das er darstellt.
Gültig bis	Die Zeit, nach der dieser Indikator nicht mehr als gültiger Indikator für die Verhaltensweisen betrachtet werden sollte, mit denen er zusammenhängt oder die er darstellt.
IoC-Klassifizierung	Die IoC-Klassifizierung der Indikatoren.
Indikatortypen	Gibt die verschiedenen Kategorien des Indikators an.
Status	Gibt den Status der Indikatoren an.
Plattformen	Definiert die Plattformen, für die dieser Indikator gilt.
TLP	Eindeutiger Wert, der die Vertraulichkeitseinstellung für Daten pro TLP angibt.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
Vertrauen	Geben Sie die Konfidenz für diesen Indikatordatensatz ein. Die Konfidenzeigenschaft gibt das Vertrauen des Erstellers in die Richtigkeit seiner Daten an. Der Konfidenzwert muss eine Zahl im Bereich von 0 bis 100 sein.
Bedrohungsstufe	Gibt die Bedrohungsstufe des Indikatordatensatzes an.
Ablaufzeit	Gibt die Ablaufzeit des Indikatordatensatzes an.
Bedrohungsschweregrad	Gibt den Bedrohungsschweregrad für den Indikatordatensatz an.
Nutzungskategorien	Kategorien, unter die das erkennbare Element fällt, z. B. Botnet oder Phishing.
Erstmals aufgetreten	Der Zeitpunkt, zu dem dieser Indikatordatensatz zum ersten Mal bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Zuletzt aufgetreten	Die Zeit, zu der dieser Indikatordatensatz zuletzt bei der Ausführung schädlicher Aktivitäten gesehen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für einen Indikator hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Indikator hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung des Indikators verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt die Zeit an, zu der der Indikator im System erstellt wird.
Aktualisiert	Gibt die Zeit an, zu der der Indikator im System aktualisiert wird.
Erweiterungen	Gibt die Erweiterungen des Indikators an.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Indikators dar.

5. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
6. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einem Indikator zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie die Taxonomie aus, die einem Indikator zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie die Taxonomiewerte hinzu, die einem Indikator zugeordnet sind.

Quelldatensätze

Feld	Beschreibung
Die Details der Quelldatensätze für einen Indikator werden angezeigt, falls vorhanden.	

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die den Indikatoren zugeordnet sind.

Zugehörige Datensätze

Zugehörige Liste	Beschreibung
Referenzen für Indikatoren	Liste der externen Referenzen, die diesen Indikator beschreiben.
Erkennbare Elemente	Listet die zugehörigen Datensätze erkennbarer Elemente auf, die sich auf diesen Indikator beziehen.
Indikatoren	Listet die Indikatoren auf, die sich auf diesen Indikator beziehen. **Hinweis:** Dieser Abschnitt enthält auch die möglichen Beziehungen zwischen zwei Indikatoren. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Indikator und potenziellem Indikator, und unter Definieren Sie Indikator-Indikator-Beziehungen finden Sie die bestätigten Beziehungen zwischen den beiden erkennbaren Elementen.
Konfigurationselemente	Listet die Konfigurationselemente auf, die sich auf diesen Indikator beziehen.
Angriffsmuster	Listet die Angriffsmusterquelle auf, die die Methoden beschreibt, mit denen Angreifer versuchen, Ziele zu gefährden, die mit diesem Indikator zusammenhängen.
Kampagnen	Listet die Kampagnenquelle auf, die eine Reihe von böswilligen Aktivitäten oder Angriffen beschreibt, die im Laufe der Zeit gegen eine bestimmte Gruppe von Zielen auftreten, die mit diesem Indikator zusammenhängen.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die sich auf diesen Indikator beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Zugehörige Liste	Beschreibung
Identitäten	Listet die Identitäten auf, die sich auf diesen Indikator beziehen.
Infrastruktur	Listet die Infrastrukturquelle auf, die alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen beschreibt, die einen Zweck eines Angriffs unterstützen sollen, der mit diesem Indikator zusammenhängt.
Angriffssätze	Listet eine Reihe von Verhaltensweisen und Ressourcen des Angreifers mit allgemeinen Eigenschaften auf, die sich auf diesen Indikator beziehen.
Standorte	Listet die geografischen Standorte auf, die dem Objekt zugeordnet sind.
Malware	Listet Malware-Quelldatensätze auf, die sich auf diesen Indikator beziehen.
Markierungsdefinitionen	Listet die Markierungsdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Datensätze der Sichtungsquelle auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet Changes auf, die dem erkennbaren Element zugeordnet sind.
Bedrohungsereignisse	Listet zugehörige erkennbare Elemente auf, die von der Bedrohungsquelle identifiziert wurden.
Tool	Listet das Tool auf, das diesem Objekt zugeordnet ist.
Schwachstellen	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die über eine übereinstimmende IP-Adresse verfügen.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Außerdem können Sie im Abschnitt **„Zugehörige Datensätze“** die Beziehungen zwischen zwei erkennbaren Elementen mithilfe des Abschnitts **„Potenzielle Beziehungen“** bestätigen, der in der Formularansicht „ **Indikatoren“** verfügbar ist. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
3. Sie können Indikatoren zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Angriffsmuster

Angriffsmuster sind eine Art von Taktiken, Techniken und Verfahren (TTPs), die die Methoden beschreiben, mit denen Angreifer versuchen, Ziele zu gefährden.

Angriffsmuster werden zur Kategorisierung von Angriffen verwendet. Sie verallgemeinern bestimmte Angriffe auf die Muster, denen sie folgen, und liefern detaillierte Informationen darüber, wie Angriffe durchgeführt werden.

Spear-Phishing ist beispielsweise eine häufige Art von Angriff, bei der ein Angreifer eine sorgfältig gestaltete E-Mail-Nachricht an eine Partei sendet, um sie dazu zu bringen, auf einen Link zu klicken oder einen Anhang zu öffnen, um Malware zu übermitteln. Angriffsmuster sind spezifischer, z. B. kann Spear-Phishing durch einen bestimmten Bedrohungsakteur (z. B. dass das Ziel einen Wettbewerb gewonnen hat) ein Angriffsmuster sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie ein Angriffsmuster

Definieren Sie ein Angriffsmuster, um Bedrohungsanalysten bei der Kategorisierung von Angriffen zu helfen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Navigieren Sie zu **Angriffsmuster**.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Detailansicht „Angriffsmuster“.

Feld	Beschreibung
ID	Eindeutige ID für ein Angriffsmuster.
Name	Geben Sie einen Namen für dieses Angriffsmuster ein.
Beschreibung	Geben Sie eine Beschreibung für ein Angriffsmuster ein.
Aliase	Alternative Namen zur Identifizierung dieses Angriffsmusters. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf das Symbol **„Neue Aliasse hinzufügen“**, das im Feld „Alias“ selbst verfügbar ist.
Angriffsphase	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
Berechtigungen erforderlich	Wählen Sie die erforderlichen Berechtigungen für dieses Angriffsmuster aus.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für diesen Angriffsmustermodus ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die Konfidenzeigenschaft gibt das Vertrauen des Erstellers in die Richtigkeit seiner Daten an. Der Konfidenzwert muss eine Zahl im Bereich von 0 bis 100 sein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.
Systemupdates verhindern	Wenn Sie diese Kennzeichnung auf „wahr“ festlegen, kann das System die Werte von Feldern im Datensatz nicht überschreiben.

Wichtig:
Nachdem Sie einen neuen Objektdatensatz erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für ein Angriffsmuster hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts (Angriffsmuster) verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt die Zeit an, zu der der Datensatz im System erstellt wird.
Aktualisiert	Gibt den Zeitpunkt an, zu dem der Datensatz im System geändert wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Angriffsmuster.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einem erkennbaren Element zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die einem Angriffsmuster zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die einem Angriffsmuster zugeordnet sind.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffsmuster zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Kampagne

Eine Kampagne wird als Gruppierung von Angreiferverhalten definiert. Sie beschreibt eine Reihe von böswilligen Aktivitäten oder Angriffen, die manchmal als „Waves“ bezeichnet werden und über einen Zeitraum hinweg gegen eine bestimmte Gruppe von Zielen auftreten.

Kampagne definieren

Definieren Sie eine Kampagne, um das Verhalten von Angreifern zu gruppieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Kampagnenobjekt**.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Kampagnenansicht

Feld	Beschreibung
ID	Eindeutige ID für konträres Verhalten.
Name	Geben Sie einen Namen für ein konträres Verhalten ein.
Beschreibung	Geben Sie eine Beschreibung für diese Kampagne ein.
Ziel	Primäres Ziel, Ziel, gewünschtes Ergebnis oder beabsichtigte Wirkung der Kampagne Was der Bedrohungsakteur oder Angriffssatz mit dieser Kampagne erreichen möchte.
Aliase	Alternative Namen zur Identifizierung für diese Kampagne. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf das Symbol **„Neue Aliasse hinzufügen“**, das im Feld „Alias“ selbst verfügbar ist.
TLP	Traffic Light Protocol (TLP) gibt an, welche vertraulichen Informationen mit der richtigen Zielgruppe geteilt werden. Es verwendet vier Farben (weiß, grün, gelb und rot), um unterschiedliche Empfindlichkeitsgrade für dieses Angriffsmuster anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Kampagne ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für eine Kampagne hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie einen zusätzlichen Kontext für diese Kampagne hinzu.
Erstmals aufgetreten	Die Zeit, zu der dieses Objekt zum ersten Mal ein Angreiferverhalten beobachtet hat.
Zuletzt aufgetreten	Die Uhrzeit, zu der dieses Objekt zuletzt bei der Ausführung eines Angreiferverhaltens gesehen wurde.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Kampagne

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einer Kampagne zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die einer Kampagne zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Kampagne zugeordnet sind.

Nächste Maßnahme
Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die der Kampagne zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Vorgehensweise

Eine Vorgehensweise ist eine Aktion, die ausgeführt wird, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren.

Vorgehensweisen beschreibt technische oder automatisierte Antworten (Patches anwenden, Firewalls neu konfigurieren). Es kann auch Aktionen auf höherer Ebene wie Mitarbeiterschulungen oder Richtlinienänderungen beschreiben.

Zum Beispiel könnte eine Vorgehensweise zum Mindern einer Schwachstelle das Anwenden des Patches beschreiben, der die Schwachstelle behebt.

Definieren Sie die Vorgehensweise

Definieren Sie eine Vorgehensweise, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum Objekt **der Vorgehensweise**.
4. Klicken Sie auf **Neu**.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Detailansicht der Vorgehensweise

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Name	Geben Sie einen beschreibenden Namen für diese Vorgehensweise ein.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Vorgehensweise enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Aktion	Um strukturierte oder automatisierte Vorgehensweisen zu erfassen.
TLP	Traffic Light Protocol (TLP) gibt an, welche vertraulichen Informationen mit der richtigen Zielgruppe geteilt werden. Es verwendet vier Farben (weiß, grün, gelb und rot), um unterschiedliche Empfindlichkeitsgrade für dieses Angriffsmuster anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für eine Vorgehensweise hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einem erkennbaren Element zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die einem Angriffsmuster zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die einem Angriffsmuster zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Vorgehensweise zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Identität

Identitäten stellen tatsächliche Personen, Organisationen oder Gruppen und Klassen von Personen, Systemen oder Gruppen dar. Identitäten gelten für STIX 2.x.

Ein Identitäts-SDO kann grundlegende Identifizierungsinformationen, Kontaktinformationen und die Sektoren erfassen, zu denen die Identität gehört. Identität stellt Angriffsziele, Informationsquellen, Objektersteller und Bedrohungsakteuridentitäten dar.

Definieren Sie Identitäten

Definieren Sie Identitäten, die tatsächliche Personen, Organisationen oder Gruppen darstellen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Identitätsobjekt**.
4. Klicken Sie auf **Neu**.

Hinweis:

Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Ansicht „Identitätsdetails“.

Feld	Beschreibung
ID	Eindeutige ID für eine Identität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für diese Identität ein. Wenn sie sich auf eine bestimmte Entität (eine Einzelperson oder Organisation) bezieht, muss diese Eigenschaft den kanonischen Namen dieser bestimmten Entität enthalten.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Vorgehensweise enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Rollen	Liste der Rollen, die diese Identität ausführt.
Identitätsklasse	Der Typ der Entität, den diese Identität beschreibt. Zum Beispiel Einzelperson oder Organisation.
Sektoren	Die Liste der Branchen, zu denen diese Identität gehört.
Kontaktinformationen	Die Kontaktinformationen wie E-Mail-Adresse und Telefonnummer für diese Identität.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen mit der entsprechenden Zielgruppe geteilt werden. Es verwendet vier Farben (weiß, grün, gelb und rot), um unterschiedliche Vertraulichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Identität ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für die Identität hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext im Zusammenhang mit dieser Identität hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Identität zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die der Identität zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Identität zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Identität zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die mit diesem Objekt verknüpft ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Infrastruktur

Infrastructure SDO stellt eine Art von Taktiken, Techniken und Verfahren (TTPs) dar. Sie beschreiben alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die einen Zweck eines Angriffs unterstützen sollen. Infrastruktur gilt für STIX 2.x.

Die Elemente eines Angriffs werden durch andere SDOs oder SCOs dargestellt. Das Infrastruktur-SDO stellt jedoch eine benannte Gruppe von Daten dar, die die Infrastruktur bilden.

Beispiele für Infrastrukturen sind C2-Server, die bei einem Angriff verwendet werden, Geräte oder Server, die Teil einer Abwehr sind, oder Datenbankserver, die Ziel eines Angriffs sind.

Definieren Sie die Infrastruktur

Definieren Sie eine Infrastruktur, bei der es sich um alle Systeme, Softwareservices und zugehörigen physischen oder virtuellen Ressourcen handelt, die einen Zweck eines Angriffs unterstützen sollen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Navigieren Sie zum **Infrastrukturobjekt**.
4. Klicken Sie auf **Neu**.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht „Infrastrukturdetails“.

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Name	Geben Sie einen beschreibenden Namen für diese Vorgehensweise ein. Wenn sie sich auf eine bestimmte Entität (eine Einzelperson oder Organisation) bezieht, muss diese Eigenschaft den kanonischen Namen dieser bestimmten Entität enthalten.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Infrastruktur enthält, möglicherweise einschließlich ihres Zwecks, ihrer Verwendung, ihrer Beziehung zu anderen Intelligence-Aktivitäten, die in zugehörigen Objekten erfasst werden, und ihrer wichtigsten Merkmale.
Infrastrukturtypen	Beschreibt die Kategorisierung der Infrastruktur.
Aliase	Alternative Namen zur Identifizierung dieser Infrastruktur. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf das Symbol **„Neue Aliasse hinzufügen“**, das im Feld „Alias“ selbst verfügbar ist.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Erstmals aufgetreten	Der Zeitpunkt, zu dem diese Infrastruktur zum ersten Mal bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Zuletzt aufgetreten	Die Uhrzeit, zu der diese Infrastruktur zuletzt bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Infrastruktur hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Infrastruktur hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt den Zeitpunkt an, zu dem der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Infrastruktur zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Infrastruktur zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Infrastruktur zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Identität zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Angriffssatz

Ein Angriffssatz ist ein gruppierter Satz von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften. Ein Angriffssatz betrifft normalerweise eine einzelne Organisation. Der Angriffssatz gilt für STIX 2.x.

Ein Angriffssatz kann mehrere Kampagnen oder andere Aktivitäten erfassen. Diese Aktivitäten teilen Attribute, die auf einen allgemein bekannten oder unbekannten Bedrohungsakteur hindeuten.

Neue Aktivität kann einem Angriffssatz zugeordnet werden, auch wenn die Bedrohungsakteure hinter dem Angriff nicht bekannt sind. Bedrohungsakteure können von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Unterstützung eines Angriffssatzes zu einem anderen oder mehreren Angriffssätzen übergehen.

Ein Angriffssatz ist das gesamte Angriffspaket und kann über einen längeren Zeitraum in mehreren Kampagnen verwendet werden, um potenziell mehrere Zwecke zu erreichen.

Definieren Sie den Angriffssatz

Definieren Sie einen Angriffssatz, bei dem es sich um einen gruppierten Satz von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften handelt.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Navigieren Sie zu **Angriffssatz**.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Ansicht Angriffssatzdetails

Feld	Beschreibung
ID	Eindeutige ID für einen Angriffssatz.
Name	Geben Sie einen beschreibenden Namen für diesen Angriffssatz ein. Wenn sie sich auf eine bestimmte Entität (eine Einzelperson oder Organisation) bezieht, muss diese Eigenschaft den kanonischen Namen dieser bestimmten Entität enthalten.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Aliase	Alternative Namen zur Identifizierung dieses Angriffssatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf das Symbol **„Neue Aliasse hinzufügen“**, das im Feld „Alias“ selbst verfügbar ist.
Ziele	Die übergeordneten Ziele dieses Angriffssatzes, d. h. was versucht wird. Zum Beispiel kann ihr persönliches Gewinnziel ihre Motivation sein, aber ihr Ziel besteht darin, Kreditkartennummern zu stehlen. Zu diesem Zweck können sie bestimmte Kampagnen mit detaillierten Zielen ausführen, z. B. die Gefährdung der Point-of-Sale-Systeme bei einem großen Einzelhandelsunternehmen.
Erstmals aufgetreten	Der Zeitpunkt, zu dem dieser Angriffssatz zum ersten Mal bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Zuletzt aufgetreten	Die Zeit, zu der dieser Angriffssatz zuletzt bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Primäre Motivation	Primärer Grund, primäre Motivation oder Zweck hinter diesem Angriffssatz. Die Motivation besteht darin, warum der Angriffssatz das Ziel erreichen möchte (was er zu erreichen versucht).
Sekundäre Motivationen	Die sekundären Gründe, Motivationen oder Zwecke hinter diesem Angriffssatz. Diese Motivationen können als gleiche oder fast gleiche Ursache zur primären Motivation existieren. Sie ersetzt jedoch nicht die primäre Motivation und erhöht sie auch nicht unbedingt, sondern kann auf zusätzlichen Kontext hindeuten. Die Position in der Liste hat keine Bedeutung.
Ressourcenebene	Diese Eigenschaft gibt die Organisationsebene an, auf der dieser Angriffssatz normalerweise funktioniert, was wiederum die für diesen Angriffssatz zur Verwendung in einem Angriff verfügbaren Ressourcen bestimmt.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für diesen Angriffssatz ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diesen Angriffssatz hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Angriffssatz hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt den Zeitpunkt an, zu dem der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Angriffssatz zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Angriffssatz zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Angriffssatz zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffssatz zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Standort

Ein Standort stellt einen geografischen Standort dar. Standorte werden hauptsächlich verwendet, um anderen SDOs Kontext zu geben. Standorte gelten für STIX 2.x.

Der Standort kann einige oder alle der folgenden Angaben enthalten: Region (Nordamerika), Bürgeradresse (New York, USA), Breitengrad und Längengrad.

Die Standort-SDO kann sich auf eine Identität oder einen Angriffssatz beziehen, um anzuzeigen, dass sich die Identität oder der Angriffssatz an diesem Standort befindet. Es kann sich auch auf eine Malware oder ein Angriffsmuster beziehen, um anzuzeigen, dass sich das Zielopfer an einem bestimmten Ort befindet.

Beispielsweise könnte ein Standort in einer Beziehung verwendet werden, um zu beschreiben, dass der Angriffssatz „Bourgeis Swallow“ aus Osteuropa stammt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mindestens eine der folgenden Eigenschaften oder Eigenschaftssätze muss angegeben werden:

- region
- country
- Breitengrad und Längengrad

Definieren Sie den Standort

Definieren Sie einen geografischen Standort, um anderen SDOs mehr Kontext bereitzustellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Standortobjekt**.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus

Ansicht „Identitätsdetails“.

Feld	Beschreibung
ID	Eindeutige ID für den Standort.
Name	Geben Sie einen beschreibenden Namen ein, um den Standort zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Breitengrad	Der Breitengrad des Standorts in Dezimalgraden. Positive Zahlen beschreiben Breitengrade nördlich des Ääquators, und negative Zahlen beschreiben Breitengrade unterhalb des Äquators. Der Wert dieser Eigenschaft muss zwischen -90,0 und 90,0 liegen.
Längengrad	Der Längengrad des Standorts in Dezimalgraden. Positive Zahlen beschreiben Längengrade östl. des Nullmeridian und negative Zahlen beschreiben Längengrade West des Nullmeridian.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss zwischen -180,0 und 180,0 (einschließlich) liegen.
Genauigkeit	Definiert die Genauigkeit der durch die Eigenschaften für den Breiten- und Längengrad angegebenen Koordinaten. Diese wird in Zählern gemessen. Der tatsächliche Standort kann bis zu einer Genauigkeit von mehreren Zählern vom definierten Punkt entfernt sein. Wenn diese Eigenschaft nicht vorhanden ist, ist die Genauigkeit nicht angegeben. Wenn diese Eigenschaft vorhanden ist, müssen die Eigenschaften für den Breitengrad und den Längengrad vorhanden sein.
Region	Die Region, in der sich dieser Standort befindet.
Land	Das Land, in dem sich dieser Standort befindet.
Verwaltungsgebiet	Das Bundesland, die Provinz oder ein anderes subnationales Verwaltungsgebiet, in dem sich dieser Standort befindet.
Stadt	Die Stadt, in der sich dieser Standort befindet.
Straße und Hausnummer	Straße, die von diesem Standort beschrieben wird. Diese Eigenschaft enthält alle Aspekte oder Teile der Straße.
Postleitzahl	Die Postleitzahl, in der sich dieser Ort befindet.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Standort hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Speicherort hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Durchwahlen für diesen Standort an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt den Zeitpunkt an, zu dem der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Standort zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Standort zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Standort zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Standort zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Malware

Malware ist eine Art von TTP, die schädlichen Code darstellt. Bezieht sich auf ein Programm, das heimlich in ein System eingefügt wird. Malware gilt für STIX 2.x.

Der Zweck einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Die Malware-SDO charakterisiert, identifiziert und kategorisiert Malware-Instanzen und -Familien aus Daten, die aus der Analyse abgeleitet werden. Dieses SDO erfasst detaillierte Informationen darüber, wie die Malware funktioniert und was sie tut.

Definieren Sie Malware

Definieren Sie eine Malware, die schädlichen Code darstellt.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Navigieren Sie zum Objekt **„Malware** Threat Intel“.
4. Klicken Sie auf **Neu**.

   Hinweis:
   Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht „Malware-Details“.

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der Malware-Instanz.
Name	Geben Sie einen Namen ein, um die Malware-Instanz oder -Familie zu identifizieren, wie vom Hersteller des SDO angegeben. Für eine Schadsoftwarefamilie muss der Name definiert werden.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Malware-Instanz oder -Familie enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Schadsoftwaretypen	Gibt die verschiedenen Kategorien der Malware an.
Ist Familie	Aktivieren Sie dieses Kontrollkästchen, um anzugeben, ob das Objekt eine Malware-Familie oder eine Malware-Instanz darstellt.
Aliase	Die alternativen Namen, die zur Identifizierung dieser Malware oder Malware-Familie verwendet werden. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf das Symbol **„Neue Aliasse hinzufügen“**, das im Feld „Alias“ selbst verfügbar ist.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
Erstmals aufgetreten	Der Zeitpunkt, zu dem diese Malware-Instanz oder -Familie zum ersten Mal bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Zuletzt aufgetreten	Die Uhrzeit, zu der diese Malware-Instanz oder -Familie zuletzt bei der Ausführung schädlicher Aktivitäten beobachtet wurde
Prozessarchitekturen	Gibt die Prozessarchitekturen für diese Malware an.
Implementierungssprachen	Gibt die Implementierungssprachen für diese Malware an.
Malware-Fähigkeiten	Die Fähigkeiten, die von einer Malware-Instanz oder -Familie gezeigt werden können.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für diese Malware ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für den Malware-Datensatz hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Malware-Datensatz hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Malware.
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Malware zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die der Malware zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Malware zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Malware zugeordnet sind.

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die mit dieser Malware zusammenhängen.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die geografischen Kontext für dieses Objekt bieten.
Malware-Analyse	Listet Malware-Analysedatensätze auf, die diesem Objekt zugeordnet sind.
Malware	Listet Malware-Datensätze auf, die diesem Objekt zugeordnet sind.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Malware-Analyse

Die Malware-Analyse erfasst die Metadaten und Ergebnisse einer Malware. Die Malware-Analyse gilt für STIX 2.x.

Die Malware-Analyse umfasst statische oder dynamische Analysen, die für eine Malware-Instanz oder -Familie durchgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie die Malware-Analyse

Definieren Sie eine Malware-Analyse, die die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse erfasst, die für eine Malware-Instanz oder -Familie ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Malware-Analyseobjekt**.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Ansicht „Malware-Analysedetails“.

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der Malware-Analyse.
Produkt	Name der verwendeten Analyse-Engine oder des Produkts. Produktnamen MÜSSEN in Kleinbuchstaben angegeben werden, wobei die Wörter durch einen Bindestrich „-“ getrennt sind. In Fällen, in denen der Name eines Produkts nicht angegeben werden kann, muss der Wert „anonymisiert“ verwendet werden.
Version	Die Version des Analyseprodukts, das zur Durchführung der Analyse verwendet wurde.
Host-VM	Eine Beschreibung der VM-Umgebung, die zum Hosten des Gastbetriebssystems verwendet wird, falls zutreffend, die für die dynamische Analyse der Malware-Instanz oder -Familie verwendet wurde. Wenn dieser Wert nicht in Verbindung mit der Eigenschaft „operating_system_ref“ enthalten ist, bedeutet dies, dass die dynamische Analyse möglicherweise für Bare-Metal-Modelle (also ohne Virtualisierung) durchgeführt wurde oder die Informationen geschwärzt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft MUSS der Bezeichner für ein SCO-Softwareobjekt sein.
Betriebssystem	Das Betriebssystem, das für die dynamische Analyse der Malware-Instanz oder -Familie verwendet wird. Dies gilt sowohl für virtualisierte Betriebssysteme als auch für solche, die auf Bare-Metal-Basis ausgeführt werden. Der Wert dieser Eigenschaft MUSS der Bezeichner für ein SCO-Softwareobjekt sein.
Konfigurationsversion	Die alternativen Namen, die zur Identifizierung dieser Malware oder Malware-Familie verwendet werden.
Module	Die spezifischen Analysemodule, die während dieser Analyseausführung im Produkt verwendet und konfiguriert wurden.
Analyse-Engine-Version	Die Version der Analyse-Engine oder des Produkts (einschließlich AV-Engines), die zur Durchführung der Analyse verwendet wurde.
Analysedefinitionsversion	Die Version der Analysedefinitionen, die vom Analysetool einschließlich AV-Tools verwendet werden.
Analyse gestartet	Datum und Uhrzeit der Initiierung der Malware-Analyse.
Analyse beendet	Datum und Uhrzeit des Endes der Malware-Analyse.
Ergebnis	Das Klassifizierungsergebnis, wie durch den Scanner- oder Toolanalyseprozess bestimmt.
Ergebnisname	Klassifizierungsergebnis oder Name, der der Malware-Instanz vom Scanner-Tool zugewiesen wurde.
Eingereicht	Datum und Uhrzeit, zu der die Malware zum Scannen oder zur Analyse übermittelt wurde. Dieser Wert bleibt unverändert, während sich das Scandatum ändern kann. Zum Beispiel, wenn Malware an ein Virenanalysetool übermittelt wurde.
Analysiertes erkennbares Element	Wählen Sie das erkennbare Element aus, das analysiert wurde.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für diese Malware-Analyse ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für den Datensatz der Malware-Familie hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Malware-Datensatz hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Malware.
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Malware zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die der Malware zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Malware zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Malware zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Malware	Listet Malware-Datensätze auf, die diesem Objekt zugeordnet sind.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Objektsichtung

Sichtungen zeigen an, dass ein Objekt gesehen wurde. Objekte können Malware, ein Tool, ein Bedrohungsakteur usw. sein.

Sichtungen erfassen, wer und was das Ziel ist, wie Angriffe durchgeführt werden und Trends beim Angriffsverhalten.

Das Sichtungsbeziehungsobjekt enthält zusätzliche Eigenschaften, die in den generischen Beziehungsobjekten nicht vorhanden sind. Diese zusätzlichen Eigenschaften stellen spezifische Daten für Sichtungsbeziehungen dar.

Definieren Sie die Objektsichtung

Definieren Sie eine Objektsichtung, die beschreibt, dass ein Objekt (Malware, Tool, Bedrohungsakteur usw.) erkannt wurde.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Objekt** Sichtungsobjekt.
4. Klicken Sie auf **Neu**.

   Hinweis:
   Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie Entität und Wert

Feld	Beschreibung
Entität	Wählen Sie den Entitätsobjekt-Sichtungsdatensatz aus. **Hinweis:** Während der Erstellung eines neuen Objektsichtungsdatensatzes ist für die Zusammenfassung ein zugehöriger Beziehungsdatensatz erforderlich.
Sichtung von	Gibt an, dass eine bestimmte Entität oder ein bestimmter Indikator in einer Umgebung beobachtet wurde, was ein Hinweis auf eine potenzielle Bedrohung sein kann. **Hinweis:** Wählen Sie den zugehörigen Datensatz der Sichtung aus, der dem im Feld „Entität“ ausgewählten Objekt zugeordnet ist, damit jetzt zugehörige Datensätze erstellt und die Sichtungsdatensätze zusammengefasst werden können.

Ansicht „Objektsichtungsdetails“.

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Sichtung enthält.
Erstmals aufgetreten	Beginn des Zeitfensters, in dem das SDO, auf das verwiesen wird, von dem die Eigenschaft gesehen wurde.
Zuletzt aufgetreten	Das Ende des Zeitfensters, in dem das SDO, auf das verwiesen wird, von dem die Eigenschaft gesehen wurde.
Anzahl	Falls vorhanden, muss eine ganze Zahl zwischen 0 und 999.999.999 (einschließlich) angegeben werden und gibt an, wie oft das SDO referenziert wurde, von dem die Eigenschaft referenziert wurde.
Ist Zusammenfassung	Gibt an, ob die Sichtung als Zusammenfassungsdaten betrachtet werden soll. Zusammenfassungsdaten sind eine Zusammenfassung früherer Sichtungsberichte und sollten nicht als primäre Quelldaten betrachtet werden.
Ist intern	Gibt an, ob die Sichtung intern ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diesen Angriffssatz hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

> **Wichtig:**
> Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.
>
> Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Identität zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Infrastruktur zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Infrastruktur zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Objektsichtung zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Objekte	Listet die Objekte auf, die den Sichtungen zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Beobachtete Daten

Beobachtete Daten vermitteln Informationen über Cybersicherheits-bezogene Entitäten wie Dateien, Systeme und Netzwerke mithilfe der STIX Cyber-observable Objects (SCOs). Beobachtete Daten gelten für STIX 2.x.

Unter „Beobachtete Daten“ wird sowohl eine einzelne Beobachtung einer einzelnen Entität (Datei, Netzwerkverbindung) als auch die Zusammenfassung mehrerer Beobachtungen einer Entität erfasst.

Sie können Beobachtete Daten allein (ohne Beziehungen) verwenden, um Rohdaten zu übermitteln, die aus einer beliebigen Quelle gesammelt wurden. Quellen umfassen Analystenberichte, Sandboxen sowie netzwerk- und hostbasierte Erkennungstools.

Beispielsweise können Beobachtete Daten Informationen über eine IP-Adresse, eine Netzwerkverbindung, eine Datei oder einen Registrierungsschlüssel erfassen. Beobachtete Daten sind keine Intelligenzaussage, es sind einfach die Rohinformationen ohne Kontext für das, was sie bedeuten.

Beobachtete Daten definieren

Vermittelt Informationen über Entitäten im Zusammenhang mit der Cybersicherheit wie Dateien, Systeme und Netzwerke mithilfe der STIX Cyber-observable Objects (SCOs).

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum Objekt **„Beobachtete Daten“**.
4. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Detailansicht „Beobachtete Daten“.

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der beobachteten Daten.
Zuerst beobachtet	Der Zeitpunkt, zu dem die Daten zum ersten Mal angezeigt wurden.
Zuletzt beobachtet	Zeitpunkt, zu dem die Daten zuletzt gesehen wurden.
Beobachtete Anzahl	Die Häufigkeit, mit der jedes erkennbare Cyber-Objekt gesehen wurde. Der Wert muss eine ganze Zahl von 1 bis 999.999.999 sein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für die beobachteten Daten ein
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese beobachteten Daten hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese beobachteten Daten hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die den beobachteten Daten zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesen beobachteten Daten zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesen beobachteten Daten zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den beobachteten Daten zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
	wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsakteur

Bedrohungsakteure sind Einzelpersonen, Gruppen oder Organisationen, die mit böswilligen Absichten handeln. Bedrohungsakteure gelten für STIX 2.x.

Ein Bedrohungsakteur ist kein Angriffssatz, kann aber im Laufe der Zeit verschiedene Angriffssätze, Gruppen oder Organisationen unterstützen oder mit ihnen verbunden sein.

Bedrohungsakteure verwenden ihre Ressourcen und die Ressourcen eines Angriffssatzes, um Angriffe durchzuführen und Kampagnen gegen Ziele auszuführen.

Sie können Bedrohungsakteure anhand ihrer Beweggründe, Fähigkeiten, Ziele, ihres Reifegrads, vergangener Aktivitäten, der Ressourcen, auf die sie Zugriff haben, und ihrer Rolle in der Organisation identifizieren.

Definieren Sie den Bedrohungsakteur

Definieren Sie Bedrohungsakteure, bei denen es sich um Einzelpersonen, Gruppen oder Organisationen handelt, die mit böswilligen Absichten handeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Bedrohungsakteurobjekt**.
4. Klicken Sie auf **Neu**.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Detailansicht des Bedrohungsakteurs

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Name	Geben Sie einen beschreibenden Namen ein, um den Standort zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Aliase	Eine Liste mit weiteren Namen zur Identifizierung dieses Bedrohungsakteurs **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf das Symbol **„Neue Aliasse hinzufügen“**, das im Feld „Alias“ selbst verfügbar ist.
Ziele	Die übergeordneten Ziele dieses Bedrohungsakteurs, d. h. was er zu tun versucht. Zum Beispiel kann ihr persönliches Gewinnziel ihre Motivation sein, aber ihr Ziel besteht darin, Kreditkartennummern zu stehlen.
Bedrohungsakteurtypen	Die Typen dieses Bedrohungsakteurs.
Bedrohungsakteurrollen	Die verschiedenen Bedrohungsakteurrollen für dieses Objekt.
Erstmals aufgetreten	Zeitpunkt, zu dem dieser Bedrohungsakteur zum ersten Mal aufgetreten ist. Diese Eigenschaft ist eine Zusammenfassungseigenschaft von Daten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	aus Sichtungen und anderen Daten, die in STIX möglicherweise nicht verfügbar sind. Wenn neue Sichtungen empfangen werden, die vor dem ersten gesehenen Zeitstempel liegen, kann das Objekt aktualisiert werden, um die neuen Daten zu berücksichtigen.
Zuletzt aufgetreten	Zeitpunkt, zu dem dieser Bedrohungsakteur zuletzt gesehen wurde.
Primäre Motivation	Primärer Grund, primäre Motivation oder Zweck hinter diesem Bedrohungsakteur. Die Motivation gibt an, warum der Bedrohungsakteur das Ziel erreichen möchte (was er zu erreichen versucht). Zum Beispiel könnte ein Bedrohungsakteur, der das Ziel hat, den Finanzsektor eines Landes zu stören, durch ideologischen Hass auf Kapitalismus geleitet werden.
Ausgereiftheit	Fähigkeit, spezifisches Wissen, spezielle Schulung oder Fachwissen, die ein Bedrohungsakteur für den Angriff benötigt.
Sekundäre Motivationen	Diese Eigenschaft gibt die sekundären Gründe, Motivationen oder Zwecke hinter diesem Bedrohungsakteur an. Diese Motivationen können als gleiche oder fast gleiche Ursache zur primären Motivation existieren. Sie ersetzt jedoch nicht die primäre Motivation und erhöht sie auch nicht unbedingt, sondern kann auf zusätzlichen Kontext hindeuten. Die Position in der Liste hat keine Bedeutung.
Ressourcenebene	Die Organisationsebene, auf der dieser Bedrohungsakteur normalerweise arbeitet, was wiederum die Ressourcen bestimmt, die diesem Bedrohungsakteur für einen Angriff zur Verfügung stehen. Dieses Attribut ist mit der Ausgereiftheitseigenschaft verknüpft – eine bestimmte Ressourcenebene impliziert, dass der Bedrohungsakteur Zugriff auf mindestens eine bestimmte Ausgereiftheitsstufe hat.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diesen Bedrohungsakteur hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

Automatische Übersetzung

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Bedrohungsakteur zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Bedrohungsakteur zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Bedrohungsakteur zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungsakteur zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die zur Kategorisierung von Angriffen dienen, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Liste der Standorte, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsereignis

Ein Ereignis oder eine Situation, das bzw. die möglicherweise unerwünschte Konsequenzen oder Auswirkungen hat.

Ein Hacker, der eine Website angreift, ist ein Bedrohungsereignis. Wenn es den Hackern gelänge, eine Website zu beschädigen oder Informationen zu stehlen, wird dies als Bedrohungsereignis definiert.

Definieren Sie das Bedrohungsereignis

Definieren Sie ein Bedrohungsereignis, wenn ein Ereignis auftritt, das zu nicht autorisiertem Zugriff auf nicht öffentliche Informationen und deren Beschaffung oder zur Störung oder zum Missbrauch eines Informationssystems führt.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum Objekt **„Bedrohungsereignis“**.
4. Klicken Sie auf **Neu**.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Detailansicht des Bedrohungsakteurs

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Bedrohungsereignisses.
Name	Geben Sie einen beschreibenden Namen ein, um das Bedrohungsereignis zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Bedrohungsereignis enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diesen Bedrohungsakteur hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Bedrohungsereignis zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Bedrohungsereignis zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Bedrohungsereignis zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungsereignis zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsgruppierung

Ein Bedrohungsgruppierungsobjekt bestätigt explizit, dass die referenzierten STIX-Objekte einen gemeinsamen Kontext haben. Bedrohungsgruppierungen gelten für STIX 2.x.

Ein Bedrohungsgruppierungsobjekt stellt einen Satz von Daten dar, die bei ausreichender Analyse ausgereift sind, um einen Incident- oder Bedrohungsbericht als STIX-Berichtsobjekt zu übermitteln. Beispielsweise kann eine Gruppierung verwendet werden, um die laufende Untersuchung eines Sicherheitsereignisses oder eines Sicherheitsincidents zu charakterisieren.

Ein Bedrohungsgruppierungsobjekt kann auch verwendet werden, um zu bestätigen, dass die referenzierten STIX-Objekte zu einem laufenden Analyseprozess gehören. Beispielsweise kann ein Bedrohungsanalyst mit anderen in seiner Trust Community zusammenarbeiten, um eine Reihe von Kampagnen und Indikatoren zu untersuchen.

Das SDO für die Bedrohungsgruppierung enthält eine Liste von Verweisen auf SDOs, SCOs und SROs, zusammen mit einer expliziten Beschreibung des vom Inhalt gemeinsam genutzten Kontexts, einer Textbeschreibung und dem Namen der Gruppierung.

Definieren Sie die Bedrohungsgruppierung

Definieren Sie Bedrohungsgruppierungen als Objekte, die einen gemeinsamen Kontext haben.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Navigieren Sie zum Objekt **„Bedrohungsgruppierung“**.
4. Klicken Sie auf **Neu**.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Details der Bedrohungsgruppierung

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise, um einen Angriff vom Typ „Bedrohungsgruppe“ zu verhindern.
Name	Geben Sie einen beschreibenden Namen ein, um die Bedrohungsgruppe zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Bedrohungsereignis enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Bedrohungsgruppierung hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsgruppierung zugeordnet sind.

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Bedrohungsereignisse	Listet die Bedrohungsereignisse auf, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungshinweis

Ein Bedrohungshinweis übermittelt informativen Text, um zusätzliche Analysen bereitzustellen, die nicht in den STIX-Objekten, Markierungsdefinitionsobjekten oder Sprachinhaltsobjekten enthalten sind, auf die sich der Hinweis bezieht. Bedrohungshinweise gelten für STIX 2.x.

Beispielsweise kann ein Analyst einem von einer anderen Organisation erstellten Kampagnenobjekt eine Notiz hinzufügen. Der Hinweis kann darauf hinweisen, dass in einem Hackerforum Beiträge zu dieser Kampagne gesehen wurden.

Notizen werden in der Regel von menschlichen Analysten erstellt und bestehen aus anwenderdefiniertem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Notiz erstellt hat.

Definieren Sie den Bedrohungshinweis

Definieren Sie Bedrohungshinweise, die Informationen vermitteln, um weiteren Kontext oder Analysen bereitzustellen, die in vorhandenen Objekten nicht verfügbar sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Navigieren Sie zu **Bedrohungshinweis**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Ansicht Bedrohungshinweisdetails

Feld	Beschreibung
ID	Eindeutige ID für einen Bedrohungshinweis.
Zusammenfassung	Geben Sie eine kurze Zusammenfassung des Notizinhalts an.
Inhalt	Gibt den Inhalt der Notiz an.
Autoren	Gibt den Namen des Autors an (z. B. ein Analyst).
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diesen Bedrohungshinweis hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungshinweis zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Bedrohungsereignisse	Listet die Bedrohungsereignisse auf, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsmeinung

Eine Meinung ist eine Bewertung der Richtigkeit der Informationen in einem STIX-Objekt, die von einer anderen Entität erstellt wurde. Die Bedrohungsmeinungen gelten für STIX 2.x.

Die Meinungseigenschaft erfasst den Grad der Zustimmung oder Nichtübereinstimmung mithilfe einer festen Skala. Die feste Skala unterstützt auch eine numerische Zuordnung, um konsistente statistische Vorgänge über Meinungen hinweg zu ermöglichen.

Beispielsweise kann ein Analyst einer verbrauchenden Organisation sagen, dass er mit einem Kampagnenobjekt „überhaupt nicht einverstanden“ ist, und eine Erklärung dafür angeben.

Meinungen sind subjektiv, und in der Spezifikation wird nicht angegeben, wie sie am besten interpretiert werden können.

Humananalysten erstellen Meinungen und bestehen aus anwenderdefiniertem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Meinung erstellt hat.

Definieren Sie die Bedrohungsmeinung

Definieren Sie Bedrohungsmeinungen als Bewertung der Richtigkeit der Informationen in einem STIX-Objekt.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum Objekt **„Bedrohungsmeinung“**.
4. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Details der Bedrohungsmeinung anzeigen

Feld	Beschreibung
ID	Eindeutige ID für eine Bedrohungsmeinung.
Meinung	Die Meinung des Erstellers zum STIX-Objekt.
Erklärung	Gibt den Inhalt der Meinung an.
Autoren	Gibt den Namen des Autors an (z. B. ein Analyst).
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Bedrohungsmeinung hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Bedrohungsmeinung hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt den Zeitpunkt an, zu dem der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsmeinung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsstellungnahme zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsstellungnahme zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsstellungnahme zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Bedrohungsereignisse	Listet die Bedrohungsereignisse auf, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsbericht

Bedrohungsberichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren. Bedrohungsberichte gelten für STIX 2.x.

Bedrohungsberichte enthalten die Beschreibung eines Bedrohungsakteurs, der Malware und der Angriffstechnik sowie des Kontexts und zugehörige Details. Sie werden verwendet, um relevante Threat Intelligence-Informationen zu gruppieren, sodass sie als umfassende Cyberbedrohungs-Story veröffentlicht werden können.

Der Bedrohungsbericht-SDO enthält eine Liste von Verweisen auf STIX-Objekte zusammen mit einer Textbeschreibung und dem Namen des Berichts.

Definieren Sie den Bedrohungsbericht

Definieren Sie Bedrohungsberichte, die einen Bedrohungsakteur, Malware, Angriffstechnik einschließlich Kontext und zugehörige Details beschreiben.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Navigieren Sie zum Objekt **„Bedrohungsbericht“**.
4. Klicken Sie auf **Neu**.

   ### Hinweis:

   Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht Bedrohungsberichtsdetails

Feld	Beschreibung
ID	Geben Sie einen Namen an, um den Bedrohungsbericht zu identifizieren.
Name	Geben Sie eine kurze Zusammenfassung des Notizinhalts an.
Beschreibung	Eine Beschreibung, die zusätzliche Einblicke und Kontext für den Bericht bietet.
Berichtstypen	Gibt den Namen des Autors an (z. B. ein Analyst).
Veröffentlicht	Das Datum, an dem dieser Bericht vom Berichtsautor offiziell veröffentlicht wurde.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diesen Bedrohungshinweis hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungsberichten zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
	wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Bedrohungsereignisse	Listet die Bedrohungsereignisse auf, die diesem Objekt zugeordnet sind.
Bedrohungsgruppierungen	Listet die Bedrohungsgruppierungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsberichte	Listet die Bedrohungsberichte auf, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren für Angriffe im Zusammenhang mit diesem Objekt verwendet wird.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Tool

Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet werden. Tools gelten für STIX 2.x.

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware befinden sich diese Tools oder Softwarepakete häufig auf einem System und dienen berechtigten Zwecken für Power-Benutzer, Administratoren, Netzwerkadministratoren oder sogar normale Benutzer.

Beispielsweise sind Remote Access Tools (RDP) und Network Scan Tools (Nmap) Tools, die ein Bedrohungsakteur während eines Angriffs verwendet.

Tools definieren

Definieren Sie Tools als legitime Software, die zum Ausführen von Angriffen verwendet wird.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Tool** -Objekt.
4. Klicken Sie auf **Neu**.

   ### Hinweis:

   Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailansicht „Tools“.

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung eines Tools.
Name	Geben Sie einen beschreibenden Namen ein, um das Tool zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Tool enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Tooltypen	Die Art(en) der beschriebenen Tools.
Aliase	Ein alternativer Name, der zum Identifizieren dieses Tools verwendet wird. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf das Symbol **„Neue Aliasse hinzufügen“**, das im Feld „Alias“ selbst verfügbar ist.
Toolversion	Der dem Tool zugeordnete Versionsbezeichner.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für dieses Tool hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Tool hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Tools zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Schwachstelle

Eine Schwachstelle ist eine Schwachstelle oder ein Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen. Schwachstellen gelten für STIX 2.x.

Die Schwachstelle oder der Fehler liegt in den Anforderungen, Designs oder Implementierungen des Codes, der in einer Software- oder Hardwarekomponente enthalten ist. Diese Schwachstelle wird direkt ausgenutzt, um die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems zu beeinträchtigen.

CVE ist eine Liste von Informationssicherheitsschwachstellen und -risiken, die gängige Namen für öffentlich bekannte Probleme [CVE] bereitstellt.

Wenn beispielsweise eine Malware CVE-2015-12345 ausnutzt, könnte ein Malware-Objekt mit einem Schwachstellenobjekt verknüpft werden, das auf CVE-2015-12345 verweist.

Definieren Sie die Schwachstelle

Definieren Sie eine Schwachstelle als eine Schwachstelle oder einen Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Schwachstellenobjekt**.
4. Klicken Sie auf **Neu**.

   Hinweis:
   Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailansicht Schwachstellen

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung einer Schwachstelle.
Name	Ein Name, der zum Identifizieren der Schwachstelle verwendet wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Schwachstelle enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Schweregrad	Gibt den normalisierten Schweregrad dieser Schwachstelle an
CVSS3.0	Gibt CVSS v3 für diese Schwachstelle an.
CVSS2.0	Gibt CVSS v2 für diese Schwachstelle an.
Nutzungsstatus	Gibt den Exploit-Status an, der dieser Schwachstelle zugeordnet ist
Veröffentlicht	Gibt an, wann die Schwachstelle veröffentlicht wird.
Datensatz zuletzt geändert	Gibt an, wann der Datensatz zuletzt geändert wurde.
Betroffene Software	Listet die betroffene Software auf, die der Schwachstelle zugeordnet ist.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Schwachstelle hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Schwachstelle hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Schwachstelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Schwachstelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die mit dieser Schwachstelle verknüpft sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Schwachstelle zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die bzw. den Angreifer ausnutzen und die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Rufen Sie Schwachstellendaten ab

Rufen Sie Daten im Zusammenhang mit Schwachstellen ab, z. B. Konfigurationselemente, angreifbare Einträge und Geschäftskontext.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Schwachstellenobjekt**.
   Die zugehörigen Schwachstellen, die diesem Objekt zugeordnet sind, werden angezeigt.
4. Wählen Sie den entsprechenden Schwachstellen-Datensatz aus.
   Wenn ihr CVEs zugeordnet sind, können Sie die zugehörigen Daten zu Schwachstellen automatisch über die bereitgestellte Schaltfläche abrufen. Diese zugeordneten Datensätze werden dann im Abschnitt „Geschäftskontext“ der Schwachstellen angezeigt.
5. Gehe zu **Interne Intelligenz** > **Angreifbare Einträge**.
   Die zugeordneten CVEs-Datensätze werden angezeigt.
6. Wählen Sie ein beliebiges CVE aus, und klicken Sie auf die Schaltfläche **Vulnerability-bezogene Daten abrufen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Dieser Link ordnet die Datensätze automatisch zu und ruft den jeweiligen Geschäftskontext der Datensätze ab.
- Wenn keine Datensätze zugeordnet sind, wird eine Informationsmeldung angezeigt, dass diesem spezifischen Schwachstellenobjekt keine angreifbaren Einträge zugeordnet sind. Sie müssen die Objekte manuell mit den angreifbaren Einträgen verknüpfen, um die Daten abzurufen.
- Diese Schaltfläche löst eine geplante Hintergrundaufgabe aus, und die Details zur Initiierung und Ausführung des Auftrags werden im Abschnitt **„Aktivitätenstrom“** angezeigt. Beispiel: Wenn der -Auftrag ausgelöst wird, zeigt der Aktivitätenstrom eine Aktivität an: Das Abrufen der zugehörigen Daten mit den Einträgen angreifbarer Elemente wurde gestartet. Weitere Informationen dazu, wie die geplanten Aufgaben zum Abrufen der Daten ausgeführt werden, finden Sie unter Geplante Aufgaben .

7. Klicken Sie auf **Link**, um die Objekte manuell zu verknüpfen.
8. Wählen Sie die zu verknüpfenden Datensätze aus, und rufen Sie die Daten im Zusammenhang mit Schwachstellen mithilfe der Schaltfläche **Daten im Zusammenhang mit Schwachstellen** abrufen ab. Wenn Sie auf diese Schaltfläche klicken, wird der Hintergrundauftrag ausgelöst und die Daten werden automatisch in den entsprechenden Abschnitt abgerufen. In einer Meldung wird angezeigt, dass der Auftrag zum Abrufen von Daten, die den angreifbaren Einträgen zugeordnet sind, gestartet wurde. Sie können den Status im Aktivitätenstrom verfolgen und die Liste aktualisieren, sobald der Auftrag abgeschlossen ist, um die Ergebnisse zu überprüfen. Wenn sich die Daten beispielsweise auf die Konfigurationselemente beziehen, überprüfen Sie die Ergebnisse im Abschnitt „Konfigurationselemente“. Weitere Informationen zum Hinzufügen von CVEs finden Sie unter CVEs zu Drittparteieinträgen hinzufügen .

Hinweis:
Auf ähnliche Weise können Sie die Daten der Datensätze erkennbarer Elemente abrufen. Weitere Informationen finden Sie unter Rufen Sie Schwachstellendaten ab.

Markierungsdefinition

Das Objekt „marking-definition“ stellt eine bestimmte Markierung dar. Datenmarkierungen stellen normalerweise Anforderungen für die Verarbeitung oder Freigabe von Daten dar.

Definieren Sie die Markierungsdefinition

Definieren Sie Markierungsdefinitionen, um die Anforderungen für die Daten zu verarbeiten und freizugeben.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Markierungsdefinitionsobjekt**.
4. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

Detailansicht der Markierungsdefinitionsquelle

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung einer Markierungsdefinition.
Name	Ein Name, der zur Identifizierung der Markierungsdefinition verwendet wird.
Definitionstyp	Die Typeigenschaft gibt den Typ des Objekts an. Die Eigenschaft „definition_type“ gibt den Typ der Markierungsdefinition an.
Definition	Die Definitionseigenschaft enthält das Markierungsobjekt selbst, z. B. TLP.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Vertrauen	Geben Sie die Konfidenz für dieses Objekt ein. Die Konfidenzeigenschaft gibt das Vertrauen des Erstellers in die Richtigkeit seiner Daten an. Der Konfidenzwert muss eine Zahl im Bereich von 0 bis 100 sein.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Markierungsdefinition hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Markierungsdefinition hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Schwachstelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Schwachstelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die mit dieser Schwachstelle verknüpft sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Schwachstelle zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die mit diesem Objekt verknüpften Angriffsmuster auf.
Kampagnen	Listet die Kampagnen auf, die diesem Objekt zugeordnet sind.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die diesem Objekt zugeordnet sind.
Identitäten	Listet die Identitäten auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von Angreiferverhalten und -ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt geografischen Kontext bieten.
Malware	Listet den Schadcode auf, der diesem Objekt zugeordnet ist.
Malware-Analyse	Listet die schädliche Analyse auf, die diesem Objekt zugeordnet ist.
Erkennbare Elemente	Listet die erkennbaren Elemente auf, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Personen, Gruppen oder Organisationen auf, die mit einer böswilligen Absicht handeln, die diesem Objekt zugeordnet ist.
Bedrohungsereignisse	Listet die Bedrohungsereignisse auf, die diesem Objekt zugeordnet sind.
Bedrohungsgruppierungen	Listet die Bedrohungsgruppierungen auf, die diesem Objekt zugeordnet sind.
Bedrohungshinweise	Listet die Bedrohungshinweise auf, die diesem Objekt zugeordnet sind.
Bedrohungsmeinungen	Listet die diesem Objekt zugeordneten Bedrohungsmeinungen auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Tools	Listet die Tools auf, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet die diesem Objekt zugeordneten Schwachstellen auf.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Datenkomponente

Datenkomponenten werden verwendet, um bestimmte Eigenschaften oder Werte einer Datenquelle zu identifizieren.

Definieren Sie die Datenkomponente

Definieren Sie eine Datenkomponente, um die Eigenschaften oder Werte einer Datenquelle zu identifizieren

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Datenkomponentenobjekt**.
4. Klicken Sie auf **Neu**.

Hinweis:

Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht „Datenkomponentendetails“.

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung einer Datenkomponente.
Name	Ein Name, der zum Identifizieren der Datenkomponente verwendet wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Schwachstelle enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Datenquelle	Gibt den normalisierten Schweregrad dieser Schwachstelle an
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Vertrauen	Gibt die Konfidenz für dieses Objekt an. Die Konfidenz muss zwischen 0 und 100 liegen.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Datenkomponente hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie einen zusätzlichen Kontext für diese Datenkomponente hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erweiterungen	Gibt die Erweiterungen der Datenkomponente an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Schwachstelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Schwachstelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die mit dieser Schwachstelle verknüpft sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Datenkomponente zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Angriffsmuster	Listet die mit diesem Objekt verknüpften Angriffsmuster auf.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Datenquellen

Datenquellen stellen die verschiedenen Themen/Themen von Informationen dar, die von Sensoren/Protokollen erfasst werden können. Datenquellen enthalten auch Datenkomponenten, die bestimmte Eigenschaften/Werte einer Datenquelle identifizieren.

Definieren Sie Datenquellen

Definieren Sie eine Datenquelle, um die verschiedenen Themen oder Themen von Informationen darzustellen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **Datenquellen** -Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:

Wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt und eine Meldung angezeigt, dass der neue Objektdatensatz erstellt wird. Anschließend wird der Benutzer zum aggregierten Datensatz weitergeleitet.

5. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailansicht Schwachstellen

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der Datenquelle.
Name	Ein Name, der zum Identifizieren der Datenquelle verwendet wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Datenquelle enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Sammlungsebenen	Gibt die Beschreibung an, wo die Datenquelle physisch gesammelt werden kann, z. B. Host, Netzwerk, Cloud-Steuerungsebene usw.
Plattformen	Gibt an, dass das System, in dem ein Angreifer tätig ist, ein Betriebssystem oder eine Anwendung sein kann.
Beitragende	Gibt die Beitragenden für diese Datenquelle an.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die entsprechende Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Datenquelle hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Datenquelle hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2.1 sein.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, diese Vorgehensweise
Erstellt	Gibt Datum und Uhrzeit der Erstellung des Objekts in der Quelle an.
Aktualisiert	Gibt Datum und Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die angibt, dass ein neuer erkennbarer Datensatz erstellt wird. Klicken Sie auf **„Fortsetzen“**, um den Datensatz zu bearbeiten und neue Beziehungen zu erstellen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für ein erkennbares Element erstellt haben, wird das Kontrollkästchen **Systemaktualisierungen verhindern** angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags und Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Datenquelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Datenquelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Datenquelle zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Datenquelle zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.

Hinweis:

1. Sie können die zugehörigen Datensätze, die diesem Objekt zugeordnet sind, verknüpfen und die Verknüpfung aufheben. Weitere Informationen finden Sie unter Zugehörige Datensätze zu Bedrohungsinformationen verknüpfen.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei Objekten herzustellen, verwenden Sie den Link **„Potenzielle Beziehungen“** aus der **Threat Intel Library,** um die Beziehungen zwischen den Objekten zu bestätigen. Weitere Informationen finden Sie unter Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten.
3. Verwenden Sie außerdem den Abschnitt **„Zugehörige Datensätze“** aus der Formularansicht „Objekte“, um die Beziehungen zwischen zwei Objekten mithilfe des Abschnitts **„Potenzielle Beziehungen“** in der Formularansicht zu bestätigen. Weitere Informationen zu finden Sie unter Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Objekte zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Definieren Sie RSS-Feeds

Ein Threat Intelligence-Feed ist ein kontinuierlicher Echtzeitdatenstrom, der Informationen zu Cyberrisiken oder -bedrohungen sammelt. RSS-Feeds bieten eine einfache Möglichkeit, über Ihre Lieblingswebsites, z. B. Blogs oder die neuesten Nachrichten zur Cybersicherheit, auf dem Laufenden zu bleiben.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum **RSS-Feeds** -Objekt.

Hinweis:

Die erfassten Feeds können in diesem Abschnitt durchsucht werden, Sie können jedoch keine neuen Datensätze erstellen.

4. Im Formular werden die folgenden Felder automatisch ausgefüllt.

Detailansicht „RSS-Feeds“.

Feld	Beschreibung
Titel	Titel des RSS-Feeds.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zu den RSS-Feeds enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Verknüpfung	Gibt den Link an, der den RSS-Feeds hinzugefügt wurde.
Quelle	Gibt die RSS-Feed-Quelle an, aus der dieser Objektdatensatz erstellt wird.
Veröffentlichungsdatum	Gibt an, wann der RSS-Feed veröffentlicht wird.
Autor	Gibt den Autor für den RSS-Feed an.

5. Klicken Sie auf **Speichern**.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Feed hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Medien-URL	Gibt die Medien-URL an.
Feedback-Kommentare	Alle zusätzlichen Feedback-Kommentare zum Feedback.

Beziehungsobjekte

Verwenden Sie die Beziehungsobjekte, um zwei erkennbare Elemente oder ein erkennbares Element und SDO miteinander zu verknüpfen und zu erklären, wie sie miteinander in Beziehung stehen.

STIX-Beziehungsobjekte (STIX Relationship Objects, SROs) stellen Arten von Beziehungen zwischen verschiedenen STIX-Objekten dar. Die folgenden Beziehungsobjekte sind verfügbar:

- **Beziehung zwischen erkennbaren Elementen und erkennbaren Elementen**: Dieses Objekt definiert Beziehungen zwischen erkennbaren Elementen.
- **Objekt-Objekt-Beziehung**: Dieses Objekt definiert Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts. Ein Beispiel für eine definierte Objekt-Objekt-Beziehung ist, dass ein Angriffsmuster Malware übermittelt.
- **Beziehung zwischen Objekt und erkennbarem Element**: Dieses Objekt definiert Beziehungen zwischen SDOs und dem erkennbaren Elementobjekt (SCO). Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus erkennbaren Cyber-Objekten besteht, die Informationen über einen potenziellen Angriff bereitstellen.
- **Objekt-Indikator-Beziehung**: Dieses Objekt definiert Beziehungen zwischen SDOs und dem Indikatorobjekt.
- **Indikator-Indikator-Beziehungen**: Dieses Objekt definiert Beziehungen zwischen Indikatorobjekten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Beziehung zwischen Indikator und erkennbarem Element**: Dieses Objekt definiert Beziehungen zwischen dem Indikatorobjekt und anderen SDOs. Ein Beispiel für eine durch Objekte und Indikatoren definierte Beziehung ist, dass ein Indikator Hinweise auf eine Kampagne erkennt.

Objektbeziehungen

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
Erkennbares Element – Beziehungen erkennbarer Elemente	IP-Adresse, Domänenname		Diese Beziehung beschreibt zwischen den erkennbaren Elementen.
Objekt-Objekt-Beziehungen	Angriffsmuster	Malware	Diese Beziehung beschreibt, dass dieses Angriffsmuster verwendet wird, um diese Malware-Instanz (oder Familie) bereitzustellen.
Objekt-Erkennbares Element-Beziehungen			Diese Beziehung beschreibt zwischen den -Objekten und den erkennbaren Elementen.
Objekt-Indikator-Beziehungen	Indikator	Angriffsmuster, Kampagne, Infrastruktur, Angriffssatz, Malware, Bedrohungsakteur, Tool	Diese Beziehung beschreibt, dass der Indikator Hinweise auf das zugehörige Angriffsmuster, die Kampagne, die Infrastruktur, den Angriffssatz, die Malware, den Bedrohungsakteur oder das Tool erkennen kann. Der Nachweis ist möglicherweise nicht direkt. Beispielsweise kann der Indikator sekundäre Nachweise der Kampagne erkennen, z. B. Malware, die häufig von dieser bestimmten Kampagne verwendet wird.
Indikator: Indikatorbeziehungen	Infrastruktur	Beobachtete Daten	Diese Beziehung beschreibt, dass der Indikator basierend auf Informationen aus einem beobachteten Datenobjekt erstellt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objektbeziehungen (Fortsetzung)

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
			Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus erkennbaren Cyber-Objekten besteht, die Informationen über einen potenziellen Angriff bereitstellen.
Indikator – erkennbares Element			Diese Beziehung beschreibt zwischen -Indikatoren und erkennbaren Elementen.

Definieren Sie Beziehungen zwischen erkennbaren Elementen und erkennbaren Elementen

Definieren Sie Beziehungen zwischen erkennbaren Elementen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Beziehungen** > **Erkennbares Element – Erkennbares Element**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.
6. Klicken Sie auf **Absenden**.

Definieren Sie Objekt-Objekt-Beziehungen

Definieren Sie Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Beziehungen** > **Objekt-Objekt**.
4. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie die Felder im Formular entsprechend aus.

6. Klicken Sie auf **Absenden**.

Definieren Sie Beziehungen zwischen Objekt und erkennbarem Element

Definieren Sie Beziehungen zwischen SDOs und dem erkennbaren Elementobjekt (SCO).

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Beziehungen** > **Objekt – erkennbares Element**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.

6. Klicken Sie auf **Absenden**.

Definieren Sie Objekt-Indikator-Beziehungen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen SDOs.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Beziehungen** > **Objektindikator**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.

6. Klicken Sie auf **Absenden**.

Definieren Sie Indikator-Indikator-Beziehungen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen. Verwenden Sie die Beziehungsobjekte, um zwei erkennbare Elemente oder ein erkennbares Element und SDO miteinander zu verknüpfen und ihre Beziehung zueinander zu erklären.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Beziehungen** > **Indikator-Indikator**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.
6. Klicken Sie auf **Absenden**.

Definieren Sie Beziehungen zwischen Indikatoren und erkennbaren Elementen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen SDOs.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Beziehungen** > **Indikator – erkennbares Element**.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.
6. Klicken Sie auf **Absenden**.

Potenzielle Beziehungen

Die Anwendung verwendet die automatisierte Korrelation, um potenziell mögliche Beziehungen zwischen zwei SDOs, zwei erkennbaren Elementen oder einem erkennbaren Element und einem SDO herzustellen.

1. Wählen Sie einen oder mehrere potenziell zugehörige Datensätze aus, und wenden Sie diese Aktion auf die Anwenderoberfläche an. Dadurch werden die Datensätze weiter in die bestätigten Beziehungen geändert und im Abschnitt „Zugehörige Datensätze“ angezeigt.
2. Alle bestätigten Korrelationen, die von einem Analysten erfasst oder manuell erstellt wurden, überschreiben die potenziellen Beziehungen, die durch die automatische Korrelation erstellt wurden.

Bestätigen Sie die Beziehung zwischen erkennbarem und potenziellem erkennbarem Element

Verwenden Sie diesen Abschnitt, um die Beziehungen zwischen den erkennbaren Elementen zu bestätigen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Potenzielle Beziehungen** > **Erkennbares Element – Erkennbares Element**.
4. Wählen Sie den Datensatz des erkennbaren Elements aus.
5. Klicken Sie auf **Beziehung bestätigen**.
   Idealerweise wird ein Datensatz für eine potenzielle Beziehung erstellt, der anhand seiner Korrelationsregeln identifiziert wird. Sobald Sie die Beziehung bestätigt haben, wird der Datensatz der erkennbaren Elemente in den Abschnitt „Beziehungen“ verschoben, was bedeutet, dass die Beziehung zwischen den erkennbaren Elementen und den erkennbaren Elementen bestätigt wird. Der Datensatz zeigt nur dann eine bestätigte Beziehung an, wenn die Korrelationsregeln übereinstimmen. Beispielsweise kann eine potenzielle Beziehung erstellt werden, wenn zwei erkennbare Elemente vom Typ „URLs“ denselben Domänennamen haben.

   Alternativ können Sie auch einen neuen Datensatz für erkennbare Elemente erstellen, indem Sie die erkennbaren Elemente aus der Liste der erkennbaren Elemente verknüpfen und die Beziehungen auf der Registerkarte „Zugehörige Datensätze“ jedes erkennbaren Elements bestätigen.

   a. Öffnen Sie einen beliebigen erkennbaren Elementdatensatz.
   b. Wechseln Sie zur Registerkarte **Zugehörige Datensätze**.
   c. Klicken Sie auf die Schaltfläche **Link**.
   d. Wählen Sie mindestens ein erkennbares Element aus.
   e. Klicken Sie auf **Link**.
      Dadurch wird eine neue Beziehung zwischen dem ausgewählten Datensatz des erkennbaren Elements und den neu verknüpften erkennbaren Elementen erstellt.
6. Klicken Sie auf **Löschen**, um die Beziehungen zu löschen.

Bestätigen Sie die Beziehungen zwischen Objekten und potenziellen Objekten

Definieren Sie die möglichen Beziehungen zwischen den Objekten.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Potenzielle Beziehungen** > **Objekt-Objekt**.
4. Wählen Sie den Datensatz des erkennbaren Elements aus.
5. Klicken Sie auf **Beziehung bestätigen**.
   Idealerweise wird ein Datensatz für eine potenzielle Beziehung erstellt, der anhand seiner Korrelationsregeln identifiziert wird. Sobald Sie die Beziehung in diesem Abschnitt bestätigt haben, wird der Datensatz der erkennbaren Elemente in den Abschnitt „Beziehungen“ verschoben, was bedeutet, dass die Beziehung zwischen den erkennbaren Elementen und den erkennbaren Elementen bestätigt wird. Der Datensatz zeigt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nur dann eine bestätigte Beziehung an, wenn die Korrelationsregeln übereinstimmen. Beispielsweise kann eine potenzielle Beziehung erstellt werden, wenn zwei erkennbare Elemente vom Typ URLs denselben Domänennamen haben.

Alternativ können Sie auch einen neuen Datensatz für erkennbare Elemente erstellen, indem Sie die erkennbaren Elemente aus der Liste der erkennbaren Elemente verknüpfen und die Beziehungen auf der Registerkarte „Zugehörige Datensätze“ jedes erkennbaren Elements bestätigen.

a. Öffnen Sie einen beliebigen erkennbaren Elementdatensatz.

b. Wechseln Sie zur Registerkarte **Zugehörige Datensätze**.

c. Klicken Sie auf die Schaltfläche **Link**.

d. Wählen Sie mindestens ein erkennbares Element aus.

e. Klicken Sie auf **Link**.
Dadurch wird eine neue Beziehung zwischen dem ausgewählten Datensatz des erkennbaren Elements und den neu verknüpften erkennbaren Elementen erstellt.

6. Klicken Sie auf **Löschen**, um die Beziehungen zu löschen.

Bestätigen Sie die Beziehungen zwischen Indikator und potenziellem Indikator

Definieren Sie die möglichen Beziehungen zwischen den Objekten.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Gehe zu **Potenzielle Beziehungen** > **Indikator-Indikator**.
4. Wählen Sie den Datensatz des erkennbaren Elements aus.
5. Klicken Sie auf **Beziehung bestätigen**.
Ein potenzieller Beziehungsdatensatz wird idealerweise basierend auf automatisierten Korrelationsregeln bestätigt. Sobald Sie die Beziehung bestätigt haben, wird der Datensatz der erkennbaren Elemente in den Abschnitt „Beziehungen“ verschoben, was bedeutet, dass die Beziehung zwischen den erkennbaren Elementen und den erkennbaren Elementen bestätigt wird.

   Der Datensatz zeigt nur dann eine bestätigte Beziehung an, wenn die Korrelationsregeln übereinstimmen. Beispielsweise wird eine potenzielle Beziehung bestätigt, wenn zwei erkennbare Elemente vom Typ URLs denselben Domänennamen aufweisen.

   Alternativ können Sie auch einen neuen Datensatz für erkennbare Elemente erstellen, indem Sie die erkennbaren Elemente aus der Liste der erkennbaren Elemente verknüpfen und die Beziehungen auf der Registerkarte „Zugehörige Datensätze“ jedes erkennbaren Elements bestätigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Öffnen Sie einen beliebigen erkennbaren Elementdatensatz.

b. Wechseln Sie zur Registerkarte **Zugehörige Datensätze**.

c. Klicken Sie auf die Schaltfläche **Link**.

d. Wählen Sie mindestens ein erkennbares Element aus.

e. Klicken Sie auf **Link**.
Dadurch wird eine neue Beziehung zwischen dem ausgewählten Datensatz des erkennbaren Elements und den neu verknüpften erkennbaren Elementen erstellt.

6. Klicken Sie auf **Löschen**, um die Beziehungen zu löschen.

Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen

Bestätigen Sie die Beziehungen zwischen den beiden SDOs.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

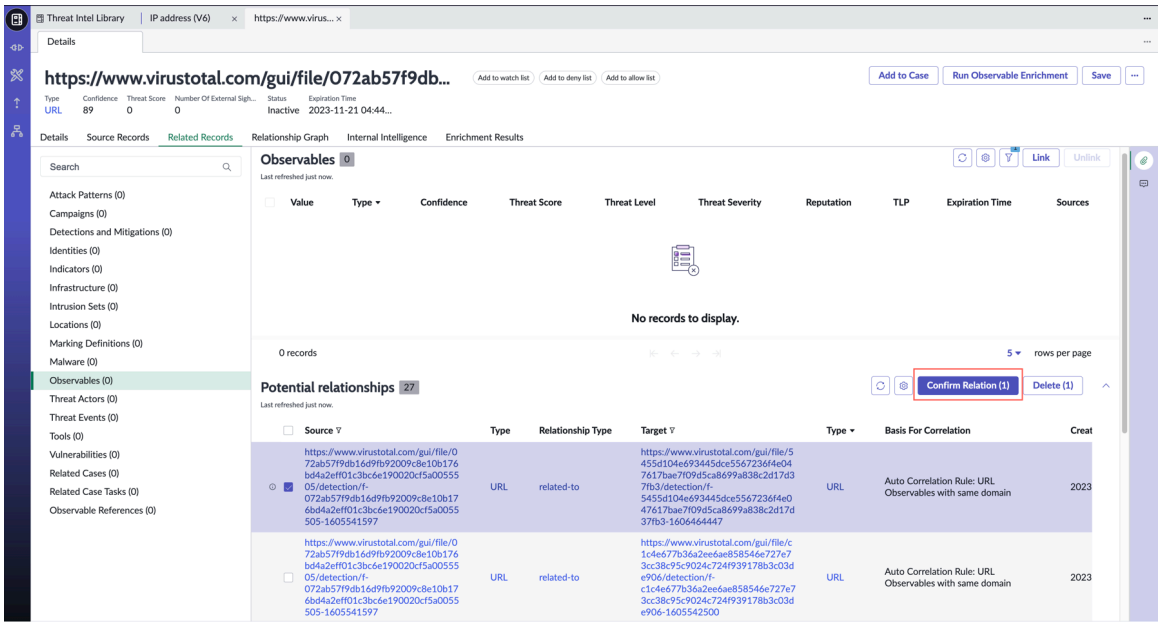
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Wechseln Sie zum Abschnitt **Zugehörige Datensätze**.
4. Erweitern Sie **potenzielle Beziehungen**.
5. Öffnen Sie einen beliebigen Datensatz wie erkennbare Elemente, Indikatoren oder andere Objekte, für die Sie die Beziehungen zwischen zwei SDOs bestätigen möchten.
6. Wählen Sie hier beispielsweise **Erkennbare Elemente** aus der linken Navigationsleiste aus.
7. Wählen Sie die Datensätze **der erkennbaren Elemente** aus der Liste aus.

Hinweis:
Im Listenabschnitt werden alle verknüpften erkennbaren Elemente des zugeordneten erkennbaren Elements angezeigt.

8. Klicken Sie auf die Schaltfläche **Beziehungen bestätigen,** um die Beziehungen zwischen den Objekten zu bestätigen.

Hinweis:
Weitere Informationen finden Sie unterBeziehungsobjekte und Potenzielle Beziehungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie auf **Löschen**, um die zugeordneten erkennbaren Elemente zu löschen.
   Informationen dazu, wie die potenziellen Beziehungen und Beziehungen zwischen den SDOs eingerichtet werden, finden Sie unter Potenzielle Beziehungen und Beziehungsobjekte.

Automatisierte Korrelation

Mithilfe der automatisierten Korrelation können Sie die Beziehungen zwischen erkennbaren Elementen, Indikatoren und Objekten identifizieren.

Beim Korrelationsprozess stellt die Anwendung automatisch die Korrelation zwischen Threat Intelligence-Datensätzen basierend auf vordefinierten Regeln her. Je nach Typ der angewendeten Regel kann die Beziehung eine bestätigte Beziehung oder eine potenzielle Beziehung sein. Wenn die Beziehungen zwischen den Objekten bestätigt werden, werden diese Objekte automatisch in der Detailansicht dieses Objekts im Abschnitt **„Zugehörige Datensätze“** angezeigt.

Im Folgenden werden die Beziehungen und potenziellen Beziehungen beschrieben:

- **Beziehungen**: Verwenden Sie die Beziehungsobjekte, um zwei erkennbare Elemente oder ein erkennbares Element und SDO miteinander zu verknüpfen und zu erklären, wie sie miteinander in Beziehung stehen.
- **Potenzielle Beziehungen**: Verwenden Sie die potenziellen Beziehungen, um potenziell mögliche Beziehungen zwischen zwei SDOs, zwei erkennbaren Elementen oder einem erkennbaren Element und SDO mithilfe der automatisierten Korrelation herzustellen.

Im Folgenden finden Sie die vordefinierten Korrelationsregeln, die im Basissystem bereitgestellt werden:

Korrelationsregeln

Regelname	Regelbeschreibung	Regeldefinition	Regelaktion
Erkennbare Elemente mit demselben Datei-Hash	Die Regel vergleicht die Hash-Werte der erkennbaren Elemente (vom gleichen Typ) und	Die Regel vergleicht die Hash-Werte (vom gleichen Typ) der -Indikatoren und erkennt,	Erstellt eine Beziehung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationsregeln (Fortsetzung)

Regelname	Regelbeschreibung	Regeldefinition	Regelaktion
	erkennt, ob sie denselben Hash verwenden.	ob sie denselben Hash verwenden.	
Erkennbare URL-Elemente mit derselben Domäne	Die Regel untersucht die Gemeinsamkeiten in der Struktur von URLs, um festzustellen, ob sie dieselbe Basisdomäne verwenden.	Die Regel untersucht die Gemeinsamkeiten in der Struktur von URLs. Sie bestimmt, ob sie dieselbe Basisdomäne verwenden und eine ähnliche Unterverzeichnisstruktur aufweisen.	Erstellt eine potenzielle Beziehung
Erkennbares Element als Quelle im Netzwerkobjekt gefunden	Die Regel gleicht den Wert des Netzwerkquellattributs mit erkennbaren IPV4-, IPV6- oder Domänennamen-Elementen im System und Links als Quelle des Datenverkehrs ab.	Die Regel gleicht den Attributwert Quelle mit erkennbaren IPV4-, IPV6- oder Domänennamen-Elementen im System ab und verknüpft sie als Quelle des Datenverkehrs.	Erstellt eine Beziehung
Erkennbares Element als Ziel in Netzwerkobjekt gefunden	Die Regel gleicht den Wert des Zielattributs des Netzwerks mit IPV4-, IPV6- oder Domänennamen-erkennbaren Elementen im System und in den Links als Ziel des Datenverkehrs ab.	Die Regel gleicht den Attributwert für die Quelle mit erkennbaren IPV4-, IPV6- oder Domänennamen-Elementen im System und Links als Ziel des Datenverkehrs ab.	Erstellt eine Beziehung
Erkennbare Elemente basierend auf Kommunikation verknüpfen	Auf Grundlage von Netzwerkobjekten identifiziert die Regel alle erkennbaren Elemente (IPV4, IPV6 und Domänenname), die mit demselben Ziel (IPV4, IPV6 oder Domänenname) kommuniziert haben, und stellt eine Beziehung zwischen diesen erkennbaren Elementen her. Außerdem zugehörige erkennbare Elemente (IPV4, IPV6 und Domänenname), wenn sie mit demselben Netzwerkobjekt	Auf der Grundlage von Netzwerkobjekten identifiziert die Regel alle Indikatoren, die mit demselben Ziel (IPV4, IPV6, MAC-Adresse oder Domänenname) kommuniziert haben, und stellt eine Beziehung zwischen diesen Indikatoren her, da sie mit derselben C2-Infrastruktur verbunden sind.	Erstellt eine Beziehung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationsregeln (Fortsetzung)

Regelname	Regelbeschreibung	Regeldefinition	Regelaktion
	verknüpft sind wie die Quelle, die mit dem Ziel kommuniziert.		
Zugehörige erkennbare Elemente der Stammdomäne zu Subdomänen	Die Regel verknüpft eine Stammdomäne mit Unterdomänen und umgekehrt für den Domänentyp von erkennbaren Elementen.	Die Regel verknüpft eine Stammdomäne mit Subdomänen.	Erstellt eine Beziehung
Zugehörige Domänen zu IPs basierend auf DNS-Auflösungen	Mithilfe der Attribute „domain-ipv4“ oder „domain-ipv6“ von erkennbaren Domänenelementen stellt die Regel Beziehungen zwischen den Domänen und IPs her.	Verwenden Sie die Attribute „domain-ipv4“ oder „domain-ipv6“. Die Regel identifiziert alle Domänen oder Subdomänen, die in dieselbe IP-Adresse aufgelöst werden, und stellt Beziehungen zwischen den -Indikatoren her, die ihre Verbindung zur selben C2-Infrastruktur angeben.	Erstellt eine Beziehung
Übereinstimmende Domänen mit SSL-Zertifikaten	Die Regel analysiert die SSL-Zertifikatinformationen, die den erkennbaren Domänenelementen zugeordnet sind, und stellt eine Beziehung zwischen ihnen her.	Die Regel analysiert die SSL-Zertifikatinformationen, die den Indikatoren zugeordnet sind, erkennt, dass beide Zertifikate von derselben Zertifizierungsstelle ausgestellt wurden und dasselbe Ablaufdatum haben, und stellt Beziehungen zwischen den Indikatoren her, die auf ihre Verbindung zu derselben C2-Infrastruktur oder Bedrohungskampagne hinweisen.	Erstellt eine Beziehung
Verknüpfen Sie Entitäten basierend auf allgemeinen erkennbaren Elementen	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Entitäten verknüpft ist, und verknüpft sie miteinander.	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Entitäten verknüpft ist, und identifiziert sie als miteinander verknüpft.	Erstellt eine potenzielle Beziehung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationsregeln (Fortsetzung)

Regelname	Regelbeschreibung	Regeldefinition	Regelaktion
Verknüpfen Sie Indikatoren basierend auf allgemeinen erkennbaren Elementen	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Indikatoren verknüpft ist, und setzt sie miteinander in Beziehung.	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Indikatoren verknüpft ist, und identifiziert sie als miteinander verknüpft.	Erstellt eine potenzielle Beziehung
Verknüpfen Sie Indikatoren mit Objekten basierend auf allgemeinen erkennbaren Elementen	Die Regel vergleicht, ob dasselbe erkennbare Element mit Indikatoren und Objekten verknüpft ist, und setzt sie miteinander in Beziehung.	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Indikatoren und Objekten verknüpft ist, und identifiziert sie als miteinander verknüpft.	Erstellt eine potenzielle Beziehung

MITRE-ATT&CK™ Repository

Das Repository MITRE-ATT&CK ist unter der Intelligenzbibliothek verfügbar, in der die Daten aus den MITRE-Quellen erfasst werden.

Die MITRE-Daten, die im Repository ankommen, werden in einem separaten MITRE-Repository aus den Daten der Threat Intel Library gespeichert, in dem MITRE-Daten nicht für den Zusammenfassungs- oder Deduplizierungs-Flow zusammengefasst werden und unabhängig sind.

Die in der Anwendung verfügbaren Datenquellen sind:

1. MITRE: Enterprise ATT&CK
2. MITRE: Mobile ATT&CK
3. MITRE: ICS ATT&CK

Die Daten für diese Quellen werden in einem separaten MITRE-Repository unter der TI-Bibliothek im Basissystem gespeichert. Wenn Sie eine neue MITRE-Quelle erstellen möchten, konfigurieren Sie eine anwenderdefinierte Quelle. Weitere Informationen finden Sie unter Anwenderdefinierten Feed anzeigen. Klicken Sie in der Formularansicht auf das Kontrollkästchen **Erweitert**, und wählen Sie folgenden **Berichtsprozessor** aus: **MITRECollectionDataProcessor**.

Matrizen verwalten

Verwalten Sie die Matrizen, die aus den MITRE TAXII-Sammlungen importiert werden. Matrizen sind eine Sammlung von Taktiken und Techniken. Sie können die Matrizen anzeigen, um zu überprüfen, ob Ihre Sammlungen im MITRE-ATT&CK-Repository verfügbar sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Nachdem Sie die auf MITRE ATT&CK bezogenen Feed-Datenquellen aktiviert haben, die im Basissystem verfügbar sind, klicken Sie auf **„Jetzt ausführen“**, um die Integrationen auszuführen und die MITRE-bezogenen Informationen abzurufen.
   Weitere Informationen zum Aktivieren der Integrationen finden Sie unter
2. Um die Daten des MITRE ATT&CK-Repository anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK**.
   Die zugehörigen MITRE ATT&CK-Datensätze werden angezeigt. Standardmäßig befinden sich alle Datensätze im Status „Aktiviert“.

   Hinweis:
   Sie können nur die Matrizen aktivieren, die für Ihre Organisation relevant sind.

3. Wählen Sie einen beliebigen Matrixdatensatz aus, und klicken Sie auf **Deaktivieren,** wenn Sie einen bestimmten Datensatz deaktivieren möchten.
4. Alternativ können Sie einen neuen Matrizendatensatz erstellen, indem Sie auf **„Neu** “ klicken, um die MITRE ATT&CK-Matrizen manuell zu erstellen.
5. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Verringerung erstellen – Details

Feld	Beschreibung
Name	Geben Sie den Namen der Matrix ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den Matrixdatensatz zu aktivieren.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Einblicke	
Notizen	Zusätzliche Informationen im Zusammenhang mit der Verringerung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie einen beliebigen zusätzlichen Kontext für diesen Objekttyp hinzu.
Kommentare	Fügen Sie ggf. zusätzliche Kommentare hinzu.

Techniken verwalten

Verwalten Sie die Techniken, die aus den MITRE TAXII-Sammlungen importiert werden. Die Techniken enthalten verschiedene Möglichkeiten, wie Angreifer eine bestimmte Taktik

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

anwenden. Sie können Techniken überprüfen und deaktivieren, die für Ihre Organisation nicht relevant sind. In STIX werden Techniken als Angriffsmuster bezeichnet.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

„Techniken“ stellt dar, wie ein Angreifer ein strategisches Ziel durch eine Aktion erreicht.

Prozedur

1. Nachdem Sie die auf MITRE ATT&CK bezogenen Feed-Datenquellen aktiviert haben, die im Basissystem verfügbar sind, klicken Sie auf **„Jetzt ausführen“**, um die Integrationen auszuführen und die MITRE-bezogenen Informationen abzurufen.
   Weitere Informationen zum Aktivieren der Integrationen finden Sie unter
2. Um die Daten des MITRE ATT&CK-Repository anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Techniken**.
   Die Datensätze für MITRE ATT&CK-Techniken werden angezeigt. Standardmäßig befinden sich alle Datensätze im Status „Aktiviert“.
3. Wählen Sie einen beliebigen Technikdatensatz aus, und klicken Sie auf **Deaktivieren**, wenn Sie einen bestimmten Datensatz deaktivieren möchten.
4. Alternativ können Sie neue Technikendatensätze erstellen, indem Sie auf **Neu** klicken, um die MITRE ATT&CK-Techniken manuell zu erstellen.
5. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Verringerung erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Technik.
Name	Geben Sie den Namen der Technik ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Plattformen	Fügen Sie die erforderlichen Plattformen hinzu.
Berechtigungen erforderlich	Fügen Sie die erforderlichen Berechtigungen hinzu.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Erkennung	Die Erkennungstechnik wird verwendet, um einen Angreiferzugriff auf oder nicht autorisierte Aktivitäten in Computernetzwerken zu identifizieren.
Einblicke	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Notizen	Zusätzliche Informationen im Zusammenhang mit der Verringerung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie einen beliebigen zusätzlichen Kontext für diesen Objekttyp hinzu.
Kommentare	Fügen Sie ggf. zusätzliche Kommentare hinzu.

Verwalten von Risikominderungen

Verwalten Sie die Minderungen, die aus den MITRE TAXII-Sammlungen importiert werden. Mit Verringerungen können Sie verhindern, dass ein Angreifer erfolgreich Techniken oder Untertechniken gegen Ihre Organisation ausführt. In STIX werden Minderungen als Vorgehensweisen bezeichnet.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Nachdem Sie die auf MITRE ATT&CK bezogenen Feed-Datenquellen aktiviert haben, die im Basissystem verfügbar sind, klicken Sie auf **„Jetzt ausführen“**, um die Integrationen auszuführen und die MITRE-bezogenen Informationen abzurufen.
   Weitere Informationen zum Aktivieren der Integrationen finden Sie unter.
2. Um die Daten des MITRE ATT&CK-Repository anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Mitigationen**.
   Klicken Sie auf eine Verringerung, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie auf **Neu**, um die MITRE ATT&CK-Minderungen manuell zu erstellen.
4. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Tools erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliase	Eine Liste mit weiteren Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Beitragende	Gibt die Beitragenden an.
Einblicke	
Notizen	Zusätzliche Informationen im Zusammenhang mit der Verringerung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie einen zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

5. Klicken Sie auf **Speichern**.

Gruppen verwalten

Verwalten Sie die Gruppen, die aus den MITRE TAXII-Sammlungen importiert werden. Gruppen sind Sätze zusammengehöriger Angriffsaktivitäten, die in der Sicherheitscommunity unter einem allgemeinen Namen verfolgt werden. Analysten verfolgen Aktivitätscluster anhand verschiedener Begriffe wie Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen. In STIX werden Gruppen als Angriffssätze bezeichnet.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Um die Daten des MITRE ATT&CK-Repository anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Gruppen**.
   Sie können die aufgelisteten Gruppen anzeigen.
2. Klicken Sie auf **Neu**, um die MITRE ATT&CK-Gruppen manuell zu erstellen.
3. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Gruppen erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliase	Eine Liste mit weiteren Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Einblicke	
Notizen	Zusätzliche Informationen im Zusammenhang mit der Verringerung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie einen zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

4. Klicken Sie auf **Speichern**.
5. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie auf **Beziehungen**.

Verwalten Sie Malware

Verwalten Sie die Malware-Informationen, die Sie aus den MITRE TAXII-Sammlungen importiert haben. Es handelt sich um einen TTP-Typ, der schädlichen Code darstellt.

Vorbereitungen

Bezieht sich auf ein Programm, das heimlich in ein System eingefügt wird. Der Zweck einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Um die Daten des MITRE ATT&CK-Repository anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Gruppen**.
   Sie können die aufgelistete Malware anzeigen.
2. Klicken Sie auf eine Malware, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie auf **Neu**, um die MITRE ATT&CK-Malware manuell zu erstellen.
4. Füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue MITRE-Malware erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliase	Eine Liste mit weiteren Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Beitragende	Gibt die Beitragenden an.
Einblicke	
Notizen	Zusätzliche Informationen im Zusammenhang mit der Verringerung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie einen zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

5. Klicken Sie auf **Speichern**.
6. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie auf **Beziehungen**.

Tools verwalten

Verwalten Sie die Toolsinformationen, die Sie aus den MITRE TAXII-Sammlungen importiert haben. Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet werden.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Warum und wann dieser Vorgang ausgeführt wird

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware befinden sich diese Tools oder Softwarepakete häufig auf einem System und dienen berechtigten Zwecken für Power-Benutzer, Administratoren, Netzwerkadministratoren oder sogar normale Benutzer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um die Daten des MITRE ATT&CK-Repository anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Tools**. Sie können die aufgelisteten Tools anzeigen.
2. Klicken Sie auf ein Tool, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie auf **Neu**, um die MITRE ATT&CK-Tools manuell zu erstellen.
4. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Tools erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zum Verhindern eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig betrachtet werden.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliase	Eine Liste mit weiteren Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt den Zeitpunkt an, zu dem das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich des Zwecks und der wichtigsten Merkmale.
Beitragende	Gibt die Beitragenden an.
Einblicke	
Notizen	Zusätzliche Informationen im Zusammenhang mit der Verringerung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie einen zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

5. Klicken Sie auf **Speichern**.
6. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie auf **Beziehungen**.

Verwalten Sie MITRE-Beziehungen

Verwalten Sie die MITRE-Beziehungsinformationen, die Sie aus den MITRE TAXII-Sammlungen importiert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.analyst

Prozedur

1. Um die Daten des MITRE ATT&CK-Repository anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Beziehungen**.
   Sie können die aufgelisteten Beziehungen anzeigen.
2. Klicken Sie auf ein Quellobjekt, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie auf **Neu**, um die MITRE ATT&CK-Beziehungen manuell zu erstellen.
4. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Tools erstellen – Details

Feld	Beschreibung
MITRE-Quellobjekt	Fügen Sie das MITRE-Quellobjekt hinzu.
MITRE-Zielobjekt	Fügen Sie das MITRE-Zielobjekt hinzu.
MITRE-Quelltyp	Geben Sie den MITRE-Quelltyp ein.
MITRE-Zieltyp	Geben Sie den MITRE-Zieltyp ein.
Beziehungstyp	Definieren Sie Beziehungen zwischen Objekten. Eine Beschreibung, die weitere Details und Kontext zum Beziehungstyp enthält. Verfügbare Optionen: Definieren Sie die Beziehungsrichtung: direkt oder invers. ○ Invers – Dies ist der Typ der Beziehung zwischen dem erkennbaren Element und dem Objekt. ○ Direkt: Dies ist der Typ der Beziehung zwischen dem Objekt und dem erkennbaren Element.
Quelle	Wählen Sie das Quellobjekt aus, und definieren Sie es.
Beziehungs-ID	Definieren Sie die Beziehungs-ID.

5. Klicken Sie auf **Speichern**.
6. Um anzuzeigen, wie diese Objekte miteinander verknüpft sind, klicken Sie auf **Beziehungen**.

Datenverwaltung und -speicherung

Daten werden in der TISC-Instanz gemäß der Objektstruktur der TIDC-Bibliothek gespeichert und verwaltet, damit die Administratoren sie entsprechend den Anforderungen ihrer Organisation anzeigen und konfigurieren können.

Die Archivierung und Wiederherstellung von Daten ist eine der Schlüsselfunktionen, um die Datensätze für ihre zukünftige Verwendung zu schützen. In den folgenden Abschnitten werden der TISC-Archivierungsprozess und die Aufbewahrung von Datensätzen definiert und erläutert, da Threat Intelligence große Mengen an Daten und Datensätzen enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenarchivierungsprozess

Die Daten in Tabellen nehmen mit zunehmender Nutzung der Plattform schnell zu. Einige Tabellen sind mit unterschiedlichen Datenverwaltungsrichtlinien im Basissystem enthalten, es sind jedoch andere Benutzer erforderlich, um sie selbst zu implementieren.

Es gibt verschiedene Möglichkeiten, wie Benutzer ihre Daten in Tabellen verwalten:

- Löschen Sie die Daten
- Archivieren Sie die Daten

Hinweis:
Wenn die Benutzer keine der folgenden Möglichkeiten zur Verwaltung ihrer Daten übernehmen, nimmt die Nutzung mit der Zeit zu, und die Daten werden viel größer, was sich erheblich auf die Leistung der Anwendungsinstanz und den Speicher auswirkt.

TISC-Datenarchivierung

Threat Intelligence-Sicherheitszentrum wird mit Archivierungsregeln im Basissystem für die Tabelle TISC bereitgestellt. Die zugehörigen Datensätze werden auch im Basissystem der Archivregel TISC hinzugefügt.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivierungsregeln**.
   Die Liste der Archivierungsregeln, die für TISC gelten, wird angezeigt. Diese Archivierungsregeln sind für jeden Objekttyp unterschiedlich und gelten unabhängig voneinander.
2. Filtern Sie nach den Tabellennamen, die mit „sn_sec_tisc“ beginnen.
3. Zeigen Sie die zugehörigen Datensätze TISC an.

   Hinweis:

   Informationen dazu, wie Archivierungsregeln erstellt werden, finden Sie unter Create an archive rule .

4. Wählen Sie eine Archivierungsregel aus.
   Wählen Sie beispielsweise den Datensatz für erkennbares Element im Verzeichnis aus, um die Archivierungsregel des Basissystems anzuzeigen.
5. Aktualisieren Sie die Regel bei Bedarf.

Archivieren Sie TISC zugehörige Datensätze

Verwenden Sie die zugehörige Liste „Zugehörige Datensätze archivieren“ für TISC, um der Archivierungsregel die zugehörigen Datensätze hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**.
2. Wählen Sie die Daten aus, die über 30 Tage inaktiv sind.
3. Wechseln Sie zur zugehörigen Liste Zugehörige **Datensätze archivieren**.

Löschen Sie Intelligenzdatensätze

Löschen Sie Datensätze aus der Bibliothek Threat Intelligence.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**.
2. Klicken Sie im Arbeitsbereich auf das Symbol **Threat Intel Library (Threat Intel Library)**.
3. Öffnen Sie einen beliebigen -Datensatz.
4. Wechseln Sie zum Abschnitt **Quelldatensätze**.
5. Wählen Sie **Löschen** aus, um die Quelldatensätze zu löschen.
6. Löschen Sie den Bibliotheksdatensatz.

Hinweis:

a. Wenn ein Bibliotheksdatensatz mit zugehörigen Quelldatensätzen gelöscht wird, werden die Quelldatensätze erneut verarbeitet, und ein neuer Bibliotheksdatensatz wird durch Aggregieren der Feldwerte aus den Quelldatensätzen erstellt.

b. Um die Daten dauerhaft aus der Bedrohungsbibliothek zu löschen, verwenden Sie Archivierungsregeln, anstatt die Bibliotheksdatensätze zu löschen. Weitere Informationen finden Sie unter Archivierungsregeln für erkennbare Elemente, Objektarchivierungsregeln und Archivierungsregeln für Indikator und zugehörige Datensätze.

Archivierungsregeln für erkennbare Elemente

Die Archivierungsregeln für erkennbare Elemente, die im Basissystem bereitgestellt werden, sind im folgenden Abschnitt aufgeführt.

- E-Mail-Nachricht
- SHA256-Hash
- Sonstiges erkennbares Element
- SHA512-Hash
- Datei
- SHA1-Hash
- E-Mail-Adresse
- URL
- AS-Nummer
- E-Mail-Betreff
- IPv4-CIDR

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mutex-Name
- Artefakt
- Benutzeraccount
- Windows-Registrierungsschlüssel
- IPv6-Adresse
- MD5-Hash
- IPv4-Adresse
- Verzeichnis
- X.509-Zertifikat
- Archivregel für RSS-Feeds
- Importiert Archivregeln
- Prozess „Standort“.

Ändern Sie die Archivierungsregeln für erkennbare Elemente

Ändern Sie Archivierungsregeln für erkennbare Elemente, und zeigen Sie eine Schätzung der Anzahl der Datensätze an, auf die sich die Regel auswirkt.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig sind die Beispielarchivierungsregeln deaktiviert.

Die Option Historisch signifikant und die Bedingung sollten für erkennbare Elemente, Indikatoren, zugehörige Datensätze und Objekte immer auf „Falsch“ festgelegt werden. Wenn Sie diese Option auf „falsch“ festlegen, können Sie die Datensätze archivieren. Wenn diese Option jedoch auf „wahr“ festgelegt ist, können Sie die Datensätze unabhängig von der Regeldefinition nicht archivieren.

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**.
   Die Liste der Archivierungsregeln, die für TISC gelten, wird angezeigt. Diese Archivierungsregeln sind für jeden Objekttyp unterschiedlich und gelten unabhängig voneinander.
2. Wählen Sie eine beliebige Archivierungsregel aus.
   Wählen Sie beispielsweise den Datensatz für erkennbares Element im Verzeichnis aus, um die Archivierungsregel des Basissystems anzuzeigen.
3. Klicken Sie auf **Filterbedingung hinzufügen**.
4. Wählen Sie die Option **Historisch signifikant** aus, und legen Sie die Bedingung auf **Falsch**fest.
   Wenn Sie diese Option auf „falsch“ festlegen, können Sie die Datensätze archivieren. Wenn diese Option jedoch auf „wahr“ festgelegt ist, können Sie die Datensätze unabhängig von der Regeldefinition nicht archivieren.
5. Legen Sie hier in diesem Beispiel den Status des erkennbaren Elements auf Inaktiv und die Ablaufzeit auf 2 Jahre fest.
   Dies bedeutet, dass der Datensatz des erkennbaren Elements archiviert werden kann, wenn der Status „Inaktiv“ ist und der Ablaufzeitraum des erkennbaren Elements auf 2 Jahre festgelegt ist. Daher wird alles vor diesem Zeitraum ab dem aktuellen Datum archiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Jede Archivierungsregel wird jede Stunde ausgelöst, sodass jede Änderung an der Regel ab dem Zeitpunkt der geplanten Aufgabe geändert wird. Wenn Sie den Auftrag explizit ausführen und nicht warten möchten, bis der Auftrag geplant ist, können Sie ihn entsprechend ändern. Führen Sie die folgenden Schritte aus.

6. Navigieren zu **Zugehörige Links** > **Schätzung neu berechnen**.

   Die Datensatzschätzung wurde neu berechnet und mit dem geschätzten Wert aktualisiert.

Hinweis:
Wenn der Wert für die Datensatzschätzung 0 ist, werden die Datensätze nicht archiviert. Wenn der Wert für die Datensatzschätzung jedoch 1 ist, identifiziert die Anwendung diesen Wert, und dieser Datensatz wird archiviert.

7. Wählen Sie **Jetzt archivieren ausführen aus**.
8. Wechseln Sie zum Abschnitt **„Archivausführung“** unten, um Ihren Archivausführungsprozess zu überprüfen.

Hinweis:
Sie werden feststellen, dass die Gesamtzahl der archivierten Datensätze nur einen Datensatz beträgt, da Ihr Datensatzschätzwert ebenfalls eins ist.

9. Navigieren zu **Threat Intel-Bibliothek** > **Erkennbare Elemente**.
10. Suchen Sie nach dem archivierten Datensatz.
    Der Datensatz muss archiviert worden sein und zeigt die Ergebnisse nicht an, wenn Sie nach dem Datensatz suchen.

Hinweis:

- Als Teil der TISC-Archivierungsregeln werden auch alle Quelldatensätze und zugehörigen Datensätze, die als Teil archivierter zugehöriger Datensätze aufgeführt sind, zusammen mit dem aggregierten Datensatz für erkennbare Elemente archiviert. Sie können einen Drilldown zum Archivprotokollabschnitt durchführen, um die Liste der archivierten Datensätze anzuzeigen, die automatisch im Hintergrund ausgeführt und in diesem Abschnitt angezeigt wurden.
- Wenn Sie den archivierten Datensatz anzeigen möchten, durchsuchen Sie den Datensatz in dieser zugehörigen Tabelle. Gleichzeitig können Sie auch Ihren archivierten Datensatz überprüfen, indem Sie zu navigieren **Systemarchivierung** > **Archivprotokoll**. Dies zeigt die Anzahl der Datensätze an, die archiviert sind.

Objektarchivierungsregeln

Die Archivierungsregeln für erkennbare Elemente, die im Basissystem bereitgestellt werden, sind im folgenden Abschnitt aufgeführt.

Standardmäßig sind die Beispielarchivierungsregeln deaktiviert.

Die Option **Historisch signifikant** und die Bedingung sollten für erkennbare Elemente, Indikatoren, zugehörige Datensätze und Objekte immer auf **„Falsch“** festgelegt werden. Wenn Sie diese Option auf „falsch“ festlegen, können Sie die Datensätze archivieren. Wenn diese Option jedoch auf „wahr“ festgelegt ist, können Sie die Datensätze unabhängig von der Regeldefinition nicht archivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Identität archivieren
- Datenkomponente archivieren
- Archiv-Malware
- Objektsichtung archivieren
- Tool archivieren
- Archiv des Bedrohungsereignisses
- Angriffsmuster archivieren
- Bedrohungsgruppierung archivieren
- Schwachstelle archivieren
- Archivinfrastruktur
- Archivieren Sie den Bedrohungshinweis
- Archivieren Sie die Vorgehensweise
- Bedrohungsakteur archivieren
- Bedrohungsbericht archivieren
- Angriffssatz archivieren
- Kampagne archivieren
- Beobachtete Daten archivieren
- Archiv-Markierungsdefinition
- Archivieren Sie die Bedrohungsmeinung
- Malware-Analyse archivieren

Hinweis:
Um andere Objekte zu archivieren, führen Sie das hier für Archivierungsregeln für erkennbare Elemente Ändern Sie die Archivierungsregeln für erkennbare Elementeerläuterte Verfahren aus.

Archivierungsregeln für Indikator und zugehörige Datensätze

Die Archivierungsregeln für -Indikatoren und zugehörige Datensätze, die im Basissystem bereitgestellt werden, sind im folgenden Abschnitt aufgeführt.

Standardmäßig sind die Beispielarchivierungsregeln deaktiviert.

Die Option **Historisch signifikant** und die Bedingung sollten für erkennbare Elemente, Indikatoren, zugehörige Datensätze und Objekte immer auf **„Falsch“** festgelegt werden. Wenn Sie diese Option auf „falsch“ festlegen, können Sie die Datensätze archivieren. Wenn diese Option jedoch auf „wahr“ festgelegt ist, können Sie die Datensätze unabhängig von der Regeldefinition nicht archivieren.

- **Indikator**: Indikatorarchivregel
- **Archivierung zugehöriger Datensätze**:
  - Archivregel für zugehöriges erkennbares Element
  - Archivregel für Objekt-Objekt-Beziehung
  - Archivregel für Objekt-Objekt-Beziehung
  - Archivregel für zugehöriges Indikatorobjekt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Archivregel für zugehörige Indikatoren
- Archivregel für zugehöriges erkennbares Element des Indikators

Hinweis:
Um Indikatoren und zugehörige Datensätze zu archivieren, führen Sie das hier für Archivierungsregeln für erkennbare Elemente Ändern Sie die Archivierungsregeln für erkennbare Elementeerläuterte Verfahren aus.

Archivierungsregeln für zugehörige Datensätze

1. Für die zugehörigen Datensätze werden die Datensätze basierend auf dem Quell- und Zielobjekt oder erkennbaren Element archiviert.
2. Die regelmäßige Aufgabe **„Aktualisierung der archivierten Beziehungsspalte“** wird einmal pro Tag ausgelöst und ausgeführt.
3. Sobald die geplante Aufgabe ausgelöst und ausgeführt wird, werden die Spalten „Quelle archiviert“ und „Ziel archiviert“ in den zugehörigen Datensätzen entsprechend aktualisiert.
4. Wenn die Archivierungsregeln für Beziehungen bei der nächsten Ausführung ausgelöst werden und die Datensätze mit den Spalten „Quellarchiviert“ und „Zielarchiviert“ identifizieren, werden sie auf „wahr“ gesetzt, und diese Datensätze werden archiviert.

Zeitplan des Archivierungsauftrags

Sobald die Archivierungsregeln eingerichtet sind und Archivierungsregeln aktiv sind, verarbeitet der Archivierungsauftrag diese Regeln und archiviert die Datensätze.

Die geplante Archivaufgabe wird als einstündiger Wiederholungsintervallauftrag eingerichtet. Sie ruft eine Klasse auf, die den Thread an einen Hintergrund-Thread namens „glide.db.archiver“ übergibt.

Um zu verhindern, dass der Archivierungsprozess zu viele Systemressourcen verbraucht, können die folgenden Archiveigenschaften verwendet werden, um zu steuern, wie viele Datensätze die Archivierungsregel in einem Intervall verarbeitet.

Durch Ändern der Archivierungseigenschaften kann der Archivierungsauftrag die Dauer von 1 Stunde überschreiten, und Sie können mehrere Archivierungsaufträge ausführen.

Eigenschaften der Archivierungsregel

Im Folgenden werden die Eigenschaften der Archivierungsregel beschrieben.

Name	Beschreibung	Typ	Ganzzahliger Wert
glide.db.archive.batch_size	Steuert, wie viele Datensätze eine Archivierungsregel pro Batch-Auftrag verarbeitet.	Ganzzahl	1000
glide.db.archive.sleep_time	Steuert die Ruhezeit zwischen den einzelnen Archivregel-Batch-Auftragsausführungen in Sekunden.	Ganzzahl	1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

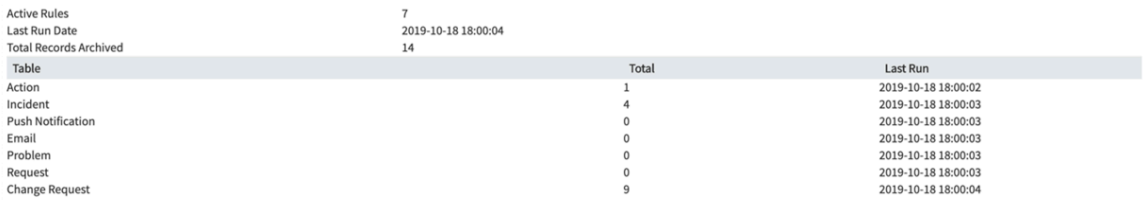
Name	Beschreibung	Typ	Ganzzahliger Wert
glide.db.archive.max_iterations	Steuert die maximale Anzahl von Batch-Aufträgen, die innerhalb einer Stunde ausgeführt werden sollen.	Ganzzahl	10

Diagnoseseite für Archivierungsregeln

Auf dieser Seite können Sie die Details zur Anzahl der aktiven Archivierungsregeln, die Gesamtzahl der archivierten Datensätze und die letzte Ausführung des Archivierungsauftrags anzeigen.

Link zum Zugriff auf die Diagnoseseite:

```
https://<your-instance>.service-now.com/ui_page.do?sys_id=71681edc9f3120007aaa207c7f4bcc2b
```



Active Rules	7
Last Run Date	2019-10-18 18:00:04
Total Records Archived	14

Table	Total	Last Run
Action	1	2019-10-18 18:00:02
Incident	4	2019-10-18 18:00:03
Push Notification	0	2019-10-18 18:00:03
Email	0	2019-10-18 18:00:03
Problem	0	2019-10-18 18:00:03
Request	0	2019-10-18 18:00:03
Change Request	9	2019-10-18 18:00:04

Archivierungsvorgang

1. Laden Sie N Datensätze, die die Archivierungsregelkriterien erfüllen (wobei N die Batchgrößeneigenschaft ist).
2. In Tabelle ar__* einfügen.
3. Löschen Sie den Datensatz aus der ursprünglichen Tabelle.
4. Erstellen Sie einen sys_archive_log-Eintrag.

Wenn ein Datensatz archiviert wird, wird ein Eintrag in die Tabelle „Archivprotokoll“ (sys_archive_log) vorgenommen, und die XML-Datei des Datensatzes wird als Nutzlast gespeichert.

Debugging

Es gibt einige Spalten, die beim Debuggen hilfreich sind: „Archivausführung“, „Archiv“, „Wiederhergestellt“, „ID“ und „Von Tabelle“.

1. **Archivierungsausführung**: Gibt Ihnen die Details, welche bestimmte Archivierungsausführung diesen Datensatz archiviert hat.
2. **Archiv**: Die Archivierungsregel, die die Bedingung erfüllt hat.
3. **Wiederhergestellt**: Dieses Feld ist leer, wenn der Datensatz nicht wiederhergestellt wurde. Wenn die Datensätze wiederhergestellt wurden, enthält dieses Feld das Datum und die Uhrzeit der Wiederherstellung des Datensatzes.
4. **Aus Tabelle**: Die Tabelle, aus der der Datensatz entfernt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Durch das Löschen eines Archivprotokolleintrags können Sie die Daten für die archivierten Datensätze nicht wiederherstellen.

Das Vorhandensein eines Eintrags im Archivprotokoll ist alles, was das System darüber wissen muss, dass der Datensatz einmal archiviert wurde (z. B. wiederhergestellt), in jedem Fall, wenn er übersprungen wurde. Dies bedeutet, dass die Archivierungs-Engine etwas nicht erneut archiviert die wiederhergestellt wurde.

Zugehörige Datensätze und Anhänge können ebenfalls archiviert werden, da Sie in der Archivierungsregel angeben können, welche zugehörigen Datensätze archiviert werden sollen. Wenn Sie den ursprünglichen Datensatz wiederherstellen, müssen auch die zugehörigen Datensätze wiederhergestellt werden (dies erfolgt nicht automatisch, da die Tabellen der zugehörigen Datensätze nach der Archivierung unabhängig sind).

Initiiert die Zerstörregel über ein Skript

Erstellen Sie eine Vernichtungsregel, um die archivierten Datensätze und zugehörigen Datensätze nach einer angegebenen Zeit zu löschen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

- `neuer GlideArchiver().archiveDestroomByRule(xxxx);` wobei xxx für die sys_id der Vernichtungsregel steht.
- Wenn Sie die Eigenschaften der Vernichtungsregel ändern müssen, die für Ihre archivierten Daten ausgeführt werden, lesen Sie die Informationen unter Archivregel- und Vernichtungsregeleigenschaften .

Zeigen Sie die Vernichtungsregeln für die archivierten Datensätze an:

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivlöschregeln**.
2. Wählen Sie einen beliebigen Datensatz aus, um die Vernichtungsregel anzuzeigen.
   Basierend auf der Archivierungsdauer werden die Datensätze automatisch aus der Anwendung entfernt. Wenn Sie die Vernichtungsregel manuell ausführen möchten, **führen Sie die Option „Archivlöschung jetzt ausführen“ aus**, oder wenn Sie die standardmäßige Archivierungsdauer ändern möchten, bearbeiten oder ändern Sie das Formular entsprechend.

   Hinweis:
   Für jede Tabelle gilt eine individuelle Vernichtungsregel.

Zeigen Sie Zerstörregeln in TISC an

Zeigen Sie die Vernichtungsregeln an, die im Basissystem bereitgestellt wurden.

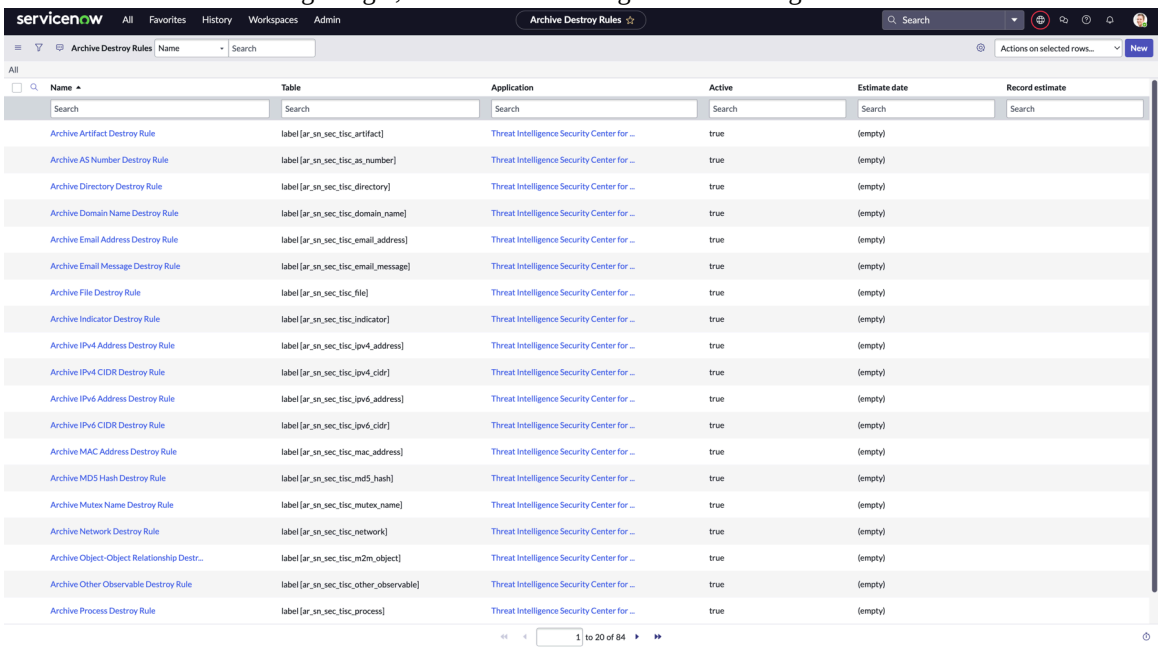
Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivlöschregeln**.
   Die Liste der Vernichtungsregeln, die für TISC gelten, wird angezeigt. Diese Vernichtungsregeln sind für jeden Objekttyp unterschiedlich und gelten unabhängig voneinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Zeigen Sie die anwendbaren Vernichtungsregeln für TISC an.
3. Klicken Sie auf eine beliebige Regel, um die Archivierungsdauer anzuzeigen.



Einschränkungen bei der Datenarchivierung

Es gibt ein Limit für die Größe einer Archivtabelle, die Sie zum Speichern von Daten erstellen können. Der Grenzwert beruht auf der Größe der Daten, nicht auf der Anzahl der Datensätze.

Wenn Sie einen Fehler erhalten, dass eine Archivtabelle nicht erstellt werden konnte, hängt dies möglicherweise mit dieser Größenbeschränkung zusammen. Weitere Informationen finden Sie unter Größenbeschränkungen für Datenarchiv-Tabellen .

Archivierungsregeln werden überwacht

Dieser Abschnitt hilft Ihnen, die Archivierungsregeln nachzuverfolgen und zu überwachen.

Regelbeschreibung	Navigieren zu	Erwartete Ausgabe
Aktive Archiv-Threads	**Systemarchivierung** > **Archivstatus**	• **Name**: glde.db.archiver.xxxx, wobei „xxxx“ für die sysid der entsprechenden Archivregel steht. • **Wert**: beginnt mit „Aktiv“ oder „Leerlauf“.
Gesamtfortschritt der Archivierung	**Systemarchivierung** > **Archivregeln**	Die Schätzungsspalte gibt an, wie viele Datensätze noch zu archivieren sind. Wird jede Stunde vor der nächsten Iteration aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelbeschreibung	Navigieren zu	Erwartete Ausgabe
Individueller Archivfortschritt	**Systemarchivierung** > **Archivregeln**	• **Dauer**: ca. 45 Minuten • **Primär gesamt**: 30.000 pro Ausführung.

Lernressourcen

Im folgenden Abschnitt erfahren Sie mehr über den Datenarchivierungsprozess und Best Practices.

Referenzen

Referenztitel	Referenzlinks
Stellt mehrere archivierte zugehörige Datensätze eines archivierten Datensatzes im Batch-Modus wieder her.	KB0819650
Datenarchivierung: Übersicht und häufig gestellte Fragen	KB0785300
Archivierung | Splunk-Suchen	KB0782324
Aufgrund der Archivierung verwaiste Anhangsdokument-Datensätze	KB0647663
Archivauftragsarchitektur, Setup von Archivregeln, Archivlöschregeln	
Multi-Thread-Archivierung	KB0821186
Best Practices für die Archivierung	KB0999731
Datenarchivierung auf servicenow.com/docs	Systemadministration der Now Platform
Archivregel- und Vernichtungsregeleigenschaften finden Sie unter servicenow.com/docs	Systemadministration der Now Platform
TOI-Aufzeichnung archivieren	Archivierung
Leistungsschulungsvideos	KB0960168

Funktions-Flow zur TISC-Datenverarbeitung

Das Threat Intelligence-Sicherheitszentrum (TISC) bietet eine Lösung, die die Datenerfassung und -verarbeitung automatisiert und so die Belastung der Threat Intel-Analysten verringert, indem manuelle Schritte vermieden werden.

Das Threat Intelligence Security Center (TISC) sammelt Informationen mit einer der folgenden Methoden:

1. Erfassung aus Datenquellen, die vorkonfiguriert sind und nach einem Zeitplan ausgeführt werden.
2. Threat Intel-Analysten importieren Daten mithilfe der Funktion „Import Intelligence“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Durch manuelle Erstellung einzelner Datensätze in der Anwendung

> **Hinweis:**
> Die in der Anwendung gesammelten Daten werden verarbeitet, um die Informationen vor dem Laden in die Threat Intel-Bibliothek zu normalisieren, zu deduplizieren und zusammenzufassen.

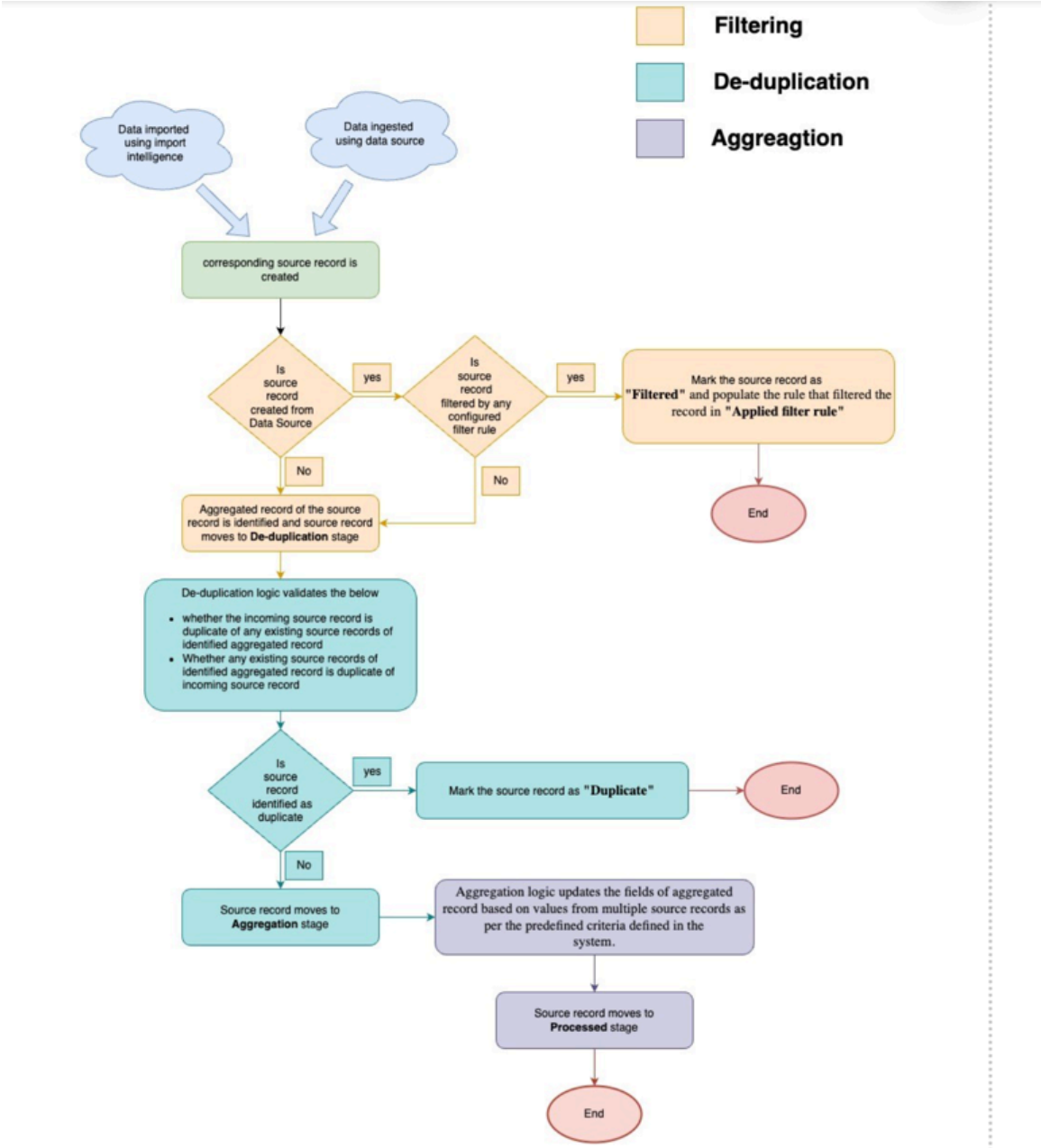
Grundlegende Begriffe aus der Datenverarbeitung

1. Quelltabellen: Die Quelltabellen enthalten die Daten, die sich auf die Entitäten beziehen, die aus mehreren Quellen abgerufen werden. Dann werden die Datensätze von jeder Quelle erstellt.
2. Aggregierte Datensätze: Die Tabelle „Aggregierte Datensätze“ enthält die Daten, die sich auf eine bestimmte Entität beziehen, indem die Daten aus allen Quelldatensätzen einer bestimmten Entität aggregiert werden.

TISC-Datenfluss

1. Bei einer erfolgreichen Ausführung des Imports der Intelligenz/Datenquelle würden die Datensätze in den entsprechenden Quelltabellen erstellt.
2. Sobald Daten in der Quelltabelle eingehen, durchlaufen die Daten eine Filterlogik, um zu validieren, ob der Datensatz basierend auf den konfigurierten **eingehenden Filterregeln**gefiltert werden sollte. (Angenommen, SourceRecord1 ist der Quelldatensatz für unsere Erklärung.)
3. Wenn der Datensatz von einer der konfigurierten eingehenden Filterregeln gefiltert wird, wird der entsprechende Quelldatensatz (SourceRecord1) als **Gefiltert** markiert, und die Regel, die den Datensatz gefiltert hat, finden Sie unter Angewendete Filterregel.
4. Angenommen, der Quelldatensatz (SourceRecord1) wird zu AggregateRecord1 zusammengefasst.
5. Wenn der Datensatz nicht gefiltert wird, wird der Datensatz für die Deduplizierung markiert, indem der Verarbeitungsstatus auf Bereit für Deduplizierung festgelegt wird.
6. Die Deduplizierungslogik validiert Folgendes:
   a. Gibt an, ob der eingehende Quelldatensatz (SourceRecord1) ein Duplikat eines vorhandenen Quelldatensatzes für AggregateRecord1 ist.
   b. Jeder der vorhandenen Quelldatensätze für AggregateRecord1 ist ein Duplikat des eingehenden Quelldatensatzes (SourceRecord1).
7. Jede Entität verfügt über bestimmte Felder und Beziehungen, auf deren Grundlage der Quelldatensatz für die Duplizierung validiert wird.
8. Wenn der eingehende Quelldatensatz (SourceRecord1) ein Duplikat eines vorhandenen Quelldatensatzes von AggregateRecord1 ist, wird der eingehende Quelldatensatz (SourceRecord1) als Duplikat markiert.
9. Wenn einer der vorhandenen Quelldatensätze (Vorhandener Quelldatensatz1) von „AggregateRecord1“ als Duplikat des eingehenden Quelldatensatzes (SourceRecord1) identifiziert wird, wird der vorhandene Quelldatensatz (Vorhandener Quelldatensatz1) als Duplikat markiert, und der eingehende Quelldatensatz (SourceRecord1) wird für die Zusammenfassung markiert durch Festlegen des Verarbeitungsstatus auf „Bereit für Zusammenfassung“.
10. Im Rahmen der Zusammenfassung werden die Felder des aggregierten Datensatzes „AggregateRecord1“ basierend auf Werten aus mehreren Quelldatensätzen aktualisiert und gemäß den im System definierten vordefinierten Kriterien aggregiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Data Loss Prevention Incident Response

Mit der Anwendung Data Loss Prevention Incident Response (DLP IR) können Sie den Nachbesserungs-Workflow von DLP-Incidents aus mehreren Quellen wie Endpunkt, Netzwerk, E-Mail und Cloud überprüfen und verwalten.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Data Loss Prevention Incident Response

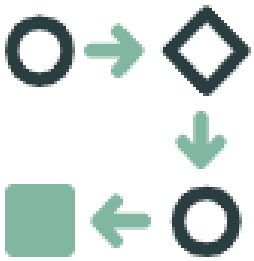
Untersuchen

Erfahren Sie, wie Analysten und Administratoren DLP Incident Response verwenden

Installieren und konfigurieren Sie

Die Anwendung „DLP Incident Response“ installieren und konfigurieren

Verwalten



Administrationsaufgaben zur Verwaltung der DLP-Incidents auf der Now Platform

Verwenden

Aktualisieren und verwalten Sie Incidents mithilfe des DLP-Endanwenderportals, des DLP-Vorgangsportals und des DLP-Dashboards.

integrieren

Erweitern Sie DLP-Fähigkeiten durch die Integration mit Anwendungen von Drittparteien

Automatische Übersetzung

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Data Loss Prevention Incident Response erkunden

Erkunden Sie die Anwendung Data Loss Prevention Incident Response, um zu erfahren, wie Sie vertrauliche Informationen für Ihre Kunden verwalten, z. B. Finanzdaten und geschützte Daten, Gesundheitsdatensätze oder Sozialversicherungsnummern.

Datenverlust tritt auf, wenn vertrauliche oder vertrauliche Informationen das Unternehmensnetzwerk aufgrund nicht autorisierter Kommunikation verlassen. Mit der DLP-Anwendung können Sie Ihre Kanäle für Datenverlust identifizieren, darauf reagieren und sie schützen.

Durch die Verwendung der Anwendung Data Loss Prevention Incident Response bietet Ihre Organisation die folgenden wichtigen Vorteile:

- Integrieren Sie in mehrere DLP-Lösungen von Drittparteien, um eine einheitliche Ansicht der Incidents im Now Platformzu erhalten.
- Überwachen Sie Incidents, und weisen Sie sie den Endanwendern zu, um das DLP-Incident-Management zu optimieren.
- Coachen Sie Ihre Mitarbeiter mithilfe der anwenderdefinierten E-Mail-Vorlagen und Benachrichtigungen, die für jeden Incident sowie in Form von Digest gesendet werden.
- Eskalieren Sie die überfälligen DLP-Incidents von den Endanwendern zu den Managern.
- Zeigen Sie Zusammenfassungsberichte über offene Incidents nach Richtlinie, Schweregrad, häufigsten Vergehen usw. an.
- Verfolgen Sie DLP-Incident-Trends, falsch positive Trends und Nachbesserungstrends.

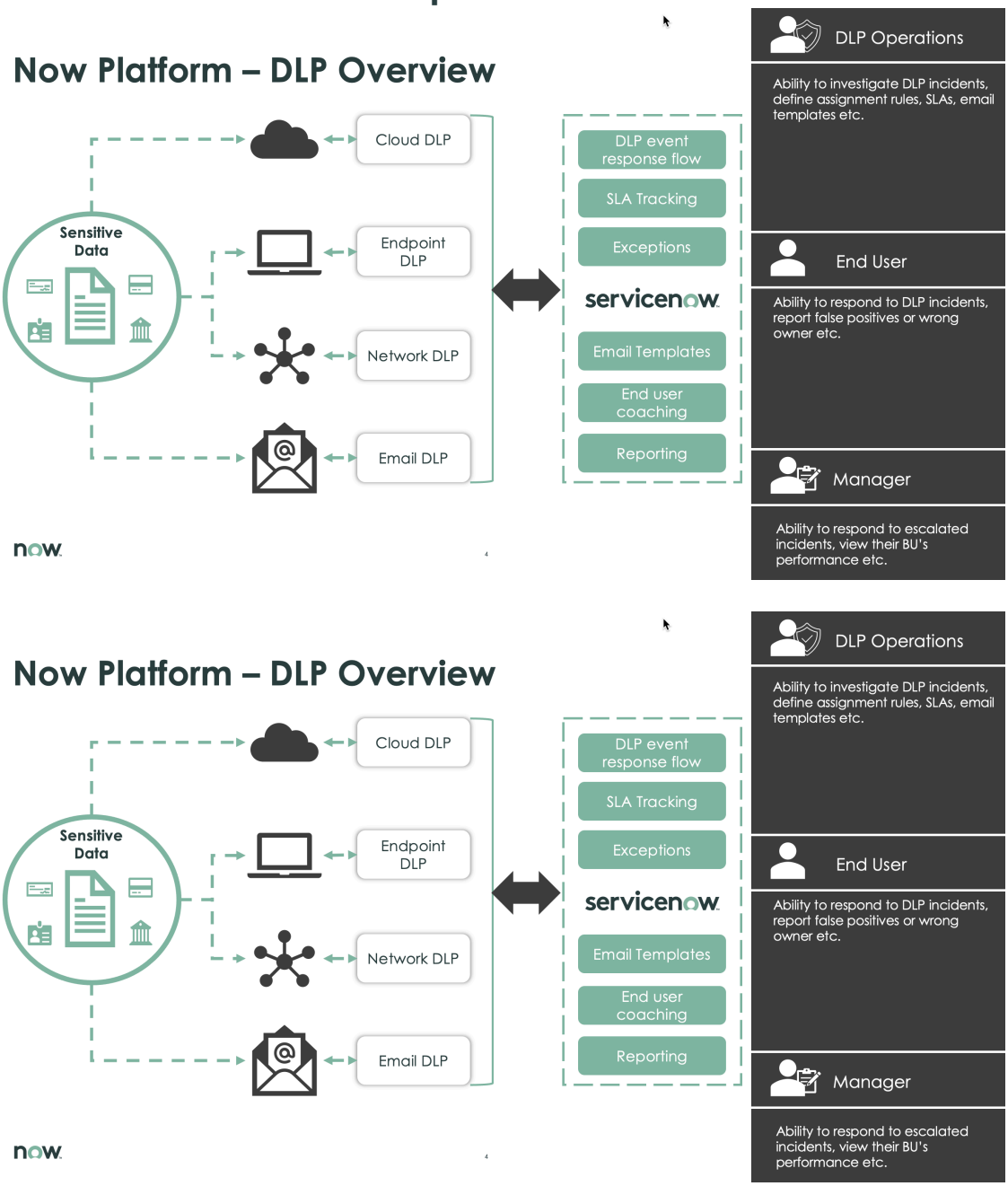
In diesem Abschnitt erfahren Sie mehr über die wichtigsten Funktionen und die verschiedenen Rollen, die bei der Arbeit mit DLP-Incidents erforderlich sind.

Übersicht über DLP Incident Response

Erfahren Sie, wie Sie die Anwendungen Now Platform und Data Loss Prevention Incident Response (DLP IR) verwenden können. Verwalten Sie vertrauliche Informationen für Ihre Kunden, z. B. Finanz- und Eigentumsdaten, Gesundheitsdatensätze oder Sozialversicherungsnummern. Automatisieren Sie Nachbesserungs-Workflows mit der Anwendung DLP Incident Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Data Loss Prevention Incident Response und Now Platform



Automatische Übersetzung

1. Dies ist ein anklickbares Bild. Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
2. DLP-Administratoraufgaben: Dies ist ein anklickbares Bild. Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
3. DLP-Endanwenderportal verwenden: Dies ist ein anklickbares Bild, Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
4. DLP-Vorgangsportal verwenden: Dies ist ein anklickbares Bild, Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
5. DLP-Dashboard wird verwendet – Dies ist ein anklickbares Bild, Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren

Die Anwendung Data Loss Prevention Incident Response enthält die folgenden Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Endanwenderarbeitsbereich, in dem Ihre Endanwender oder Mitarbeiter die zugewiesenen DLP-Incidents überprüfen und darauf reagieren können.
- Ein Manager-Arbeitsbereich, in dem Manager die eskalierten DLP-Incidents überprüfen und entsprechend reagieren können.
- Ein einheitlicher Arbeitsbereich, in dem Ihr DLP-Betriebsteam die Trends für offene Incidents, Top-Angreifer und Incidents nach Scan-Quelle nachverfolgen und die DLP-Incidents über mehrere Quellen (Endpunkte, Netzwerke und E-Mail) hinweg anzeigen, bearbeiten, zuweisen und schließen kann.
- Administrative Steuerungen, die E-Mail-Vorlagen für Coaching und Kommunikation mit Endanwendern, Zuweisungsregeln für die automatische Zuweisung von Incidents, Regeln für automatische Eskalation und Delegierung von Antworten auf Incidents definieren.

Erste Schritte mit DLP Incident Response

Lesen Sie sich die folgenden Informationen durch, bevor Sie mit der Einrichtung Ihrer Data Loss Prevention Incident Response (DLP IR)-Anwendung beginnen.

Prüfliste

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie die erforderlichen Rollen Now Platform und DLP zugewiesen haben.	DLP Incident Response unterstützt die folgenden Rollen: • Der -Administrator (admin) installiert die Anwendungen aus ServiceNow Store und weist den DLP-Administrator (sn_dlir.admin) zu. • sn_dlir.admin • sn_dlir.analyst
Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Anwendung Data Loss Prevention Incident Response erforderlich sind, installiert und aktiviert sind.	Das Plugin Data Loss Prevention Incident Response (com.snc.data_loss_incident) ist erforderlich, um das Produkt Data Loss Prevention Incident Response zu unterstützen. Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Storeinstalliert und aktiviert sind. Falls nicht installiert, installieren und aktivieren Sie jeweils nur eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten: • Data Loss Prevention Incident Response (com.snc.data_loss_incident) • Security Support Common Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Berechtigungen für ein Produkt oder eine Anwendung von Security Operations

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	erhalten oder eine Anwendung aus dem ServiceNow Store aktivieren.
Domänentrennung	Überprüfen Sie das Thema Domain Separation und DLP Incident Response, wenn Sie Daten, Prozesse und administrative Aufgaben trennen möchten.

DLP IR Incident Response installieren und konfigurieren

Laden Sie die Anwendung Data Loss Prevention Incident Response (DLP IR) von ServiceNow Store herunter, und installieren Sie sie in Ihrer -Instanz.

Bevor Sie die Workflows für die Integration aufrufen, installieren und konfigurieren Sie die Anwendung Data Loss Prevention Incident Response aus dem ServiceNow Store in Ihrer Instanz Now Platform.

Installieren und konfigurieren Sie die Anwendung „DLP Incident Response“.

Verwalten Sie vertrauliche Informationen, und automatisieren Sie die Nachbesserungs-Workflows mithilfe der Anwendung Data Loss Prevention Incident Response (DLP IR) in Ihrer Instanz Now Platform.

Vorbereitungen

Bevor Sie die Konfigurationsschritte abschließen können, müssen Sie die Anwendung von ServiceNow Store herunterladen und in Ihrer -Instanz installieren.

Erforderliche Rolle: admin und sn_dlir.admin

Prozedur

1. Befolgen Sie die Anweisungen zum Herunterladen einer Anwendung aus dem ServiceNow Store.
2. Nachdem Sie die Anwendung **DLP Incident Response** und alle zugehörigen Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **DLP-Administration** > **Standardkonfiguration** um die restliche Anwendungskonfigurationabzuschließen.

Domain Separation und DLP Incident Response

Sie können Domain Separation mit DLP Incident Response verwenden, um die Daten, Prozesse und Verwaltungsaufgaben in logische Gruppen zu unterteilen, die als Domänen bezeichnet werden. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe: Standard

- Umfasst alle Aspekte des **Basis** -Supports.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation mit DLP Incident Response

- Erstellen Sie in der entsprechenden Domäne einen Anwender mit den erforderlichen Rollen „sn_dlir.admin“ und „sn_dlir.analyst“.
- Führen Sie die Konfigurationen von DLP Incident Response in der entsprechenden Domäne durch.

Verwaltung von DLP Incident Response

Sie können Regeln einrichten und zuweisen, Fälligkeitsdatumsregeln konfigurieren, E-Mail-Vorlagen verwenden, Antwortaktionen für Endanwender konfigurieren und vieles mehr, um die Data Loss Prevention Incident Response (DLP IR) Incidents in Now Platformzu verwalten.

Mit der Anwendung Data Loss Prevention Incident Response können Sie die folgenden Konfigurationen durchführen.

Standardmäßige DLP-Konfigurationseinstellungen

Definieren Sie die Standardkonfigurationseinstellungen für Data Loss Prevention Incident Response (DLP IR) Incidents, um die Einstellungen für Incident-Benachrichtigungen und Incident-Zuweisungen für Ihre Endanwender zu identifizieren und einzurichten.

Vorbereitungen
Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird
Sie können dieses Modul verwenden, um die Standardkonfigurationseinstellungen zu definieren, wenn die Core-Zuweisungsregeln und Identifier-Regeln ausgeschöpft sind und keiner Bedingung oder keinem Benutzer zugeordnet werden können. Sie können auch Endanwender-Suchregeln und Zuweisungsregeln definieren und erneut auf vorhandene aktive DLP-Incidents anwenden.

Mit der Endanwender-Incident-Benachrichtigung können Sie die Häufigkeit angeben, mit der E-Mail-Benachrichtigungen an Ihre Endanwender gesendet werden. Sie können beispielsweise Benachrichtigungseinstellungen einrichten, um Incidents zu sammeln und einmal pro Woche einen E-Mail-Digest zu senden. Durch das Zuweisen eines incident können Sie angeben, welcher Gruppe die DLP-Incidents zunächst zugewiesen werden. Sie

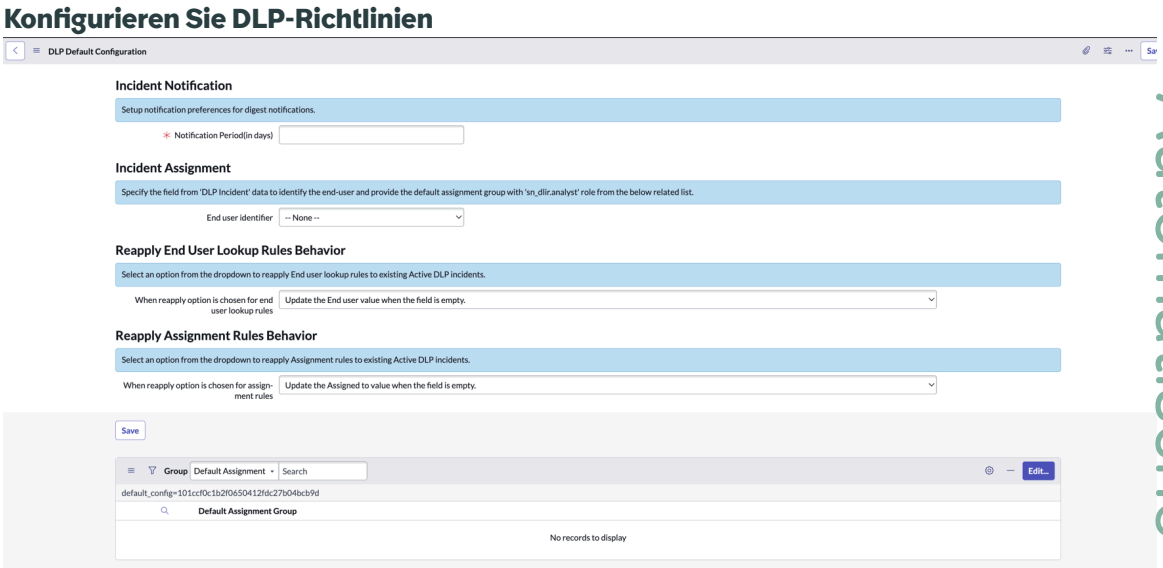
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können auch angeben, wie die Endanwender vom DLP-Betriebsteam weiter identifiziert werden.

Angenommen, ein Benutzer hat Kreditkarteninformationen in einer Datei in einem Netzwerk gespeichert. Wenn das DLP-Integrationsprodukt einer Drittpartei einen Incident für einen Verstoß gegen die Richtlinie für vertrauliche Daten erstellt, enthalten die von Now Platform DLP erfassten Incident-Daten Informationen über den Endanwender. Sie können den Incident dann dem richtigen Endanwender zuweisen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Standardkonfiguration**.



2. Füllen Sie die Felder des Formulars aus.

Formular „DLP-Standardkonfiguration“.

Konfigurationsname	Feld	Beschreibung
Endanwender-Incident-Benachrichtigung	Benachrichtigungszeitraum (Tage)	Definieren Sie die Anzahl der Tage, nach denen eine E-Mail-Benachrichtigung an den Endanwender gesendet werden soll. Die Anzahl der Tage muss zwischen 1 und 60 Tagen liegen.
	Übergeordneten Status automatisch basierend auf geklonten/untergeordneten Incidents aktualisieren	Option zur automatischen Aktualisierung des übergeordneten Status-Incident basierend auf den geklonten oder untergeordneten Incidents.
Incident-Zuweisung	Bezeichner des Endanwenders	Geben Sie das Feld aus Incident-Daten an, das zum Identifizieren des Endanwenders verwendet werden soll. Mögliche Werte: ○ **E-Mail des Datenbesitzers** ○ **Ziel** ○ **Datei erstellt von** ○ **Datei geändert von**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsname	Feld	Beschreibung
		○ **Dateibesitzer** ○ **FTP-Anwendername** ○ **Absender**
Verhalten der Endanwender-Suchregeln erneut anwenden	Wenn die Option „Erneut anwenden“ für Suchregeln für Endanwender ausgewählt ist	Option zum erneuten Anwenden von Endanwender-Suchregeln auf vorhandene aktive DLP-Incidents Sie können eine der folgenden Optionen auswählen, um sie erneut anzuwenden: ○ **Endanwenderwert aktualisieren, wenn das Feld leer ist**: Aktualisiert den Endanwenderwert der vorhandenen aktiven DLP-Incidents, wenn dieses Feld leer ist. ○ **Endanwenderwert aktualisieren**: Aktualisiert den Endanwenderwert der vorhandenen aktiven DLP-Incidents. ○ **Werte für „Endanwender“ und „Zugewiesen an“ aktualisieren, wenn beide Felder leer sind**: Aktualisiert die Werte „Endanwender“ und „Zugewiesen an“ der vorhandenen aktiven DLP-Incidents, wenn beide Felder leer sind. **Hinweis:** Wenn diese Option ausgewählt ist, **wird die Option Wert für „Zugewiesen an“ aktualisieren, wenn das Feld leer ist** im Abschnitt „Verhalten bei Zuweisungsregeln erneut anwenden“ automatisch deaktiviert, da sie für beide gilt. ○ **Aktualisiert die Werte „Endanwender“ und „Zugewiesen an“ für alle aktiven DLP-Incidents**: Aktualisiert die Werte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsname	Feld	Beschreibung
		„Endanwender“ und „Zugewiesen an“ für alle aktiven DLP-Incidents. **Hinweis:** Wenn diese Option ausgewählt ist, wird **die Option „Wert für alle aktiven DLP-Incidents aktualisieren“** im Abschnitt „Verhalten von Zuweisungsregeln erneut anwenden“ automatisch deaktiviert, da sie für beide gilt.
Verhalten von Zuweisungsregeln erneut anwenden	Wenn die Option „Erneut anwenden“ für Zuweisungsregeln ausgewählt ist	Option, um Zuweisungsregeln erneut auf vorhandene aktive DLP-Incidents anzuwenden. Sie können eine der folgenden Optionen auswählen, um sie erneut anzuwenden: ○ **Aktualisieren Sie den Wert „Zugewiesen an“, wenn das Feld leer ist.** ○ **Aktualisieren Sie den Wert „Zugewiesen an“ für alle aktiven DLP-Incidents.**

3. Wählen Sie im zugehörigen Listenabschnitt, dem alle DLP-Incidents zugewiesen sind, die **Standardzuweisungsgruppe** aus.
   Klicken Sie auf **Bearbeiten**, um die Benutzergruppe hinzuzufügen. Wenn Sie im Abschnitt „Zugehörige Liste“ **auf „Bearbeiten“** klicken, in den Spalten „ **Sammlungen** “ ein Element auswählen, den ausgewählten Beauftragten dann den Gruppenspalten auf der Seite **„Mitglieder bearbeiten“** hinzufügen und die Liste speichern.

   Hinweis:
   Sie können in der zugehörigen Liste nur Gruppen anzeigen und auswählen, denen die Rolle sn_dlir.analyst zugewiesen wurde. Sie können nur eine Gruppe auswählen.

4. Klicken Sie auf **Speichern**.

Erstellen Sie Suchregeln für Endanwender

Sie können Suchregeln für Endanwender erstellen und konfigurieren und die DLP-Incidents basierend auf diesen Regeln den entsprechenden Endanwendern zuweisen.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Suchregeln für Endanwender, um die Endanwender automatisch DLP-Incidents zuzuweisen, indem nur das Feld „Endanwender“ verwendet wird. Mit der DLP-Endanwender-Suchregel können Sie den Endanwender für DLP-Incidents basierend auf dem Endanwender-Identifier, anwenderdefinierten Attributen oder dem Skript zuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **DLP-Endanwender-Suchregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „DLP-Endanwender-Suchregel“.

Feld	Beschreibung
Name	Name für die Endanwender-Suchregel.
Aktiv	Option, um anzugeben, ob die Endanwender-Suchregel aktiv ist.
Ausführungsreihenfolge	Die Priorität der Endanwender-Suchregel. Dieses Feld gibt die Reihenfolge an, in der die Endanwender-Suchregeln ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen. Die Endanwender-Suchregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für die Endanwender-Suchregel.
Bedingung	Bedingungen im Bedingungsgenerator Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Endanwender-Suchregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**. ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Sie können beispielsweise die Bedingungen für diese Endanwender-Suchregel festlegen, indem Sie die Bedingung **Integrationsquelle**, **enthält**, **Symantec**auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

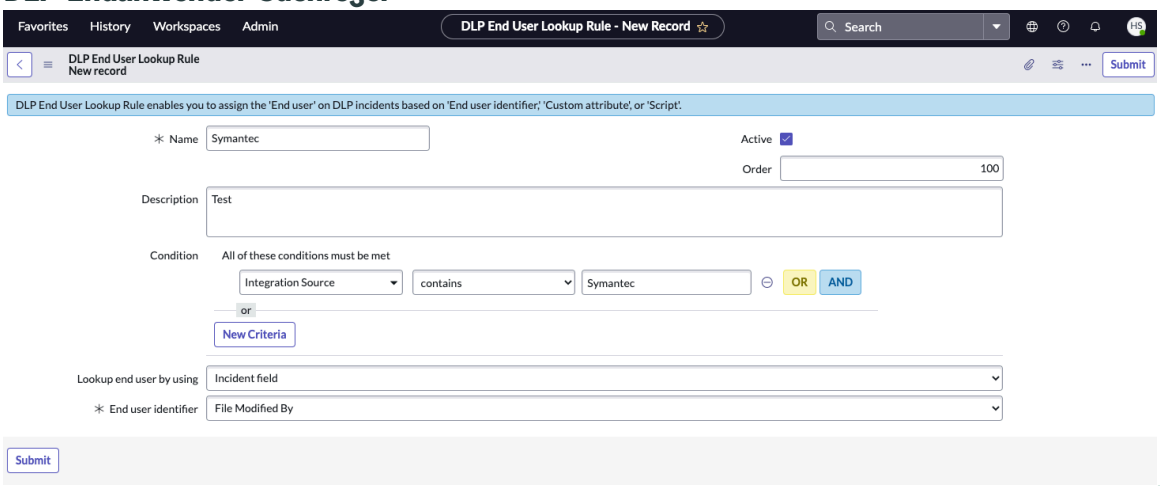
Feld	Beschreibung
	Hinweis: Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Endanwender suchen mithilfe von	Option zur Suche nach Endanwendern mithilfe **des Incident-Felds** oder **Skripts**
Bezeichner des Endanwenders	Der Endanwenderbezeichner des DLP-Incidents. Dieses Feld wird angezeigt, wenn **das Feld Incident** im Feld „ **Endanwender suchen mithilfe von“** ausgewählt wird. Sie können einen der folgenden Endanwender-Bezeichner auswählen: ○ **E-Mail des Datenbesitzers** ○ **Ziel** ○ **Datei erstellt von** ○ **Datei geändert von** ○ **Dateibesitzer** ○ **FTP-Anwendername** ○ **Absender** **Hinweis:** Die oben aufgeführten Endanwender-Bezeichner können mit der Systemeigenschaft `sn_dlir.assignment.fields`konfiguriert werden. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren. ○ **Benutzerdefinierter Benutzer aus Incident**
Anwenderdefiniertes Attribut	Option zum Angeben eines anwenderdefinierten Attributs aus dem Incident, das den Verweis auf einen Benutzer enthält. Dieses Feld wird nur angezeigt, wenn im Feld **Endanwender-Bezeichnerdie Option** ausgewählt ist.
Skript	Sie können den Skript-Editor verwenden, um die Feldwerte während der Erstellung der Endanwender-Suchregel anzupassen und zu formatieren. Sie können beispielsweise das E-Mail-Adressfeld verwenden, um den Endanwender zu identifizieren.

Example

Das folgende Beispiel zeigt eine Endanwender-Suchregel mit dem Namen „Symantec“. Der Bedingungsgenerator erfordert, dass die „Integrationsquelle“ als „Symantec“ angegeben wird. Die Option **„Endanwender suchen mithilfe“** ist auf „Incident-Feld“ und die Option **„Endanwender-Identifier“** auf „Datei geändert von“ festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Endanwender-Suchregel



4. Klicken Sie auf **Absenden**.
   Sie haben auch die Möglichkeit, eine oder mehrere Endanwender-Suchregeln auszuwählen und auf alle vorhandenen DLP-Incidents erneut anzuwenden.
5. Um eine Endanwender-Suchregel erneut auf alle vorhandenen DLP-Incidents anzuwenden, klicken Sie auf **Erneut anwenden**.

Erstellen Sie Zuweisungsregeln

Verwenden Sie diesen Abschnitt, um Zuweisungsregeln zu erstellen. Weisen Sie dann die Incidents Data Loss Prevention Incident Response (DLP IR) Benutzergruppen, Endanwendern, Managern oder Benutzern aus dem Incident zu.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können Zuweisungsregeln verwenden, um DLP-IR-Incidents Benutzergruppen, Endanwendern oder Managern zuzuweisen. Die Zuweisung der DLP-Incidents erfolgt, wenn die Bedingungen in der Zuweisungsregel erfüllt sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Zuweisungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „DLP-Zuweisungsregel“.

Feld	Beschreibung
Name	Name für die Zuweisungsregel.
Aktiv	Option, um anzugeben, ob die Zuweisungsregel aktiv ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ausführungsreihenfolge	Die Priorität der Zuweisungsregel. Dieses Feld gibt die Reihenfolge an, in der die Zuweisungsregeln ausgeführt werden, wenn mindestens zwei Regeln die Auslösebedingungen gemeinsam nutzen. Die Zuweisungsregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für diese Zuweisungsregel.
Bedingung	Bedingungen im Bedingungsgenerator Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Zuweisungsregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**. ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Angenommen, Sie erstellen eine DLP-Zuweisungsregel für einen Endpunkt. Sie können angeben, dass die Bedingungsscanquelle ein Endpunkt-Dateisystem ist, das erfüllt sein muss, bevor Sie einen Incident zuweisen. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Zuweisen an	Zuweisung an eine der folgenden Optionen: ○ Anwendergruppe ○ Endanwender ○ Manager ○ Benutzer aus Incident Die Zuweisung erfolgt, wenn die Bedingungen im Bedingungsgenerator erfüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendergruppe	Option zum Suchen und Auswählen einer Anwendergruppe, der die DLP-Incidents zugewiesen werden sollen. Dieses Feld wird angezeigt, wenn im Feld **Zuweisen aneine Anwendergruppe** ausgewählt wird. **Hinweis:** Sie können nur Gruppen anzeigen und auswählen, denen die Rolle sn_dlir.analyst zugewiesen wurde.
Endanwender	Option, um den DLP-Incident dem Endanwender zuzuweisen. Die Zuweisung erfolgt, wenn die Bedingungen im Bedingungsgenerator erfüllt sind.
Zuweisen mithilfe von Manager-Feldern	Manager des Endanwenders. Dieses Feld wird angezeigt, wenn im Feld **Zuweisen** an die Option **Manager** ausgewählt wird. Sie können die DLP-Incidents einem bestimmten Manager zuweisen, indem Sie eines der Manager-Felder auswählen, z. B. Nachname, E-Mail, Stadt, Mitarbeiternummer.
Anwenderbezeichner	Der Benutzerbezeichner des incident. Dieses Feld wird angezeigt, wenn im Feld **Zuweisen** an die Option **Benutzer aus Incident** ausgewählt wird. Sie können einen der folgenden Benutzerbezeichner auswählen: ○ **E-Mail des Datenbesitzers** ○ **Ziel** ○ **Datei erstellt von** ○ **Datei geändert von** ○ **Dateibesitzer** ○ **FTP-Anwendername** ○ **Absender** ○ **Benutzerdefinierter Benutzer aus Incident**
Anwenderdefiniertes Attribut	Option zum Angeben eines anwenderdefinierten Attributs aus dem Incident, das den Verweis auf einen Benutzer enthält. Dieses Feld wird nur angezeigt, wenn im Feld Benutzer **-BezeichnerAnwenderdefinierter Benutzer aus Incident** ausgewählt ist.
Bewertung anhängen	Option, um anzugeben, ob dem Incident eine Bewertung angefügt werden soll.
Antwortstatus vor der Bewertung	Option zum Auswählen des Status des Incidents, bevor der Endanwender antwortet. Er kann auch ein anwenderdefinierter Status sein.

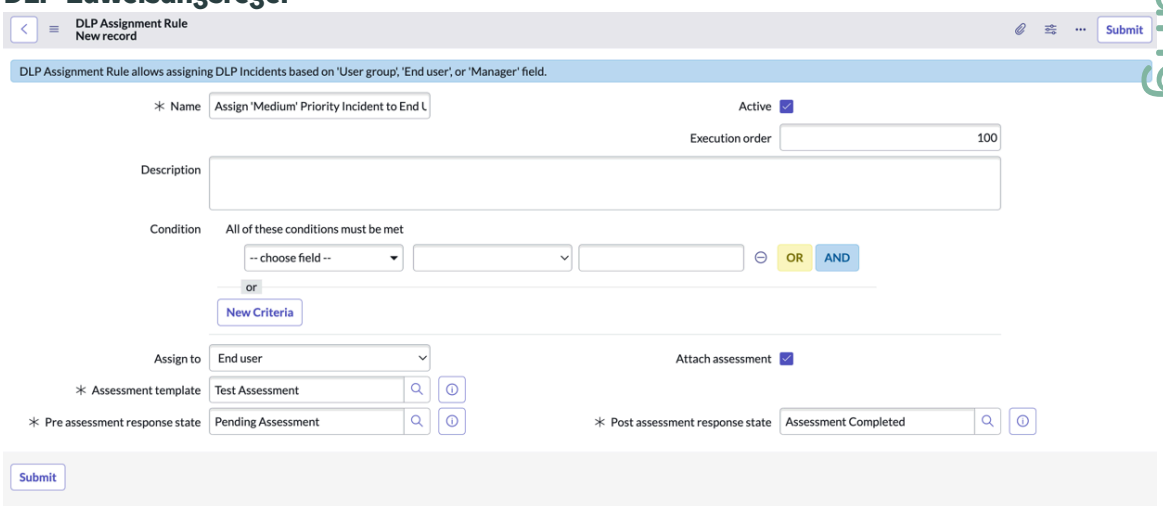
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Standardwert ist Ausstehende Bewertung.
Antwortstatus nach der Bewertung	Option zum Auswählen des Status des DLP-Incident, nachdem der Anwender geantwortet hat. Der Standardwert ist Bewertung abgeschlossen.
Erweitert	Erweiterte Option zum Identifizieren des Endanwenders. Dieses Feld wird nur angezeigt, wenn im Feld Benutzer **-BezeichnerAnwenderdefinierter Benutzer aus Incident** ausgewählt ist. Sie können den Skript-Editor zum Anpassen und Formatieren der Feldwerte während der Erstellung von Zuweisungsregeln verwenden, um den Endanwender zu identifizieren. Anschließend wählen Sie aus, wem Sie den DLP-Incident zuweisen möchten. Dies kann ein Endanwender oder der Manager des Endanwenders sein. Sie können beispielsweise das E-Mail-Adressfeld verwenden, um den Endanwender zu identifizieren.

Example

Das folgende Beispiel zeigt eine Zuweisungsregel mit der Bezeichnung Incident 'Medium' Priority Incident to End User zuweisen. Der Bedingungsgenerator erfordert, dass die Scanquelle auf „Medium“-Prioritäts-Incident an Endanwender zuweisen festgelegtist und dass das Feld Zuweisen an auf Endanwenderfestgelegt ist. Anschließend können Sie nach der E-Mail-Adresse des Endanwenders suchen.

DLP-Zuweisungsregel



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie im zugehörigen Listenabschnitt, in dem alle DLP-Incidents zugewiesen sind, das Feld **Zuweisen an** aus.
   Klicken Sie auf **Bearbeiten**, um die Benutzergruppe hinzuzufügen. Wenn Sie im Abschnitt „Zugehörige Liste“ **auf „Bearbeiten“** klicken, in den Spalten „ **Sammlungen** “ ein Element auswählen, den ausgewählten Beauftragten dann den Gruppenspalten auf der Seite **„Mitglieder bearbeiten“** hinzufügen und die Liste speichern.

   Hinweis:
   Sie können in der zugehörigen Liste nur Gruppen anzeigen und auswählen, denen die Rolle sn_dlir.analyst zugewiesen wurde. Sie können nur eine Gruppe auswählen.

5. Klicken Sie auf **Absenden**.
   Sie haben auch die Möglichkeit, eine oder mehrere Zuweisungsregeln auszuwählen und auf alle vorhandenen DLP-Incidents erneut anzuwenden.
6. Um eine Zuweisungsregel erneut auf alle vorhandenen DLP-Incidents anzuwenden, klicken Sie auf **Erneut anwenden**.

Erstellen Sie Incident-Konsolidierungsregeln

Erstellen Sie eine Incident-Konsolidierungsregel, um mehrere Incidents ähnlicher Art unter einem übergeordneten Incident zu konsolidieren.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Incident-Konsolidierungsregeln, um die DLP-Incidents gleicher Art automatisch unter einem übergeordneten Incident zu konsolidieren. Mit der Konsolidierungsregel für DLP-Incidents können Sie die DLP-Incidents basierend auf der Konfiguration konsolidieren, die für Konsolidierungsdauer und Konsolidierungsidentifizierung angegeben ist.

Hinweis:

Wenn ein konsolidierter Incident erstellt wird, wird er zu einem untergeordneten Element des übergeordneten DLP-Incident. Wenn der Schweregrad des konsolidierten Incidents höher ist als der des übergeordneten Incidents, wird der Schweregrad des übergeordneten Incidents entsprechend dem Schweregrad des untergeordneten Incidents aktualisiert.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Konsolidierungsregeln für DLP-Incidents**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „DLP-Zuweisungsregel“.

Feld	Beschreibung
Name	Name der Incident-Konsolidierungsregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option, um anzugeben, ob die Incident-Konsolidierungsregel aktiv ist.
Ausführungsreihenfolge	Die Priorität der Konsolidierungsregel für Incidents. Dieses Feld gibt die Reihenfolge an, in der die Incident-Konsolidierungsregeln ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen. Die Incident-Konsolidierungsregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für die Incident-Konsolidierungsregel.
Bedingung	Bedingungen im Bedingungsgenerator Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Incident-Konsolidierungsregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**. ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Sie können beispielsweise die Bedingungen für diese Incident-Konsolidierungsregel festlegen, indem Sie die Bedingung **Integrationsquelle**, **enthält**, **Symantec**auswählen. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Konsolidierungsdauer	Option zum Festlegen der Dauer für die Incident-Konsolidierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Incidents in diesem Zeitraum mit denselben Werten für die ausgewählten Felder werden unter dem ersten Incident konsolidiert. Der erste Incident, der dieser Regel entspricht, ist der übergeordnete Incident, und die restlichen Incidents sind untergeordnete Incidents.
Incidents konsolidieren nach	Wählen Sie das Feld „DLP-Incident“ aus, um die Incidents zu konsolidieren, wenn Sie denselben Wert im ausgewählten Feld für verschiedene Incidents haben. Wählen Sie mindestens ein Feld aus.Wählen Sie mindestens ein Feld aus.

Das folgende Beispiel zeigt eine Incident-Konsolidierungsregel mit dem Namen Consolidate incidents for Symantec Integration (Incidents für Symantec-Integration konsolidieren). Der Bedingungsgenerator erfordert Symantec als Integrationsquelle. Die Option **Bedingungsdauer** ist auf 1 Stunde festgelegt, und die Option Richtlinienname ist für **Incident konsolidieren bis**ausgewählt.

Zum Zeitpunkt der Erfassung des Symantec-DLP-Incident wird diese Regel ausgeführt. Wenn mehrere Incidents denselben Richtliniennamen aufweisen, wird der Incident unter dem ersten erfassten Incident konsolidiert, der dieser Regel entspricht.

4. Klicken Sie auf **Absenden**.
   Basierend auf der Konsolidierungsregel konsolidierte Incidents sind in der Liste „Untergeordnete Incidents“ im DLP-Arbeitsbereich für Analysten verfügbar.

Erstellen Sie Regeln für das Fälligkeitsdatum der Antwort

Richten Sie die Regeln für das Fälligkeitsdatum der Antwort ein, um die Zeit zu bestimmen, in der Ihre Endanwender auf die zugewiesenen Data Loss Prevention Incident Response (DLP IR) Incidents reagieren können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können dieses Modul verwenden, um die Regeln für das Fälligkeitsdatum der Antwort für die verschiedenen Arten von DLP-Incidents und die Regeln für die Zählung des Fälligkeitsdatums zu definieren. Nach Ablauf des Fälligkeitsdatums werden die Benutzer über den überfälligen Incident benachrichtigt. Sie haben auch die Möglichkeit, einen überfälligen Incident an eine der folgenden Personen zu eskalieren:

- Manager
- Anwenderdefinierter Anwender aus Incident
- Anwendergruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Beispiel, wenn Sie den überfälligen Incident an einen -Manager eskalieren und Sie maximal drei Eskalationsstufen angegeben haben. Die erste Managerebene wird zuerst benachrichtigt. Wenn der Incident erneut überfällig ist, wird die zweite Managerebene benachrichtigt, gefolgt von der dritten Ebene, wenn der Incident noch überfällig ist. Wenn der Manager einen Delegierten hat, kann er dem Delegierten die Eskalation oder den überfälligen Incident zuweisen.

Sie haben auch die Möglichkeit, mehrere Fälligkeitsdatumsregeln für Antworten zu erstellen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Regeln für Fälligkeitsdatum der Antwort**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Regel für Fälligkeitsdatum der Antwort“.

Feld	Beschreibung
Name	Name der Regel für das Fälligkeitsdatum der Antwort.
Aktiv	Option, um anzugeben, ob die Regel für das Fälligkeitsdatum der Antwort aktiv ist.
Fällig in (Tagen)	Anzahl der Fälligkeitstage.
Fälligkeitsdatum gezählt ab	Startdatum, das zur Berechnung des Fälligkeitsdatums verwendet wird. Das Fälligkeitsdatum kann entweder ab dem Zeitpunkt, zu dem der Benutzer zum ersten Mal über den Incident benachrichtigt wurde, oder ab dem Datum der Incident-Zuweisung berechnet werden.
Vor dem Fälligkeitsdatum benachrichtigen	Option, den Endanwender vor dem Fälligkeitsdatum über den DLP-Incident zu benachrichtigen.
Benachrichtigen am (Tage vor dem Fälligkeitsdatum)	Anzahl der Tage vor dem Fälligkeitsdatum, wenn die Regel eine Benachrichtigung an den Endanwender auslöst.
Beschreibung	Eindeutige Beschreibung für diese Regel für das Fälligkeitsdatum der Antwort.
Bedingung	Bedingungen im Bedingungsgenerator Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Regel für das Fälligkeitsdatum der Antwort zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Eskalation	Option, um den DLP-Incident an jemanden zu eskalieren, wenn das Fälligkeitsdatum der Antwort verletzt wurde. Weitere Informationen finden Sie unter Fügen Sie mehrere Anwender hinzu, um auf DLP-Incidents zuzugreifen
Überfälligen Incident eskalieren an	Option, um anzugeben, ob der Incident an einen Manager, einen anwenderdefinierten Benutzer oder eine Benutzergruppe eskaliert werden soll. Dieses Feld wird nur angezeigt, wenn die Option **Eskalieren** aktiviert ist.
Zuweisen mit	Geben Sie an, wie ein Manager identifiziert werden soll. Dieses Feld wird nur angezeigt, wenn im Feld **Überfälligen Incident eskalieren an** die Option **Manager** ausgewählt wird.
Maximale Eskalationsebenen	Option zum Definieren der maximalen Anzahl von Eskalationsstufen für einen Manager und einen anwenderdefinierten Benutzer. Als Manager-Benutzer oder anwenderdefiniert können Sie eine beliebige Anzahl von Eskalationsebenen definieren. Standardmäßig werden drei Eskalationsstufen bereitgestellt. ○ Als Manager können Sie eine beliebige Anzahl von Eskalationsebenen definieren, indem Sie den Wert in diesem Feld aktualisieren. ○ Als anwenderdefinierter Benutzer können Sie das Symbol + verwenden, um eine beliebige Anzahl von Eskalationsstufen zu definieren.
Anwenderdefiniertes Attribut	Option zum Angeben eines anwenderdefinierten Attributs aus dem Incident, das den Verweis auf einen Benutzer enthält.

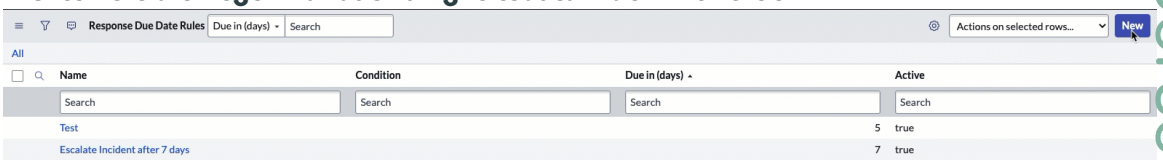
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Feld wird nur angezeigt, wenn im Feld **Überfälligen Incident eskalieren an die Option AnwenderdefinierterAnwender aus Incident** ausgewählt ist.
Anwendergruppe	Option zum Suchen und Auswählen einer Anwendergruppe, an die DLP-Incidents eskaliert werden sollen. Dieses Feld wird nur angezeigt, wenn im Feld **Überfälligen Incident eskalieren an** die **Anwendergruppe** ausgewählt ist. **Hinweis:** Sie können nur Gruppen anzeigen und auswählen, denen die Rolle sn_dlir.analyst zugewiesen wurde.

Example

Das folgende Beispiel zeigt die Regel für das Fälligkeitsdatum der Antwort, um zu bestimmen, wie viel Zeit Sie Ihren Endanwendern geben möchten, um auf die zugewiesenen Data Loss Prevention Incident Response (DLP-)Incidents zu reagieren. Nach der ersten Benachrichtigung des Endanwenders wird das Fälligkeitsdatum der Antwort auf zwei Tage festgelegt. Der Bedingungsgenerator zeigt, dass die Scan-Quelle mit dem Endpunkt-Dateisystem übereinstimmen muss, um mit der Erstellung des Fälligkeitsdatums der Antwort fortzufahren. Die Eskalationsoption ist ausgewählt. Wenn das Fälligkeitsdatum der Antwort nicht eingehalten wird, wird der Incident an den Manager eskaliert.

Richten Sie die Regeln für das Fälligkeitsdatum der Antwort ein



4. Klicken Sie auf **Absenden**.

Fügen Sie mehrere Anwender hinzu, um auf DLP-Incidents zuzugreifen

Verwenden Sie die Eskalationskettenfunktion, um allen entsprechenden Anwendern, die an dem Incident beteiligt sind, den Zugriff auf die DLP-Incidents in der Listenansicht zu ermöglichen, auch wenn der Incident einem anderen Anwender zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

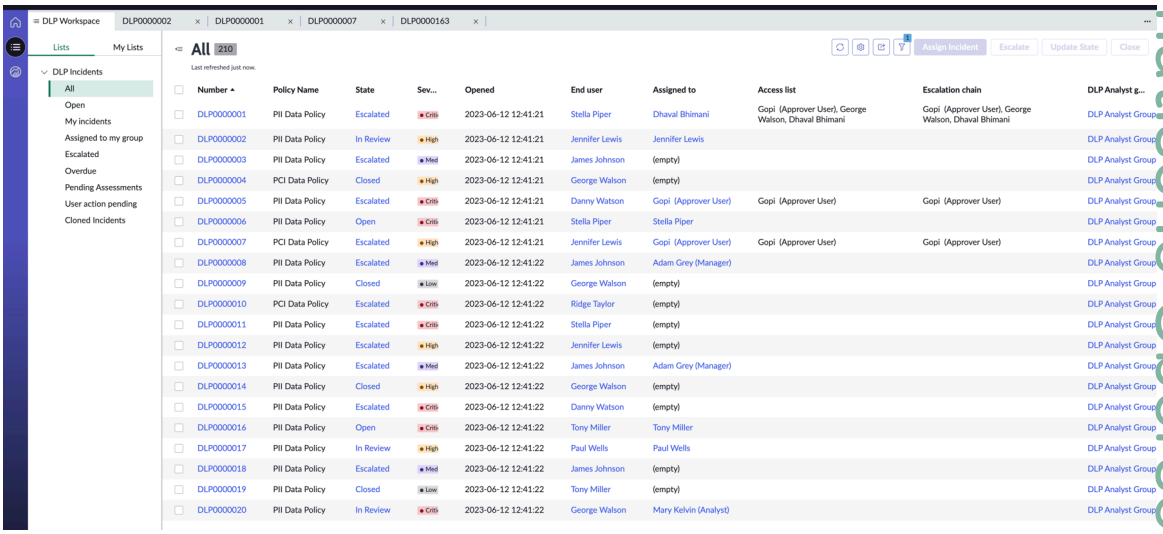
Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.read, sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Prozedur

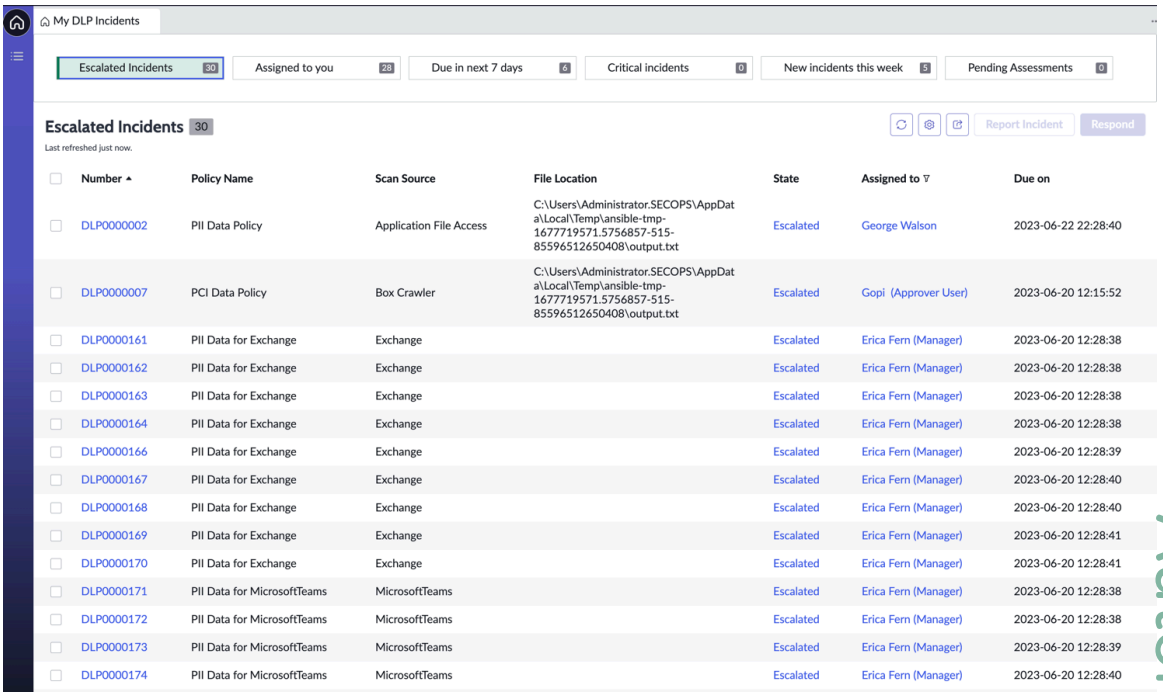
1. Navigieren zu **DLP** > **DLP-Arbeitsbereich für Analysten**.
   In der Listenansicht sollten die Benutzer und ihre Delegierten den DLP-Incident auf der Registerkarte **Eskalierte** Incidents im Endbenutzerportal anzeigen können.
2. Öffnen Sie einen beliebigen Incident.
3. Klicken Sie auf die Schaltfläche **Eskalieren**, um einen Incident zu eskalieren.
4. Wählen Sie den Anwender oder die Anwendergruppe aus der Dropdown-Liste aus.
   Sie können der Eskalationskette mehrere Benutzer hinzufügen. Alle Benutzer, die Zugriff haben, werden im Abschnitt „Details“ der Formularansicht und auf der Registerkarte **Alle** Incidents aufgelistet. Die Eskalationskette wird basierend auf den Konfigurationseinstellungen angezeigt. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren



5. Klicken Sie auf **Absenden**.
   Nach dem Senden wird der Incident einem Manager zugewiesen, der Endanwender kann den Incident jedoch weiterhin anzeigen.
6. Um dies zu überprüfen, navigieren Sie als Endanwender zum **DLP-Anwenderarbeitsbereich**.
   Alle Incidents, die dem Endanwender zugewiesen sind, werden angezeigt.
7. Zeigen Sie die Liste der eskalierten Incidents im Abschnitt **Eskalierte Incidents** an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Zugriffsliste der Anwender auch unter der Spalte **Eskalationskette**in der Listenansicht anzeigen.

8. Öffnen Sie einen beliebigen Incident.
9. Klicken Sie auf die Schaltfläche **Antworten**, um die Antwort auf den Incident zu übermitteln.
10. Wählen Sie die Antwort aus der Dropdown-Liste aus.
11. Klicken Sie auf **Absenden**.

Erstellen Sie Genehmigungsregeln

Erstellen Sie Genehmigungsregeln, um Genehmigungen von verschiedenen Ebenen von genehmigenden Anwendern einzuholen, wenn eine erweiterte Antwortoption ausgewählt wird.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Genehmigungsregeln, um die Einwilligung in Anforderungen zu erteilen, die von Endanwendern für die Genehmigung eines erweiterten Antworttyps gestellt wurden. Der DLP-Administrator kann hier auch mehrere Genehmigungsebenen definieren.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **DLP-Genehmigungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „DLP-Zuweisungsregel“.

Feld	Beschreibung
Name	Name für die Genehmigungsregel.
Aktiv	Option, um anzugeben, ob die Genehmigungsregel aktiv ist.
Ausführungsreihenfolge	Die Priorität der Genehmigungsregel. Dieses Feld gibt die Reihenfolge an, in der die Genehmigungsregeln ausgeführt werden, wenn mindestens zwei Regeln die Auslösebedingungen gemeinsam nutzen. Die Genehmigungsregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für die Genehmigungsregel.
Bedingung	Bedingungen im Bedingungsgenerator Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Genehmigungsregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**. ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Sie können beispielsweise die Bedingungen für diese Incident-Konsolidierungsregel festlegen, indem Sie die Bedingung **Integrationsquelle**, **enthält**, **Microsoft**auswählen.
Gilt für Antwortoptionen	Option zum Auswählen der Antwortoption des Typs „Erweitert“. Sie können mehrere Antwortoptionen auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Genehmigende Person	Wählen Sie aus, welchen Typ von Genehmiger-Anwender Sie festlegen möchten. ○ **Anwendertabelle**: Wählen Sie diese Option aus, wenn Sie den Genehmigeranwender aus der Anwendertabelle (sys_user) auswählen möchten. ○ **Anwenderdefinierte Genehmigungsliste**: Wählen Sie diese Option aus, wenn Sie mehrere Ebenen von anwenderdefinierten Genehmigern für eine einzige Anforderung konfigurieren möchten
Bezeichner des Genehmigers	Dieses Feld wird angezeigt, wenn **Anwendertabelle** für die Option **Genehmiger** ausgewählt ist. Wählen Sie das Feld aus, um den Genehmiger aus der Tabelle „Anwender (sys_user)“ zu identifizieren.
Anzahl der Ebenen	Dieses Feld wird angezeigt, wenn **Anwendertabelle** für die Option **Genehmiger** ausgewählt ist. Endnummer in diesem Feld zum Definieren der Genehmigungsebenen. Wenn beispielsweise im Feld „Anzahl der Ebenen“ der Wert 3 hinzugefügt wird und im Feld „Genehmiger-Identifier“ Manager ausgewählt ist, wird die Genehmigungsanforderung auf drei Genehmigungsebenen übertragen.

Das folgende Beispiel zeigt die Genehmigungsregel, die für eine der erweiterten Antwortoptionen erstellt wurde. Die Bedingung erfordert, dass der Name der Integrationsquelle das Microsoft-Stichwort enthält, das dann diese Konfiguration auslöst.

4. Wählen Sie für die Option **Genehmigerdie Option Anwenderdefinierte Genehmigungsliste**aus.
5. Klicken Sie auf **Absenden**.
6. Die zugehörige Liste**der Genehmigungsebenen** wird in der Formularansicht ausgefüllt.
7. Klicken Sie im Abschnitt **Genehmigungsebenen** auf **Neu**.
8. Füllen Sie die Felder des Formulars aus.

Formular „Genehmigungsebene“

Feld	Beschreibung
Name	Name für die Genehmigungsebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option, um anzugeben, ob die Genehmigungsebene aktiv ist.
level	Die Ebene für die Genehmigungsregel. Dieses Feld gibt die Reihenfolge an, in der die Genehmigungsebenen ausgeführt werden, wenn zwei oder mehr Ebenen konfiguriert sind. Die Genehmigungsebene mit der niedrigsten Nummer hat die höchste Priorität. Um die Betriebsebene festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw. Der Standardwert ist 100.
Genehmigungsregel	Genehmigungsregel, für die Sie diese Konfiguration definieren möchten. Dies ist ein schreibgeschütztes Feld.
Beschreibung	Eindeutige Beschreibung für die Genehmigungsregel.
Genehmigungen erforderlich	Wählen Sie eine Option aus, um zu definieren, ob die Genehmigung von allen konfigurierten Anwendern/Gruppen erforderlich ist oder nur von einem beliebigen Anwender.
Verantwortliche Vertragsgenehmigung	Option zum Auswählen der Genehmiger. **a.** Anwender und Gruppen: **i. Benutzer**: Klicken Sie auf das Symbol um einen bestimmten Benutzer aus der Liste hinzuzufügen. Sie können einen Anwender auch hinzufügen, indem Sie seine E-Mail-Adresse oder Suchoption verwenden. Um sich selbst als Benutzer hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf das . **ii. Gruppen**: Klicken Sie auf<add_icon> um eine bestimmte Gruppe aus der Liste hinzuzufügen. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen. **b. Mithilfe von Skript suchen**: Sie können den Skript-Editor verwenden, um die Feldwerte während der Erstellung der Genehmigungsebene anzupassen und zu formatieren. Sie können beispielsweise

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	das Feld „E-Mail-Adresse“ verwenden, um den Benutzer der genehmigenden Person zu identifizieren.

9. Klicken Sie auf **Absenden**.

Erstellen Sie Vorlagen für Benutzeranweisungen

Erstellen und verwalten Sie Vorlagen für Benutzeranweisungen für DLP-Incidents, damit die Anwender die Anweisungen zur Lösung von Incidents und die nächsten Schritte im Lösungsprozess verstehen.

Vorbereitungen

Die Kartenvorlage für Benutzeranweisungen enthält zwei verschiedene Header, die Ihnen weitere Informationen zu einem bestimmten Incident in der Formularansicht bieten.

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein Incident dem Endanwender zugewiesen wird, muss der Benutzer möglicherweise zusätzliche Anweisungen zur Reaktion auf die Incidents kennen, die Benutzer in die Terminologie einführen und zusätzliche Informationen zum Incident bereitstellen. Diese Vorlagen können Anwender dabei unterstützen, die richtige Antwort auf die DLP-Incidents zu geben.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Vorlagen für Anwenderanweisungen**.

2. Klicken Sie auf **Neu**.

3. Füllen Sie die Felder des Formulars aus.

Bewertung von DLP-Incidents

Feld	Beschreibung
Name	Name der Benutzeranweisungsvorlage.
Kurzbeschreibung	Eindeutige Beschreibung dieser Vorlage für Benutzeranweisungen.
Aktiv	Option, um anzugeben, ob die Benutzeranweisungsvorlage aktiv ist.
Ausführungsbefehl	Priorität der Vorlage für Benutzeranweisungen für Incidents. Dieses Feld gibt die Reihenfolge an, in der der Auftrag ausgeführt wird, um die Vorlage für Benutzeranweisungen auszuwerten, wenn ein Incident erstellt wird. Die Option mit der niedrigsten Nummer hat die höchste Priorität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine beliebige andere Zahl. Der Standardwert ist 100.
Incidents, die der Bedingung entsprechen	Es werden Incidents angezeigt, die den im Bedingungsgenerator definierten Bedingungen entsprechen. Diese Bedingungen basieren auf den DLP-Incident-Daten. Um eine Bedingung für eine Benutzeranweisung zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf UND oder ODER: Wenn AND ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn ODER ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Betrifft	Wählen Sie den Anwender oder die Anwendergruppen aus, für den die Vorlage gilt. Die anderen verfügbaren Optionen sind: ○ **Alle Endanwender**: Aktivieren Sie dieses Kontrollkästchen, wenn die Anweisungsvorlage für alle Anwender gilt. ○ **Alle Prüfer eskalierter Incidents**: Aktivieren Sie dieses Kontrollkästchen, wenn die Vorlage für alle Prüfer der eskalierten Incidents gilt. ○ **Bestimmte Benutzer**: Klicken Sie auf das Symbol, um einen bestimmten Benutzer aus der Liste hinzuzufügen, für den die Bedingungen für DLP-Incidents gelten. Sie können einen Anwender auch hinzufügen, indem Sie seine E-Mail-Adresse oder Suchoption verwenden. Beispiel: Manager der Rechtsabteilung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Um sich selbst als Benutzer hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf das Symbol **Mich hinzufügen**. ○ **Bestimmte Anwendergruppen**: Klicken Sie auf das Symbol, um eine bestimmte Gruppe aus der Liste hinzuzufügen, für die die DLP-Incident-Bedingungen gelten. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen. Beispiel: Umfrageersteller.
Vorlage für Anweisungen: Anweisungen	Fügen Sie Anweisungen im Rich-Text-Editor mit Variablen hinzu, die auf Incident-Ebene verfügbar sind.

4. Führen Sie einen Drilldown zum Abschnitt **„Anweisungsvorlage“** durch, geben Sie die Vorlagenanweisung ein, und fügen Sie in diesem Abschnitt bei Bedarf Informationen zur Incident-Ebene hinzu.
5. Ziehen Sie die erforderlichen Variablen per Drag-and-Drop, um bestimmte Felder dynamisch anzuzeigen.
6. Klicken Sie auf **Absenden**.
   Die Vorlagen für Benutzeranweisungen werden jetzt erstellt, und Sie können auf einen beliebigen Header einer Benutzeranweisung klicken, um die zusätzlichen Details eines DLP-Incident anzuzeigen.

   Weitere Informationen finden Sie unter Data Loss Prevention Incident Response Benutzerarbeitsbereich.

Anwenderanweisungen für die DLP-UI konfigurieren

Konfigurieren Sie die UI-Nachrichten des Systems, um nach Bedarf detaillierte Header für Benutzeranweisungen hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-UI** > **Nachrichten**.
2. Suchen Sie nach **user_instance_card_heading**.

   Standardmäßig sind die beiden UI-Nachrichtenkonfigurationen, die Anwendern bereitgestellt werden, „user_insstruct_card_heading“ und „user_insstruct_modal_window_heading“.

3. Klicken Sie auf eine der Anwenderanweisungen, um sie zu aktualisieren oder zu ändern.

Erstellen Sie E-Mail-Vorlagen

Erstellen und verwalten Sie die vorkonfigurierten E-Mail-Vorlagen zum Senden von Benachrichtigungen an Endanwender, Benutzergruppen oder Manager. Mit diesen Vorlagen können Sie Endanwender über Incidents Data Loss Prevention Incident Response (DLP IR) beraten und mit ihnen kommunizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

> **Wichtig:**
> Damit Analysten die E-Mail-Kommunikation eines DLP-Incident im Aktivitätenstrom anzeigen können, müssen Sie die Rolle „sn_dlir.analyst“ in der globalen Systemeigenschaft „glide.ui.activity.email_roles“hinzufügen oder anfügen.

Warum und wann dieser Vorgang ausgeführt wird

E-Mail-Benachrichtigungen werden nach den Incident-Benachrichtigungen, die an die Endanwender gesendet werden, den Eskalationsbenachrichtigungen, die an die Manager gesendet werden, oder den Fälligkeitsdatumsbenachrichtigungen kategorisiert. Sie können E-Mail-Benachrichtigungen über die Fälligkeitstermine von DLP-Incidents senden oder Endanwender sogar beraten, was zu tun ist, wenn bestimmte Bedingungen im E-Mail-Bedingungsfilter erfüllt sind.

Mit DLP-E-Mail-Vorlagen können Sie E-Mail-Benachrichtigungen für Endanwender, Manager und Analysten senden. Sie können die Vorlagen so konfigurieren, dass sie pro Incident oder als Digest gesendet werden. Ihr E-Mail-Betreff und -Text können Variablen enthalten, sodass Sie Ihre vorhandenen Inhalte wiederverwenden können.

DLP stellt die folgenden vorkonfigurierten E-Mail-Vorlagen basierend auf den -Kategorien bereit:

- **DLP-E-Mail-Vorlage – Genehmigung pro Incident – Benachrichtigung:** Benachrichtigen Sie Anwender über die Genehmigung ihrer Anforderungen.
- **DLP-E-Mail-Vorlage – Eskalationsbenachrichtigung:** Senden Sie Eskalationsbenachrichtigungen in Form von Digests an Manager.
- **DLP-E-Mail-Vorlage – Benachrichtigung über ausstehende Genehmigung:** Benachrichtigen Sie Genehmiger über ausstehende Elemente.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Stornierung der Genehmigungsanforderung pro Incident:**Benachrichtigen Sie Anwender über eine Genehmigungsanforderung, die vom DLP-Analystenteam abgebrochen wurde.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Abschluss der Anwenderantwort:** Benachrichtigen Sie das DLP-Analystenteam über die von Anwendern übermittelte Antwort.
- **DLP-E-Mail-Vorlage – Anwender-Incident-Benachrichtigung:**Dies ist eine Standardvorlage für Anwender-Digest-Benachrichtigungen. Senden Sie alle paar Tage Incident-Benachrichtigungen in Form von Zusammenfassungen an die Endanwender, auch wenn keine neuen Incidents vorhanden sind, um die Anwender über die Gesamtzahl der Incidents für den Namen des jeweiligen Anwenders zu informieren. Sie können auch Digest-Benachrichtigungen senden, um die Benutzer über die nächsten Fälligkeitstermine von DLP-Incidents mit dem Schweregrad „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ zu benachrichtigen.
- **DLP-E-Mail-Vorlage – Pro Incident – Benachrichtigung über ausstehende Genehmigung**: Benachrichtigen Sie Genehmiger über ausstehende Genehmigungen.
- **DLP-E-Mail-Vorlage – Ablehnungsbenachrichtigung:** Ablehnungsbenachrichtigung an anfordernde Person senden.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Fälligkeitsdatum:** Senden Sie eine Benachrichtigung über das Fälligkeitsdatum des Incidents. Wenn dem Endanwender ein DLP-Incident zugewiesen wird und der Endanwender vor dem Fälligkeitsdatum keine Aktion ausgeführt hat, wird eine E-Mail-Benachrichtigung an den Endanwender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gesendet. Sie haben auch die Möglichkeit, den DLP-Incident an einen Manager, einen anwenderdefinierten Benutzer oder eine Benutzergruppe zu eskalieren, wenn das Fälligkeitsdatum der Antwort nicht eingehalten wurde.

Hinweis:
Benachrichtigungen über Fälligkeitstermine müssen in Form von Digest-Formularen vorliegen.

- **DLP-E-Mail-Vorlage – Benutzerantwortbenachrichtigung pro Incident:** Benachrichtigen Sie Analysten über die von Anwendern pro Incident übermittelte Antwort.
- **DLP-E-Mail-Vorlage – Eskalationsbenachrichtigung pro Incident:** Benachrichtigen Sie Manager über Eskalationen pro Incident.
- **DLP-E-Mail-Vorlage – Benutzerbenachrichtigung pro Incident:** Benachrichtigen Sie Benutzer über Zuweisungen pro Incident.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **E-Mail-Vorlagen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „DLP-E-Mail-Vorlage“.

Feld	Beschreibung
Name	Name der E-Mail-Vorlage.
Aktiv	Option, um anzugeben, ob die DLP-E-Mail-Vorlage aktiv ist. Wenn diese Option nicht aktiviert ist, werden für diese E-Mail-Vorlage keine Benachrichtigungen gesendet.
Kategorie	Kategorie der E-Mail-Benachrichtigung. DLP unterstützt die folgenden Optionen: ○ **Incident-Benachrichtigung an Endanwender**: Wird gesendet, wenn die Incidents den Endanwendern zugewiesen werden. ○ **Eskalationsbenachrichtigung an Manager**: Wird gesendet, wenn das Fälligkeitsdatum der Antwort überschritten oder dem Manager manuell über das DLP-Vorgangsportal zugewiesen wird. ○ **Benachrichtigung über Fälligkeitsdatum**: Wird gesendet, wenn das Fälligkeitsdatum der Antwort verletzt wird. ○ **Benachrichtigung über Benutzerantwort an Analysten**: Wird gesendet, wenn der Endanwender eine Aktion für den DLP-Incident ausführt. ○ **Benachrichtigung über ausstehende Genehmigungen**: Benachrichtigen Sie Genehmiger über ausstehende Elemente. ○ **Genehmigungsbenachrichtigung an die anfordernde Person**: Benachrichtigen Sie Anwender über die Genehmigung ihrer Anforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Benachrichtigung an anfordernde Person ablehnen**: Benachrichtigen Sie Anwender über die Ablehnung ihrer Anforderungen. ○ **Benachrichtigung an anfordernde Person abbrechen**: Benachrichtigt Anwender über den Abbruch ihrer Anforderungen.
Typ	Option, um anzugeben, ob die E-Mail pro Incident oder als Digest gesendet wird. **Hinweis:** Wenn Sie **„Benachrichtigung über Fälligkeitsdatum“** im Feld **„Kategorie“** ausgewählt haben, können Sie nur Digests verwenden. Wählen Sie diese Option aus.
Beschreibung	Eindeutige Beschreibung für diese E-Mail-Vorlage.
Ausführungsbefehl	Priorität für E-Mail-Vorlagen. Dieses Feld gibt die Reihenfolge an, in der die E-Mail-Vorlagen ausgeführt werden, wenn zwei oder mehr E-Mail-Vorlagen die Auslösebedingungen gemeinsam verwenden. Die E-Mail-Vorlage mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine beliebige andere Zahl. Der Standardwert ist 100.
Vorlagenbedingung	Optionen in den Vorlagenbedingungen, die auf der DLP-Incident-Tabelle basieren. Sie können jedes der Incident-Felder auswählen, um die Auslösebedingung für die E-Mail-Vorlage zu erstellen. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**. ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Zielanwender	Zielbenutzer für die Vorlage, wenn die Bedingungen erfüllt sind. Bei den Zielanwendern handelt es sich um:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Alle Empfänger**: Sendet die E-Mail an Zielanwender. ○ **Empfänger in der Gruppe:** Senden Sie die E-Mail mithilfe der Filteroption nur an Empfänger innerhalb einer bestimmten Gruppe. ○ **Empfänger, die den Kriterien entsprechen**: Senden Sie die E-Mail an Zielanwender, die die Kriterien erfüllen. Sie können den Filter verwenden, um Zielbenutzer basierend auf den Bedingungen aufzuschlüsseln. Beispiel: Stadt.

E-Mail-Vorlage	Auswählbare E-Mail-Vorlage. Sie können die Variablen definieren, um vorhandene Inhalte wiederzuverwenden und der E-Mail-Benachrichtigung hinzuzufügen.
	Die Felder **Kategorie** und **Typ** bestimmen die Variablen, die zur Auswahl stehen. Angenommen, die E-Mail-Kategorie ist auf „Incident-Benachrichtigung“ festgelegt und der E-Mail-Typ ist ein Digest. Dann sind die Variablen für die Auswahl Digest-Felder, um die Häufung mehrerer DLP-Incidents zu ermöglichen.
	Hier ist ein Beispiel-HTML-Text für den E-Mail-Text jeder E-Mail-Vorlage:
	○ **Standardvorlage für Genehmigungsbenachrichtigung pro Incident**:
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	`- Date protection team`
	○ **Benachrichtigung über Stornierung der Genehmigungsanforderung pro Incident**
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	`- Data protection team`
	○ **Standardvorlage für Fälligkeitsdatumsbenachrichtigung**:
	`Dear ${target_user.name},`
	`Following incidents require your response.`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	${due_days_table} - Data protection team

- **Standardvorlage für Anwenderbenachrichtigungen pro Incident**:

  Dear ${assigned_to.name},

  DLP Incident ${number} is assigned to you.

  Please review and submit your response.

  - Data protection team

- **Standardvorlage für Benutzer-Incident-Benachrichtigung**:

  Hello ${target_user.name},

  You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication.

  Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}.

  Please log in to the ${link_to_dlp_portal} and submit your response.

  - Data protection team

- **Standardvorlage für Eskalation – Digest**:

  Hi ${target_user.name},

  The following data security incidents have been escalated to you due to lack of response from the assignees.

  Please login to the incident response workspace to review the incidents and submit your response.

  ${overdue_table}

  - Data protection team

- **Standardvorlage für Eskalation – Pro Incident**:

  Dear ${assigned_to.name},

  Data security incident ${number} has been escalated to you.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Please review and submit your response or assign the incident back to the user. - Data protection team ○ **Standardvorlage für Benachrichtigung über ausstehende Genehmigung**: Dear ${approver.first_name}, Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests. - Data protection team ○ **Standardvorlage für Benachrichtigung für ausstehende Genehmigung pro Incident**: Dear ${Approver}, Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team ○ **Standardvorlage für Pro Incident-Ablehnungsbenachrichtigung**: Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team ○ **Standardvorlage für Benutzerantwortbenachrichtigung pro Incident**: Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}. ○ **Standardvorlage für Benachrichtigung über Abschluss der Anwenderantwort**:

Automatische Übersetzung

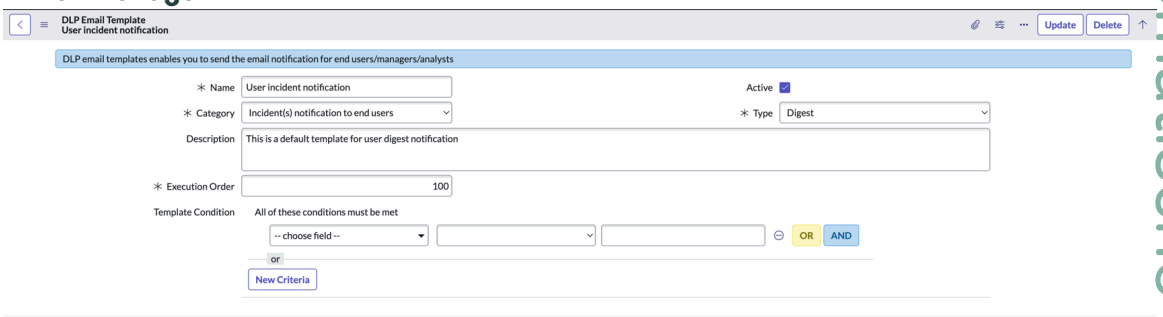
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.

Example

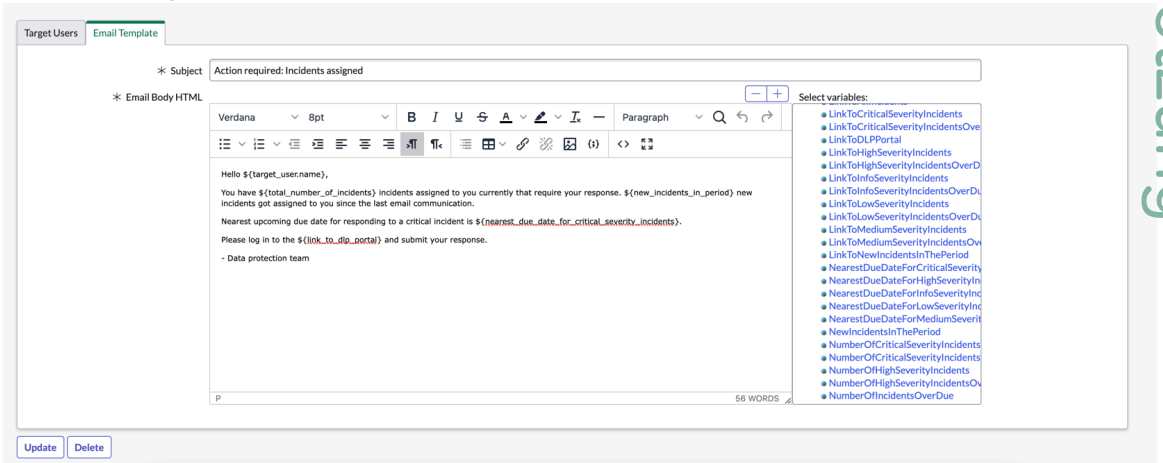
Das folgende Beispiel zeigt die DLP-E-Mail-Vorlage, bei der die Zielbenutzer als alle Empfänger definiert sind.

E-Mail-Vorlage



Das folgende Beispiel zeigt eine E-Mail-Vorlage mit dem Betreff „User Incident Notification“ und der Variablen *`new_incidents_in_period`*. Der E-Mail-Text enthält mehrere Variablen, die aus der Spalte Variablen auswählen hinzugefügt werden.

E-Mail-Vorlagenvariablen



4. Klicken Sie auf **Absenden**.

Ergebnisse

Der Endanwender erhält eine Digest-Benachrichtigungs-E-Mail mit allen ausgewählten Variablenfeldern in der Vorlage.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertungen erstellen

Erstellen und verwalten Sie Bewertungen, damit Endanwender auf DLP-Incidents reagieren können. Sie können die Bewertungen verwenden, um Informationen über die vertraulichen Daten zu sammeln, die durch DLP-Incidents offengelegt oder geleakt wurden.

Bewertungen für DLP-Incidents erstellen und verwalten Sie

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Bewertungen von DLP-Incidents helfen Ihnen, potenzielle Bedrohungen und Schwachstellen für Ihre Daten basierend auf der Reaktion der Endanwender zu identifizieren. Sie können diese Informationen verwenden, um die vorhandenen Lücken, Bedenken und Erwartungen Ihrer Endanwender zu ermitteln.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Bewertungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Bewertung von DLP-Incidents

Feld	Beschreibung
Name	Name der DLP-Incident-Bewertung.
Aktiv	Option, um anzugeben, ob die DLP-Incident-Bewertung aktiv ist.
Beschreibung	Eindeutige Beschreibung für diese DLP-Incident-Bewertung.
Einführung in die Bewertung	Geben Sie eine Einführung oder einen Kontext für Ihre Bewertung an. Sie können auch Variablen aus dem Abschnitt Variablen auswählen verwenden, um bestimmte Felder dynamisch anzuzeigen.

4. Klicken Sie auf **Absenden**.
5. Öffnen Sie nach dem Erstellen einer Bewertung die Bewertung, und klicken Sie auf **Bewertungsdesigner**.
6. Wählen Sie im Abschnitt „Neue Bewertung“ im Abschnitt „Steuerungen“ eine Art von Bewertungsfrage aus.
7. Ziehen Sie den gewünschten Bewertungsfragetyp per Drag-and-Drop unter den Abschnitt „Neue Bewertung“. Sie können beispielsweise das **Auswahl-** Steuerelement per Drag-and-Drop unter den Abschnitt „Neue Bewertung“ oder „Neue Kategorie“ ziehen.
8. Um weitere Kategorien für die Bewertung hinzuzufügen, klicken Sie auf das Symbol .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Um eine vorhandene Kategorie zu ändern, klicken Sie auf das Symbol .
10. Nachdem Sie die verschiedenen Bewertungsfragen zum ersten Mal erstellt haben, klicken Sie auf **Speichern**und dann **auf Veröffentlichen**.

Erstellen Sie Optionsregeln für die Reaktion auf Incidents

Erstellen Sie die Optionsregeln für die Reaktion auf Incidents, die Endanwender oder Analysten bei der Reaktion auf einen Incident verwenden können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Art der Antwort konfigurieren, die ein Endanwender basierend auf dem Typ des DLP-Incident ausführen soll. Die Anwendung „DLP Incident Response“ des Basissystems bietet für Benutzer folgende Antwortoptionen:

- Bewertung abgeschlossen
- Gelöschter Inhalt
- Datei löschen
- Verschlüsselte Datei
- Maskierter Inhalt
- Falsch positives Ergebnis melden
- Falschen Besitzer melden
- Erforderlich für Geschäftsprozess
- Überprüfte Berechtigungen

Angenommen, ein Endanwender meldet einen DLP-Incident als falsch positiv. Der Status für diesen Incident wird dann automatisch als geschlossen markiert, da der von Ihnen konfigurierte Zielstatus geschlossen ist.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Optionsregeln für die Reaktion auf Incidents**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Regeln für Reaktion auf Incidents“.

Feld	Beschreibung
Name	Name der Option zur Reaktion auf Incidents.
Aktiv	Option, um anzugeben, ob die Option zur Reaktion auf Incidents aktiv ist.
Ausführungsreihenfolge	Priorität der Option zur Reaktion auf Incidents. Dieses Feld gibt die Reihenfolge an, in der die Optionen zur Reaktion auf Incidents ausgeführt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

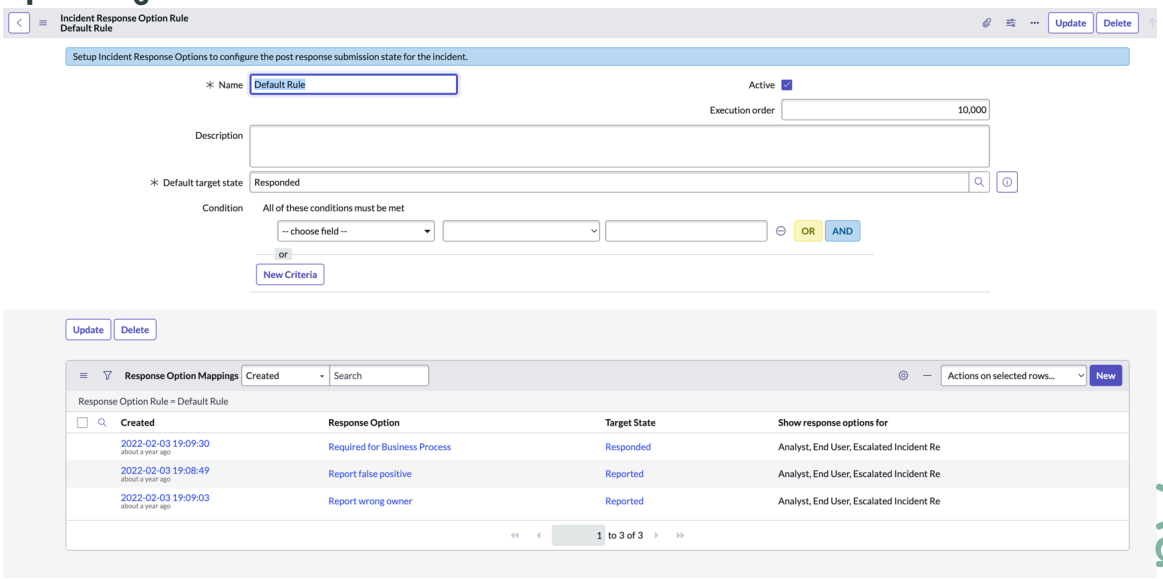
Feld	Beschreibung
	werden, wenn mindestens zwei Optionen zur Reaktion auf Incidents die auslösenden Bedingungen gemeinsam nutzen. Die Antwortoption auf Incidents mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine beliebige andere Zahl. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für diese Option zur Reaktion auf Incidents.
Standardzielstatus	Der von Ihnen konfigurierte Standardzielstatus.
Bedingung	Bedingungen im Bedingungsgenerator Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Optionen zur Reaktion auf Incidents zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**: ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.

Example

Das folgende Beispiel zeigt die Konfiguration der Endanwenderaktion für einen -Endpunkt. Die Bedingung erfordert, dass die Scan-Quelle ein Endpunkt-Dateisystem ist, das dann diese Endanwender-Aktionskonfiguration auslöst. Die Zuordnung zeigt, dass die Antwortoptionen, die dem Endanwender zur Verfügung stehen, „Falschen Besitzer melden“, „Falsch positiv melden“ und „Gelöschte Datei“ sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionsregel für die Reaktion auf Incidents



4. Klicken Sie im Abschnitt **„Zuordnungen der Antwortoptionen“** auf **Neu**.
5. Füllen Sie die Felder des Formulars aus.

Formular „Zuordnung der Antwortoptionen“.

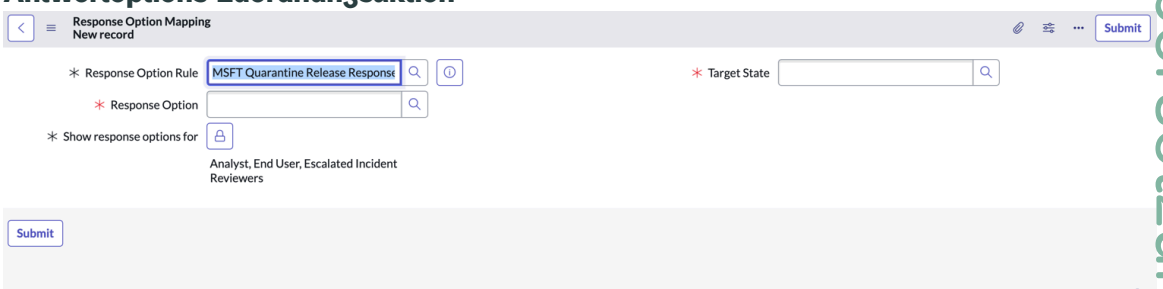
Regel für Antwortoption	Name der Optionsregel für die Reaktion auf Incidents. SharePoint impliziert beispielsweise, dass die Scanquelle SharePoint ist. Sie können entweder den Namen der Incident-Antwort eingeben oder mithilfe der Suche suchen.
Antwortoption	Option zum Auswählen der Antwortoption. Sie können entweder die Antwortoption eingeben oder mithilfe der Suche suchen.
Zielstatus	Der Zielstatus des DLP-Incidents, nachdem der Endanwender die entsprechende Aktion ausgewählt hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Hinweis: **a.** Das Feld **Zielstatus** wird nur angezeigt, wenn Sie **Antwortoption** vom **Typ Standard**auswählen. Weitere Informationen zur Konfiguration der Zielstatustypen finden Sie unter Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents. **b.** Wenn eine Antwortoption vom **Typ „Erweitert“** ausgewählt ist, können Sie den Zielstatus nicht festlegen und werden ausgeblendet. Der Zielstatus wird basierend auf dem anwenderdefinierten Status zugewiesen, der über den Flow Designer-Subflow konfiguriert wurde.
Antwortoptionen anzeigen für	Option zum Bestimmen der Anwenderrollen, für die die Antwortoptionen angezeigt werden sollen. Mit der Option zum Entsperren können Sie zwischen **Analysten**, **Endanwendern**und **eskalierten Prüfern für Analysten** auswählen. Sie können eine oder alle Rollen auswählen.

Antwortoptions-Zuordnungsaktion



6. Klicken Sie auf **Absenden**.

Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents

Verwenden Sie diese Funktion, um die Art der Antwort zu konfigurieren, die ein Endanwender oder Analyst ausführen soll.

Vorbereitungen

Die Anwendung „DLP Incident Response“ des Basissystems bietet die folgenden Antwortoptionen:

1. Bewertung abgeschlossen
2. Gelöschter Inhalt
3. Datei löschen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Verschlüsselte Datei
5. Maskierter Inhalt
6. Falsch positives Ergebnis melden
7. Falschen Besitzer melden
8. E-Mail-Freigabe aus der Quarantäne anfordern

   Hinweis:
   Diese Option ist für die DLP Microsoft Exchange-Datensätze verfügbar.

9. Erforderlich für Geschäftsprozess
10. Überprüfte Berechtigungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Antwortoptionen**.

   Standardmäßig bietet das Basissystem zwei Arten von Antwortoptionen:

   a. **Standard**: Eine manuelle Antwortoption, die vom Anwender übermittelt wird.

   b. **Erweitert**: Eine automatisierte Antwortoption löst einen Flow Designer-Subflow aus, wenn der Anwender die Antwortoption übermittelt.

2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Antwortoptionsformular vom Typ: Standard

Feld	Beschreibung
Name	Geben Sie den Namen der Option zur Reaktion auf Incidents ein.
Typ	Option zum Auswählen des Antwortoptionstyps.

Antwortoptionsformular vom Typ: Erweitert

Feld	Beschreibung
Name	Geben Sie den Namen der Option zur Reaktion auf Incidents ein.
Typ	Option zum Auswählen der Antwortoption. Standardmäßig zeigt dieses Feld die folgenden beiden Arten von Optionen an: ○ **Standard**: Wenn Sie diese Option beim Erstellen einer neuen Antwortoption auswählen, müssen Sie möglicherweise einen Antwortoptionsnamen und den Typ hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Erweitert**: Wenn Sie diese Option auswählen, stehen Ihnen die folgenden Felder zur Auswahl: ▪ **Flow**: Wählen Sie den Flow Designer-Subflow aus. ▪ **MID-Server erforderlich**: Aktivieren Sie dieses Kontrollkästchen, wenn der ausgewählte Flow den MID-Server verwendet.
Flow	Wählen Sie den erforderlichen Flow Designer-Flow aus, um die MID-Anwendung und MID-Fähigkeit zu aktivieren. Wenn Sie einen Subflow für die Antwortoption erstellen, fügen Sie die folgenden Subflow-Eingaben hinzu: **a. Name**: ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b. Typ**: ▪ Referenz (zur DLP-Incident-Tabelle) ▪ Sys-ID für MID-Server-Anwendung und MID-Server-Fähigkeit
MID-Server erforderlich	Option zum Bestimmen dieser MID-Server-Konfiguration. Durch Aktivieren der Felder **MID-Server-** Anwendung des Kontrollkästchens **MID-Server-Anwendung** und **MID-Server-Fähigkeit** können Sie die MID-Anwendung und die MID-Fähigkeit konfigurieren. **Hinweis:** Abhängig von der Konfiguration der MID-Server-Anwendung und der MID-Server-Fähigkeiten und wenn ein MID aktiv ist und ausgeführt wird, ist nur die Antwortoption im Arbeitsbereich sichtbar.
MID-Server-Anwendung	Wählen Sie die erforderliche MID-Server-Anwendung aus der Dropdown-Liste aus.
MID-Server-Fähigkeit	Wählen Sie in der Dropdown-Liste die erforderliche MID-Server-Fähigkeit aus.

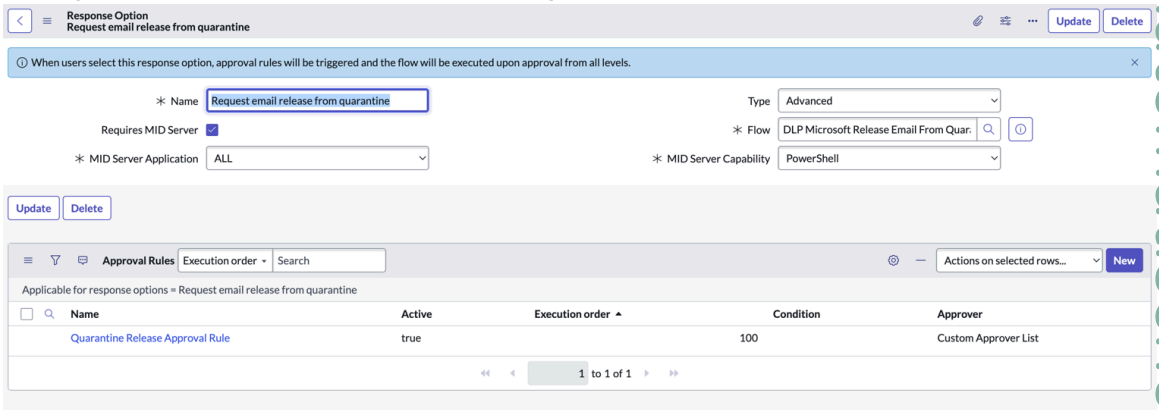
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn für die ausgewählte MID-Server-Fähigkeit kein MID-Server verfügbar ist, wird die Antwortoption nicht angezeigt. Wenn Sie einen bestimmten MID-Server aus der Liste möchten, müssen Sie die MID-App konfigurieren und in der Liste sichtbar machen. Dann sollte mindestens ein konfigurierter MID-Server über die ausgewählten MID-Anwendungen aktiv sein und über Folgendes verfügen: ausgewählte MID-Server-Fähigkeit

4. Klicken Sie auf **Absenden**.

Hinweis:
Wenn Sie eine Antwortoption des Typs **„Erweitert“** erstellen, wird die zugehörige Liste **„Genehmigungsregeln“** ausgefüllt, damit Sie die Genehmigungsregel für diese neue Antwortoption konfigurieren können. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsregeln.

Konfigurieren Sie die Antwortoption vom Typ „Erweitert“.



Erstellen Sie Altersdiagrammkonfigurationen

Konfigurieren Sie das Altersdiagramm, das im Ops-Portal Data Loss Prevention Incident Response (DLP IR) angezeigt wird. Dieses Diagramm zeigt die Anzahl der offenen Incidents nach Anzahl der Tage.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Konfiguration des Altersdiagramms**.
2. Überprüfen Sie die Altersdiagrammeinträge in der folgenden Tabelle, und passen Sie die Einträge für Ihre Umgebung an.

Formular „DLP-Altersdiagrammkonfigurationen“.

Name	Bedingung
0–30 Tage	Alter des offenen Incidents, das zwischen 0 und 30 Tagen liegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Bedingung
31–60 Tage	Alter des offenen Incidents, das zwischen 31 und 60 Tagen liegt.
61–90 Tage	Alter des offenen Incidents, das zwischen 61 und 90 Tagen liegt.
Über 90 Tage	Alter des offenen Incidents, der über 90 Tage liegt.

3. Fügen Sie eine neue Altersdiagrammkonfiguration hinzu, indem Sie auf **Neu**klicken.
4. Geben Sie im Feld Name einen **Namen** für die Konfiguration des DLP-Altersdiagramms ein.
5. Legen Sie die Bedingungen für die Konfiguration des DLP-Altersdiagramms fest.

   a. Um Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.
      - Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
      - Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.

      Hinweis:
      Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.

   b. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.

6. Klicken Sie auf **Absenden**.

Erstellen Sie Konfigurationen für Benutzerdelegierte

Verhindern Sie, dass bestimmte Führungskräfte in der Organisation Benachrichtigungen über die ihnen zugewiesenen oder eskalierten Incidents erhalten.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Betrachten Sie ein Szenario, in dem die Führungskraft ein Benutzer ist, der einer Führungsebene oder Führungsebene angehört. An die Führungskraft dürfen keine E-Mails zur Incident-Zuweisung oder Eskalation gesendet werden. Ein delegierter Benutzer kann dann im Namen der Führungskraft die erforderliche Aktion ausführen.

Sobald ein Benutzer eine bestimmte Person, Henry, als Delegierten zugewiesen hat, kann ein anderer Benutzer Henry nicht erneut als Delegierten zuweisen. Ebenso kann ein Delegierter keinen anderen Benutzer als Delegierten zuweisen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Delegierten-Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Delegierten-Konfiguration“.

Feld	Beschreibung
Anwender	Name des Anwenders, der einen Delegierten für DLP-Incidents benötigt.
Delegierter	Name des Anwenders, der im Namen des ursprünglichen Endanwenders auf den DLP-Incident reagieren kann.

4. Klicken Sie auf **Absenden**.

Erstellen Sie Regeln zur Identifizierung von Wiederholungsvergehen

Erstellen Sie Identifizierungsregeln für Wiederholungsvergehen, um Benutzer zu identifizieren, die dasselbe Problem mehrmals wiederholen.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können Wiederholungsfälle anhand bestimmter Regeln oder Kriterien identifizieren. Data Loss Prevention Incident Response stellt Felder bereit, mit denen Sie Wiederholungstäter identifizieren können.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Wiederholen Sie die Regeln zur Identifizierung von Straftätern**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Regeln zur Identifizierung von Wiederholungsvergehen“.

Feld	Beschreibung
Name	Name der Regel zur Identifizierung von Wiederholungsvergehen.
Ausführungsreihenfolge	Priorität der Regeln zur Identifizierung von Wiederholungsvergehen. Dieses Feld gibt die Reihenfolge an, in der die Regeln zur Identifizierung von Wiederholungsvergehen ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen. Die Regel zur Identifizierung von Wiederholungsvergehen mit der niedrigsten Nummer hat die höchste Priorität.

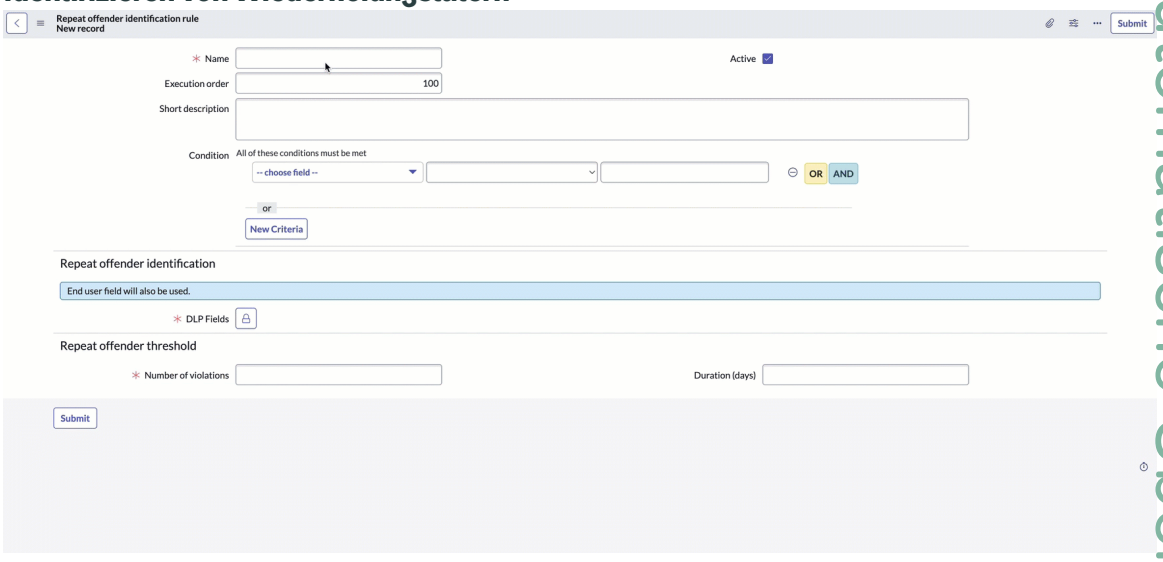
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine beliebige andere Zahl. Der Standardwert ist 100.
Kurzbeschreibung	Eindeutige Beschreibung für diese Regel zur Identifizierung von Wiederholungsvergehen.
Bedingung	Bedingungen im Bedingungsgenerator, die auf der DLP-Incident-Tabelle basieren. Sie können jedes der Incident-Felder auswählen, um die Auslöserbedingung für die Regel zur Identifizierung von Wiederholungsvergehen zu erstellen. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**: ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
DLP-Felder	Identifizieren Sie Wiederholungstäter basierend auf den erforderlichen DLP-Feldern. Klicken Sie auf das neben den DLP-Feldern, um die Liste der verfügbaren DLP-Felder anzuzeigen. Wählen Sie die DLP-Felder, die Sie verwenden möchten, aus der Spalte Verfügbar aus, und verschieben Sie sie in die Spalte Ausgewählt. Sie können beispielsweise die Felder**Dateiname** und **Dateibesitzer** aus der Spalte Verfügbar auswählen und in die Spalte Ausgewählt verschieben. Anschließend können Sie die Wiederholungstäter anhand der Felder **Dateiname** und **Dateibesitzer** identifizieren. Wenn also ein Anwender gegen den Schwellenwert für Wiederholungsvergehen (Anzahl der Verstöße und Dauer) verstößt und wenn derselbe Anwender mit den DLP-Feldern übereinstimmt,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	wird dieser bestimmte Anwender als Wiederholungsvergehender identifiziert.
Anzahl der Verstöße	Definieren Sie den Schwellenwert für Wiederholungsvergehen. Nachdem der Benutzer dieselben Aktionen wiederholt und gegen die angegebene Anzahl von Verstößen verstößt, wird der Benutzer als Wiederholungstäter identifiziert.
Dauer (in Tagen)	Definieren Sie den Schwellenwert für Wiederholungsvergehen in Tagen. Nachdem der Benutzer dieselben Aktionen wiederholt und gegen die Schwellenwertdauer verstößt, wird er als Wiederholungstäter identifiziert.

Identifizieren von Wiederholungstätern



4. Klicken Sie auf **Absenden**.

Zusätzliche Incident-Datenfelder erstellen

Erstellen Sie zusätzliche Incident-Datenfelder für die DLP-Incidents. Sie können verschiedene Arten von zusätzlichen Incident-Datenfeldern erstellen, z. B. Zeichenfolge, Nummer, Kontrollkästchen, Auswahl, Datum und Uhrzeit, und sie in den DLP-Incident-Formularen verwenden.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Wichtig:
Zusätzliche Incident-Datenfelder für DLP-Incidents werden nur ab Version San Diego unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Zusätzliche Incident-Datenfelder sind Einschränkungen auf Feldebene zugeordnet. Wenn also Einschränkungen auf Feldebene vorhanden sind, gelten sie für zusätzliche Incident-Datenfelder im DLP-Vorgangsportal und im Endanwenderportal.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Zusätzliche Incident-Datenfelder**.
2. Erstellen Sie zusätzliche Incident-Datenfelder, indem Sie auf **Neu**klicken.
3. Füllen Sie die Felder des Formulars aus.

Formular „Zusätzliche DLP-Incident-Datenfelder“.

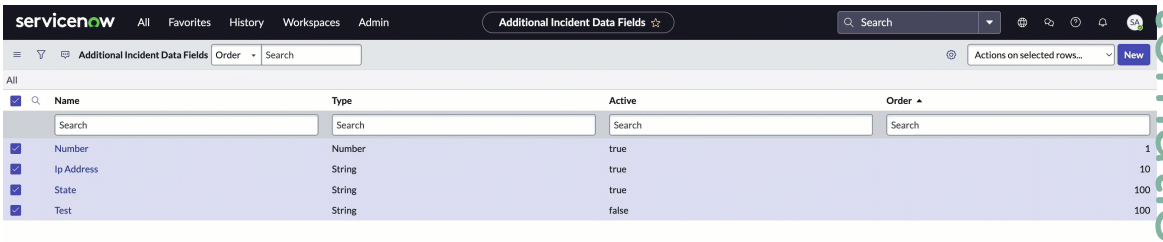
Feld	Beschreibung
Name	Name der zusätzlichen Incident-Datenfelder
Typ	Option zum Auswählen des Typs zusätzlicher Incident-Datenfelder. Sie können einen der folgenden Typen auswählen: ○ **Zeichenfolge** ○ **Nummer** ○ **Checkbox** ○ **Auswahl** Wenn Sie für den Typ Zusätzliche Incident-Datenfelder **Auswahl**auswählen, können Sie nach dem Erstellen der Zusätzlichen Incident-Datenfelder die Auswahloptionen für Zusätzliche Incident-Datenfelder definieren. So erstellen Sie eine Auswahloption für zusätzliche Incident-Datenfelder: **a.** Öffnen Sie die erforderlichen zusätzlichen Incident-Datenfelder. **b.** Klicken Sie im Abschnitt Optionen für anwenderdefiniertes Auswahlfeld auf **Neu**. **c.** Definieren Sie im Feld Optionsname den Namen der gewünschten Option. **d.** Klicken Sie auf **Absenden**. ○ **Datum** ○ **Datum/Uhrzeit** **Hinweis:** Nachdem Sie einen Typ für Ihre neuen zusätzlichen Incident-Datenfelder ausgewählt haben, dürfen Sie ihn nicht mehr ändern. Wenn Sie den Typ ändern möchten, müssen Sie erneut ein neues Zusätzliche Incident-Datenfeld mit dem erforderlichen Typ erstellen.
Bestellung	Option zum Auswählen der Reihenfolge, in der die zusätzlichen Incident-Datenfelder angezeigt werden sollen. Sie können den Reihenfolgewert für jedes zusätzliche Incident-Datenfeld definieren. Die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zusätzlichen Incident-Datenfelder werden basierend auf den von Ihnen definierten Reihenfolgenwerten sortiert. Standardmäßig sind die Felder mit zusätzlichen Incident-Daten in aufsteigender Reihenfolge sortiert. Sie können die Felder Zusätzliche Incident-Daten in absteigender Reihenfolge sortieren, indem Sie auf die **Spalte** Reihenfolge klicken.
Aktiv	Option, um anzugeben, ob das zusätzliche Incident-Datenfeld aktiv ist.
Beschreibung	Beschreibung für die von Ihnen erstellten zusätzlichen Incident-Datenfelder.

Zusätzliche DLP-Incident-Datenfelder



4. Klicken Sie auf **Absenden**.

Erweiterte Einstellungen konfigurieren

Konfigurieren Sie die erweiterten Einstellungen so, dass Sie die Felder im Incident unter anderem für die Identifizierung der Endanwender festlegen können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Die Konfiguration erweiterter Einstellungen für Data Loss Prevention Incident Response ist optional. Einige erweiterte Einstellungen sind:

- Definieren Sie die maximale Anzahl von Incidents, die in einer Digest-E-Mail gesendet werden können.
- Aktivieren Sie den Schnellmodus, um E-Mails schneller zu senden.
- Bestimmen Sie die Protokollausführlichkeit der Anwendung.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**.
2. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Einstellungen“

Feld	Beschreibung
Sollen die vertraulichen Daten, die den Verstoß verursacht haben, im Incident angezeigt werden?	Option zum Auswählen, ob die vertraulichen Daten angezeigt werden sollen, die den Verstoß für den DLP-Incident verursacht haben. Standardmäßig ist diese Option aktiviert.
Sollen die vertraulichen Daten, die den Verstoß verursacht haben, auch in den untergeordneten Incidents angezeigt werden?	Option zur Auswahl, ob die vertraulichen Daten, die den Verstoß verursacht haben, auch für den untergeordneten DLP-Incident angezeigt werden sollen. Standardmäßig ist diese Option deaktiviert.
Liste der Felder im Incident, die zur Identifizierung des Endanwenders verwendet werden	Liste der Felder im Incident des Moduls „Zuweisungsregel“, die zur Identifizierung des Endanwenders verwendet werden. Sie können auch eigene anwenderdefinierte Attribute angeben, um den Endanwender zu identifizieren.
Maximale Anzahl von Incidents in einer Digest-E-Mail	Die maximale Anzahl von Incidents, die in einer Digest-E-Mail gesendet werden können. Der Standardwert ist 100.
Maximale Dauer des Wiederholungsvergehens (in Tagen)	Die maximale Dauer zur Identifizierung eines Wiederholungsvergehens. Standardmäßig beträgt der Wert 90 Tage.
Schnellmodus zum Senden von E-Mails	Option zum Validieren von E-Mails und Identifizieren von Problemen. Sie können die Validierung durchführen, indem Sie die Option **Ja** aktivieren. Standardmäßig ist diese Option aktiviert.
Diese Eigenschaft wird verwendet, um die Protokollausführlichkeit der Anwendung festzulegen	Die Protokollausführlichkeitsstufe der Anwendung, d. h. den Namen des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **Fehler** ○ **warnen** ○ **Info** ○ **debuggen** Standardmäßig lautet der Wert **„info“**.
Geklonte und untergeordnete Incidents aus Berichten ausschließen	Option zum Ausschließen geklonter und untergeordneter Incidents aus den Berichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standardmäßig ist diese Option auf **Ja festgelegt**.
Wartezeit in Tagen für das Löschen von Abgleichsinhalten im Cloud-Speicher, nachdem der Incident geschlossen wurde	Option zum Auswählen der Anzahl der Wartetage für die Bereinigung des Übereinstimmungsinhalts der Incidents, die für eine bestimmte Zeitdauer inaktiv sind. Der Standardwert ist 90. Wenn der DLP-Incident nach 90 Tagen inaktiv ist, wird der Übereinstimmungsinhalt im Cloud-Speicher bereinigt.
Incident nach der letzten Eskalationsstufe der DLP-Analystengruppe zuweisen	Aktivieren Sie dieses Kontrollkästchen, um den Incident dem Analysten nach der letzten Eskalationsstufe zuzuweisen.
Anwendern den Zugriff auf Incidents nach der Eskalation ermöglichen	Aktivieren Sie dieses Kontrollkästchen, um den zugewiesenen Anwendern den Zugriff auf die Incidents nach der Eskalation zu ermöglichen. Wenn Sie diese Option auswählen, können alle Anwender, die der Eskalationskettenliste hinzugefügt wurden, auf den/die Incident(s) zugreifen.
Zulassen, dass Analysten abgeschlossene Bewertungen bearbeiten	Aktivieren Sie dieses Kontrollkästchen, damit der Analyst die abgeschlossene Bewertung bearbeiten kann. Wenn Sie diese Option auswählen, können Analysten die Bewertungen bearbeiten. Wenn diese Option deaktiviert ist, können Sie die Bewertungen im schreibgeschützten Modus anzeigen.
Vorschaueigenschaften für Nachweisdateien	
Durch Aktivieren dieser Systemeigenschaft wird die Vorschaufunktion für Nachweisdateien im DLP-Analystenarbeitsbereich aktiviert. sn_dlir.enable_evidence_file_preview	Option zum Auswählen, ob die Vorschau der Nachweisdateien direkt im Arbeitsbereich angezeigt werden soll. Standardmäßig ist diese Option auf **Ja festgelegt**.
Dadurch können DLP-Anwender die angezeigten Nachweisdateien herunterladen. Sobald diese Eigenschaft aktiviert ist, wird Anwendern im Dokument-Viewer eine Download-Schaltfläche zum Herunterladen der Nachweisdatei angezeigt. sn_dlir.enable_download in_preview	Option zum Auswählen, ob die Download-Schaltfläche im Dokument-Viewer angezeigt werden soll, mit der Sie die angezeigten Beweisdateien herunterladen können. Standardmäßig ist diese Option auf **Ja festgelegt**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Diese Eigenschaft bestimmt die Dauer, für die Dateien zur Vorschau auf Nachweisdateien vorübergehend aufbewahrt werden. (in Minuten) sn_dlir.preview_temp_files_cleanup_interval	Die maximale Dauer, für die Dateien für die Vorschau der Nachweisdatei vorübergehend gespeichert werden. Der Standardwert ist 10. Wenn der DLP-Incident nach 10 Minuten inaktiv ist, wird die Nachweisdatei im Analystenarbeitsbereich bereinigt.
Durch Aktivieren dieser Eigenschaft wird das Bereinigungsintervall verlängert, wenn Nachweisdateien verwendet werden. Dadurch kann das System die Ablaufzeit von Nachweisdateien basierend auf dem Wert verlängern, der in der Systemeigenschaft „sn_dlir.preview_temp_files_cleanup_interval“ festgelegt ist. sn_dlir.extend_cleanup_interval_on_usage	Option zum Verlängern der Zeit bis zum Löschen von Nachweisdateien, wenn sie verwendet werden. Standardmäßig ist diese Option auf **Ja festgelegt**.
Die maximale Dauer für die Verlängerung des Bereinigungsintervalls von Nachweisdateien (in Minuten). sn_dlir.max_extension_duration_for_cleanup	Option zum Auswählen, wie lange (in Minuten) das System Ihre Nachweisdateien aufbewahrt, bevor sie bereinigt werden. Der Standardwert ist 60.

3. Klicken Sie auf **Speichern**.

Überwachen Sie den DLP-Integrationsausführungsprozess

Verfolgen und überwachen Sie die laufende Erfassung oder den Integrationsausführungsprozess. Die Integrationsausführungsprozesse enthalten Statistiken dazu, wie viele Daten verarbeitet wurden, und den Integrationsstatus.

Erforderliche Rolle: sn_dlir.admin.

Der Integrationsausführungsprozess listet die Details dazu auf, wie viele Datensätze erfasst werden. Zum Beispiel:

1. In der Symantec-Integration enthält der Prozess sowohl untergeordnete als auch übergeordnete Integrationsausführungen. Der übergeordnete Datensatz gibt die Erfassungsdaten an, der untergeordnete Datensatz die Ergänzungsaufrufe und Datensätze für anwenderdefinierte Attribute.
2. In der Microsoft-Integration muss nur der Erfassungsprozess für übergeordnete Datensätze ausgeführt werden.

DLP-Integrationsausführungsprozesse: Hier werden die Warteschlangeneinträge, der Status von Warteschlangeneinträgen und die abgerufenen Datensätze angezeigt.

Die Integrationsausführung enthält die Quelle, für die das Integrationsprofil und der Datensatz der Integrationsausführung erstellt werden, Profilabfrageintervalle, Erfassungsstatus und -substatus sowie die Anzahl der Incidents, die die Anzahl der erfassten Datensätze angibt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **DLP-Administration** > **Integrationsausführungen**.
2. Wählen Sie die Integrationsausführung aus der Liste aus.
3. Navigieren Sie zu **DLP-Integrationsausführungsprozess**.
4. Zeigen Sie den Warteschlangeneintragsstatus des Datensatzes an.

Zugriffsbeschränkungen für DLP-Incidents

Verwalten Sie die Sichtbarkeit eines bestimmten DLP-Incidents, der vertrauliche Informationen enthält. Sie können Zugriffsbeschränkungen für Incidents verwenden, um zu definieren, wer auf einen bestimmten DLP-Incident zugreifen kann, und um den Zugriff bestimmter Benutzer oder Gruppen auf diesen Incident zu beschränken.

Erstellen Sie Einschränkungen auf Feldebene

Legen Sie Einschränkungen auf Feldebene in DLP-Incidents fest, um zu verhindern, dass vertrauliche Informationen verfügbar gemacht werden. Sie können Einschränkungen auf Feldebene verwenden, um die Benutzer oder Gruppen zu steuern, die in den DLP-Incidents auf bestimmte Felder zugreifen können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Einschränkungen auf Feldebene ermöglichen es Ihnen, nur bestimmte Felder für bestimmte Anwender oder Gruppen anzuzeigen. Dadurch können Sie die Daten, auf die ein Anwender zugreifen kann, präziser steuern. Sie können eine Einschränkung auf Feldebene erstellen, indem Sie die Bedingungen für die DLP-Incident-Übereinstimmung definieren, die Benutzer oder Gruppen auswählen, für die diese Bedingungen gelten, und dann die DLP-Felder auswählen, die diese Benutzer oder Gruppen anzeigen können.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Incident-Zugriffsbeschränkungen** > **Einschränkungen auf Feldebene**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „DLP-Einschränkung auf Feldebene“.

Feld	Beschreibung
Name	Name der Einschränkung auf Feldebene.
Aktiv	Option, um anzugeben, ob die Einschränkung auf Feldebene aktiv ist.
Ausführungsreihenfolge	Priorität der Einschränkungen auf Feldebene. Dieses Feld gibt die Reihenfolge an, in der Einschränkungen auf Feldebene ausgeführt werden, wenn mindestens Einschränkungen auf Feldebene die Auslösebedingungen gemeinsam nutzen. Die Einschränkung auf Feldebene mit der niedrigsten Nummer hat die höchste Priorität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

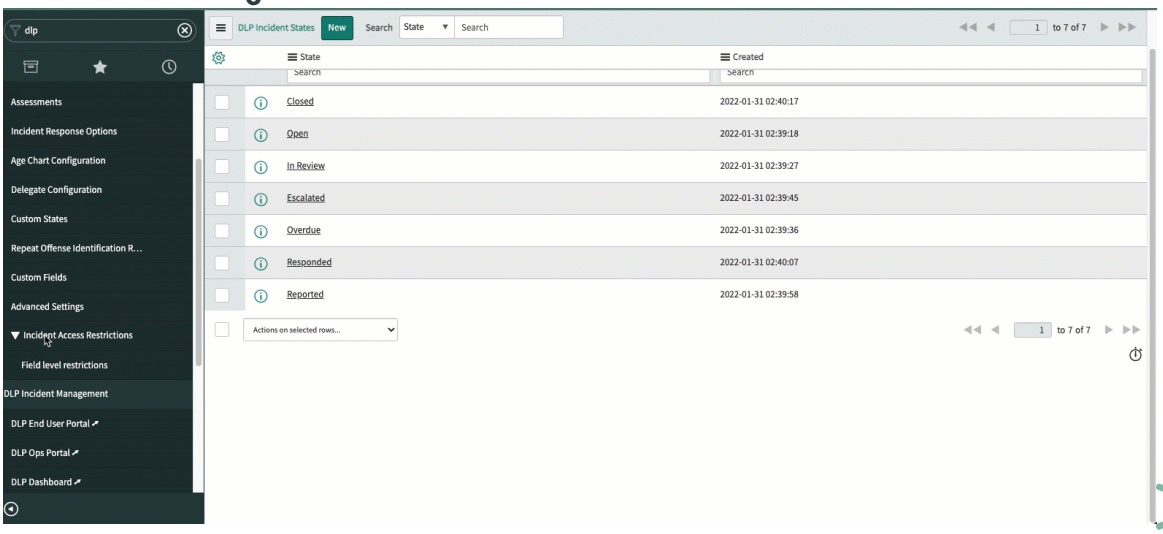
Feld	Beschreibung
	Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine beliebige andere Zahl. Der Standardwert ist 100.
Kurzbeschreibung	Eindeutige Beschreibung für diese Einschränkung auf Feldebene.
Incident erfüllt die Bedingung	Optionen im Incident, die den definierten Bedingungen entsprechen. Sie können jedes der Incident-Felder auswählen, um die Auslöserbedingung für die Einschränkungen auf Feldebene zu definieren. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**: ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Sie können beispielsweise das Feld Richtliniennameauswählen und die Bedingung aufsowie Name der Richtliniefestlegen. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Betrifft	Option, um die Incident-Übereinstimmungsbedingungen auf bestimmte Benutzer oder Gruppen anzuwenden. Sie können die Bedingungen auf Folgendes anwenden: ○ **Alle Endanwender**: Option zum Auswählen aller Endanwender, für die die DLP-Incident-Bedingungen gelten. ○ **Alle Prüfer von eskalierten Incidents**: Option zum Auswählen aller Prüfer von eskalierten Incidents, für die die DLP-Incident-Bedingungen gelten. Dies bezieht sich auf alle DLP-Incidents, die an den Manager eskaliert wurden. ○ **Benutzer**: Klicken Sie auf das , um einen bestimmten Benutzer aus der Liste hinzuzufügen, für den die DLP-Incident-Bedingungen gelten. Sie können einen Anwender auch hinzufügen, indem Sie seine E-Mail-Adresse oder Suchoption verwenden. Beispiel: Manager der Rechtsabteilung. Um sich selbst als Benutzer hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf das

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Gruppen**: Klicken Sie auf das um eine bestimmte Gruppe aus der Liste hinzuzufügen, für die die DLP-Incident-Bedingungen gelten. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen. Beispiel: Umfrageersteller.
Nur Zugriff auf folgende Felder zulassen	○ **DLP-Felder**: Option zum Definieren der DLP-Felder, die den ausgewählten Anwendern oder Gruppen Zugriff gewähren sollen. Wählen Sie in der Spalte Verfügbar die DLP-Felder aus, auf die Sie Zugriff gewähren möchten, und verschieben Sie sie in die Spalte Ausgewählt. **Hinweis:** Die ausgewählten Anwender oder Gruppen können nur auf die ausgewählten DLP-Felder zugreifen. Sie können beispielsweise die Felder**Zugewiesen an** und **Geöffnet** in der Spalte Verfügbar auswählen und in die Spalte Ausgewählt verschieben. Dann haben die ausgewählten Benutzer oder Gruppen nur Zugriff auf die Felder Zugewiesen an und Geöffnet. ○ **Anhänge hochladen**: Option, um anzugeben, ob die ausgewählten Anwender oder Gruppen Anhänge hochladen dürfen. ○ **Anwenderdefinierte Felder**: Option zum Definieren der anwenderdefinierten Felder, die den ausgewählten Anwendern oder Gruppen Zugriff gewähren sollen. Sie können die anwenderdefinierten Felder, die Sie erstellt haben, in der Spalte Verfügbar anzeigen. Wählen Sie in der Spalte Verfügbar die anwenderdefinierten Felder aus, auf die Sie Zugriff gewähren möchten, und verschieben Sie sie in die Spalte Ausgewählt. **Wichtig:** ▪ Anwenderdefinierte Felder für DLP-Incidents werden nur ab Version San Diego unterstützt. ▪ Die ausgewählten Anwender oder Gruppen können nur auf die ausgewählten anwenderdefinierten Felder zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Einschränkung auf Feldebene



4. Klicken Sie auf **Absenden**.

Erstellen Sie Einschränkungen auf Datensatzebene

Legen Sie Einschränkungen auf Datensatzebene in DLP-Incidents fest, um vertrauliche Datensätze vor der Offenlegung zu schützen. Sie können Einschränkungen auf Datensatzebene verwenden, um die Benutzer oder Gruppen zu steuern, die in den DLP-Incidents auf bestimmte Datensätze zugreifen können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read: Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Einschränkungen auf Datensatzebene ermöglichen es Ihnen, bestimmten Anwendern oder Gruppen Zugriff auf Datensätze zu gewähren und so die Datensätze, auf die ein Anwender zugreifen kann, präziser zu steuern. Sie können eine Einschränkung auf Datensatzebene erstellen, indem Sie die Bedingungen für die DLP-Incident-Übereinstimmung definieren, die Benutzer oder Gruppen auswählen, für die diese Bedingungen gelten, und dann die DLP-Datensätze auswählen, die diese Benutzer oder Gruppen anzeigen können.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Incident-Zugriffsbeschränkungen** > **Einschränkungen auf Datensatzebene**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „DLP – Einschränkung auf Datensatzebene“

Feld	Beschreibung
Name	Name der Einschränkung auf Datensatzebene.
Kurzbeschreibung	Eindeutige Beschreibung für diese Einschränkung auf Datensatzebene.

Automatische Übersetzung

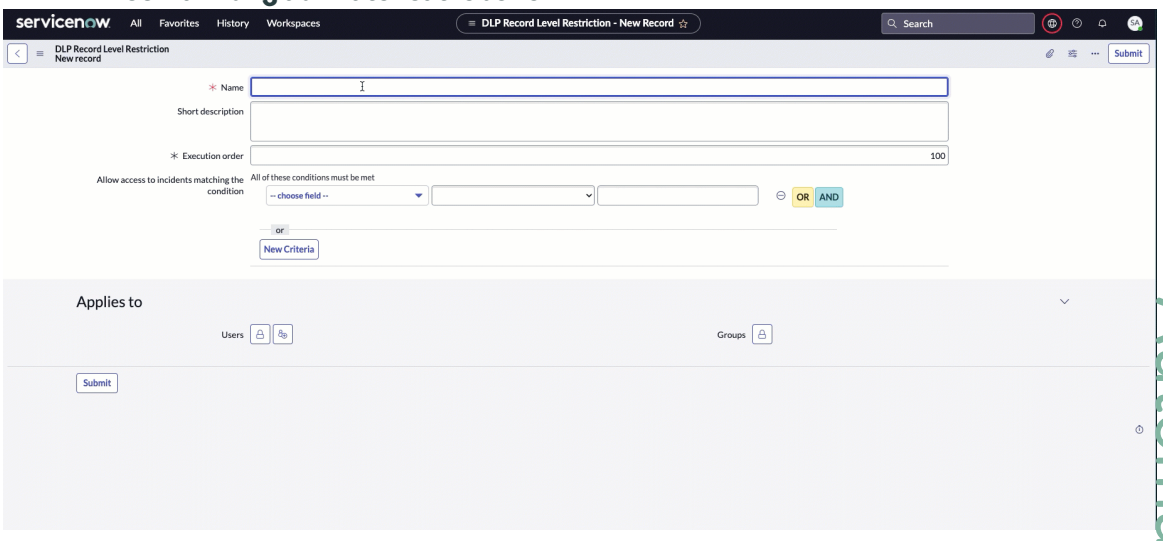
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ausführungsreihenfolge	Priorität der Einschränkungen auf Datensatzebene. Dieses Feld gibt die Reihenfolge an, in der die Einschränkungen auf Datensatzebene ausgeführt werden, wenn mindestens zwei Einschränkungen auf Datensatzebene die Auslösebedingungen gemeinsam nutzen. Die Einschränkung auf Datensatzebene mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge der Vorgänge festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine beliebige andere Zahl. Der Standardwert ist 100.
Erlauben Sie den Zugriff auf Incidents, die der Bedingung entsprechen	Optionen ermöglichen den Zugriff auf die Incidents, die den definierten Bedingungen entsprechen. Sie können jedes der Incident-Felder auswählen, um die Auslöserbedingung für die Einschränkungen auf Datensatzebene zu definieren. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**: ○ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. Sie können beispielsweise das Feld als Aktivauswählen und die Bedingung auf isund truefestlegen.
Betrifft	Option, um Einschränkungen auf Datensatzebene auf bestimmte Anwender oder Gruppen anzuwenden. Sie können die Bedingungen wie folgt anwenden: ○ **Benutzer**: Klicken Sie auf das, um einen bestimmten Benutzer aus der Liste hinzuzufügen, für den der ausgewählte Datensatz gilt. Sie können einen Anwender auch hinzufügen, indem Sie seine E-Mail-Adresse oder Suchoption verwenden. Beispiel: Manager der Rechtsabteilung. Um sich selbst als Benutzer hinzuzufügen, für den dieser Datensatz gilt, klicken Sie auf das. Beispiel: Systemadministrator ○ **Gruppen**: Klicken Sie auf das, um eine bestimmte Gruppe aus der Liste hinzuzufügen, für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die der ausgewählte Datensatz gilt. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen. Beispiel: Umfrageersteller.

DLP – Einschränkung auf Datensatzebene



4. Klicken Sie auf **Absenden**.

Archivierung von DLP-Incidents

Data Loss Prevention Incident Response wird mit einer Archivierungsregel im Basissystem für die DLP-Incident-Tabelle bereitgestellt. Die zugehörigen Datensätze werden auch im Basissystem der Archivregel für DLP-Incidents hinzugefügt.

Vorbereitungen

Erforderliche Rolle: Administrator

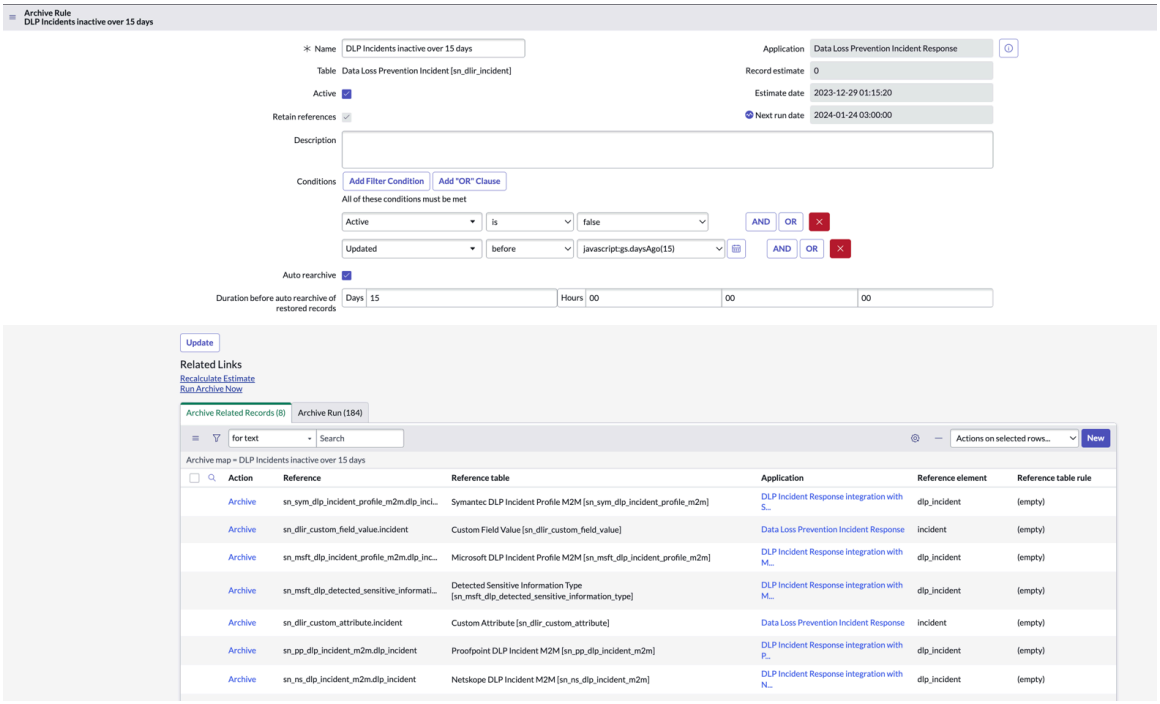
Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**.
   Die Systemarchivierungsregeln, die im Basissystem vorhanden sind, werden angezeigt.
2. Zeigen Sie die DLP-Archivierungsregel an.

Hinweis:
„DLP-Incidents inaktiv über 15 Tage“ ist die standardmäßige Archivierungsregel des Basissystems für DLP-Incidents. Sie können die Archivierungsregel bei Bedarf ändern. Diese Regel bedeutet, dass Incidents, die seit mehr als 15 Tagen inaktiv sind, automatisch archiviert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Informationen dazu, wie Archivierungsregeln erstellt werden, finden Sie unter Archivierungsregeln erstellen .

3. **Aktualisieren Sie** bei Bedarf die Regel.

Archivieren Sie zugehörige DLP-Datensätze

Verwenden Sie die zugehörige Liste „Zugehörige Datensätze archivieren“ für DLP-Incidents, um der Archivierungsregel die zugehörigen Datensätze hinzuzufügen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**.
2. Wählen Sie die Archivierungsregel **„DLP-Incidents inaktiv“ über 15 Tage** aus.
3. Wechseln Sie zur zugehörigen Liste Zugehörige **Datensätze archivieren**.
4. Zeigen Sie die zugehörigen DLP-Datensätze an.

Anwendung	Referenztabelle
Integration von DLP Incident Response mit Symantec	Symantec-DLP-Incident-Profil M2M [sn_sym_dlp_incident_profile_m2m]
Reaktion auf Incident zur Vermeidung von Datenverlust	Benutzerdefinierter Feldwert [sn_dlir_custom_field_value]
Integration von DLP Incident Response mit Microsoft	Microsoft DLP-Incident-Profil M2M [sn_msft_dlp_incident_profile_m2m]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Referenztabelle
Integration von DLP Incident Response mit Microsoft	Typ der erkannten sensiblen Informationen [sn_msft_dlp_detected_sensitive_information_type]
Reaktion auf Incident zur Vermeidung von Datenverlust	Anwenderdefiniertes Attribut [sn_dlir_custom_attribute]
Integration von DLP Incident Response mit Proofpoint	Proofpoint-DLP-Incident M2M [sn_pp_dlp_incident_m2m]
DLP Incident Response integration with Netskope	Netskope-DLP-Incident M2M [sn_ns_dlp_incident_m2m]
Integration von DLP Incident Response mit Symantec	Typ der erkannten sensiblen Informationen [sn_sym_dlp_detected_sensitive_information_type]

Hinweis:
Alle Systemtabellen wie E-Mails, Bewertungen, Anhänge leiten automatisch zum archivierten DLP-Datensatz weiter.

5. Wählen Sie die zugehörige Datensatzregel aus, die Sie archivieren möchten.

Hinweis:
Weitere Informationen zum Hinzufügen weiterer zugehöriger Datensätze finden Sie unter Zugehörige DLP-Datensätze archivieren unter Now Platform.

Data Loss Prevention Incident Response Incident Management

Verwenden Sie Incident-Management Data Loss Prevention Incident Response, um Incidents zu aktualisieren und zu verwalten, indem Sie den DLP-Anwenderarbeitsbereich, den DLP-Analystenarbeitsbereich und das DLP-Dashboard nutzen.

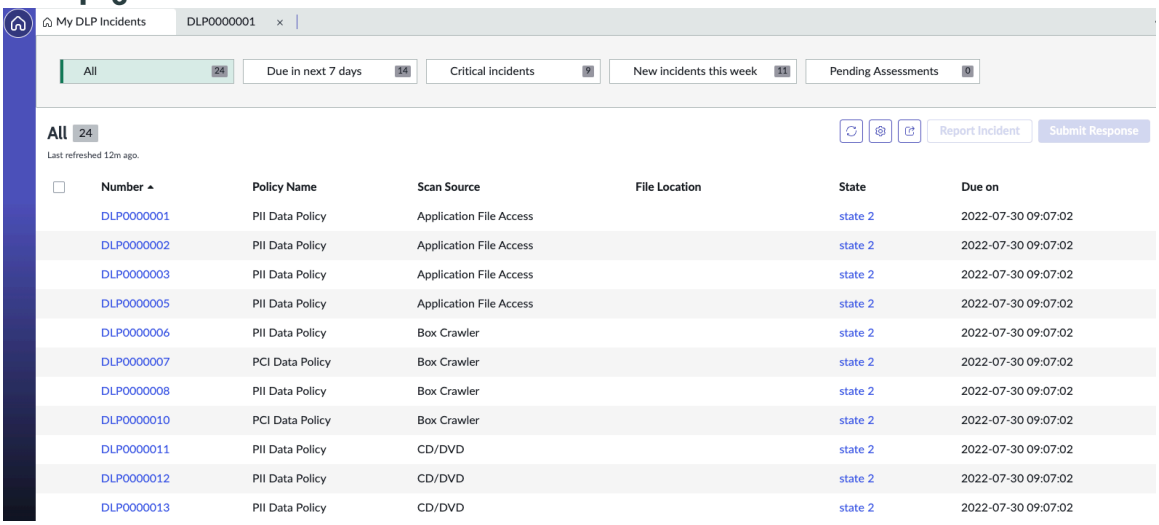
Data Loss Prevention Incident Response Benutzerarbeitsbereich

Der Data Loss Prevention Incident Response (DLP IR)-Benutzerarbeitsbereich ist ein Arbeitsbereich, in dem Endanwender, Manager und Genehmiger auf die zugewiesenen DLP-Incidents reagieren können. Endanwender, Manager und Genehmiger können dann auf die Incidents reagieren, indem sie die richtigen Aktionen angeben.

Sie können auch Bewertungen erstellen und verwalten, damit Endanwender auf DLP-Incidents reagieren können. Der -Arbeitsbereich besteht aus einer Zielseite und Listenansichten, in denen Sie die zugewiesenen DLP-Incidents anzeigen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Homepage des DLP-Anwenderarbeitsbereichs



Melden Sie DLP-Incidents, oder reagieren Sie darauf

Greifen Sie auf den -Benutzerarbeitsbereich Data Loss Prevention Incident Response (DLP) zu, überprüfen Sie die zugewiesenen DLP-Incidents, und melden Sie Incidents, oder reagieren Sie darauf.

Vorbereitungen

Erforderliche Rolle:

- Jeder gültige Anwender/Mitarbeiter

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Anwenderarbeitsbereich**.
   Die Seite „My DLP Incidents“ (Meine DLP-Incidents) wird in einer neuen Registerkarte geöffnet.
2. Klicken Sie auf eine Listenansicht, um die Ihnen zugewiesenen Incidents zu überprüfen.

Listenansicht	Beschreibung
Alle	Zeigen Sie alle zugewiesenen Incidents an.
Fällig in den nächsten 7 Tagen	Zeigen Sie alle Incidents an, die in den nächsten 7 Tagen fällig sind.
Kritische Incidents	Zeigen Sie alle Incidents mit dem Schweregrad „Kritisch“ an.
Neue Incidents diese Woche	Zeigen Sie alle Incidents an, die diese Woche zugewiesen wurden.
Ausstehende Bewertungen	Zeigen Sie alle Bewertungen an, die noch ausstehen.

3. Sie können die DLP-Incidents auf zwei Arten überprüfen:

   a. Die erste Möglichkeit besteht darin, einen oder mehrere DLP-Incidents zu suchen und auszuwählen, die Sie überprüfen möchten, und auf das Kontrollkästchen neben den Incidents zu klicken.

   b. Wählen Sie die für Sie geeignete Option aus.

Automatische Übersetzung

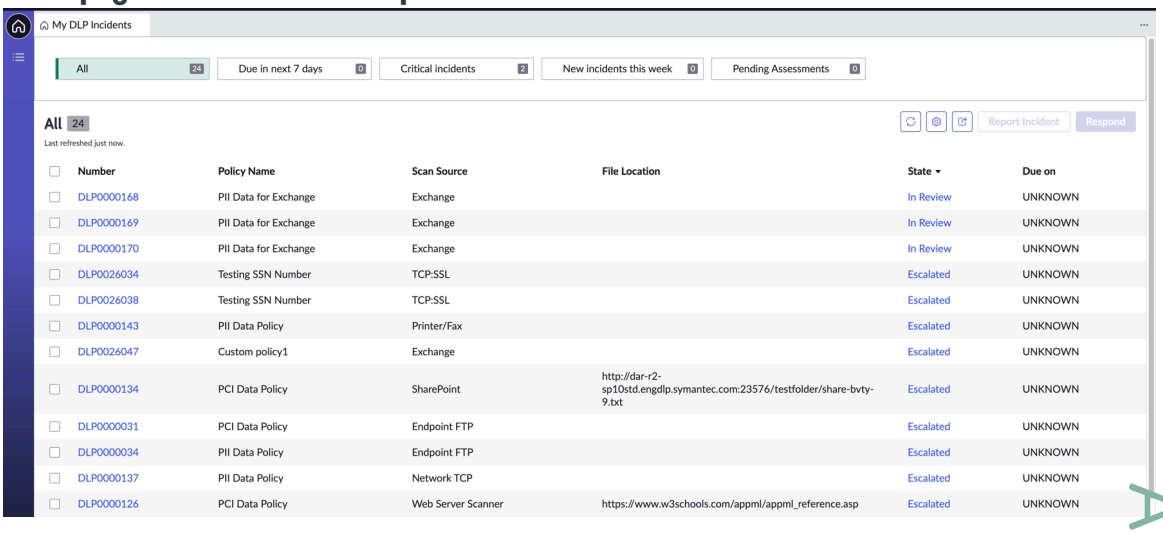
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Homepage des DLP-Endanwenderportals

Option	Beschreibung
Liste neu laden	Option zum Aktualisieren der Liste der DLP-Incidents, wenn Sie eine Aktualisierung vorgenommen haben.
Listenaktionen	Liste der Aktionen, die Sie ausführen können. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Speichern unter** ▪ **Spalten bearbeiten** ▪ **Breiten zurücksetzen** **Hinweis:** Wenn Sie über eine eigene anwenderdefinierte Liste verfügen, die im Abschnitt **„Meine Listen“** für Ihren Arbeitsbereich konfiguriert wurde, können Sie auch die folgenden zusätzlichen Listenaktionen ausführen: ▪ **Umbenennen** ▪ **Speichern** ▪ **Löschen**
URL für alle kopieren	Option zum Kopieren der URLs aller DLP-Incidents.
Incident melden	Aktion, um den Incident als falsch positiv oder als falscher Besitzer zu melden. Sie können beispielsweise den falschen Besitzer melden und einen anderen Besitzer vorschlagen oder den Incident als falsch positiv melden.
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option **„Gelöschte Datei“** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare anzugeben. Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Homepage des DLP-Anwenderportals



c. Die zweite Möglichkeit besteht darin, auf einen bestimmten DLP-Incident zu klicken, um ihn zu öffnen. Auf der Registerkarte **Details** werden die folgenden Abschnitte angezeigt:

- Details: Sie können die Details des DLP-Incidents anzeigen, z. B. Incident-Nummer, Schweregrad, Dateiname.
- Verfassen: Um Kommentare zum DLP-Incident hinzuzufügen, die für alle sichtbar sind, geben Sie die Kommentare auf der Registerkarte Kommentare ein. Um Kommentare hinzuzufügen, die für bestimmte Personen sichtbar sind, geben Sie die Kommentare auf der Registerkarte Arbeitsnotizen (privat) ein.
- Aktivität: Sie können die Details der verschiedenen Aktivitäten für den DLP-Incident anzeigen.
- Anhänge: Wenn Sie Anhänge im Zusammenhang mit dem DLP-Incident haben, klicken Sie auf **Durchsuchen**, und wählen Sie den Anhang von Ihrem lokalen Laufwerk aus.

  Auf der Registerkarte **„Zusätzliche Details“** werden alle zusätzlichen Informationen zum DLP-Incident angezeigt, einschließlich anwenderdefinierter Felder.

> **Wichtig:**
>
> - Anwenderdefinierte Felder für DLP-Incidents werden nur ab Version San Diego unterstützt.
> - Wenn für einen bestimmten DLP-Incident anwenderdefinierte Felddaten verfügbar sind, können Sie sie auf der Registerkarte **„Zusätzliche Details“** anzeigen. Wenn keine anwenderdefinierten Felder für den DLP-Incident vorhanden sind, wird eine leere Seite angezeigt.

- **Typ der erkannten vertraulichen Informationen**: Zeigt die erkannten vertraulichen Informationen des Incidents an.

> **Hinweis:**
> Diese zugehörige Liste ist nur für die DLP-Incidents sichtbar, die für Microsoft- oder Symantec-Integrationen erstellt wurden. Wenn der Benutzer im Microsoft- oder Symantec-Incident-Datensatz auf den erkannten Datensatz des vertraulichen Informationstyps zugreift, wird der hervorgehobene Übereinstimmungsinhalt in Bezug auf diese Integration angezeigt.

d. Wählen Sie die für Sie geeignete Option aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

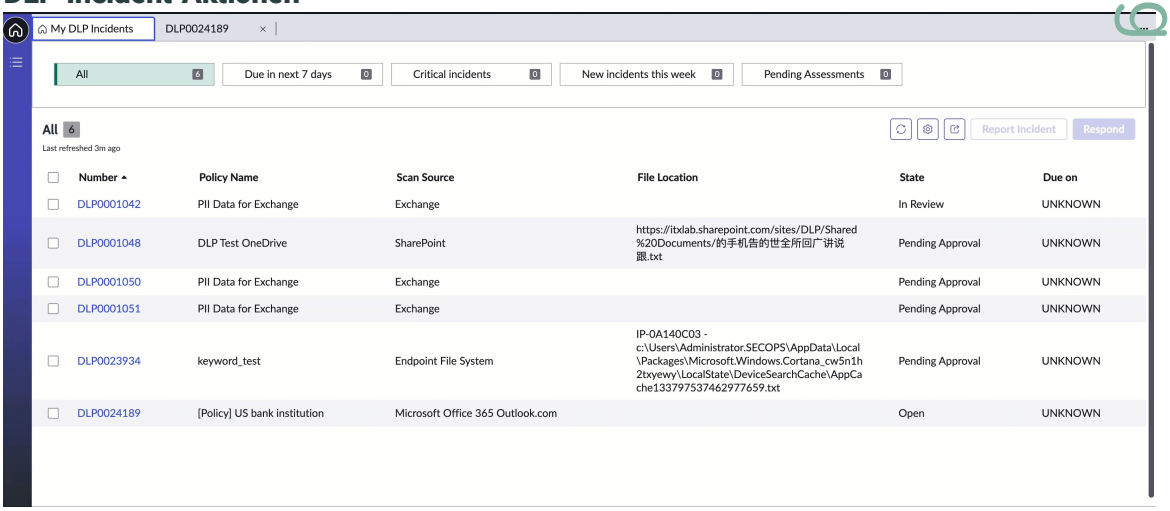
Option	Beschreibung
Falsch positives Ergebnis melden	Aktion zum Melden, dass der DLP-Incident fälschlicherweise ausgelöst oder erstellt wurde. Sie können im Feld Kommentare Details dazu angeben, warum Sie den Incident als falsch positiv markiert haben.
Falschen Besitzer melden	Aktion, um zu melden, dass der DLP-Incident dem falschen Anwender zugewiesen wurde. Wenn Sie den richtigen Besitzer für den Incident kennen, können Sie den Namen des Besitzers im Feld Besitzer vorschlagen auswählen. Verwenden Sie das Feld Kommentare, um zusätzliche Details hinzuzufügen.
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option **„Gelöschte Datei“** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare anzugeben. Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern**.

e. Wählen Sie die Schaltfläche **Antworten** aus, nachdem Sie die Frage des Analysten beantwortet haben. Ein Popup-Fenster zum Senden einer Incident-Antwort wird angezeigt. Wählen Sie die Antwort aus dem Dropdown-Menü aus, und fügen Sie Kommentare hinzu.

f. Wählen Sie **Absenden**.
Ein Banner bestätigt, dass Ihre Antwort erfolgreich übermittelt wurde.

Hinweis:
Der Incident wird dem entsprechenden Genehmiger oder Analysten zugewiesen, und der Endanwender verliert den Zugriff auf den Incident.

DLP-Incident-Aktionen



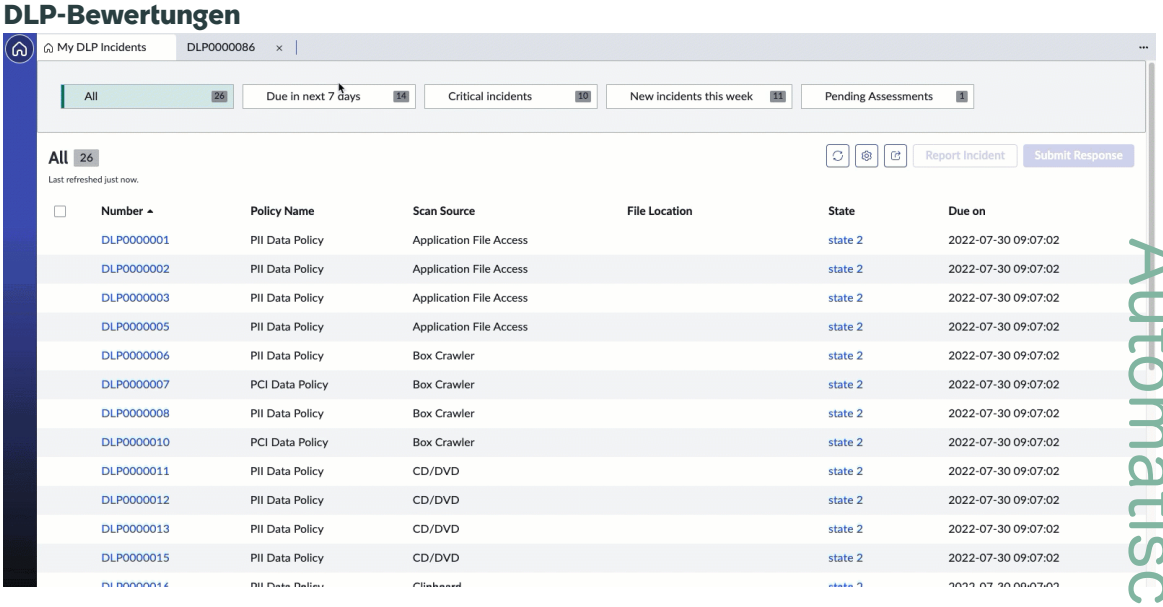
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Um Bewertungen vorzunehmen, wählen Sie die Listenansicht **Ausstehende Bewertungen** aus.

   a. Klicken Sie auf eine bestimmte Bewertungsnummer, um sie zu öffnen.

   b. Beantworten Sie die Bewertungsfragen, und klicken Sie je nach Ihren Anforderungen **auf Speichern** oder **Absenden**.



5. Klicken Sie auf den Kartenabschnitt **Anweisungen**, der über allen Feldern in der DLP-Incident-Formularansicht angezeigt wird, um die zusätzlichen Informationen zu einem bestimmten Incident anzuzeigen.

> **Hinweis:**
> Dieser Abschnitt im Arbeitsbereich führt Benutzer zu den Incident-Informationen, die zum Verständnis der nächsten Schritte der Incident-Lösung beitragen.
>
> Auf der Karte mit den Benutzeranweisungen werden zwei verschiedene Header angezeigt, die Ihnen in der Formularansicht weitere Informationen zu einem bestimmten Incident bieten. Klicken Sie auf den Header einer Benutzeranweisung, um die zusätzlichen Details anzuzeigen.

Weitere Informationen finden Sie unter Erstellen Sie Vorlagen für Benutzeranweisungen und Anwenderanweisungen für die DLP-UI konfigurieren.

Mit dem Modul „Meine Genehmigungen“ arbeiten

Das Modul „Meine Genehmigungen“ steht den angemeldeten Anwendern im Arbeitsbereich für DLP-Anwender zur Verfügung. Anwender können die Zuweisungsgenehmigungsanforderungen hier genehmigen oder ablehnen.

Vorbereitungen
Erforderliche Rolle:

- Endanwender
- Manager
- Genehmigende Person

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Anwenderarbeitsbereich**.
   Die Seite **„My DLP Incidents“ (Meine DLP-Incidents)** wird auf einer neuen Registerkarte angezeigt.
2. Klicken Sie auf das Modul **Meine Genehmigungen** unter dem Modul **Meine DLP-Incidents**.
   Die Listenansicht „Meine Genehmigungen“ wird angezeigt.

   Genehmiger können die Anforderungen in der Listenansicht der Seite „ **Meine Genehmigungen“** genehmigen oder ablehnen. In der Listenansicht können Sie mehrere Anforderungen genehmigen oder ablehnen.

   Genehmiger können die Details der zugewiesenen Anforderung in der Formularansicht anzeigen. Durch Klicken auf die Aktion **Genehmigen** oder **Ablehnen** in der Formularansicht können Sie die Einzelanforderung genehmigen oder ablehnen.

Hinweis:

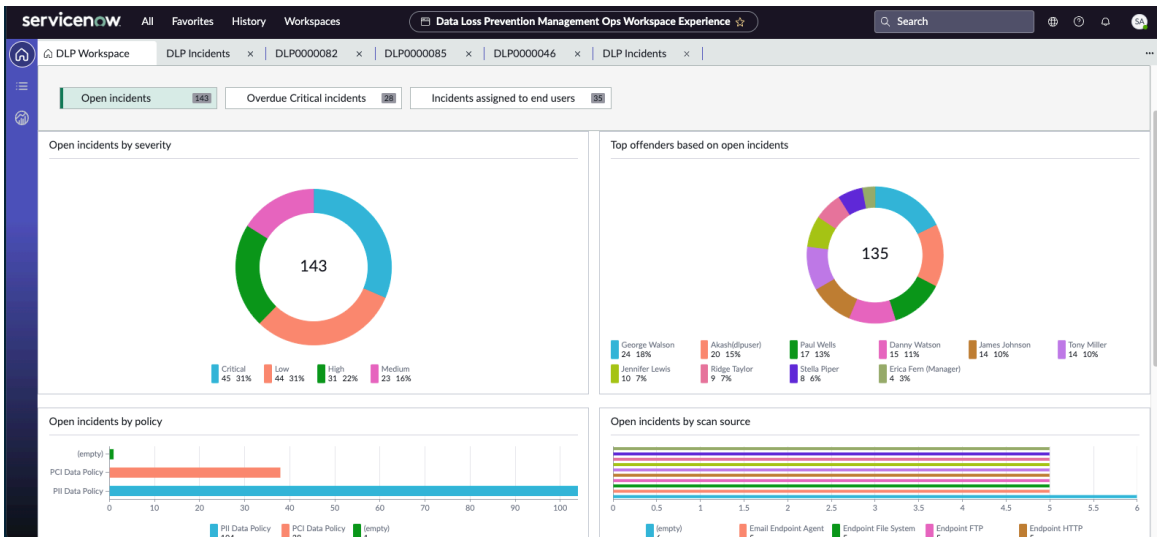
Um die DLP-Incident-Details anzuzeigen, klicken Sie auf verfügbar im Feld **Genehmigen**.

Data Loss Prevention Incident Response Arbeitsbereich für Analysten

Verwenden Sie den Analystenarbeitsbereich Data Loss Prevention Incident Response (DLP IR), um die DLP-Incidents anzuzeigen. Weisen Sie Endanwendern Incidents zur Lösung und weiteren Aufgaben zu.

Der DLP-Arbeitsbereich besteht aus einer Homepage mit Dashboards, Listenansichten und Formularansichten, mit denen Sie DLP-Incidents überwachen können.

Übersichtsseite des DLP-Arbeitsbereichs



Überprüfen Sie Ihre DLP-Incidents, und weisen Sie sie zu

Greifen Sie auf den Analystenarbeitsbereich Data Loss Prevention Incident Response (DLP IR) zu, um die DLP-Incidents zu überprüfen und sie zuzuweisen oder zu lösen. Sie können Trends für Incidents nach Schweregrad, Top-Angreifer, Incidents nach Scan-Quelle und Incidents nach Richtlinie verfolgen.

DLP-Arbeitsbereichs-Homepage

DLP-Arbeitsbereich – Übersicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.analyst: DLP-Incidents bearbeiten und anzeigen
- sn_dlir.analyst_read und sn_dlir.read: DLP-Incidents anzeigen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
   Die Listenseite „DLP-Arbeitsbereich – Meine Incidents-Vorgänge“ wird in einer neuen Registerkarte geöffnet.
2. Klicken Sie auf das Symbol für die Startseite **des DLP-Arbeitsbereichs**, um die Homepage-Ansicht des Arbeitsbereichs anzuzeigen.
3. Überprüfen Sie die Dashboard-Widgets, um Trends nach Incidents nach Schweregrad, Top-Angreifer, Incidents nach Scan-Quelle und Incidents nach Richtlinie zu identifizieren.
4. Klicken Sie auf die entsprechenden Filter auf der -Homepage, um die Widgets nach ihren verschiedenen Kategorien anzuzeigen.

Filter	Beschreibung
Offene Incidents	Alle offenen Incidents anzeigen
Überfällige kritische Incidents	Zeigen Sie die Incidents mit dem Schweregrad „Kritisch“ an, die überfällig sind.
Incidents, die Endanwendern zugewiesen sind	Zeigen Sie die Incidents an, die Endanwendern zugewiesen sind.

5. Sie können die DLP-Incidents auf zwei Arten überprüfen und zuweisen:

   a. Die erste Möglichkeit besteht darin, einen oder mehrere DLP-Incidents zu suchen und auszuwählen, die Sie überprüfen möchten, und auf das Kontrollkästchen neben den Incidents zu klicken.

   b. Wählen Sie die für Sie geeignete Option aus.

Option	Beschreibung
Liste neu laden	Mit dieser Option können Sie die Liste der DLP-Incidents aktualisieren, wenn Sie eine Aktualisierung vornehmen.
Listenaktionen	Liste der Aktionen, die Sie ausführen können. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Speichern unter** ▪ **Spalten bearbeiten** ▪ **Breiten zurücksetzen**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Hinweis: Wenn Sie über eine eigene anwenderdefinierte Liste verfügen, die im Abschnitt **„Meine Listen“** für Ihren Arbeitsbereich konfiguriert wurde, können Sie auch die folgenden zusätzlichen Listenaktionen ausführen: ▪ **Umbenennen** ▪ **Speichern** ▪ **Löschen**
URL für alle kopieren	Option zum Kopieren der URLs aller DLP-Incidents.
Filterbereich anzeigen	Option zum Drilldown der erforderlichen Incidents mithilfe der Filteroption. **i.** Klicken Sie auf den Filter oben links auf der Seite, und wählen Sie **Erweiterte Ansicht**aus. **ii.** Verwenden Sie einen vorhandenen Filter, oder erstellen Sie einen eigenen, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und Werte enthalten. **iii.** Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**: ▪ Wenn **AND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. ▪ Wenn **ODER** ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden. **iv.** Klicken Sie auf **Aktualisieren**.
Incident zuweisen	Aktion, um zu bestimmen, wem der DLP-Incident zugewiesen werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Incident zuweisen an**: Option, um den Incident einem Analysten, Endanwender oder einer anderen Person zuzuweisen. ▪ **Anwender**: Option, um zu bestimmen, welchem Anwender der Incident zugewiesen werden soll. ▪ **Incident-Status vor Anwenderantwort**: Option, um zu bestimmen, in welchem Status sich der Incident befinden soll, bevor der Anwender antwortet. Er kann auch ein anwenderdefinierter Status sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	▪ **Bewertung anhängen**: Option, um anzugeben, ob Sie dem Incident eine Bewertung anhängen möchten. Wenn diese Option aktiviert ist, sind die folgenden Optionen verfügbar: ▪ **Bewertungsvorlage**: Option zur Auswahl einer Bewertungsvorlage für den DLP-Incident. ▪ **Incident-Status nach Benutzerantwort** Option zum Auswählen des Status des DLP-Incidents, nachdem der Benutzer geantwortet hat.
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option **„Gelöschte Datei“** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare anzugeben. Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern**.
Eskalation	Aktion zum Eskalieren des incident. Sie können den Incident eskalieren, indem Sie den Benutzer auswählen, an den Sie ihn eskalieren möchten. Sie können auch zusätzliche Informationen im Feld Kommentare eingeben.
Status aktualisieren	Aktion zum Aktualisieren des Status des incident. Sie können den Status des incident aktualisieren, indem Sie einen der Status aus den Dropdown-Optionen auswählen. Er kann auch ein anwenderdefinierter Status sein.
Schließen	Aktion zum Schließen der Incidents. Wählen Sie den entsprechenden **Abschlusscode** aus der Dropdown-Liste aus, und fügen Sie Abschlusskommentare hinzu. Die Funktion **zum Schließen** in Data Loss Prevention Incident Response erfolgt sowohl asynchron als auch synchron über die Listenansicht. **i.** Synchroner Abschluss: Das synchrone Schließen von Incidents bedeutet, dass die Abschlussaktion sofort ausgeführt wird. Wenn Sie mehrere Incidents zum Schließen auswählen und die Incident-Anzahl kleiner oder gleich 100 ist, werden die Incidents in der Listenansicht der DLP-Incidents im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Vordergrund geschlossen. Hier ist 100 der Standardwert. **ii.** Asynchroner Abschluss: Dies bedeutet, dass die Abschlussanforderung übermittelt wird und die Anwendung die Anforderung im Hintergrund ausführt, wenn die Anzahl der ausgewählten Incidents größer als 100 ist. Sie müssen die Listenansicht der DLP-Incidents aktualisieren, um zu sehen, dass der Incident-Status aktualisiert wurde. **Hinweis:** ▪ Die Anzahl der ausgewählten Incidents für den asynchronen oder synchronen Abschluss wird mit der Systemeigenschaft *sn_dlir.closure_sync_count_limit* konfiguriert. ▪ Standardmäßig ist die Incident-Anzahl auf 100 festgelegt.

c. Die zweite Möglichkeit besteht darin, auf einen bestimmten DLP-Incident zu klicken, um ihn zu öffnen.

- Registerkarte **„Details** “: Zeigt die folgenden Abschnitte an:
  - **Details**: Sie können die Details des DLP-Incidents anzeigen, z. B. Incident-Nummer, Schweregrad, Dateiname usw. Sie haben auch die Möglichkeit, die Felder Schweregrad, Status, Endanwender und DLP-Analystengruppe jeweils zu ändern und zu speichern.
  - **Verfassen**: Um Kommentare zum DLP-Incident hinzuzufügen, die für alle sichtbar sind, geben Sie die Kommentare auf der Registerkarte Kommentare ein. Um Kommentare hinzuzufügen, die für bestimmte Personen sichtbar sind, geben Sie die Kommentare auf der Registerkarte Arbeitsnotizen (privat) ein.
  - **Aktivität**: Sie können die Details der verschiedenen Aktivitäten für den DLP-Incident anzeigen.
  - **Anhänge**: Wenn Sie Anhänge im Zusammenhang mit dem DLP-Incident haben, klicken Sie auf **Durchsuchen**, und wählen Sie den Anhang von Ihrem lokalen Laufwerk aus.
- Registerkarte **Zusätzliche Details** : Zeigt alle zusätzlichen Informationen zum DLP-Incident an, einschließlich anwenderdefinierter Felder.

  Wichtig:
  - Anwenderdefinierte Felder für DLP-Incidents werden nur ab Version San Diego unterstützt.
  - Auf der Registerkarte **„Zusätzliche Details“** können Sie überprüfen, ob anwenderdefinierte Felder für einen bestimmten DLP-Incident erstellt wurden.

- Registerkarte **Anwenderdefinierte Attribute** : Zeigt die Liste der anwenderdefinierten Attribute im Zusammenhang mit dem DLP-Incident an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Andere Incidents von Endanwender**: Zeigt den Incident desselben Endanwenders an. Sie können Incidents konsolidieren, indem Sie die Aktion **Als untergeordneten Incident hinzufügen** in dieser zugehörigen Liste ausführen.
- **Typ der erkannten vertraulichen Informationen**: Zeigt die erkannten vertraulichen Informationen des Incidents an.

  Hinweis:
  Diese zugehörige Liste ist nur für die DLP-Incidents sichtbar, die für Microsoft- oder Symantec-Integrationen erstellt wurden. Wenn der Benutzer im Microsoft- oder Symantec-Incident-Datensatz auf den erkannten Datensatz des vertraulichen Informationstyps zugreift, wird der hervorgehobene Übereinstimmungsinhalt in Bezug auf diese Integration angezeigt.

- **Untergeordnete Incidents**: Zeigt die untergeordneten Incidents an, die manuell (durch Ausführen der Aktion „Als untergeordneten Incident hinzufügen“) oder aus den DLP-Konsolidierungsregeln erstellt wurden. Sie können die Verknüpfung des untergeordneten Incident aufheben, indem Sie in dieser zugehörigen Liste den Vorgang „Verknüpfung des untergeordneten Incident aufheben“ ausführen.
- **Geklonte Incidents**: Zeigt die geklonten Incidents aus dem übergeordneten Incident an. Indem Sie auf die Aktion **Incident klonen** in der Formularansicht klicken, können Sie einen neuen geklonten Incident erstellen.
- Registerkarte**„Bewertungen** “: Zeigt die Liste der Bewertungen an, die dem DLP-Incident zugewiesen sind.

d. Wählen Sie die für Sie geeignete Option aus.

Option	Beschreibung
Incident zuweisen	Aktion, um zu bestimmen, wem der DLP-Incident zugewiesen werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Incident zuweisen an**: Option, um den Incident einem Analysten, Endanwender oder einer anderen Person zuzuweisen. ▪ **Anwender**: Option zum Auswählen des Anwenders, dem der Incident zugewiesen werden soll. ▪ **Incident-Status vor Anwenderantwort**: Option zum Auswählen des Status des Incidents, bevor der Anwender antwortet. Er kann auch ein anwenderdefinierter Status sein. ▪ **Bewertung anhängen**: Option, um anzugeben, ob Sie dem Incident eine Bewertung anhängen möchten. Wenn diese Option aktiviert ist, sind die folgenden Optionen verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	▪ **Bewertungsvorlage**: Option zur Auswahl einer Bewertungsvorlage für den DLP-Incident. ▪ **Incident-Status nach Anwenderantwort**: Option zum Auswählen des Status des DLP-Incidents, nachdem der Anwender geantwortet hat.
Genehmigung aufheben	Aktion zum Abbrechen der Genehmigungsanforderung. Diese Aktion ist für Analysten in der Formularansicht nur sichtbar, wenn sich der DLP-Incident im Status **„Genehmigung ausstehend** “ befindet. Verfügbare Optionen: ▪ **Incident zuweisen an**: Option, um den Incident niemandem, einem Analysten oder einer anderen Person zuzuweisen. ▪ **Anwender**: Option zum Auswählen des Anwenders, dem der Incident zugewiesen werden soll. ▪ **Incident-Status nach Abbruch**: Option zum Auswählen des Status, in dem sich der Incident befinden soll, nachdem die Anforderung abgebrochen wurde. ▪ **Kommentare**: Um zusätzliche Details für den Abbruch bereitzustellen.
Bewertung zuweisen	Aktion zum Anhängen einer Bewertung beim Zuweisen des Incidents. Die Auswahlmöglichkeiten sind wie folgt: ▪ **Bewertungsvorlage**: Option zur Auswahl einer Bewertungsvorlage für den DLP-Incident. ▪ **Incident-Status nach Anwenderantwort**: Option zum Auswählen des Status des DLP-Incidents, nachdem der Anwender geantwortet hat.
Datei herunterladen	Aktion zum Herunterladen der Datei oder E-Mail mit dem verstoßenden Inhalt. Diese Aktion kann für Incidents ausgeführt werden, die für Microsoft OneDrive, SharePoint Online oder Exchange Online erstellt wurden.
Speichern	Aktion zum Speichern der von Ihnen vorgenommenen Änderungen. Sie können die Felder Schweregrad, Status und Endanwender des DLP-Incidents ändern und speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option **„Gelöschte Datei“** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare anzugeben. Hier können Sie auch die erweiterten Antwortoptionen auswählen. **Beispiel: E-Mail-Freigabe aus Quarantäne anfordern**.
Eskalation	Aktion zum Eskalieren des incident. Sie können den Incident eskalieren, indem Sie den Benutzer auswählen, an den Sie ihn eskalieren möchten. Sie können auch zusätzliche Informationen im Feld Kommentare eingeben.
Incident klonen	Aktion zum Erstellen eines Klon-Incidents, wenn der Incident-Datensatz mehrere Anwender betrifft. Sie können die geklonten Incidents mehreren Stakeholdern zuweisen, z. B. Rechtsabteilung/IT. Nachdem Sie einen Klon-Incident-Datensatz erstellt haben, wird unter dem übergeordneten DLP-Incident eine neue Registerkarte **Geklonte Incidents** erstellt, und alle geklonten Incidents werden in dieser Ansicht aufgelistet.

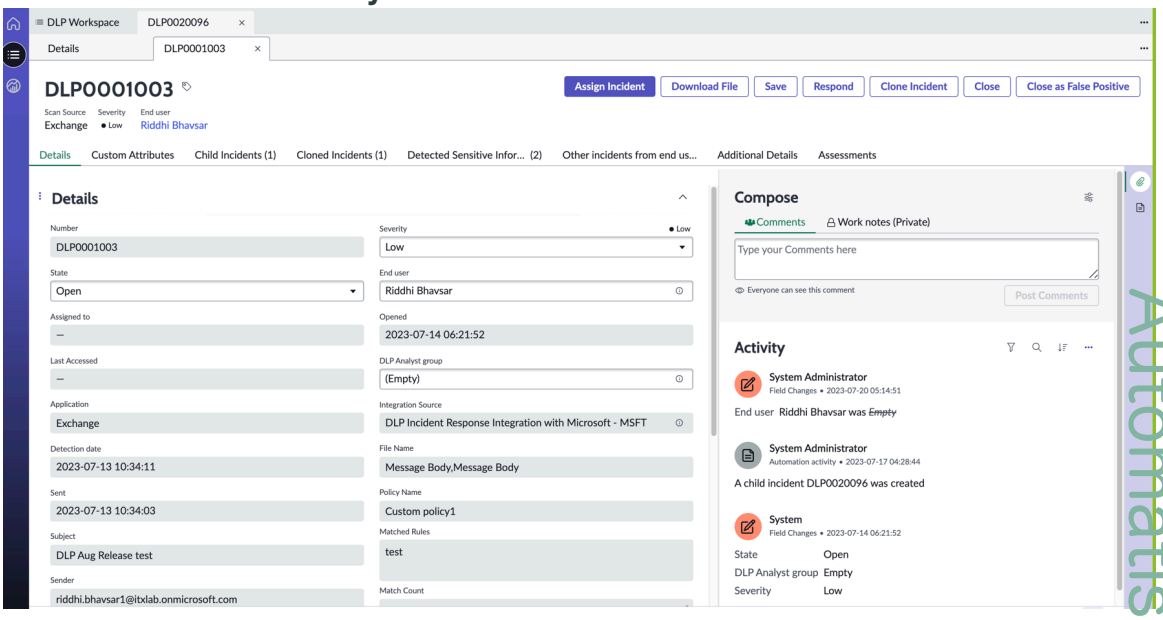
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Hinweis: ▪ Wenn der übergeordnete DLP-Incident-Datensatz geschlossen wird, werden alle geklonten Incident-Datensätze automatisch geschlossen. ▪ Wenn ein DLP-Incident-Datensatz einen geklonten Incident enthält, kann er Endanwendern nicht zugewiesen werden. Die Datensätze für übergeordnete DLP-Incidents können nur von Anwendern mit der Rolle „Analyst“ verwaltet werden. ▪ Sie haben auch die Option, den übergeordneten Status automatisch basierend auf dem Status der geklonten Incidents im Modul „Standardkonfiguration“ zu aktualisieren. Wenn beispielsweise alle geklonten Incidents in den Status Eskaliert verschoben werden, wird der übergeordnete Incident ebenfalls in den Status Eskaliert verschoben.
Schließen	Aktion zum Schließen des incident. Sie müssen den entsprechenden **Abschlusscode** aus der Dropdown-Liste auswählen und bei Bedarf Abschlusskommentare hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Als falsch positiv schließen	Aktion zum Schließen des incident als falsch positiv. Sie können auch zusätzliche Kommentare hinzufügen, bevor Sie den Incident schließen.

DLP-Arbeitsbereich für Analysten



6. Sie können die Listenansicht auf der Homepage anzeigen, indem Sie oben links auf der Seite auf die Registerkarte **Listen** klicken.
   Die Kategorie Listen besteht aus den standardmäßigen und anwenderdefinierten Listenseiten für DLP-Incidents.
   - Registerkarte **Listen**: Standardlisten für DLP-Incidents. Im Folgenden finden Sie die Standardlisten:
     - Alle
     - Öffnen
     - Meine Incidents
     - Meiner Gruppe zugewiesen
     - Eskaliert
     - Überfällig
     - Ausstehende Bewertungen
     - Anwenderaktion ausstehend
     - Geklonte Incidents
     - Archivierte Incidents
   - Registerkarte **Meine Listen**: Zeigt alle Listen an, die Sie umbenannt haben, und alle Listen, die Sie erstellt haben.

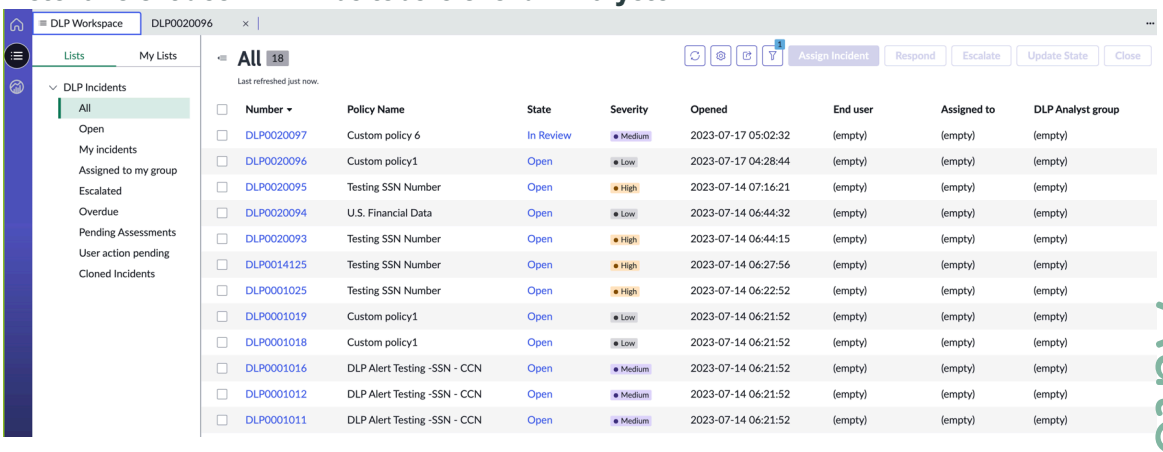
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example

Das folgende Beispiel zeigt den DLP-Arbeitsbereich mit den Listenansichtskategorien. Die Option Listenansicht **Alle** ist ausgewählt.

Listenansicht des DLP-Arbeitsbereichs für Analysten



Zeigen Sie eine Vorschau der Nachweisdateien an

Zeigen Sie eine Vorschau der Nachweisdateien Data Loss Prevention Incident Response im DLP-IR-Arbeitsbereich für Analysten an.

Vorbereitungen

Wichtig:
Bei Verwendung der Aktion Nachweisdateien im DLP-Analystenarbeitsbereich werden die Nachweisdateien vorübergehend in einem unverschlüsselten Format in der ServiceNow-Datenbank gespeichert. Wenn Sie die Nachweisdateien nicht speichern möchten, deaktivieren Sie die Vorschaufunktion für Nachweisdateien. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.analyst

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie das Symbol für Nachweisdateien ( ), das in der kontextbezogenen Sidebar verfügbar ist.
4. Wählen Sie auf der Registerkarte **Nachweisdateien** die Karte **Nachweisdatei**, um eine Vorschau der Nachweisdateien im Dokument-Viewer anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Vorschaufunktion ist für jeden Dateityp unterschiedlich, wie in der folgenden Tabelle aufgeführt.

Dateiformat	Dateierweiterung
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg und .webp Bilddateien werden im Dokument-Viewer-Modus geöffnet.
MicrosoftMicrosoft Azure Event Hubs Office-Dateien	.doc, .docx, .ppt, .pptx, .xls und .xlsx Office-Dateien werden im Dokument-Viewer-Modus geöffnet.
Textdateien	.txt Textdateien werden im Texteditor-Modus geöffnet.
Mail-Dateien	.eml **Hinweis:** Die Dateigröße muss weniger als 5 MB betragen. Sie müssen die Datei zuerst herunterladen, um eine Vorschau des Inhalts anzuzeigen.
PDF-Dateien	PDF-Datei

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateiformat	Dateierweiterung
	○ Geben Sie ein Stichwort ein, um das Dokument zu durchsuchen. ○ Vergrößern und Verkleinern von Funktionen zum Anpassen der Ansicht für bessere Lesbarkeit. ○ Rotieren Sie die Seite im oder gegen den Uhrzeigersinn, um den Inhalt deutlicher anzuzeigen.

Hinweis:

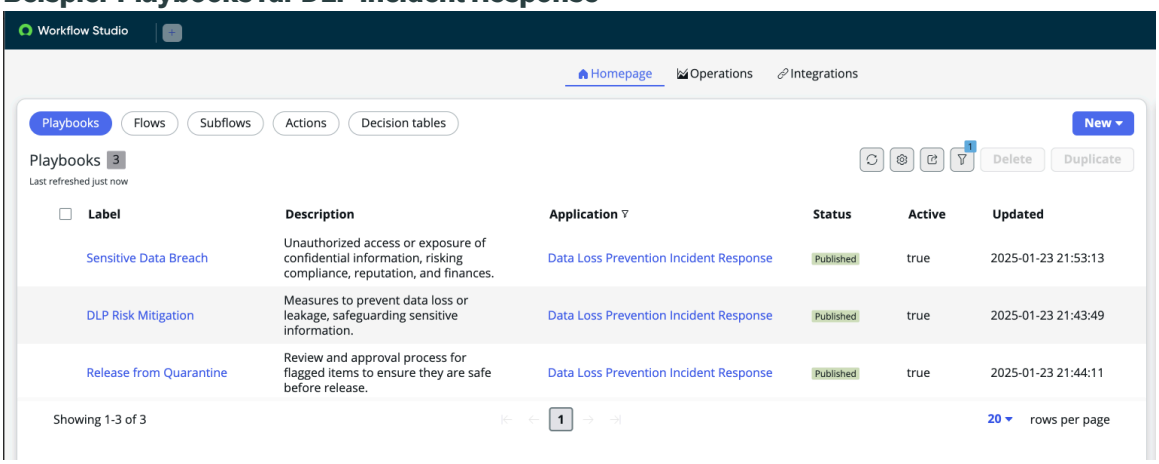
Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion zur Vorschau der Nachweisdatei funktioniert auch für archivierte Incidents.

Playbook für Data Loss Prevention Incident Response

Ein Data Loss Prevention Incident Response Playbook ist eine Schritt-für-Schritt-Anleitung zum Behandeln und Minimieren von Datenverlust-Incidents. Dazu können nicht autorisierte Offenlegungen, Datenverluste oder Verstöße gegen vertrauliche Informationen gehören, die die Sicherheit Ihres Unternehmens gefährden können.

Die folgende Abbildung zeigt die Beispiel-Playbooks, die für DLP IR verfügbar sind.

Beispiel-Playbooks für DLP Incident Response



In der folgenden Tabelle sind die Aktivitäten und Phasen aufgeführt, die beim Erstellen eines Playbooks ausgeführt werden. Weitere Informationen finden Sie unter Fügen Sie ein DLP-Playbook hinzu:

Aktivität	Beschreibung
Erkennung	Identifizieren und bestätigen Sie nicht autorisierten Zugriff oder Offenlegung vertraulicher Daten.
Aufnahme	Isolieren Sie betroffene Systeme oder Anwender, um weiteren Datenverlust oder nicht autorisierten Zugriff zu verhindern.

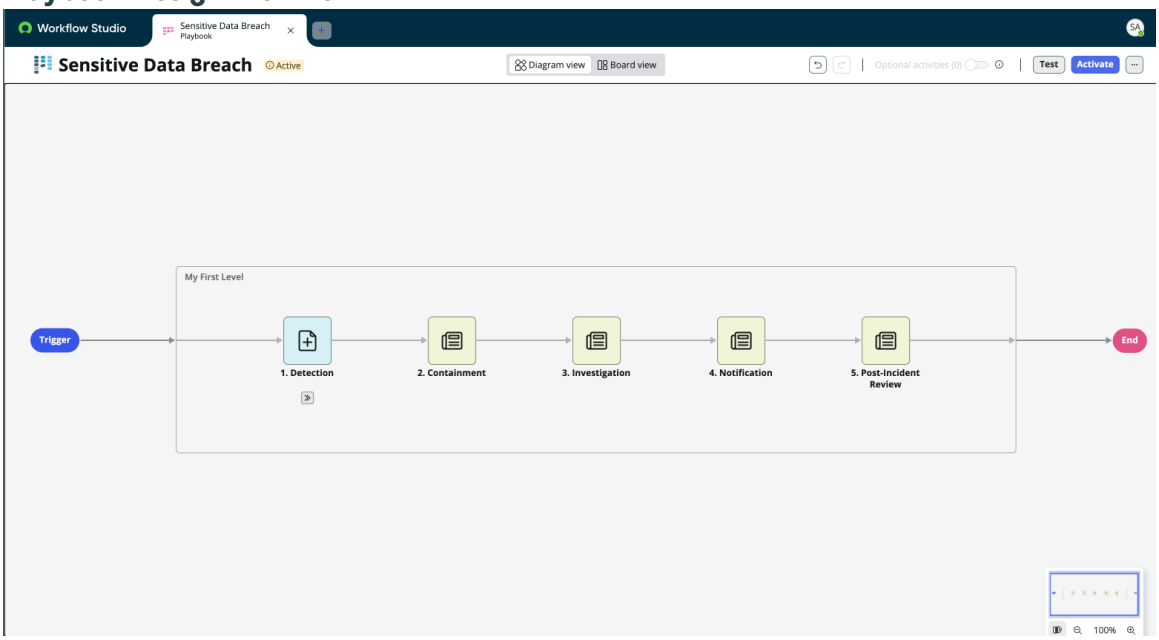
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivität	Beschreibung
Ermittlung	Untersuchen Sie den Verstoß, um zu verstehen, wie er entstanden ist, welche Daten betroffen waren und welche möglichen Auswirkungen er hatte.
Benachrichtigung	Benachrichtigen Sie interne Teams, externe Stakeholder und Aufsichtsbehörden, wenn dies per Gesetz oder Richtlinie erforderlich ist.
Korrektur	Wenden Sie Korrekturmaßnahmen an, um Schwachstellen zu beheben, Richtlinien zu aktualisieren und zukünftige Verstöße zu verhindern.
Wiederherstellung	Stellen Sie Systeme aus sicheren Sicherungen wieder her, und validieren Sie die Integrität von Daten nach einem Incident.
Überprüfung nach Incident	Analysieren Sie den Incident, um die Ursachen zu identifizieren, die Sicherheitskontrollen zu verbessern und Richtlinien zu stärken.

Die folgende Abbildung zeigt den Workflow der Aktivitäten und Phasen, die an der Playbook-Erstellung beteiligt sind.

Playbook-Design-Workflow



Hinweis:
Dies ist das Beispiel-Playbook für die Verletzung sensibler Daten. Je nach Playbook-Typ kann sich der Workflow ändern.

Zugehörige Informationen

Fügen Sie ein DLP-Playbook hinzu

Brechen Sie ein DLP-Playbook ab

Fügen Sie ein DLP-Playbook hinzu

Fügen Sie im Analystenarbeitsbereich Data Loss Prevention Incident Response ein Playbook hinzu, das als Leitfaden für die Behebung und Minimierung von Datenverlust-Incidents dienen kann, die die Sicherheit Ihres Unternehmens gefährden können.

Automatische Übersetzung

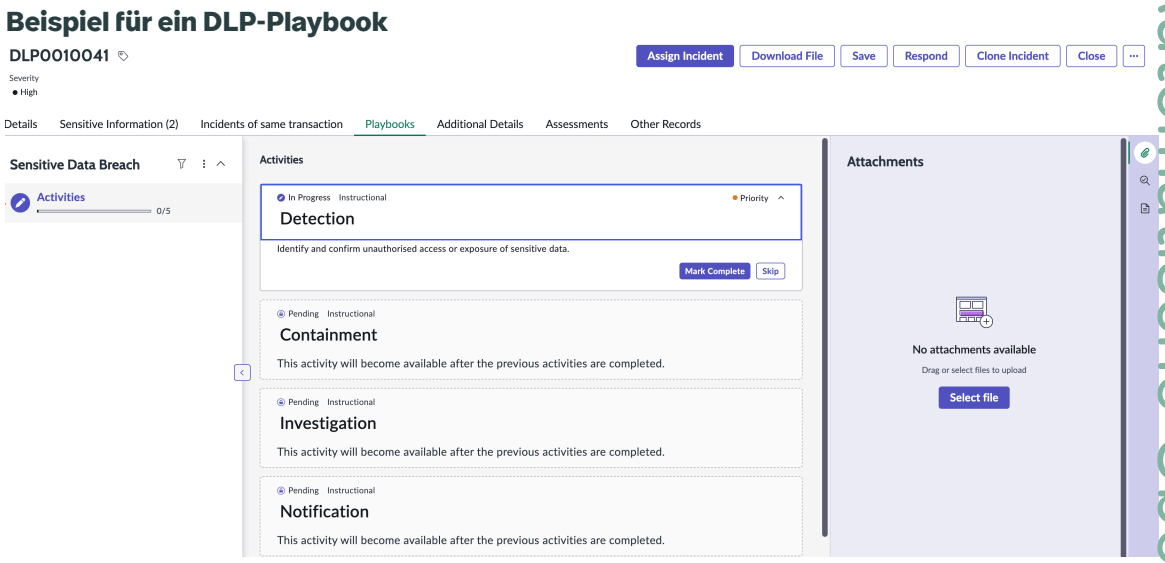
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_dlir.analyst: Hinzufügen oder Anzeigen von Playbooks im DLP-Arbeitsbereich.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie auf der Seite „DLP-Analystenarbeitsbereich – Meine Incidents“ einen beliebigen DLP-Incident.
3. Navigieren Sie zur Registerkarte **Playbooks**.
4. Wählen Sie im Menü (“) die Option **Playbooks hinzufügen** und anschließend ein Playbook aus dem Dropdown-Menü aus.
5. Wählen Sie **Playbooks hinzufügen aus**.
6. Wählen Sie jede Spur aus, um die Aufgaben zu erkunden, die dieses Playbook ausführt.



Brechen Sie ein DLP-Playbook ab

Brechen Sie ein Data Loss Prevention Incident Response Playbook ab, um einen Business Flow zu stoppen, wenn es nicht mehr gültig ist.

Vorbereitungen

Hinweis:
Playbooks werden automatisch abgebrochen, wenn der zugehörige DLP-Incident geschlossen wird.

Erforderliche Rolle: sn_dlir.admin.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen beliebigen DLP-Incident.
3. Navigieren Sie zur Registerkarte **Playbooks**.
4. Wählen Sie im Header des Playbooks, das Sie abbrechen möchten, das Symbol ( ) und dann **Playbook abbrechen aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie einen Grund für den Abbruch des Playbooks an.
6. Wählen Sie **Playbook abbrechen aus**.

Ergebnisse
Unter dem Header des Playbooks wird ein Banner angezeigt, das bestätigt, dass das Playbook abgebrochen wurde.

Zeigen Sie archivierte DLP-Incidents an

Verwenden Sie den DLP-Analystenarbeitsbereich, um die archivierten DLP-Incidents anzuzeigen

Vorbereitungen
Erforderliche Rolle:

- sn_dlir.analyst: DLP-Incidents bearbeiten und anzeigen
- sn_dlir.analyst_read und sn_dlir.read: DLP-Incidents anzeigen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
   Standardmäßig wird der Abschnitt Meine Incidents angezeigt.
2. Klicken Sie auf **Archivierte Incidents**.
   Die Liste der archivierten DLP-Incidents wird angezeigt.
3. Klicken Sie auf die Schaltfläche **Incident-Anzahl anzeigen,** um die Anzahl der archivierten Incidents anzuzeigen.

   Hinweis:
   - Standardmäßig wird die Anzahl der archivierten Incidents ausgeblendet, um die Ladezeit der Liste zu verbessern. Sie müssen auf die Schaltfläche **Incident-Anzahl anzeigen** klicken, um die Anzahl der Incidents anzuzeigen. Außerdem wird eine Informationsnachricht angezeigt, die die Anzahl der Incidents angibt.
   - Im Basissystem ist für archivierte Incidents die Systemeigenschaft „glide.ui.list.seismic.omit.count“ aktiviert, um die Anzahl der Incidents-Listen auszublenden.

4. Wählen Sie einen oder mehrere DLP-Incidents aus, die Sie anzeigen möchten.
   Im DLP-Incident wird der Abschnitt mit den Incident-Details angezeigt.

   Hinweis:
   - Die Registerkarte **Andere Incidents von Endanwendern** enthält auch die archivierten Incidents.
   - **„Inhalt abgleichen“** wird für alle archivierten Incidents unterstützt (die auch in allen Integrationen unterstützt werden), **das Herunterladen von Dateien** wird jedoch nur für Microsoft-Integrationen unterstützt.

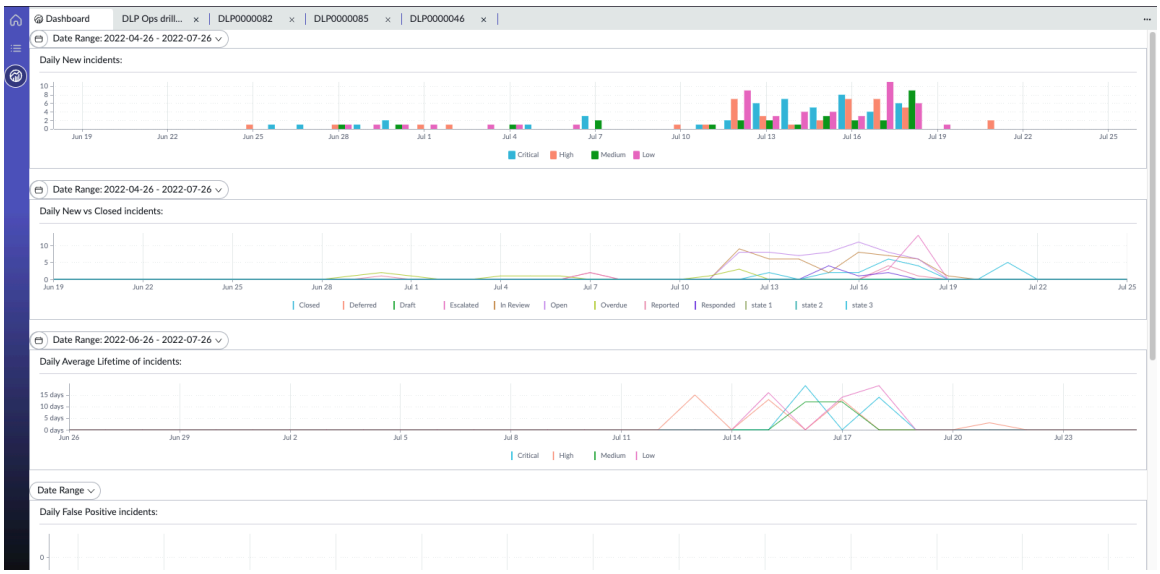
Data Loss Prevention Incident Response-Dashboard

Das Dashboard Data Loss Prevention Incident Response (DLP IR) bietet einen allgemeinen Überblick über Ihre DLP-Incidents und täglichen Incident-Trends in Ihrer Instanz in Form von grafischen Diagrammen. Diese Diagramme helfen Ihnen, die DLP-Incidents effektiv anzuzeigen, zu verwalten und zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Dashboard Data Loss Prevention Incident Response bietet täglich wichtige Einblicke zu Ihren DLP-Incidents. Sie können Indikatoren einrichten und regelmäßig Daten-Snapshots der Incidents sammeln, die den Bedingungen in den Indikatoreigenschaften entsprechen. Die gesammelten Daten werden dann mithilfe von Widgets im Dashboard visualisiert. Um die DLP-Incidents in verschiedenen Zeitintervallen zu analysieren, können Sie verschiedene Datumsbereiche anwenden.

DLP-Dashboard



Analysieren Sie tägliche Incident-Trends in Ihren DLP-Incidents

Greifen Sie auf das Dashboard Data Loss Prevention Incident Response (DLP IR) zu, um die täglichen Trends in Ihren DLP-Incidents zu analysieren und effektiv zu beheben.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.analyst: DLP-Incidents bearbeiten und anzeigen.
- sn_dlir.analyst_read und sn_dlir.read: DLP-Incidents anzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die täglichen Trends mithilfe von Widgets im DLP-Dashboard visualisieren. Die Daten oder Statistiken für die täglichen Trends Ihrer DLP-Incidents werden aus den Eigenschaften des Indikators für tägliche Incidents gesammelt, die von Ihrer Organisation definiert wurden. Sie können wichtige Einblicke gewinnen, indem Sie verschiedene Datenbereiche anwenden, um die DLP-Incidents in verschiedenen Zeitintervallen für die folgenden Diagramme zu analysieren:

- **Tägliche neue Incidents**: Daten aller täglich erstellten DLP-Incidents, unabhängig vom Status der Incidents. DLP-Incidents werden basierend auf den Schweregraden Mittel, Kritisch, Hoch und Niedrig kategorisiert. Jeder Schweregrad von DLP-Incidents wird im Diagramm durch eine bestimmte Farbe dargestellt.
- **Tägliche neue vs. geschlossene Incidents**: Die verschiedenen Status der DLP-Incidents und ein Vergleich zwischen den täglichen neuen Incidents und den täglichen geschlossenen Incidents. Die Kategorie „Täglich Neu“ enthält alle DLP-Incidents in den Status „Offen“, „Entwurf“, „Eskaliert“, „In Überprüfung“, „Überfällig“, „Gemeldet“, „Beantwortet“ oder „Anwenderdefiniert“ (falls vorhanden). Die Incident-Kategorie „Geschlossen“ enthält die geschlossenen DLP-Incidents. Jeder DLP-Incident-Status wird im Diagramm durch eine bestimmte Farbe dargestellt.

Automatische Übersetzung

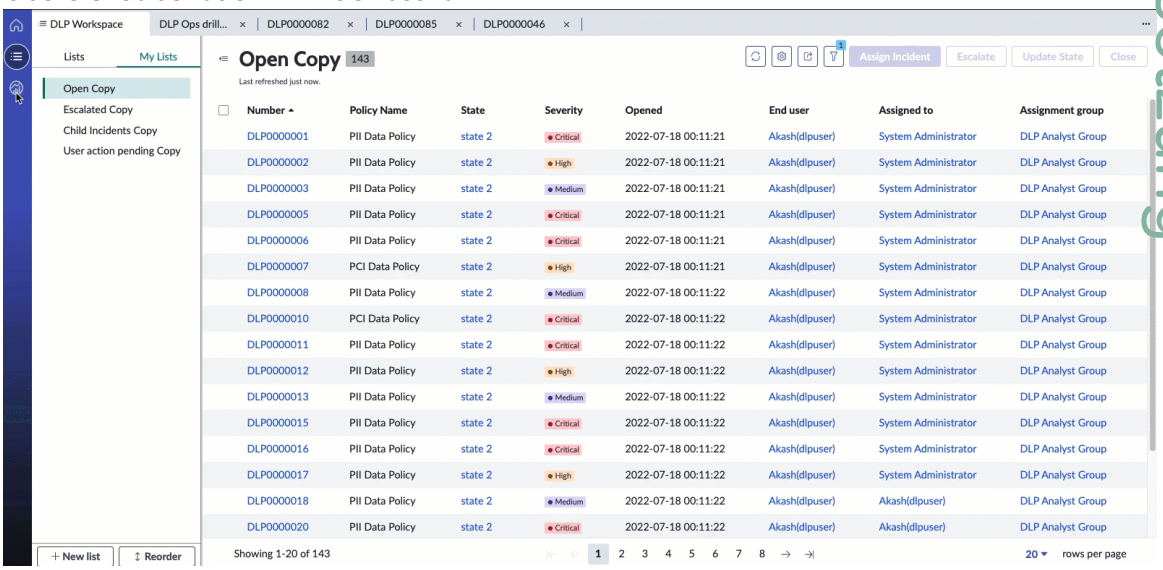
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Tägliche durchschnittliche Lebensdauer von Incidents**: Die Lebensdauer eines incident ist der Zeitraum zwischen dem Öffnen und dem Schließen eines bestimmten DLP-Incidents. Die tägliche durchschnittliche Lebensdauer wird nur für die geschlossenen DLP-Incidents berechnet.
- **Tägliche falsch positive Incidents**: Daten aller DLP-Incidents, die als tägliche falsch positive Incidents gemeldet wurden. Die täglichen falsch positiven Incidents werden basierend auf den Schweregraden Mittel, Kritisch, Hoch und Niedrig kategorisiert. Jeder tägliche Schweregrad von falsch positiven Incidents wird durch eine bestimmte Farbe im Diagramm dargestellt.
- **Alter vs. Schweregrad von Incidents**: Datenvergleich aller DLP-Incidents, kategorisiert nach Alter und konfiguriert mit dem Schweregrad der DLP-Incidents. Die Kategorie „Alter“ enthält alle DLP-Incidents unter dem von Ihrer Organisation definierten Alter. Weitere Informationen zu Altersdiagrammen finden Sie unter Erstellen Sie Altersdiagrammkonfigurationen. Der Schweregrad der Incidents umfasst alle DLP-Incidents in der Kategorie „Hoch“ oder „Niedrig“. Jeder Schweregrad wird im Diagramm durch eine bestimmte Farbe dargestellt.
- **Täglich eskalierte Incidents**: Daten aller täglich eskalierten DLP-Incidents. Die täglich eskalierten Incidents werden basierend auf den Schweregraden Mittel, Kritisch, Hoch und Niedrig kategorisiert. Jeder täglich eskalierte Incident-Schweregrad wird im Diagramm durch eine bestimmte Farbe dargestellt.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Dashboard**.
   Die Seite „Mein DLP-Dashboard“ wird in einer neuen Browserregisterkarte angezeigt.
2. Wählen Sie ein Dashboard-Widget aus, für das Sie eine tägliche Trendanalyse durchführen möchten.
   Beispiel: Tägliche neue Incidents.
3. Überprüfen Sie die Dashboard-Widgets, um Trends zu identifizieren.
4. Klicken Sie auf **Datumsbereich**.

Übersicht über das DLP-Dashboard



5. Wählen Sie einen Datumsbereich aus dem Kalender aus, und klicken Sie auf **Übernehmen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example
Beispielsweise wird das Diagramm Tägliche neue Incidents für den ausgewählten Datenbereich aktualisiert.

6. Verwenden Sie die Filter unter dem Diagramm, um Detailinformationen anzuzeigen und eine eingehendere Analyse durchzuführen.

Eingehende Integration für Data Loss Prevention Incident Response

Erstellen Sie einzelne oder mehrere DLP-Incidents mithilfe der eingehenden REST API.

Erstellen Sie einen einzelnen DLP-Incident

Erforderliche Rolle: sn_dlir.api_integration_user.

Um einen einzelnen DLP-Incident zu erstellen, definieren Sie nach Bedarf die folgenden Parameter:

Feld	Beschreibung
HTTP-Methode	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import
Anforderungs-Header	**Akzeptieren:** `application/json` **Inhaltstyp:** `application/json`
Beispielnutzlast	{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>", "data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>", "dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "",

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	"printer_type": "", "print_job_name": "", "recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"", "url":"", "user_justification":"" }

Beispielantwort	{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id": "7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

Erstellen Sie mehrere DLP-Incidents

Erforderliche Rolle: sn_dlir.api_integration_user.

Um mehrere DLP-Incidents aus derselben Anforderung zu erstellen, definieren Sie die folgenden Parameter nach Bedarf:

Feld	Beschreibung
HTTP-Methode	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple
Anforderungs-Header	**Akzeptieren:** `application/json` **Inhaltstyp:** `application/json`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

Beispielnutzlast	<pre>{
	  "records": [
	  {
	  "file_name": "<value>",
	  "file_modified_by": "<value>",
	  "work_notes": "<value>",
	  "url": "<value>",
	  "scan_source": "<value>",
	  "data_owner_email": "<value>",
	  "file_created_by": "<value>",
	  "file_owner": "<value>",
	  "policy_name": "<value>"
	  },
	  {
	  "dest_ip": "<value>",
	  "dest_ip_port": "<value>",
	  "detection_date": "<value>",
	  "endpoint_on_corporate_net": "<value>",
	  "files": "<value>",
	  "file_created": "<value>",
	  "file_created_by": "<value>",
	  "file_location": "<value>",
	  "file_modified_by": "<value>",
	  "file_name": "<value>",
	  "file_owner": "<value>",
	  }
	  ]
	}</pre>

Beispielantwort	<pre>{
	  "import_set_id": "a38f69229734dd1056a43d1e6253af75",
	  "multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}</pre>

Hinweis:
Standardmäßig ist die Transformation asynchron. Um die synchrone Transformation festzulegen, erstellen Sie einen neuen Datensatz in der Tabelle REST Insert Multiples [sys_rest_insert_multiple], wählen Sie **sn_dlir_incident_import**als Quelltabelle aus, und legen Sie die Transformation auf **synchron**fest.

DLP-Integrationen

Das -Basissystem Data Loss Prevention Incident Response enthält Integrationen für Drittanbieter-Softwarepakete zur Verhinderung von Datenverlust.

Dieser Abschnitt enthält Anweisungen zum Aktivieren der -Plugins und zum Konfigurieren von ServiceNow und Drittanbieterintegrationen. Außerdem enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten im Basissystem enthaltenen Integrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationskonfigurationen

Das Basissystem enthält eine Reihe von Karten für jede Integrationsimplementierung, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von Plugins Security Operations aufweisen. Die Integrationskarten können durch Auswahl von angezeigt werden **Security Operations** > **Integrationskonfigurationen**.

Data Loss Prevention Incident Response unterstützt die folgenden Drittanbietersoftwarepakete zur Verhinderung von Datenverlust:

Symantec Integration für Data Loss Prevention Incident Response

Die Symantec DLP-Integration unterstützt die Erfassung von Data Loss Prevention Incident Response Incidents, die in der Symantec Data Loss Prevention Incident Response -Bereitstellung erstellt wurden. Nach der Erfassung können Sie die Incident-Management-Funktionen verwenden, um die DLP-Incidents zu korrigieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht und wichtige Funktionen von

Die Symantec DLP-Integration hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Möglichkeit zum Erstellen mehrerer Integrationsprofile für verschiedene Symantec API-Endpunkte.
- Geplante Erfassung von DLP-Incidents von Symantec in Ihrer Instanz ServiceNow.
- Möglichkeit, API-Filter anzuwenden, um die Incidents abzurufen, die den Filterkriterien entsprechen, und den Filter für Symantec DLP-Incidents anzugeben, die importiert werden müssen.
- Zuordnung der DLP-Incident-Status in Ihrer Instanz ServiceNow zu DLP-Incident-Status in Symantec.
- Aktualisiert den Incident-Status in Symantec automatisch, wenn sich der Status in der Instanz ServiceNow ändert.
- Möglichkeit zum Anpassen und Definieren der Schweregradzuordnung zwischen Symantec DLP-Incidents und ServiceNow-Incidents.

Weitere Informationen zur Integration finden Sie in der Symantec-Produktdokumentation .

Erste Schritte mit der Symantec DLP-Integration für Data Loss Prevention

Bevor Sie die Integration verwenden können, müssen Sie sie von ServiceNow® Storeherunterladen.

Prüfliste

Lesen Sie sich die folgenden Informationen durch, bevor Sie mit der Einrichtung Ihrer Symantec DLP-Integration zur Verhinderung von Datenverlust beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Feld	Beschreibung
Stellen Sie sicher, dass Ihnen die erforderlichen Now Platform, Anwendung zur Verhinderung von Datenverlust, MID-Anwendungsrollen zugewiesen sind.	Die folgenden Rollen werden in der DLP-Integration von Symantec auf Now Platformverwendet: • Der -Administrator (admin) installiert die Anwendungen aus ServiceNow® Store und weist den Administrator für die Verhinderung von Datenverlust (sn_dlir.admin) zu. • Benutzer mit der Rolle sn_dlir.admin können die Integration konfigurieren und die Incident-Profile einrichten. • Anwender mit der Rolle sn_dlir.analyst verfügen über Leserollen in der gesamten Integration.
Weisen Sie die erforderlichen Symantec DLP-Anwenderrollen zu.	Überprüfen Sie die Rollen und Berechtigungen für die Symantec DLP-Integration.
Stellen Sie sicher, dass Sie Symantec DLP 15.8 verwenden	Die Symantec DLP-Integration für Data Loss Prevention wird mit Version 15.8 von Symantec Data Loss Prevention getestet. **Hinweis:** Stellen Sie sicher, dass Sie Symantec DLP 15.8 verwenden
Stellen Sie sicher, dass die Kernanwendung ServiceNow®, die zur Unterstützung der DLP-Integration Symantec erforderlich ist, installiert und aktiviert ist.	Stellen Sie sicher, dass die folgenden DLP-Anwendungen und allgemeinen Anwendungen zur Unterstützung der Sicherheit im ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie die Symantec DLP-Integration für die Verhinderung von Datenverlust

Installieren und konfigurieren Sie die Symantec DLP-Integration aus ServiceNow® Store in Ihrer Instanz Now Platform. Starten Sie die Untersuchung von DLP-Incidents anhand der DLP-Incident-Daten Symantec.

Vorbereitungen

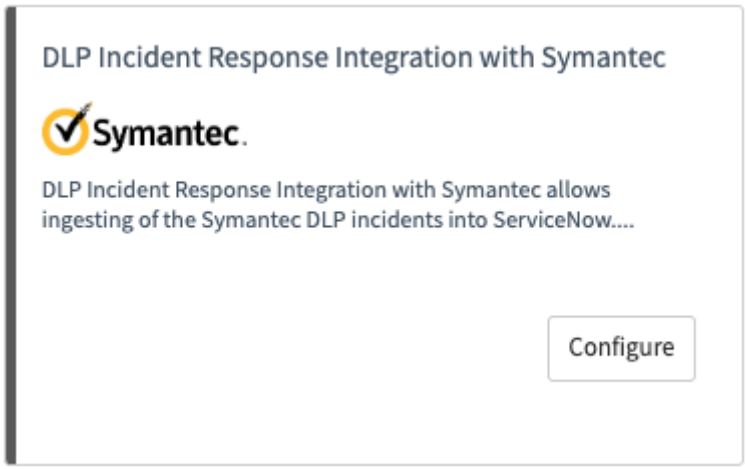
Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Laden Sie die DLP-Integration Symantec von ServiceNow® Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Suchen Sie nach der Kachel „DLP Incident Response Integration with [] (DLP Incident Response-Integration mit Symantec) , und klicken Sie auf **Konfigurieren**.

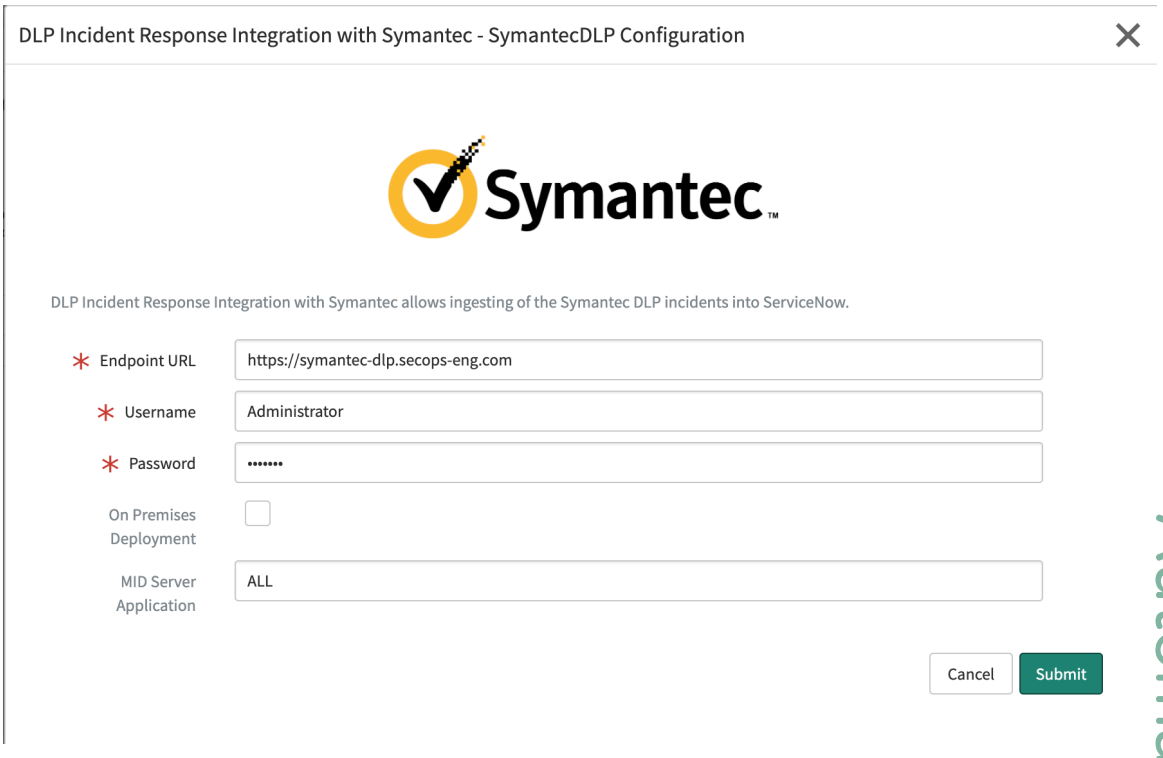


4. Füllen Sie die Felder des Formulars aus.

Formular „Symantec DLP-Integrationskonfiguration“.

Feld	Beschreibung
Name	Name der Symantec DLP-Integrationskonfiguration.
Endpunkt-URL	Symantec REST API-Endpunkt.
Anwendername	Symantec Kontoname. Informationen zu den erforderlichen Rollen und Berechtigungen finden Sie unter Rollen und Berechtigungen .
Passwort	Symantec Account-Passwort.
Lokale Bereitstellung	Option, die Sie auswählen können, wenn Symantec in einer lokalen Instanz bereitgestellt wird. Wenn Sie diese Option auswählen, müssen Sie den MID-Server verwenden, um eine Verbindung zu Symantec herzustellen.
MID-Server-Anwendung	Der Name der MID-Anwendung, die für die Kommunikation mit Symantecverwendet wird. Dieses Feld ist erforderlich, wenn Sie die Option **Lokale Bereitstellung** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.

Ergebnisse

Hinweis:

Verbinden Sie die Symantec-Sub-Prod mit der ServiceNow-Sub-Prod. Synchronisieren Sie alle Anwendernamen und Passwörter über alle Instanzen hinweg, um zu vermeiden, dass Accounts abgemeldet werden.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die DLP-Integration Symantec auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für die Symantec DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform. Bestimmen Sie die Symantec DLP-Incidents, die zum Erstellen von DLP-Incidents geeignet sind.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Now Platform®, um die DLP-Incidents vom Endpunkt Symantec abzurufen. Speichern Sie diese Incidents in Ihrer -Instanz ServiceNow® als DLP-Incidents.

Prozedur

1. Navigieren zu **Symantec DLP-Integration** > **Incident-Profil**.

2. Klicken Sie auf **Neu**.

3. Füllen Sie im Formular die Felder im Abschnitt „Name“ aus.

Automatische Übersetzung

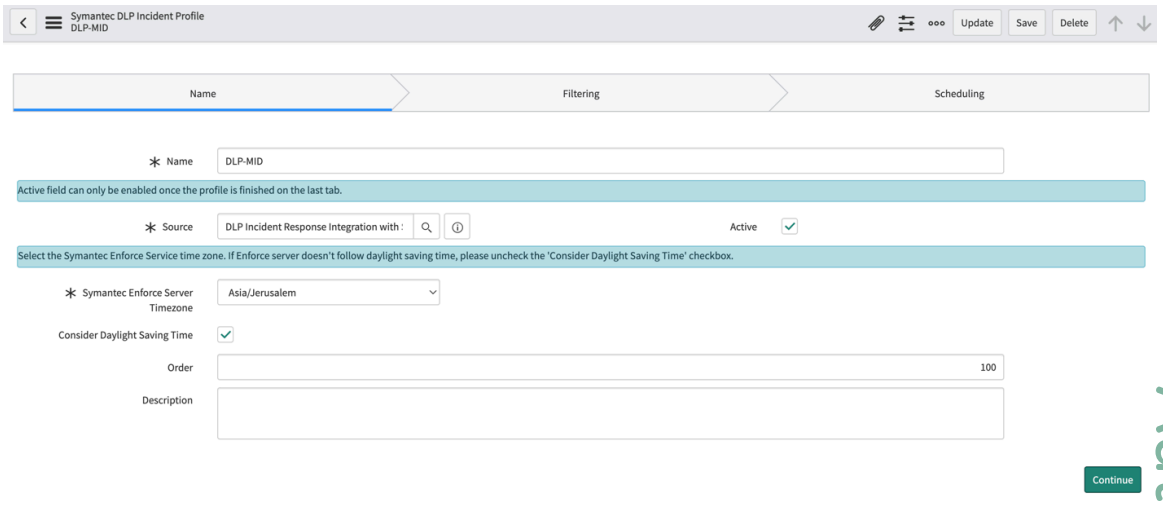
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Profil

Feld	Beschreibung
Name	Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Symantec DLP-Instanz, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die für das Profil erfasst werden sollen.
Aktiv	Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann erst aktiviert werden, nachdem Sie im Abschnitt „ **Zeitplanung** “ auf „Fertigstellen“ geklickt haben. Wenn das Profil aktiv ist, impliziert dies, dass [Now Platform DLP-Incidents Symantec von aktiv abfragt. Die entsprechenden DLP-Incidents werden in DLP erstellt, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Planungsparametern übereinstimmen.
Symantec Enforce Server – Zeitzone	Wählen Sie die Zeitzone für „Symantec Enforcement Server“ im Profil aus, damit Incidents nicht aufgrund von Zeitzonenproblemen übersehen werden.
Sommerzeit berücksichtigen	Aktivieren Sie dieses Kontrollkästchen, wenn der Erzwingungsserver die Sommerzeit berücksichtigt.
Bestellung	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge wird als höchste Priorität betrachtet. Der Standardwert ist 100.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Eindeutige Beschreibung für dieses Profil.



Nächste Maßnahme

Um zum Abschnitt „Filtern“ zu wechseln, klicken Sie auf **Fortfahren**.

Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden

Definieren Sie Filterbedingungen, um die eingehenden Symantec DLP-Incidents aufzuschlüsseln, und legen Sie sie fest. Bestimmen Sie die Incidents, die als DLP-Incidents in ServiceNow® erstellt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Mithilfe von Filtern können Sie DLP-Incidents isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Incidents erstellt, die den Bedingungen entsprechen.

Prozedur

1. Aktivieren Sie das Kontrollkästchen **API-basierter Filter für Incident-Erfassung**, um die API-Filter anzuwenden und die Incidents abzurufen, die den Filterkriterien entsprechen.
2. Fügen Sie die API-Filter hinzu.
   Im Folgenden finden Sie ein Beispiel für die API-Filter.

```
{
        "operandOne": {
           "name": "incidentStatusName"
        },
        "filterType": "string",
        "operator": "EQ",
        "operandTwoValues": [
           "incident.status.New"
        ]
     }
```

Automatische Übersetzung

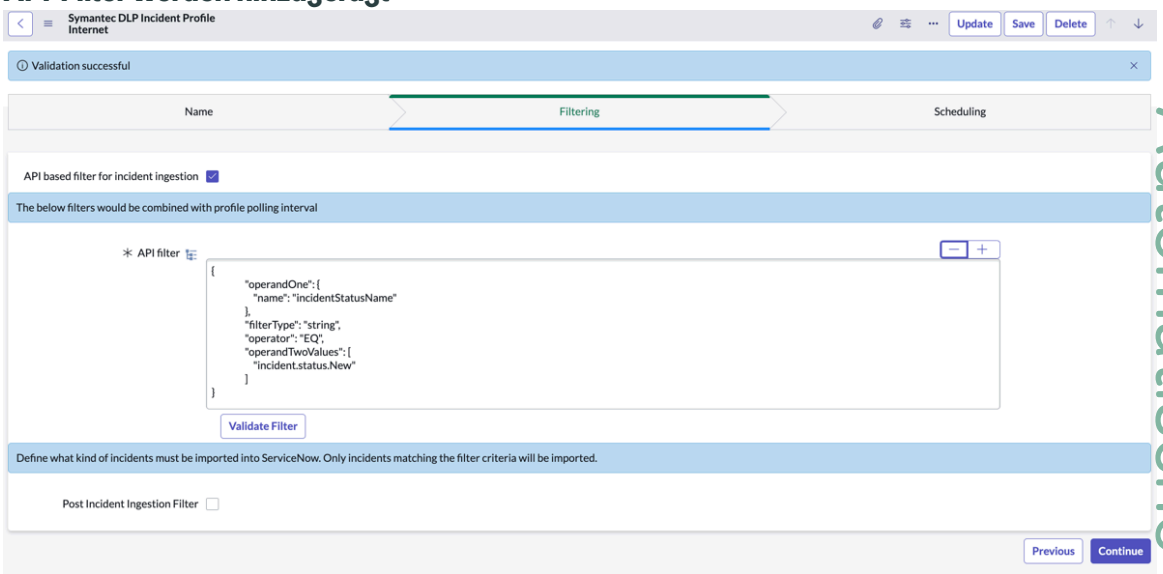
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Weitere Informationen zu den API-Filtern für die Symantec-Integration finden Sie unter Incident-Listen: Parameter – Anforderungsobjektdetails .

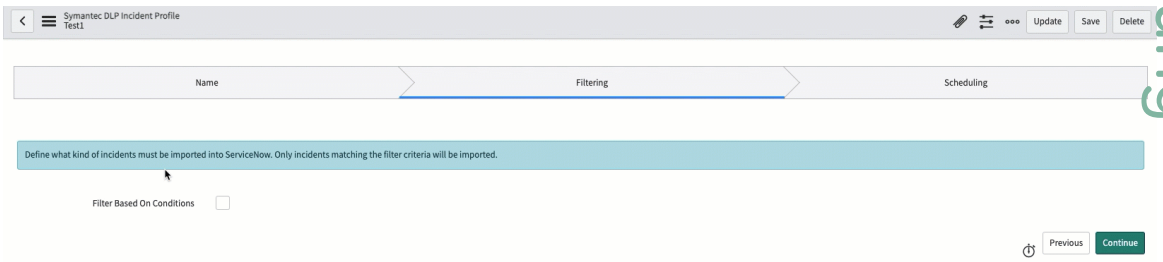
3. Klicken Sie auf **Filter validieren,** nachdem Sie die API-Filter angewendet haben.

Hinweis:
Wenn die Validierung nicht erfolgreich ist, wird eine Fehlermeldung angezeigt, dass die Validierung fehlgeschlagen ist. Dies geschieht, wenn die Filter nicht ordnungsgemäß gemäß den Symantec-APIs eingegeben wurden.

API-Filter werden hinzugefügt



4. Aktivieren Sie das Kontrollkästchen **Incident-Erfassungsfilter posten**, um die Kriterien zu definieren, die ein eingehender Symantec-DLP-Incident erfüllen muss, damit ein DLP-Incident erstellt wird.
Die Optionen im ersten Feld der Filterbedingungen entsprechen den Feldern, die im DLP-Incident verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des incident übereinstimmen.
5. Legen Sie im Bedingungsgenerator die Filter im Feld **Filterbedingungen** fest.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND**oder **ODER**.
   - Wenn **AND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER**ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.

Nächste Maßnahme
Klicken Sie zum Konfigurieren des Zeitplans **auf Fortfahren**.

Konfigurieren Sie den Nachweisdateispeicher

Konfigurieren Sie den Nachweisdateispeicher, um die Nachweisdatei für die DLP-Incidents sicher zu speichern.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Stellen Sie sicher, dass für den Anwender Symantec, den Sie für die ServiceNow-DLP-Integration Symantec konfigurieren, die Optionen Textkörper, Anhänge und Ursprüngliche Nachricht auf der Konfigurationsseite „Rollen“ im DLP-Portal Symantec aktiviert sein müssen. Weitere Informationen finden Sie im Abschnitt Anzeigeattribute im Dokument Rollen konfigurieren .

Warum und wann dieser Vorgang ausgeführt wird
Sie können den Nachweisdateispeicher für die sichere Speicherung von Dateien konfigurieren. Dies stellt eine Option für den internen Speicher in der ServiceNow-Instanz bereit und stellt sicher, dass Dateien mit Feldverschlüsselungvon ServiceNow gespeichert und verschlüsselt werden. Weitere Informationen finden Sie in der Dokumentation zu Feldverschlüsselung in Now Platform.

Wenn ein DLP-Analyst die Aktion Nachweisdateien für DLP-Incidents herunterladen aus dem Analystenarbeitsbereich ausführt, wird die Datei aus dem ausgewählten Speicher heruntergeladen, wenn die Option zum Speichern der Nachweisdatei aktiviert ist. Andernfalls wird die Datei direkt aus der Symantec-Quelle heruntergeladen und nicht in der ServiceNow-Instanz gespeichert.

Hinweis:
Wenn ein DLP-Analyst die Aktion Nachweisdateien für DLP-Incidents herunterladen aus dem Analystenarbeitsbereich ausführt, wird die Datei aus dem ausgewählten Speicher heruntergeladen, wenn die Option zum Speichern der Nachweisdatei aktiviert ist. Andernfalls wird die Datei direkt aus der Symantec-Quelle heruntergeladen und nicht in der ServiceNow-Instanz gespeichert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Symantec DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf den Abschnitt **„Nachweisspeicher“** im Formular „Incident-Profil“.
3. Aktivieren Sie das Kontrollkästchen **Nachweisdateispeicher,** um den Dateispeicher zu aktivieren.
4. Wählen Sie den bevorzugten Speichertyp aus.
5. Klicken Sie auf **Fortsetzen** und wechseln Sie zum Abschnitt **Zeitplanung**.

Ergebnisse

Die Nachweisdateien werden gemäß der Konfiguration gespeichert, nachdem die Incident-Erfassung abgeschlossen wurde.

Nachweisdateien herunterladen

Laden Sie DLP-Incident-Beweisdateien, die gegen die DLP-Richtlinie verstoßen, auf Symantec herunter.

Vorbereitungen

Laden Sie diese Datei aus dem DLP-IR-Arbeitsbereich für Analysten und dem DLP-IR-Endanwender-Arbeitsbereich auf Ihren lokalen Computer herunter. Die Aktion „Dateien herunterladen“ ist nur für die Genehmiger im Arbeitsbereich „DLP-IR-Endanwender“ verfügbar.

Erforderliche Rolle:

- sn_dlir.analyst
- sn_dlir.secure_file_download (jeder Genehmiger mit dieser Rolle)

Prozedur

1. Navigieren zu **Alle** > **Symantec DLP-Integration** > **Einstellung**.
2. Aktivieren Sie die Eigenschaft **Sollte das Herunterladen der Datei mit Verstößen des gemeldeten Incidents zulässig sein**.
   Nachdem Sie diese Eigenschaft aktiviert haben, wird jetzt die Aktion **„Datei herunterladen“** im DLP-Arbeitsbereich für Analysten für jeden Symantec DLP-Incident angezeigt.
3. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
4. Öffnen Sie einen DLP-Incident-Datensatz, der aus der Symantec-Quelle erfasst wurde.
5. Klicken Sie auf **Datei herunterladen**.

Hinweis:
Die Datei, die die DLP-Richtlinie in Symantec verletzt hat, wird auf den lokalen Computer des Anwenders heruntergeladen.

Führen Sie die folgenden Schritte aus, damit der Genehmiger die Aktion Datei herunterladen anzeigen kann:

6. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Anwenderarbeitsbereich**.
   Die Seite „Meine DLP-Incidents“ wird auf einer neuen Registerkarte angezeigt.
7. Wählen Sie das Modul **Meine Genehmigungen** aus, das unter dem Modul Meine DLP-Incidents verfügbar ist.
   Die Listenansicht „Meine Genehmigungen“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Öffnen Sie einen Genehmigungsanforderungsdatensatz, der für den Symantec-DLP-Incident ausgelöst wird.
9. Klicken Sie auf das Informationssymbol (i), das im Feld „DLP-Incident“ in der Formularansicht verfügbar ist.
10. Klicken Sie auf **Datei herunterladen**.

Ergebnisse

Nach dem Ausführen dieser Aktion wird die Nachweisdatei entweder im ZIP-Format (wenn der Incident Verstöße in mehreren Komponenten aufweist und/oder die ursprünglichen Nachrichtendaten ebenfalls verfügbar sind) oder als einzelne Datei (wenn der Incident Verstöße in einer einzelnen Komponente aufweist oder nur die ursprünglichen Nachrichtendaten vorliegen) angezeigt verfügbar) werden auf den lokalen Computer des Anwenders heruntergeladen.

Hinweis:
Als DLP-Administrator können Sie den Zugriff auf die Aktion **Datei herunterladen** steuern, indem Sie die Option **Sollte das Herunterladen der verletzten Datei des gemeldeten Incidents zulässig sein**auf der Seite **„Erweiterte Einstellungen“** deaktivieren. Weitere Informationen finden Sie unter Erweiterte Einstellungen für Data Loss Prevention Incident Response konfigurieren .

Zeigen Sie eine Vorschau der Nachweisdateien an

Zeigen Sie eine Vorschau der DLP-Incident-Beweisdateien im DLP-IR-Analystenarbeitsbereich an.

Vorbereitungen

- Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**.
- Stellen Sie sicher, dass die Eigenschaft **sn_sym_dlp.enable_evidence_file_preview** bereits aktiviert ist.

Wichtig:
Bei Verwendung der Aktion „Nachweisdateien“ im DLP-Analystenarbeitsbereich werden die Nachweisdateien für die Dauer, die Sie mit der Eigenschaft **„sn_dlir.preview_temp_files_cleanup_interval“** auf der Seite **„Erweiterte Einstellungen“** ausgewählt haben, in einem unverschlüsselten Format vorübergehend in der ServiceNow-Datenbank gespeichert. Sie können die Vorschaufunktion **für Nachweisdateien** deaktivieren, wenn Sie keine Daten in der ServiceNow-Datenbank speichern möchten. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.analyst

Prozedur

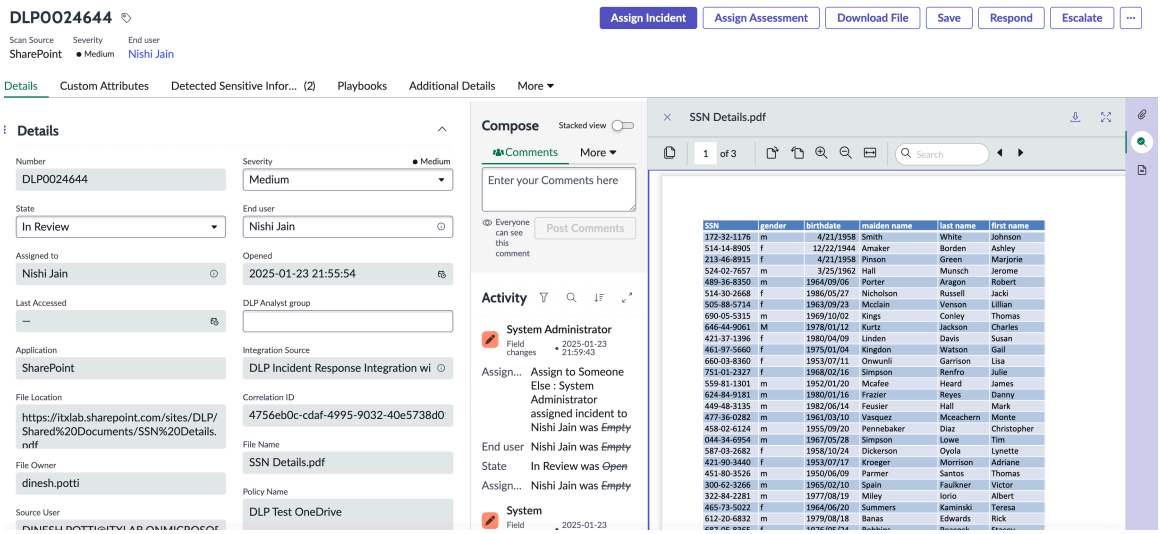
1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie das Symbol **Nachweisdateien**, das im Kontextmenü verfügbar ist.
   Eine Registerkarte wird geöffnet, auf der alle Nachweisdateien abgerufen werden. Sobald der Download abgeschlossen ist, können Sie alle Nachweisdateien auf der Registerkarte **Nachweisdateien** anzeigen.
4. Wählen Sie die **Nachweisdateikarte** aus, die Sie in der Vorschau anzeigen möchten.
   Die Vorschaufunktion ist für jeden Dateityp unterschiedlich.
5. Zeigen Sie eine Vorschau von PDF- und Office-Dokumenten im Dokument-Viewer an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen, um die PDF-Datei im Vollbildmodus zu öffnen. Zu den Office-Erweiterungen, für die der Dokument-Viewer die Nachweisdateien öffnet, gehören: doc, docx, ppt, pptx, xls, xlsx.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Suchen Sie die Suchleiste, und geben Sie das gesuchte Stichwort ein.

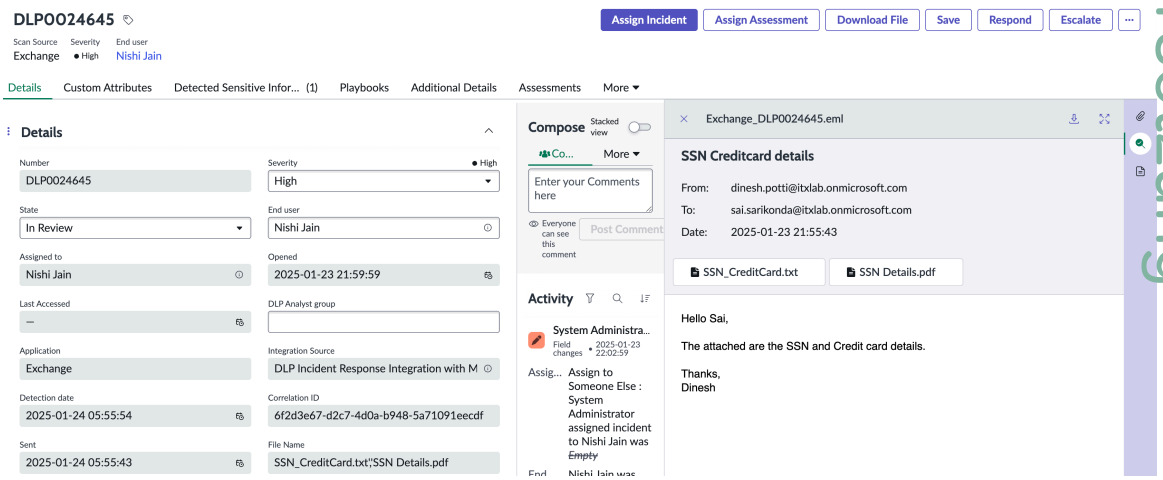
b. Verwenden Sie die Funktionen zum Vergrößern und Verkleinern, um die Ansicht für eine bessere Lesbarkeit anzupassen.

c. Rotieren Sie die Seite im oder gegen den Uhrzeigersinn, um den Inhalt deutlicher anzuzeigen.
Diese Steuerungsoptionen verbessern Ihre Fähigkeit, die Nachweisdatei umfassend zu verstehen. Nur die PDF-Datei hat Steuerungsoptionen im Header.



6. Zeigen Sie eine Vorschau der EML-Dateien an.
Wählen Sie die Anhänge in der E-Mail aus, und zeigen Sie eine Vorschau an.

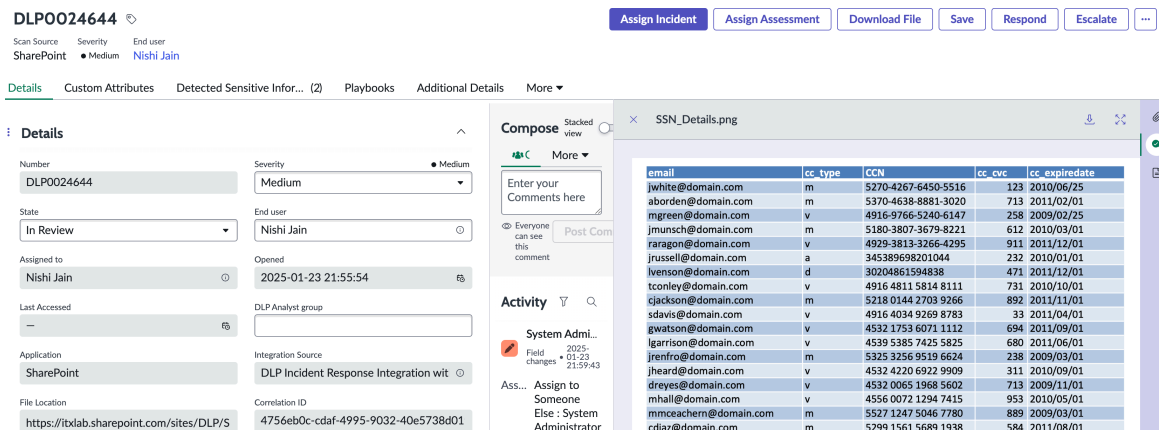
> **Hinweis:**
> Wenn die ausgewählte Nachweisdatei die Grenze von 5 MB überschreitet, kann sie im Analystenarbeitsbereich nicht in der Vorschau angezeigt werden. Sie müssen die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen. Diese Beschränkung gilt nur für EML-Dateien.



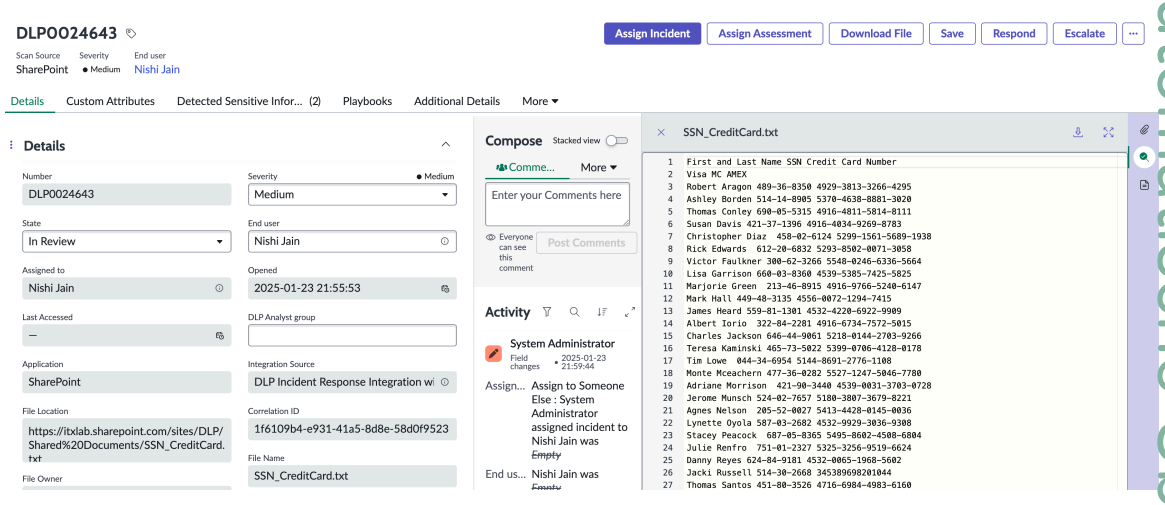
7. Zeigen Sie eine Vorschau der Bilder im DLP-Analystenarbeitsbereich an.
Es werden nur Bilder mit den Erweiterungen .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg und .webp unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Zeigen Sie eine Vorschau von Textdateien im Texteditor an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen.



Automatische Übersetzung

Hinweis:
Andere Nachweisdateien als Office-Dokumente, EML-Dateien, Text- und Bilderweiterungen werden für die Vorschau nicht unterstützt. Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion zur Vorschau der Nachweisdatei funktioniert auch für archivierte Incidents.

Planen Sie den Abruf des DLP-Incident Symantec

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und Symantec DLP-Incidents zu erfassen, die den Kriterien im Profil entsprechen. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus Symantecabrufen.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie zukünftige Incidents abfragen, die der Konfiguration des Incident-Profils entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann mit dem Kontrollkästchen Einmaliger Abruf so konfiguriert werden **, dass ein einmaliger** Abruf erfolgt. Als Verlaufsdatum können die letzten drei Monate ab dem aktuellen Datum angegeben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die verschiedenen Abfrageintervalle können sich auf die Leistung der Symantec Integration für DLP-Incidents auswirken. Planen Sie bei der Zeitplanung, die Systemlast gegen die Dringlichkeit eines incident abzuwägen.

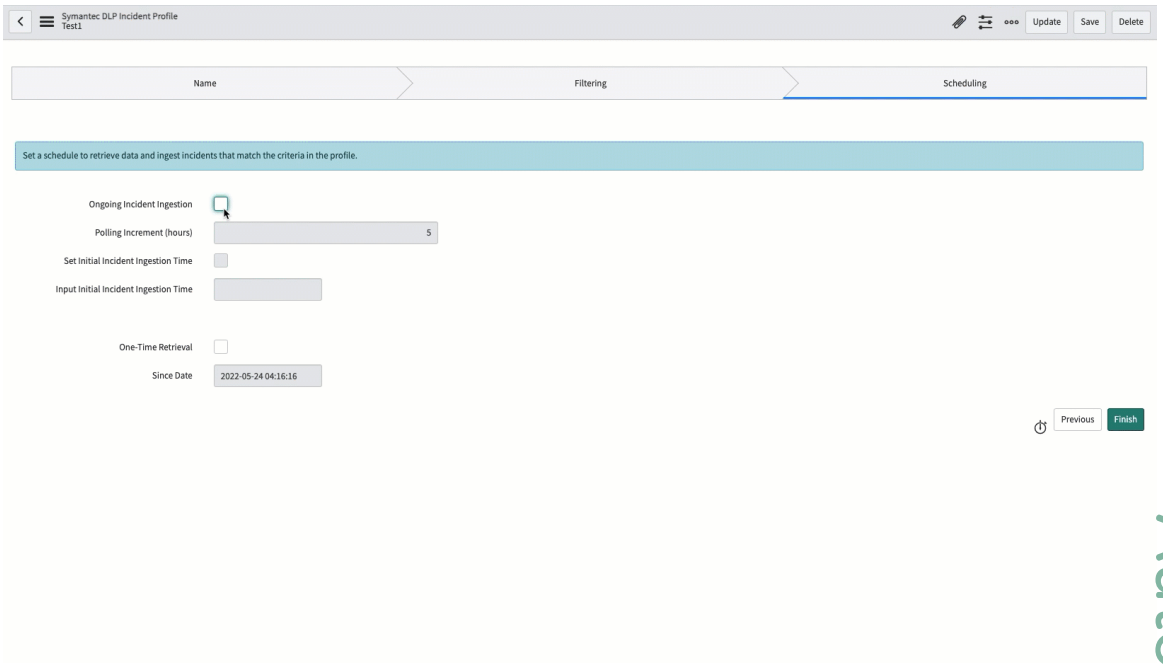
Prozedur

1. Legen Sie einen Zeitplan fest, um Daten abzurufen und Incidents zu erfassen, die den Kriterien im Profil entsprechen.
2. Füllen Sie die Felder im Formular aus.

Zeitplan für den DLP-Incident

Feld	Beschreibung
Laufende Incident-Erfassung	Die laufende Incident-Erfassung, die die Instanz Now Platform für neue Incidents von Symantec abruft. DLP-Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung erfüllt sind.
Abfrageschritt (Minuten)	Die Abfragehäufigkeit, die in Minuten definiert ist. Dieses Feld wird automatisch auf 300 Minuten festgelegt.
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Definieren eines Datums und einer Uhrzeit für die erste Erfassung. Nachfolgende Erfassungen basieren auf dem Zeitraum des Abfrageintervalls.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Zeitpunkt der ersten Incident-Erfassung	Zeitpunkt der ersten Erfassung der Daten. Sie können im sehen, dass Werte angezeigt werden, wenn die Zeit für die erste Incident-Erfassung festgelegt wird.
Nächste Incident-Erfassungszeit (geschätzt)	Nächster Zeitraum für eine geschätzte Incident-Erfassung.
Einmaliger Abruf	Option zum einmaligen Abrufen historischer Daten. Wenn dieses Feld ausgewählt ist, werden Verlaufsdaten gemäß dem im Feld **„Seit Datum“** hinzugefügten Datum aus Symantec DLP abgerufen.
Seit Datum	Datum, ab dem Daten von Symantec abgerufen werden sollen. Dieses Feld kann auf höchstens drei Monate festgelegt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um die erstellte Profilkonfiguration zu speichern, klicken Sie im Popup-Fenster auf **Fertig stellen**.
4. Um das Profil zu aktivieren, öffnen Sie das erstellte Profil.
5. Aktivieren Sie die Option **Aktiv**.
6. Klicken Sie auf **Aktualisieren**.

Ergebnisse
Nach der erfolgreichen Erstellung und Aktivierung des Profils werden die Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen und der DLP-Incidents-Tabelle hinzugefügt.

Zuordnung von Symantec DLP-Incident-Status zu ServiceNow Incident-Status

Synchronisieren Sie den Status der in ServiceNow erfassten DLP-Incidents mit den DLP-Incidents von Symantec. Ordnen Sie das Feld **„ServiceNow-Incident-Status“** dem Feld **„Symantec-Incident-Status“** zu.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Der Incident-Status wird dynamisch aus der Endpunktquelle Symantec abgerufen, die in der Zuordnung hinzugefügt wird. Sie müssen eine 1:1-Zuordnung des Incident-Status durchführen.

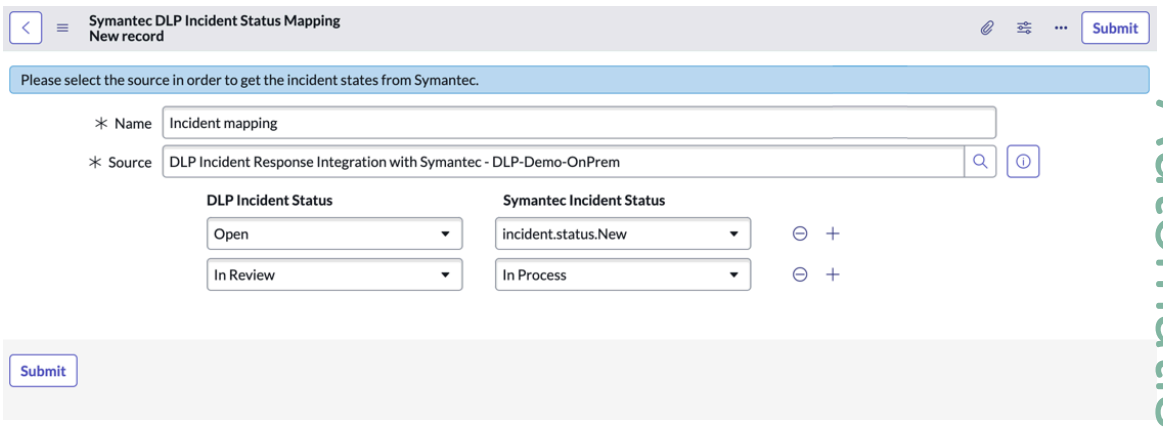
Prozedur
1. Navigieren zu **Symantec DLP-Integration** > **Zuordnung des Incident-Status**.
2. Geben Sie einen **Namen** an, um die Zuordnung zu identifizieren.
3. Wählen Sie die **Quellintegration** aus, aus der Sie den Status abrufen möchten.
4. Ordnen Sie den **DLP-Incident-Status** dem **Symantec-Incident-Status**zu.

Hinweis:
Es ist nicht erforderlich, alle Status zuzuordnen. Sie können nur die erforderlichen Status zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Statuszuordnung für Symantec-DLP-Incident

Feld	Beschreibung
Name	Name des Zuordnungsdatensatzes.
Quelle	Die konfigurierte Symantec-Endpunktquelle, von der Sie den Incident-Status abrufen möchten.
DLP-Incident-Status	Statusliste von DLP-Incidents.
Symantec-Incident-Status	Liste der Status, die aus der Quelle (Symantec-Endpunkt) abgerufen wurden.



5. Klicken Sie auf **Absenden**.

Ergebnisse

Nach der erfolgreichen Erstellung des Datensatzes für die Zuordnungsstatus der ServiceNow Incidents wird der Status der ServiceNow Incidents mit dem Status der DLP-Incidents Symantec synchronisiert.

Wenn Sie den Status eines DLP-Incidents in Ihrer Instanz ServiceNow ändern, wird der Status der zugehörigen DLP-Incidents Symantec auf der Quellplattform Symantec basierend auf der im Datensatz festgelegten Zuordnung geändert.

Schweregradzuordnung zwischen Symantec DLP-Incidents und ServiceNow-Incidents

Verwenden Sie die Schweregradzuordnung, um die Zuordnung zwischen Symantec Incidents und Now Platform® Incidents zu konfigurieren und zu synchronisieren.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Mit der DLP-Schweregradzuordnung können Sie den Quellschweregrad dem DLP-Incident-Schweregrad zuordnen. Sie können den Quellschweregradwert anpassen, definieren und dem gewünschten DLP-Incident-Schweregradwert zuordnen.

Prozedur

1. Navigieren zu **Symantec DLP-Integration** > **Incident-Schweregradzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

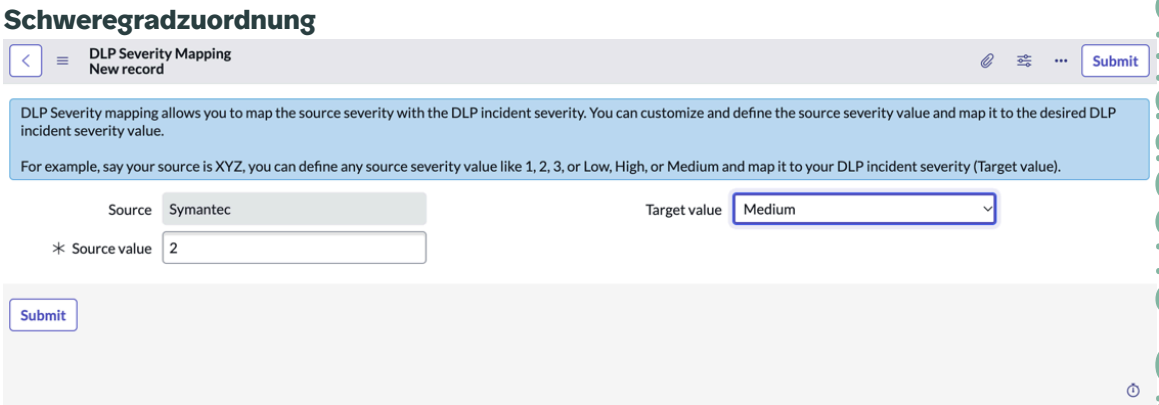
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Schweregradzuordnung

Feld	Beschreibung
Quelle	Die konfigurierte Symantec-Endpunktquelle, von der Sie den Incident abrufen möchten.
Zielwert	Der Zielwert ist die Schweregrad-ID des DLP-Incidents. Die verfügbaren Werte sind „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Info“ (verwendet als Schweregrad für Informationen in Symantec).
Quellwert	Der Quellwert ist der Schweregrad des Symantec-Incidents.

Hinweis:
Im Basissystem gibt es vier Schweregradzuordnungen, die an DLP-Benutzer ausgeliefert werden.

4. Klicken Sie auf **Absenden**.



Konfigurieren Sie intelligente Antwortregeln

Konfigurieren Sie die Symantec-Regeln für intelligente Reaktion, um Antwortaktionen für die erfassten Symantec-DLP-Incidents auszuführen.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie sicher, dass für den Symantec-Anwender, den Sie für die ServiceNow Symantec DLP-Integration konfigurieren, diese Regeln für intelligente Antwort auf der Konfigurationsseite **für Rollen** ausgewählt sind. Weitere Informationen finden Sie im Abschnitt **„Aktionen“** im Dokument „Rollen konfigurieren“ .

Für die abgerufenen intelligenten Antwortregeln kann der DLP-Administrator die Option „Regel(n) für die Reaktion auf Incidents“ und „Zuordnungen für Antwortoption“ erstellen, um die Antwortaktion(en) zu konfigurieren, die für erfasste Symantec-DLP-Incidents ausgeführt werden soll.

Prozedur

1. Navigieren zu **Alle** > **Symantec DLP-Integration** > **Intelligente Antwortregeln**.
   Sie können alle verfügbaren intelligenten Antwortoptionen für jede konfigurierte Integrationskonfiguration anzeigen. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Symantec

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Integration für die Verhinderung von Datenverlust. Folgen Sie dem erläuterten Verfahren (Konfigurationsquelle für Symantec-Integration konfigurieren, falls nicht konfiguriert).

2. Klicken Sie auf eine der intelligenten Antwortregeln, um die Formularansicht zu öffnen.

   Folgen Sie Erstellen Sie Optionsregeln für die Reaktion auf Incidents, um Optionsregeln für die Reaktion auf Incidents und Antwortoptionszuordnungen zu erstellen, um diese Regel für intelligente Antworten im modalen Element „Reagieren“ des DLP-Arbeitsbereichs anzuzeigen.

3. Erstellen Sie die Genehmigungsregeln für die intelligente Antwortregel mithilfe der Registerkarte **Genehmigungsregeln** in der zugehörigen Liste oder des folgenden Verfahrens, das im Abschnitt „Genehmigungsregeln konfigurieren“ erläutert wird.
   Genehmigungsregeln für alle intelligenten Antwortregeln werden in der zugehörigen Liste „Genehmigungsregeln“ angezeigt.
4. Nach dem Erstellen der Optionsregel(en) zur Reaktion auf Incidents wird der Datensatz in der zugehörigen Liste des Datensatzes „Regel für intelligente Antwort“ angezeigt.
5. Verwenden Sie die Schaltfläche **Intelligente Antwortregel aktualisieren** in der Listenansicht, um die Quelle manuell zu aktualisieren.
   Die intelligenten Antwortregeln fügen täglich für jede Quelle automatisch hinzu, aktualisieren oder löschen sie.

Führen Sie intelligente Antwortregeln aus

Verwenden Sie diese Funktion, um intelligente Antwortregeln für Symantec-DLP-Incidents auszuführen.

Vorbereitungen

Sie müssen die Regeln für intelligente Antworten anhand des folgenden Verfahrens konfigurieren, das hier in diesem Abschnitt Konfigurieren Sie intelligente Antwortregelnerläutert wird.

Erforderliche Rolle: sn_dlir.admin

Hinweis:

Die Antwortoptionen im Arbeitsbereich sind für den Endanwender oder Analysten oder Manager basierend auf der im Abschnitt Konfigurieren Sie die Antwortoption für Ihre DLP-Incidentsgenannten Konfiguration verfügbar.

Prozedur

1. Navigieren zu **Alle** > **DLP** > **DLP-Anwenderarbeitsbereich**.
2. Öffnen Sie einen beliebigen Symantec DLP-Incident.
3. Klicken Sie **auf Antworten**.
4. Wählen Sie die Antwortoption in der Dropdown-Liste Antwort aus.
   Die Antwortoptionen werden basierend auf der Konfiguration der **Regel für die Reaktion auf Incidents** und **der Antwortoptionszuordnungen**angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.

> **Hinweis:**
> Sie können auch die Genehmigungsregel(n) für die Antwortoptionen konfigurieren, indem Sie das im Abschnitt Erstellen Sie Genehmigungsregeln erläuterte Verfahren befolgen. Wenn eine Genehmigungsregel für die Regel für intelligente Antwort konfiguriert ist, wird zuerst der Genehmigungs-Flow ausgelöst. Nach Erhalt aller Genehmigungen wird dann der Flow für die Option für intelligente Antwort ausgelöst. Der Status des DLP-Incident wird nach der erfolgreichen Ausführung der Antwortoption gemäß dem Zielstatus der Antwortoptionszuordnung aktualisiert.

Konfigurieren Sie die Symantec DLP-Integrationseinstellungen

Ändern Sie die Standardsystemeigenschaften für Symantec DLP-Integration.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Prozedur

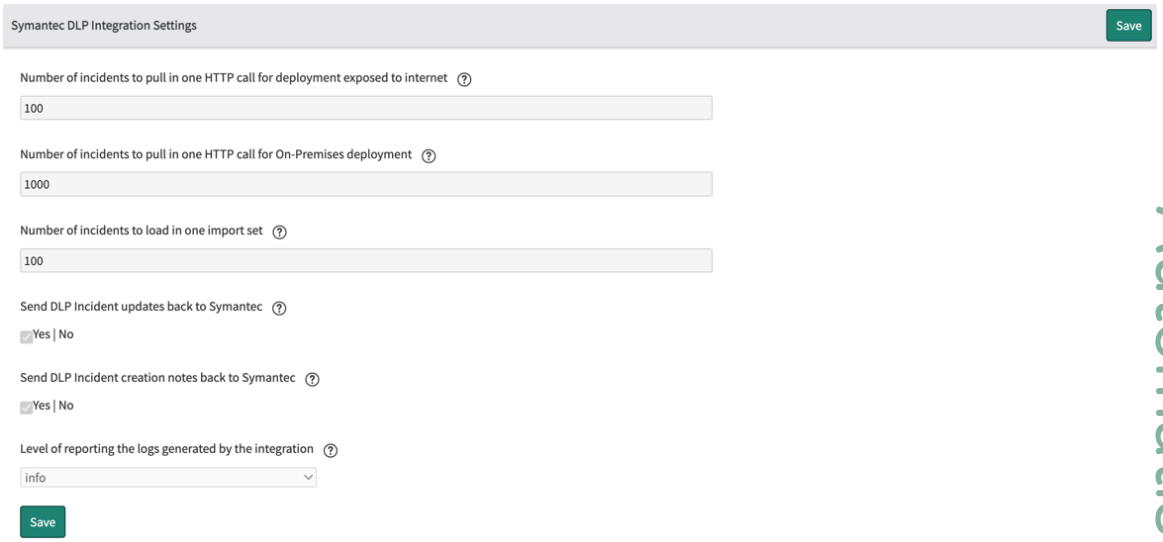
1. Navigieren zu **Symantec DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

Einstellungen

Feld	Beschreibung
Erzwingt einen Grenzwert für die Anzahl von Incidents, die in einem HTTP-Aufruf für die lokale Bereitstellung „sn_sym_dlp.page_size_on_prem“ abgerufen werden sollen	Maximale Anzahl von Incidents, die in einem HTTP-Aufruf für die lokale Bereitstellung von Symantecabgerufen werden sollen. ○ Typ: Ganzzahl ○ Standardwert: 1000
Erzwingt einen Grenzwert für die Anzahl von Incidents, die in einem HTTP-Aufruf für die Bereitstellung im Internet „sn_sym_dlp.page_size_on_internet“ abgerufen werden sollen	Maximale Anzahl von Incidents, die in einem HTTP-Aufruf für die im Internet verfügbar gemachte Bereitstellung Symantec abgerufen werden sollen. ○ Typ: Ganzzahl ○ Standardwert: 100
Anzahl der in einem Importsatz „sn_sym_dlp.incidents_per_attachment“ zu ladenden Incidents	Anzahl der Datensätze, die in einer Anhangdatei zur Verarbeitung gespeichert werden sollen. ○ Typ: Ganzzahl ○ Standardwert: 100
Senden Sie DLP-Incident-Updates zurück an Symantec sn_sym_dlp.incident_update	Mit dieser Eigenschaft können Sie die Statussynchronisierung zwischen den DLP-Incidents ServiceNow und Symantec einschränken. ○ Typ: Boolesch ○ Standardwert: **true**
Senden Sie Notizen zur DLP-Incident-Erstellung zurück an Symantec sn_sym_dlp.incident_creation_notes	Mit dieser Eigenschaft können Sie eine Notiz an Symantec zurücksenden, sobald ein Incident in ServiceNowerstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Typ: Boolesch ○ Standardwert: **true**
Ebene der Berichterstellung für die von der Integration „sn_sym_dlp.ging.verbosity“ generierten Protokolle	Eigenschaft, die die Berichterstellung für die von der Integration generierten Protokolle definiert.



3. Klicken Sie auf **Speichern**.

Domain Separation in der Symantec DLP-Integration

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe

Support: Standard.

So funktioniert Domain Separation mit der DLP-Integration Symantec .

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die Symantec DLP-Integrationsvorgänge in der entsprechenden Domäne aus.

Integration von Data Loss Prevention Incident Response mit Proofpoint

Die Proofpoint DLP-Integration unterstützt die Erfassung von Incidents zur Verhinderung von Datenverlust, die in der Bereitstellung von Proofpoint Verhinderung von Datenverlust erstellt wurden. Nach der Erfassung können Sie die Incident-Management-Funktionen verwenden, um die DLP-Incidents zu korrigieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht und wichtige Funktionen von

Die Proofpoint DLP-Integration hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Erstellung mehrerer Profile für verschiedene Proofpoint -Endpunkte.
- Automatisierung der Erstellung von DLP-Incidents.
- Zuordnung des Felds „DLP-Incident-Status“ Proofpoint zum Feld „DLP-Incident-Status“.
- Filterung von Proofpoint DLP-Incidents.
- Erfassung von Incidents in Ihrer Instanz ServiceNow, sobald die Incidents im DLP-Mandanten Proofpoint erstellt werden.
- Proofpoint Die DLP-Integration unterstützt sowohl Endpunkte als auch E-Mail-Typen von Incidents.
- Automatische Aktualisierungen für den DLP-Incident-Status Proofpoint und Kommentare für die DLP-Incident-Erstellung sowie für Statusänderung und -abschluss auf Seite ServiceNow.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
Proofpoint Website mit Produktdokumentation	Proofpoint-Produktdokumentation
ServiceNow® Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

Erste Schritte mit der Proofpoint -Integration für Data Loss Prevention

Die Proofpoint DLP-Integration unterstützt die Erfassung von Incidents zur Verhinderung von Datenverlust, die im Mandanten von Proofpoint zur Verhinderung von Datenverlust erstellt wurden. Nach der Erfassung werden die Incident-Management-Funktionen verwendet, die die DLP-Incidents beheben.

Prüfliste

Lesen Sie sich die folgenden Informationen durch, bevor Sie mit der Einrichtung Ihrer Proofpoint DLP-Integration für Data Loss Prevention beginnen.

Prüfliste

Feld	Beschreibung
Vergewissern Sie sich, dass Ihnen die erforderlichen Anwendungsrollen Now Platform und Data Loss Prevention Incident Response zugewiesen wurden.	Die folgenden Rollen werden in der DLP-Integration Proofpoint in Now Platformverwendet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Feld	Beschreibung
	• Der -Administrator (admin) installiert die Anwendungen aus ServiceNow® Store und weist den Administrator für die Verhinderung von Datenverlust (sn_dlir.admin) zu. • Benutzer mit der Rolle sn_dlir.admin können die Integration konfigurieren und die Incident-Profile einrichten. • Benutzer mit der Rolle sn_dlir.analyst verfügen über Leserollen in der gesamten Integration.
Weisen Sie die erforderlichen Proofpoint DLP-Anwenderrollen zu.	Überprüfen Sie die Rollen und Berechtigungen für die Proofpoint DLP-Integration.
Vergewissern Sie sich, dass Sie Proofpoint DLP 1.0.1 oder höher verwenden.	Die Proofpoint DLP-Integration für Data Loss Prevention wird mit Proofpoint Data Loss Prevention, Version 1.0.1 oder höher, getestet.
Stellen Sie sicher, dass die zur Unterstützung der Proofpoint DLP-Integration erforderliche Endanwender-Core-Anwendung installiert und aktiviert ist.	Stellen Sie sicher, dass die folgenden DLP-Anwendungen und allgemeinen Anwendungen zur Unterstützung der Sicherheit im ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie die Proofpoint -Integration für die Verhinderung von Datenverlust

Installieren und konfigurieren Sie die Proofpoint DLP-Integration aus ServiceNow® Store in Ihrer Instanz Now Platform. Starten Sie die Untersuchung von DLP-Incidents anhand der DLP-Incident-Daten Proofpoint.

Vorbereitungen

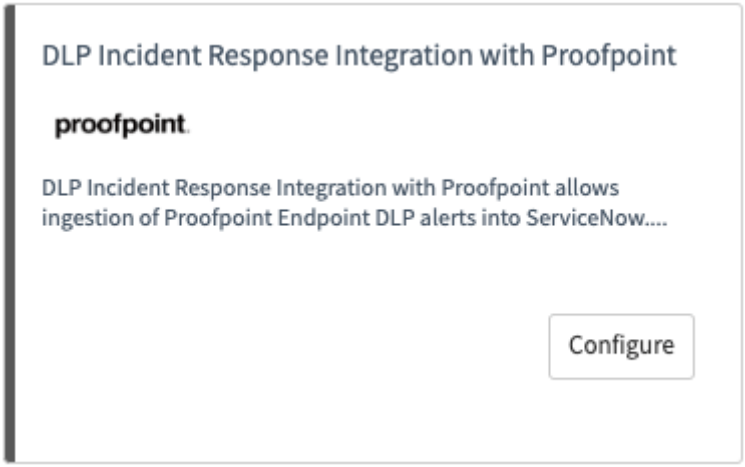
Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Laden Sie die DLP-Integration Proofpoint von ServiceNow® Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel Integration von DLP Incident Response mit Proofpoint, und klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

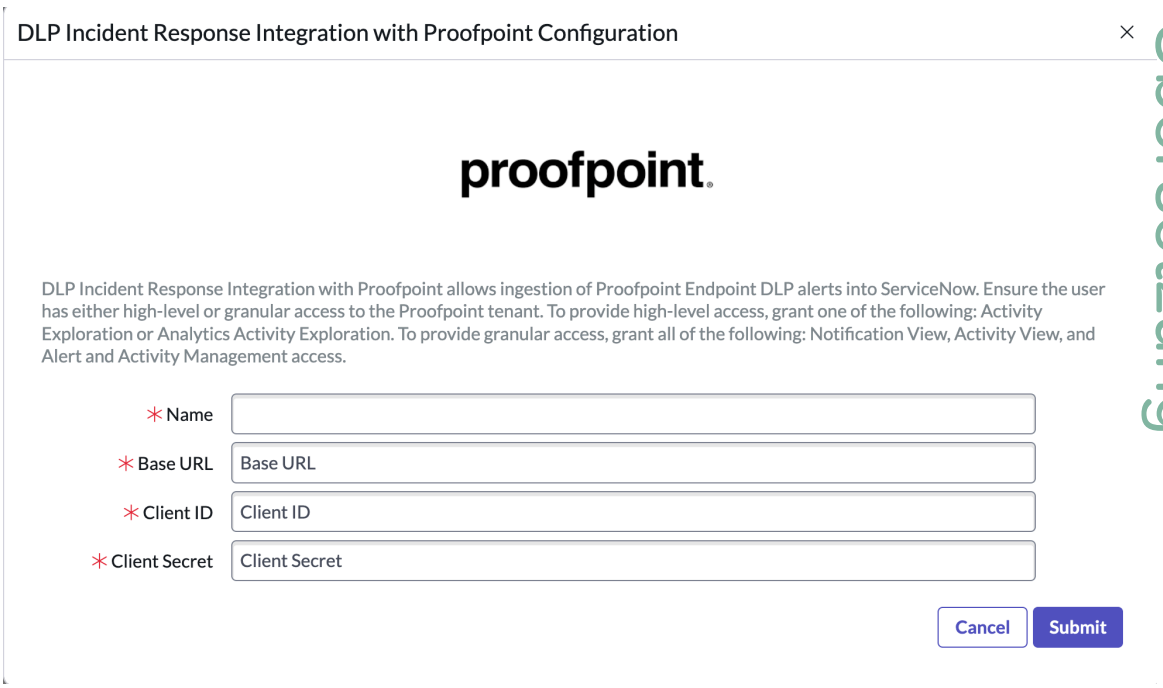
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Felder des Formulars aus.

Proofpoint Formular „DLP-Integrationskonfiguration“.

Feld	Beschreibung
Name	Name der Proofpoint DLP-Integrationskonfiguration.
Basis-URL	URL für Proofpoint, die als REST-Endpunkt dient.
Client-ID	Die ID des zu verwendenden Clients Proofpoint
Geheimer Clientschlüssel	Das für Ihr Benutzerkonto unter Proofpointkonfigurierte Geheimnis.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Anwendername und Passwort werden für die Konfiguration nicht mehr unterstützt. Die vorhandene Kachel „DLP Incident Response Integration with Proofpoint“, die mit dem Anwendernamen und Passwort erstellt wurde, funktioniert jedoch weiterhin normal.

5. Klicken Sie auf **Absenden**.

Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die DLP-Integration Proofpoint auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Konfigurieren Sie den Webhook im DLP-Mandanten Proofpoint für Warnungsbenachrichtigungen an ServiceNow

Konfigurieren Sie mit dem REST API-Endpunkt einen Webhook in Proofpoint, um die Warnungen vom DLP-Mandanten Proofpoint abzurufen. Ihre Instanz ServiceNow von erstellt DLP-Incidents aus diesen Warnungen. Die Proofpoint DLP-Integration bietet einen REST API-Endpunkt, über den Endanwender den Webhook konfigurieren können.

Vorbereitungen
Erforderliche Rolle: sn_pp_dlp.api_integration_user

Prozedur

1. Melden Sie sich bei **Proofpoint**an.
2. Navigieren zu **Proofpoint-Mandant** > **Administrationsanwendung** > **Integration** > **Benachrichtigungsrichtlinien**.
3. Erstellen Sie eine Benachrichtigungsrichtlinie mit einem entsprechenden Namen.
4. Klicken Sie auf die **Benachrichtigungsrichtlinie**, und verwalten Sie die in der Benachrichtigungsrichtlinie konfigurierten Webhooks.
5. Erstellen Sie eine neue Webhook-Konfiguration, indem Sie **auf Webhooks hinzufügen**klicken.
6. Wählen Sie den Webhook-Typ als **Generisch**aus.
7. Geben Sie unter URL-Eingabe eine URL im folgenden Format ein: https://<Instance_Name> .service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts .
8. Behalten Sie die Methode als **POST**bei.
9. Fügen Sie dem Webhook die folgenden Header hinzu:
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. D ändert die anderen Werte nicht.
11. Klicken Sie auf **Speichern**.
12. Navigieren zu **Proofpoint-Mandant** > **Administrationsanwendung** > **Richtlinien** > **Regeln**.
13. Wählen Sie im Abschnitt „Aktionen“ die Regeln aus, für die die Webhook-Benachrichtigung generiert werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

14. Fügen Sie die neu erstellten Benachrichtigungsrichtlinien hinzu, für die ein Webhook konfiguriert ist.
15. Klicken Sie auf **Speichern**.

Erstellen Sie ein Profil für die DLP-Integration Proofpoint .

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform. Bestimmen Sie die Proofpoint DLP-Incidents, die zum Erstellen von DLP-Incidents geeignet sind.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

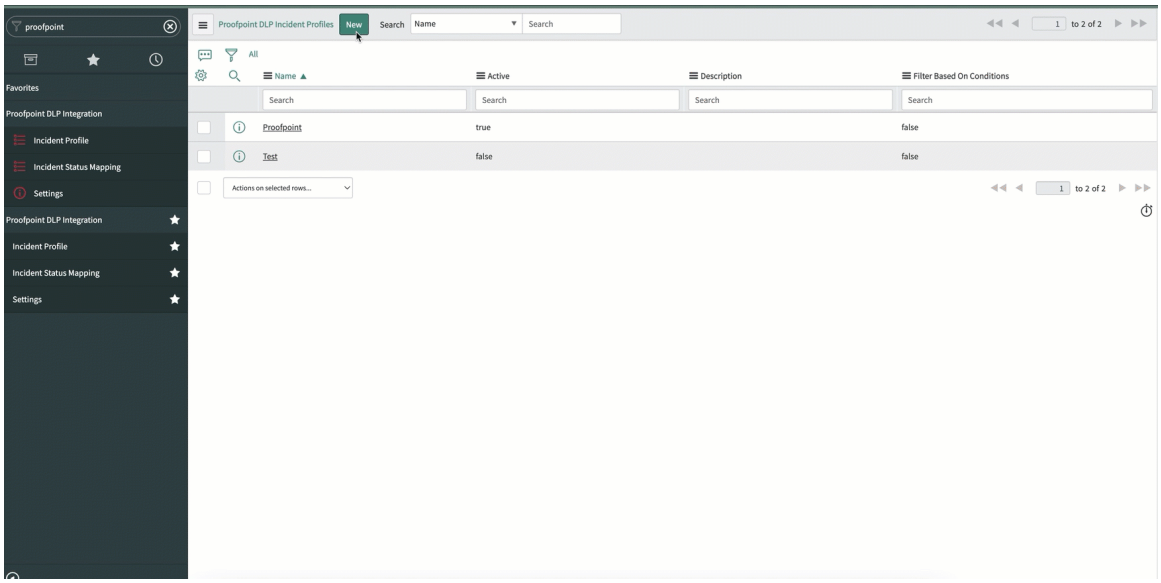
Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie Now Platform, um DLP-Warnungen von Proofpointauszufüllen. Speichern Sie die Warnungen als DLP-Incidents in Ihrer Instanz ServiceNow.

Prozedur
1. Navigieren zu **Proofpoint-DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt **„Name“** aus.

Erstellen Sie ein Profil für das Formular Proofpoint DLP-Integration

Feld	Beschreibung
Name	Name des Profils. Anhand dieses Namens können Sie das Profil identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Die DLP-Instanz Proofpoint, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die für das Profil erfasst werden sollen.
Aktiv	Option zum Aktivieren des Profils. Wenn das Profil aktiv ist, ist die Instanz Now Platform bereit für den Empfang der Incidents von Proofpoint.
Beschreibung	Beschreibung, anhand derer dieses Profil von anderen Profilen unterschieden werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Fortsetzen** und wechseln Sie zum Abschnitt Filtern.

Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden

Definieren Sie Filterbedingungen, um die eingehenden Proofpoint DLP-Incidents zu filtern, und legen Sie sie fest. Steuern Sie, welche DLP-Incidents unter ServiceNow® erstellt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

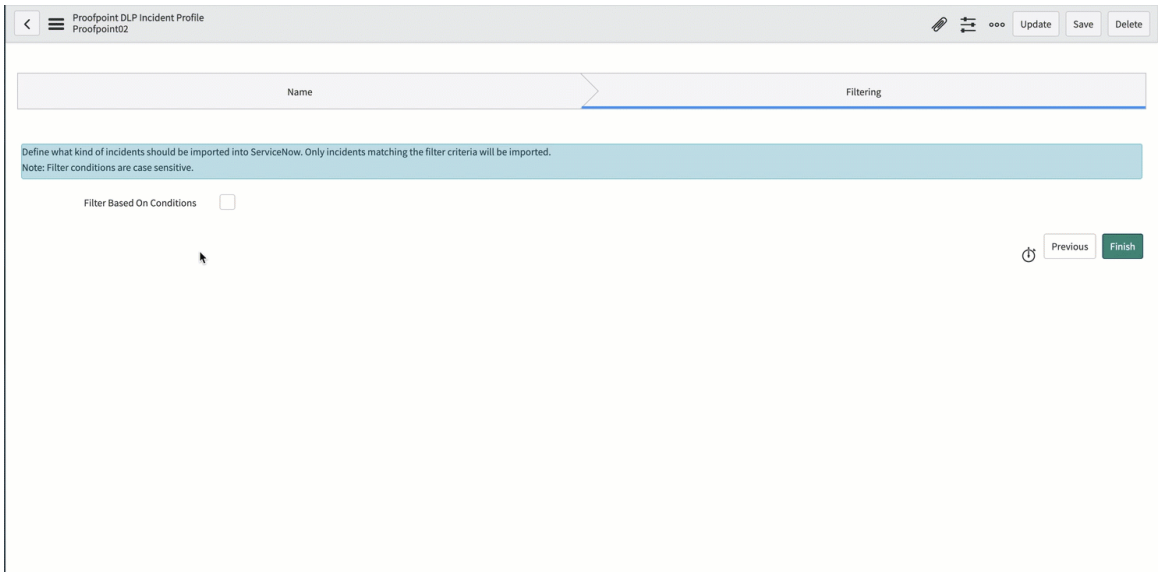
Diese Art der Filterung hilft Ihnen, DLP-Incidents zu isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Incidents erstellt, die den Bedingungen entsprechen.

Prozedur

1. Wählen Sie die Option **Basierend auf Bedingungen filtern** aus, und definieren Sie die Kriterien, die ein eingehender Proofpoint DLP-Incident erfüllen muss, damit ein Security Incident erstellt wird.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter im Feld **Filterbedingungen** fest.

   Die Optionen im ersten Feld in den **Filterbedingungen** entsprechen den Feldern, die im DLP-Incident verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des incident übereinstimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf **AND**oder **OR**klicken.
   - Wenn **AND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER**ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.
4. Klicken Sie auf **Fertigstellen**.

Konfigurieren Sie den Nachweisdateispeicher

Konfigurieren Sie den Nachweisdateispeicher, um die Nachweisdateien für die Proofpoint-E-Mail-DLP-Incidents sicher in der ServiceNow-Instanz oder extern zu speichern.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können den Nachweisdateispeicher für die sichere Speicherung von Dateien konfigurieren. Dies bietet eine Option für den internen Speicher in einer ServiceNow-Instanz oder einen externen Speicher, um sicherzustellen, dass Dateien mit Verschlüsselung auf Spaltenebenegespeichert und verschlüsselt werden. Weitere Informationen finden Sie in der Dokumentation zu Feldverschlüsselung in Now Platform.

Wenn ein DLP-Analyst die Aktion Nachweisdateien für DLP-Incidents herunterladen aus dem Analystenarbeitsbereich ausführt, wird die Datei aus dem ausgewählten Speicher heruntergeladen, wenn die Option zum Speichern der Nachweisdatei aktiviert ist. Andernfalls wird die Datei direkt aus der Proofpoint-Quelle heruntergeladen und nicht in der ServiceNow-Instanz gespeichert. Weitere Informationen finden Sie unter Laden Sie die Nachweisdateien für DLP-Incidents auf Proofpoint herunter.

Prozedur

1. Wählen Sie im Formular „Incident-Profil“ den Abschnitt **„Nachweisspeicher“**.
2. Aktivieren Sie das Kontrollkästchen **Nachweisdateispeicher,** um den Dateispeicher zu aktivieren.
3. Wählen Sie den bevorzugten Speichertyp aus.

Interner Speicher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Externer Speicher

4. Klicken Sie auf **Fertigstellen**.

Ergebnisse

Wenn die Option **Nachweisdateispeicher** aktiviert und ServiceNow-Speicher ausgewählt ist, werden die Nachweisdateien intern in einem verschlüsselten Format gespeichert, nachdem die Incidents von Proofpoint abgerufen wurden. Wenn Sie für einen dieser Proofpoint-Incidents die Aktion **Datei herunterladen** ausführen, wird das System dies tun Nachweisdatei aus dieser Tabelle abrufen.

Laden Sie die Nachweisdateien für DLP-Incidents auf Proofpoint herunter

Laden Sie DLP-Incident-Beweisdateien herunter, die gegen die DLP-Richtlinie verstoßen, auf Proofpoint.

Vorbereitungen

Laden Sie diese Datei aus dem DLP-IR-Arbeitsbereich für Analysten und dem DLP-IR-Endanwender-Arbeitsbereich auf Ihren lokalen Computer herunter.

Hinweis:
Die Aktion**„Datei herunterladen“** ist nur für die Genehmiger verfügbar, die über die Rolle für den sicheren Dateizugriff (gilt nur für ServiceNow-Speichertyp; für externen Speicher ist keine Rolle erforderlich) im DLP-IR-Endanwender-Arbeitsbereich verfügen.

Stellen Sie sicher, dass die Eigenschaft **Sollte das Herunterladen der Verstoßdatei des gemeldeten Incidents zulässig sein** unter den **Einstellungen** aktiviert ist (oder auf aktiv wahr festgelegt) ist.

Erforderliche Rolle:

- sn_dlir.analyst
- sn_dlir.secure_file_download

Hinweis:
Jeder Genehmiger mit dieser Rolle, die nur für den internen Speicher gilt, kann die Datei herunterladen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen Proofpoint-DLP-Incident mit der Scan-Quelle als **E-Mail SMTP**.
3. Klicken Sie auf **Datei herunterladen**.

Führen Sie die folgenden Schritte aus, damit der Genehmiger die Aktion Datei herunterladen anzeigen kann:

4. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Anwenderarbeitsbereich**.
   Die Seite „Meine DLP-Incidents“ wird auf einer neuen Registerkarte angezeigt.
5. Wählen Sie das Modul **Meine Genehmigungen** aus, das unter dem Modul Meine DLP-Incidents verfügbar ist.
   Die Listenansicht „Meine Genehmigungen“ wird angezeigt.
6. Öffnen Sie einen Genehmigungsanforderungsdatensatz, der für den Proofpoint-DLP-Incident ausgelöst wird, mit „Quell-E-Mail-SMTP scannen“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf das Informationssymbol (i), das im Feld „DLP-Incident“ in der Formularansicht verfügbar ist.
8. Klicken Sie auf **Datei herunterladen**.

Ergebnisse

Nach Ausführung dieser Aktion wird die Datei, die die DLP-Richtlinie verletzt hat, auf den lokalen Computer des Anwenders heruntergeladen.

Hinweis:

DLP-Administratoren können auch den Zugriff auf die Aktion **Datei herunterladen** deaktivieren, indem sie auf der Seite „Erweiterte Einstellungen“ die Einstellung **Sollte das Herunterladen der Datei mit der Verletzung des gemeldeten Incidents zulässig sein** deaktivieren. Weitere Informationen finden Sie unter Erweiterte Einstellungen für Data Loss Prevention Incident Response konfigurieren .

Zeigen Sie eine Vorschau der Nachweisdatei an

Zeigen Sie eine Vorschau der DLP-Incident-Beweisdateien im DLP-IR-Analystenarbeitsbereich an.

Vorbereitungen

- Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**.
- Stellen Sie sicher, dass die Eigenschaft **sn_pp_dlp.enable_evidence_file_preview** bereits aktiviert ist.

Wichtig:

Bei Verwendung der Aktion „Nachweisdateien“ im DLP-Analystenarbeitsbereich werden die Nachweisdateien für die Dauer, die Sie mit der Eigenschaft **„sn_dlir.preview_temp_files_cleanup_interval“** auf der Seite **„Erweiterte Einstellungen“** ausgewählt haben, in einem unverschlüsselten Format vorübergehend in der ServiceNow-Datenbank gespeichert. Sie können die Vorschaufunktion **für Nachweisdateien** deaktivieren, wenn Sie keine Daten in der ServiceNow-Datenbank speichern möchten. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.analyst

Prozedur

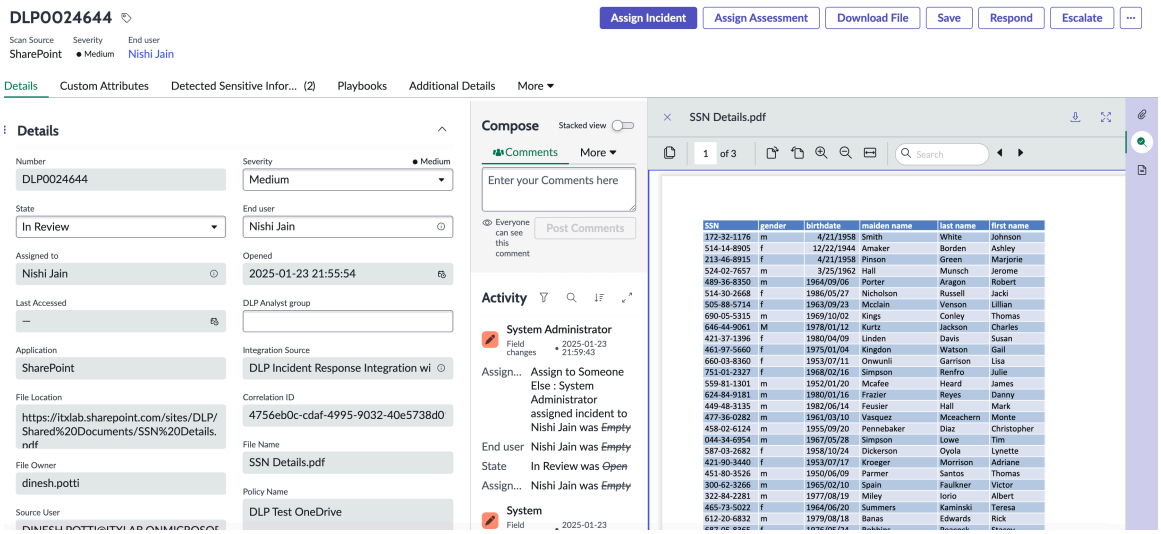
1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie das Symbol **Nachweisdateien**, das im Kontextmenü verfügbar ist.
   Eine Registerkarte wird geöffnet, auf der alle Nachweisdateien abgerufen werden. Sobald der Download abgeschlossen ist, können Sie alle Nachweisdateien auf der Registerkarte **Nachweisdateien** anzeigen.
4. Wählen Sie die **Nachweisdateikarte** aus, die Sie in der Vorschau anzeigen möchten.
   Die Vorschaufunktion ist für jeden Dateityp unterschiedlich.
5. Zeigen Sie eine Vorschau von PDF- und Office-Dokumenten im Dokument-Viewer an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen, um die PDF-Datei im Vollbildmodus zu öffnen. Zu den Office-Erweiterungen, für die der Dokument-Viewer die Nachweisdateien öffnet, gehören: doc, docx, ppt, pptx, xls, xlsx.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Suchen Sie die Suchleiste, und geben Sie das gesuchte Stichwort ein.

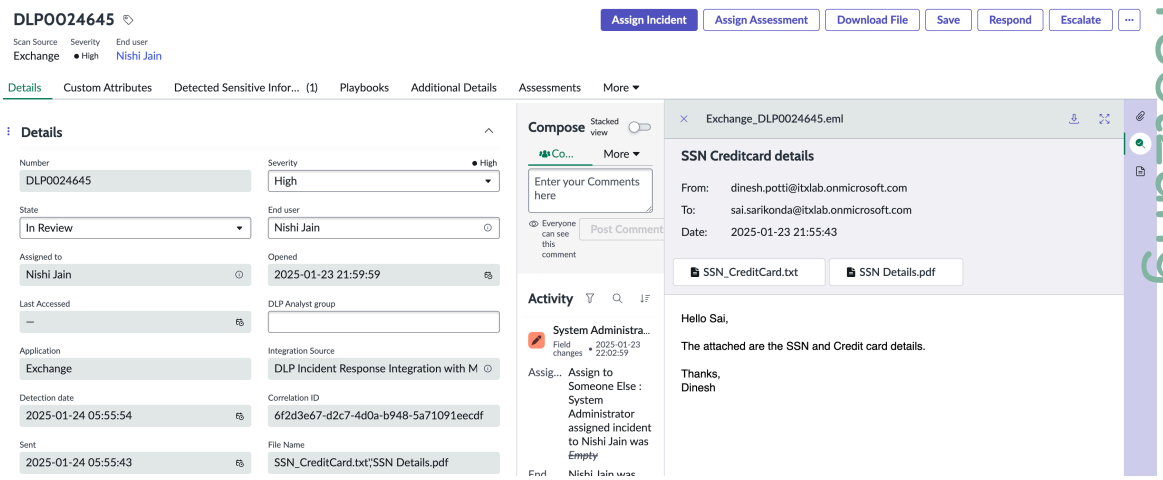
b. Verwenden Sie die Funktionen zum Vergrößern und Verkleinern, um die Ansicht für eine bessere Lesbarkeit anzupassen.

c. Rotieren Sie die Seite im oder gegen den Uhrzeigersinn, um den Inhalt deutlicher anzuzeigen.
Diese Steuerungsoptionen verbessern Ihre Fähigkeit, die Nachweisdatei umfassend zu verstehen. Nur die PDF-Datei hat Steuerungsoptionen im Header.



6. Zeigen Sie eine Vorschau der EML-Dateien an.
Wählen Sie die Anhänge in der E-Mail aus, und zeigen Sie eine Vorschau an.

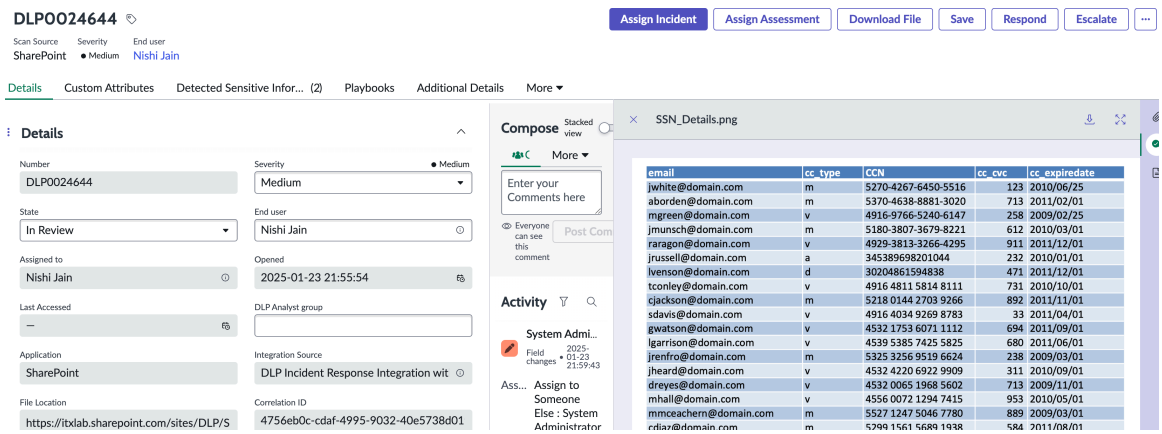
Hinweis:
Wenn die ausgewählte Nachweisdatei die Grenze von 5 MB überschreitet, kann sie im Analystenarbeitsbereich nicht in der Vorschau angezeigt werden. Sie müssen die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen. Diese Beschränkung gilt nur für EML-Dateien.



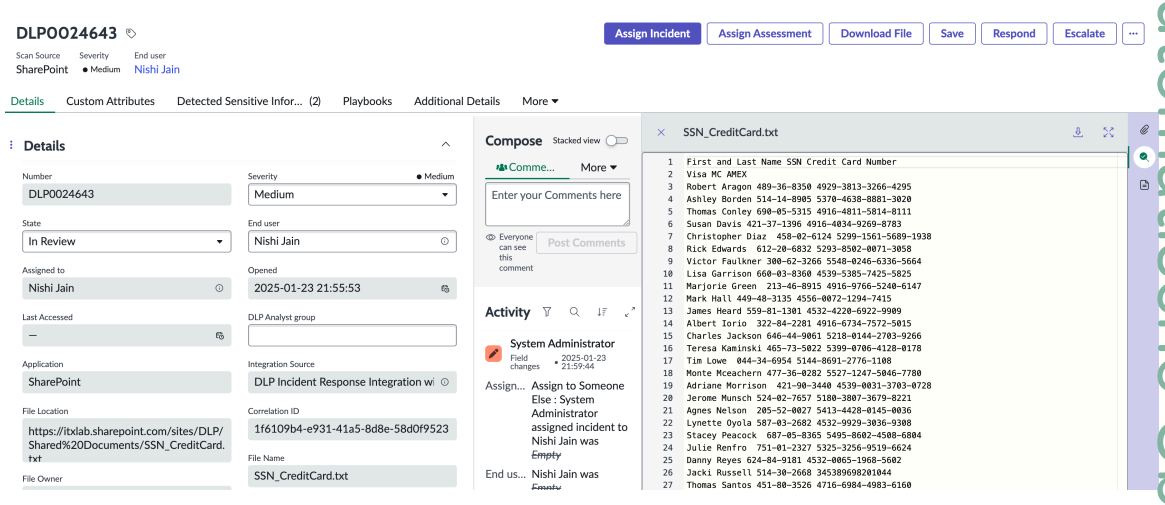
7. Zeigen Sie eine Vorschau der Bilder im DLP-Analystenarbeitsbereich an.
Es werden nur Bilder mit den Erweiterungen .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg und .webp unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Zeigen Sie eine Vorschau von Textdateien im Texteditor an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen.



Hinweis:
Andere Nachweisdateien als Office-Dokumente, EML-Dateien, Text- und Bilderweiterungen werden für die Vorschau nicht unterstützt. Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion zur Vorschau der Nachweisdatei funktioniert auch für archivierte Incidents.

E-Mail-Korrekturaktionen

Führen Sie die Korrekturaktion für die für Proofpoint unter Quarantäne gestellte E-Mail durch.

Vorbereitungen
Proofpoint bietet vier Korrekturaktionen:

1. Release-E-Mail mit Scan
2. Geben Sie E-Mail ohne Scan frei
3. Geben Sie die verschlüsselte E-Mail mit Scan frei
4. E-Mail löschen

Standardmäßig **wählen Sie E-Mail mit Scan freigeben**, **E-Mail ohne Scan freigeben, Verschlüsselte E-Mail mit Scan freigeben**und **E-Mail löschen** sowie **die Korrekturaktionsregel für Proofpoint**, um die Korrekturaktion für die E-Mail auszuführen. Mit diesen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortoptionen ist auch die **Proofpoint-Genehmigungsregel für E-Mail-Release** konfiguriert, um die Genehmigungsfunktion für diese Aktionen zu nutzen. Diese Korrekturaktionen stehen Endanwendern, Analysten und Prüfern von eskalierten Incidents zur Ausführung zur Verfügung.

Weitere Informationen finden Sie unter Optionsregeln für die Reaktion auf Incidents für Ihre DLP-Incidents einrichten , Antwortoption für Ihre DLP-Incidents konfigurieren und Genehmigungsregeln konfigurieren .

Erforderliche Rolle:

- sn_dlir.admin
- sn_dlir.analyst

Proofpoint-Quarantänefreigabe-Antwortoptionsregel

Zuordnungen der Antwortoption für die Proofpoint-Quarantänefreigabe

Prozedur

Im folgenden Verfahren wird erläutert, wie Sie die Korrekturaktion aus dem DLP-Arbeitsbereich für Analysten übermitteln. Als DLP-Administrator und DLP-Analyst können Sie:

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen beliebigen Proofpoint-DLP-Incident mit **Scanquelle** als E-Mail SMTP.
3. Klicken Sie **auf Antworten**.
4. Wählen Sie die Antwortoption in der Dropdown-Liste **Antwort** aus.
5. Klicken Sie auf **Absenden**.

Im folgenden Verfahren wird erläutert, wie Sie die Korrekturaktion aus dem DLP-Anwenderarbeitsbereich übermitteln. Als Endanwender können Sie:

6. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
7. Öffnen Sie einen beliebigen Proofpoint-DLP-Incident mit **Scanquelle** als E-Mail SMTP.
8. Klicken Sie **auf Antworten**.
9. Wählen Sie die Antwortoption in der Dropdown-Liste **Antwort** aus.
10. Klicken Sie auf **Absenden**.

Hinweis:

- Wenn eine Genehmigungsregel für diese Aktion konfiguriert ist, wird zuerst der Genehmigungs-Flow ausgelöst. Nach Erhalt aller Genehmigungen wird der E-Mail-Korrektur-Flow ausgelöst und anschließend die Aktion ausgeführt.
- Wenn **„E-Mail löschen“** ausgeführt wird, wird der Status des DLP-Incident in **„Datei löschen“**aktualisiert. Bei jeder anderen Antwortoption wird der Status des DLP-Incidents in **Freigegebene E-Mail aus Quarantäne** aktualisiert, nachdem die E-Mail erfolgreich freigegeben wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie den DLP-Incident-Status ServiceNow dem Incident-Status [] Proofpoint zu

Synchronisieren Sie den Status der in Ihrer Instanz ServiceNow von erfassten DLP-Incidents und der DLP-Incidents von Proofpoint. Ordnen Sie den Incident-Status ServiceNow dem Incident-Status Proofpoint zu.

Vorbereitungen

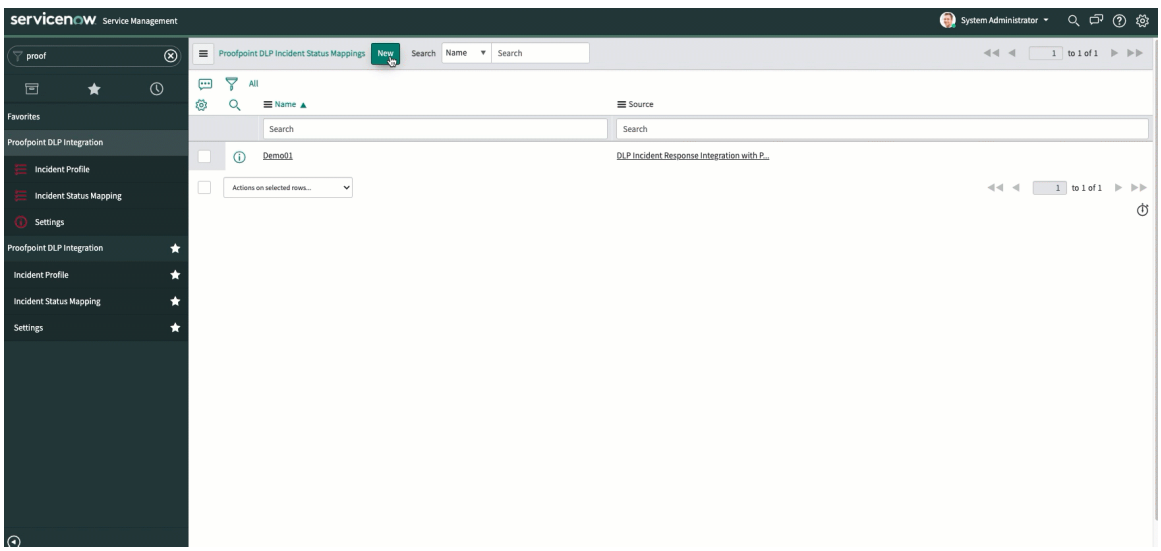
Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Navigieren zu **Proofpoint-DLP-Integration** > **Incident** > **Incident-Statuszuordnung**.
2. Geben Sie einen **Namen** an, um die Zuordnung zu identifizieren.
3. Wählen Sie die Kachel **Quelle** (Integrationskonfiguration), für die die Statuszuordnung angewendet werden soll.
4. Ordnen Sie den **ServiceNow-DLP-Incident-Status** dem **Proofpoint-Incident-Status**zu.

Ordnen Sie den Status von Proofpoint-DLP-Incidents dem ServiceNow-Formular „Incident-Status“ zu

Feld	Beschreibung
Name	Platzhalter für den Zuordnungsdatensatz.
Quelle	Konfigurierte Proofpoint – Endpunktquelle, von der Sie den Incident-Status abrufen möchten.
Status des ServiceNow-Incidents	Statusliste von DLP-Incidents.
Status des Proofpoint-Incidents	Standardmäßig zugeordnete Werte für Standardstatus, die in DLP-Incidents verfügbar sind. Für anwenderdefinierte Status lautet der Standardstatus Proofpoint**Neu**. Sie können den erforderlichen Status Proofpoint im Eingabefeld ändern und hinzufügen.



5. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Ein Datensatz für die Zuordnung wurde erfolgreich erstellt. Die Status der ServiceNow Incidents werden mit Proofpoint den DLP-Incidents synchronisiert.

Wenn Sie den Status eines DLP-Incidents in Ihrer Instanz ServiceNow ändern, wird der Status des zugehörigen DLP-Incidents Proofpoint auf der Quellplattform Proofpoint gemäß der im Datensatz festgelegten Zuordnung geändert.

Konfigurieren Sie die DLP-Integrationseinstellungen für Proofpoint .

Ändern Sie die Standardsystemeigenschaften für Proofpoint DLP-Integration.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Prozedur
1. Navigieren zu **Proofpoint-DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.
3. Klicken Sie auf **Speichern**.

Ergebnisse
Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Domain Separation in DLP-Integration Proofpoint .

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe

Support: Standard.

So funktioniert Domain Separation mit der DLP-Integration Proofpoint .

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die Proofpoint DLP-Integrationsvorgänge in der entsprechenden Domäne aus.

Integration von Data Loss Prevention Incident Response mit Netskope

Die Netskope DLP-Integration unterstützt die Erfassung von Incidents zur Verhinderung von Datenverlust, die in der Bereitstellung von Netskope Verhinderung von Datenverlust erstellt wurden. Netskope DLP hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Nach der Erfassung können Sie die Incident-Management-Funktionen verwenden, um die DLP-Incidents zu korrigieren.

Schlüsselfunktionen

Diese Integration umfasst die folgenden Schlüsselfunktionen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellung mehrerer Profile für verschiedene Netskope -Mandanten.
- Automatisierung der Erstellung von ServiceNow-DLP-Incidents aus Netskope DLP-Incidents.
- Filterung von Netskope DLP-Incidents.
- Geplante Erfassung von Netskope DLP-Incidents, die DLP-Incidents in ServiceNow erstellen.
- Aktualisieren Sie den Objektstatus auf Netskope automatisch, wenn sich der DLP-Status in Ihrer ServiceNow-Instanz ändert.
- Zeigen Sie die forensischen Details (verstoßender Inhalt) des DLP-Incident im DLP IR-Arbeitsbereich für Analysten und im DLP-Endanwender-Arbeitsbereich an.

Hinweis:
Der verstoßende Inhalt wird in ServiceNow nicht beibehalten. Der Inhalt wird abgerufen, wenn der Incident im -Arbeitsbereich geöffnet wird.

- Nachweisdatei wird bei Bedarf direkt von Netskope heruntergeladen.

Hinweis:
Die Nachweisdatei wird in ServiceNow nicht beibehalten. Die Nachweisdatei wird abgerufen, wenn der Analyst im Arbeitsbereich auf **Datei herunterladen** klickt.

- Benachrichtigung per E-Mail an DLP-Administratoranwender bei Ablauf des Tokens Netskope.
- Eine Benachrichtigung per E-Mail wird an DLP-Administratoranwender gesendet, wenn das definierte Wiederholungslimit für Fehler bei Incident-API-Aufrufen überschritten wird.
- Netskope unterstützt auch den Integrationsausführungsprozess. Weitere Informationen finden Sie unter Überwachen Sie den DLP-Integrationsausführungsprozess.

Erste Schritte mit der Netskope DLP-Integration für Data Loss Prevention

Lesen Sie sich die folgenden Informationen durch, bevor Sie mit der Einrichtung Ihrer Netskope DLP-Integration für Data Loss Prevention beginnen.

Setup-Aufgabe	Beschreibung
Vergewissern Sie sich, dass Sie die erforderliche Now Platform Anwendung zur Verhinderung von Datenverlust zugewiesen haben.	Die folgenden Rollen werden in der DLP-Integration Netskope in Now Platformverwendet: • Der Administrator (admin) installiert die Anwendungen aus ServiceNow Store und weist den Administrator für die Verhinderung von Datenverlust (sn_dlir.admin) zu. • Benutzer mit der Rolle sn_dlir.admin können die Integration konfigurieren und die Incident-Profile einrichten. • Anwender mit der Rolle sn_dlir.analyst verfügen über Leserollen in der gesamten Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setup-Aufgabe	Beschreibung
Weisen Sie die erforderlichen Berechtigungen für das API v2-Token Netskope zu.	Die folgenden Endpunktberechtigungen werden für die gesamte Tokenisierung der Netskope API v2 verwendet. • Lesen Sie: /api/v2/incidents/dlpincidents • Lesen Sie: /api/v2/events/dataexport/events/incident • Lesen + Schreiben: /api/v2/incidents/update
Stellen Sie sicher, dass die zur Unterstützung der Netskope DLP-Integration erforderliche Endanwender-Core-Anwendung installiert und aktiviert ist.	Stellen Sie sicher, dass die folgenden DLP-Anwendungen und allgemeinen Anwendungen zur Unterstützung der Sicherheit im ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie die Netskope DLP-Integration für die Verhinderung von Datenverlust

Installieren und konfigurieren Sie die Netskope DLP-Integration über die Instanz ServiceNow StoreNow Platform. Sie können die Untersuchung von DLP-Incidents mit den DLP-Incident-Daten Netskope starten.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

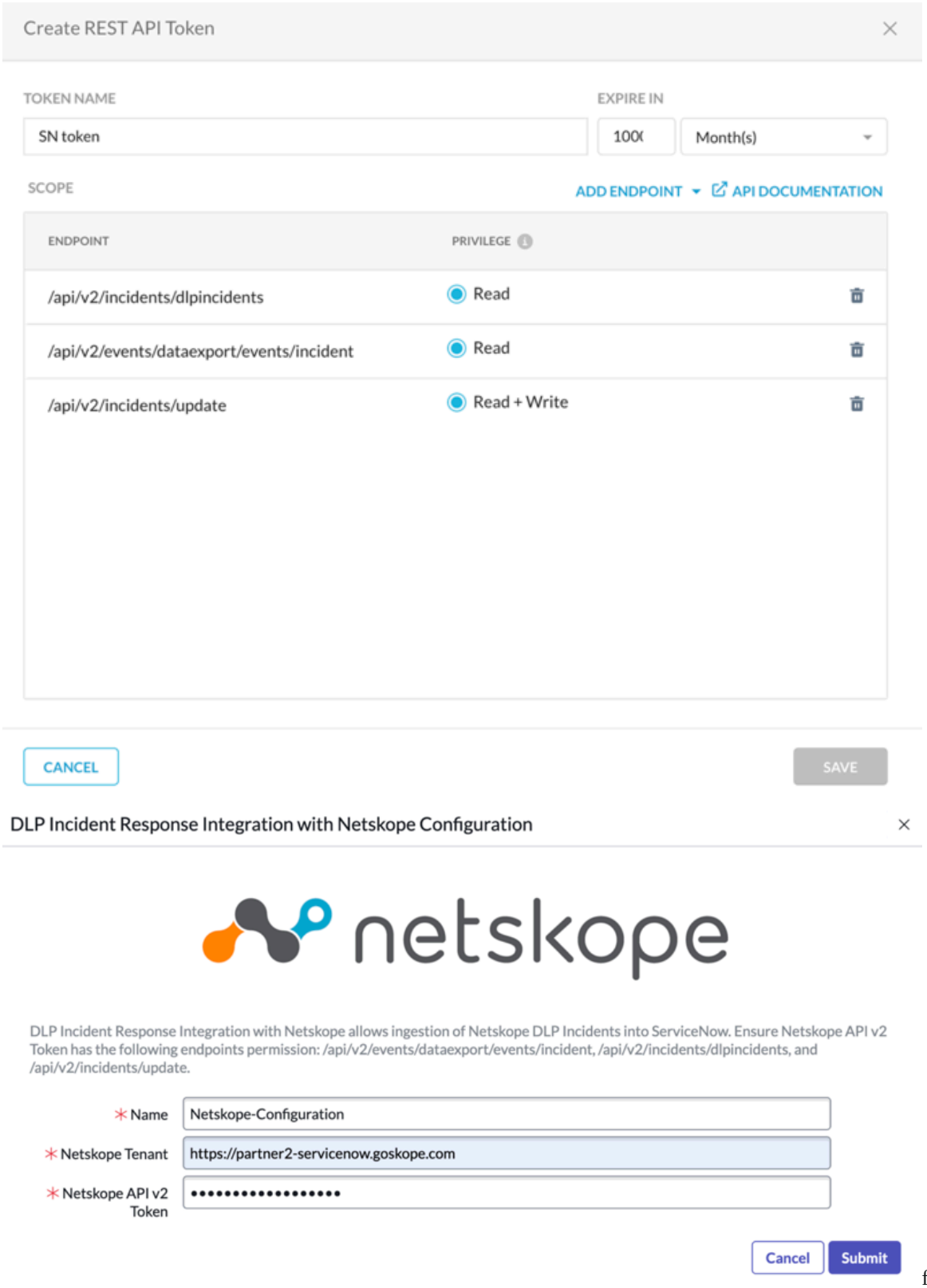
Prozedur

1. Laden Sie die DLP-Integration Netskope von ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**
3. Suchen Sie nach der Kachel „DLP Incident Response Integration with Netskope“, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Stellen Sie sicher, dass Ihr Netskope API v2 Token über die folgenden Endpunktberechtigungen verfügt:

- Lesen Sie: /api/v2/incidents/dlpincidents
- Lesen Sie: /api/v2/events/dataexport/events/incident
- Lesen + Schreiben: /api/v2/incidents/update



für das REST-API-Token

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name der Netskope DLP-Integrationskonfiguration.
Netskope-Mandant	Die Basis-URL Netskope für den Mandanten Netskope.
Netskope-API-v2-Token	Das Token wurde für die REST API v2 in Ihrem -Benutzeraccount unter Netskopekonfiguriert.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Hinweis:
Verbinden Sie die Netskope-Subproduktion mit der ServiceNow-Subproduktion. Synchronisieren Sie alle Anwendernamen und Passwörter über alle Instanzen hinweg, um zu vermeiden, dass Accounts abgemeldet werden.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die DLP-Integration Netskope auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für die DLP-Integration Netskope .

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Now Platform, um die DLP-Incidents vom Endpunkt Netskope abzurufen. Speichern Sie die Incidents in der Instanz ServiceNow als DLP-Incidents.

Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Erstellen Sie ein Profil

Feld	Beschreibung
Name	Name des Profils. De Name muss für jedes Profil eindeutig sein. Anhand dieses Namens können Sie das Profil identifizieren.
Quelle	Netskope DLP-Instanz, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die für das Profil erfasst werden sollen. **Hinweis:** Pro Quelle ist nur ein aktives Profil zulässig.
Aktiv	Indikator, der angibt, dass das Profil aktiv ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Dieses Feld ist erst verfügbar, nachdem Sie im letzten Abschnitt „Zeitplanung“ **auf Fertigstellen** geklickt haben. Wenn das Profil aktiv ist, fragt Ihre Instanz Now Platform aktiv DLP-Incidents von Netskope ab. Entsprechende DLP-Incidents werden als ServiceNow-DLP-Incidents erstellt, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Planungsparametern übereinstimmen.
Bestellung	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge wird als höchste Priorität betrachtet. Der Standardwert ist 100.
Beschreibung	Beschreibung, anhand derer Sie dieses Profil von anderen Profilen unterscheiden können.

4. Klicken Sie auf **Fortsetzen** und wechseln Sie zum Abschnitt Filtern.

Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden sollen

Definieren Sie Filterbedingungen, um die eingehenden Netskope DLP-Incidents zu filtern, und legen Sie sie fest. Steuern Sie, welche dieser Incidents als DLP-Incidents in Ihrer Instanz ServiceNow erstellt werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Art der Filterung hilft Ihnen, DLP-Incidents zu isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Incidents erstellt, die den Bedingungen entsprechen.

Prozedur

1. Wählen Sie die Option **Basierend auf Bedingungen filtern** aus, und definieren Sie die Kriterien, die ein eingehender Netskope-DLP-Incident erfüllen muss, damit ein DLP-Incident erstellt wird.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter im Feld **Filterbedingungen** fest.

   Die Optionen im ersten Feld der **Filterbedingungen** entsprechen den Feldern, die in der **Netskope-DLP-Incident-Importtabelle** verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des incident übereinstimmen.
3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf **AND**oder **OR**klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn **AND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
- Wenn **ODER**ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.

4. Klicken Sie auf **Fortsetzen** und wechseln Sie zum Abschnitt Zeitplanung.

Planen Sie den Abruf von Netskope DLP-Incidents

Legen Sie einen Zeitplan fest, um Netskope DLP-Incidents abzurufen, die den Kriterien im Profil entsprechen.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie nach neuen Netto-Incidents Netskope suchen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann mit dem Kontrollkästchen Einmaliger Abruf so konfiguriert werden **, dass ein einmaliger** Abruf erfolgt. Das Verlaufsdatum kann bis zu einen Monat in der Vergangenheit liegen.

Prozedur

1. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus Netskopeabrufen.
2. Füllen Sie die Felder des Formulars aus.

Planen Sie die Netskope DLP-Incidents

Feld	Beschreibung
Laufende Incident-Erfassung	Fortlaufende Incident-Erfassung, die Ihre Instanz Now Platform für neue Incidents aus Netskope abruft. Wenn ausgelöste Incidents gefunden werden, die den Incident-Filterkriterien entsprechen, werden DLP-Incidents erstellt.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist. Dieser Standardwert ist auf **5**festgelegt.
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Festlegen der ersten Incident-Erfassung basierend auf dem konfigurierten Datum und der konfigurierten Uhrzeit. Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Zeitraum des Abfrageintervalls.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Zeitpunkt der ersten Incident-Erfassung	Zeitpunkt der ersten Erfassung von Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Der Wert ist nur sichtbar, wenn die Option **Zeit für erste Incident-Erfassung festlegen** ausgewählt ist.
Nächste Incident-Erfassungszeit (geschätzt)	Die nächste geschätzte Zeit der Incident-Erfassung.
Einmaliger Abruf	Option zum einmaligen Abrufen historischer Daten. **Hinweis:** Wenn diese Option ausgewählt ist, werden Verlaufsdaten aus Netskope DLP gemäß dem in **Seit Datum**hinzugefügten Datum abgerufen.
Seit Datum	Datum, ab dem Daten von Netskopeabgerufen werden. **Hinweis:** Von Netskopekönnen höchstens die Daten der letzten 30 Tage abgerufen werden.

3. Klicken Sie auf **Fertigstellen**.
4. Speichern Sie im Popup-Fenster die erstellte Profilkonfiguration, indem Sie auf **Fertigstellen**klicken.
5. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Setzen Sie **Aktiv** auf **true**.
   c. Klicken Sie auf **Aktualisieren**.

Ergebnisse
Nach der erfolgreichen Erstellung und Aktivierung des Profils werden Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen. Die Incidents werden der DLP-Incidents-Tabelle hinzugefügt.

Zuordnung des DLP-Incident-Status zu Netskope

Im Abschnitt „Incident-Statuszuordnung“ können Anwender die Zuordnungen zwischen dem DLP-Incident-Status in ServiceNow und Netskope dem Objektstatus angeben.

Vorbereitungen
Die Zuordnung wird verwendet, wenn ein DLP-Incident von Netskope in ServiceNow erfasst wird und Statusänderungen eines DLP-Incidents in ServiceNow zurück mit Netskopesynchronisiert werden.

Synchronisieren Sie den Status der in ServiceNow erfassten DLP-Incidents mit dem DLP-Incident von Netskope. Ordnen Sie das Feld ServiceNow-Incident-Status dem Feld Netskope Objektstatus zu.

Erforderliche Rolle: sn_dlir.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen eine 1:1-Zuordnung des Incident-Status von Netskope und dem ServiceNow-Status erstellen.

Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Zuordnung des Incident-Status**.
2. Geben Sie einen Namen an, um die Zuordnung zu identifizieren.
3. Wählen Sie die Quellintegration aus.
4. Ordnen Sie den DLP-Incident-Status dem Objektstatus Netskope zu (der Status „Duplikat Netskope “ kann ebenfalls zugeordnet werden).
   Die Statussynchronisierung von ServiceNow mit Netskope wird deaktiviert, wenn Sie keinen Zuordnungsdatensatz erstellen.

Wichtig:
Sie müssen alle Netskope -Objektstatus allen ServiceNow-Status zuordnen. Wählen Sie die Quelle aus, um den DLP-Incident-Status wieder mit dem Objekt Netskope zu synchronisieren.

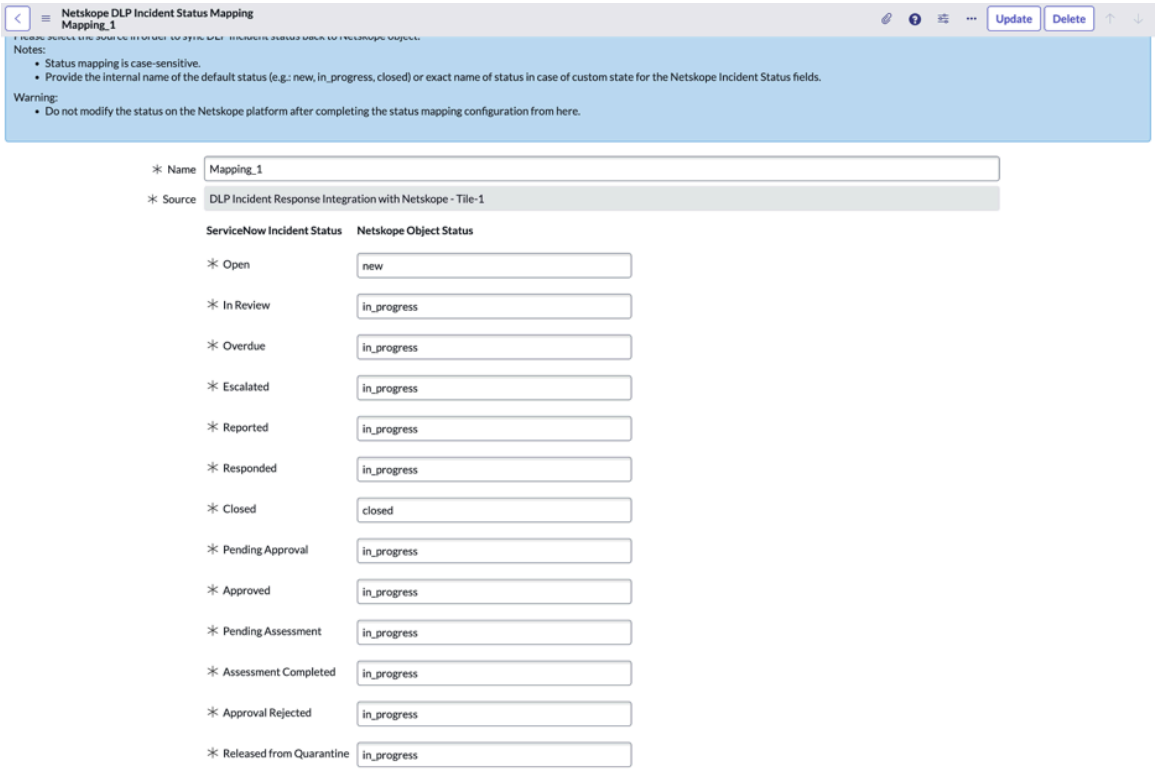
Die folgenden Informations- und Warnmeldungen werden angezeigt, wenn Sie den Incident-Status zuordnen, die Nachrichten überprüfen und fortfahren.

Hinweis:

- Bei der Statuszuordnung wird zwischen Groß- und Kleinschreibung unterschieden.
- Geben Sie den internen Namen des Standardstatus (z. B. new, in_progress, closed) oder den genauen Namen des Status im Falle eines anwenderdefinierten Status für die Felder Netskope „ Objektstatus“ an.

Warnung:
Ändern Sie den Status auf der Plattform Netskope nicht, nachdem Sie die Konfiguration der Statuszuordnung von hier abgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Netskope Zuordnung des DLP-Incident-Status

Feld	Beschreibung
Name	Name des Zuordnungsdatensatzes.
Quelle	Die konfigurierte Netskope -Endpunktquelle, von der Sie den Incident-Status synchronisieren möchten.
DLP-Incident-Status	Gibt die Liste der DLP-Incident-Status an.
Netskope Objektstatus	Gibt die Liste der Netskope -Objektstatus an.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nach der erfolgreichen Erstellung des Datensatzes für die Statuszuordnung wird der Status des ServiceNow-DLP-Incidents bei jeder Aktualisierung automatisch gemäß der Zuordnung auf Seite Netskope angezeigt.

Hinweis:

Wenn Sie den Status eines DLP-Incidents im Mandanten Netskope direkt ändern, funktioniert die Statussynchronisierung von SN mit Netskope unter Berücksichtigung der API-Einschränkungen nicht. Stellen Sie sicher, dass Sie alle DLP-Incident-Status sorgfältig dem Objektstatus Netskope zuordnen.

Konfigurieren Sie die DLP-Integrationseinstellungen für Netskope .

Ändern Sie die Standardsystemeigenschaften für Netskope DLP-Integration.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

Konfigurieren Sie die DLP-Integrationseinstellungen für Netskope .

Feld	Beschreibung
Soll das Herunterladen der Datei mit Verstößen des gemeldeten Incidents zulässig sein? sn_ns_dlp.enable_file_download	Option zum Auswählen, ob Sie den Download der Datei aktivieren möchten. Standardmäßig ist diese Option aktiviert.
Maximale Zeitüberschreitung für HTTP-Aufrufe, in Sekunden sn_ns_dlp.maximum_http_time_out.	Maximale Zeitüberschreitung für HTTP-Aufrufe in Sekunden. Dieses Feld wird automatisch auf 30 festgelegt.
Maximale Anzahl von Wiederholungen, die für API-Fehler durchgeführt werden sollen. sn_ns_dlp.maximum_retry	Maximale Anzahl von Wiederholungen, die für API-Fehler durchgeführt werden sollen. Der Standardwert ist 3.
Ebene der Berichterstellung für die von der Integration „sn_ns_dlp.ging.verbosity“ generierten Protokolle.	Definieren Sie die Ebene der von der Integration generierten Berichterstellungsprotokolle. Dieses Feld wird automatisch auf **„Info“**gesetzt.

3. Klicken Sie auf **Speichern**.

Ergebnisse

Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Zeigen Sie eine Vorschau der Nachweisdateien an

Zeigen Sie eine Vorschau der DLP-Incident-Beweisdateien im DLP-IR-Analystenarbeitsbereich an.

Vorbereitungen

- Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**.
- Stellen Sie sicher, dass die Eigenschaft **sn_ns_dlp.enable_evidence_file_preview** bereits aktiviert ist.

Wichtig:
Bei Verwendung der Aktion „Nachweisdateien“ im DLP-Analystenarbeitsbereich werden die Nachweisdateien für die Dauer, die Sie mit der Eigenschaft **„sn_dlir.preview_temp_files_cleanup_interval“** auf der Seite **„Erweiterte Einstellungen“** ausgewählt haben, in einem unverschlüsselten Format vorübergehend in der ServiceNow-Datenbank gespeichert. Sie können die Vorschaufunktion **für Nachweisdateien** deaktivieren, wenn Sie keine Daten in der ServiceNow-Datenbank speichern möchten. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

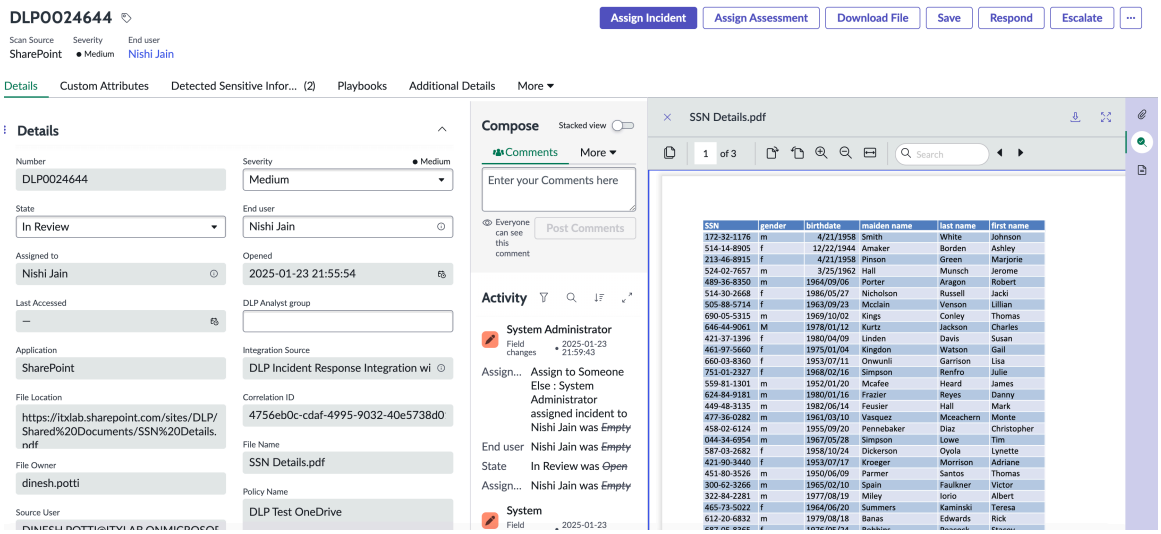
Erforderliche Rolle: sn_dlir.analyst

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen DLP-Incident-Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie das Symbol **Nachweisdateien**, das im Kontextmenü verfügbar ist.
   Eine Registerkarte wird geöffnet, auf der alle Nachweisdateien abgerufen werden. Sobald der Download abgeschlossen ist, können Sie alle Nachweisdateien auf der Registerkarte **Nachweisdateien** anzeigen.
4. Wählen Sie die **Nachweisdateikarte** aus, die Sie in der Vorschau anzeigen möchten.
   Die Vorschaufunktion ist für jeden Dateityp unterschiedlich.
5. Zeigen Sie eine Vorschau von PDF- und Office-Dokumenten im Dokument-Viewer an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen, um die PDF-Datei im Vollbildmodus zu öffnen.
   Zu den Office-Erweiterungen, für die der Dokument-Viewer die Nachweisdateien öffnet, gehören: doc, docx, ppt, pptx, xls, xlsx.
   a. Suchen Sie die Suchleiste, und geben Sie das gesuchte Stichwort ein.
   b. Verwenden Sie die Funktionen zum Vergrößern und Verkleinern, um die Ansicht für eine bessere Lesbarkeit anzupassen.
   c. Rotieren Sie die Seite im oder gegen den Uhrzeigersinn, um den Inhalt deutlicher anzuzeigen.
   Diese Steuerungsoptionen verbessern Ihre Fähigkeit, die Nachweisdatei umfassend zu verstehen. Nur die PDF-Datei hat Steuerungsoptionen im Header.

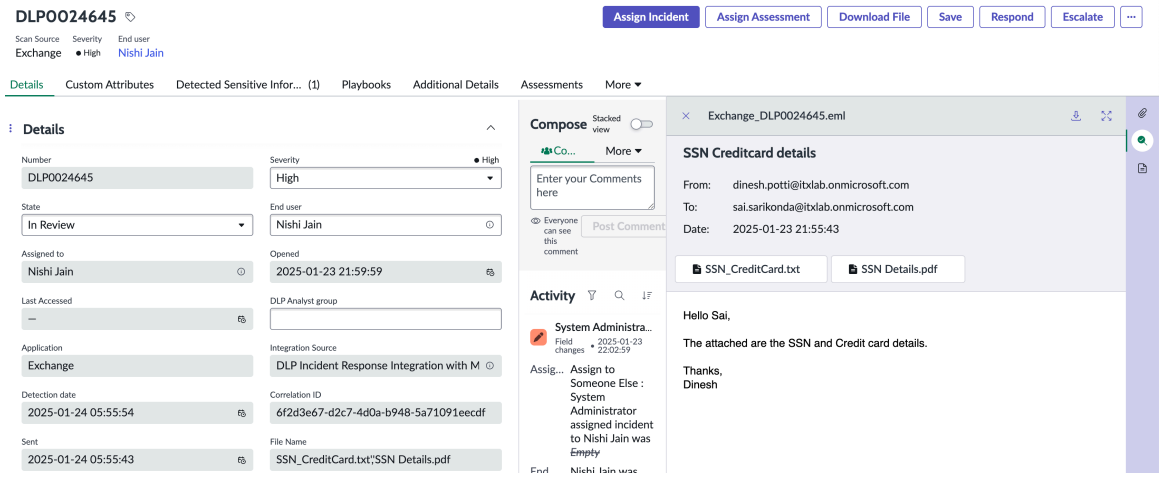


6. Zeigen Sie eine Vorschau der EML-Dateien an.
   Wählen Sie die Anhänge in der E-Mail aus, und zeigen Sie eine Vorschau an.

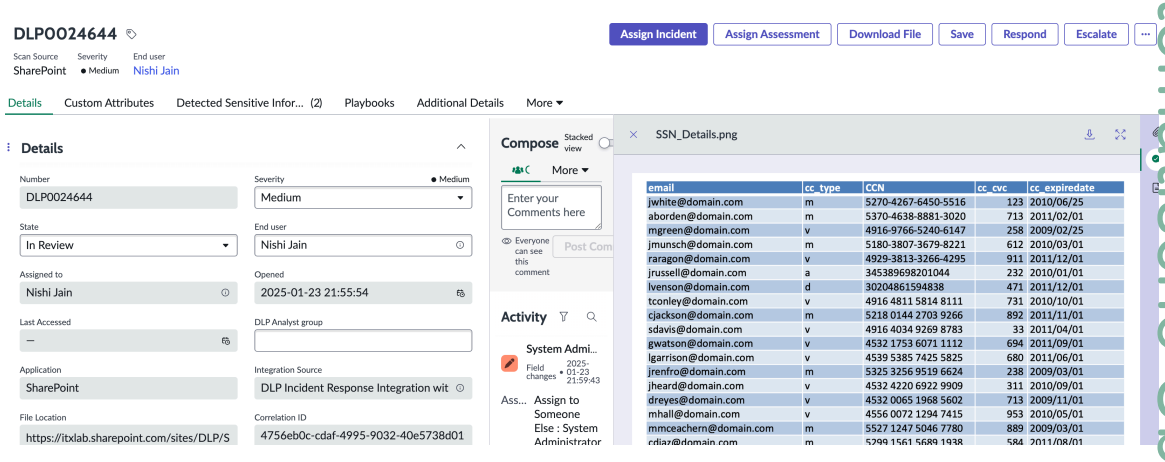
> **Hinweis:**
> Wenn die ausgewählte Nachweisdatei die Grenze von 5 MB überschreitet, kann sie im Analystenarbeitsbereich nicht in der Vorschau angezeigt werden. Sie müssen die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen. Diese Beschränkung gilt nur für EML-Dateien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



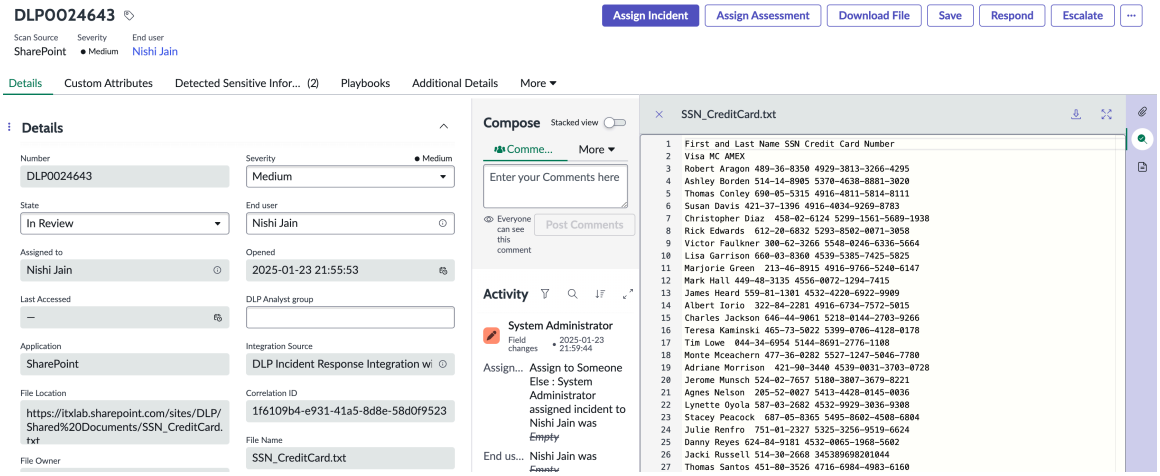
7. Zeigen Sie eine Vorschau der Bilder im DLP-Analystenarbeitsbereich an.
Es werden nur Bilder mit den Erweiterungen .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg und .webp unterstützt.



8. Zeigen Sie eine Vorschau von Textdateien im Texteditor an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Andere Nachweisdateien als Office-Dokumente, EML-Dateien, Text- und Bilderweiterungen werden für die Vorschau nicht unterstützt. Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion zur Vorschau der Nachweisdatei funktioniert auch für archivierte Incidents.

Nachweisdateien herunterladen

Laden Sie Dateien herunter, die gegen die DLP-Richtlinie verstoßen, unter Netskope. Laden Sie diese Datei aus dem DLP-IR-Arbeitsbereich für Analysten und dem DLP-IR-Endanwender-Arbeitsbereich für Genehmiger auf Ihren lokalen Computer herunter.

Vorbereitungen
Erforderliche Rolle:

- sn_dlir.analyst
- sn_dlir.secure_file_download (jeder Genehmiger mit dieser Rolle)

Warum und wann dieser Vorgang ausgeführt wird
Sie müssen den Dateidownload für Netskope aktivieren, bevor Sie fortfahren.

Prozedur

1. Navigieren zu **Alle** > **Netskope-DLP-Integration** > **Einstellungen**.
2. Aktivieren Sie die Eigenschaft **Soll das Herunterladen der Datei mit Verstößen des gemeldeten Incidents zulässig sein**?
   Die Schaltfläche **„Datei herunterladen“** wird im DLP IR-Arbeitsbereich für Analysten und im DLP IR-Endanwender-Arbeitsbereich angezeigt.
3. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
4. Öffnen Sie einen DLP-Incident-Datensatz, der aus der Quelle Netskope erfasst wird.
5. Klicken Sie auf **Datei herunterladen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Datei, die gegen die DLP-Richtlinie auf Netskope verstößt, wird auf den lokalen Computer des Anwenders heruntergeladen.

Hinweis:
DLP-Administratoren können den Zugriff auf die Aktion **Datei herunterladen** für alle Integrationen steuern, indem sie die Option **Sollte das Herunterladen der Datei mit Verstößen des gemeldeten Incidents zulässig sein** auf der Seite **„Erweiterte Einstellungen“** der DLP-Verwaltung deaktivieren. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Benachrichtigungen für Anwender über Wiederholungsmechanismus

Netskope Bei API-Fehlern während der DLP-Incident-Erfassung versucht die -Integration die konfigurierte Anzahl von Wiederholungen.

Sobald das maximale Wiederholungslimit überschritten ist, sendet die Integration Netskope eine E-Mail-Benachrichtigung an Benutzer, die über die Rolle „DLP-Administrator“ (sn_dlir.admin) verfügen.

Nachdem Sie das Setup und die Konfiguration der Integration abgeschlossen haben, stellen Sie die Rolle „DLP-Administrator“ (sn_dlir.admin) den Anwendern bereit, die benachrichtigt werden sollen, wenn das maximale Wiederholungslimit überschritten wird.

Sobald das maximale Wiederholungslimit überschritten ist, überspringt das Profil die Erfassung für bis zu eine Stunde. Die maximalen Wiederholungen werden mit der folgenden Eigenschaft konfiguriert: Maximale Anzahl der Wiederholungen, die für API-Fehler durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren Sie die DLP-Integrationseinstellungen für Netskope ..

E-Mail-Benachrichtigungen bei Ablauf der Anmeldeinformationen

Wenn das in der Instanz ServiceNow verwendete Token abläuft, sendet die Integration Netskope eine E-Mail-Benachrichtigung an Benutzer mit der Rolle „DLP-Administrator“ (sn_dlir.admin).

Nachdem das Setup der Integrationskonfiguration abgeschlossen ist, stellen Sie die Rolle „DLP-Administrator“ (sn_dlir.admin) für die Benutzer bereit, die benachrichtigt werden sollen, wenn das Token abgelaufen ist.

Wenn das Token abläuft, wird die Datenerfassung für zugeordnete Profile angehalten, bis die Netskope-Integrationskonfiguration mit einem gültigen Token aktualisiert wird.

Sie müssen ein Token erstellen oder das alte in Netskopeverlängern und dann das Token in der Instanz ServiceNow aktualisieren. Wenn Sie das Token durch Verlängern der Ablaufzeit verlängern, erkennt die Anwendung Netskope die Verlängerung automatisch und setzt die Datenerfassung fort. Wenn Sie ein Token erstellen, müssen Sie das Token in der Konfiguration aktualisieren.

Domain Separation in DLP-Integration Netskope .

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe

Support: Standard.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So funktioniert Domain Separation mit der DLP-Integration Netskope .

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die Netskope DLP-Integrationsvorgänge in der entsprechenden Domäne aus.

Internet Content Adaption Protocol (ICAP)-Integration für DLP IR

Die DLP-Integration für Internet Content Adaption Protocol (ICAP) unterstützt die Erfassung von Data Loss Prevention Incident Response -Warnungen und ermöglicht das Abrufen von Übereinstimmungsinhalten und Nachweisdateien aus Amazon S3, die in der von ICAP unterstützten Data Loss Prevention Incident Response -Bereitstellung erstellt wurden.

Nachdem die Warnungen erfasst wurden, können Sie den DLP-Arbeitsbereich verwenden, um die erforderlichen wichtigen Informationen anzuzeigen, z. B. Übereinstimmungsinhalt, Warnungsschweregrad und verschiedene Incident-Management-Funktionen, um die DLP-Incidents zu korrigieren.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht und wichtige Funktionen von

Mit der Internet Content Adaption Protocol (ICAP)-Integration können Sie die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachverfolgen.

Diese Integration umfasst die folgenden Schlüsselfunktionen:

- Erfassung von DLP-Warnungen: Anwender können die Erfassung von DLP-Warnungen aus angegebenen Amazon S3-Buckets konfigurieren und planen. Dies umfasst die Möglichkeit zur Durchführung von Delta-Importen, um sicherzustellen, dass nur neue Daten erfasst werden.
- Erfasste Warnungen im DLP-Arbeitsbereich anzeigen: Sobald die Warnungen erfasst wurden, sollten sie im DLP-Arbeitsbereich angezeigt werden und wichtige Details zu jeder Warnung enthalten, z. B. Übereinstimmungsinhalt, Warnungsschweregrad und relevante Metadaten.
- Inhalt abgleichen: Während der Erfassung werden Datensätze mit sensiblen Informationen erstellt. Der Inhalt wird abgerufen, wenn der Datensatz geöffnet wird.
- Download der Nachweisdatei: Das System ermöglicht es Anwendern, zugehörige Nachweisdateien direkt aus dem DLP-Arbeitsbereich für weitere Untersuchungen oder Überprüfungen herunterzuladen.
- Möglichkeit, die Schweregradzuordnung zwischen ICAP-DLP-Incidents und ServiceNow-Incidents anzupassen und zu definieren.

Erste Schritte mit der ICAP-DLP-Integration für Data Loss Prevention

Bevor Sie die Integration verwenden können, müssen Sie sie aus dem herunterladen ServiceNow® Store

Prüfliste

Lesen Sie sich die folgenden Informationen durch, bevor Sie mit der Einrichtung der ICAP-DLP-Integration Ihres Anbieters zur Verhinderung von Datenverlust beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Feld	Beschreibung
Stellen Sie sicher, dass Ihnen die erforderlichen Anwendungsrollen Now Platform, Anwendung zur Vermeidung von Datenverlust zugewiesen sind.	Die folgenden Rollen werden in der ICAP-DLP-Integration auf Now Platformverwendet: • Der Administrator (admin) installiert die Anwendungen aus ServiceNow® Store und weist den Administrator für die Verhinderung von Datenverlust (sn_dlir.admin) zu. • Benutzer mit der Rolle sn_dlir.admin können die Integration konfigurieren und die Incident-Profile einrichten. • Anwender mit der Rolle sn_dlir.analyst verfügen über Leserollen in allen Integrationskonfigurationen.
Stellen Sie sicher, dass Sie die erforderlichen Amazon S3-Bucket-Richtlinien zugewiesen haben.	Die offizielle AWS-Dokumentation zum Erstellen und Verwalten von IAM-Anwendern, -Richtlinien und -Berechtigungen finden Sie unter den folgenden Links: • Erstellen eines IAM-Benutzers • Erstellen von IAM-Richtlinien • Amazon S3-Berechtigungen **Hinweis:** Über die obigen Links erfahren Sie mehr über die detaillierten Anweisungen und weiteren Optionen für die Verwaltung von IAM-Anwendern und S3-Berechtigungen in AWS. Außerdem erfahren Sie, wie Sie einen IAM-Anwender in Ihrem AWS-Konto erstellen – AWS Identity and Access Management und erhalten eine grundlegende Übersicht über den Prozess zum Erstellen eines IAM-Anwenders und von Anmeldeinformationen in AWS Identity and Access Management.
Stellen Sie sicher, dass die Kernanwendung ServiceNow®, die zur Unterstützung der ICAP-DLP-Integration erforderlich ist, installiert und aktiviert ist.	Stellen Sie sicher, dass die folgenden DLP-Anwendungen und allgemeinen Anwendungen zur Unterstützung der Sicherheit im ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Feld	Beschreibung
	• Security Support Common • Komponenten des gemeinsamen Arbeitsbereichs für die Verwaltung von Sicherheitsfällen. • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie die ICAP-DLP-Integration

Installieren und konfigurieren Sie die Provider-ICAP-DLP-Integration aus ServiceNow® Store in Ihrer Instanz Now Platform. Beginnen Sie mit der Untersuchung von DLP-Incidents anhand der ICAP-DLP-Incident-Daten des Anbieters.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

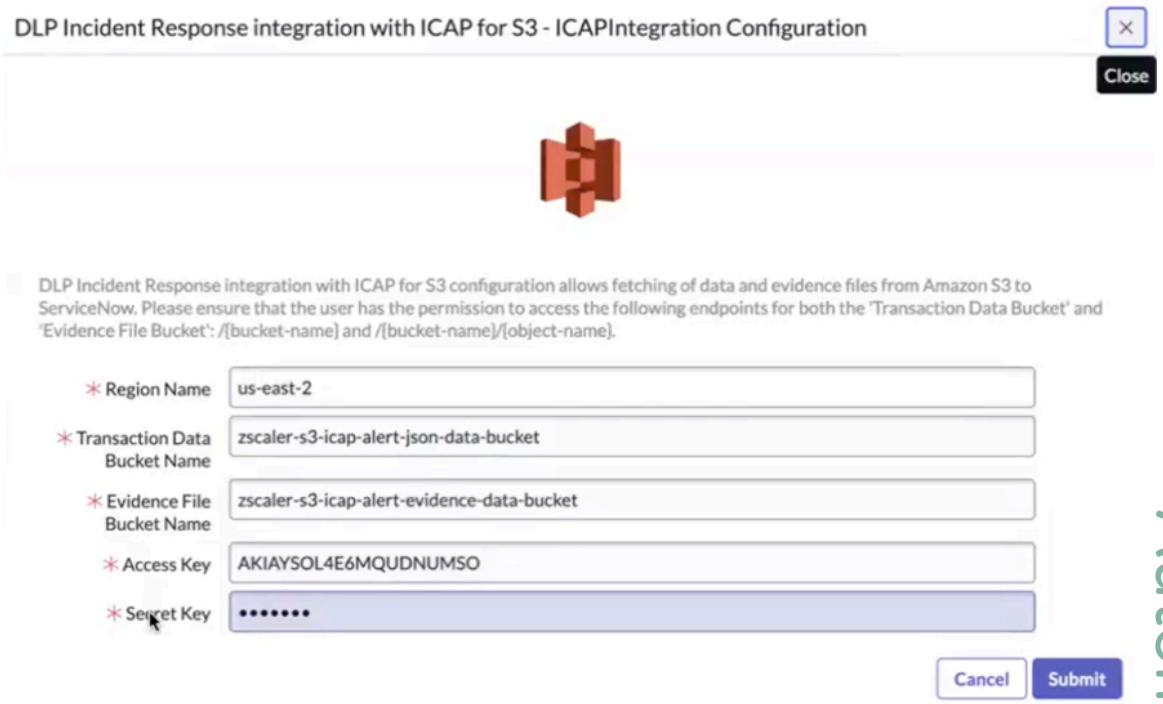
Prozedur

1. Laden Sie die Provider-ICAP-DLP-Integration von ServiceNow® Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel Integration von DLP Incident Response mit ICAP, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

Formular „ICAP-DLP-Integrationskonfiguration“.

Feld	Beschreibung
Regionsname	Regionsname des Amazon S3-Bucket-Namens.
Name des Transaktionsdaten-Buckets	Der Name des Transaktionsdaten-Buckets ist der Bucket, in dem eine DLP-Verstoßtransaktion aufgetreten ist.
Name des Nachweisdatei-Buckets	Der Name des Nachweisdatei-Buckets ist der Bucket, in dem Sie die DLP-Datei finden, die den Verstoß verursacht hat.
Zugriffsschlüssel	AWS IAM-Zugriffsschlüssel für die ICAP-Konfiguration.
Geheimer Schlüssel	Geheimer AWS IAM-Schlüssel für die ICAP-Konfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.

Ergebnisse

Hinweis:
Verbinden Sie die ICAP-Sub-Prod mit der ServiceNow-Sub-Prod. Synchronisieren Sie alle Anwendernamen und Passwörter über alle Instanzen hinweg, um zu vermeiden, dass Accounts abgemeldet werden.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, werden die Konfigurationen der ICAP-DLP-Integration gespeichert.

Erstellen Sie ein Profil für die ICAP-DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrer Now Platform-Instanz. Bestimmen Sie die ICAP-DLP-Warnungen, die zum Erstellen von DLP-Incidents geeignet sind.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Now Platform, um die DLP-Warnungen aus der Amazon S3-Konfiguration abzurufen. Speichern Sie diese Warnungen als DLP-Incidents in Ihrer ServiceNow-Instanz.

Prozedur

1. Navigieren zu **Alle** > **ICAP-DLP-Integration** > **Incident-Profil**.

2. Klicken Sie auf **Neu**.

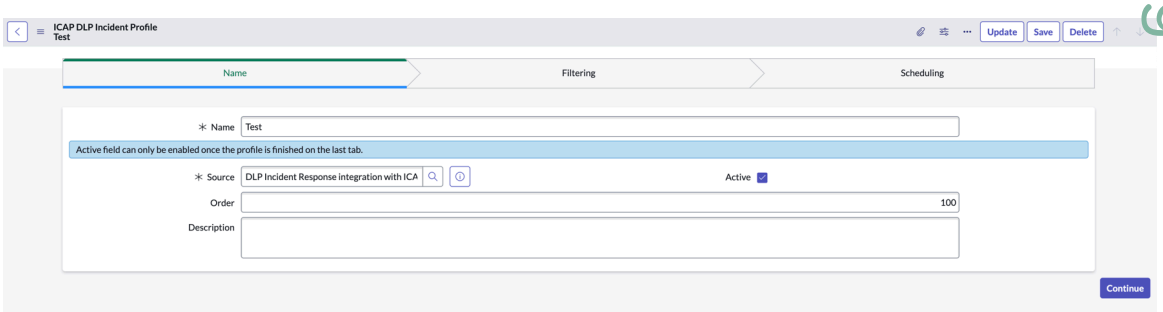
3. Füllen Sie im Formular die Felder im Abschnitt „Name“ aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Profil

Feld	Beschreibung
Name	Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Amazon S3-Konfiguration, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Quellen konfiguriert haben, wählen Sie die entsprechende Quelle für den Incident-Typ aus, den Sie für das Profil erfassen möchten. **Hinweis:** Für das aktive Profil ist nur eine einzige Quelle zulässig.
Aktiv	Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann erst aktiviert werden, nachdem Sie im Abschnitt „ **Zeitplanung** “ auf „Fertigstellen“ geklickt haben. Wenn das Profil aktiv ist, impliziert dies, dass Now Platform aktiv ICAP-DLP-Warnungen abfragt. Die entsprechenden DLP-Warnungen werden in DLP erstellt, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Planungsparametern übereinstimmen.
Bestellung	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge wird als höchste Priorität betrachtet. Der Standardwert ist 100.
Beschreibung	Beschreibung für dieses Profil.



Nächste Maßnahme

Um zum Abschnitt „Filtern“ zu wechseln, klicken Sie auf **Fortfahren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden

Definieren und legen Sie Filterbedingungen fest, um die eingehenden DLP-Warnungen zu filtern. Legen Sie die Warnungen fest, die in ServiceNow als DLP-Incidents erstellt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

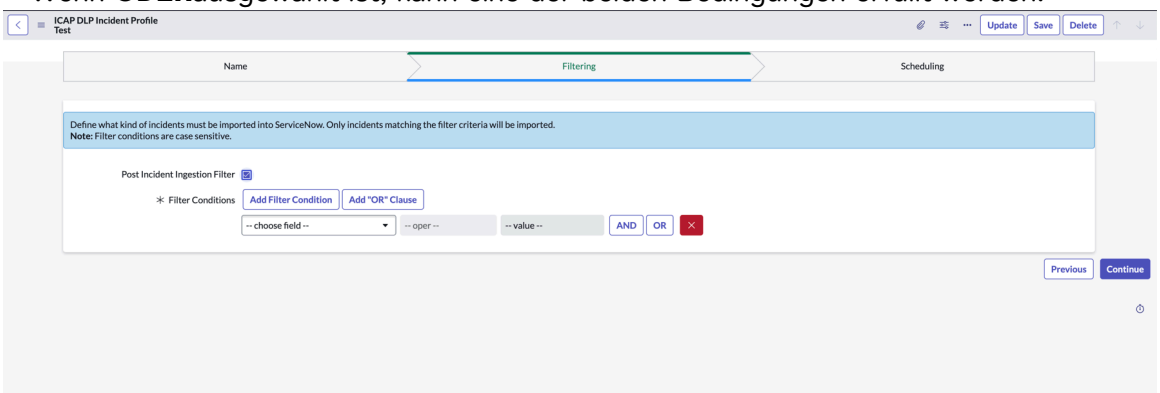
Warum und wann dieser Vorgang ausgeführt wird

Mithilfe von Filtern können Sie DLP-Warnungen isolieren und die Anzahl der von Ihnen erstellten DLP-Warnungen begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Warnungen erstellt, die den Bedingungen entsprechen.

Prozedur

1. Aktivieren Sie das Kontrollkästchen **Filter nach Incident-Erfassung,** um die Filter nach Incident-Erfassung anzuwenden und die Incidents abzurufen, die den Filterkriterien entsprechen.
2. Wählen Sie die Option **Basierend auf Bedingungen filtern** aus, und definieren Sie die Kriterien, die ein eingehender ICAP-DLP-Incident erfüllen muss, damit ein DLP-Incident erstellt wird.
3. Legen Sie die Filter im Feld **Filterbedingungen** fest.

   Die Optionen in der Dropdown-Liste **Filterbedingungen** entsprechen den Feldern, die in der Importtabelle **für ICAP-DLP-Incidents** verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des incident übereinstimmen.
4. Fügen Sie weitere Bedingungen hinzu, indem Sie auf **AND**oder **OR**klicken.
   - Wenn **AND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER**ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.



Nächste Maßnahme

Klicken Sie zum Konfigurieren des Zeitplans **auf Fortfahren**.

Planen Sie den Abruf von ICAP-DLP-Incidents

Legen Sie einen Zeitplan fest, um ICAP-DLP-Warnungen abzurufen, die den Kriterien im Profil entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft Sie nach neuen ICAP-Incidents suchen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann mit dem Kontrollkästchen Einmaliger Abruf so konfiguriert werden **, dass ein einmaliger** Abruf erfolgt.

Prozedur

1. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus ICAP abrufen.
2. Füllen Sie die Felder des Formulars aus.

Planen Sie die ICAP-DLP-Incidents

Feld	Beschreibung
Laufende Incident-Erfassung	Fortlaufende Incident-Erfassung, die Ihre Instanz Now Platform aus ICAP für neue Incidents abruft. Wenn ausgelöste Incidents gefunden werden, die den Incident-Filterkriterien entsprechen, werden DLP-Incidents erstellt.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist. Dieser Standardwert ist auf **5**festgelegt.
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Festlegen der ersten Incident-Erfassung basierend auf dem konfigurierten Datum und der konfigurierten Uhrzeit. Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Zeitraum des Abfrageintervalls.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Zeitpunkt der ersten Incident-Erfassung	Zeitpunkt der ersten Erfassung von Daten. **Hinweis:** Der Wert ist nur sichtbar, wenn die Option **Zeit für erste Incident-Erfassung festlegen** ausgewählt ist.
Nächste Incident-Erfassungszeit (geschätzt)	Die nächste geschätzte Zeit der Incident-Erfassung.
Einmaliger Abruf	Option zum einmaligen Abrufen historischer Daten. **Hinweis:** Wenn diese Option ausgewählt ist, werden Verlaufsdaten gemäß dem in **Seit Datum**hinzugefügten Datum aus ICAP DLP abgerufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ordnername	Name des Ordners, aus dem Sie die Daten abrufen möchten. Alle Ordner, deren Namen lexikografisch größer als der angegebene Ordnername sind, werden im einmaligen Abruf erfasst.

3. Klicken Sie auf **Fertigstellen**.
4. Speichern Sie im Popup-Fenster die erstellte Profilkonfiguration, indem Sie auf **Fertigstellen**klicken.
5. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Setzen Sie **Aktiv** auf **true**.
   c. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Nach der erfolgreichen Erstellung und Aktivierung des Profils werden Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen. Die Warnungen werden der DLP-Incident-Tabelle hinzugefügt.

Zeigen Sie vertrauliche Informationen für DLP-Warnungen an

Zeigen Sie die erkannten vertraulichen Informationen für DLP-Warnungen an.

Vorbereitungen

In der jeweiligen Integration sind bestimmte Regeln und Richtlinien konfiguriert. Wenn Sie jemals gegen die definierten Richtlinien verstoßen, wird ein DLP-Incident erstellt, und im Übereinstimmungsinhalt werden die verletzten Informationen im Abschnitt „Sensible Informationen“ dieses DLP-Incident-Datensatzes angezeigt.

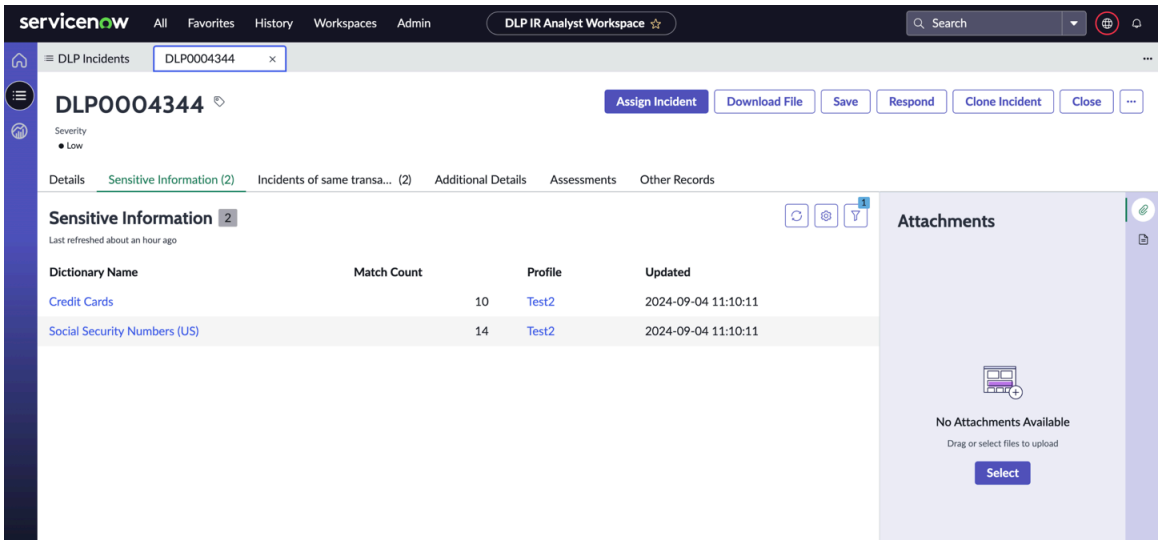
Erforderliche Rolle: sn_dlir.analyst

Hinweis:
Endanwender können die vertraulichen Informationen auch anzeigen, indem sie sich beim DLP-Anwenderarbeitsbereich anmelden.

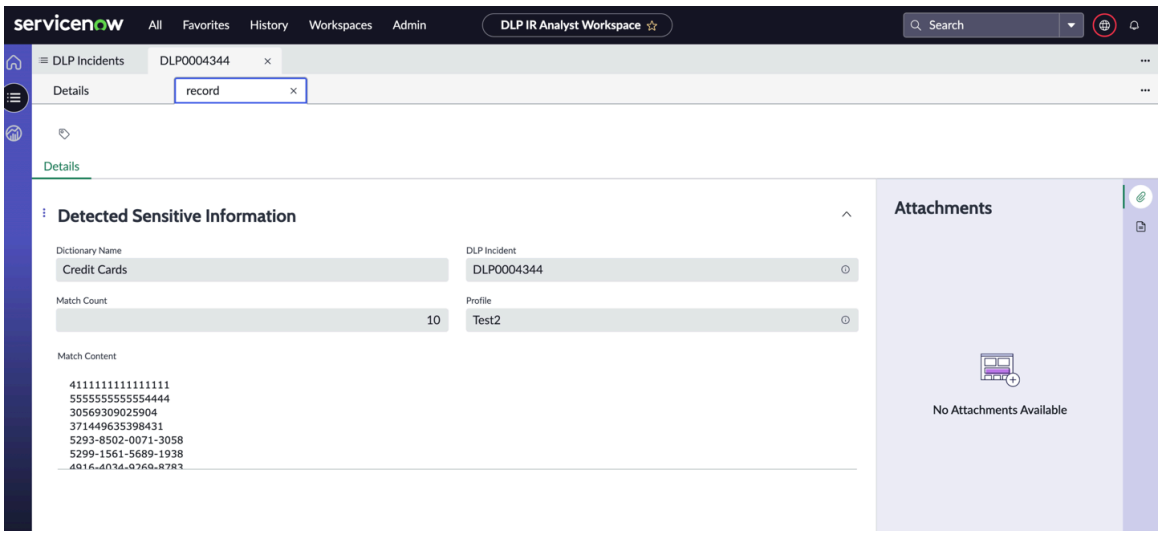
Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
   Die Seite „DLP-Arbeitsbereich – Meine Incidents“ wird im DLP-Arbeitsbereich für Analysten für Analysten angezeigt.
2. Öffnen Sie einen beliebigen DLP-Incident.
3. Navigieren Sie zur Registerkarte **Sensible Informationen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf den verletzten Datensatz.
5. Zeigen Sie die Informationen zum Abgleichsinhalt an, und ergreifen Sie nach Bedarf entsprechende Maßnahmen.



Laden Sie Nachweisdateien für DLP-Warnungen herunter

Laden Sie Dateien herunter, die gegen die DLP-Richtlinie eines Anbieters verstoßen, der ICAP unterstützt. Laden Sie diese Datei aus dem DLP-IR-Arbeitsbereich für Analysten und dem DLP-IR-Endanwender-Arbeitsbereich für Genehmiger auf Ihren lokalen Computer herunter.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.analyst und Genehmiger herunterladen können

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen den Dateidownload für ICAAP aktivieren, bevor Sie fortfahren.

Prozedur

1. Navigieren zu **Alle** > **ICAP-DLP-Integration** > **Einstellungen**.
2. Aktivieren Sie die Eigenschaft sn_icap_dlp.enable_file_download **Durch Aktivieren dieser Eigenschaft können Sie die Nachweisdatei des gemeldeten ICAP-Incident herunterladen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Schaltfläche **„Datei herunterladen“** wird im DLP-IR-Arbeitsbereich für Analysten und im DLP-IR-Endanwender-Arbeitsbereich angezeigt.

3. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
4. Öffnen Sie einen DLP-Incident-Datensatz, der aus der ICAP-Anbieterquelle erfasst wird.
5. Klicken Sie auf **Datei herunterladen**.

Hinweis:
DLP-Administratoren können den Zugriff auf die Aktion **Datei herunterladen** für alle Integrationen steuern, indem sie die Option **Sollte das Herunterladen der Datei mit Verstößen des gemeldeten Incidents zulässig sein** auf der Seite **„Erweiterte Einstellungen“** der DLP-Verwaltung deaktivieren. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Zeigen Sie eine Vorschau der Nachweisdateien für ICAP an

Zeigen Sie eine Vorschau der DLP-Incident-Beweisdateien im DLP-IR-Analystenarbeitsbereich an.

Vorbereitungen

- Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**.
- Stellen Sie sicher, dass die Eigenschaft **sn_icap_dlp.enable_evidence_file_preview** bereits aktiviert ist.

Wichtig:
Bei Verwendung der Aktion „Nachweisdateien“ im DLP-Analystenarbeitsbereich werden die Nachweisdateien für die Dauer, die Sie mit der Eigenschaft **„sn_dlir.preview_temp_files_cleanup_interval“** auf der Seite **„Erweiterte Einstellungen“** ausgewählt haben, in einem unverschlüsselten Format vorübergehend in der ServiceNow-Datenbank gespeichert. Sie können die Vorschaufunktion **für Nachweisdateien** deaktivieren, wenn Sie keine Daten in der ServiceNow-Datenbank speichern möchten. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.analyst

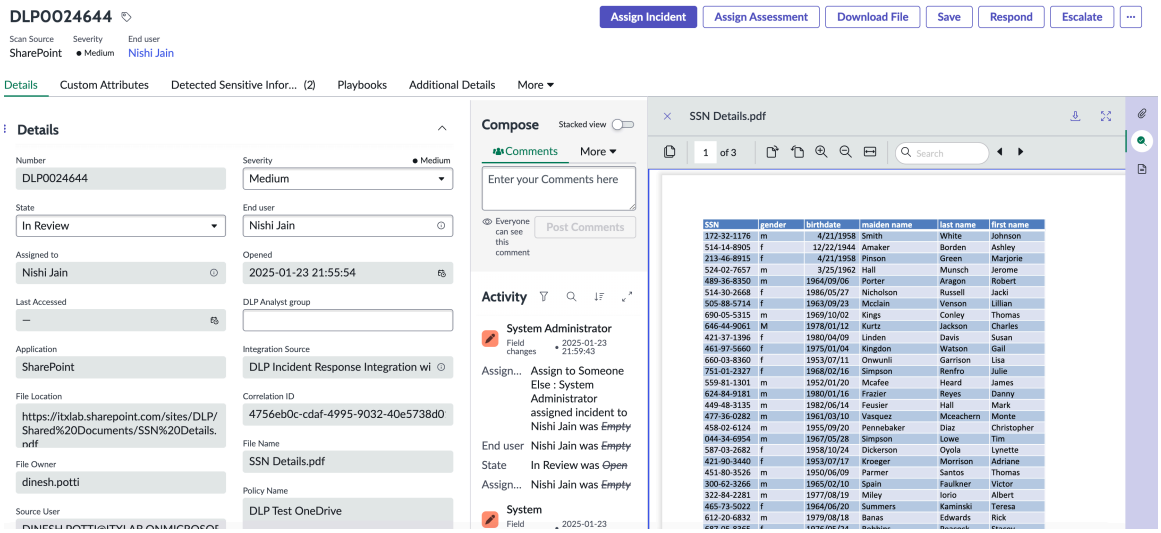
Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie das Symbol **Nachweisdateien**, das im Kontextmenü verfügbar ist.
   Eine Registerkarte wird geöffnet, auf der alle Nachweisdateien abgerufen werden. Sobald der Download abgeschlossen ist, können Sie alle Nachweisdateien auf der Registerkarte **Nachweisdateien** anzeigen.
4. Wählen Sie die **Nachweisdateikarte** aus, die Sie in der Vorschau anzeigen möchten.
   Die Vorschaufunktion ist für jeden Dateityp unterschiedlich.
5. Zeigen Sie eine Vorschau von PDF- und Office-Dokumenten im Dokument-Viewer an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen, um die PDF-Datei im Vollbildmodus zu öffnen. Zu den Office-Erweiterungen, für die der Dokument-Viewer die Nachweisdateien öffnet, gehören: doc, docx, ppt, pptx, xls, xlsx.
   a. Suchen Sie die Suchleiste, und geben Sie das gesuchte Stichwort ein.
   b. Verwenden Sie die Funktionen zum Vergrößern und Verkleinern, um die Ansicht für eine bessere Lesbarkeit anzupassen.
   c. Rotieren Sie die Seite im oder gegen den Uhrzeigersinn, um den Inhalt deutlicher anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

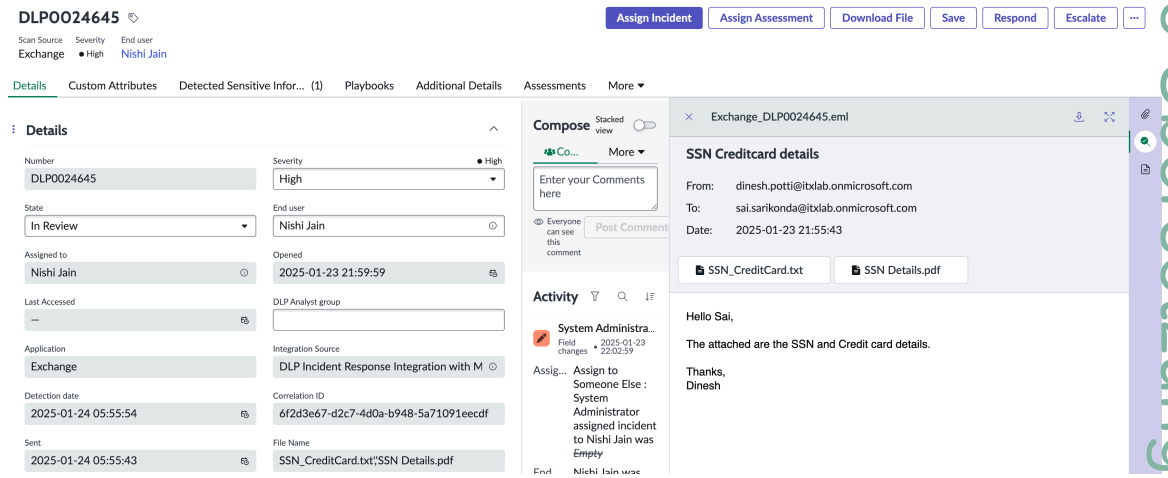
Diese Steuerungsoptionen verbessern Ihre Fähigkeit, die Nachweisdatei umfassend zu verstehen. Nur die PDF-Datei hat Steuerungsoptionen im Header.



6. Zeigen Sie eine Vorschau der EML-Dateien an.
   Wählen Sie die Anhänge in der E-Mail aus, und zeigen Sie eine Vorschau an.

Hinweis:

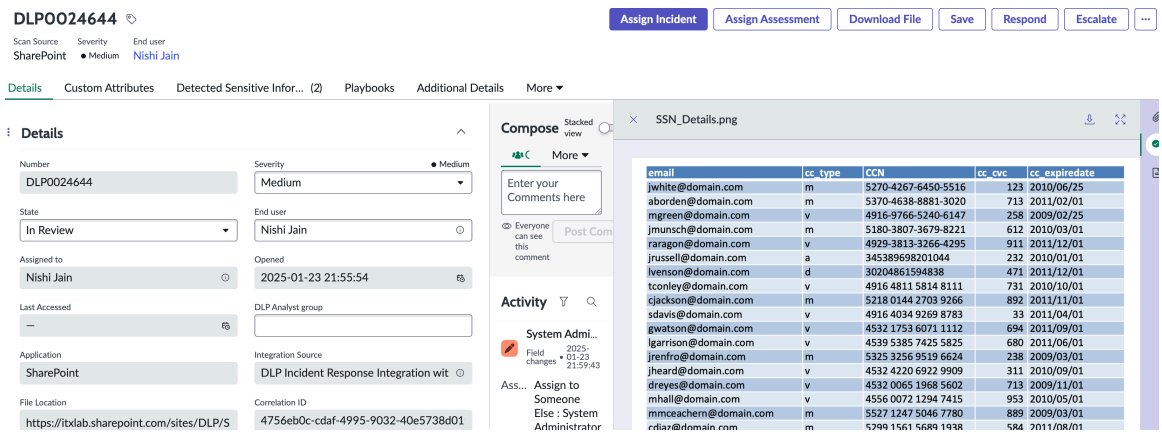
Wenn die ausgewählte Nachweisdatei die Grenze von 5 MB überschreitet, kann sie im Analystenarbeitsbereich nicht in der Vorschau angezeigt werden. Sie müssen die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen. Diese Beschränkung gilt nur für EML-Dateien.



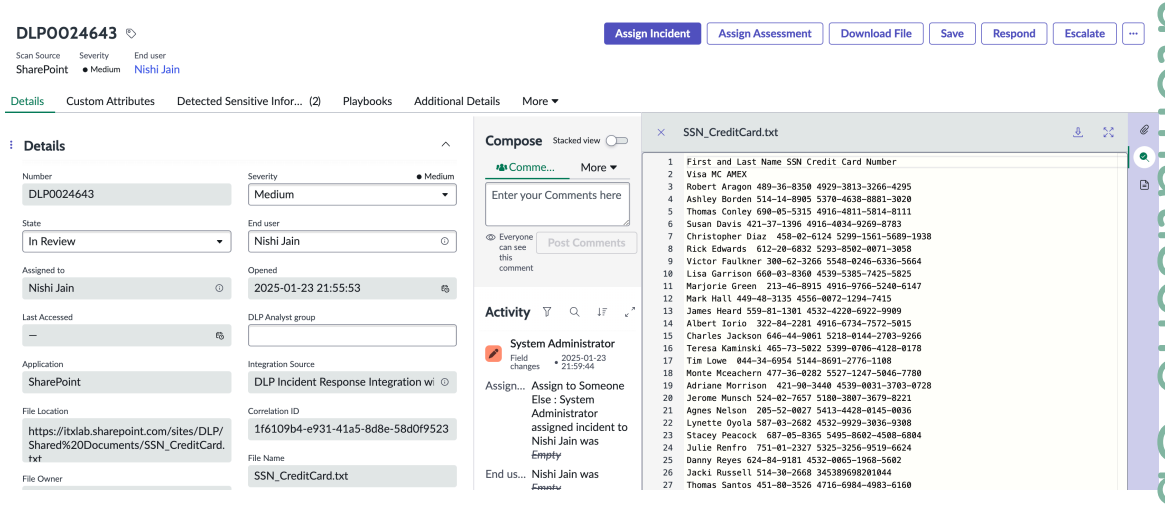
7. Zeigen Sie eine Vorschau der Bilder im DLP-Analystenarbeitsbereich an.
   Es werden nur Bilder mit den Erweiterungen .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg und .webp unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Zeigen Sie eine Vorschau von Textdateien im Texteditor an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen.



Hinweis:
Andere Nachweisdateien als Office-Dokumente, EML-Dateien, Text- und Bilderweiterungen werden für die Vorschau nicht unterstützt. Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion zur Vorschau der Nachweisdatei funktioniert auch für archivierte Incidents.

Überprüfen Sie die ICAP-DLP-Integrationseinstellungen

Überprüfen Sie die Einstellungen für die ICAP-DLP-Integration des Anbieters, und ändern Sie die Standardsystemeigenschaften an Ihre Umgebung.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Navigieren zu **Alle** > **ICAP-DLP-Integration** > **Einstellungen**.
2. Das Überprüfen und Ändern der Einstellungen ist erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Data Loss Prevention Incident Response mit MicrosoftMicrosoft Azure Event Hubs

Data Loss Prevention Incident Response mit MicrosoftMicrosoft Azure Event Hubs bietet ein Core Framework für den Import von DLP-Incidents (Data Loss Prevention) aus mehreren Quellen, z. B. MicrosoftMicrosoft Azure Event Hubs Vorschau-Apps (MicrosoftMicrosoft Azure Event Hubs Teams, Exchange Online, SharePoint Online, OneDrive for Business) und andere Ereignistypen. Endpunktgeräte ermöglichen einen Nachbesserungs-Workflow unter Einbeziehung von Endanwendern, Managern und DLP-Betriebsteams mit automatisierter Zuweisung und Eskalation von Incidents.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erstellen Sie mehrere Profile für verschiedene Accounts.
- Automatisieren Sie die Erstellung von Incidents DLP IR.
- Ordnen Sie die Ereignisfelder MicrosoftMicrosoft Azure Event Hubs DLP IR den Incident-Feldern DLP IR zu.
- Filtern Sie MicrosoftMicrosoft Azure Event Hubs DLP IR Ereignisse.
- Planen Sie die Erfassung von DLP IR Ereignissen, die regelmäßig Incidents vom DLP IR Typ erstellen.
- Speichern Sie den übereinstimmenden Inhalt jedes Microsoft DLP-Ereignisses im externen Cloud-Speicher.
- Löschen Sie übereinstimmende Inhalte im externen Cloud-Speicher, wenn Sie den Incident DLP IR in ServiceNowlöschen.
- Laden Sie Dateien für DLP IR Incidents vom Typ Exchange, OneDrive und SharePoint herunter.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
MicrosoftMicrosoft Azure Event Hubs Website mit Produktdokumentation	Microsoft-Website mit Produktdokumentation
ServiceNow Website mit Produktdokumentation	Website mit Produktdokumentation von ServiceNow

Erste Schritte mit der Microsoft-Integration DLP IR zur Verhinderung von Datenverlust

Lesen Sie sich die folgenden Informationen durch, bevor Sie mit der Einrichtung Ihrer MicrosoftMicrosoft Azure Event Hubs DLP IR -Integration zur Verhinderung von Datenverlust beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Setupaufgabe	Beschreibung
Rufen Sie die Microsoft Purview-Anmeldeinformationen ab, um die Ereignisdaten abzurufen, und die Anmeldeinformationen für das AWS/Azure Storage-Konto, um den Übereinstimmungsinhalt zu speichern Registrieren Sie eine Anwendung bei der Microsoft Identity Platform	Registrieren Sie hier eine Anwendung auf der Microsoft Azure-Plattform, um die Client-ID, den geheimen Clientschlüssel und die Mandanten-ID zu erhalten. Informationen zu den Rollen, die zum Erstellen einer Anwendung erforderlich sind, finden Sie unter Voraussetzungen. Informationen zu den API-Berechtigungen/-Rollen, die für eine Microsoft Azure-Anwendung erforderlich sind, um sie in der Microsoft DLP-Integration ServiceNow zu konfigurieren, finden Sie in der folgenden Tabelle.
Berechtigungen, die für den Azure-Anwender erforderlich sind, um Lese-/Schreib-/Löschzugriff für Blobs in Azure Storage zu erhalten	Der Azure-Anwender muss die Rolle **„Beitragender für Speicher-Blobdaten“** haben, um Blobs in Azure Storage zu lesen, zu schreiben und zu löschen.
Berechtigungen, die für den AWS-Anwender erforderlich sind, um Lese-/Schreib-/Löschobjekte in AWS Storage zu erhalten	Es muss eine Richtlinie erstellt werden, die Listen-, Lese-, Schreib- und Löschzugriff für das Objekt in AWS S3-Speicher gewährt.

Weisen Sie zu und überprüfen Sie, ob Sie über die erforderlichen Rollen für Now Platform und die Rollen für die Verwaltung von Datenverlust verfügen.	Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:
	• Die Administratorrolle installiert die Integration aus ServiceNow Store und weist die Rolle sn_dlir.admin zu.
	• Die Rolle sn_dlir.admin führt die folgenden Aufgaben aus:
	  ○ Konfiguriert die Integration.
	  ○ Richtet die Incident-Profile ein.

Stellen Sie sicher, dass die ServiceNow Core-Anwendungen, die zur Unterstützung der Microsoft-Integration DLP IR erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren.	Vergewissern Sie sich, dass die folgenden DLP IR -Anwendungen und allgemeinen Anwendungen zur Unterstützung der Sicherheit im ServiceNow -Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche API-Berechtigungen/-Rollen für eine Microsoft Azure-Anwendung

Sie benötigen die folgenden API-Berechtigungen/Rollen in einer Microsoft Azure-Anwendung, um sie in der Microsoft DLP-Integration **ServiceNow** *zu konfigurieren.*

API	Berechtigungsnam	Typ	Beschreibun	Für welche Funktion von ServiceNow erforderlich?	Ist Administrator erforderlich?
Office 365 Management API	Aktivitäts-Feed.LesenDLP	Anwendung	Lesen Sie DLP-Richtlinienereignisse einschließlich erkannter vertraulicher Daten.	Erfassung der DLP-Ereignisse aus MSFT-Ereignisse in ServiceNow. **Hinweis:** Diese Berechtigung ist erforderlich, um die MSFT-Daten in ServiceNowabzurufen.	Ja
Microsoft Graph-API	Dateien.Lesen.Alle	Anwendung	Lesen Sie Dateien in allen Websitesammlungen, auf die Sie zugreifen können.	Datei herunterladen: Zum Herunterladen des Anhangs in der ServiceNow-Instanz, der das DLP-Ereignis von OneDrive oder SharePoint verursacht hat **Hinweis:** Dies ist optional. Sie können diese API-Berechtigung überspringen, wenn Sie nicht möchten, dass die Analysten den Anhang herunterladen, der das DLP-Ereignis verursacht hat.	Ja
	E-Mail.Lesen	Anwendung	E-Mails in allen Postfächern lesen.	Datei herunterladen: Zum Herunterladen des E-Mail-Inhalts (Text und Anhang) in der ServiceNow-Instanz, die das DLP-Ereignis von Exchange verursacht hat.	Ja

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche API-Berechtigungen/-Rollen für eine Microsoft Azure-Anwendung
Sie benötigen die folgenden API-Berechtigungen/Rollen in einer Microsoft Azure-Anwendung, um sie in der Microsoft DLP-Integration **ServiceNow** *zu konfigurieren.*

(Fortsetzung)

API	Berechtigungsnam	Typ	Beschreibun	Für welche Funktion von ServiceNow erforderlich?	Ist Administrator erforderlich?
				Hinweis: Dies ist optional. Sie können diese API-Berechtigung überspringen, wenn Sie nicht möchten, dass die Analysten den E-Mail-Inhalt (Text, Anhang) herunterladen, der das DLP-Ereignis verursacht hat.	
	Anwender.Lesen	Delegiert	Melden Sie sich an, und lesen Sie das Anwenderprofil.	Dies ist die Standardberechtigung, die für alle neuen Anwendungen verfügbar ist.	Nein

Erkannte sensible Informationen (optional)

Der Übereinstimmungsinhalt wird extern in Azure Blob Storage oder einem Amazon S3-Bucket gespeichert und aus dem externen Speicher abgerufen, wenn der Benutzer einen Incident anzeigt.

Eine der folgenden Berechtigungen ist erforderlich, wenn Anwender den Abgleichinhalt/die erkannten vertraulichen Informationen in der DLP Core-Anwendung anzeigen möchten:

1. Wenn Sie ein Microsoft Azure -Benutzer sind, müssen Sie über die Rolle Beitragender zu Speicher-Blobdaten verfügen, um Blobs in Azure Storage zu lesen, zu schreiben und zu löschen.
2. Wenn Sie ein Amazon S3-Benutzer sind, müssen Sie eine Richtlinie erstellen, die Listen-, Lese-, Schreib- und Löschzugriff für das Objekt im Amazon S3-Speicher gewährt.

Installieren und konfigurieren Sie die Microsoft DLP-Integration

Installieren und konfigurieren Sie die Integration von DLP Incident Response mit MicrosoftMicrosoft Azure Event Hubs DLP aus ServiceNow® Store in Ihrer Instanz Now Platform. Starten Sie die Untersuchung von DLP-Incidents anhand der DLP-Ereignisdaten MicrosoftMicrosoft Azure Event Hubs.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

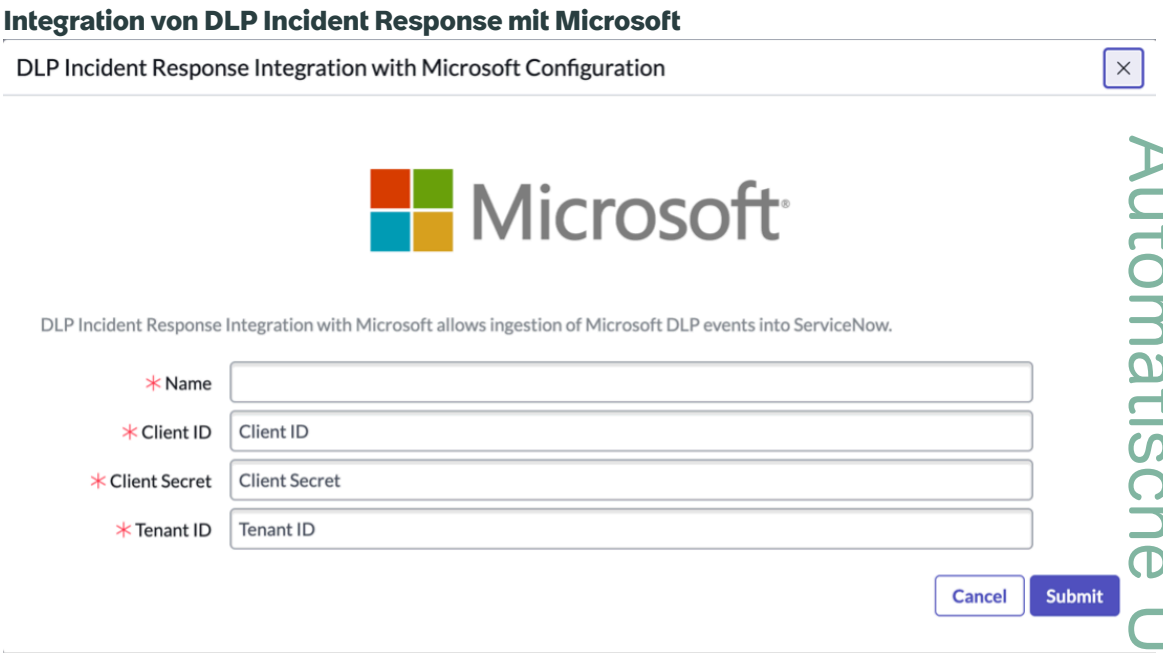
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie die DLP-Integration MicrosoftMicrosoft Azure Event Hubs von ServiceNow® Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Konfigurieren Sie die DLP-Integration MicrosoftMicrosoft Azure Event Hubs.

   a. Suchen Sie nach der Kachel **Integration von DLP Incident Response mit Microsoft**, und klicken Sie auf **Konfigurieren**.



   b. Füllen Sie die Felder des Formulars aus.

Formular „Microsoft DLP-Integrationskonfiguration“.

Feld	Beschreibung
Name	Name der MicrosoftMicrosoft Azure Event Hubs DLP-Integrationskonfiguration.
Client-ID	Client-ID der im Microsoft Azure-Portal erstellten App.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der im Microsoft Azure-Portal erstellten App.
Mandanten-ID	Mandanten-ID des Anwenders.

   c. Klicken Sie auf **Absenden**.

   Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die DLP-Integration MicrosoftMicrosoft Azure Event Hubs auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

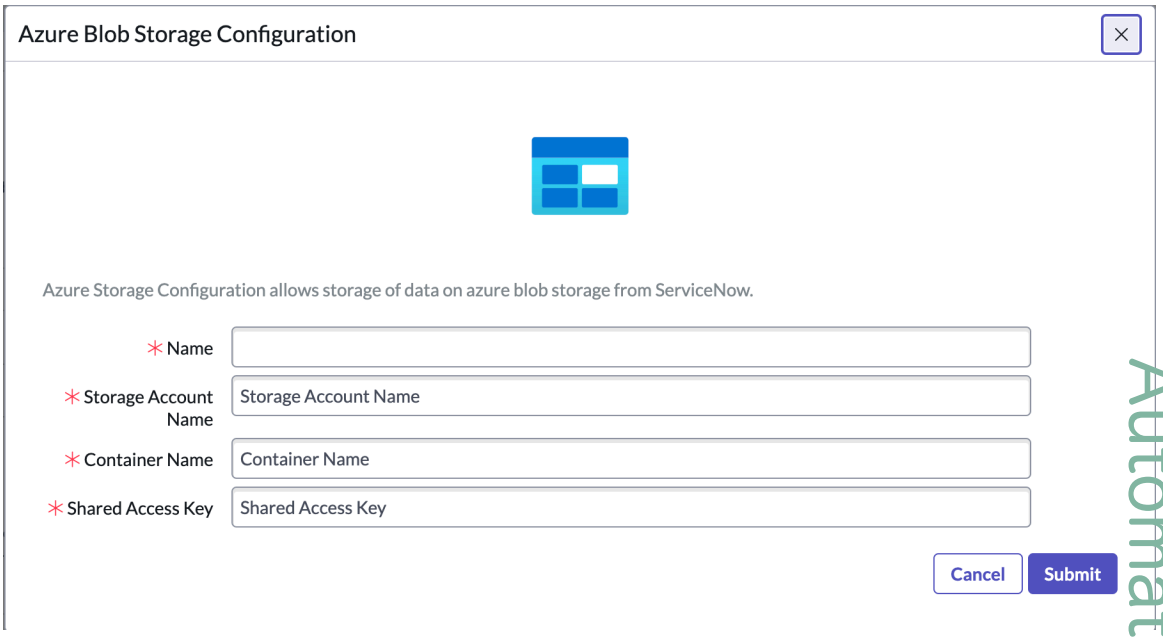
4. Aktualisiert die Azure Storage-Konfiguration.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Suchen Sie auf der Seite „Sicherheitsintegrationen“ nach der Kachel **Azure Storage-Konfiguration**.

b. Klicken Sie auf der Kachel Azure Storage-Konfiguration **auf Aktualisieren**.



c. Füllen Sie die Felder des Formulars aus.

Formular „Azure Storage-Konfiguration“.

Feld	Beschreibung
Name	Name der Azure Storage-Konfiguration.
Name des Speicher-Accounts	Name des Speicherkontos, der im Azure-Portal erstellt wurde
Containername	Containername, der im Speicherkonto im Azure-Portal erstellt wurde.
Freigegebener Zugriffsschlüssel	Freigegebener Zugriffsschlüssel für das Speicherkonto.

d. Klicken Sie auf **Absenden**.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Azure Storage-Konfiguration auf der Seite „Security Integrations“ (Sicherheitsintegrationen) als Kachel gespeichert.

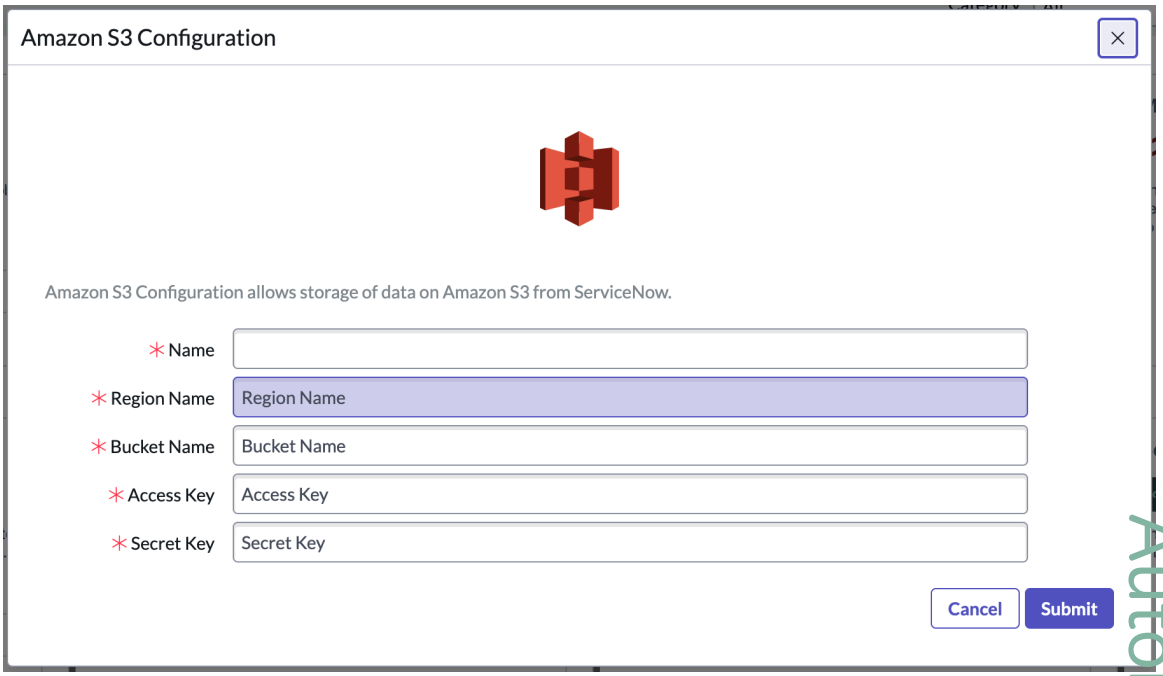
5. Aktualisiert die AWS-Speicherkonfiguration.

a. Suchen Sie auf der Seite „Security Integrations“ (Sicherheitsintegrationen) nach der Kachel **AWS Storage Configuration (AWS-Speicherkonfiguration)**.

b. Klicken Sie auf der Kachel AWS Storage Configuration (AWS-Speicherkonfiguration) auf **Update (Aktualisieren)**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Füllen Sie die Felder des Formulars aus.

Formular „AWS-Speicherkonfiguration“.

Feld	Beschreibung
Name	Name der AWS-Speicherkonfiguration.
Regionsname	Regionsname des AWS Storage-Accounts.
Bucket-Name	Im AWS-Portal erstellter Bucket-Name.
Zugriffsschlüssel	Zugriffsschlüssel mit Lese-, Schreib- und Löschzugriff.
Geheimer Schlüssel	Freigegebener Schlüssel mit Lese-, Schreib- und Löschzugriff

d. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die AWS S3-Konfiguration auf der Seite „Security Integrations“ (Sicherheitsintegrationen) als Kachel gespeichert.

Erstellen Sie ein neues Incident-Profil für die MicrosoftMicrosoft Azure Event Hubs DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform, um die Daten aus Microsoft Purview abzurufen und die Daten der Incident-Tabelle ServiceNow DLP IR hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

sn_dlir.analyst – Ansicht (schreibgeschützt)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Now Platform®, um die Ereignisse aus dem Purview MicrosoftMicrosoft Azure Event Hubs abzurufen. Speichern Sie diese Ereignisse in der Incident-Tabelle DLP IR in Ihrer Instanz ServiceNow®.

Prozedur

1. Navigieren zu **Microsoft DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt „Name“ aus.

Erstellen Sie ein Profilformular

Feld	Beschreibung
Name	Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Die Instanz MicrosoftMicrosoft Azure Event Hubs DLP IR, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie über mehrere Integrationskonfigurationen verfügen, wählen Sie den entsprechenden Integrationskonfigurationsdatensatz für die Incident-Typen aus, die für das Profil erfasst werden sollen.
Aktiv	Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann erst aktiviert werden, nachdem Sie im Abschnitt „Zeitplanung“ auf das Feld „**Fertigstellen“** geklickt haben. Wenn das Profil aktiv ist, impliziert dies, dass Now Platform basierend auf der im Profil definierten Konfiguration aktiv Ereignisse MicrosoftMicrosoft Azure Event Hubs DLP IR von abfragt.
Bestellung	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge wird als höchste Priorität betrachtet. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für das Profil.

Nächste Maßnahme

Um zum Abschnitt „Filtern“ zu wechseln, klicken Sie auf **Fortfahren**.

Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden

Definieren und legen Sie Filterbedingungen fest, um die eingehenden Microsoft-DLP-Ereignisse zu filtern. Steuern Sie, welche dieser Ereignisse als DLP IR Incidents in Ihrer Instanz von ServiceNow erstellt werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

sn_dlir.analyst – Ansicht (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird

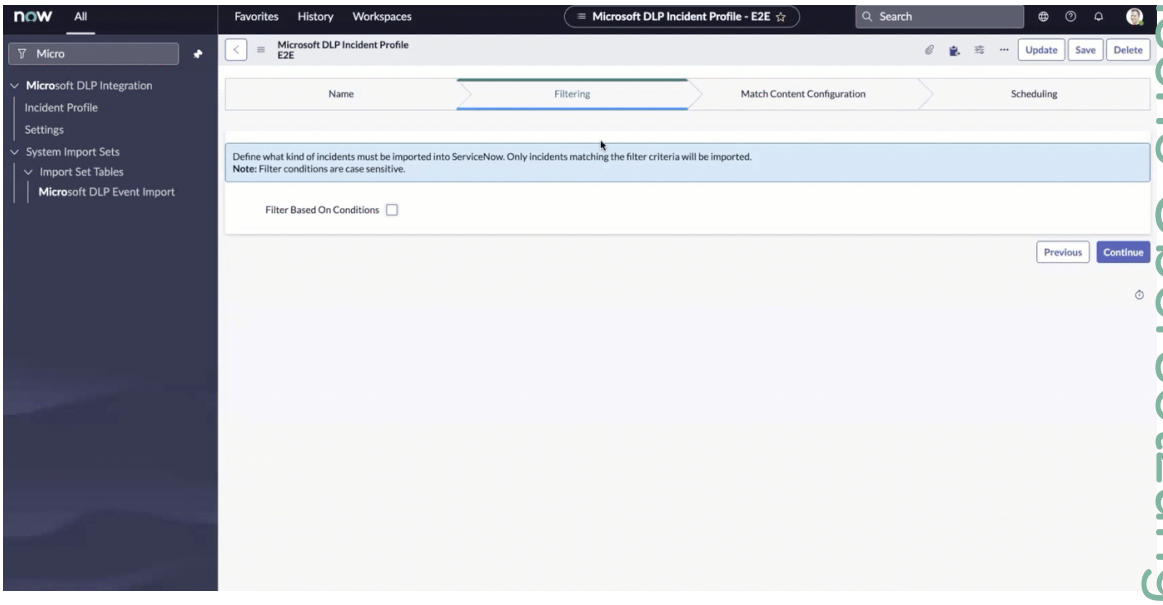
Mit dieser Art der Filterung können Sie Microsoft-DLP-Ereignisse isolieren, um die Anzahl der von Ihnen erstellten DLP IR Incidents zu begrenzen. Wenn die Filterkriterien festgelegt sind, werden nur Ereignisse, die den Bedingungen entsprechen, als DLP-Incidents erstellt.

Prozedur

1. Wählen Sie die Option **Basierend auf Bedingungen filtern** aus.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter im Feld **Filterbedingungen** fest.

   Definieren Sie die Kriterien, die ein eingehendes MicrosoftMicrosoft Azure Event Hubs DLP-Ereignis erfüllen muss, damit ein DLP-Incident erstellt wird.

   Die Optionen im ersten Feld der **Filterbedingungen** entsprechen den Feldern, die im Microsoft DLP-Ereignis verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des Ereignisses übereinstimmen.



3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf **AND**oder **OR**klicken.
   - Wenn **AND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER**ausgewählt ist, kann eine der beiden Bedingungen erfüllt werden.
4. Klicken Sie auf **„Fortsetzen“**, und wechseln Sie zum Abschnitt „Inhaltskonfiguration abgleichen“.

Konfigurieren Sie die Übereinstimmung des Inhalts für den Incident

Geben Sie die Konfiguration zum Speichern der vertraulichen Informationen in einem externen Cloud-Speicher wie Azure Storage oder AWS S3-Bucket an, um diese Inhalte während des Zugriffs auf den DLP IR Incident abzurufen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_dlir.analyst – Ansicht (schreibgeschützt)

Prozedur

1. Klicken Sie in der Fortschrittsleiste auf den Schritt **„Inhaltskonfiguration abgleichen“**.
2. Füllen Sie die Felder des Formulars aus.

Inhaltskonfiguration abgleichen

Feld	Beschreibung
Abgleichsinhalt speichern	Option zum Speichern des übereinstimmenden Inhalts im Cloud-Speicher. **Wichtig:** Wenn diese Option nicht ausgewählt ist, werden die Richtlinienübereinstimmungsinhalte für DLP-Incidents nicht im DLP-Arbeitsbereich angezeigt. Durch Aktivieren dieser Option wird sichergestellt, dass in den DLP-Incidents zurückgegebene Übereinstimmungsinhalte im externen Cloud-Speicher (z. B. Azure, AWS) gespeichert werden. Sie können den Übereinstimmungsinhalt auch abrufen und anzeigen, wenn ein DLP-Incident im Arbeitsbereich geöffnet wird. Informationen zur Konfiguration des externen Cloud-Speichers finden Sie unter Installieren und konfigurieren Sie die Microsoft DLP-Integration.
Abgleichsinhalt beim Löschen des Incidents löschen	Option zum Löschen des Inhalts der Incident-Übereinstimmung aus dem externen Cloud-Speicher. Diese Option ist nur sichtbar, wenn das Feld **Store Match Content** ausgewählt ist.
Externe Cloud-Anmeldeinformationen	Der externe Cloud-Speicher, in dem der Übereinstimmungsinhalt gespeichert wird. Sie können auf die externen Cloud-Anmeldeinformationen verweisen, die für die Speicherkonfiguration hinzugefügt wurden. Diese Option ist nur sichtbar, wenn das Feld **Store Match Content** ausgewählt ist.

3. Klicken Sie auf **Fortsetzen** und wechseln Sie zum Abschnitt Zeitplanung.

Planen Sie den Abruf des Microsoft-Incident DLP IR

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und Incidents MicrosoftMicrosoft Azure Event Hubs DLP IR zu erfassen, die den Kriterien im Profil entsprechen. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus MicrosoftMicrosoft Azure Event Hubsabrufen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

sn_dlir.analyst – Ansicht (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft Sie zukünftige Incidents abfragen, die der Konfiguration des Incident-Profils entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann mit dem Kontrollkästchen Einmaliger Abruf so konfiguriert werden **, dass ein einmaliger** Abruf erfolgt. Als Verlaufsdatum können die letzten drei Monate ab dem aktuellen Datum angegeben werden.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die unterschiedlichen Abfrageintervalle können sich auf die Leistung der Incident-Integration MicrosoftMicrosoft Azure Event Hubs DLP IR auswirken. Planen Sie bei der Zeitplanung, die Systemlast gegen die Dringlichkeit eines incident abzuwägen.

Prozedur

1. Legen Sie einen Zeitplan fest, um Daten abzurufen und Incidents zu erfassen, die den Kriterien im Profil entsprechen.
2. Füllen Sie die Felder des Formulars aus.

Zeitplan für das DLP-Incident-Formular

Feld	Beschreibung
Laufende Incident-Erfassung	Die laufende Incident-Erfassung, die die Instanz Now Platform von Microsoft für neue Incidents abruft. DLP IR Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung erfüllt sind.
Abfrageschritt (Minuten)	Die Abfragehäufigkeit von Microsoft. Dieses Feld wird automatisch auf 300 Minuten festgelegt.
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Definieren eines Datums und einer Uhrzeit für die erste Erfassung. Nachfolgende Erfassungen basieren auf dem Zeitraum des Abfrageintervalls. Diese Option ist nur sichtbar, wenn das Feld **Fortlaufende Incident-Erfassung** ausgewählt ist.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben. ○ Wenn der Wert festgelegt ist, beginnt das Abrufen von Daten von Microsoft ab dem hinzugefügten zukünftigen Datum. ○ Dieses Feld ist nur sichtbar, wenn **Zeit der ersten Erfassung** festlegen ausgewählt ist.
Zeitpunkt der ersten Incident-Erfassung	Zeitpunkt der ersten Erfassung der Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können im sehen, dass Werte angezeigt werden, wenn die Zeit für die erste Incident-Erfassung festgelegt wird.
Nächste Incident-Erfassungszeit (geschätzt)	Der nächste Zeitraum für eine geschätzte Incident-Erfassung.
Einmaliger Abruf	Option zum Aktivieren einmaliger Verlaufsdatenabrufe. Wenn dieses Feld ausgewählt ist, werden Verlaufsdaten entsprechend dem im Feld **Seit Datum** hinzugefügten Datum aus Microsoft DLP IR abgerufen.
Seit Datum	Datum, ab dem Daten von Microsoft abgerufen werden sollen. Dieses Feld kann auf maximal 7 Tage festgelegt werden.

3. Speichern Sie die erstellte Profilkonfiguration, indem Sie im Popup-Fenster auf **Fertigstellen** klicken.
4. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Aktivieren Sie die Option **Aktiv**.
   c. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Nach der erfolgreichen Erstellung und Aktivierung des Profils werden die Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen und der DLP-Incidents-Tabelle hinzugefügt.

Konfigurieren Sie die Einstellungen für die Microsoft-Integration DLP IR .

Ändern Sie die standardmäßigen Systemeigenschaften der MicrosoftMicrosoft Azure Event Hubs DLP IR -Integration.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Navigieren zu **Microsoft-DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Eigenschaften nach Bedarf.

Microsoft DLP-Integrationseinstellungen

Feld	Beschreibung
Maximale Zeitüberschreitung für HTTP-Aufrufe (sn_pp_dlp.maximum_http_time_out)	Maximale Zeitüberschreitung für HTTP-Aufrufe (in Sekunden).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Typ: Ganzzahl ○ Standardwert: 30
Ebene der Berichterstellung für die von der Integration generierten Protokolle (sn_pp_dlp.ging.verbosity)	Die Ebene der von der Integration generierten Berichterstellungsprotokolle, d. h. den Namen des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **Fehler** ○ **warnen** ○ **Info** ○ **debuggen** ○ **aus** Standardmäßig lautet der Wert **„info“**.
Ziel der Berichterstellung für die von der Integration generierten Protokolle (sn_pp_dlp.ging.destination)	Das Ziel für die Protokolle, die von der Integration generiert werden. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **db** ○ **Datei** ○ **Keine** Standardmäßig lautet der Wert **„db“**.

3. Klicken Sie auf **Speichern**.

Ergebnisse

Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Fordern Sie eine Release-E-Mail aus der Quarantäne an

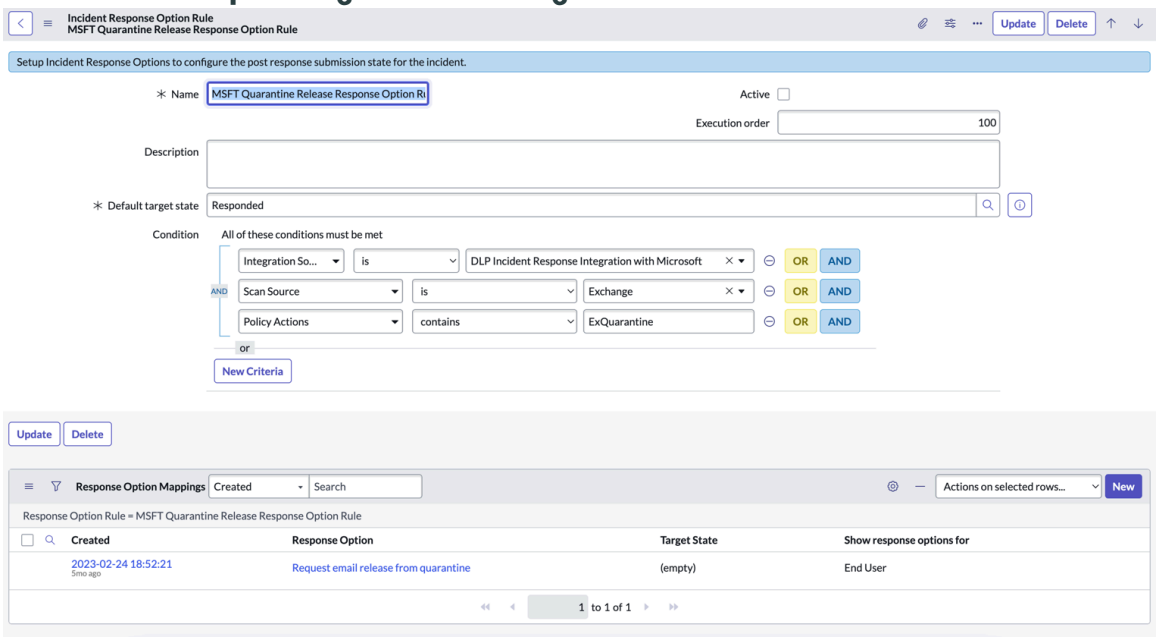
Verwenden Sie diese Funktion, um die E-Mail freizugeben, die aus dem Microsoft Purview-Compliance-Portal unter Quarantäne gestellt wird.

Vorbereitungen

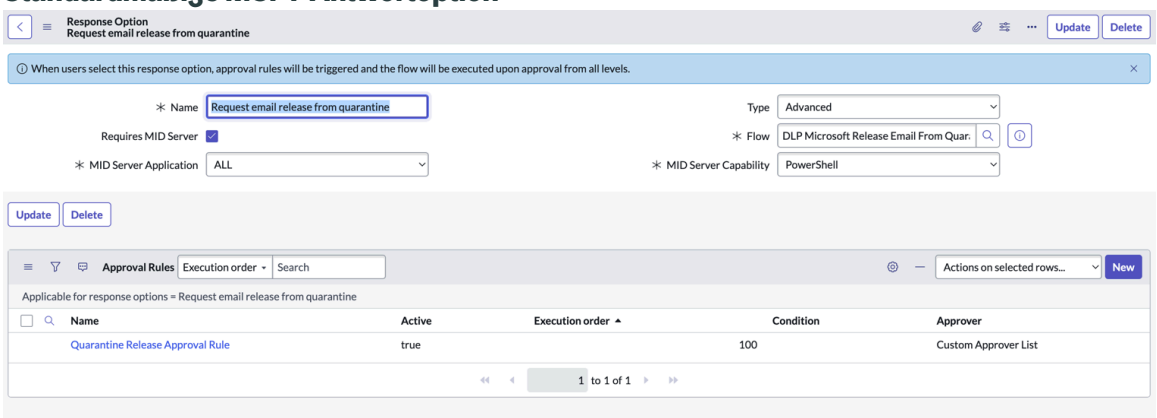
Standardmäßig stellt das Basissystem die Antwortoption **„E-Mail-Freigabe aus Quarantäne anfordern“** und **die Regel für die MSFT-Quarantänefreigabe-Antwortoption** bereit, um die E-Mail aus der Quarantäne freizugeben. Mit diesem Standarddatensatz ist auch die **Genehmigungsregel für Quarantäne-Release** konfiguriert, um die Genehmigungsfunktion für diese Aktion zu nutzen. Weitere Informationen finden Sie unter Erstellen Sie Optionsregeln für die Reaktion auf Incidents, Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents und Erstellen Sie Genehmigungsregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MSFT – Antwortoptionsregel für Entlassung aus Quarantäne



Standardmäßige MSFT-Antwortoption



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie diese Antwortoption verwenden, stellen Sie sicher, dass der MID-Server mit PowerShell-Fähigkeit aktiv ist. Wenn ein MID-Server nicht in Betrieb ist und nicht über PowerShell-Funktionen verfügt, kann der Endanwender im Arbeitsbereich für DLP-Anwender die Aktion **„E-Mail-Freigabe aus Quarantäne anfordern“** nicht auswählen. Weitere Informationen finden Sie unter Erstellen Sie Optionsregeln für die Reaktion auf Incidents und Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents.

- Wenn Sie einen bestimmten MID-Server aus der Liste möchten, müssen Sie die MID-App konfigurieren und in der Liste sichtbar machen. Dann sollte mindestens ein konfigurierter MID-Server über die ausgewählten MID-Anwendungen aktiv sein und über Folgendes verfügen: PowerShell-Fähigkeit
- Damit Sie die Option Aus Quarantäne freigeben verwenden können, benötigen Sie API-Berechtigungen. Überprüfen Sie auf der Seite mit den Microsoft-API-Berechtigungen **Office 365 Exchange Online** > **Exchange.VerwaltenAlsApp** wird aufgelistet und enthält die folgenden Werte:
  - **Typ**: **Anwendung**.
  - **Administratorzustimmung erforderlich**: **Ja**.
  - **Status**: Der derzeit falsche Wert ist **„Nicht gewährt für“.** <Organization> für den Eintrag **„Office 365 Exchange Online“** > **„Exchange.ManageAsApp“**, und ändern Sie den Statuswert. Weitere Schritte zu den API-Berechtigungen finden Sie unter Der Anwendung API-Berechtigungen zuweisen auf der Microsoft-Dokumentationswebsite.

    Hinweis:
    Dieser Schritt ist erforderlich, um über das Serviceprinzip eine Verbindung zu Exchange Online herzustellen.

- Sie sollten auch die Rolle **„Sicherheitsadministrator“** in „Serviceprinzip“ benötigen.
  - Suchen Sie im Microsoft Azure-Portal nach **Microsoft Entra ID-Rollen und Administratoren**, fügen Sie der registrierten App Zuweisungen hinzu (Serviceprinzip). Befolgen Sie dann das in der Microsoft-Dokumentation erläuterte Verfahren zum Zuweisen einer Rolle .
- Diese Option gilt nur für Microsoft Exchange-Incidents, für die in der Incident-Formularansicht die Option **ExQuarantine** für **Richtlinienaktion** festgelegt ist.

Erforderliche Rolle: Endanwender

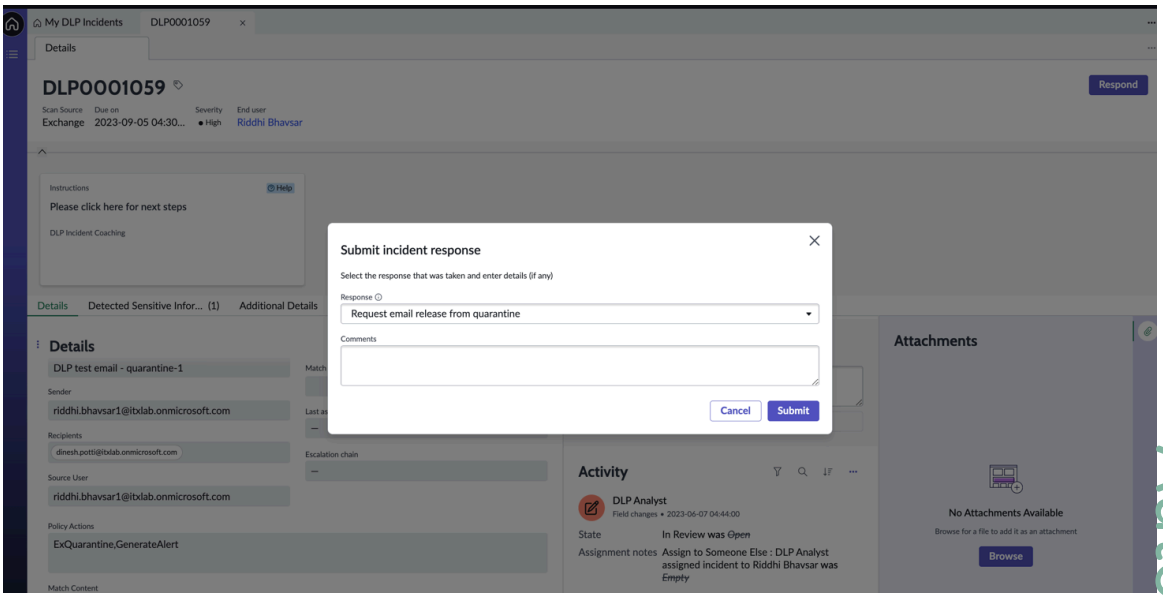
Im folgenden Verfahren wird erläutert, wie Sie diese Aktion über den DLP-Anwenderarbeitsbereich übermitteln.

Prozedur

1. Navigieren zu **DLP** > **DLP-Anwenderarbeitsbereich**.
2. Öffnen Sie einen beliebigen Microsoft Exchange DLP-Incident.
   Vergewissern Sie sich, dass die **Richtlinienaktion** für Incidents auf ExQuarantine festgelegt ist.
3. Klicken Sie **auf Antworten**.
4. Wählen Sie in der Dropdown-Liste Antwort die Option **E-Mail-Release aus Quarantäne anfordern** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incident-Antwort übermitteln – Option zum Freigeben von Quarantäne per E-Mail anfordern



5. Klicken Sie auf **Absenden**.

> **Hinweis:**
> Wenn eine Genehmigungsregel für diese Aktion konfiguriert ist, wird zuerst der Genehmigungs-Flow ausgelöst. Nach Erhalt aller Genehmigungen wird der Flow „E-Mail-Freigabe aus Quarantäne anfordern“ ausgelöst, und die E-Mail wird aus der Quarantäne freigegeben. Der Status des DLP-Incident wird nach der erfolgreichen Freigabe in **„Aus Quarantäne freigegeben“** aktualisiert.

Zeigen Sie eine Vorschau der Nachweisdateien für DLP-Incidents vom Typ Exchange Online, OneDrive und SharePoint an

Zeigen Sie eine Vorschau der DLP-Incident-Beweisdateien im DLP-IR-Analystenarbeitsbereich an.

Vorbereitungen

- Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**.
- Stellen Sie sicher, dass die Eigenschaft **sn_msft_dlp.enable_evidence_file_preview** bereits aktiviert ist.

> **Wichtig:**
> Bei Verwendung der Aktion „Nachweisdateien“ im DLP-Analystenarbeitsbereich werden die Nachweisdateien für die Dauer, die Sie mit der Eigenschaft **„sn_dlir.preview_temp_files_cleanup_interval“** auf der Seite **„Erweiterte Einstellungen“** ausgewählt haben, in einem unverschlüsselten Format vorübergehend in der ServiceNow-Datenbank gespeichert. Sie können die Vorschaufunktion **für Nachweisdateien** deaktivieren, wenn Sie keine Daten in der ServiceNow-Datenbank speichern möchten. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.analyst

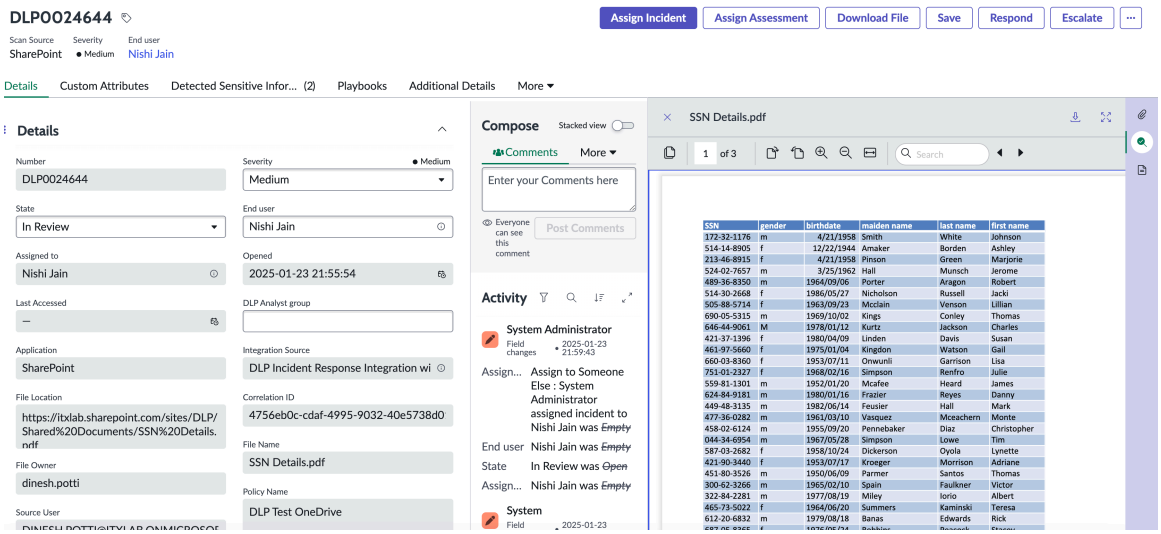
Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen DLP-Incident-Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie das Symbol **Nachweisdateien**, das im Kontextmenü verfügbar ist.
   Eine Registerkarte wird geöffnet, auf der alle Nachweisdateien abgerufen werden. Sobald der Download abgeschlossen ist, können Sie alle Nachweisdateien auf der Registerkarte **Nachweisdateien** anzeigen.
4. Wählen Sie die **Nachweisdateikarte** aus, die Sie in der Vorschau anzeigen möchten.
   Die Vorschaufunktion ist für jeden Dateityp unterschiedlich.
5. Zeigen Sie eine Vorschau von PDF- und Office-Dokumenten im Dokument-Viewer an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen, um die PDF-Datei im Vollbildmodus zu öffnen.
   Zu den Office-Erweiterungen, für die der Dokument-Viewer die Nachweisdateien öffnet, gehören: doc, docx, ppt, pptx, xls, xlsx.
   a. Suchen Sie die Suchleiste, und geben Sie das gesuchte Stichwort ein.
   b. Verwenden Sie die Funktionen zum Vergrößern und Verkleinern, um die Ansicht für eine bessere Lesbarkeit anzupassen.
   c. Rotieren Sie die Seite im oder gegen den Uhrzeigersinn, um den Inhalt deutlicher anzuzeigen.
   Diese Steuerungsoptionen verbessern Ihre Fähigkeit, die Nachweisdatei umfassend zu verstehen. Nur die PDF-Datei hat Steuerungsoptionen im Header.

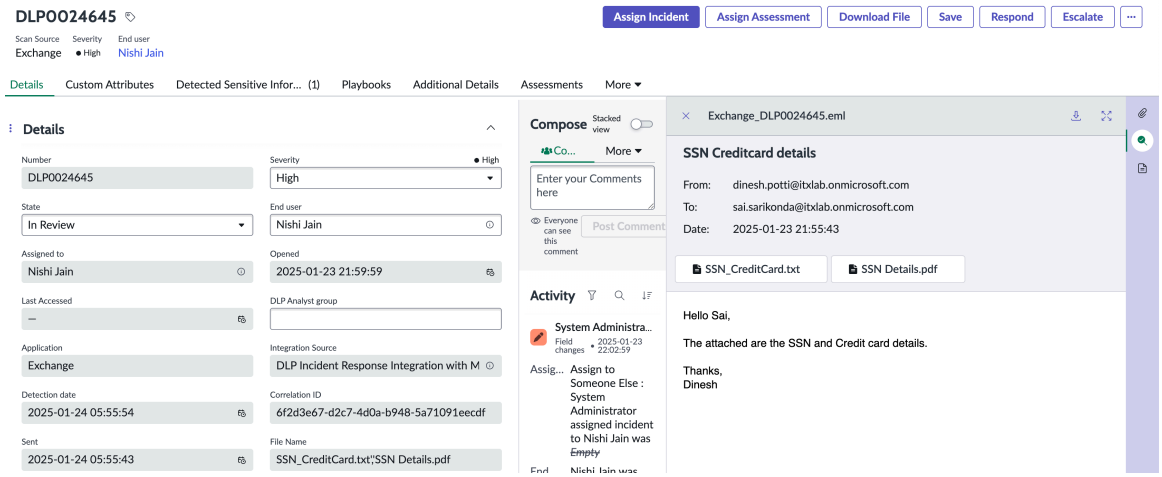


6. Zeigen Sie eine Vorschau der EML-Dateien an.
   Wählen Sie die Anhänge in der E-Mail aus, und zeigen Sie eine Vorschau an.

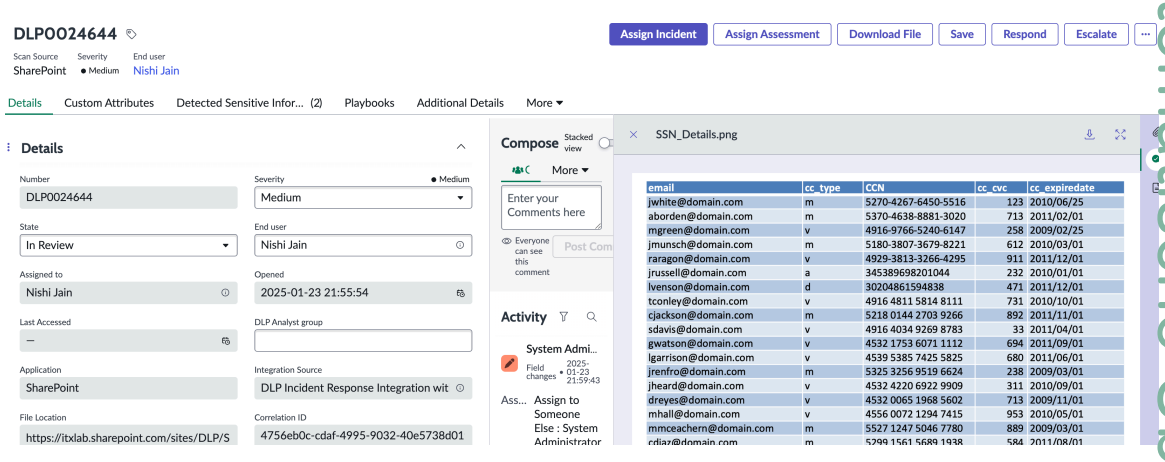
> **Hinweis:**
> Wenn die ausgewählte Nachweisdatei die Grenze von 5 MB überschreitet, kann sie im Analystenarbeitsbereich nicht in der Vorschau angezeigt werden. Sie müssen die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen. Diese Beschränkung gilt nur für EML-Dateien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



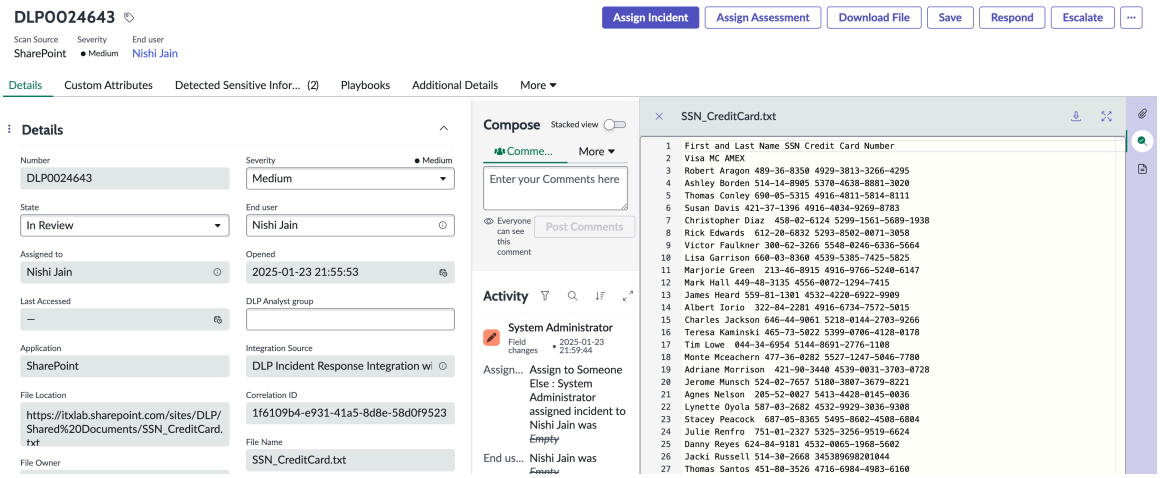
7. Zeigen Sie eine Vorschau der Bilder im DLP-Analystenarbeitsbereich an.
Es werden nur Bilder mit den Erweiterungen .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg und .webp unterstützt.



8. Zeigen Sie eine Vorschau von Textdateien im Texteditor an, indem Sie oben rechts in der Nachweisdatei das Symbol **Erweitern** wählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Andere Nachweisdateien als Office-Dokumente, EML-Dateien, Text- und Bilderweiterungen werden für die Vorschau nicht unterstützt. Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion zur Vorschau der Nachweisdatei funktioniert auch für archivierte Incidents.

Laden Sie Dateien für DLP-Incidents vom Typ Exchange Online, OneDrive und SharePoint herunter

Laden Sie Dateien oder E-Mails herunter, die gegen die DLP-Richtlinie in Microsoft Purview verstoßen. Laden Sie diese Datei herunter, oder senden Sie sie per E-Mail aus der Ansicht DLP IR Incident auf Ihren lokalen Computer. Sie können die Dateien für Incidents DLP IR vom Typ Scan-Quelle – Exchange Online, OneDrive und SharePoint herunterladen.

Vorbereitungen
Erforderliche Rolle:

- sn_dlir.admin, sn_dlir.analyst
- Jeder gültige Genehmiger

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**.
2. Öffnen Sie einen DLP-Incident-Datensatz vom Typ Scan-Quelle – Exchange Online, OneDrive oder SharePoint, der aus der Microsoft-Quelle erfasst wird.
3. Klicken Sie auf **Datei herunterladen**.
   Die Datei oder E-Mail, die bzw. die die DLP-Richtlinie auf der Microsoft Purview-Seite verletzt hat, wird auf den lokalen Computer des Anwenders heruntergeladen.

Hinweis:
Der DLP-Administrator kann den Zugriff auf die Aktion **„Datei herunterladen“** steuern, indem er die Einstellung **Sollte das Herunterladen der Datei mit Verstößen des gemeldeten Incidents zulässig sein** auf der Seite „Erweiterte Einstellungen“ deaktiviert. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Domain Separation in MicrosoftMicrosoft Azure Event Hubs DLP-Integration

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe

Support: Standard.

So funktioniert Domain Separation mit der DLP-Integration MicrosoftMicrosoft Azure Event Hubs .

Führen Sie diese Schritte aus, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die MicrosoftMicrosoft Azure Event Hubs DLP-Integrationsvorgänge in der entsprechenden Domäne aus.

Security Operations allgemeine Funktionalität

Jedes Mal, wenn eines der Plugins für die Security Operations -Hauptanwendungen (Security Incident Response, Vulnerability Response, Threat Intelligenceoder Configuration Compliance) aktiviert wird, wird das Plugin Security Support Common aktiviert. Dieses Plugin lädt verschiedene Module, die eine Funktionalität bereitstellen, die allen Security Operations -Anwendungen gemeinsam ist.

Hinweis:
Nur Benutzer mit der Rolle [sn_sec_cmn.admin] können das Modul Security Operations anzeigen und verwenden. Diese Rolle wird geerbt, wenn Ihnen in einer der Security Operations -Anwendungen eine Administratorrolle zugewiesen wird.

Security Operations-Module

Funktion	Beschreibung
Referenzen zur Integration mit Security Operations, Threat Intelligence-Integrationen, Vulnerability Response-Integrationen	In den Anwendungen Security Operations sind mehrere Integrationen enthalten (Security Incident Response, Threat Intelligenceund Vulnerability Response). Dieser Abschnitt enthält Anweisungen zum Aktivieren der -Plugins und zum Konfigurieren ServiceNow von und Drittanbieterintegrationen. Außerdem enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten im Basissystem enthaltenen Integrationen.
Security Operations E-Mail-Verarbeitung	Mit E-Mail-Verarbeitungkönnen Sie die Integration von Informationen aus externen Erkennungssystemen einrichten, Granularität bei der Verarbeitung von Security Operations-Datensätzen bereitstellen, nicht abgeglichene E-Mails verarbeiten und die Duplizierung von Datensätzen verhindern.
Gruppen	• **Filtergruppen** Erstellen und verwenden Sie Filtergruppen, um Datensätze aus einer beliebigen Tabelle in Ihrer -Instanz zu finden. Sie können beispielsweise eine Gruppe mit allen Computern desselben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
	Herstellers erstellen. Sie können auch Configuration Items (CIs) filtern, die ähnliche Schwachstellen aufweisen oder in einen bestimmten IP-Adressbereich für das Subnetz fallen. • **Eskalationen** Sie können einen Eskalationspfad für Security Incidents für Probleme erstellen, die mehr Aufmerksamkeit oder Fachwissen erfordern. Sobald eine Eskalationsgruppe vorhanden ist, wird für jeden Security Incident in dieser Gruppe eine Schaltfläche angezeigt.
Sicherheits-Tags	**Tags**: Sicherheits-Tag-Regeln bieten Filterung für den Zugriff auf Sicherheits-Tags.
Workflows	• **Sicherheitsworkflows anzeigen** Sie können die vielen Workflows anzeigen, die in den Security Operations-Anwendungen enthalten sind. Sie können Workflows aus Vorlagen und im Workflow-Editor erstellen. • **Workflow-Auslöser** Security Operations Workflow-Auslöser enthalten eine Bedingung in einer Tabelle. Alle an den Workflow-Auslöserdatensatz angehängten Workflows werden ausgeführt, wenn die Bedingung erfüllt ist.
Dienstprogramme	• **Ergänzungsdatenzuordnung** Ergänzungsdatenzuordnung wandelt Daten aus XML-, JSON- oder Eigenschaften -Dateien in ServiceNow -Datensätze um. Security Operations -Workflows verwenden Ergänzungsdatenzuordnungen und stellen Ausgabedaten für Security Incidents bereit. • **Feldwertumwandlungen** Wandelt eindeutige Kundenfeldwerte in Feldwerte um, die von der E-Mail-Analyse Security Operations von , Datenanreicherung oder Tabellen mithilfe von Feldzuordnungen erkannt werden. Unterstützt Auswahlfelder, Referenzen und richtet externe Daten an der Standardterminologie und dem Standardformat für Ihren neuen Datensatz aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
	• **Feldzuordnung** Security Operations -Tabellen können anderen Tabellen zugeordnet werden, und verknüpfen so einen Security Incident mit einem Kundenservicefall oder ein Problem mit anderen Teilen des Security Operations -Systems. Sie können beispielsweise ein -Plugin in eine Security Incident Response -Aufgabe integrieren. • **Orchestration bei Bedarf** Während der Analyse Security Incident Response von möchte ein Sicherheitsanalyst möglicherweise eine Aufgabe ausführen, die von einem Security Incident-Workflow gesteuert wird. Führen Sie beispielsweise eine Prozesssicherung für ein bestimmtes CI aus. Dies kann mit bedarfsgesteuerter Orchestrierung erreicht werden. • **Betriebssystemgruppen** N/V • **SecOps-Applikationsregistrierung** N/V
CMDB	**CI-Bezeichnerregeln**: CI-Bezeichner sind Regeln, die zum Suchen eines Configuration Items (CI) in der CMDB verwendet werden, die übereinstimmende Informationen aus einer Drittanbieterintegration enthalten. Diese Regeln definieren die Felder, die übereinstimmende Daten enthalten, und die Rangfolge, nach der sie ausgewertet werden. Der niedrigste **Reihenfolgenwert** wird zuerst ausgewertet.

Erstellen und definieren Sie Filtergruppen in Security Operations

Erstellen und verwenden Sie Filtergruppen, um Datensätze aus einer beliebigen Tabelle in Ihrer -Instanz zu finden. Sie können beispielsweise eine Gruppe mit allen Computern desselben Herstellers erstellen. Sie können auch Configuration Items (CIs) filtern, die ähnliche Schwachstellen aufweisen oder in einen bestimmten IP-Adressbereich für das Subnetz fallen.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.write

Warum und wann dieser Vorgang ausgeführt wird

Filtergruppen können dynamisch aktualisierte Datensätze, eine Reihe von statischen Datensätzen, die nicht anhand von Bedingungen gefiltert werden, oder eine Kombination

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aus dynamisch aktualisierten und statischen Datensätzen enthalten. Einige Filtergruppen sind im Basissystem enthalten, z. B. CI-Ausschlüsse.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Gruppen** > **Filtergruppen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Filtergruppe.
Aktiv	Feld zum Aktivieren der Gruppe.
Beschreibung	Beschreibung für die Filtergruppe.
IP-Adresse für Netzwerk	Die Netzwerk-IP-Adresse, die die IP-Adressen der CIs enthält, die Sie der Gruppe hinzufügen möchten. Dieses Feld wird nur angezeigt, wenn Sie Konfigurationselement [cmdb_ci] oder eine Tabelle ausgewählt haben, die das **Konfigurationselement** erweitert.
Subnetzmaske	Das Subnetz mit den IP-Adressen der CIs, die Sie der Gruppe hinzufügen möchten, z. B. 255.255.255.0. Dieses Feld wird nur angezeigt, wenn Sie Konfigurationselement [cmdb_ci] oder eine Tabelle ausgewählt haben, die das **Konfigurationselement** erweitert.
Tabelle	Die Tabelle, nach der gefiltert werden soll.
Bedingung	Verwenden Sie den Bedingungsgenerator , um die zu filternden Kriterien zu definieren.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Registerkarte **Erweiterte Bedingungen** wird angezeigt.

   Abhängig vom Tabellentyp, den Sie im Feld **Tabelle** angegeben haben, werden wie folgt weitere Registerkarten angezeigt:

Tabelle	Angezeigte Registerkarten
Configuration Item [cmdb_ci] oder eine Tabelle, die die Configuration Item-Tabelle erweitert	**Manuell hinzugefügte CIs** und **übereinstimmende CIs**
Aufgabe [task] oder eine Tabelle, die die Aufgabentabelle erweitert	**Manuell hinzugefügte Aufgaben** und **übereinstimmende Aufgaben**
Eine Tabelle, die nicht mit einem CI oder einer Aufgabe in Zusammenhang steht	**Manuell hinzugefügter Datensatz**

5. So definieren Sie weitere Bedingungen für Ihre Filtergruppe:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Erweiterte Bedingungen**.

b. Fügen Sie eine neue Zeile in die eingebettete Liste **Zusätzliche Filtergruppenbedingungen** ein, um andere vordefinierte Filtergruppen auszuwählen, die Sie mit der zu aktualisierenden Filtergruppe kombinieren möchten.
Wenn die ausgewählte Filtergruppe Datensätze basierend auf einem Referenzfeld filtern soll, wird beim Speichern des aktuellen Datensatzes automatisch ein zugeordnetes Feld ausgewählt.

> **Hinweis:**
> Der Feldwert **„Zugeordnet“** kann nicht in der eingebetteten Liste **„Zusätzliche Filtergruppenbedingungen“** bearbeitet werden. Um das Feld zu ändern, klicken Sie auf das Informationssymbol, um den Datensatz zu öffnen.

c. Klicken Sie auf **Aktualisieren**.

6. So fügen Sie der Filtergruppe manuell weitere CIs oder Aufgaben hinzu:
   a. Klicken Sie auf die Registerkarte **Manuell hinzugefügte CIs** oder **Manuell hinzugefügte Aufgaben**.
   b. Klicken Sie auf **Bearbeiten**.
   c. Wählen Sie die CIs oder Aufgaben aus, die Sie hinzufügen möchten.
   d. Klicken Sie auf **Speichern**.
7. So zeigen Sie die CIs oder Aufgaben an, die Ihren Auswahlkriterien entsprechen:
   a. Klicken Sie auf die Registerkarte **Übereinstimmende CIs** oder **Übereinstimmende Aufgaben**.
   b. Wenn Sie die Kriterien geändert haben, aktualisieren Sie die Liste, indem Sie mit der rechten Maustaste in den Formularheader klicken und **Liste neu laden**auswählen.

Transformation freigegebener Daten

Die Plugins Security Incident Response, Vulnerability Responseund Threat Intelligence haben gemeinsame Funktionen für Beziehungsdaten und Duplizierungsregeln, die zum Importieren externer und interner Informationen in Security Operationsverwendet werden.

E-Mail-Analyse, Duplizierungsregelnund Feldzuordnung nehmen Eingabedaten (eine E-Mail, JSON- oder XML-Datei oder einen Datensatz) und wandeln diese Daten in das richtige Format um, um einen neuen Datensatz zu erstellen. Jede dieser Funktionen ruft Daten auf ihre eigene Weise ab, aber sie werden mit vielen der gleichen Prozesse in den neuen Datensatz umgewandelt.

Beziehungsdaten

Wenn Sie einer zugehörigen Liste (z. B. einem zugeordneten erkennbaren Element in einem Security Incident) Informationen hinzufügen, können Sie einen Beziehungsdatensatz erstellen, der aus einer m2m-Tabelle besteht. Manchmal sind in diesem Beziehungsdatensatz zusätzliche Daten festzulegen. Beispielsweise kann ein erkennbares Element eine Quell-IP sein (im Gegensatz zu einer Ziel-IP). Diese Informationen werden in das Feld **Beziehungsdaten** des **Feldtransformationsformulars,** das von **der E-Mail-Analyse** verwendet wird, oder in eine zugehörige Liste **der Feldzuordnungsfelder** im **Feldzuordnungsformular** eingefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Feld **„Beziehungsdaten“** ist normalerweise leer. Sie wird am häufigsten für IP-Adressen für erkennbare Elemente bei **der E-Mail-Analyse**verwendet.

Sie können Daten aus jedem ServiceNow -Datensatz in einen anderen ServiceNow -Datensatz umwandeln, indem Sie **Feldzuordnungsfelder** in der Funktion **„Feldzuordnung“** verwenden. Beispielsweise um Daten von einem Incident in einen Security Incident oder einen Security Incident in einen PRB umzuwandeln.

Duplizierungsregeln für Security Operations

Verwenden Sie Duplizierungsregeln, um doppelte Datensätze für Sicherheit, Schwachstelle, IoCs usw. zu behandeln.

Duplizierungsregeln haben zwei Zwecke. Sie verhindern, dass zu viele doppelte Datensätze erstellt werden, und geben an, welche Felder im Datensatz aktualisiert werden, wenn ein Duplikat erkannt wird. Es wird nur nach aktiven Duplikaten gesucht. Wenn der Datensatz nicht aktiv ist, z. B. wenn der Incident geschlossen wird, wird jedes neue identische Problem zu einem neuen Incident.

Duplizierungsregeln werden von **E-Mail-Analysen**, **Feldzuordnungen**und **Ergänzungsdatenzuordnungen**verwendet.

Zugehörige Informationen

Erstellen Sie E-Mail-Parser in Security Operations

Ordnen Sie Tabellen Tabellen mit Security Operations-Feldzuordnung zu

Erstellen Sie Duplizierungsregeln in Security Operations

Sie können Duplizierungsregeln verwenden, um neue E-Mails, Ergänzungsdaten oder Feldzuordnungen mit aktiven doppelten Datensätzen zu identifizieren und entsprechend zu verarbeiten.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.write

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Duplizierungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus:

Duplizierungsregel

Feld	Beschreibung
Name	Der Name der Duplizierungsregel.
Tabelle	Tabelle, in der Datensätze erstellt und zur Bestimmung der Duplizierung verwendet werden.
Identifizierende Felder	Wählen Sie eine Reihe von Feldern aus, die auf einen doppelten Security Incident, ein erkennbares Element, eine Schwachstelle usw. hinweisen, wenn die Werte in diesen Feldern identisch sind.
Duplikataktion	Steuert den Umgang mit doppelten E-Mails. Die Auswahlmöglichkeiten lauten wie folgt: **Als untergeordnet erstellen**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Erstellt einen Datensatz als untergeordnetes Element des Originals. Das Feld, das das untergeordnete Element mit dem übergeordneten Element verknüpft, ist das Feld **Übergeordnet**. **Datensätze nicht erstellen oder aktualisieren** (Standard) Führt nichts. Ignoriert Duplikate. **Duplizierten Datensatz aktualisieren** Aktualisiert die Felder im vorhandenen Datensatz wie in **Duplizierungsaktionen angegeben.** **Hinweis:** Wenn Sie **Update duplizierter Datensatz**wählen, wird die zugehörige Liste **Duplizierungsaktionen** angezeigt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Regel zu aktivieren.
Beschreibung	Beschreibt den Zweck und die Anwendung dieser Duplizierungsregel; wann sie verwendet werden sollte, z. B. eine Regel, die für IP-basierte erkennbare Elemente entwickelt wurde, oder Security Incidents von der Firewall.

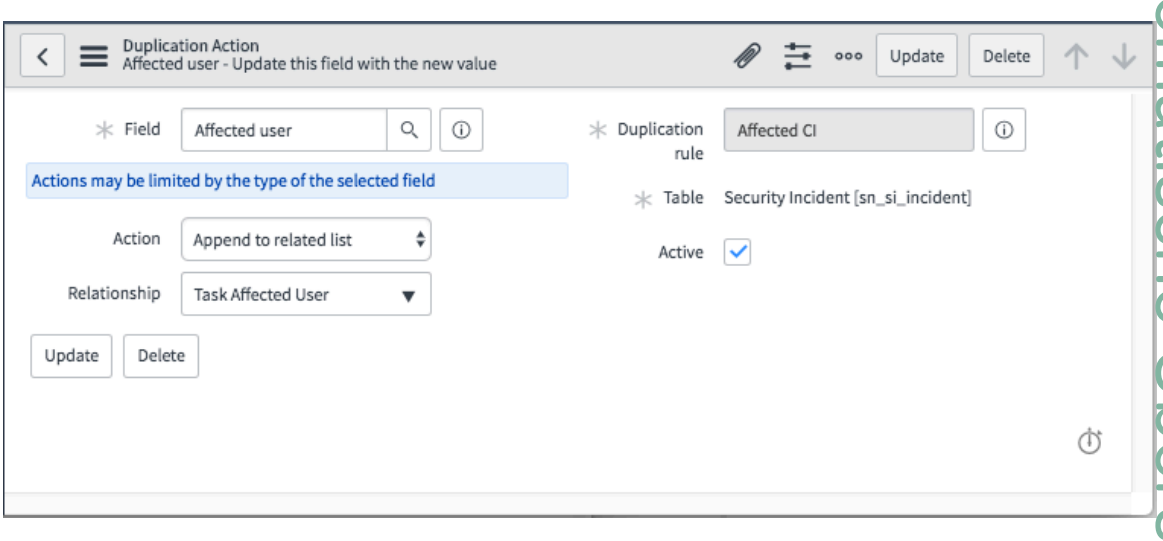
4. Klicken Sie mit der rechten Maustaste auf den Datensatz-Header, und wählen Sie **Speichern**, oder wählen Sie **Aktualisieren**aus.
5. Um Duplizierungsaktionen festzulegen, klicken Sie, wenn Sie **Update duplikatsdatensatz**ausgewählt haben, auf **Neu**, um Duplizierungsaktionen für jedes Feld zu erstellen, das Sie im Incident aktualisieren möchten.
6. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie, um zu beschreiben, wie das Feld aktualisiert wird:

Duplizierungsaktionen

Feld	Beschreibung
Feld	Der Name des Felds, das für die Duplizierungsaktion verwendet werden soll.
Aktion	Die unterstützten Aktionen variieren je nach Feldtyp. Die Auswahlmöglichkeiten lauten wie folgt: **Dieses Feld mit dem neuen Wert aktualisieren** Ersetzt den vorherigen Wert im vorhandenen Datensatz durch diesen Wert. **Neuen Wert an eine kommagetrennte Liste anhängen, falls einzigartig** Behandelt den Wert als Eintrag in einer durch Kommas getrennten Liste und fügt die neuen Daten (falls vorhanden) als neuen Eintrag in dieser Liste hinzu. Wenn die Daten bereits in der Liste enthalten sind, werden sie nicht zweimal hinzugefügt. **Neuen Wert an dieses Feld anhängen** Hängt den neuen Wert an das Ende des vorhandenen Texts im Feld an. **Einmal zu einem Zählerfeld hinzufügen** Addiert eins zum numerischen Feld. **Feld auf heute einstellen**

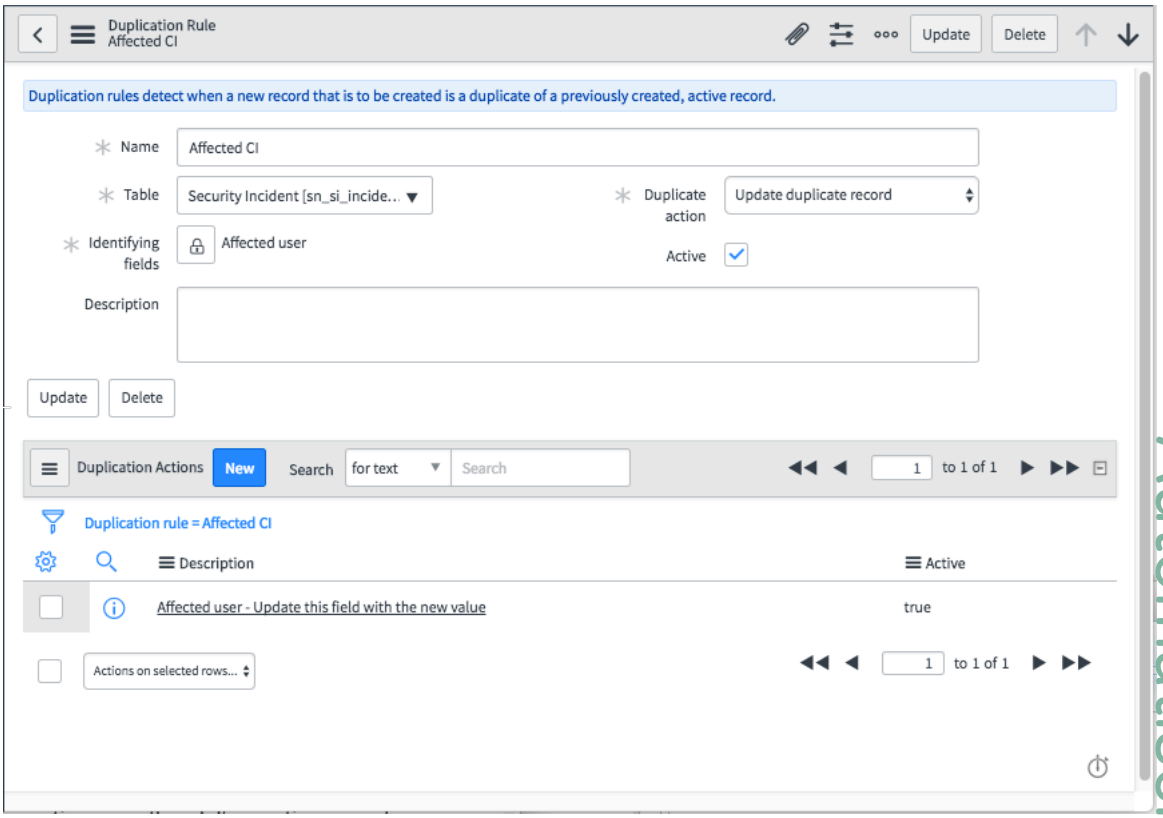
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Legt das Feld auf das aktuelle Datum und die aktuelle Uhrzeit fest. **An zugehörige Liste anhängen** Fügt den zugehörigen Datensatz mit diesem Wert der zugehörigen Liste des aktuellen Datensatzes hinzu. Wird angezeigt, wenn eine Viele-zu-Viele-Tabelle mit einer Spalte des gleichen Typs vorhanden ist, die mit der zu aktualisierenden Tabelle verknüpft ist. Beispiel: **Betroffenes CI** oder **Betroffener Anwender**.
Beziehung	[Optional] Dieses Feld wird nur angezeigt, wenn die Aktion **An zugehörige Liste** anhängen ausgewählt ist. Dies ist der Name der zugehörigen Liste, die Sie dieser Regel zuordnen möchten.
Duplizierungsregel	Regel, zu der diese Aktion gehört.
Tabelle	Tabelle, in der Datensätze erstellt werden. Wird nur zur Information angezeigt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Aktion zu aktivieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Absenden**.



Security Operations E-Mail-Verarbeitung

Mit E-Mail-Verarbeitungkönnen Sie die Integration von Informationen aus externen Erkennungssystemen einrichten, Granularität bei der Verarbeitung von Security Operations-Datensätzen bereitstellen, nicht abgeglichene E-Mails verarbeiten und die Duplizierung von Datensätzen verhindern.

E-Mail-Verarbeitung besteht aus den folgenden Funktionen:

Funktion	Beschreibung
E-Mail-Analyse	Generieren Sie neue Security Operations -Datensätze aus externen System-E-Mails.
Duplizierungsregeln	Identifiziert neue E-Mails mit bekannten Incidents und verarbeitet sie entsprechend.
Eigenschaften	Gibt Accounts an, die in E-Mail-Analyse als Eingabe für Sicherheit, Schwachstelle und IoCs verwendet werden. Sorgt für Granularität bei der Verarbeitung von Security Operations -Datensätzen.
Nicht übereinstimmende E-Mails	Listet E-Mails auf, die keinem Security Operations -Datensatz entsprechen.

E-Mail-Eigenschaften für Security Operations

E-Mail Eigenschaften geben Sie an, welche Posteingänge als Eingabe in E-Mail-Analyse für den Import von Informationen aus externen Erkennungssystemen verwendet werden, um Datensätze für Sicherheit, Schwachstelle und IoCs zu erstellen. Sie können einen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

allgemeinen Account für alle externen Erkennungssysteme oder individuelle E-Mail-Accounts für Security Incident Response, Threat Intelligenceoder Vulnerability Responseeinrichten.

Erstellen Sie Security Operations -E-Mail-Eigenschaften

Sie können E-Mail-Adressen für Berichte angeben und automatische E-Mail-Verhaltensweisen mithilfe von E-Mail Eigenschaftensteuern.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Richten Sie externe Erkennungstools ein, um E-Mails an Ihren Posteingang zur Analyse von E-Mails zu senden.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Eigenschaften**.
2. Geben Sie entsprechend Ihre Empfängerpostfächer ein:
   Dies sind eingehende E-Mail-Adressen, die von **der E-Mail-Analyse**verarbeitet werden, und nicht **eingehende Aktionen**.

Eigenschaften zum Analysieren von E-Mails

Feld	Beschreibung
Postfach für Security Operations Tools	Vollständige E-Mail-Adresse für Security Operations. Beispiel:secops_support@yourcompany.com.
Postfach für Security Incident-Tools	Vollständige E-Mail-Adresse für Security Incident Response. Beispiel: sir_support@ihr.unternehmen.com.
Postfach für Vulnerability Response Tools	Vollständige E-Mail-Adresse für Vulnerability Response. Beispiel: Vuln_resp@yourcompany.com.
Postfach für Threat Intelligence Tools	Vollständige E-Mail-Adresse für Threat Intelligence. Beispiel: Threat_Intel@IhrUnternehmen.com.

3. Klicken Sie auf **Speichern**.

Security Operations E-Mail-Analyse

Generieren Sie neue Security Operations -Datensätze aus externen Erkennungssystemen mit E-Mail-Analyse. Diese Funktion bietet eine Methode zur Integration von Informationen aus externen Tools wie Malware-Erkennung, Schwachstellen-Erkennung, Firewalls, Threat Intelligence und mehr.

Wie E-Mails analysiert werden

Jedes System, das eine E-Mail senden kann, kann Security Operations -Datensätze erstellen, z. B. Security Incidents, Anforderungen, angreifbare Elemente, Schwachstellen, erkennbare Elemente von Security Incidents, Angriffsmethoden und vieles mehr.

Alle Security Operations -Plugins (Security Incident Response, Threat Intelligenceund Vulnerability Response) haben eine Eigenschaft (**email_to**), die die E-Mail-Adresse definiert, an die externe Integrationen E-Mails senden sollen, damit sie von den E-Mail-Parsern analysiert werden. Siehe **E-Mail-Verarbeitung** > **Eigenschaften** , um weitere Informationen zu erhalten.

E-Mails, die an eine der E-Mail-Adressen Security Operations gesendet werden, werden in einer E-Mail-Ereignistabelle gespeichert. Diese E-Mails werden verarbeitet, um zu bestimmen, ob sie mit einem E-Mail-Parser übereinstimmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mails mit einer Übereinstimmung werden gekennzeichnet, und die Transformations- und Duplizierungsregeln erstellen oder aktualisieren einen Security Operations -Datensatz. Die E-Mail wird mit diesem Datensatz verknüpft und als Übereinstimmunggekennzeichnet.

E-Mails, die nicht übereinstimmen, werden in Nicht übereinstimmende E-Mails als Datensatz Security Operations aufgeführt. Sie können überprüft werden, um E-Mail-Parser für die Verarbeitung dieser E-Mails zu erstellen. Mit der Aktion Erneut verarbeiten können Sie die nicht abgeglichene E-Mail erneut durch die Parser ausführen. Das ursprüngliche E-Mail-Protokoll ist mit diesem Datensatz verknüpft.

Die Duplizierungsregeln für die E-Mail-Transformation verwalten mehrere E-Mails, die sich auf dasselbe Problem beziehen. Diese Regeln definieren, was einen doppelten Datensatz ausmacht, und können verhindern, dass doppelte Datensätze erstellt werden. Wenn ein Duplikat erkannt wird, gibt die Regel an, welche Aktion ausgeführt werden soll: keine Aktion (keinen neuen Datensatz erstellen), neuen Datensatz als untergeordneten Datensatz des vorhandenen Datensatzes erstellen oder den vorhandenen Datensatz aktualisieren. Beim Aktualisieren gibt die Duplikatregel an, welche Felder im vorhandenen Datensatz aktualisiert werden.

Hinweis:
Ein Security Operations -E-Mail-Parser funktioniert in Verbindung mit eingehenden Plattformaktionen und ersetzt diese nicht. Das Festlegen von Werten für indirekte Felder (z. B. **sys_journal_field** -Einträge) wird nicht unterstützt.

Standardmäßig werden E-Mail-Ereignisse nach 30 Tagen gelöscht.

Mehrere Datensätze

Externe Erkennungssysteme (Malware-Detektoren, Schwachstellen usw.) können E-Mails senden, die mehrere Elemente gleichzeitig melden. Der E-Mail-Parser unterstützt Trennzeichen innerhalb der E-Mail.

Beispielsweise könnte Ihnen ein Malware-Detektor einen E-Mail-Bericht über alle Systeme in Ihrem Netzwerk senden, die von einer bestimmten Malware infiziert sind, wobei zuerst Informationen zur Malware angezeigt werden, gefolgt von einer Liste der betroffenen Systeme.

Beispiel für schädliche E-Mail

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 2038028509826092349O723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==========
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==========
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==========
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

Wenn in diesem Beispiel das **Datensatztrennzeichen** in Ihrer **E-Mail-Transformation**auf
==========
Dadurch wird für jedes der drei betroffenen Systeme ein Security Incident erstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Der Headerabschnitt wurde erkannt, weist jedoch keine betroffenen Systeme auf. Daher wird er in allen drei Datensätzen verwendet und erstellt keinen vierten Datensatz.

Feldtransformationen rufen Daten aus jedem Abschnitt ab. Wenn etwas im Header oder Footer der E-Mail für alle Datensätze gilt, z. B. Malware-Hash, Malware-Name und Typ in diesem Beispiel, sollte die Feldtransformation für sie **die Suche nach Wert** auf einen Wert festlegen, der innerhalb des E-Mail-Textes sucht, entweder **At Beginn einer Zeile im E-Mail-Text** oder **an einer beliebigen Stelle im E-Mail-Text**.

Feldtransformationenmüssen so festgelegt werden, **dass am Anfang einer Zeile innerhalb des Datensatzabschnitts** oder **Abschnitts** nach Daten gesucht wird, die in jedem Abschnitt definiert sind, z. B. System, IP-Adresse oder Status. Die Datensatzabschnittsoptionen sind nur verfügbar, wenn in der E-Mail-Transformation ein Datensatztrennzeichen definiert ist.

Beim Analysieren einer E-Mail mit definiertem Trennzeichen werden Datensätze nur für Abschnitte erstellt, die mindestens ein abschnittsspezifisches Datenelement enthalten.

In diesem Beispiel werden drei Datensätze erstellt, obwohl vier Abschnitte definiert sind. Der erste Abschnitt ist ein Header, in dem alles fehlt, was nur für ein System spezifisch ist. Wenn eines der Felder im ersten Abschnitt ausgefüllt würde (System, IP oder Status), wird auch für diesen Abschnitt ein Datensatz erstellt.

Zugehörige Informationen

Erstellen Sie E-Mail-Parser in Security Operations

Security Operations Zuordnung von Ergänzungsdaten

Security Operations Feldzuordnung

Erstellen Sie E-Mail-Parser in Security Operations

E-Mail-Analyse erstellt aus Ihrer E-Mail Security Operations -Datensätze für Sicherheit, Schwachstelle und erkennbare Elemente, um die Reaktion auf Bedrohungen und die Korrektur zu beschleunigen.

Vorbereitungen

- Richten Sie externe Erkennungstools ein, um E-Mails an eine zentrale E-Mail-Adresse zu senden.
- Legen Sie die E-Mail-Adresse in den Security Operations-Eigenschaften fest. Weitere Informationen finden Sie unter Erstellen Sie Security Operations -E-Mail-Eigenschaften.
- Weisen Sie dieser E-Mail-Adresse ein Anwenderkonto zu, und gewähren Sie diesem Anwender Sicherheitszugriffssteuerungen, um die E-Mail-Ereignisdatensätze zu erstellen und zu aktualisieren.
- Halten Sie eine Kopie der relevanten E-Mail aus Ihrem externen Erkennungstool bereit.
- Entscheiden Sie, welche Art von Datensatz Sie erstellen möchten (Security Incident, Schwachstellendatensatz, Aufgabe usw.). Diese Auswahl bestimmt die Tabelle, die Sie auswählen.

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Analyse**.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die entsprechenden Felder im Formular aus.

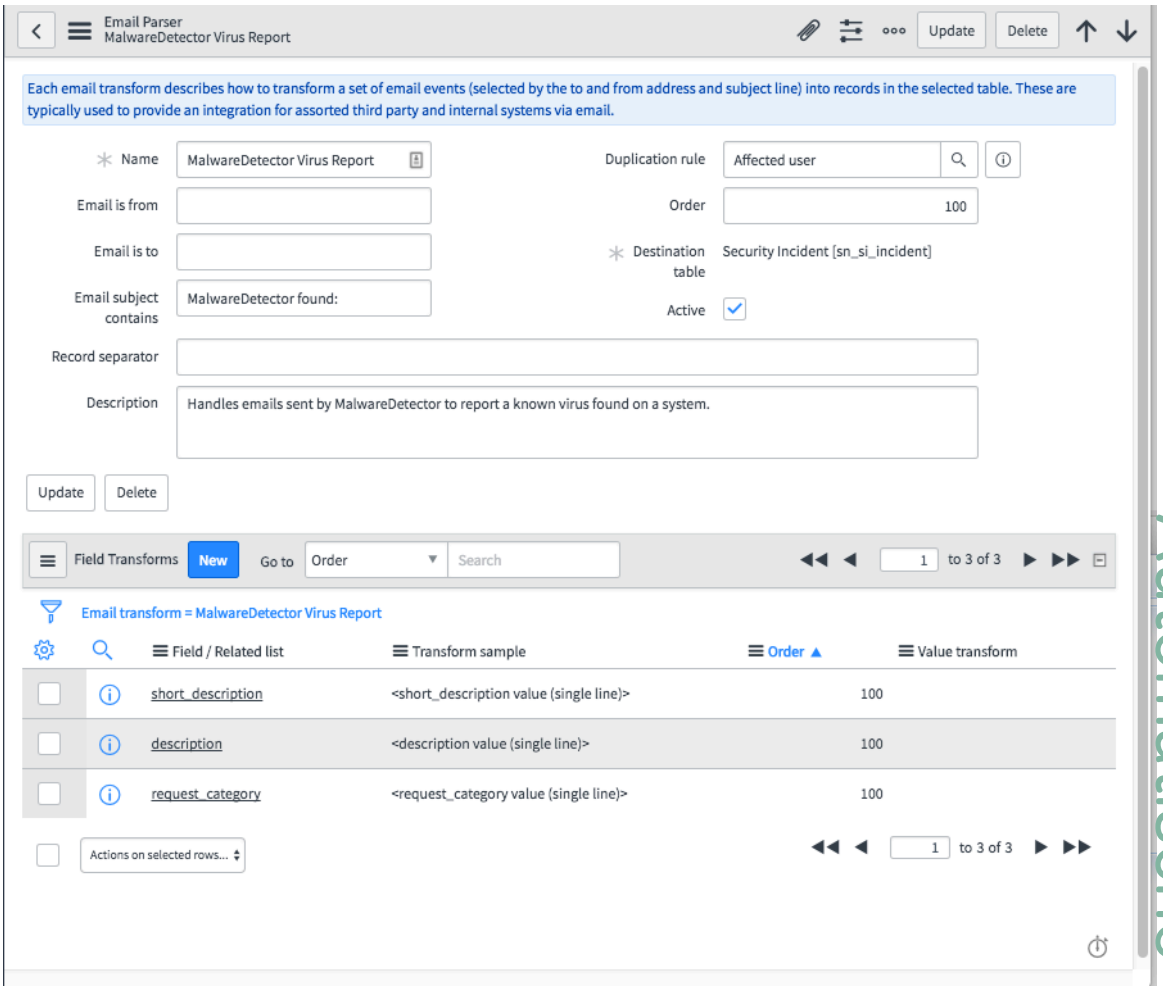
Hinweis:
Wenn mehr als ein Feld angegeben ist, müssen alle Felder mit der E-Mail-Adresse übereinstimmen, um einen Datensatz zu erstellen.

E-Mail-Parser

Feld	Beschreibung
Name	Der Name des E-Mail-Parsers.
E-Mail ist von	Wenn ausgefüllt, werden nur E-Mails von dieser Adresse von diesem E-Mail-Parser umgewandelt.
E-Mail an	Wenn ausgefüllt, werden nur E-Mails von dieser Adresse von diesem E-Mail-Parser umgewandelt.
E-Mail Betreff enthält	Wenn ausgefüllt, werden nur E-Mails von diesem E-Mail-Parser transformiert, bei denen der Betreff diesen Ausdruck enthält.
Duplizierungsregel	Steuert, wie doppelte E-Mails für alle E-Mails behandelt werden, die von dieser Transformation verarbeitet werden. Weitere Informationen finden Sie unter Transformation freigegebener Daten.
Bestellung	In welcher Reihenfolge die Transformationen berücksichtigt werden sollen. Die erste übereinstimmende E-Mail-Transformation wird verwendet. Normalerweise möchten Sie die spezifischsten E-Mail-Parser in den niedrigeren Nummern mit einem Fallback einrichten. Geben Sie E-Mail-Parsern für Ausweichkontakt höhere **Auftragsnummern**, damit sie ausgeführt werden, wenn keine Übereinstimmung mit anderen Elementen vorliegt. Der Standardwert ist 100. Wenn alles übereinstimmt, wird der spezifischste E-Mail-Parser (entspricht **von**, **bis**und **Betreff**) verwendet.
Zieltabelle	Die Tabelle, in der Sie Datensätze erstellen möchten.
Aktiv	Gibt an, ob diese Transformation aktiv ist, verwendet wird oder nicht aktiv ist. Wenn diese Option deaktiviert ist, werden keine E-Mails mit diesem Code umgewandelt.
Datensatztrennzeichen	Wenn von diesem E-Mail-Parser verarbeitete E-Mails mehrere Datensätze erstellen, enthält dieses Feld das Trennzeichen zwischen den Informationen für diese Datensätze. Weitere Informationen finden Sie unter Security Operations E-Mail-Analyse.
Beschreibung	Beschreibung des E-Mail-Parsers, des verwendeten Tools, des Zwecks usw.

4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie **Speichern**aus.
Die Registerkarte **Feldtransformationen** wird angezeigt. Diese Registerkarte zeigt, wie einzelne Felder in der Zieltabelle basierend auf dem E-Mail-Inhalt festgelegt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Um **Feldtransformationen**hinzuzufügen, führen Sie die folgenden Schritte aus.
   a. Klicken Sie auf der Registerkarte **Feldtransformationen** auf **Neu**.
   b. Füllen Sie die entsprechenden Felder im Formular aus.

Option	Bezeichnung
Feld	**Beschreibung**
Wert in einem Feld oder einer zugehörigen Liste speichern	Wählen Sie aus, wo der Wert gefunden werden soll. Zur Auswahl stehen: ○ Speichern Sie den Wert in einem Feld im neuen Datensatz ○ Verknüpfung mit diesem Wert in einer zugehörigen Liste erstellen ○ Verknüpfung mit diesem Wert erstellen und neuen Datensatz erstellen, wenn kein übereinstimmender Datensatz vorhanden ist **Hinweis:** Wenn die Zieltabelle keine zugehörigen Listen enthält, wird dieses Feld nicht angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Feld	Wählen Sie das Feld aus, das mit diesem Wert ausgefüllt werden soll. **Hinweis:** Bei Auswahlfeldern werden Übereinstimmungen mit vorhandenen Auswahlmöglichkeiten anhand der zugrunde liegenden Auswahlbezeichnung oder des zugrunde liegenden Auswahlwerts vorgenommen. Wenn keine Übereinstimmung gefunden wird, wird das Feld festgelegt, aber der Auswahlliste wird kein neuer Eintrag hinzugefügt. Weitere Informationen finden Sie unter Auswahllisten . Für Referenzfelder wird ein Eintrag nur festgelegt, wenn ein Wert gefunden wird, der dem Anzeigenamen des Datensatzes entspricht oder eine gültige sys_id gefunden wird. Weitere Informationen finden Sie unter Referenzfelder .
Zugehörige Liste	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“auf „Mit diesem Wert in einer zugehörigen Liste verknüpfen“** oder **„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhanden ist**. Gibt dieses Feld die zugehörige Liste an, der Informationen hinzugefügt werden sollen.
Wertfeld	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“auf „Mit diesem Wert in einer zugehörigen Liste verknüpfen“** oder **„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhanden ist**, gibt dieses Feld das Feld innerhalb der im zugehörigen angezeigten Tabelle an Liste Es wird verwendet, um einen vorhandenen Datensatz zu suchen und zu finden. Lautet Ihre zugehörige Liste beispielsweise **„Betroffene CIs“**, kann dieses Feld **„Name“** oder **„Vollständig qualifizierter Domänenname“**oder ein beliebiges anderes Feld im CI-Datensatz enthalten, das zum Suchen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	des CI verwendet werden soll, das der Liste **„Betroffene CIs“** hinzugefügt wurde.
Beziehungsdaten	Wenn **Wert in einem Feld oder einer zugehörigen Liste speichernauf Mit diesem Wert in einer zugehörigen Liste verknüpfen**festgelegt ist, wird ein Datensatz erstellt, um diesen Datensatz (z. B. einen Security Incident) mit dem Wert (ein CI, ein erkennbares Element usw.) zu verknüpfen.). Dieses Feld gibt zusätzliche Informationen (Feld-Wert-Paare) an, die dem Verknüpfungsdatensatz hinzugefügt werden sollen. Wenn Sie beispielsweise ein erkennbares Element für eine Quell-IP hinzufügen, geben Sie an, dass diese IP die Quelle und nicht die Ziel-IP ist. Verwenden Sie für mehrere Werte ein ^-Trennzeichen, z. B. type= Source IP^Active=true.
Neue Datensatzdaten	Wenn **„Wert speichern“ in einem Feld oder einer zugehörigen Liste** auf **„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein über einstimmender Datensatz vorhanden ist**. Wenn kein zugehöriger Datensatz gefunden wird, der dem analysierten Wert entspricht, wird ein Datensatz erstellt. Dieses Feld gibt die statischen Daten an, die diesem Datensatz hinzugefügt werden sollen. (Für **betroffene CIs**wird ein CI-Datensatz erstellt, wenn keine übereinstimmenden CIs gefunden werden.) In diesem Fall wird der in der E-Mail gefundene Wert auf das Feld **Wert** im CI-Datensatz festgelegt. Sie können zusätzliche Daten festlegen – einen Hinweis, der angibt, warum das CI erstellt wurde, einige Informationen darüber, mit welcher Art von CIs Sie arbeiten, usw. Ein Beispiel wäre: description=Created by Malware Scanner email parser^type=autodetect.
Suche nach Wert	Wählen Sie den Ort in der zu suchenden E-Mail aus. Zur Auswahl stehen: ○ **Am Anfang einer Zeile im E-Mail-Text** ○ **Irgendwo im E-Mail-Text** ○ **In der E-Mail-Betreffzeile** ○ **Immer der statische Wert**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Wenn Sie ein **Datensatztrennzeichen**definiert haben, ermöglichen Ihnen weitere Optionen (**Beliebig im Datensatzabschnitt** und **Am Anfang einer Zeile im Datensatzabschnitt),** nur innerhalb des aktuellen Abschnitts anstatt im gesamten E-Mail-Text zu suchen (weitere Informationen finden Sie unter Security Operations E-Mail-Analyse. Informationen. Informationen, die sich in einem Header oder Footer befinden und für alle Datensätze gelten, werden im gesamten E-Mail-Text gesucht. Die Informationen, die sich zwischen Datensätzen unterscheiden, werden nur innerhalb des Abschnitts gesucht.
Werttrennzeichen	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“auf „Mit diesem Wert in einer zugehörigen Liste verknüpfen“** oder **„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhanden ist**. Gibt dieses Feld das Trennzeichen an, das für Listen von Elementen verwendet werden soll. Zum Beispiel ein Komma oder Semikolon, wenn die Daten aus der E-Mail eine Liste von IP-Adressen sind.
Wertepräfix	Der Text, der immer vor dem Wert steht, der in diesem zu extrahierenden Feld platziert ist.
Ende des Werts	Wählen Sie aus, was das Ende des Werts angibt. Auswahlmöglichkeiten: **Zeilenende**, **E-Mail-Ende** (zieht den gesamten verbleibenden Text in der E-Mail ein), **Bis** (wird angehalten, wenn der angegebene Text gefunden wird) oder **Bis** (wird angehalten, wenn der angegebene Text gefunden wird).
Wertesuffix	Wenn das **Ende des Werts** auf **Bis**festgelegt ist, gibt dieses Feld an, welcher Text immer auf den in diesem Feld angegebenen Wert folgt. Beispiel: Suchen Sie nach einem Wert, der nach „Betroffener Computer ist“ und vor „.“ kommt. analysiert „AB123“ aus „Der dementierte Häschenvirus wurde gefun–

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	den“. Der betroffene Computer ist AB123. Geschätzte Zeit der Ansteckung war 15:45 Uhr“ in einer E-Mail.
Wertumwandlung	Wählen Sie den anzuwendenden Feldtransformationseintrag. Konvertiert den in der E-Mail gefundenen Wert in einen anderen Wert, der zum Ausfüllen von Auswahlfeldern, gelegentlich Referenz- und anderen Feldern verwendet wird.
Bestellung	Die Reihenfolge, in der die Feldtransformationen ausgeführt werden, vom niedrigsten zum höchsten. Zuerst wird versucht, eine Feldtransformation mit einem Reihenfolgeeintrag von 100 durchzuführen. Nur wenn diese Feldtransformation keinen Wert findet, wird ein Feldtransformation mit einer höheren Reihenfolge (200) im selben Feld ausgeführt.
E-Mail-Transformation	Die Transformation, zu der diese Feldtransformation gehört.
Zieltabelle	Zieltabelle der E-Mail-Transformation. Sie enthält Informationsdaten aus der E-Mail-Transformation.
Aktiv	Standardmäßig ist diese Option aktiviert. Wenn diese Option aktiviert ist, ist die Feldtransformation aktiviert. Deaktivieren Sie dieses Kontrollkästchen, um die Feldtransformation zu deaktivieren.

a. Klicken Sie auf **Absenden**.
Der neue Datensatz wird verwendet, um die Informationen in der E-Mail in einem neuen Datensatz zu analysieren.

Zugehörige Informationen

Erstellen Sie Duplizierungsregeln in Security Operations

Erstellen Sie Werttransformationen für das Feld Security Operations .

Definieren Sie E-Mail-Benachrichtigungen Vulnerability Response .

Bearbeiten Sie E-Mail-Datensätze in Security Operations

Fügen Sie in Ihren vorhandenen E-Mail-Ereignis-Datensätzen Transformationen hinzu, oder erstellen Sie Transformationen.

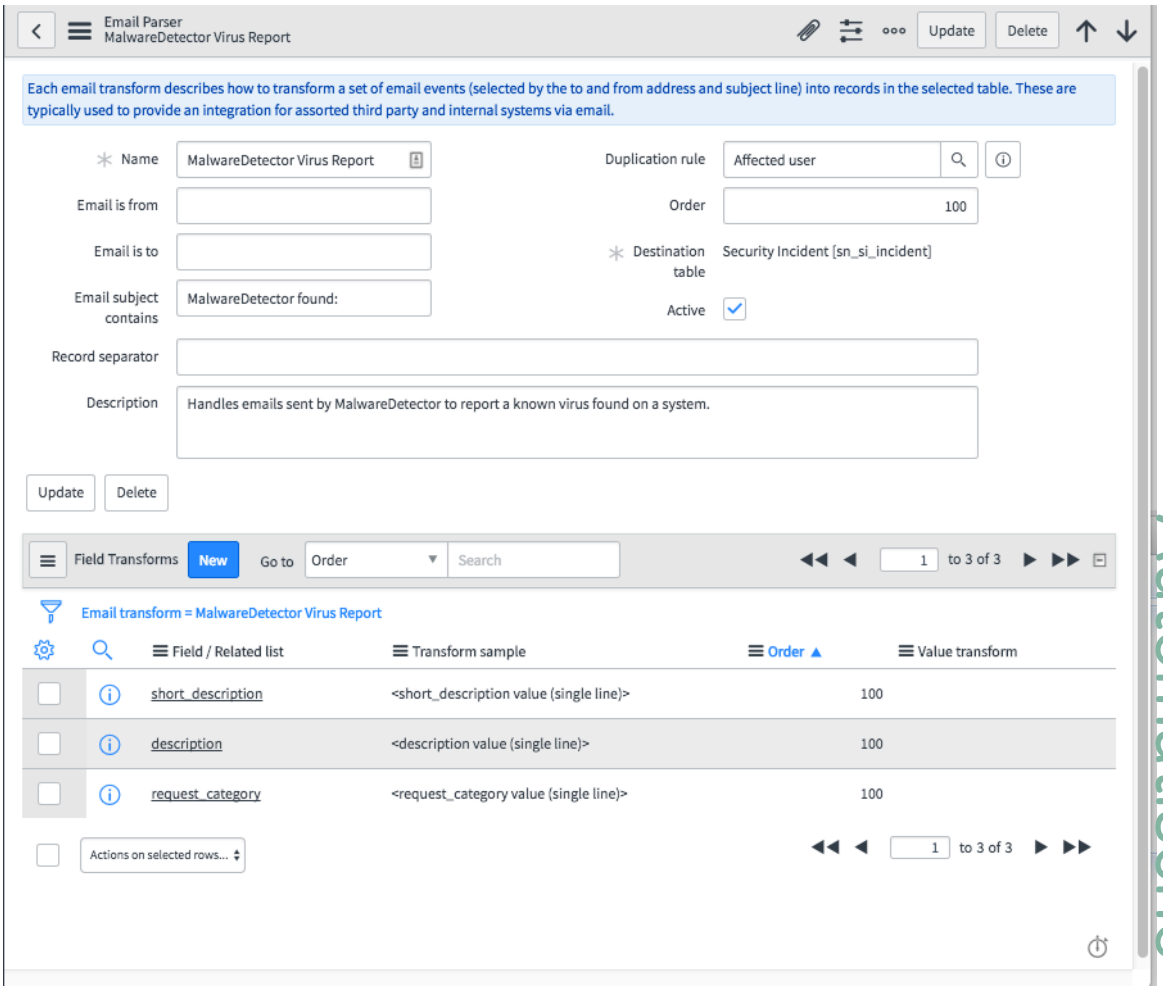
Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Analyse**.
2. Klicken Sie zum Bearbeiten auf den E-Mail-Parser.
   Wenn der Datensatz schreibgeschützt ist, klicken Sie auf den Link hier in der Header-Nachricht.
   Sie gelangen zum bearbeitbaren Formular der Transformation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Bearbeiten Sie die Felder entsprechend.
4. Klicken Sie zum Bearbeiten von **Feldtransformationen**in das Feld, und ändern Sie entsprechend.
5. Klicken Sie auf **Aktualisieren.**

Nicht abgeglichene Security Operations E-Mail-Ereignisse

Bei E-Mail-Ereignisse, die nicht mit einem E-Mail-Parser übereinstimmen, ist die Kennzeichnung „Übereinstimmend“ deaktiviert. Sie können diese E-Mail-Ereignisdatensätze in der Liste Nicht übereinstimmende E-Mails anzeigen, um externe Erkennungssysteme anzuzeigen, deren E-Mails noch nicht analysiert wurden.

Beim Erstellen von E-Mail-Parsern können Sie versuchen, das E-Mail-Ereignis (aus dem Formular oder der Liste) erneut zu verarbeiten, um einen neuen E-Mail-Parser zu validieren.

Nicht abgeglichene Security Operations-E-Mails anzeigen und erneut verarbeiten

Sie können Nicht übereinstimmende E-Mails für eingestellte Filter oder als Kandidaten für einen neuen Filter überprüfen, um die Rate, mit der Sie E-Mail-Bedrohungen erkennen, aufrechtzuerhalten oder zu verbessern.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.read

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Nicht übereinstimmende E-Mails**.
   Wenn E-Mail-Adressen ohne Übereinstimmung gefunden wurden, werden sie aufgelistet.
2. Das Formular enthält folgende Felder:

Sicherheits-E-Mail-Ereignisse

Feld	Beschreibung
Von	E-Mail-Adresse des Absenders.
An	E-Mail-Adresse der Empfänger.
Betreff	Betreffzeile in der E-Mail.
Textkörper	Inhalt des Textkörpers der E-Mail.
Abgleich	Gibt an, ob mit diesem E-Mail-Ereignis abgeglichen wurde.

3. Um diese E-Mail erneut zu verarbeiten, erstellen Sie einen E-Mail-Datensatz, oder bearbeiten Sie einen vorhandenen E-Mail-Datensatz so, dass er den Informationen in dieser E-Mail entspricht.
   Weitere Informationen finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
4. Navigieren Sie zurück zu **Security Operations** > **Nicht übereinstimmende E-Mails**.
5. Klicken Sie auf **„E-Mail-Ereignis erneut verarbeiten“,** um zu versuchen, diese E-Mail zu verarbeiten. Sie kehren zur Hauptliste Nicht übereinstimmende E-Mails zurück. Wenn der neue E-Mail-Datensatz übereinstimmt, wird das E-Mail-Ereignis nicht mehr in der Liste angezeigt. Eine Nachricht gibt an, ob eine Übereinstimmung gefunden wurde oder nicht.

Security Operations Feldzuordnung

Security Operations -Tabellen können anderen Tabellen zugeordnet werden, und verknüpfen so einen Security Incident mit einem Kundenservicefall oder ein Problem mit anderen Teilen des Security Operations -Systems.

Die Feldzuordnung definiert die Zuordnung, die verwendet wird, wenn ein Datensatz aus der Quelltabelle zum Erstellen eines neuen Datensatzes in der Zieltabelle verwendet wird. Diese Zuordnungen werden in der Regel verwendet, um einen Security Incident aus einem anderen Datensatz zu erstellen. Sie definieren, welche Felder in einem Security Incident in ein neues Problem eingefügt werden oder welche Felder aus einem vorhandenen Kunden-Incident einen neuen Security Incident füllen.

Ordnen Sie Tabellen Tabellen mit Security Operations-Feldzuordnung zu

Security Operations bietet Ihnen eine präzisere Feldzuordnungsgranularität, sodass Sie eine Tabelle Security Operations jeder anderen Tabelle zuordnen können.

Vorbereitungen

Erforderliche Rolle:sec_cmn.write

Prozedur

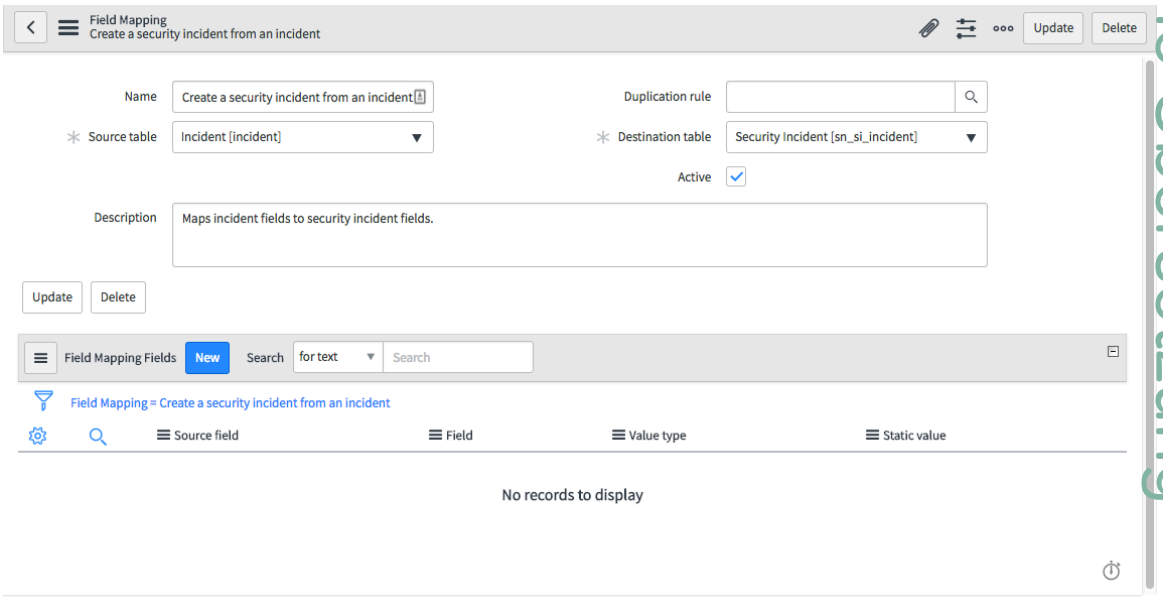
1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldzuordnung

Feld	Beschreibung
Name	Der Name der Feldzuordnung.
Quelltabelle	Die Tabelle, die die Daten bereitstellt, die zum Erstellen eines Datensatzes in der Zieltabelle verwendet werden.
Duplizierungsregel	Steuert den Umgang mit Quelldatensätzen, die einen doppelten Datensatz generieren würden. Weitere Informationen finden Sie unter Transformation freigegebener Daten.
Zieltabelle	Die Tabelle, in der neue Datensätze erstellt werden.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Zuordnung zu aktivieren. **Hinweis:** Es kann jeweils nur eine Zuordnung zwischen Tabellen aktiv sein. Wenn zwei Karten dieselben Tabellen enthalten, wird die ältere Version automatisch deaktiviert.
Beschreibung	Beschreibung für die Feldzuordnung.

4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie **Speichern**aus.
Die Registerkarte**Feldzuordnungsfelder** wird angezeigt. Dieser Datensatz definiert, welche Daten im Zielfeld in Datensätzen platziert werden, die von dieser Feldtransformation erstellt wurden.



5. Klicken Sie auf **Neu**.

6. Füllen Sie die entsprechenden Felder im Formular aus.

Option	Bezeichnung
Feld	**Beschreibung**
Wert in einem Feld oder einer zugehörigen Liste speichern	Wählen Sie aus, wo der Wert gefunden werden soll. Zur Auswahl stehen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	○ Neuen Wert in einem Feld im Datensatz hinzufügen ○ Verknüpfung mit diesem Wert in einer zugehörigen Liste erstellen ○ Verknüpfung mit diesem Wert erstellen und Datensatz erstellen, wenn kein übereinstimmender Datensatz vorhanden ist **Hinweis:** Wenn die Zieltabelle keine zugehörigen Listen enthält, wird dieses Feld nicht angezeigt.
Feld	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“** auf **„Neuen Wert in ein Feld im Datensatz hinzufügen“** festgelegt ist, gibt dieses Feld das auszufüllende Feld an. **Hinweis:** Bei Auswahlfeldern werden Übereinstimmungen mit vorhandenen Auswahlmöglichkeiten anhand der zugrunde liegenden Auswahlbezeichnung oder des zugrunde liegenden Auswahlwerts vorgenommen. Wenn keine Übereinstimmung gefunden wird, wird das Feld festgelegt, aber der Auswahlliste wird kein neuer Eintrag hinzugefügt. Weitere Informationen finden Sie unter Auswahllisten. Für Referenzfelder wird ein Eintrag nur festgelegt, wenn ein Wert gefunden wird, der dem Anzeigenamen des Datensatzes entspricht oder eine gültige `sys_id` gefunden wird. Weitere Informationen finden Sie unter Referenzfelder.
Zugehörige Liste	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“auf „Mit diesem Wert in einer zugehörigen Liste verknüpfen“** oder **„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhanden ist**. Gibt dieses Feld die zugehörige Liste an, der Informationen hinzugefügt werden sollen.
Wertfeld	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“auf „Mit diesem Wert in einer zugehörigen Liste verknüpfen“** oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhan den ist, gibt dieses Feld das Feld innerhalb der im zugehörigen angezeigten Tabelle an Liste, die zum Suchen und Finden eines vorhandenen Datensatzes verwendet wird. Wenn Ihre zugehörige Liste beispielsweise **Betroffene CIs**lautet, kann dieses Feld **Na me** oder **Vollständig qualifizierter Domänen name**enthalten. Oder jedes andere Feld im CI-Datensatz, das zum Suchen des CI ver–wendet werden soll, wird der Liste **Betroffe ne CIs** hinzugefügt.
Beziehungsdaten	Wenn **Wert in einem Feld oder einer zugehö rigen Liste speichernauf Mit diesem Wert in einer zugehörigen Liste verknüpfen**festge–legt ist, wird ein neuer Datensatz erstellt, um diesen Datensatz (z. B. einen Security Incident) mit dem Wert (ein CI, ein erkenn–bares Element usw.) zu verknüpfen). Die–ses Feld gibt alle zusätzlichen Informatio–nen (Feld-Wert-Paare) an, die diesem Ver–knüpfungsdatensatz hinzugefügt werden sollen. Wenn Sie beispielsweise ein erkenn–bares Element für eine Quell-IP hinzufü–gen, können Sie angeben, dass diese IP die Quelle und nicht die Ziel-IP ist. Verwenden Sie für mehrere Werte ein ^-Trennzeichen, z. B. type= Source IP^active=true.
Neue Datensatzdaten	**Wenn „Wert speichern“ in einem Feld oder einer zugehörigen Liste** auf **„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein überein stimmender Datensatz vorhanden ist.**Wenn kein zugehöriger Datensatz gefunden wird, der dem analysierten Wert entspricht, wird ein neuer Daten-satz erstellt. Dieses Feld gibt die statischen Daten an, die diesem Datensatz hinzugefügt werden sol-len. Beispiel: Wenn das CI für **„Betroffene CIs**“ nicht gefunden werden kann, zeigt diese Einstellung an, dass ein neues CI erstellt wird. Der im Quelldaten-satz gefundene Wert wird auf das Feld **„Wert“** im CI-Datensatz festgelegt. Sie können zusätzliche Daten festlegen – eine Notiz, die angibt, warum die-ses CI erstellt wurde, einige Informationen darüber, mit welcher Art von CIs Sie arbeiten. Beispiel: de–scription=Created by Malware Incident Re–ports^type=autodetect

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Werttrennzeichen	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“auf „Mit diesem Wert in einer zugehörigen Liste verknüpfen“** oder **„Mit diesem Wert verknüpfen“ festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhanden ist**. Dieses Feld gibt das Trennzeichen an, das für Elementlisten verwendet werden soll. üblicherweise ein Komma oder Semikolon.
Werttyp	Wenn **„Wert in einem Feld oder einer zugehörigen Liste speichern“** auf **„Neuen Wert in ein Feld im Datensatz hinzufügen“** festgelegt ist, gibt dieses Feld den Typ des Werts an. Zur Auswahl stehen: ○ **Quellfelddatensatz** ○ **Dem Feld als neue Zeile anfügen** ○ **Statischer Wert** ○ **Statischer Wert plus Quelldatensatz-Feldwert**
Quellenfeld	Wählen Sie das Quellfeld, das den Wert enthält, der im Zielfeld platziert werden soll, oder wählen Sie die ausgewählte zugehörige Liste aus.
Statisches Feld	Statischer Wert für das Feld.
Wertumwandlung	Wählen Sie den anzuwendenden Feldwert-Transformationseintrag. Es wird verwendet, um Auswahlfelder zwischen Datensätzen zuzuordnen, z. B. zum Konvertieren der **Kategorieauswahl** für einen Security Incident in das entsprechende **Typfeld** für eine Change-Anforderung.
Zieltabelle	Wird automatisch mit der Zieltabelle ausgefüllt.
Feldzuordnung	Wird automatisch mit der übergeordneten Feldzuordnung ausgefüllt.
Quelltabelle	Wird automatisch mit der Quelltabelle ausgefüllt.

7. Klicken Sie auf **Absenden**.

Security Operations Feldwerttransformationen

Wandelt eindeutige Kundenfeldwerte in Feldwerte um, die von der E-Mail-Analyse Security Operations von , Datenanreicherung oder Tabellen mithilfe von Feldzuordnungen erkannt werden. Unterstützt Auswahlfelder, Referenzen und richtet externe Daten an der Standardterminologie und dem Standardformat für Ihren neuen Datensatz aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Daten für Felder wie Kategorie, Status oder Zuweisungsgruppe den Werten zuordnen, die in der Tabelle „Security Operations“ verwendet werden. Ordnen Sie beispielsweise „In Analyse“ dem Wert „In Arbeit“ zu.

Erstellen Sie Werttransformationen für das Feld Security Operations .

„Feldwerttransformationen“ definiert eine Transformation zwischen den bereitgestellten Quelldaten und dem zu verwendenden Ersatzwert.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.basic oder sn_si.basic

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie, dass jeder Transformationseintrag angewendet wird, wenn eine Übereinstimmung mit dem Suchwert besteht oder wenn der Suchwert in den bereitgestellten Quelldaten enthalten ist oder wenn keine Übereinstimmungen gefunden werden. Legen Sie einen Standardwert fest, wenn keine Übereinstimmung gefunden wird. Wenn kein Standardwert festgelegt ist und keine Übereinstimmungen gefunden werden, werden die ursprünglichen Quelldaten verwendet.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldwertumwandlungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldwert transformiert

Feld	Beschreibung
Name	Der Name der Feldwerttransformation.
Beschreibung	Beschreibung für die Feldzuordnung.
Feldwert-Umwandlungseinträge	Die Tabellenliste der Einträge. **a.** Doppelklicken Sie unter **Daten ersetzen**auf die Option Neue Zeile einfügen. **b.** Wählen Sie eine der folgenden Optionen: Wenn das Datum für dieses Feld übereinstimmt Wenn die Daten für dieses Feld Folgendes enthalten Wenn kein anderer Transform-Eintrag mit den Daten (Standard) übereinstimmt **c.** Klicken Sie auf das grüne Häkchen. **d.** Doppelklicken Sie unter **Suchwert**, und fügen Sie Ihren Suchwert hinzu. **e.** Klicken Sie auf das grüne Häkchen. **f.** Doppelklicken Sie unter **Ersatzwert,** und fügen Sie den entsprechenden Wert ServiceNow hinzu. **g.** Wiederholen Sie dies bei Bedarf.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Transformation zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Umfang der Anwendung.

4. Klicken Sie auf **Absenden**.

Security Operations Zuordnung von Ergänzungsdaten

Ergänzungsdatenzuordnung wandelt Daten aus XML-, JSON- oder Eigenschaften -Dateien in ServiceNow -Datensätze um. Security Operations -Workflows verwenden Ergänzungsdatenzuordnungen und stellen Ausgabedaten für Security Incidents bereit.

Security Operations enthält mehrere Ergänzungsdatenzuordnungen, die von verschiedenen Workflows ausgelöst werden, z. B. Flow für Security Operations-Integrationen – Netzwerkstatistiken abrufen und Security Operations-Systembefehlsintegration: Flow zum Abrufen laufender Prozesse. Die Ausgabe der Ergänzungsdatenzuordnung von Security Operations -Workflows wird auf der Registerkarte **Ergänzungsdaten** im Formular „Security Incident“ angezeigt.

Erstellen Sie eine Security Operations Ergänzungsdatenzuordnung

Transformieren Sie Daten aus dem JSON-, XML- oder Eigenschaften -Dateiformat in ServiceNow -Datensätze mithilfe von Ergänzungsdatenzuordnungen.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.write

Warum und wann dieser Vorgang ausgeführt wird
Vorhandene Ergänzungsdatenzuordnungen werden von in Security Operationsbereitgestellten Workflows verwendet. Sie können die Liste unter **Ergänzungsdatenzuordnung**anzeigen. Zur Verwendung einer Zuordnung benötigen Sie einen Auslöser, entweder eine Geschäftsregel oder einen Workflow.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Ergänzungsdatenzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Eine Ergänzungsdatenzuordnung wird erstellt

Feld	Beschreibung
Name	Name dieser Ergänzungsdatenzuordnung.
Eingabeformat	Wählen Sie ein Format aus der Liste aus: JSON (Standard) XML Dateiformat für Eigenschaften
Präfixschlüssel	Dient zum Beschränken des Eingabedatensatzes auf einen angegebenen Schlüssel. Der Stamm des Eingabedatensatzes ist auf diesen Schlüssel festgelegt. Wenn Sie in diesem Beispiel „file_info“ eingeben, werden die Eingabewerte auf die Werte in „file_info“ beschränkt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	<?xml version="1.0" encoding="UTF-8"?> <malware> <version>2.0</version> <file_info> <malware>yes</malware> <sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1> <filetype>PE</filetype> <sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
Anwendung	Umfang der Anwendung.
Duplizierungsregel	Regel, die definiert, wann ein Datensatz als Duplikat betrachtet wird und welche Aktionen mit doppelten Datensätzen auszuführen sind.
Zieltabelle	Wählen Sie eine Tabelle aus der Liste aus.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Zuordnung zu aktivieren.
Beschreibung	Geben Sie eine Beschreibung der Ergänzungsdatenzuordnung ein.

4. Klicken Sie auf **Absenden**.
   Die Registerkarte Ergänzungsdaten-Zuordnungsfelder wird angezeigt.
5. Klicken Sie auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.

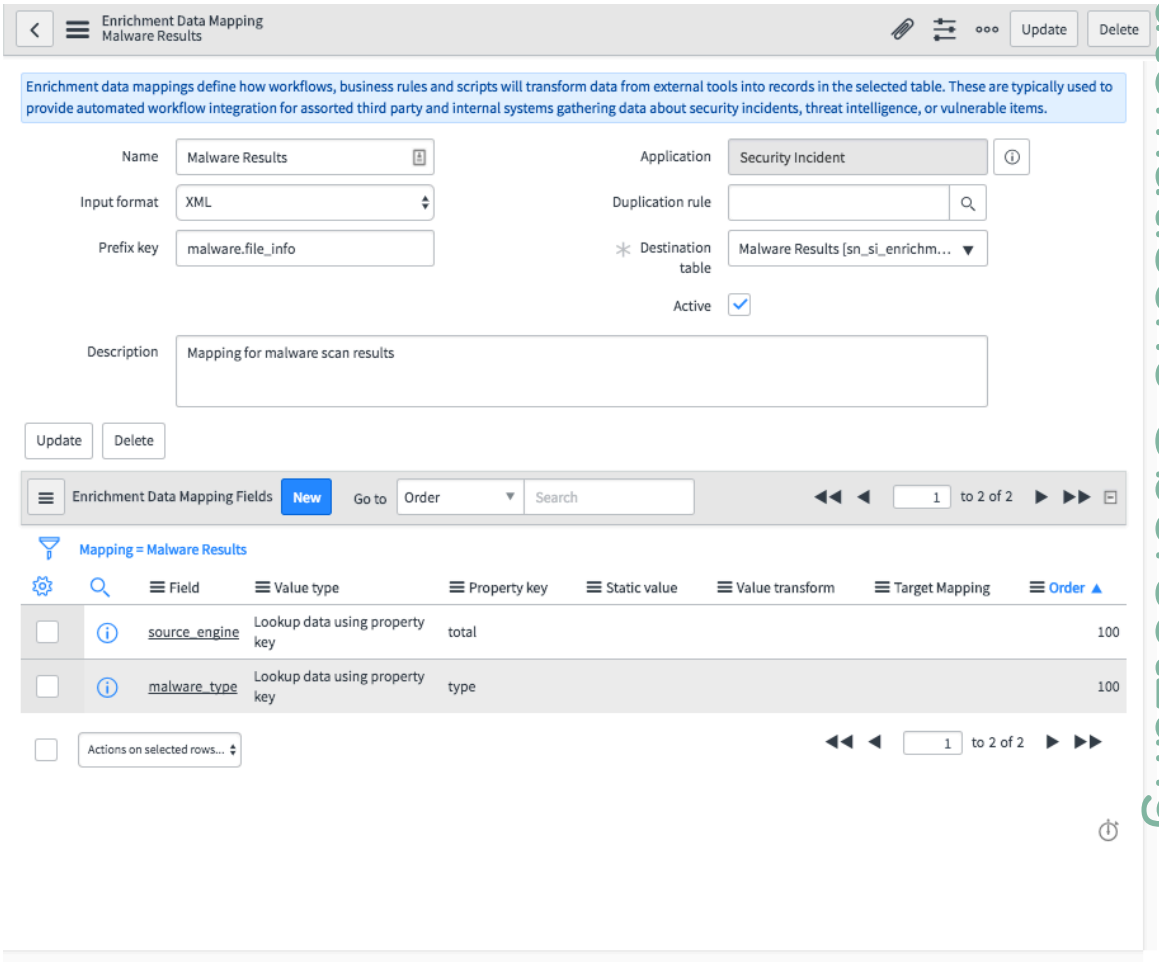
Zuordnungsfelder für Ergänzungsdaten

Feld	Beschreibung
Feld	Name der Ergänzungsdatenzuordnung.
Werttyp	Aus der Liste auswählen: Suchdaten, die einen Eigenschaftsschlüssel verwenden Statischer Wert Statischer Wert plus Daten aus dem Eigenschaftsschlüssel Feld ist ein Array oder Objekt (Rohdatenschachtelung) Jede Auswahl hat andere Einträge. Feldwerte und Arrays oder Objekte erfordern einen Eigenschaftsschlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Eigenschaftsschlüssel	Bestimmt den Schlüssel für die Suche der Eingabedaten und den in das Zielfeld geschriebenen Wert
Wertumwandlung	Die Feldwerttransformation, die einen Wert einem anderen zuordnet.
Anwendung	Umfang der Anwendung.
Bestellung	In welcher Reihenfolge die Zuordnung berücksichtigt werden soll. Die erste Übereinstimmung wird verwendet. Der Standardwert ist 100.
Zuordnung	Name der Ergänzungsdatenzuordnung.
Zieltabelle	Die Tabelle, an die die zuzuordnenden Felder gehen.

7. Klicken Sie auf **Absenden**.
   Im Folgenden finden Sie ein Beispiel für eine Ergänzungsdatenzuordnung.



Security Operations Anwenderdefinierte Eskalation

Sie können einen Eskalationspfad für Security Incidents für Probleme erstellen, die mehr Aufmerksamkeit oder Fachwissen erfordern. Sobald eine Eskalationsgruppe vorhanden ist, wird für jeden Security Incident in dieser Gruppe eine Schaltfläche angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine anwenderdefinierte Eskalationsgruppe Security Operations .

Eskalieren Sie einen Security Incident mithilfe von Eskalationen an eine beliebige Gruppe, die dem Incident zugeordnet ist.

Vorbereitungen

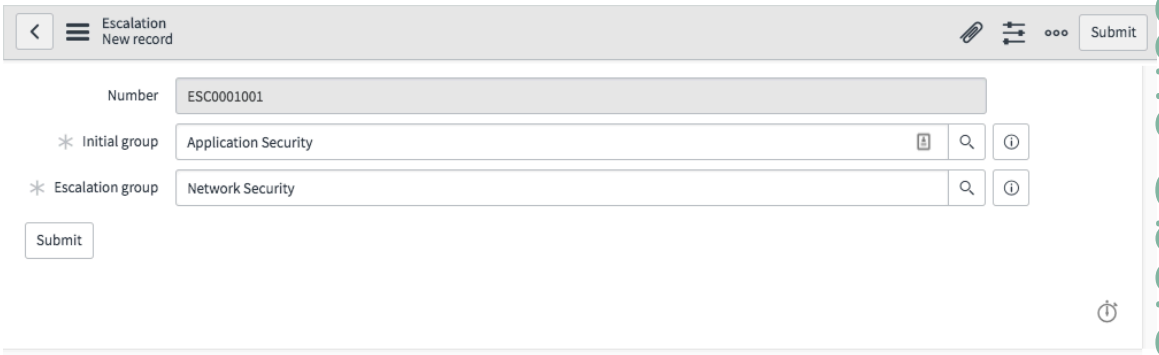
Erforderliche Rolle: sn_si.admin

Prozedur

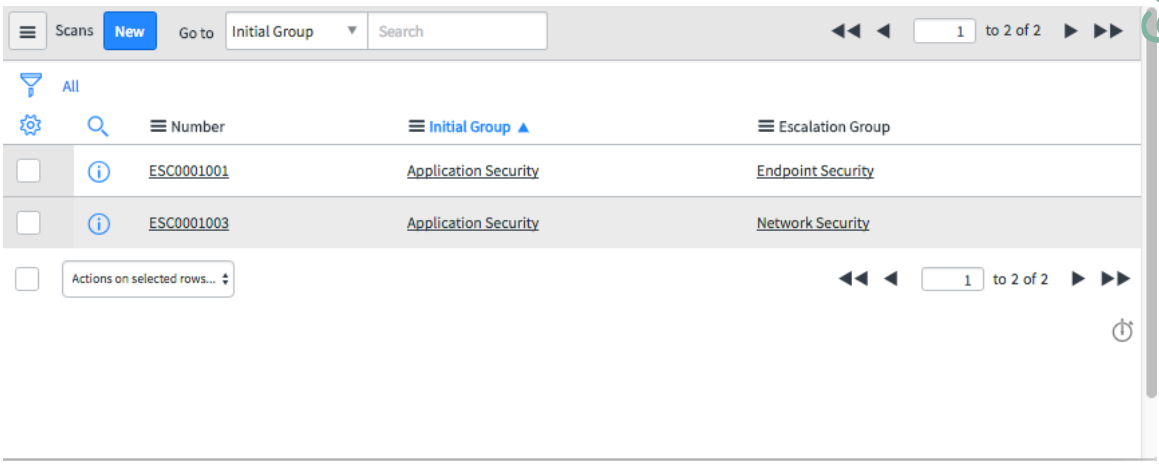
1. Navigieren zu **Alle** > **Security Operations** > **Gruppen** > **Eskalationen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Eskalationen

Feld	Beschreibung
Nummer	Eskalations-Incident-Nummer (Feld wird automatisch generiert).
Ursprungsgruppe	Wählen Sie die Gruppe aus, zu der dieser Security Incident gehört.
Eskalationsgruppe	Wählen Sie die Gruppe aus, an die der Security Incident eskaliert werden soll.



4. Klicken Sie auf **Absenden**.
   Eine Eskalationsgruppe ist für alle Security Incidents in der ursprünglichen Gruppe verfügbar. Sie können mehrere Gruppen erstellen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie domänengetrennte Eigenschaftsüberschreibungen

Wenn Sie Domain Separation verwenden, können Sie Überschreibungen für vorhandene Security Operations-Eigenschaften erstellen, mit denen Sie die Funktionen der Anwendungen in jeder Ihrer Domänen anpassen können.

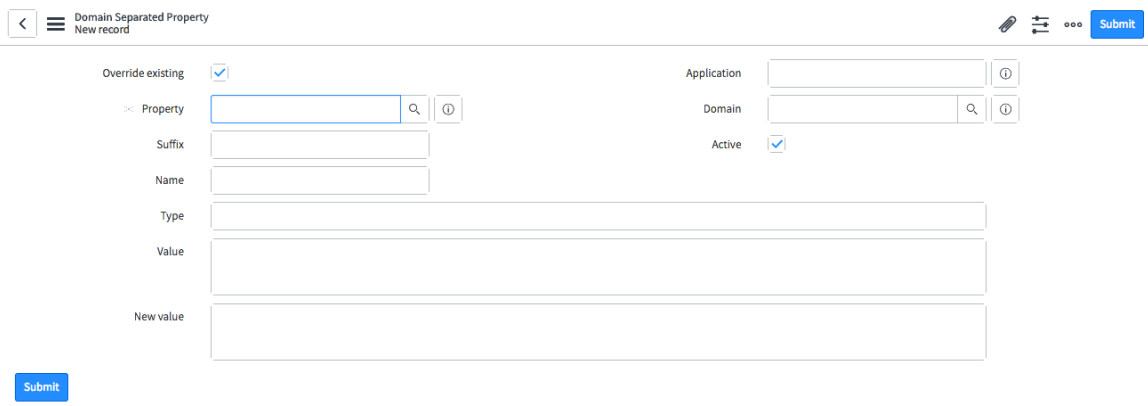
Vorbereitungen

Erfordert, dass Domain Support - Domain Extensions aktiviert wird. Sie können auch mehr über den Domänenüberschreibungs-Viewer erfahren.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Nach Domäne getrennte Eigenschaften**.
2. Klicken Sie auf **Neu**.



3. Füllen Sie die Felder des Formulars aus.

Formular „Domain Separation-Eigenschaft“.

Feld	Beschreibung
Vorhandene überschreiben	Aktivieren Sie dieses Kontrollkästchen, um einen domänenspezifischen Wert für eine vorhandene Eigenschaft zu erstellen.
Anwendung	Wählen Sie die Anwendung aus, die die Eigenschaft enthält, die Sie überschreiben möchten.
Eigenschaft	Wählen Sie die Eigenschaft für die ausgewählte Anwendung aus, für die Sie eine domänenspezifische Überschreibung erstellen möchten.
Domäne	Wählen Sie die Domäne aus, für die Sie diese Eigenschaftsüberschreibung erstellen.
Aktiv	Aktivieren oder deaktivieren Sie die Überschreibung.
Suffix	Zeigt das Eigenschaftssuffix an.
Name	Zeigt den Eigenschaftsnamen an.
Typ	Zeigt den Eigenschaftstyp an.
Wert	Zeigt den aktuellen Wert an, der für die Eigenschaft festgelegt ist.
Neuer Wert	Geben Sie einen neuen Wert für die Eigenschaft ein, die auf diese Domäne angewendet werden soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
   Die Überschreibung der Eigenschaft wird auf die ausgewählte Eigenschaft in der angegebenen Domäne angewendet. Wenn die Logik für diese Eigenschaft ausgelöst wird, sucht das System nach domänengetrennten Eigenschaftsüberschreibungen. Wenn eine Überschreibung für die Domäne gefunden wird, wird der neue Wert verwendet. Andernfalls wird der Wert für die Standarddomäne verwendet.

Zugehörige Informationen

Domänentrennung verstehen

Erstellen Sie eine Betriebssystemgruppe

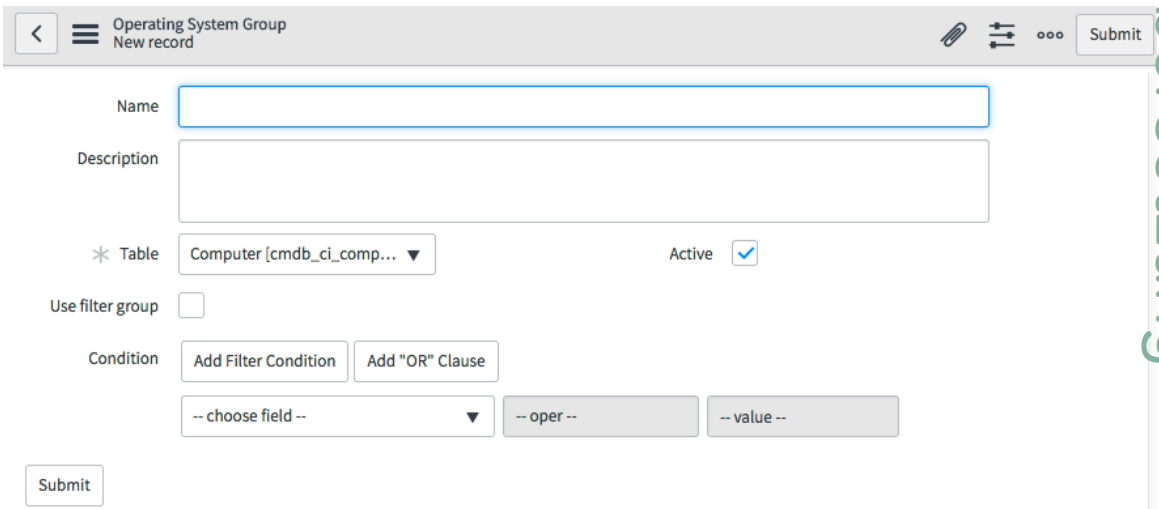
Betriebssystemgruppen werden verwendet, um ein Betriebssystem bestimmten Prozesstypen und Skripts in Workflows Security Incident Response zuzuordnen. Die Skripts definieren, wie laufende Prozesse für die definierten Betriebssystemgruppen abgerufen werden. Neue Betriebssysteme können nach Bedarf hinzugefügt werden.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Betriebssystemgruppen**.
   Das Basissystem enthält Skripts für drei Betriebssysteme:
   - BSD-basiertes Betriebssystem
   - POSIX-basiertes Betriebssystem
   - Betriebssystem Windows
2. Klicken Sie auf **Neu**.



3. Füllen Sie die Felder nach Bedarf aus.

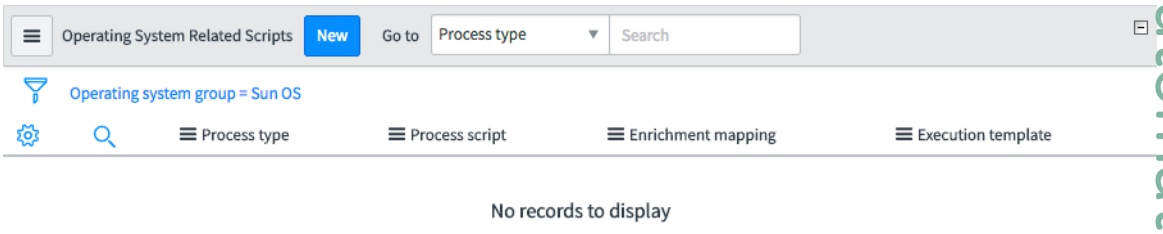
Feld	Beschreibung
Name	Der Name der Betriebssystemgruppe.
Beschreibung	Eine Beschreibung für die Betriebssystemgruppe.
Tabelle	Die betroffene Tabelle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Betriebssystemgruppe zu aktivieren.
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine Filtergruppe für die Suche nach übereinstimmenden Datensätzen in der ausgewählten Tabelle zu verwenden.
Filtergruppe	Wählen Sie die Filtergruppe zum Suchen nach übereinstimmenden Datensätzen in der ausgewählten Tabelle aus. Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert haben.
Bedingung	Die zugehörigen Listen namens Die Felderdes Bedingungsgenerators werden nur angezeigt, wenn Sie das Kontrollkästchen **Filtergruppe verwenden** nicht aktiviert haben.

4. Klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und wählen Sie **Speichern** aus.
   Die zugehörige Liste „Zugehörige Betriebssystemskripts“ wird geöffnet.



5. Klicken Sie auf **Neu**.
6. Wählen Sie Skripts aus, die den von Ihnen verwendeten Workflows entsprechen, um laufende Prozesse, Services und/oder Netzwerkstatistiken abzurufen.
7. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Fügen Sie eine Skriptdatei an einen mit einer Datei synchronisierten MID-Server an

Richten Sie Sicherheits-Tag-Gruppen und Tags ein

Sie können Security Incidents, Antwortaufgaben, angreifbaren Elementen, erkennbaren Elementen, IoCs und Sicherheitsfällen Tags zuweisen, um Metadaten für den antwortenden Datensatz zu erstellen und zu definieren, wer Zugriff auf bestimmte Arten von Sicherheitsinhalten haben soll. Die Tags können Sicherheitsgruppen hinzugefügt werden, um sie zu organisieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Gruppen**.
   Im Basissystem sind drei Standardklassifizierungsgruppen enthalten.
   - **Ergänzung: Zulassungsliste/Deny-Liste**: Diese Gruppe definiert, ob ein Datensatz als Datensatz auf der Zulassungsliste oder auf der Deny-Liste behandelt werden soll. Datensätze der Allow-Liste sind im Allgemeinen von geringerer Bedeutung und können daher ignoriert werden. Datensätze in der Deny-Liste sind im Allgemeinen von höherem Interesse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Metatag**: Diese Gruppe wird als Demodaten bereitgestellt. Sie können damit anwenderdefinierte Klassifizierungs-Tags erstellen, die von Security Operations-Anwendungen verwendet werden.
- **Traffic Light-Protokoll**: Diese Gruppe wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die richtige Zielgruppe freigegeben werden. Vier Farben (weiß, grün, gelb und rot) kennzeichnen unterschiedliche Empfindlichkeitsgrade. Für jede Farbe können Sie die entsprechenden Lese-/Schreibzugriffsrollen zuweisen. Bei der Freigabe von erkennbaren Elementen für einen vertrauenswürdigen Sicherheitskreis bestimmt das dem Profil des vertrauenswürdigen Sicherheitskreises zugewiesene Tag, welche erkennbaren Elemente mit TLP-Tags für den Kreis freigegeben werden können:
  - **TLP:WEISS:** Nur erkennbare Elemente mit TLP:WEISS können für ein TLP:WEISS-Profil freigegeben werden.
  - **TLP: GREEN:** Erkennbare Elemente mit TLP: GREEN und TLP: White können für ein TLP: GREEN-Profil freigegeben werden.
  - **TLP: GELB:** Erkennbare Elemente mit TLP: GELB, TLP: GREEN und TLP: WEISS können für ein TLP: GELB-Profil freigegeben werden.
  - **TLP: ROT:**Alle erkennbaren Elemente können, unabhängig von ihrem TLP-Tag, mit einem TLP: ROT-Profil geteilt werden, da „TLP: ROT“ das TLP-Tag mit dem höchsten Rang ist.

Hinweis:
Sie können andere TLP-Farben hinzufügen, aber alle zusätzlichen Farben werden vom Forum for Incident Response and Security Teams (FIRST) als nicht gültig angesehen.

2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie den Namen der Sicherheitsgruppe ein.
Mehrfachauswahl zulassen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie einem Datensatz, der eine Gruppe gemeinsam nutzt, mehrere Sicherheits-Tags zuweisen möchten.
Aktiv	Aktivieren oder deaktivieren Sie die Gruppe.
Beschreibung	Geben Sie eine Beschreibung für diese Gruppe ein.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die zugehörige Liste Sicherheits-Tags wird angezeigt.
5. Klicken Sie in der zugehörigen Liste Sicherheits-Tags auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name des Klassifizierungs-Tags.
Sicherheits-Tag-Gruppe	Wenn das Tag mit der Schaltfläche **„Neu“** in der zugehörigen Gruppenliste erstellt wurde, wird in diesem Feld standardmäßig die aktuelle Gruppe angezeigt. Bei Bedarf können Sie das Tag einer anderen Gruppe hinzufügen, dies ist jedoch optional.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bestellung	Geben Sie die Reihenfolge an, in der das Tag in Formularen oder in einer Liste angezeigt wird.
Farbe	Wählen Sie die Farbe für dieses Tag aus.
Eingeschränkten Zugriff erzwingen	Aktivieren Sie dieses Kontrollkästchen, um Lese- und/oder Schreibrollen zuzuweisen, die Anwender zum Lesen oder Schreiben von Datensätzen mit diesem Sicherheits-Tag benötigen.
Aktiv	Aktivieren oder deaktivieren Sie das Tag.
Beschreibung	Eine Beschreibung dieses Tags.
Rollen (Lesezugriff)	Um einem Sicherheits-Tag Lesezugriff zuzuweisen, klicken Sie auf das Sperrsymbol, wählen Sie die entsprechenden Zugriffsrollen aus, und klicken Sie erneut auf das Sperrsymbol. Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Eingeschränkten Zugriff** erzwingen aktiviert haben.
Rollen (Schreibzugriff)	Um einem Sicherheits-Tag Schreibzugriff zuzuweisen, klicken Sie auf das Sperrsymbol, wählen Sie die entsprechenden Zugriffsrollen aus, und klicken Sie erneut auf das Sperrsymbol. Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Eingeschränkten Zugriff** erzwingen aktiviert haben.

7. Wiederholen Sie diese Schritte nach Bedarf, um weitere Sicherheits-Tags zu erstellen.
8. Klicken Sie auf **Aktualisieren**.

> **Hinweis:**
> Sie können auch neue Tags erstellen, indem Sie zu navigieren **Security Operations** > **Sicherheits-Tags** > **Tags**. Das Verfahren ist das gleiche.

Erstellen Sie Sicherheits-Tag-Regeln

Sicherheits-Tag-Regeln filtern den Zugriff auf Sicherheits-Tags.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Tags**.
2. Wählen oder erstellen Sie ein Sicherheits-Tag.
3. Klicken Sie auf der zugehörigen Registerkarte **Security Tag Rules (Sicherheits-Tag-Regeln)** auf **New (Neu)**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Sicherheits-Tag-Regel.
Sicherheits-Tag	Das Sicherheits-Tag, das an die Regel angehängt werden soll.
Aktiv	Aktivieren oder deaktivieren Sie das Sicherheits-Tag.
Beschreibung	Eine Beschreibung dieser Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Bestimmen Sie **die Datensatzfilterung.**
6. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Filtergruppe verwenden	Ordnet der Regel eine Filtergruppe zu.
Tabelle	Die Tabelle, die die Regel enthalten soll.
Bedingung	Fügen Sie eine oder mehrere Filterbedingungen hinzu.

7. Klicken Sie auf **Absenden**.

Sicherheits-Tag-Regeln importieren

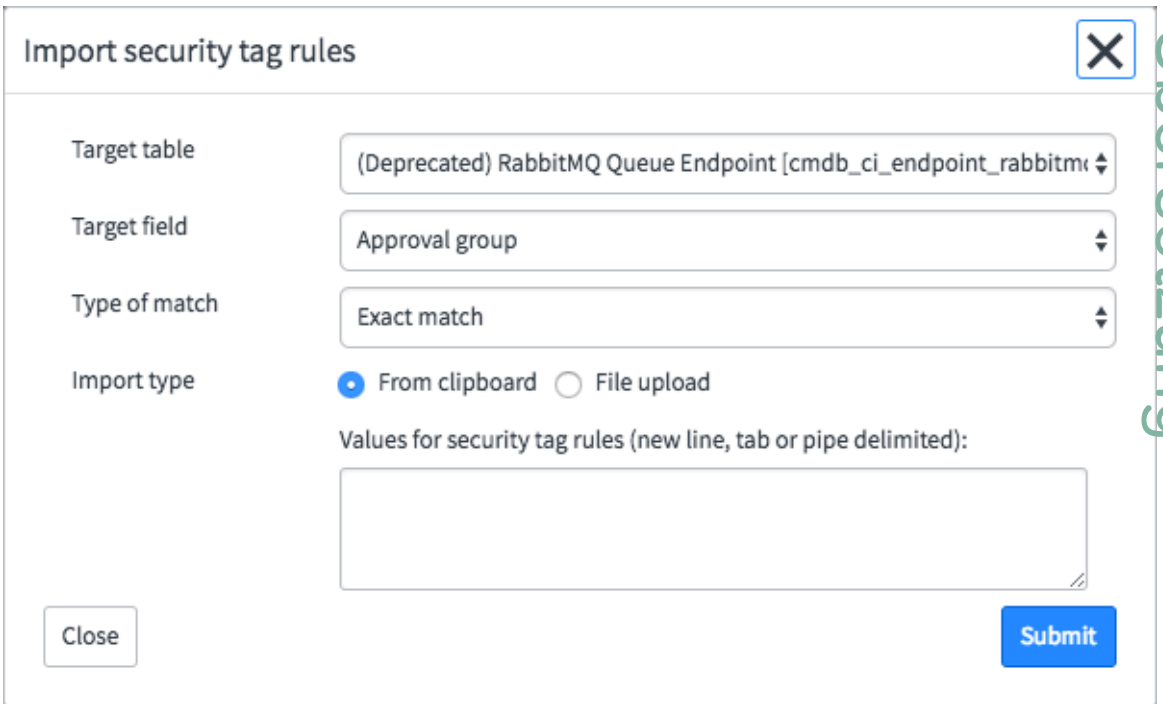
Sie können Sicherheits-Tag-Regeln aus anderen Tabellen in Ihrer Bereitstellung importieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Tags**.
2. Wählen oder erstellen Sie ein Sicherheits-Tag.
3. Klicken Sie auf den zugehörigen Link **Sicherheits-Tag-Regeln importieren**.



4. Füllen Sie die entsprechenden Felder im Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zieltabelle	Wählen Sie die Tabelle aus, die zum Importieren von Regeln verwendet werden soll.
Zielfeld	Wählen Sie das Feld aus, das zum Importieren von Regeln verwendet werden soll.
Typ der Übereinstimmung	Wählen Sie aus, wie die importierten Regeln mit **Sicherheits-Tags** abgeglichen werden sollen: Genaue Übereinstimmung (Standard) Enthält Beginnt mit Endet mit Regulärer Ausdruck
Importtyp	Wählen: **Aus Zwischenablage** Kopieren Sie eine Liste begrenzter Werte in den Textbereich. Die Werte werden in Sicherheits-Tags analysiert. **Aus Datei-Upload** Laden Sie eine Datei mit getrennten Werten hoch. Die Werte werden in Sicherheits-Tags analysiert. Fügen Sie Werte für die Sicherheits-Tag-Regeln mithilfe von neuen Zeilen- oder Pipeline-Begrenzern hinzu.

5. Klicken Sie auf **Absenden**.

Sicherheitsanmerkungen

Eine Sicherheitsanmerkung ist eine Notiz mit Erklärungen oder Kommentaren, die einem Konfigurationselement, einem erkennbaren Element oder einer Verwendung für einen Security Incident hinzugefügt werden.

Für Anwender und erkennbare Elemente sind mehrere Sicherheitsanmerkungen verfügbar (erfordert das Plugin Threat Intelligence). Berichte zu Sicherheitsanmerkungen sind ebenfalls verfügbar.

Erstellen Sie Sicherheitsanmerkungen für CIs

Mithilfe von Anmerkungen zu CIs können Sie die Aktivität über Incidents hinweg nachverfolgen. Sie können Anmerkungen zu einem einzelnen oder mehreren CIs hinzufügen.

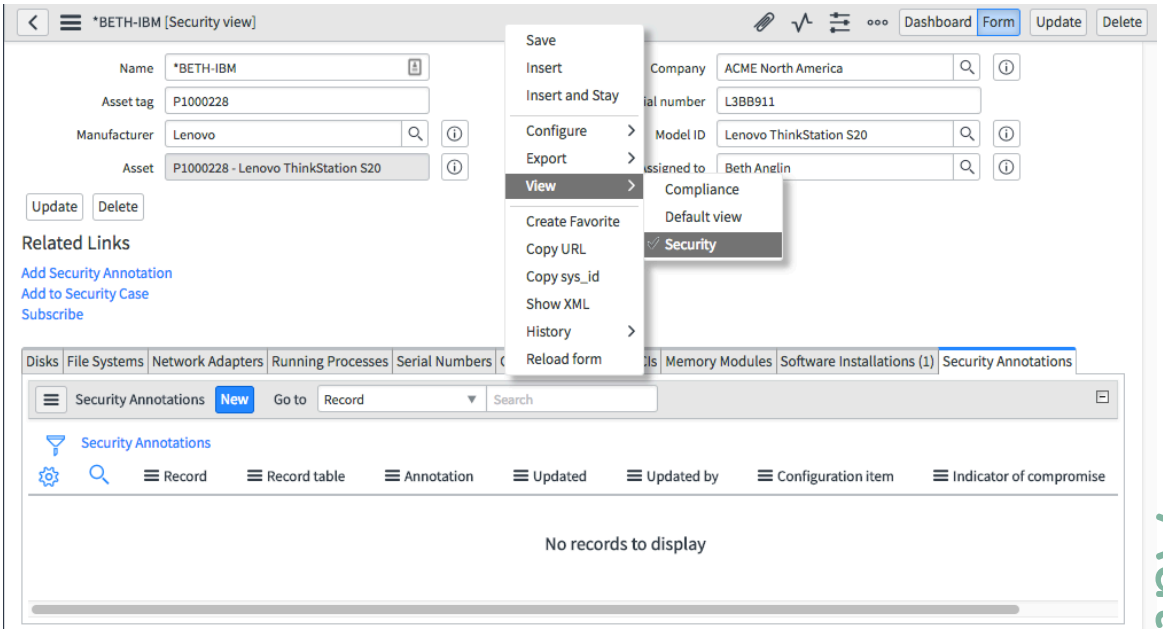
Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie ein CI aus einem Security Incident oder der Configuration Item-Tabelle.
2. Klicken Sie mit der rechten Maustaste in den Header, und wählen Sie **Ansicht** > **Sicherheit**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf der Registerkarte der zugehörigen Liste **Sicherheitsanmerkungen** auf **Neu**.
4. Geben Sie eine Anmerkung ein.
   Anmerkungen können ein beliebiges Textformat aufweisen.
5. Klicken Sie auf **Absenden**.

> **Hinweis:**
> Sie können dieselbe Anmerkung zu mehreren CIs hinzufügen, indem Sie CIs in der Liste auswählen, **Sicherheitsanmerkung hinzufügen**wählen, eine Anmerkung in einem beliebigen Textformat eingeben und auf **Absenden**klicken.

Erstellen Sie Sicherheitsanmerkungen für erkennbare Elemente

Sie können ein oder mehrere erkennbare Elemente auswählen und über das Auswahlmenü **Aktionen für ausgewählte Zeilen** Sicherheitsanmerkungen darauf anwenden.

Vorbereitungen

- Erfordert das Plugin Threat Intelligence und die Aktivierung. Das Threat Intelligence-Plugin ist als separates Abonnement verfügbar.

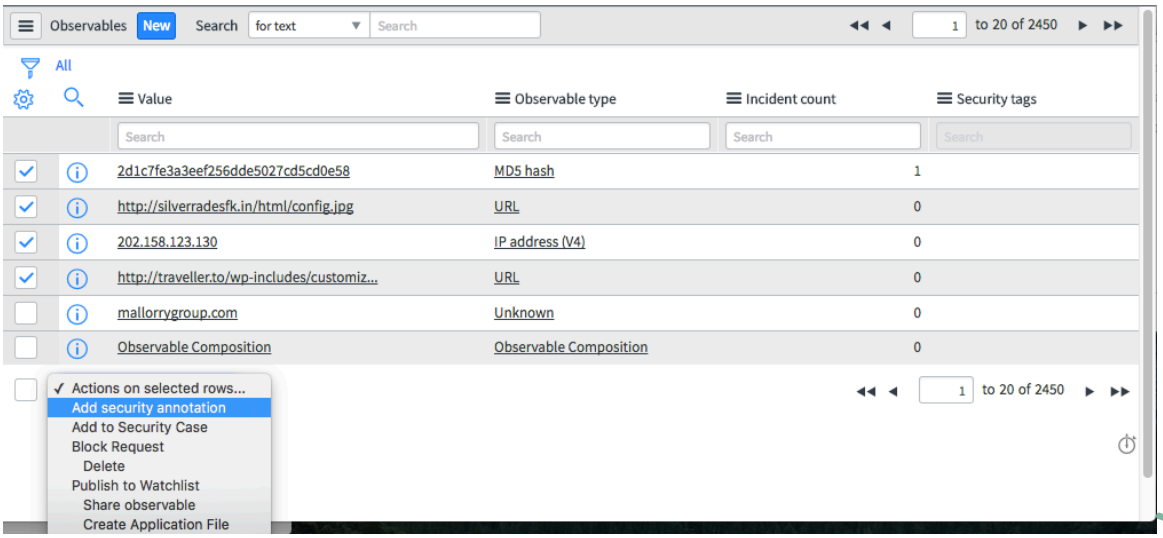
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Erkennbare Elemente**
2. Wählen Sie ein oder mehrere erkennbare Elemente in der Liste aus.
3. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilendie Option Sicherheitsanmerkung hinzufügen aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie eine Anmerkung ein.
   Anmerkungen können ein beliebiges Textformat aufweisen.
5. Klicken Sie auf **Absenden**.

Erstellen Sie Sicherheitsanmerkungen für Anwender

Sie können einen oder mehrere Anwender auswählen und über das Auswahlmenü **Aktionen für ausgewählte Zeilen** Sicherheitsanmerkungen auf sie anwenden.

Vorbereitungen

Erfordert das Plugin Threat Intelligence und die Aktivierung. Das Threat Intelligence-Plugin ist als separates Abonnement verfügbar.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**
2. Wählen Sie einen oder mehrere Anwender in der Liste aus.
3. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilendie Option Sicherheitsanmerkung hinzufügen aus**.
4. Geben Sie eine Anmerkung ein.
   Anmerkungen können ein beliebiges Textformat aufweisen.
5. Klicken Sie auf **Absenden**.

Zeigen Sie Berichte mit Sicherheitsanmerkungen an

Der Bericht „Sicherheitsanmerkungen“ enthält Details, die in der Tabelle „Sicherheitsanmerkungen“ [sn_sec_cmn_security_annotations] gespeichert sind. Sie können die Spalten im Bericht anpassen und die Daten nach Belieben gruppieren.

Vorbereitungen

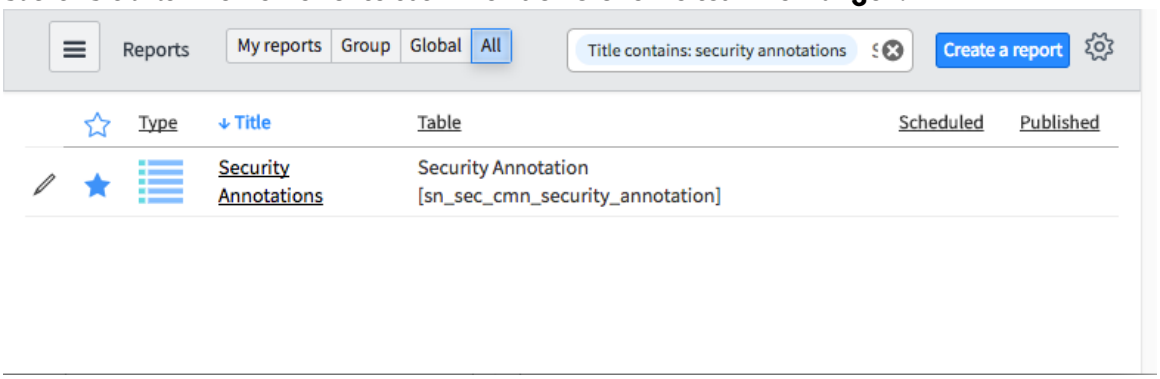
Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Berichte** > **Anzeigen/Ausführen**.
2. Suchen Sie unter **Meine Berichte** oder **Alle nach Sicherheitsanmerkungen.**



Zugehörige Informationen

Liste „Berichte“ anzeigen

Mit Security Support Common installierte Komponenten

Mit Security Support Common werden verschiedene Arten von Komponenten installiert. Sie bieten allgemeine Funktionen für die Verwendung in verschiedenen Sicherheitsanwendungen, z. B. Security Incident Response.

Auffinden und Anzeigen von installierten Komponenten

Weitere Informationen zum Auffinden und Anzeigen installierter Komponenten finden Sie unter Zeigen Sie mit installierte Komponenten an Security Support Common.

Zeigen Sie mit installierte Komponenten an Security Support Common

Wenn Sie das Plugin Security Support Common aktivieren, werden verschiedene Arten von Komponenten installiert, unter anderem Tabellen, Anwenderrollen und Module.

Lokalisierung von Komponenten

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Wenn Sie die Liste der installierten Komponenten für die Anwendung Security Support Common auf Rollen, geplante Aufgaben und Tabellen beschränken möchten, gehen Sie wie folgt vor:

Zeigen Sie gefilterte Listen für mit einer Anwendung installierte Komponenten an

Filtern Sie die Tabelle „Anwendungsdateien“, damit nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert wurden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert werden, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie diese Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Geben Sie im Filternavigator **sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung.
3. Klicken Sie im Bedingungsgenerator auf **UND**, und wählen Sie dann aus, um einen zweiten Filter hinzuzufügen: **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

[store-future: BEGIN review]

Modulzugriff nach Rolle für Security Operations-Anwendungen

Zeigen Sie für jede Anwendung die Menüelemente an, auf die von einer bestimmten Rolle zugegriffen werden kann.

[End]
[store-future: BEGIN review]

Modulzugriff nach Rolle für Konfigurations-Compliance

Informationen zur Konfigurations-Compliance finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
(Haupt-App-Gruppe)				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

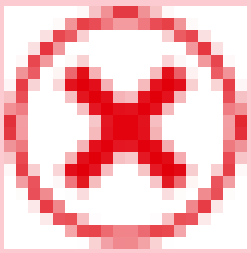
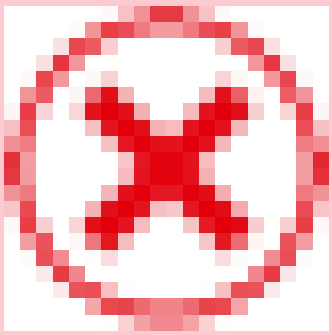
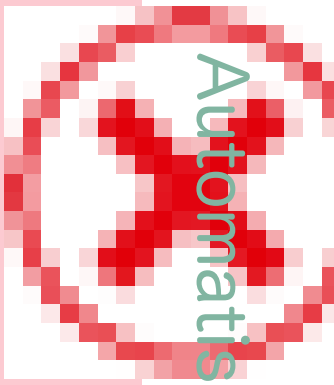
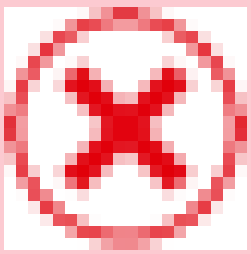
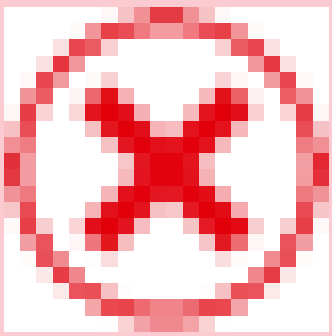
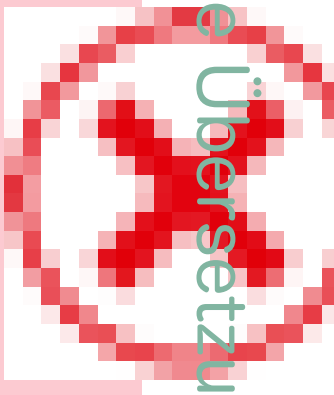
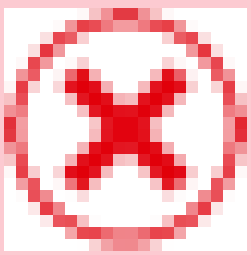
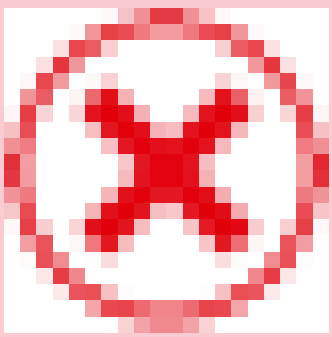
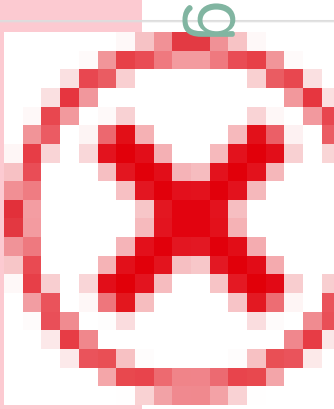
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Übersicht				
Richtlinien				
Tests				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

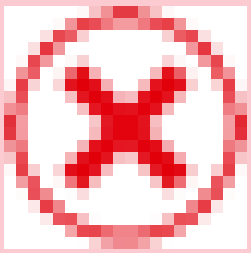
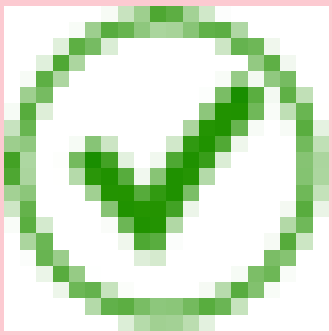
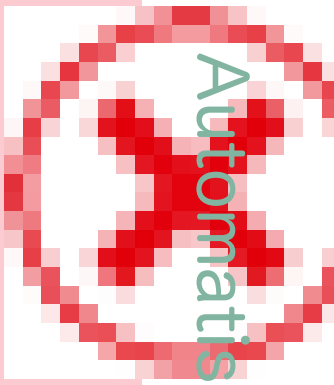
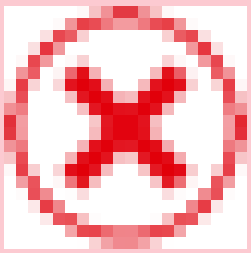
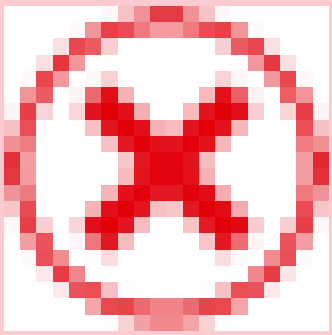
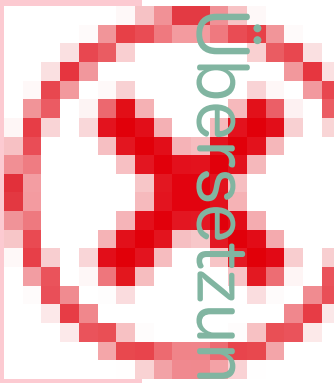
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Meine Genehmigungen				
Testergebnisse				
Nicht selektierte Testergebnisse				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

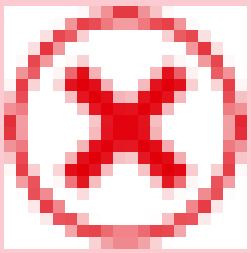
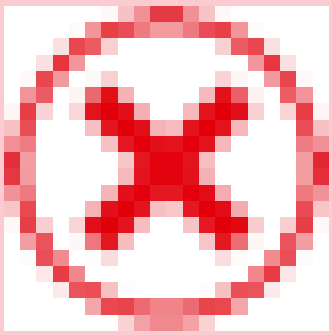
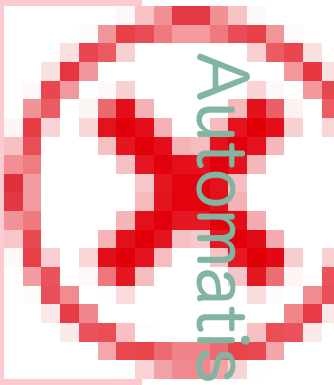
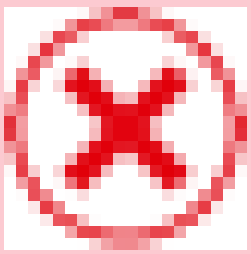
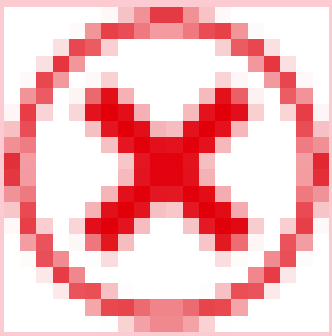
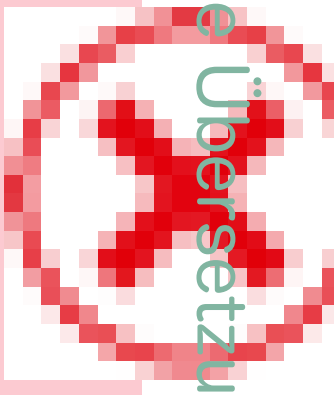
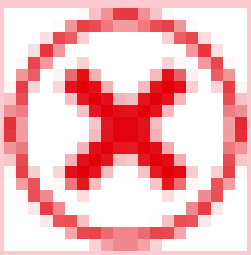
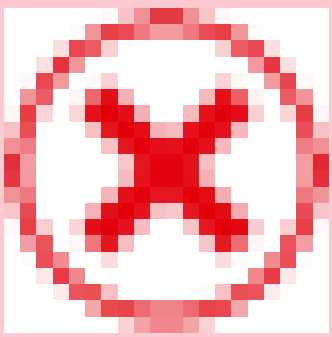
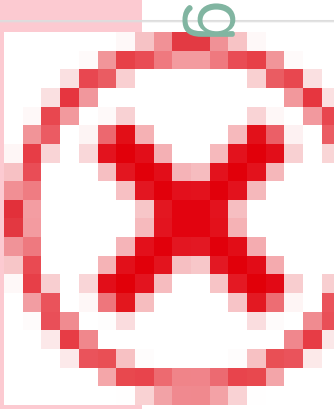
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Meine offenen Testergebnisse				
Offene Testergebnisse				
Ziel rückt näher				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

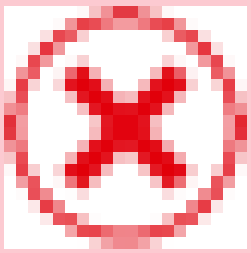
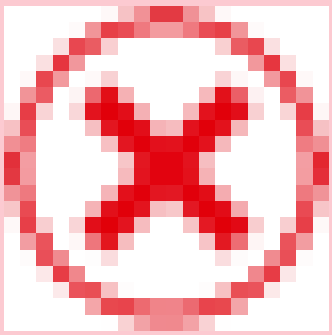
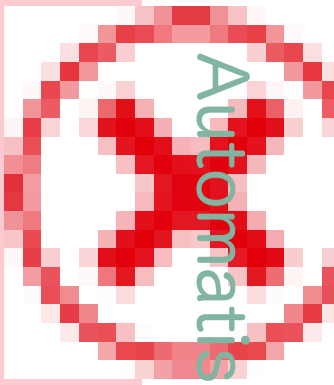
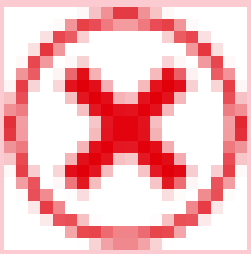
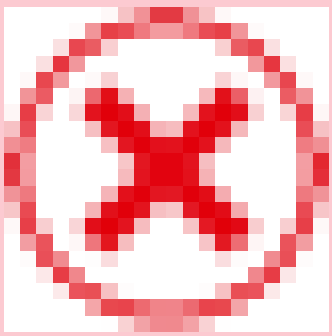
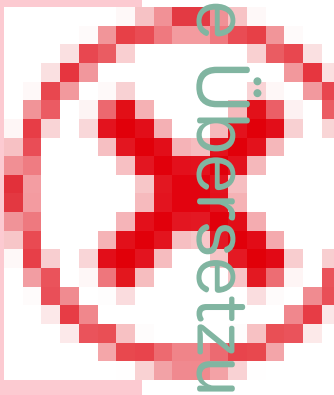
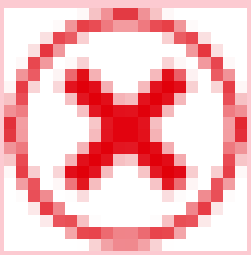
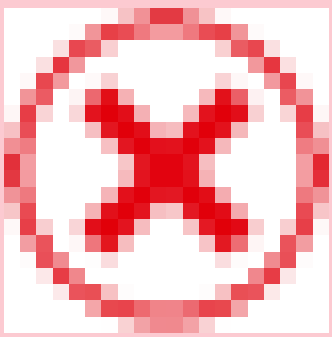
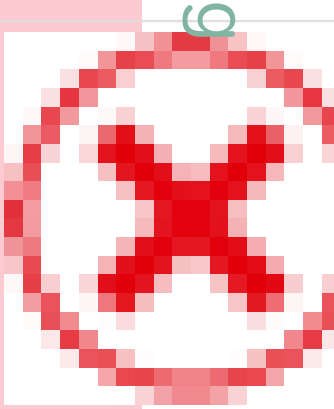
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Verfehltes Ziel				
Nicht zugewiesen				
Mehrere Zurückstellungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

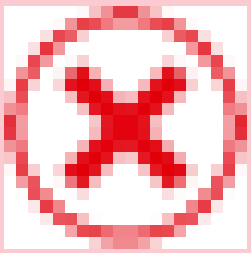
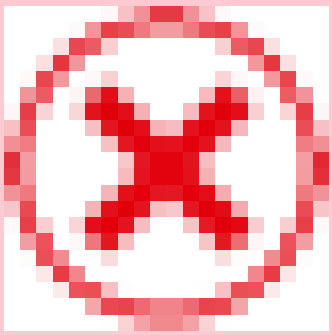
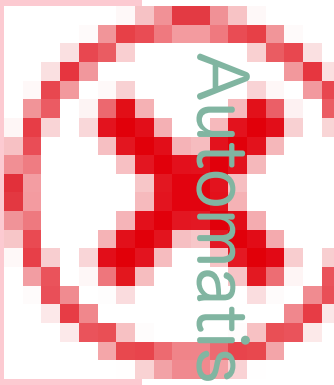
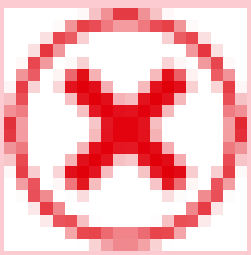
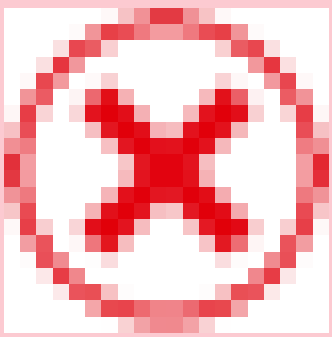
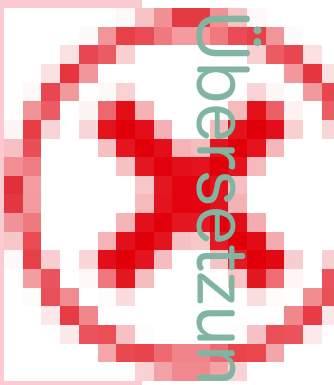
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Alle				
Testergebnisgruppen				
Meine offenen Gruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

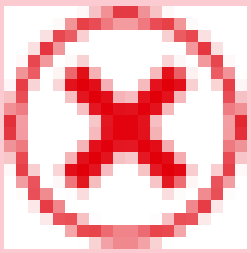
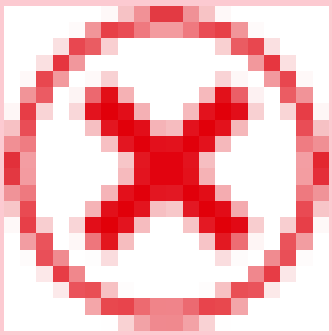
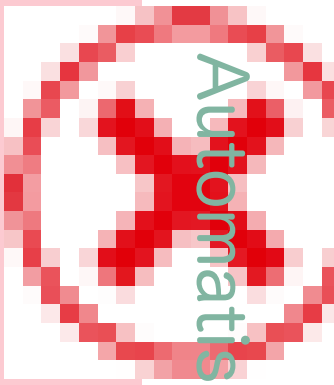
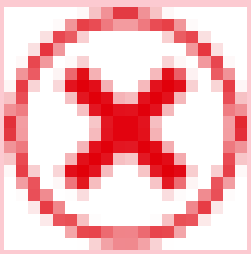
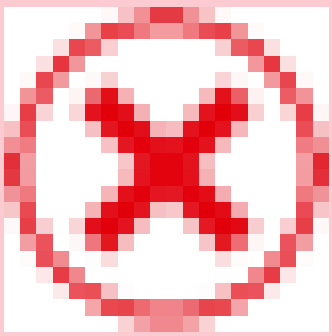
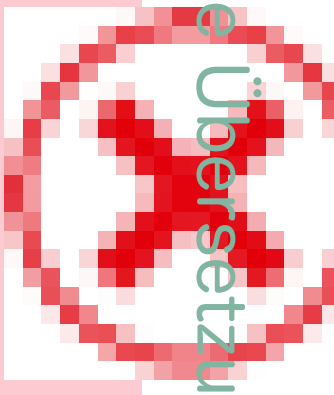
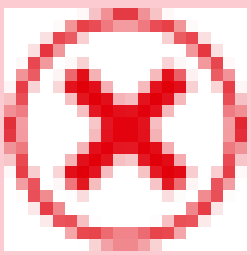
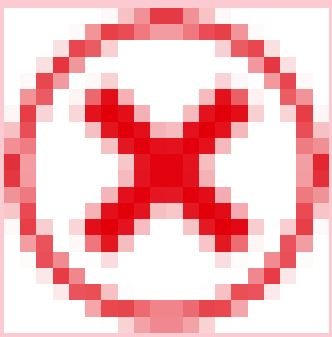
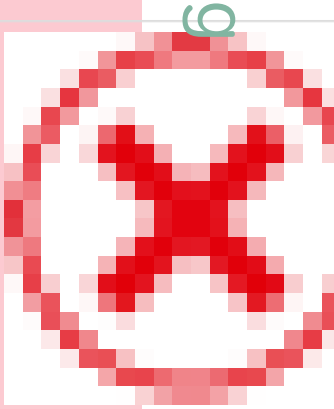
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Alle offenen Gruppen				
Mehrere Zurückstellungen				
Alle Gruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

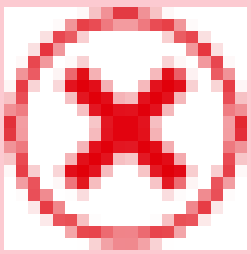
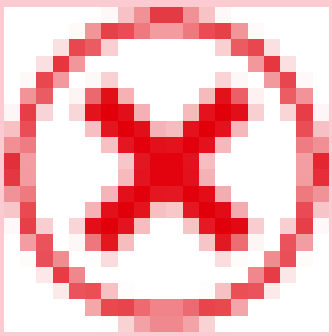
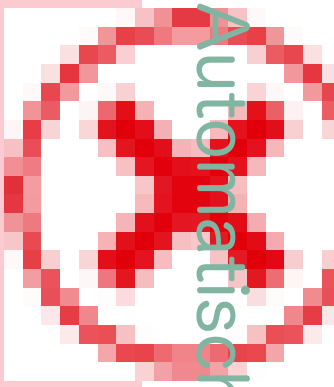
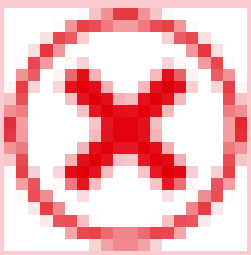
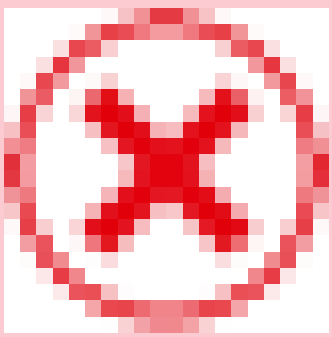
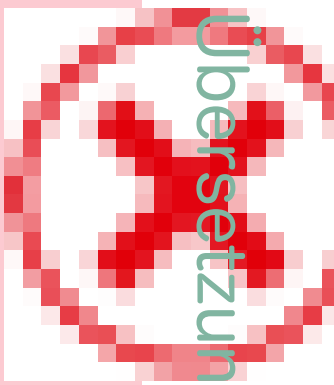
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Unterstützungsdaten				
Autoritative Quellen				
Technologien				
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

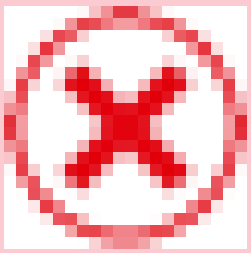
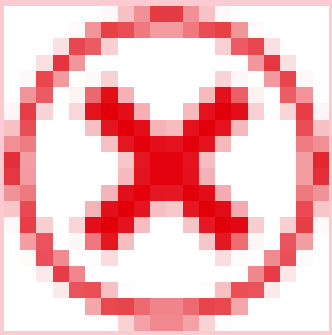
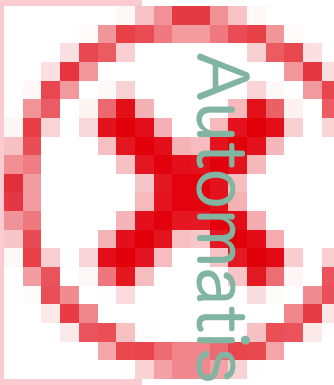
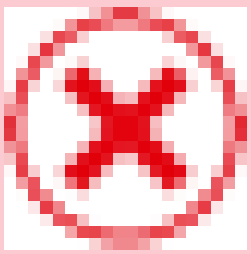
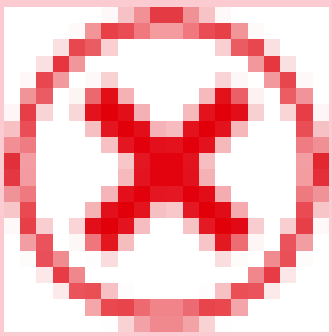
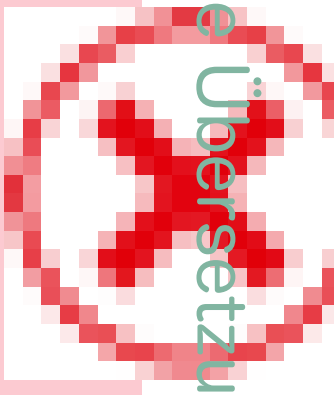
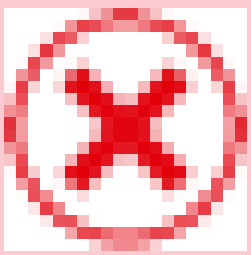
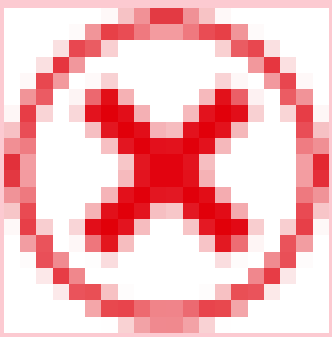
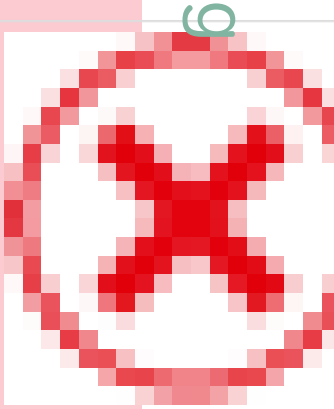
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Zuweisungsregeln				
Veraltete Testergebnisse automatisch schließen				
Gruppenregeln				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

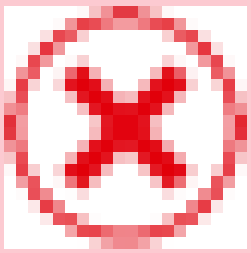
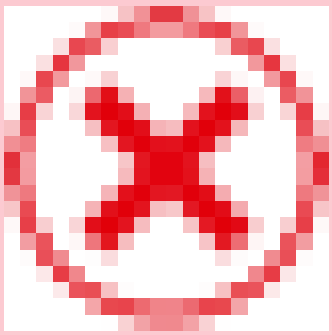
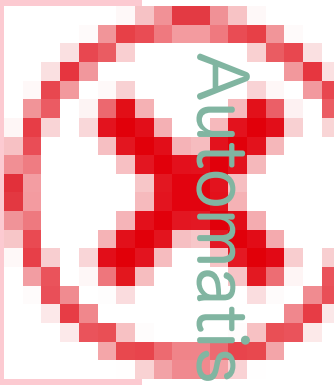
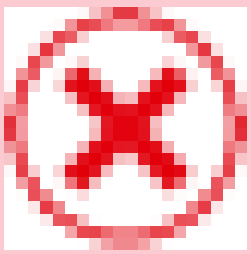
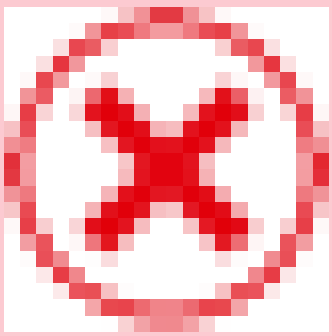
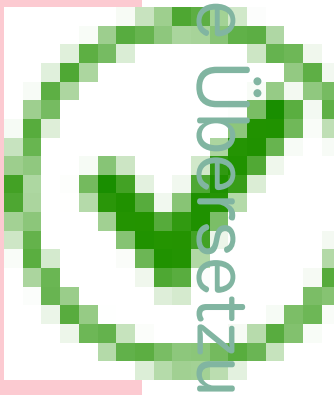
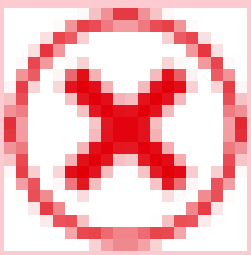
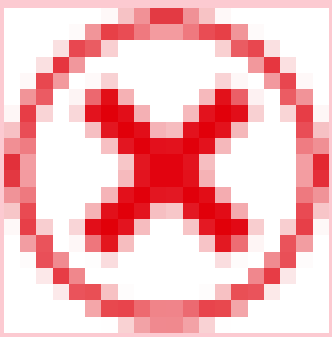
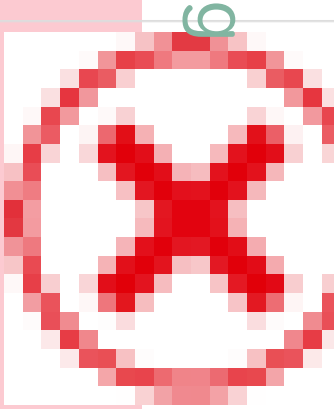
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Automatische Ausnahmeregel				
Genehmigungsregeln				
Risikorechner				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

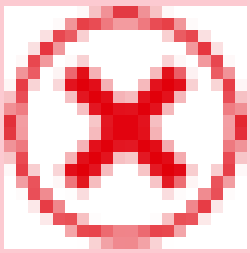
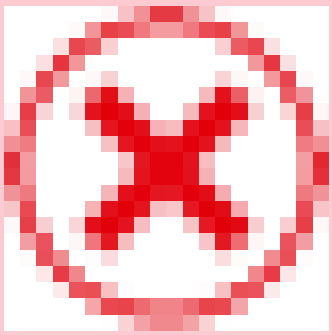
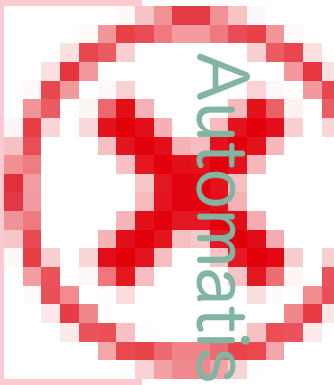
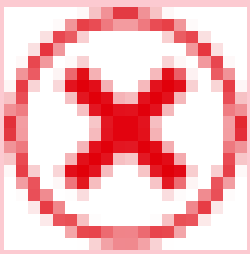
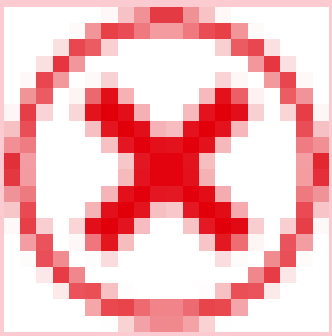
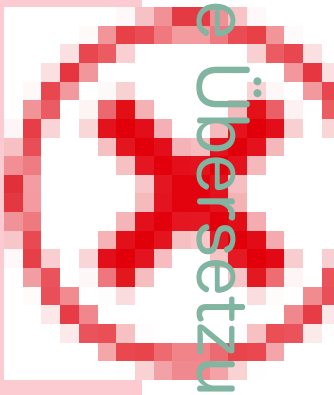
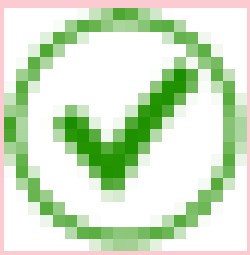
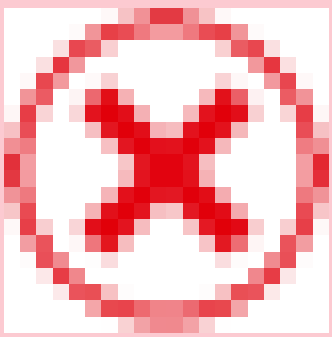
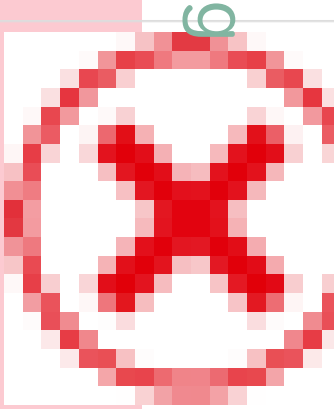
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Rollup-Rechner für Risikopunktzahl				
Korrekturzielregeln				
Relevanz-Zuordnung				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

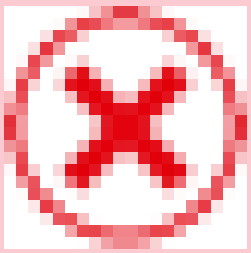
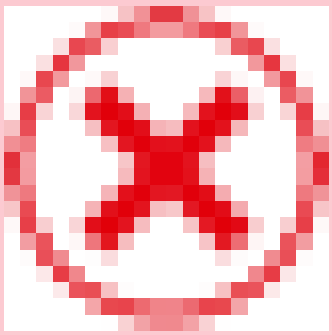
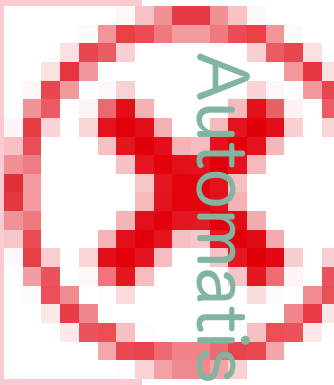
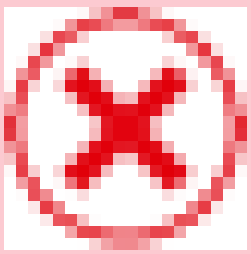
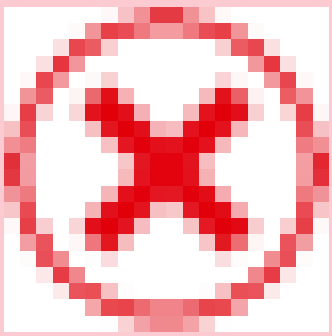
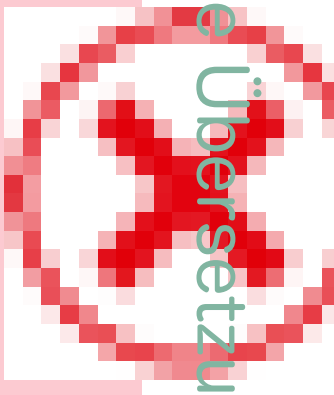
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informationen für andere Rollen:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_r
Benachrichtigungen				
Ausnahmenverwaltung				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

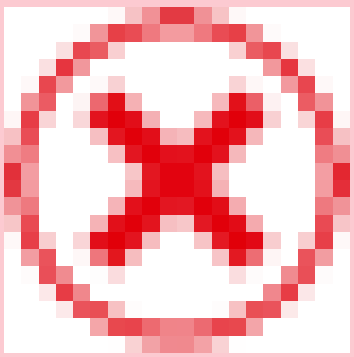
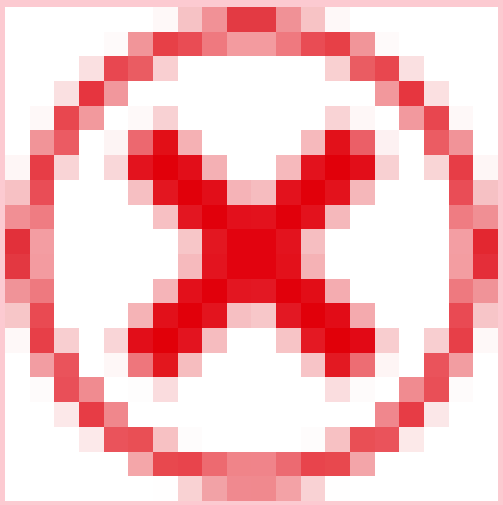
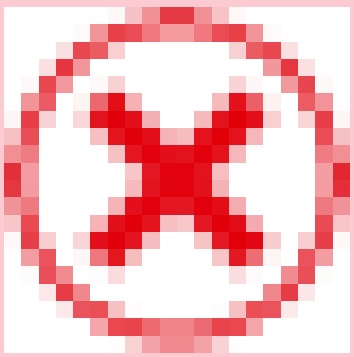
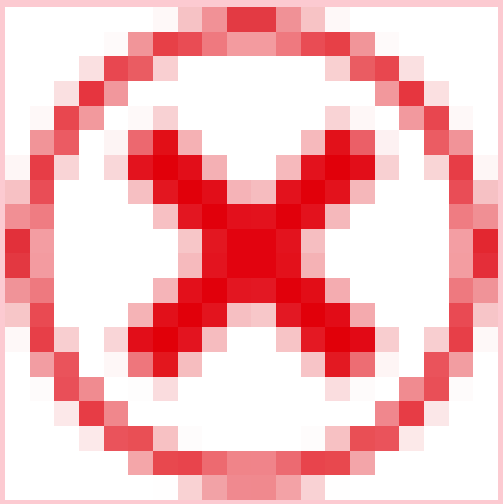
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
(Haupt-App-Gruppe)				
Übersicht				
Richtlinien				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

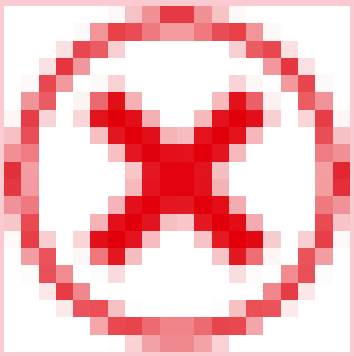
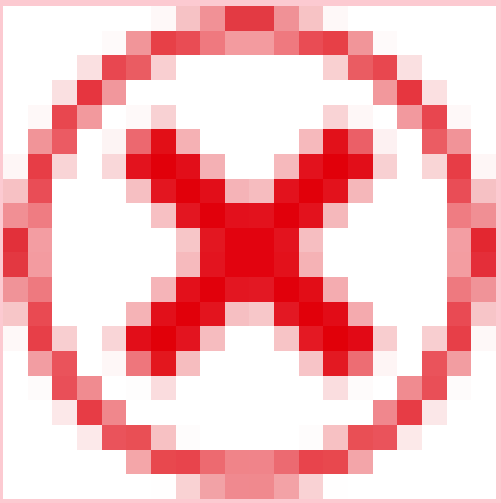
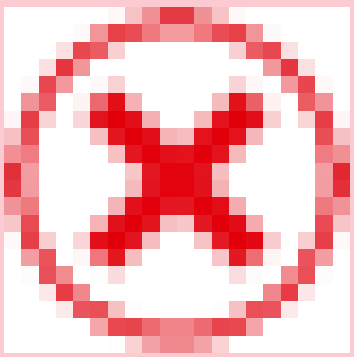
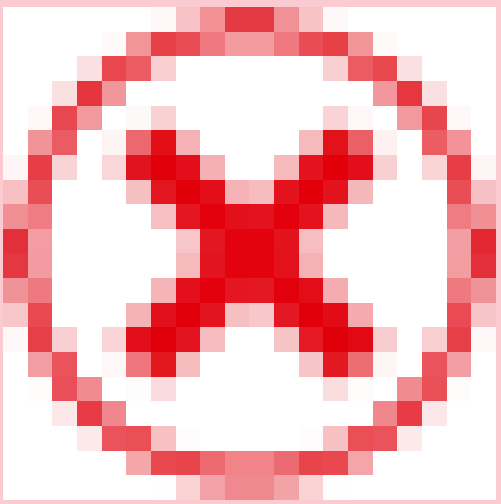
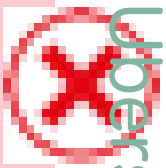
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Tests				
Meine Genehmigungen				
Testergebnisse				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Nicht selektierte Testergebnisse	✗	✗	✓	
Meine offenen Testergebnisse	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

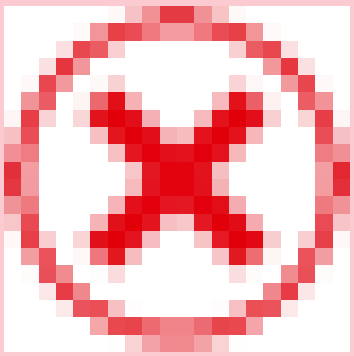
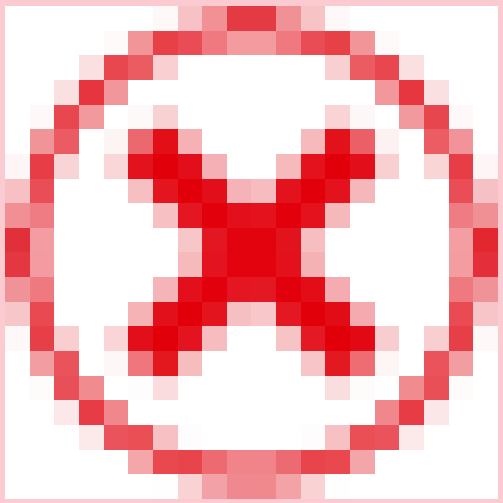
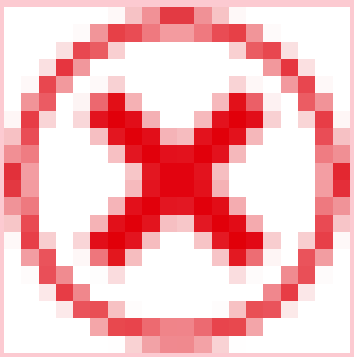
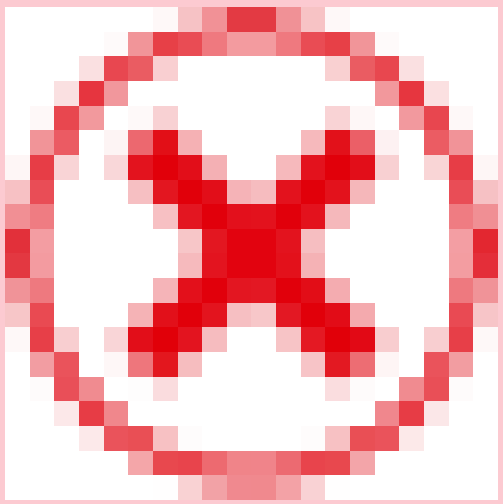
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Offene Testergebnisse				
Ziel rückt näher				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

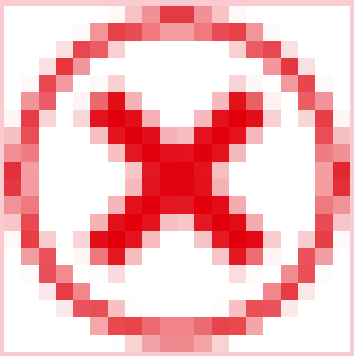
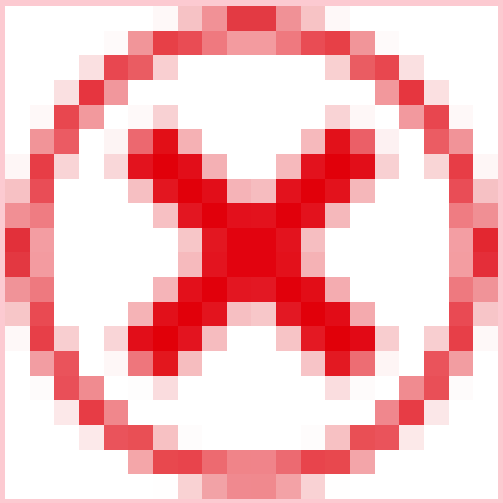
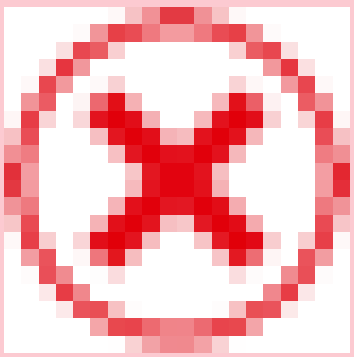
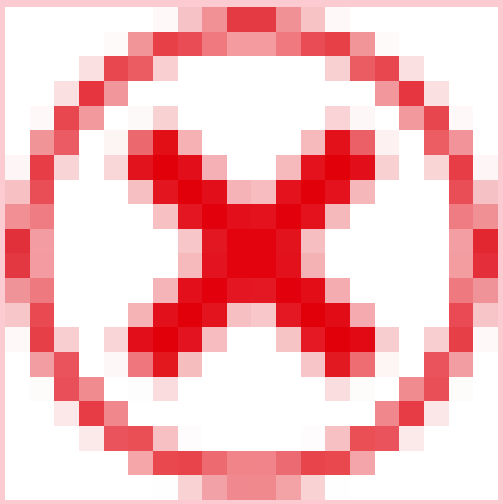
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Verfehltes Ziel				
Nicht zugewiesen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

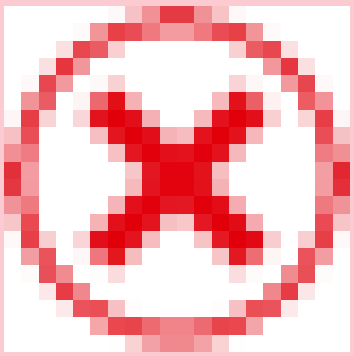
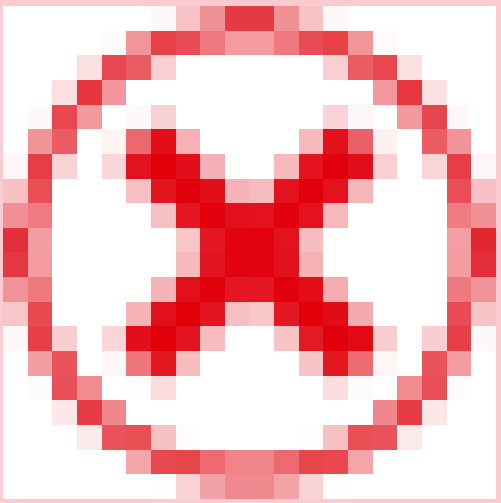
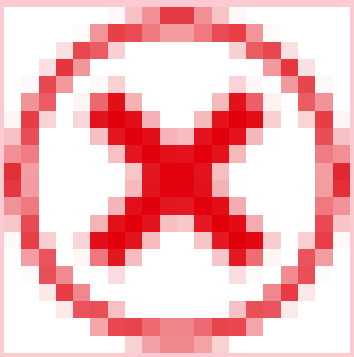
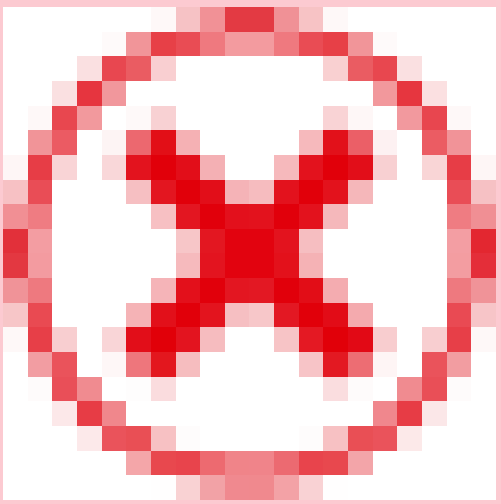
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Mehrere Zurückstellungen				
Alle				
Testergebnisgruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

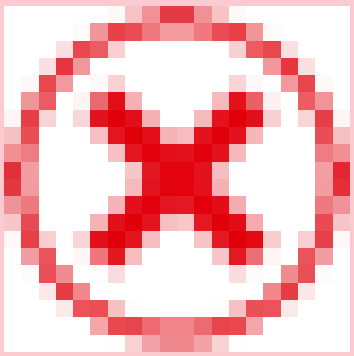
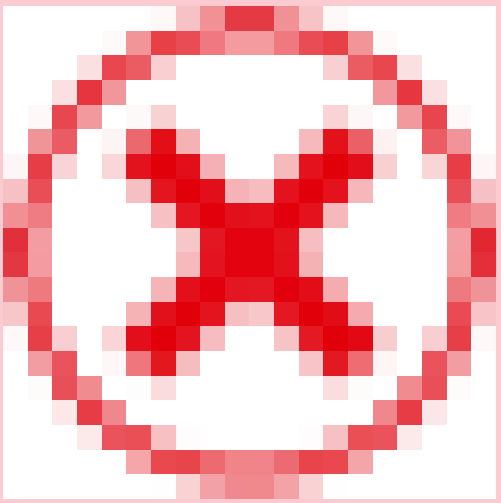
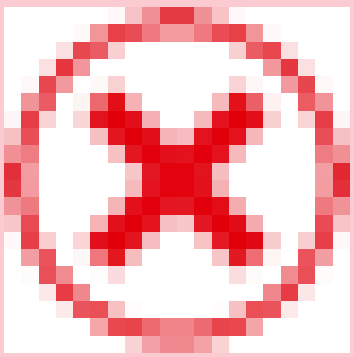
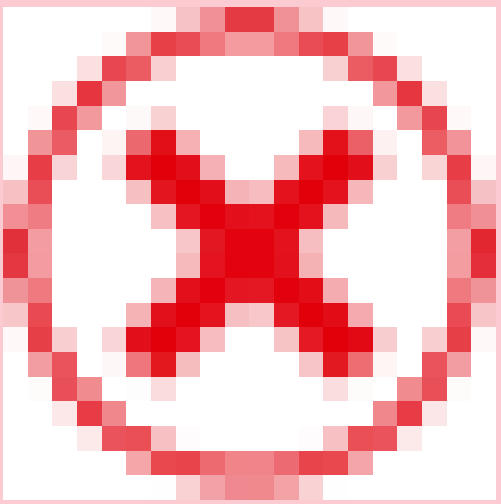
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Meine offenen Gruppen				
Alle offenen Gruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

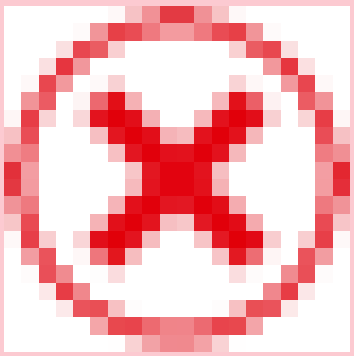
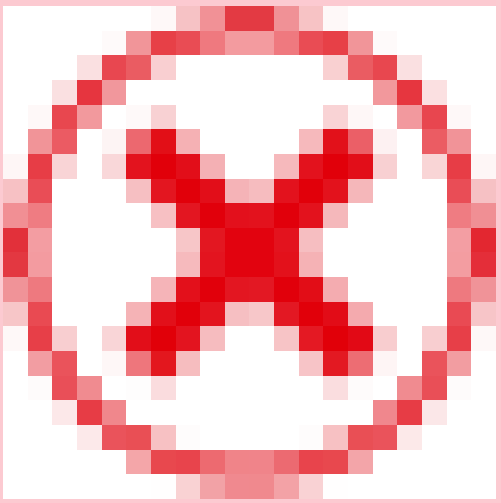
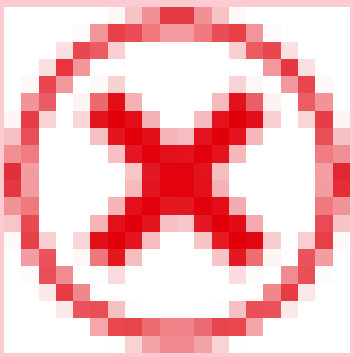
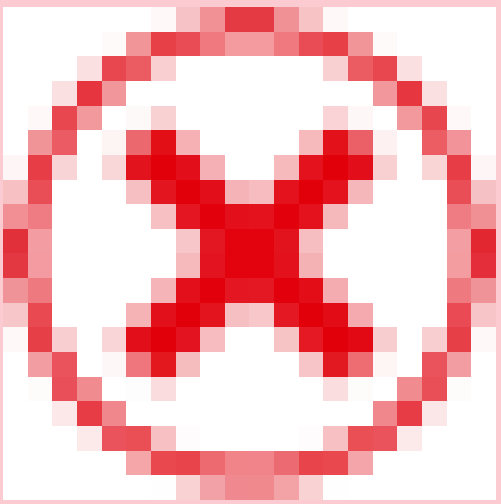
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Mehrere Zurückstellungen				
Alle Gruppen				
Unterstützungsdaten				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

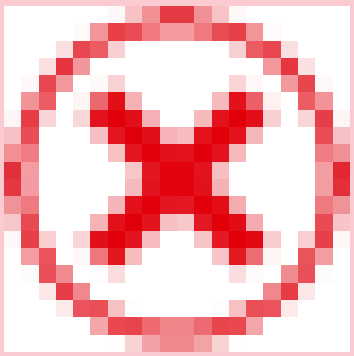
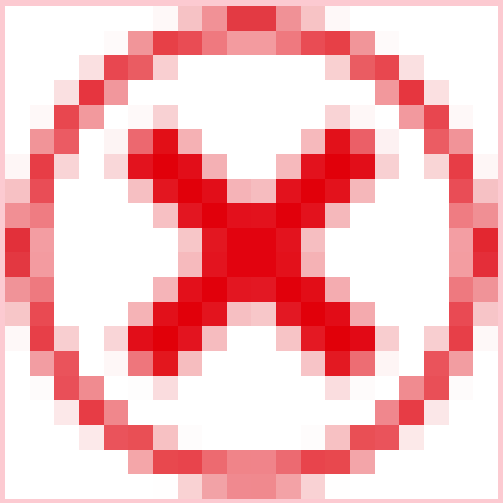
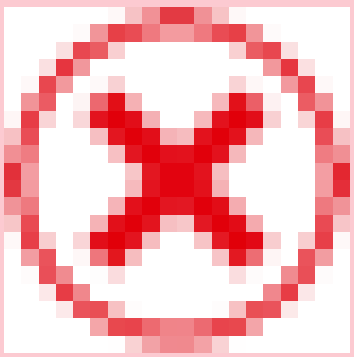
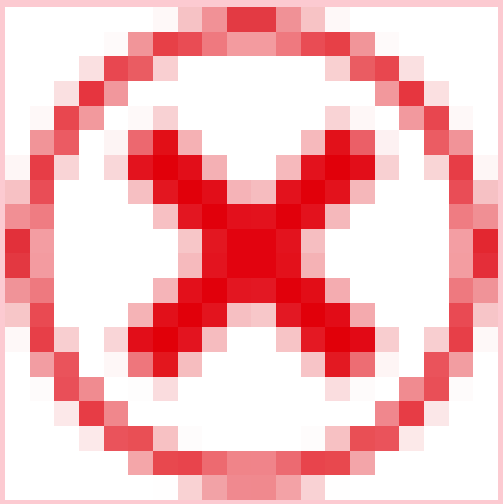
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Autoritative Quellen				
Technologien				
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

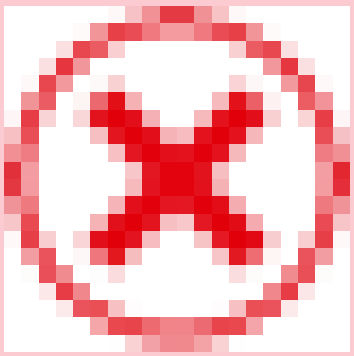
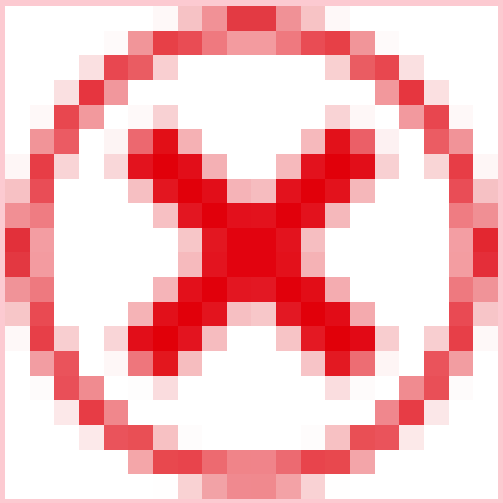
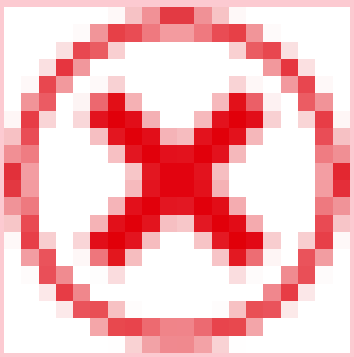
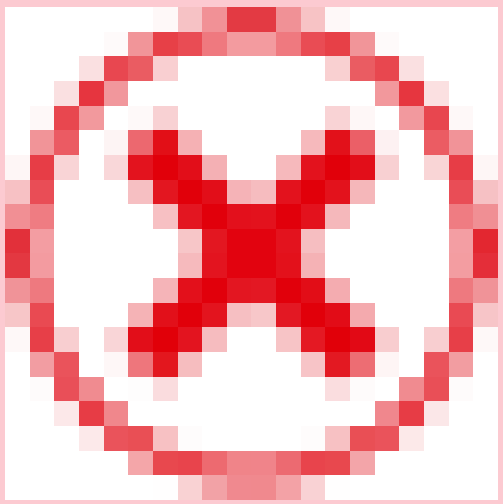
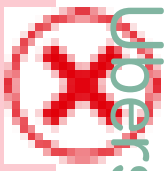
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Zuweisungsregeln				
Veraltete Testergebnisse automatisch schließen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

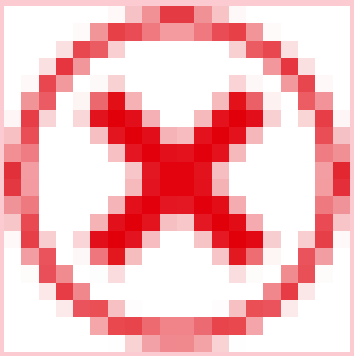
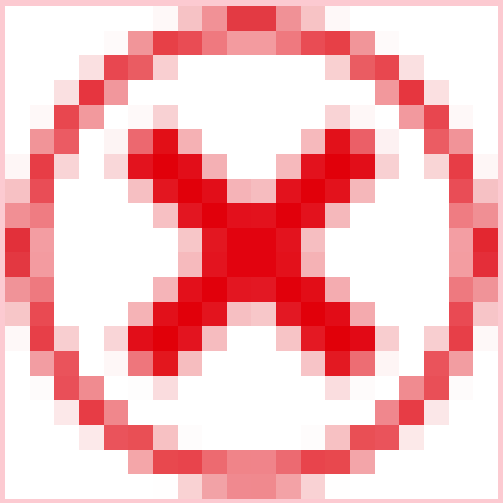
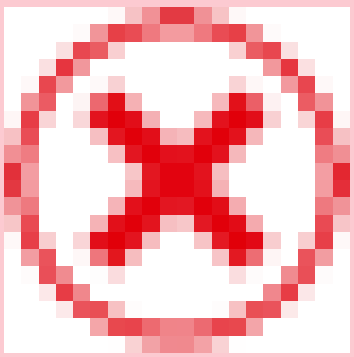
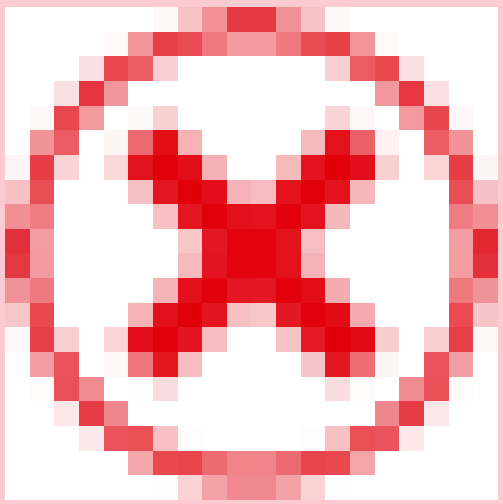
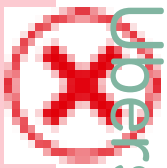
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Gruppenregeln				
Automatische Ausnahmeregel				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

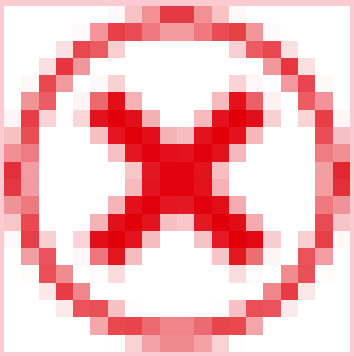
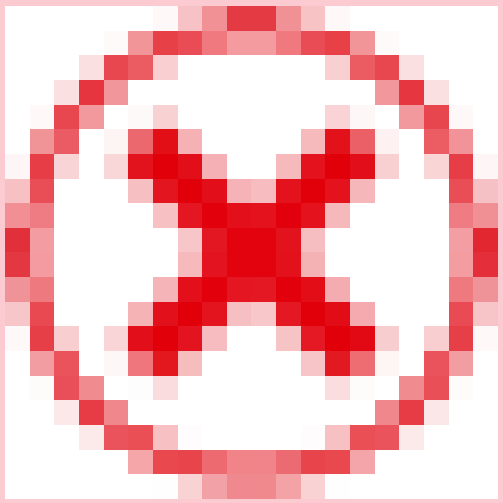
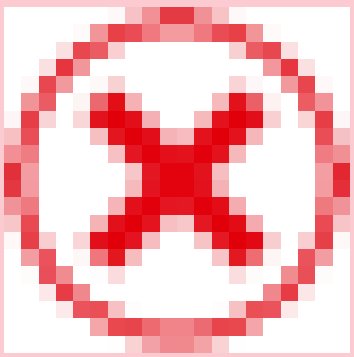
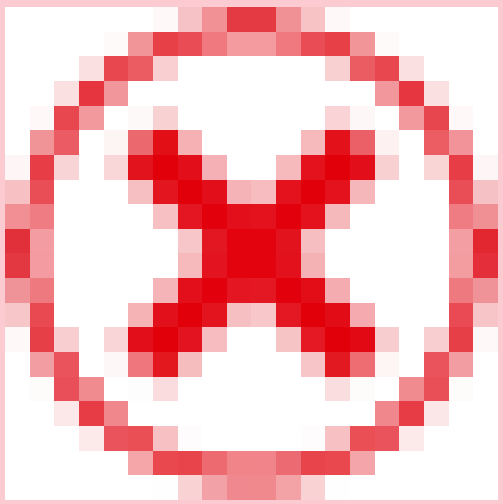
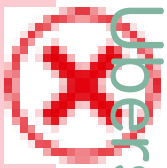
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Genehmigungsregeln				
Risikorechner				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

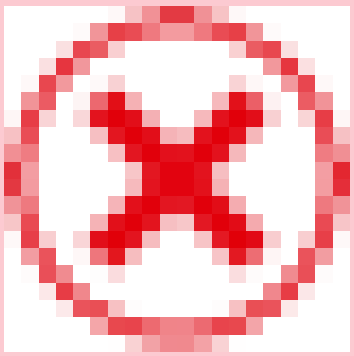
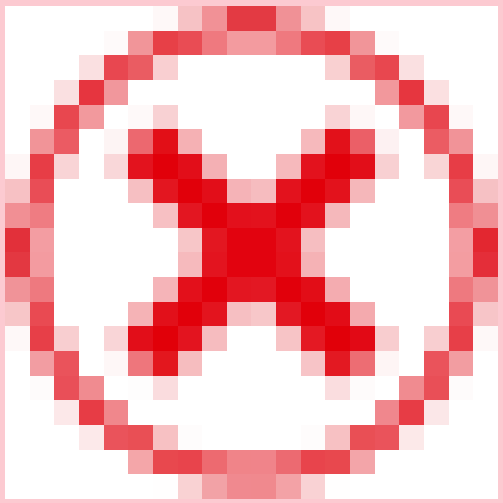
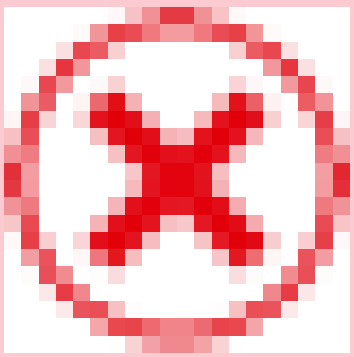
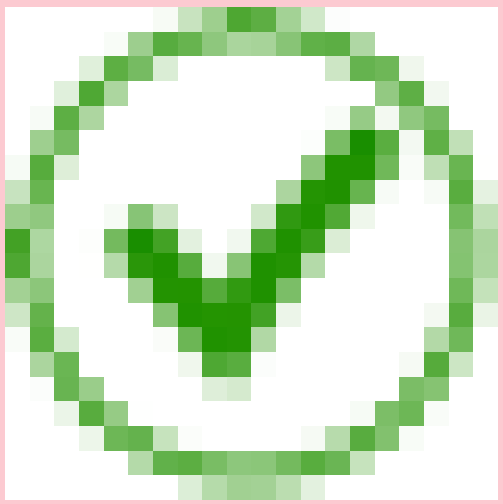
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Rollup-Rechner für Risikopunktzahl				
Korrekturzielregeln				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

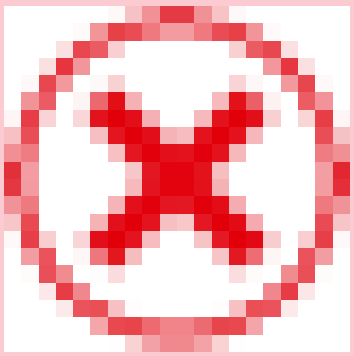
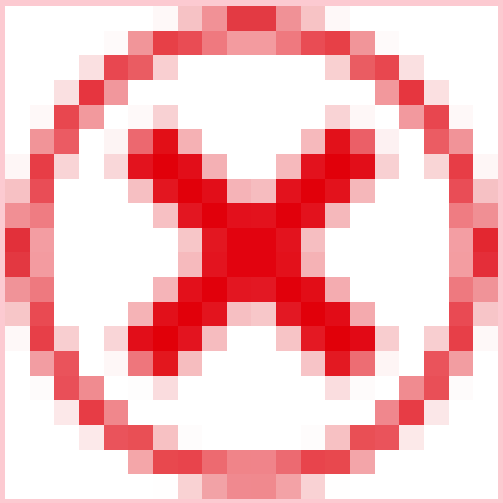
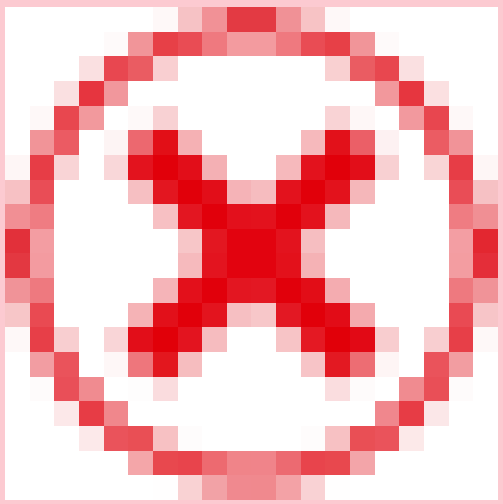
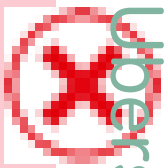
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Relevanz-Zuordnung				
Benachrichtigungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

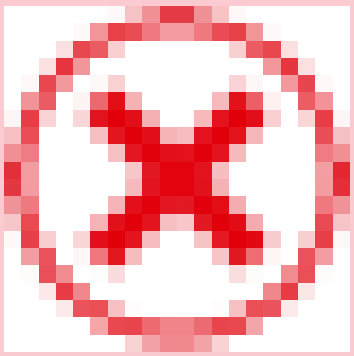
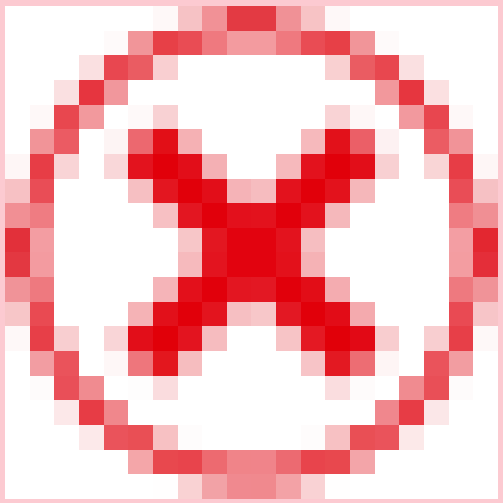
Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

(Fortsetzung)

Modul	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.lesen	sn_vu
Ausnahmenverwaltung				

Modulzugriff für: sn_vulc.remediation_owner

Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Modul	sn_vulc.remediation_owner
(Haupt-App-Gruppe)	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

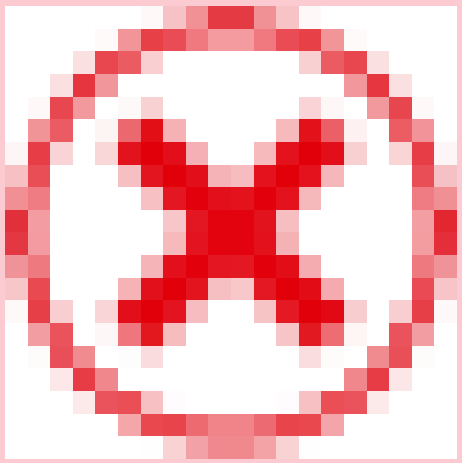
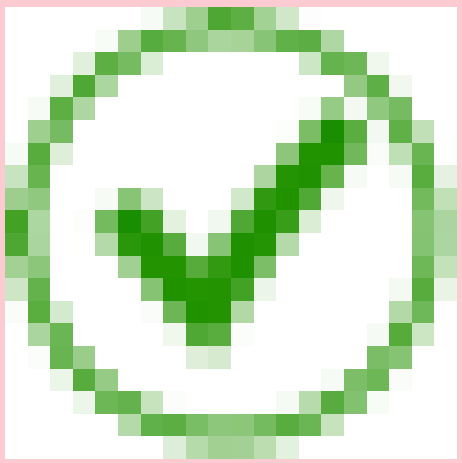
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Übersicht	
Richtlinien	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

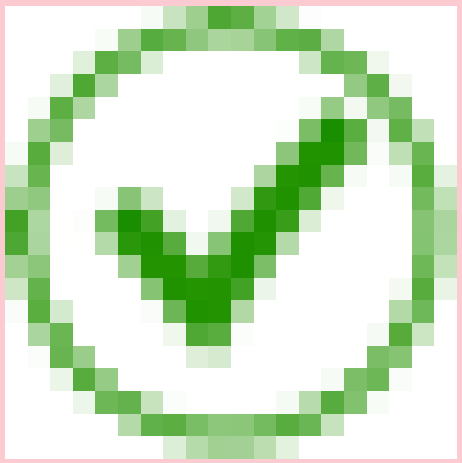
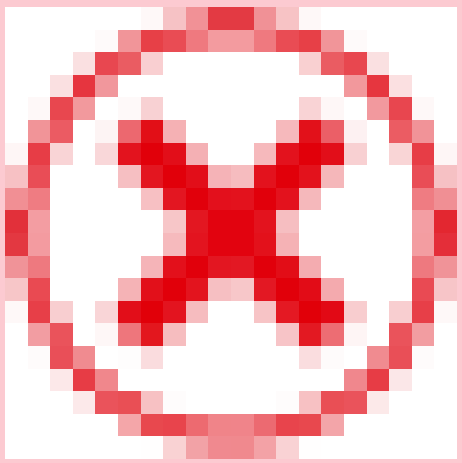
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Tests	
Meine Genehmigungen	
Testergebnisse	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

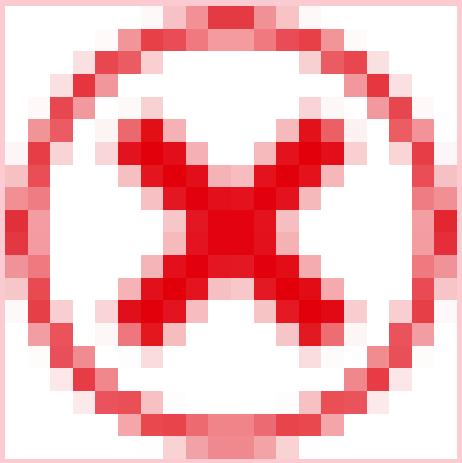
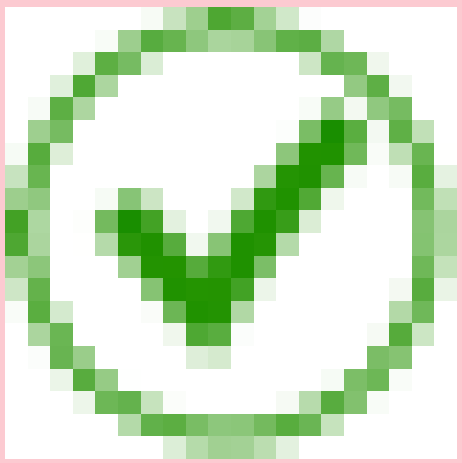
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Nicht selektierte Testergebnisse	
Meine offenen Testergebnisse	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Offene Testergebnisse	✗
Ziel rückt näher	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

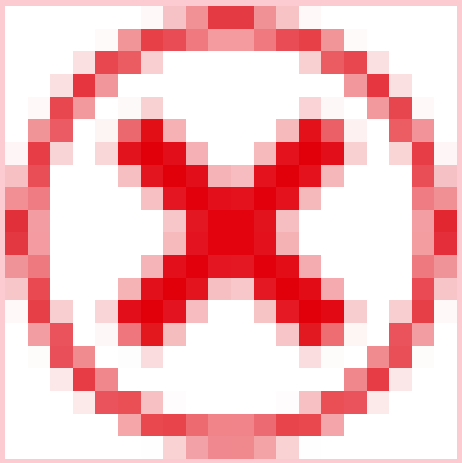
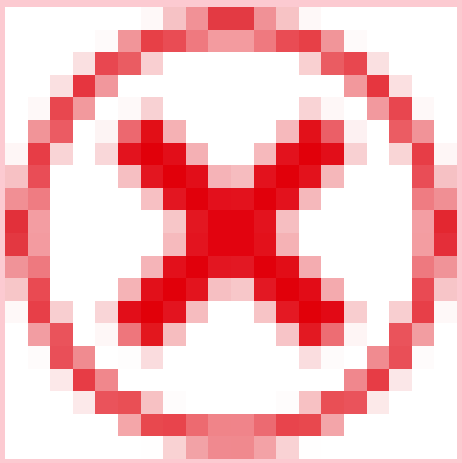
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Verfehltes Ziel	
Nicht zugewiesen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

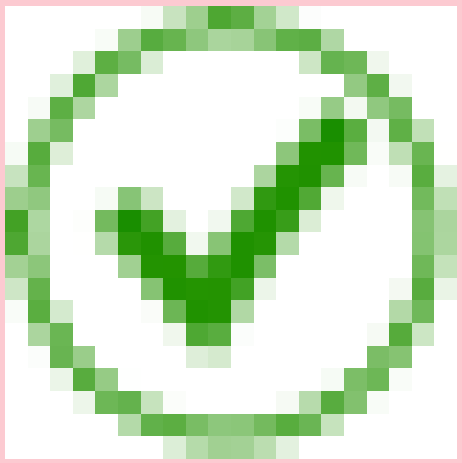
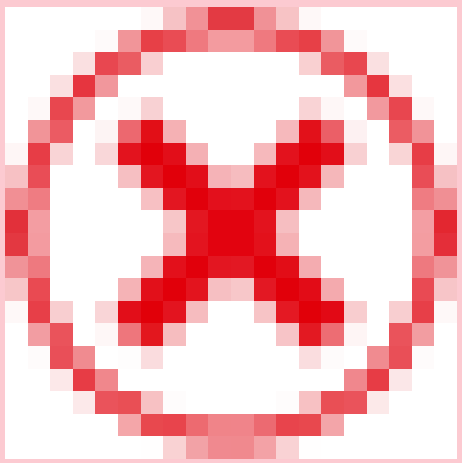
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Mehrere Zurückstellungen	
Alle	
Testergebnisgruppen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

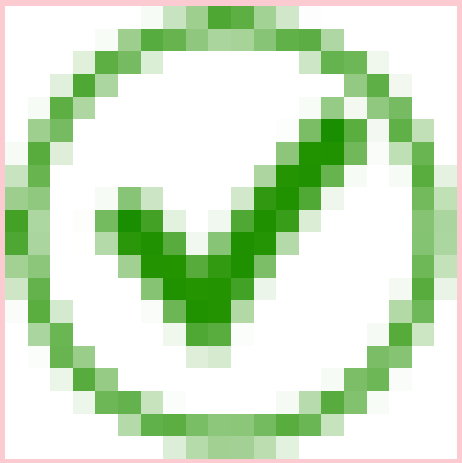
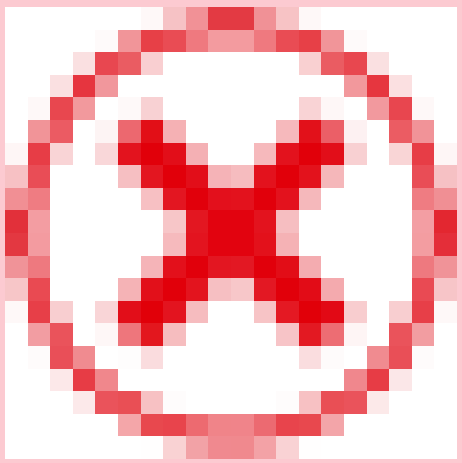
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Meine offenen Gruppen	
Alle offenen Gruppen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

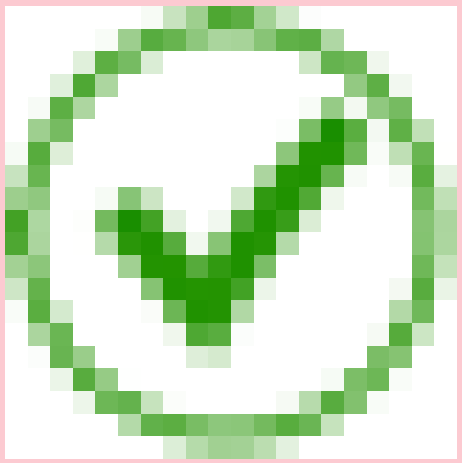
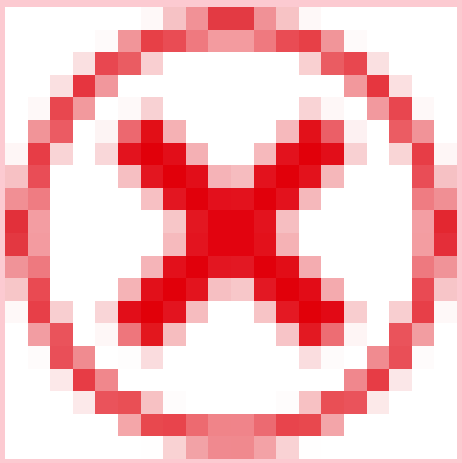
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Mehrere Zurückstellungen	
Alle Gruppen	
Unterstützungsdaten	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

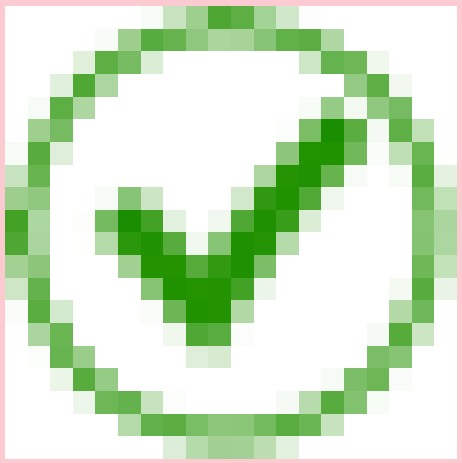
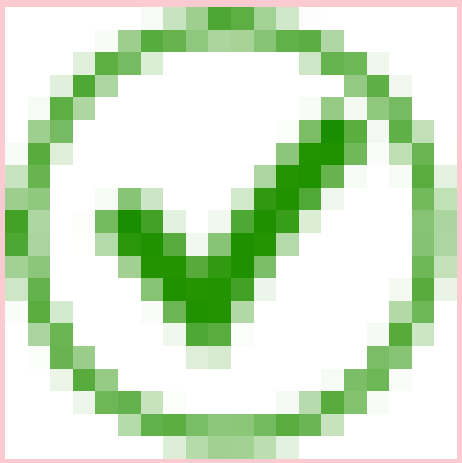
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Autoritative Quellen	
Technologien	
Administration	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

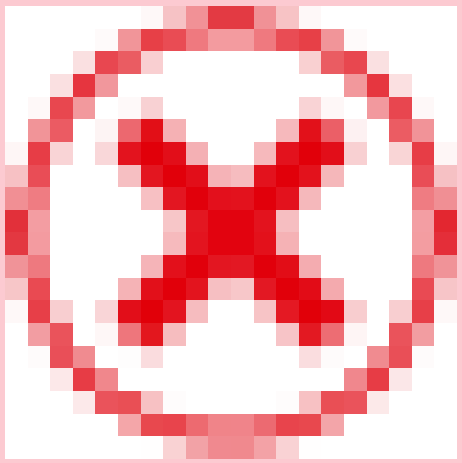
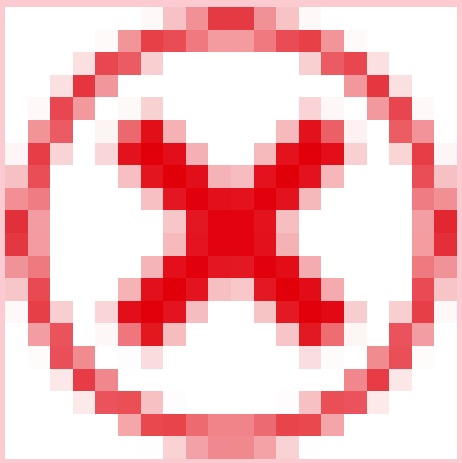
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Zuweisungsregeln	
Veraltete Testergebnisse automatisch schließen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

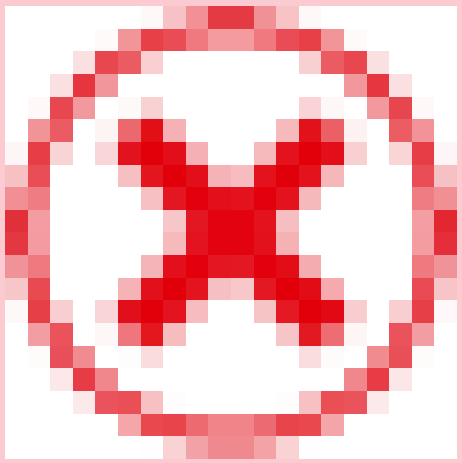
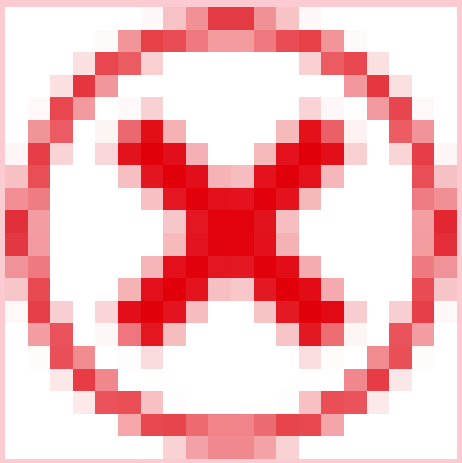
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Gruppenregeln	
Automatische Ausnahmeregel	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

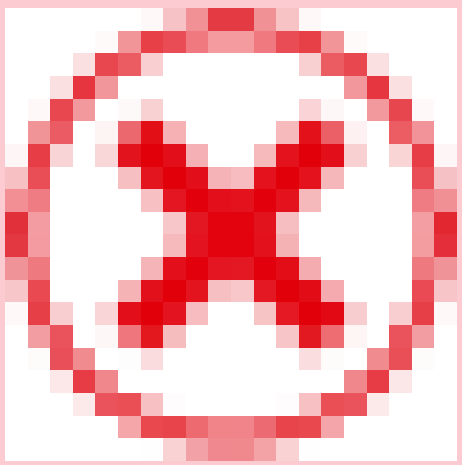
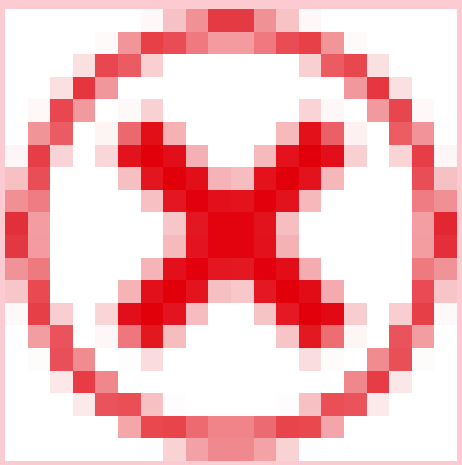
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Genehmigungsregeln	
Risikorechner	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

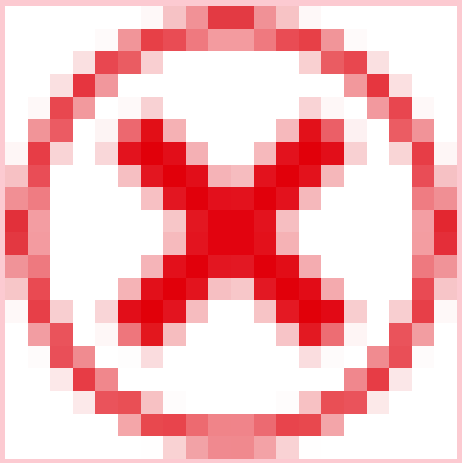
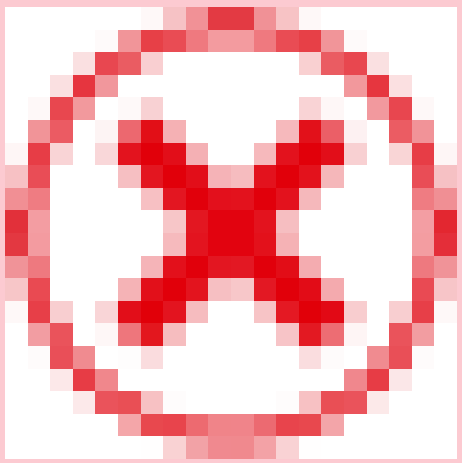
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Rollup-Rechner für Risikopunktzahl	
Korrekturzielregeln	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

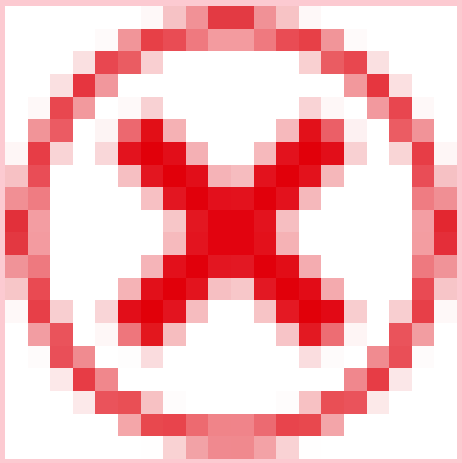
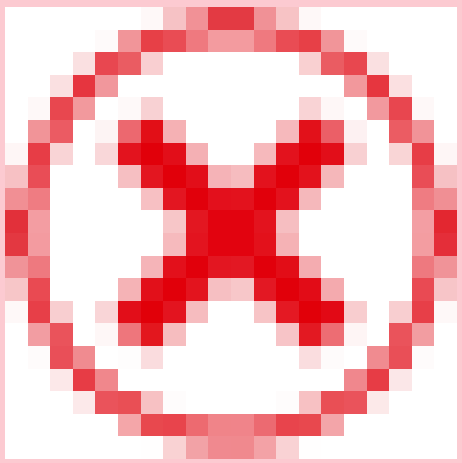
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Relevanz-Zuordnung	
Benachrichtigungen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

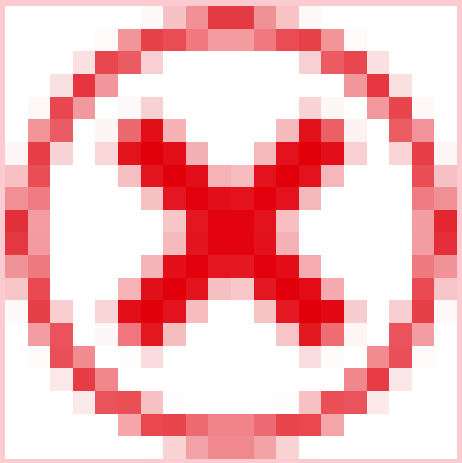
Modulzugriff für: sn_vulc.remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

(Fortsetzung)

Modul	sn_vulc.remediation_owner
Ausnahmenverwaltung	

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Container Vulnerability Response

Informationen zu Container Vulnerability Response finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

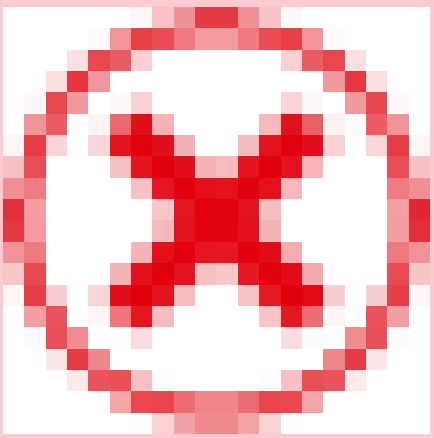
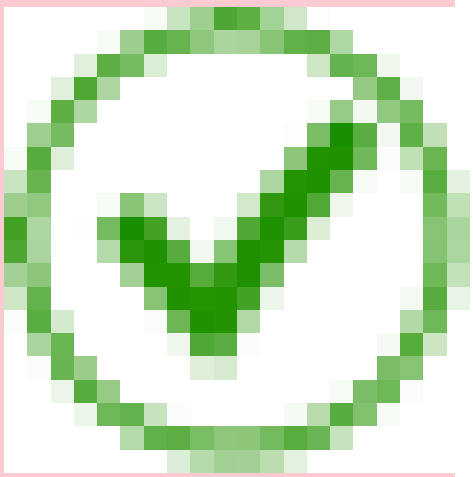
Informationen für andere Rollen:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
(Haupt-App-Gruppe)			
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

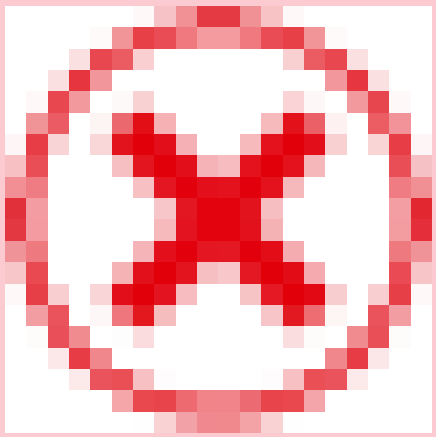
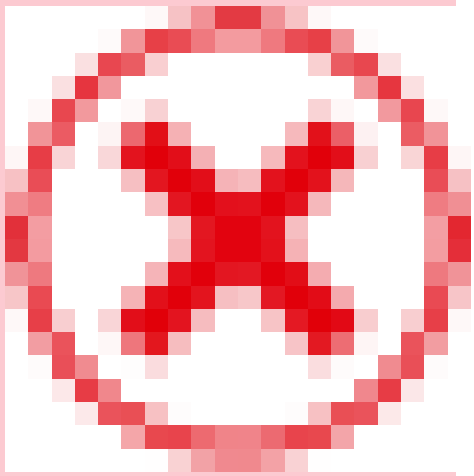
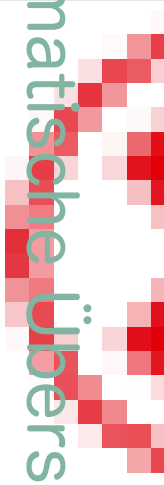
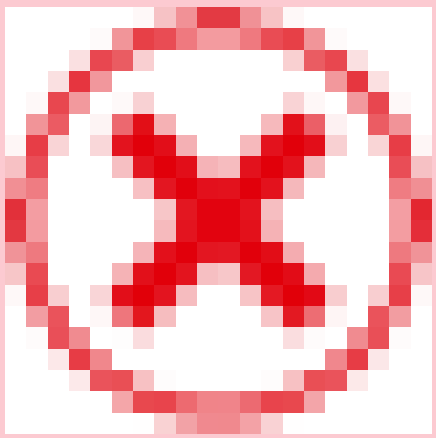
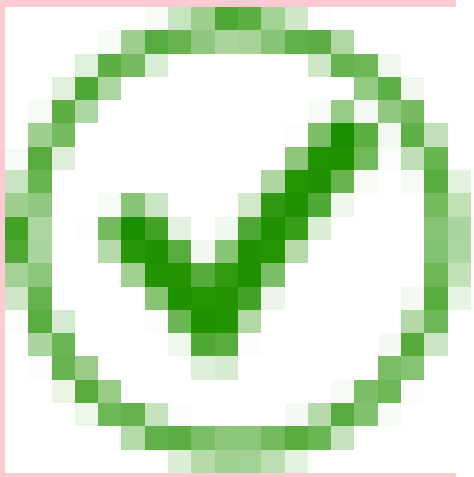
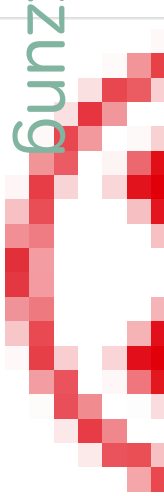
sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Meine Genehmigungen			
Angreifbare Container-Elemente			
Mir zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

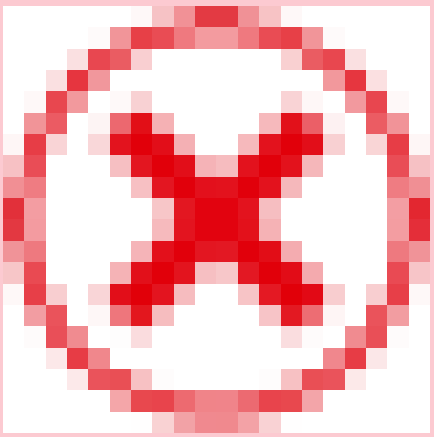
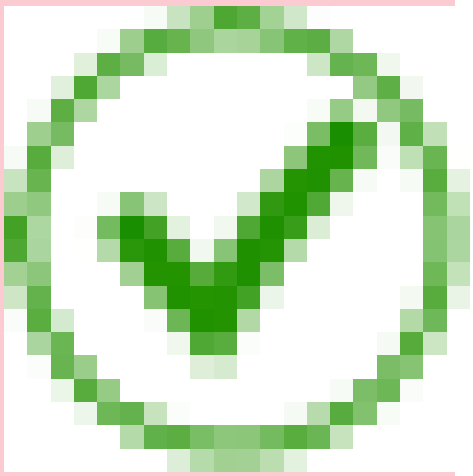
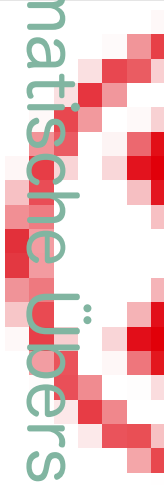
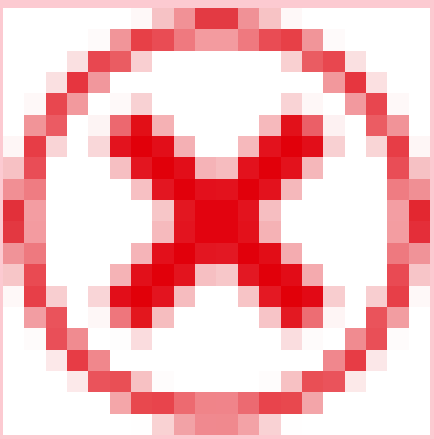
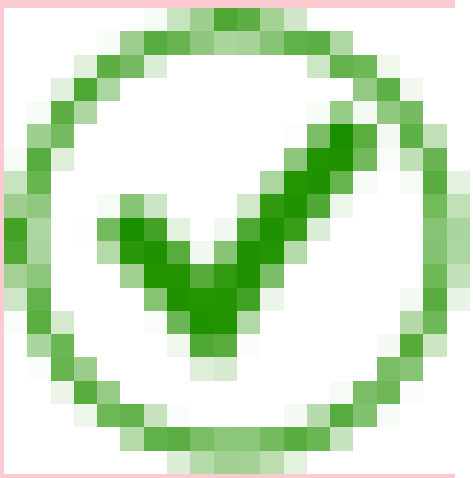
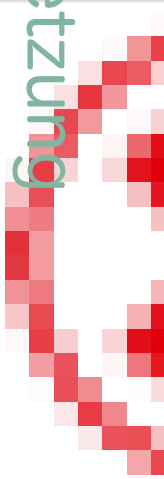
sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Meinen Gruppen zugewiesen			
Kritisches und hohes Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Nutzbar	✗	✓	
Ziel rückt näher	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

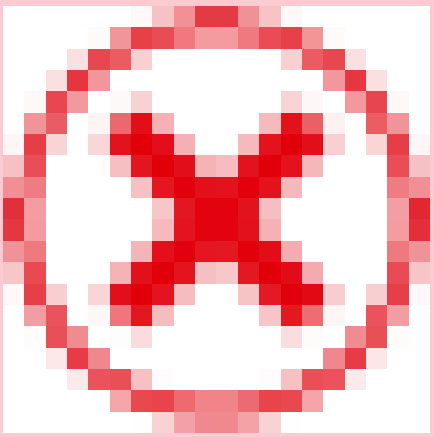
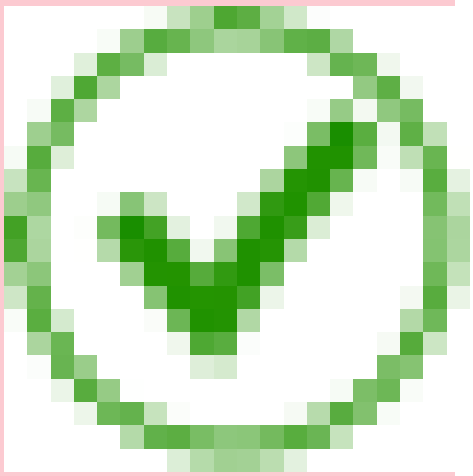
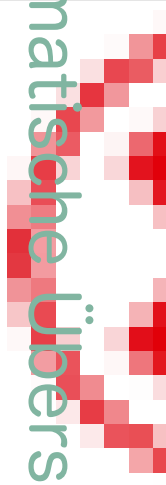
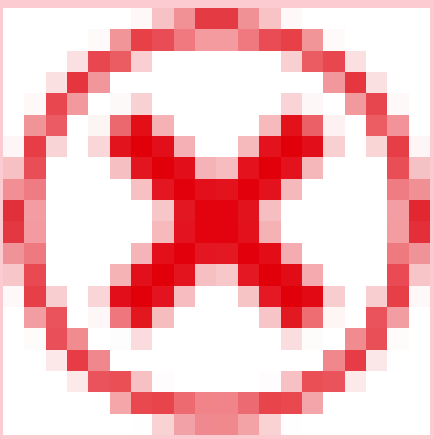
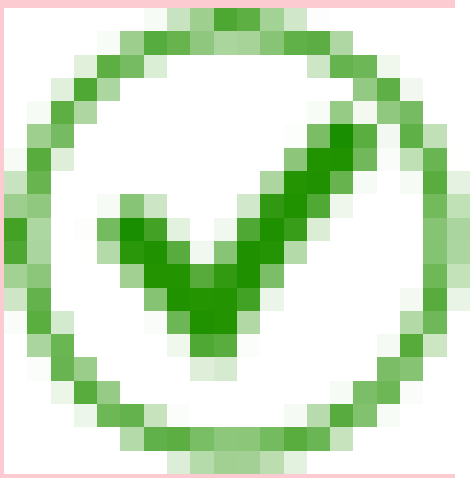
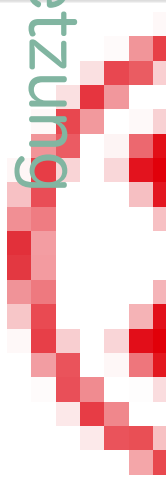
sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Verfehltes Ziel			
Alle			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
NVD	✗	✓	
Drittpartei	✗	✓	
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Zuweisungsregeln	✗	✗	✗
Schwachstellen-Rechner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Korrekturzielregeln	✗	✗	✗
VI-Granularität konfigurieren	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Ausnahmeregeln	✗	✗	✗
Genehmigungsregeln	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

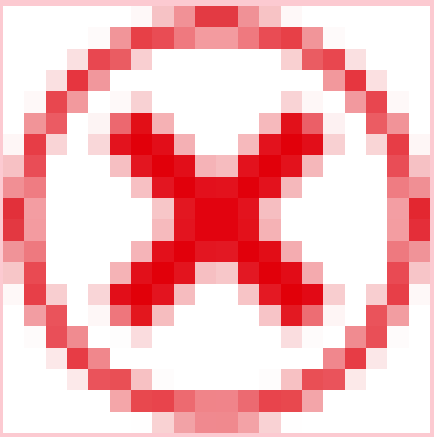
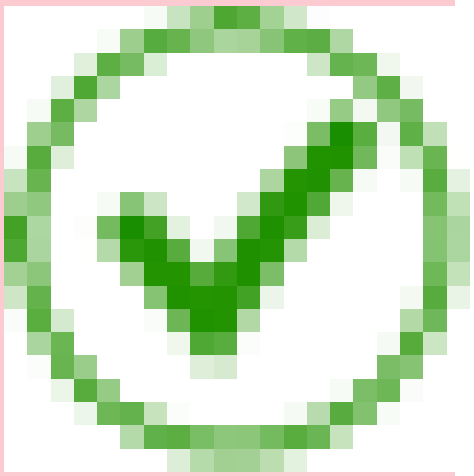
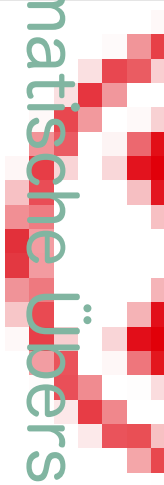
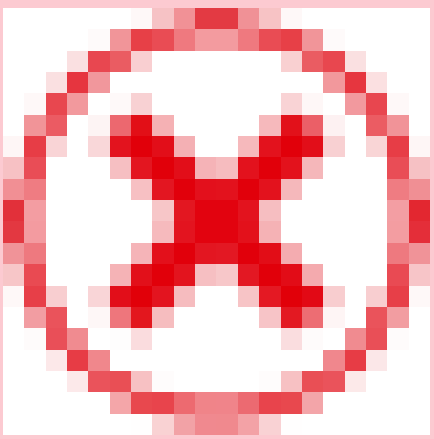
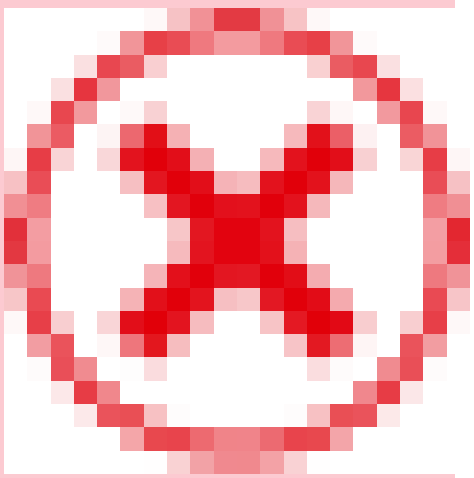
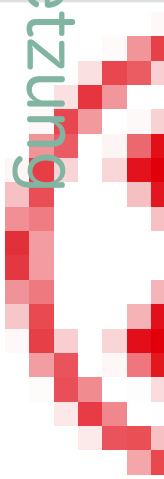
sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Container-Sicherheitsintegrationen			
Angreifbare Elemente automatisch schließen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informationen für andere Rollen:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_contai
Normalisierte Schweregradzuordnungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

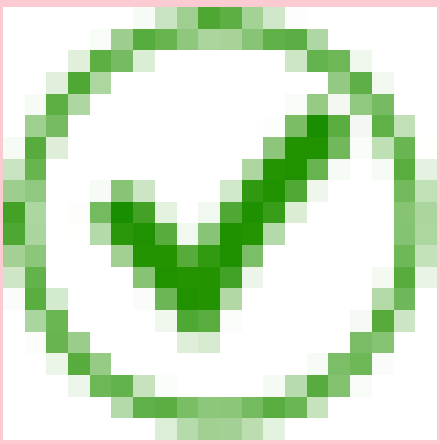
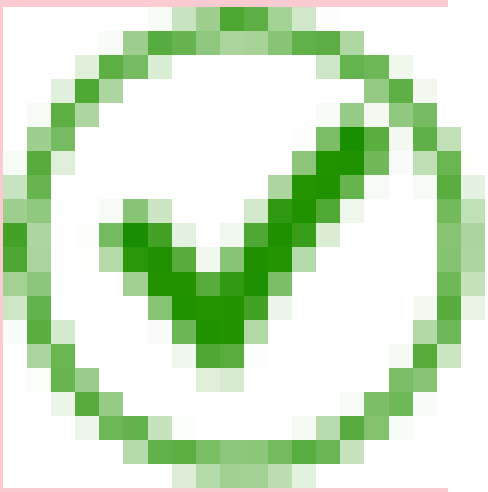
Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
(Haupt-App-Gruppe)			
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

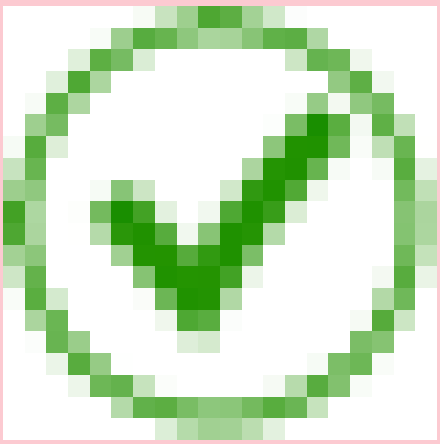
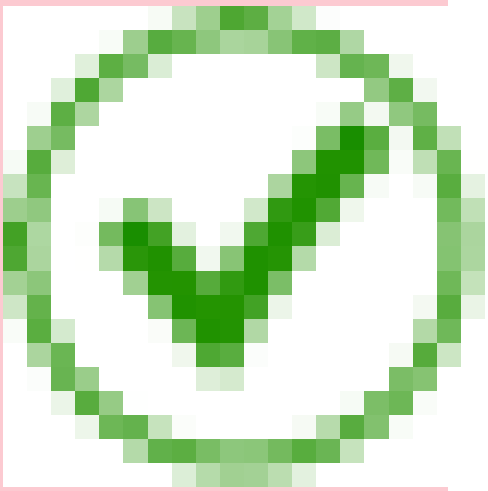
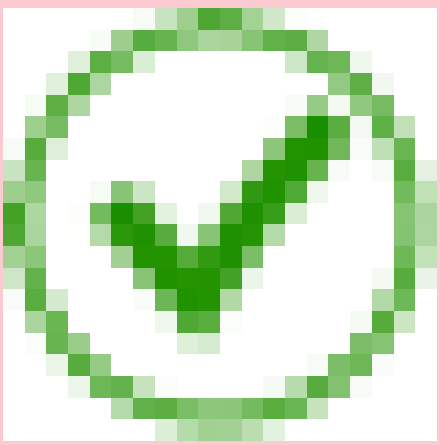
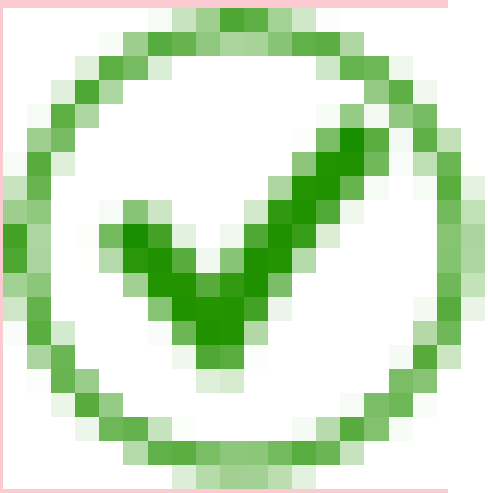
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Meine Genehmigungen			
Angreifbare Container-Elemente			
Mir zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

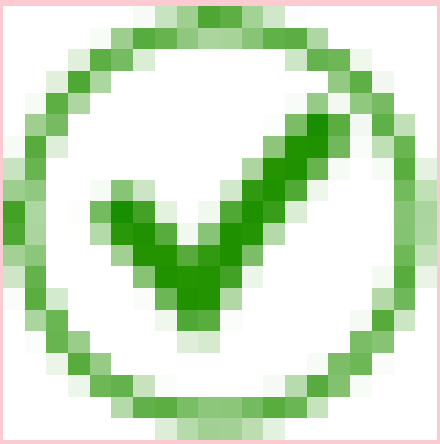
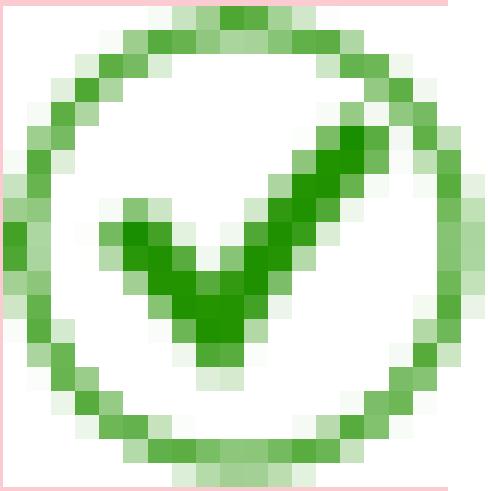
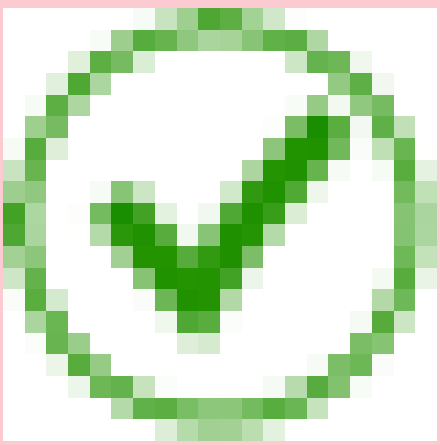
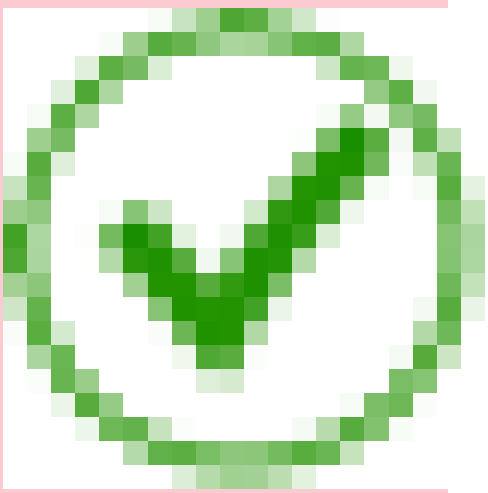
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Meinen Gruppen zugewiesen			
Kritisches und hohes Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

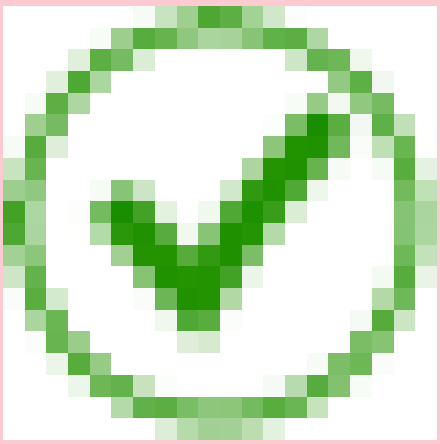
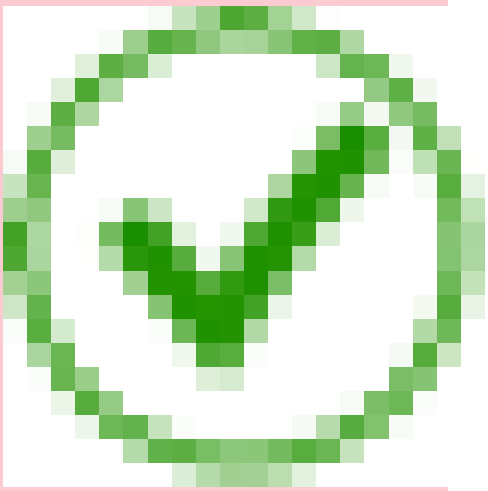
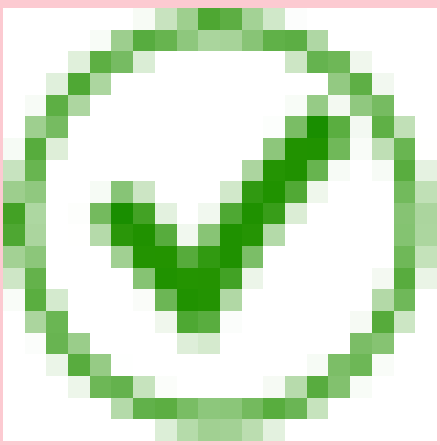
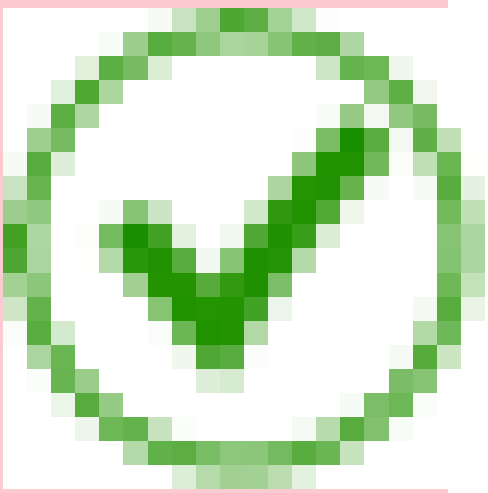
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Nutzbar			
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

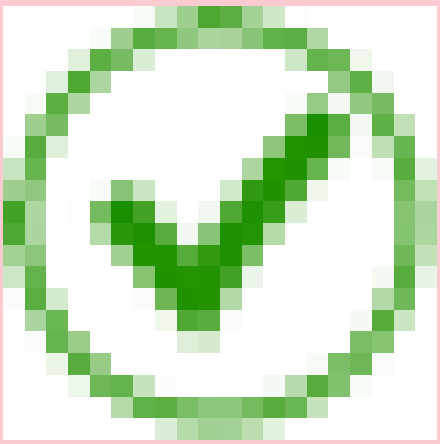
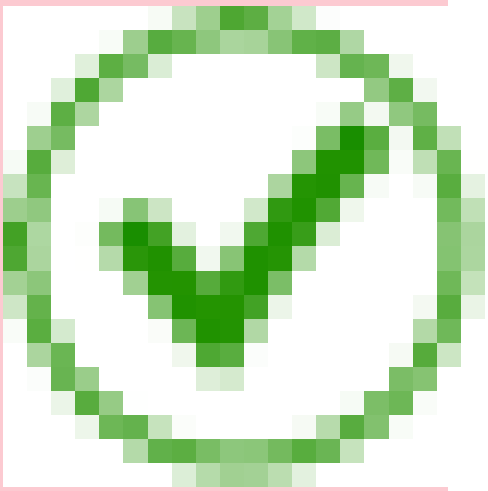
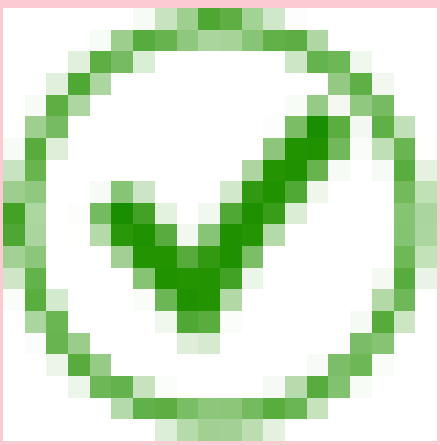
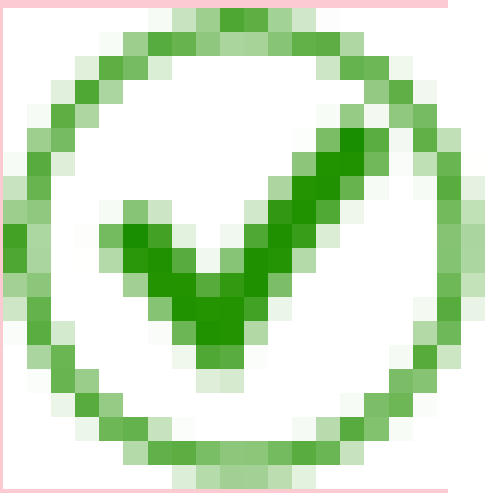
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Verfehltes Ziel			
Alle			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

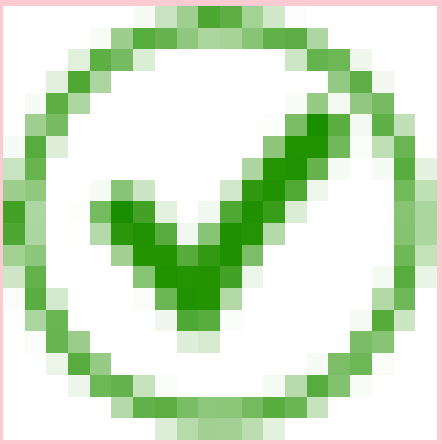
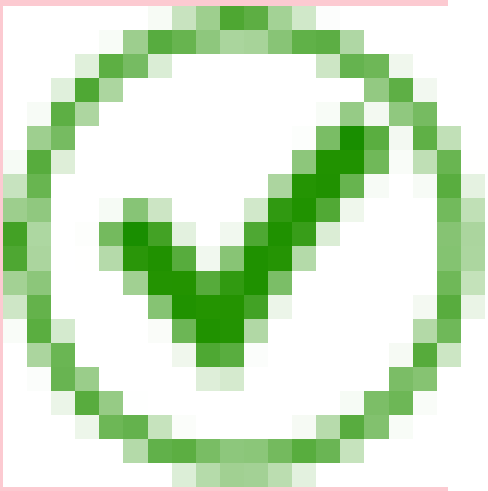
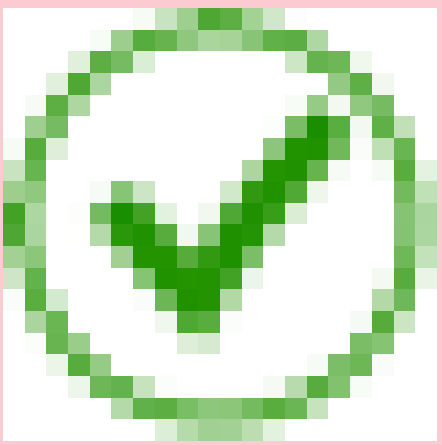
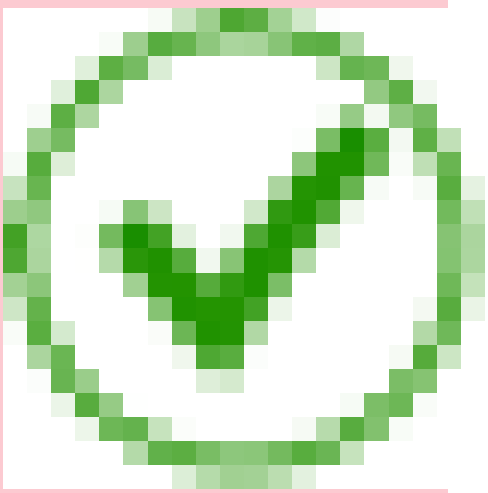
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
NVD			
Drittpartei			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

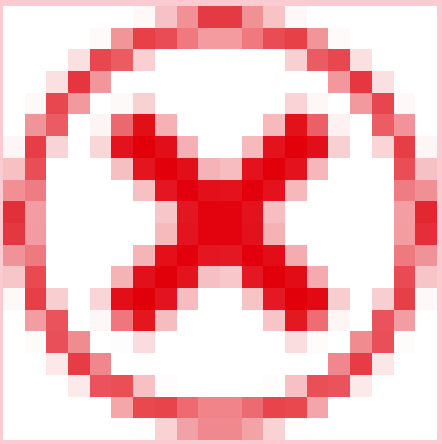
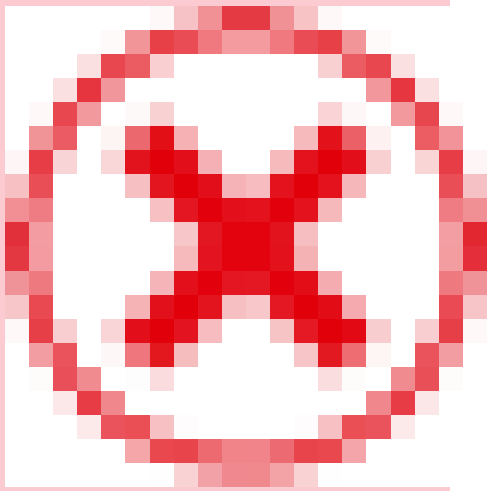
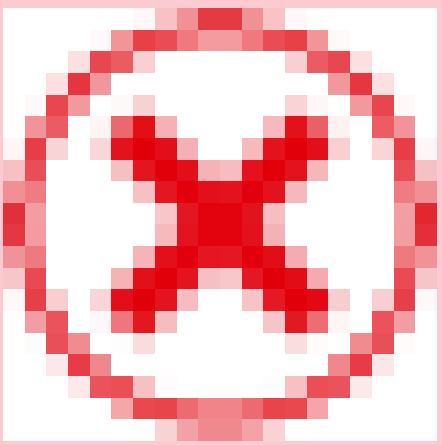
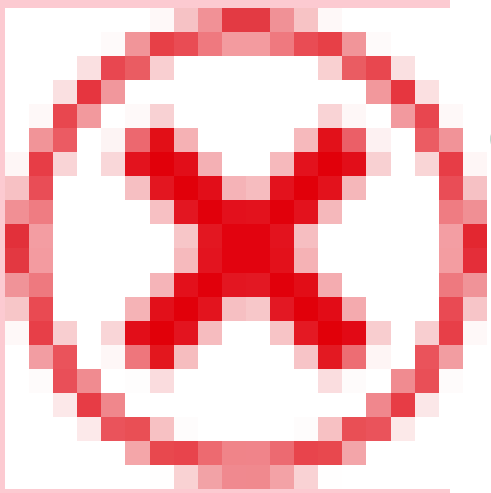
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Zuweisungsregeln			
Schwachstellen-Rechner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

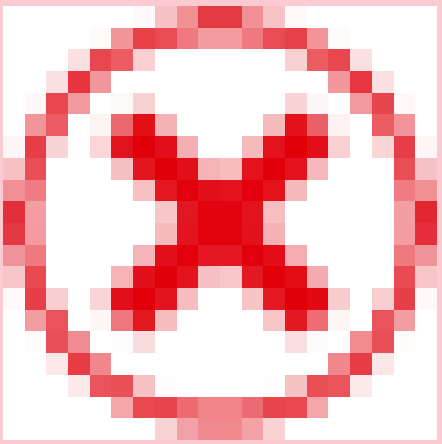
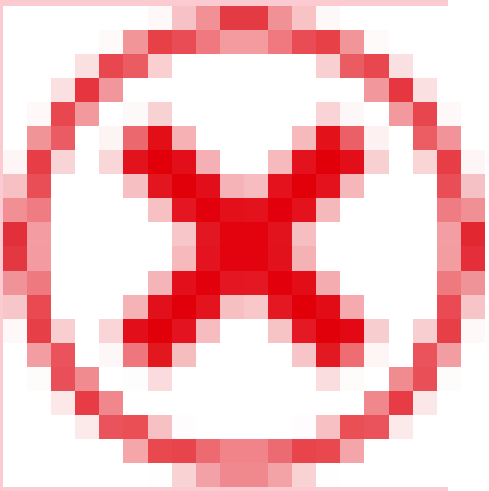
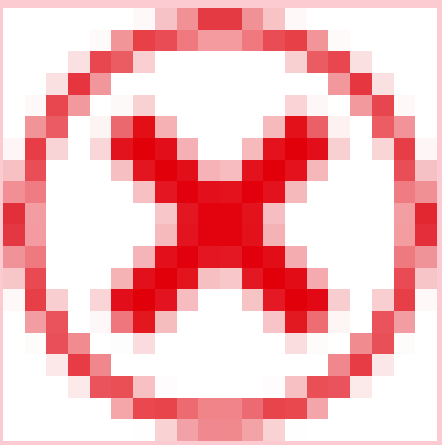
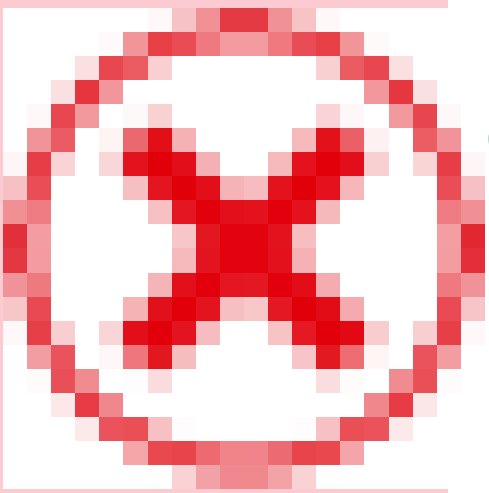
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Korrekturzielregeln			
VI-Granularität konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

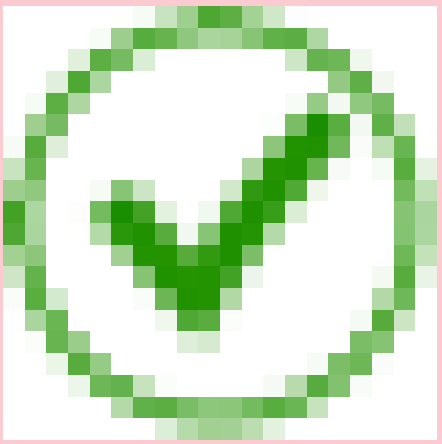
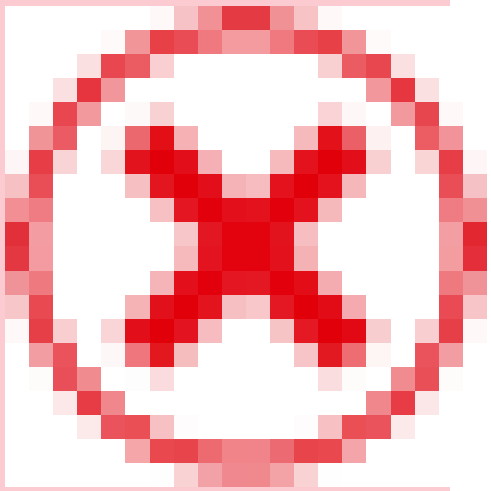
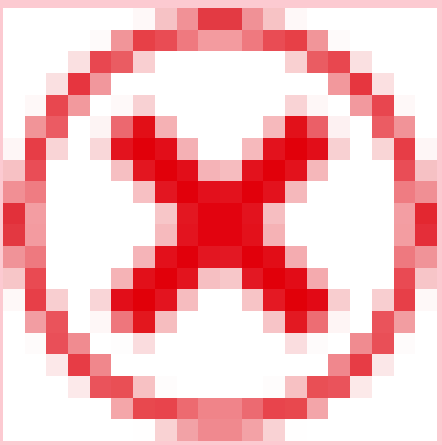
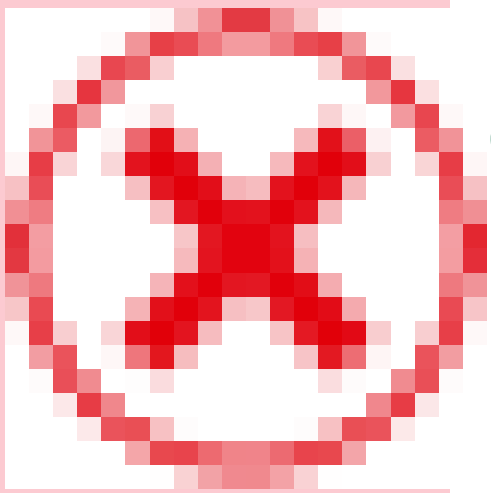
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Ausnahmeregeln			
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

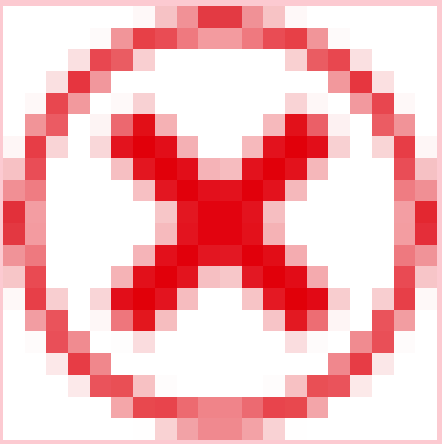
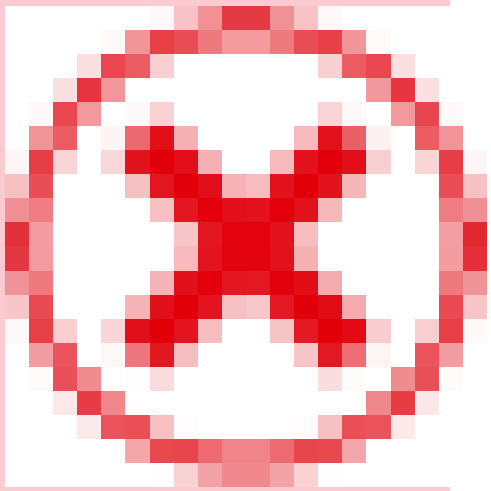
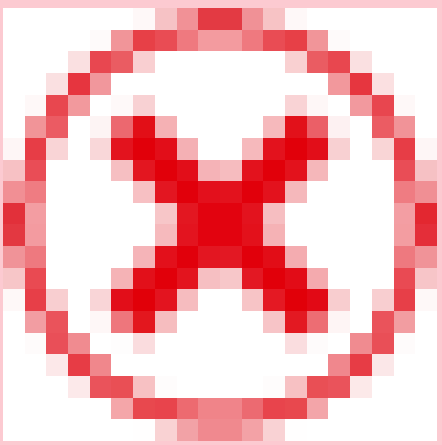
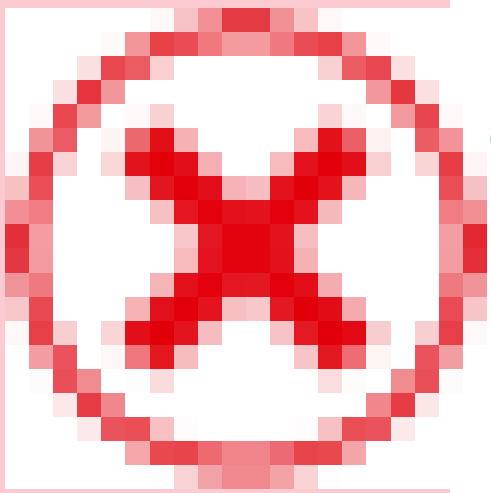
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Container-Sicherheitsintegrationen			
Angreifbare Elemente automatisch schließen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Informationen für andere Rollen:

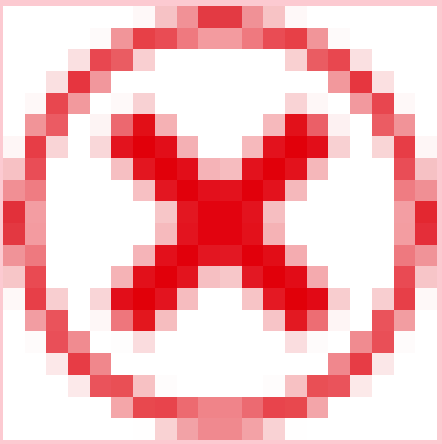
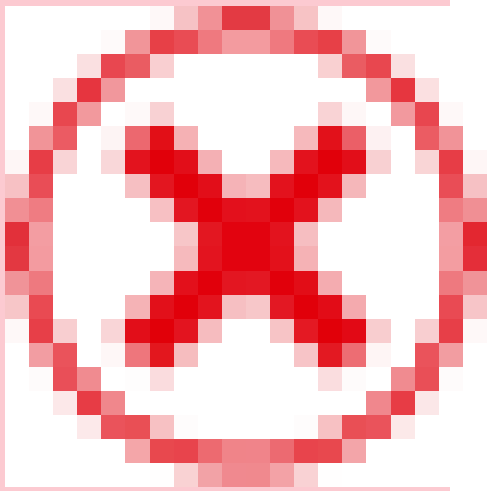
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_cont
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

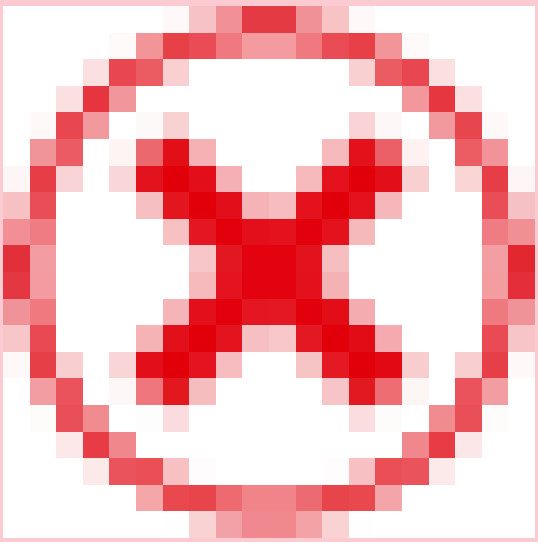
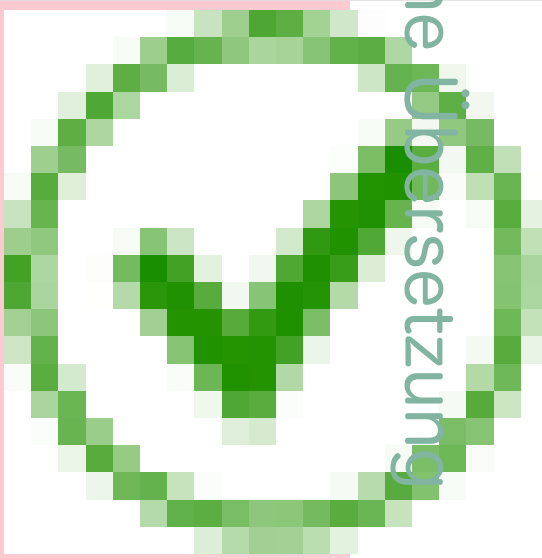
Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
(Haupt-App-Gruppe)		
Übersicht		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

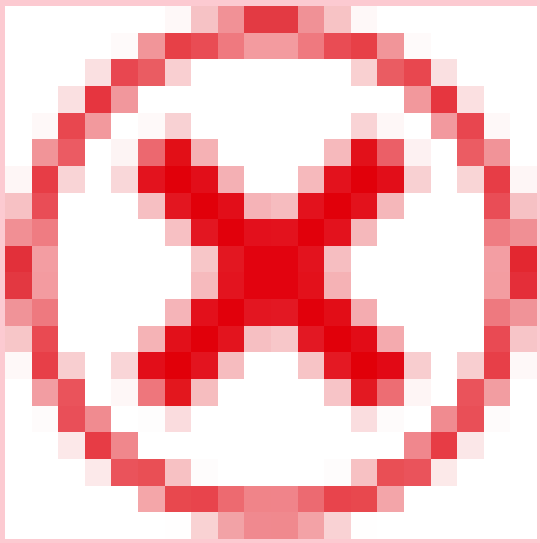
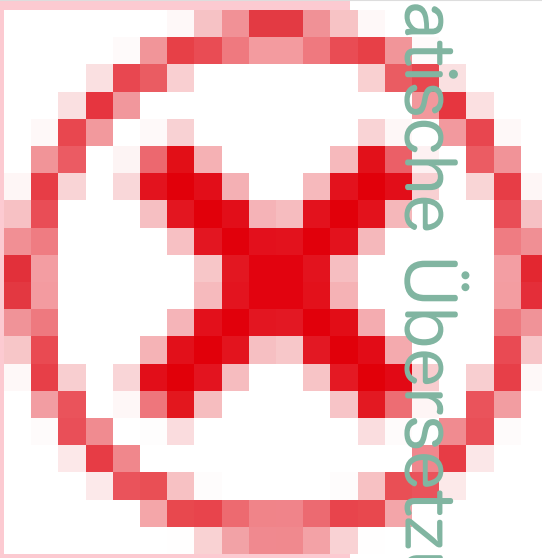
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Meine Genehmigungen		
Angreifbare Container-Elemente		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

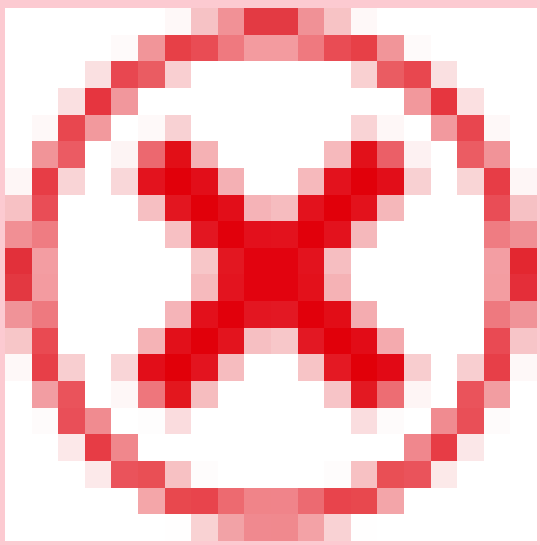
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Mir zugewiesen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

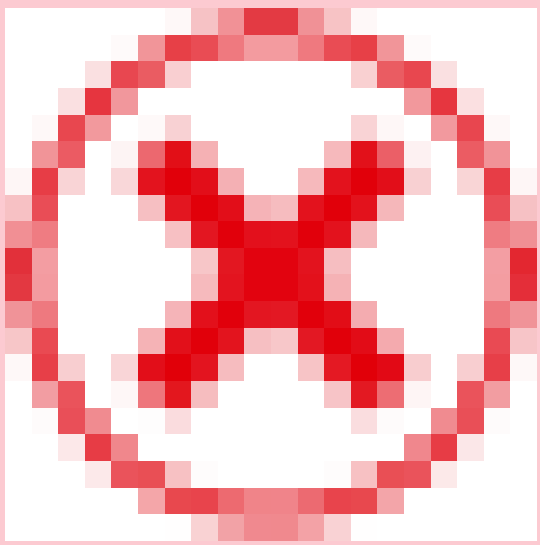
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Meinen Gruppen zugewiesen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

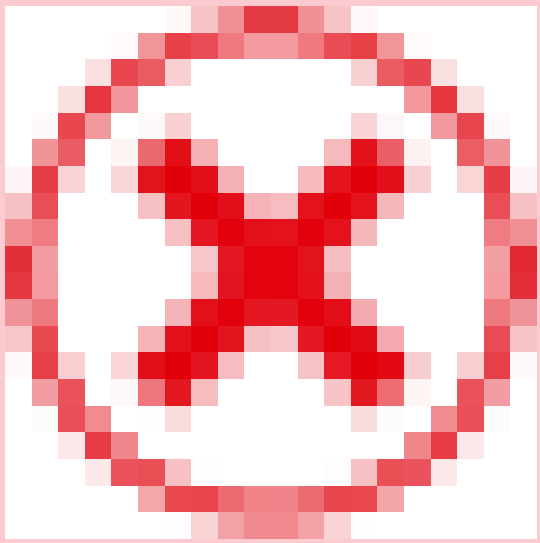
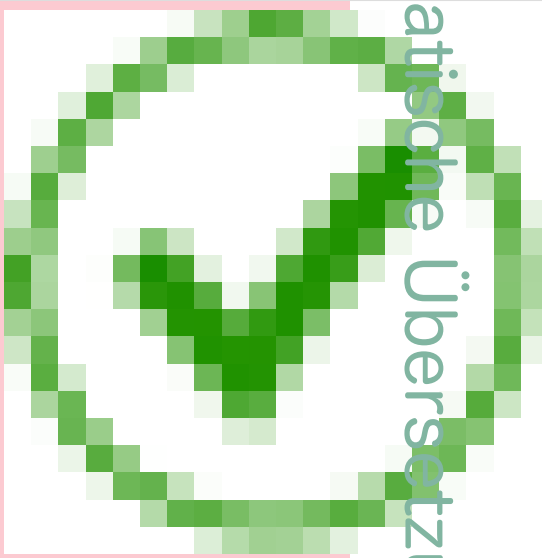
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Kritisches und hohes Risiko		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

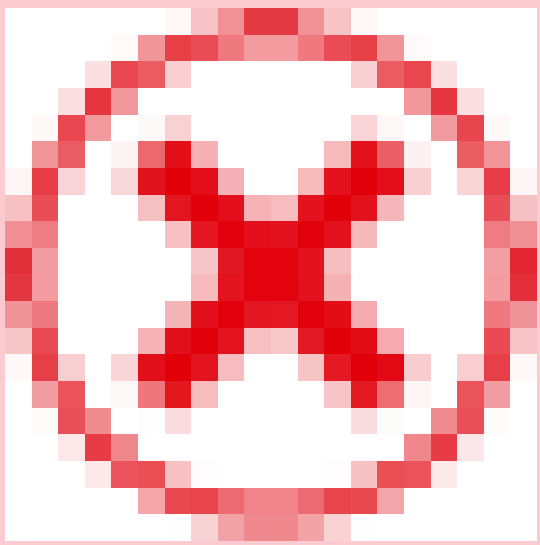
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Nutzbar		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

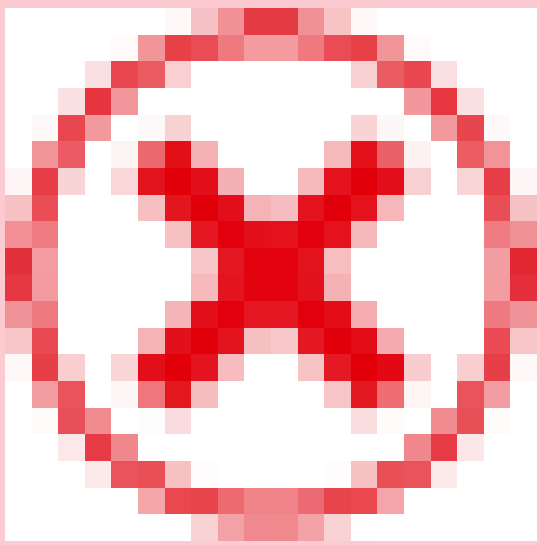
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Ziel rückt näher		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

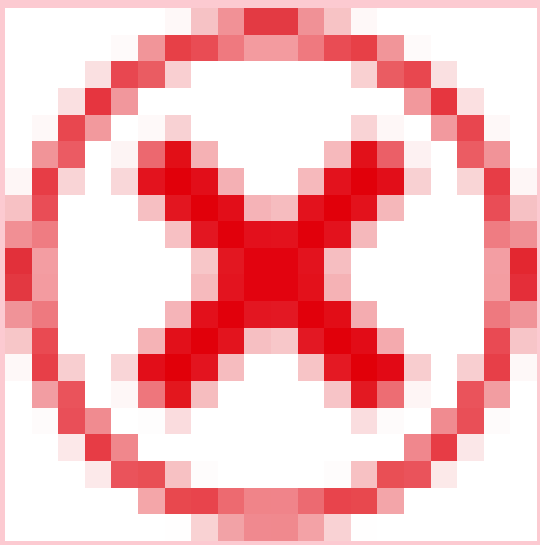
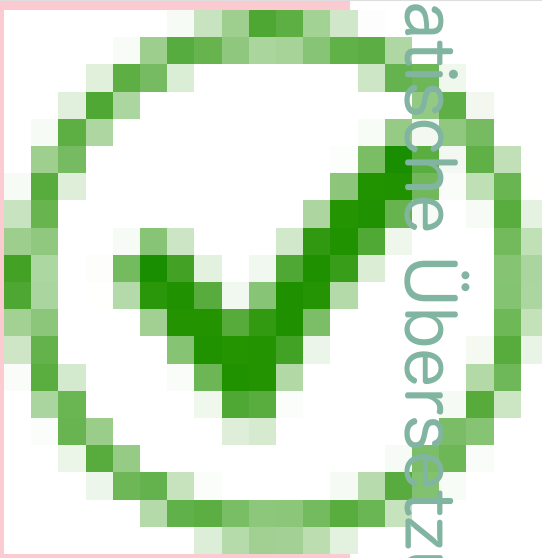
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Verfehltes Ziel		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

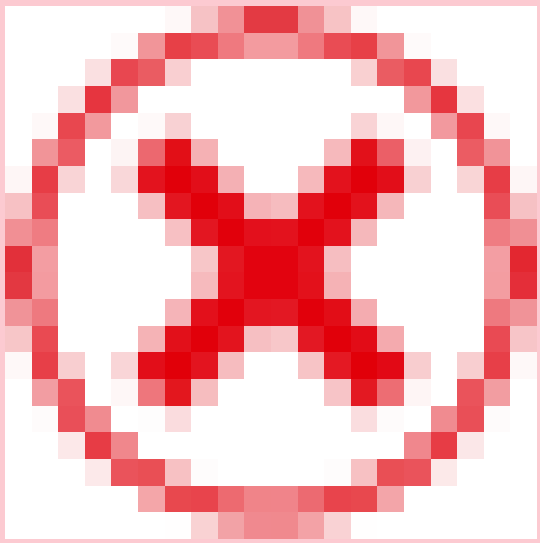
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Alle		
Bibliotheken		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

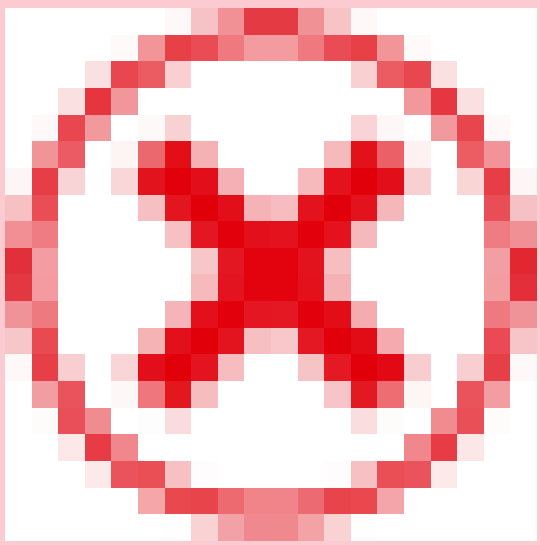
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
NVD		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

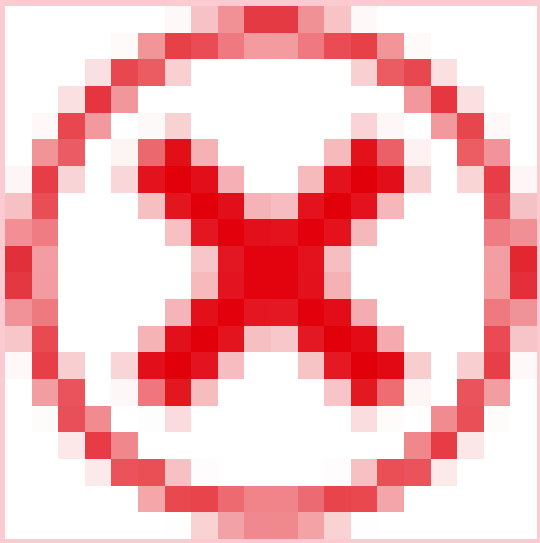
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Drittpartei		
Administration		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

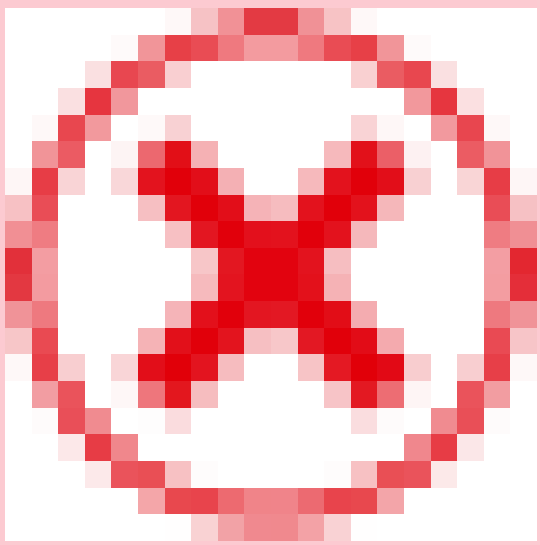
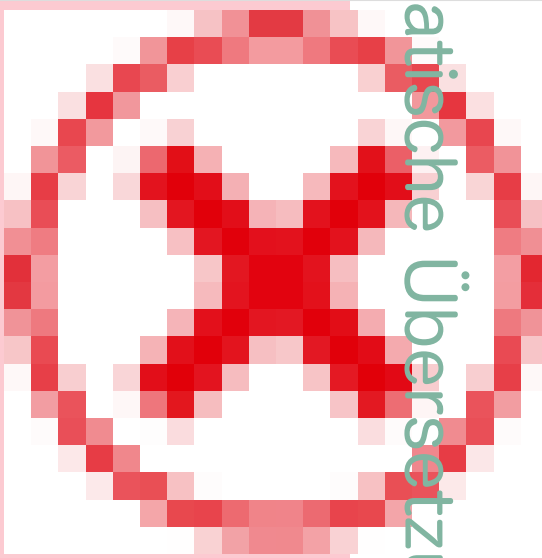
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Zuweisungsregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

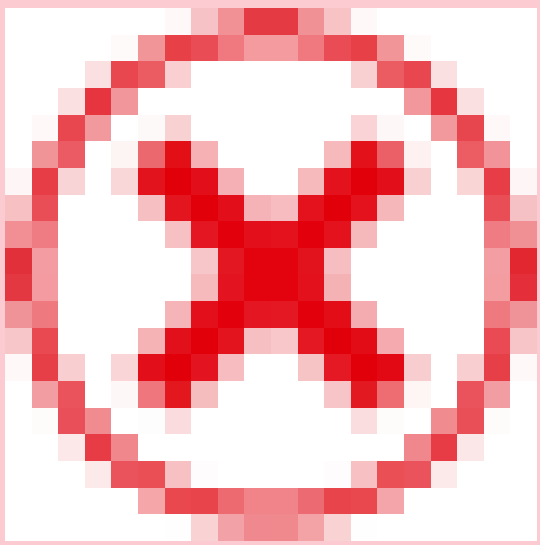
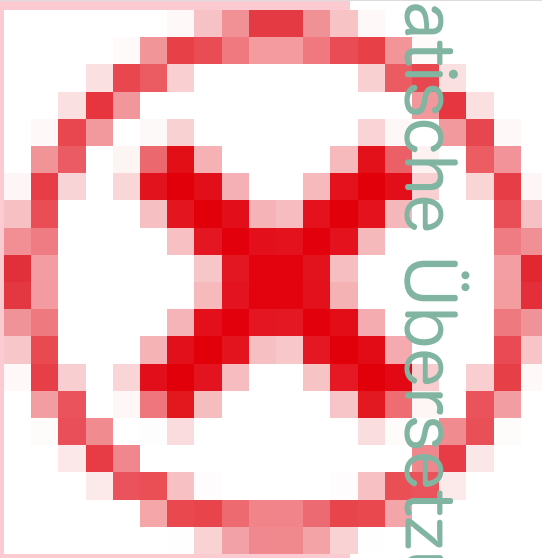
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Schwachstellen-Rechner		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

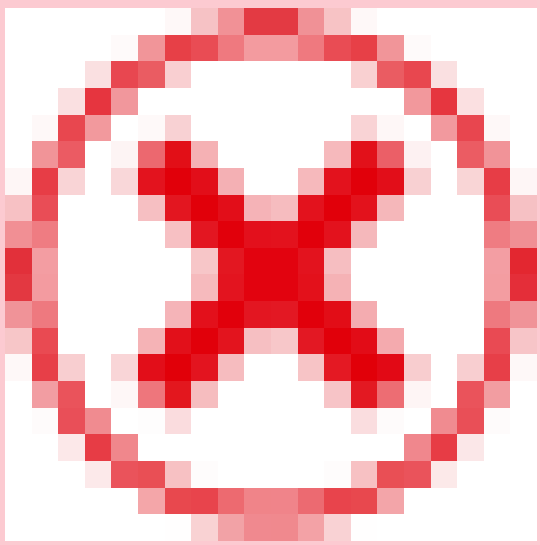
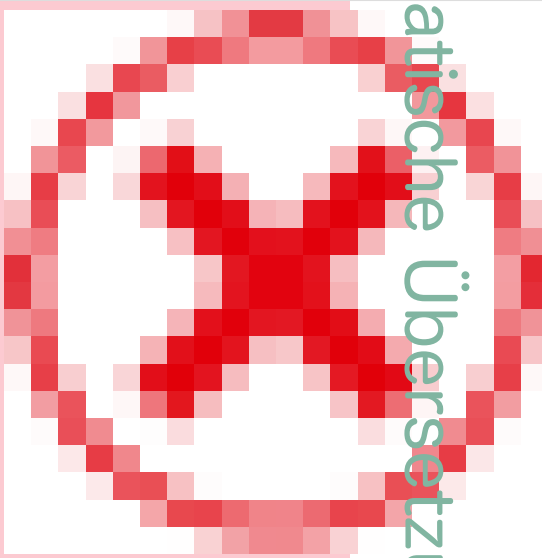
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Korrekturzielregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

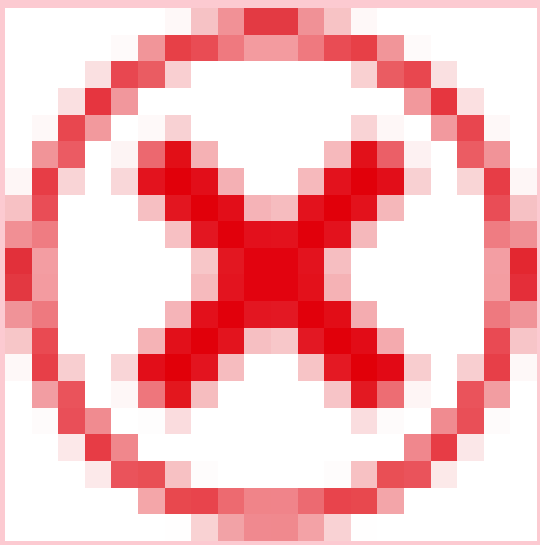
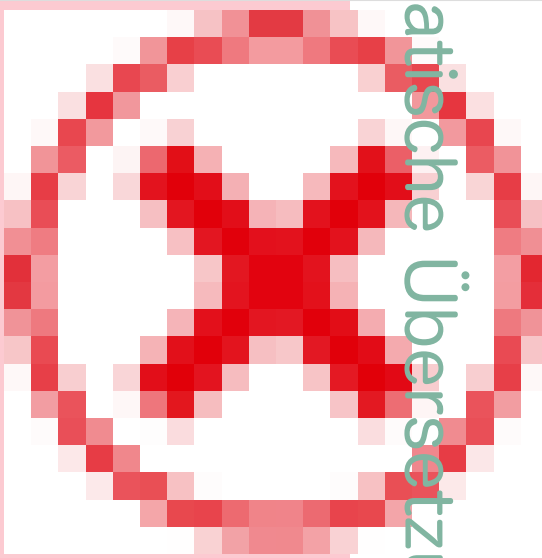
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
VI-Granularität konfigurieren		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

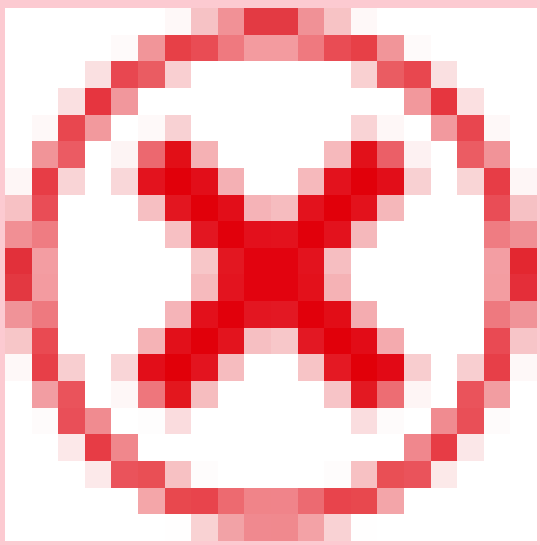
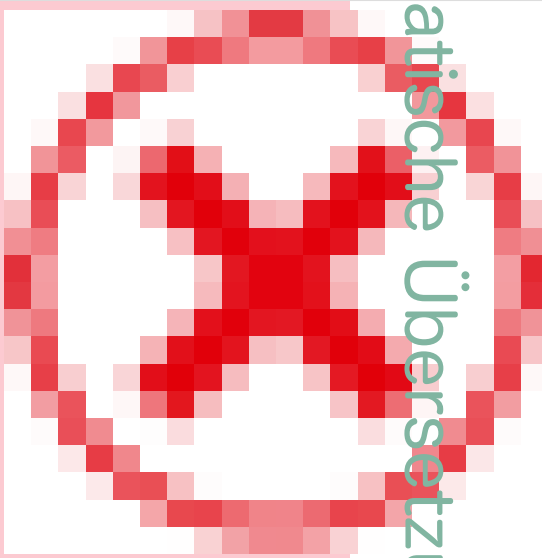
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Ausnahmeregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

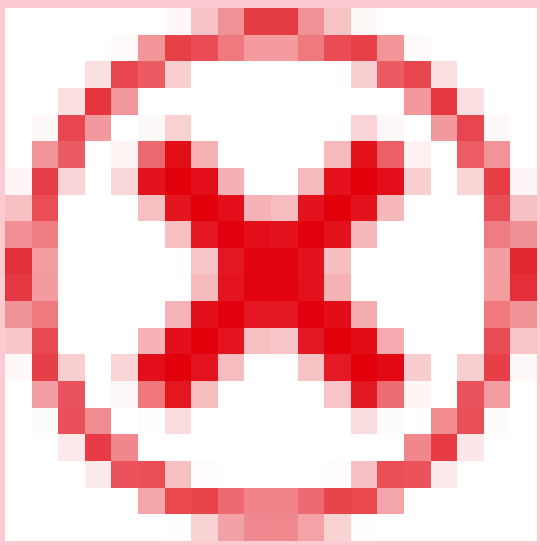
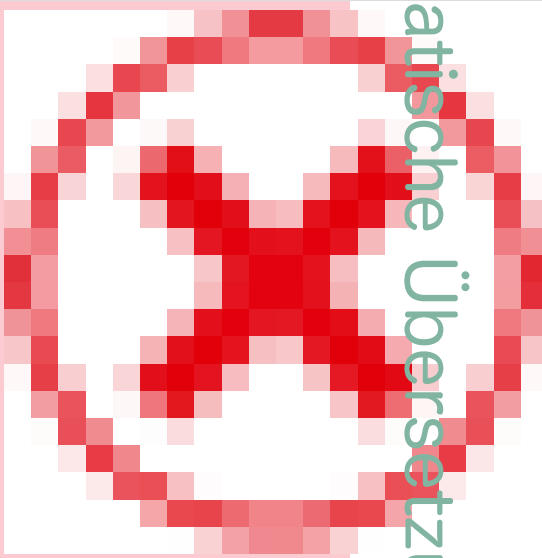
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Genehmigungsregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

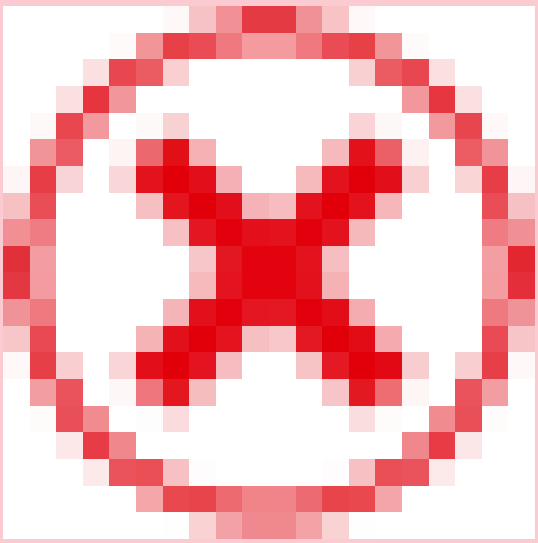
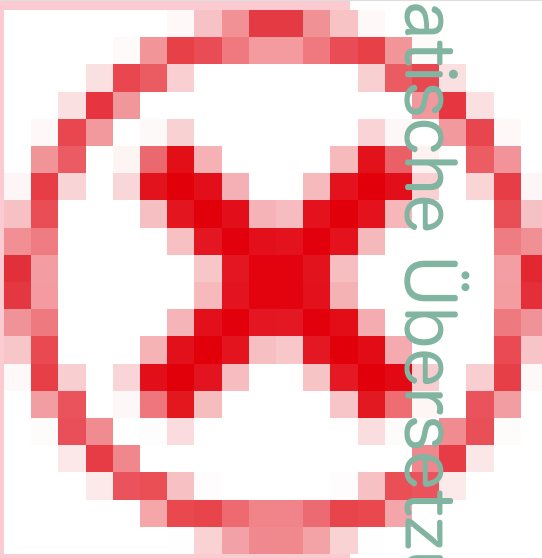
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Container-Sicherheitsintegrationen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

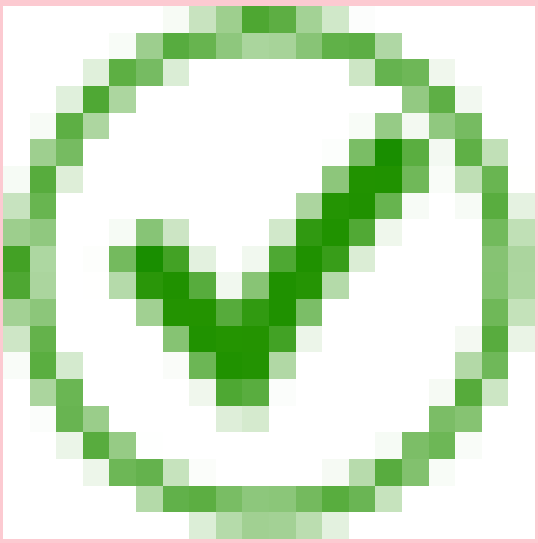
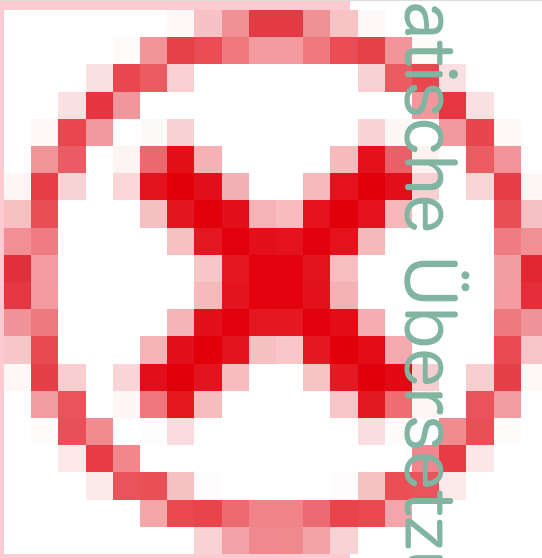
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Angreifbare Elemente automatisch schließen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Informationen für andere Rollen:

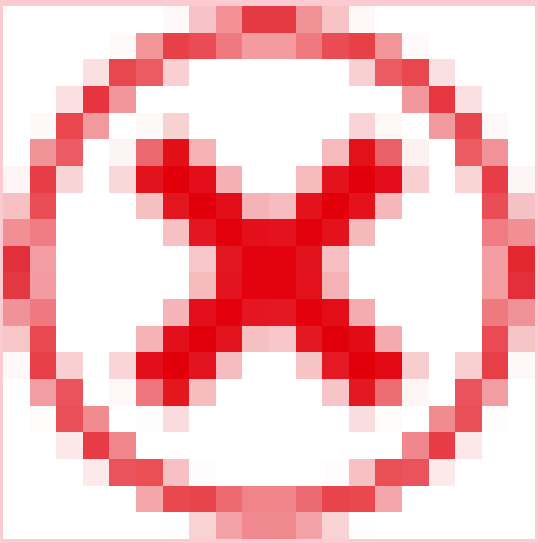
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity
Normalisierte Schweregradzuordnungen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

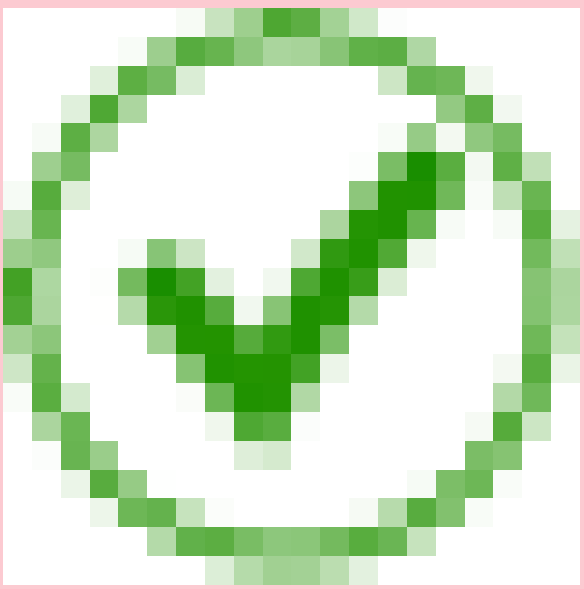
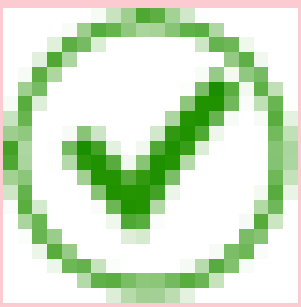
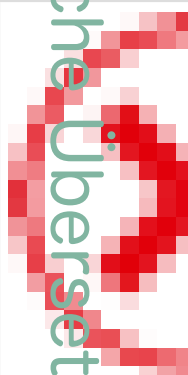
Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
(Haupt-App-Gruppe)			
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Meine Genehmigungen	✗	✗	✗
Angreifbare Container-Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Mir zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

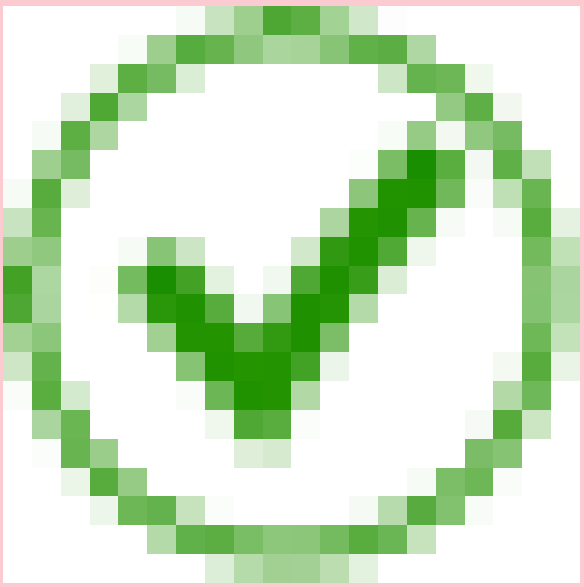
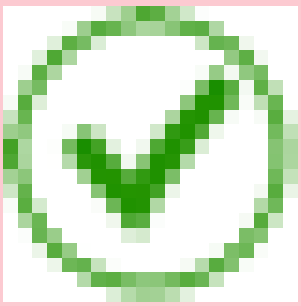
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Meinen Gruppen zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

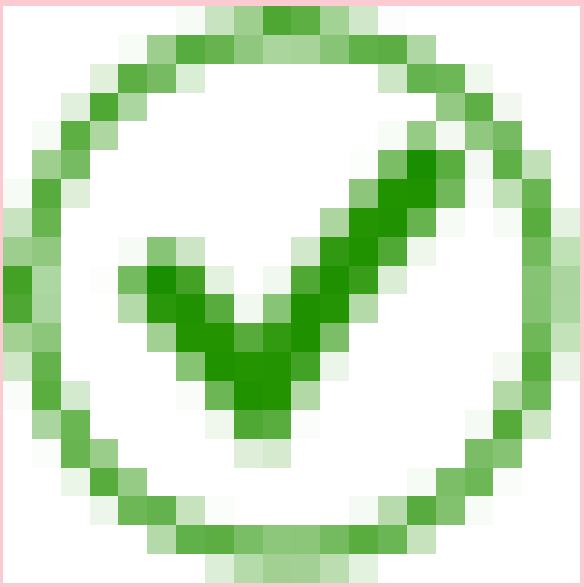
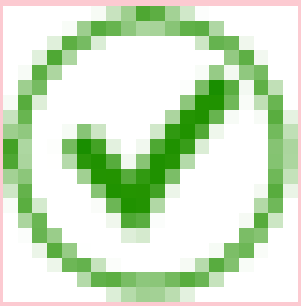
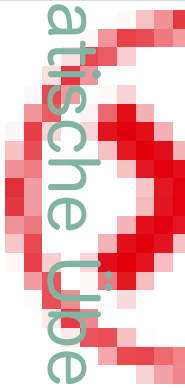
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Kritisches und hohes Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

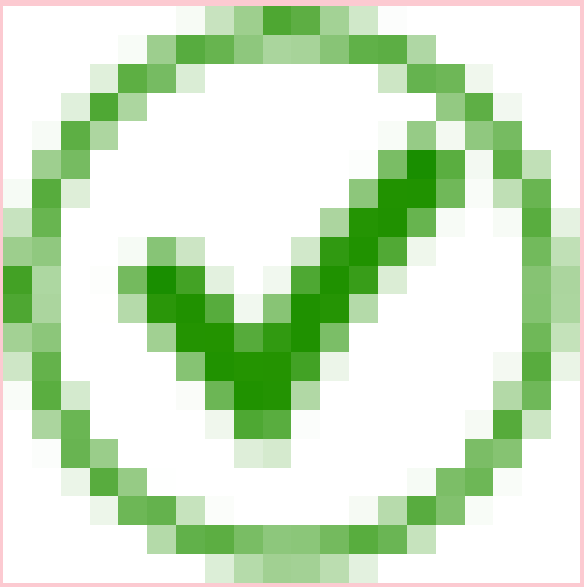
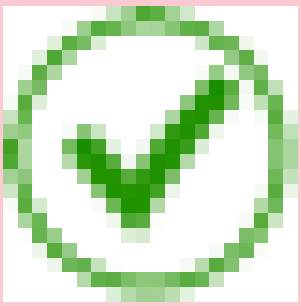
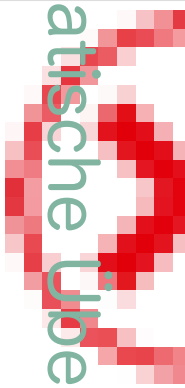
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Nutzbar			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

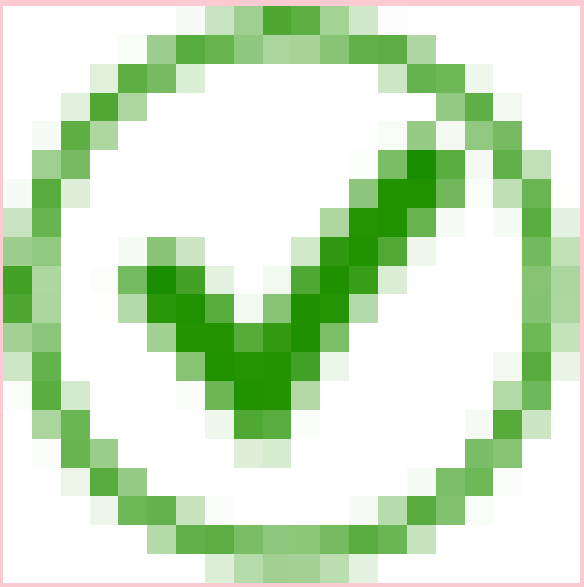
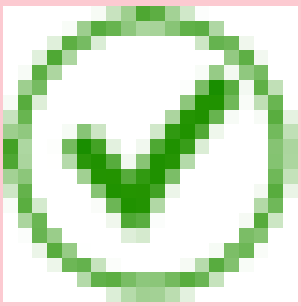
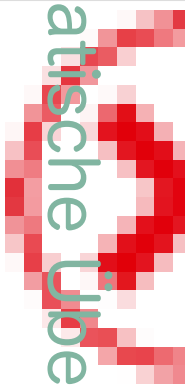
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Verfehltes Ziel	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

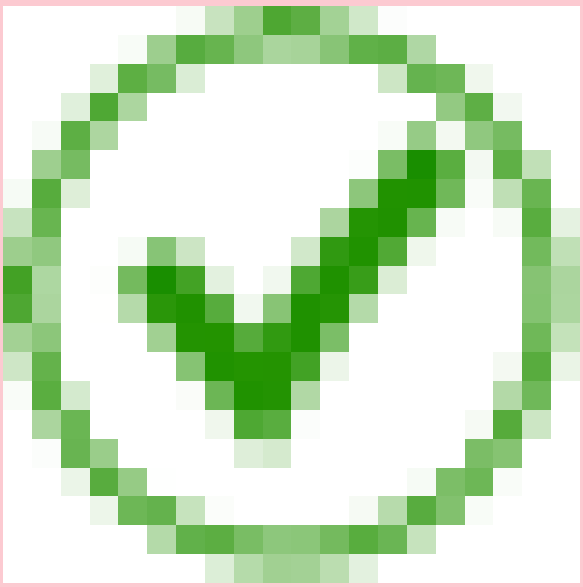
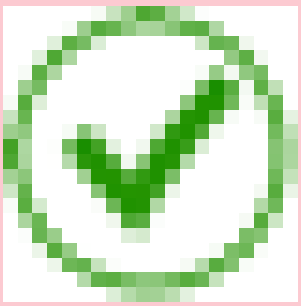
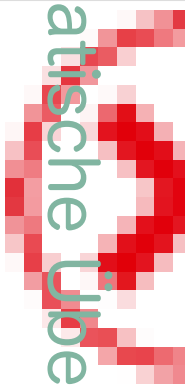
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Alle			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

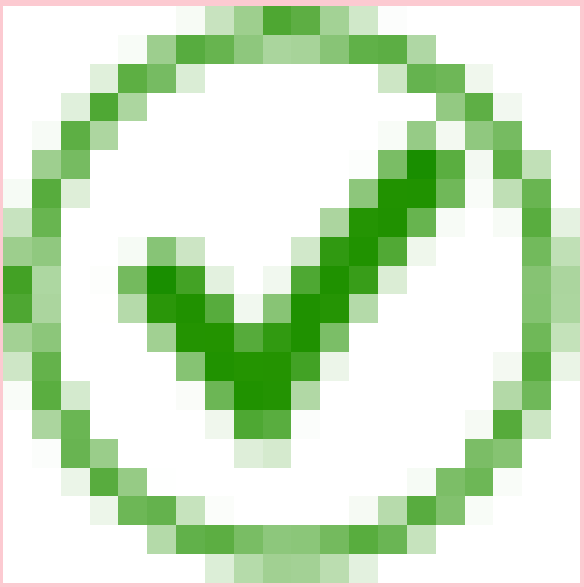
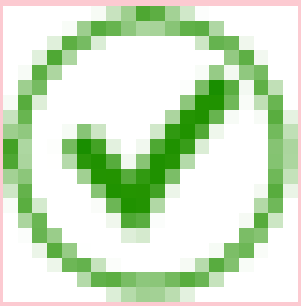
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
NVD			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

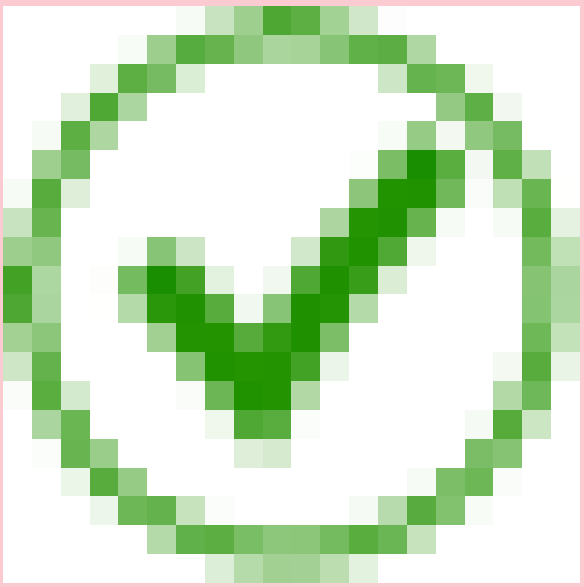
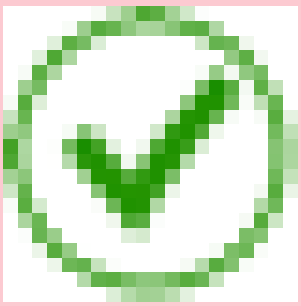
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Drittpartei			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Schwachstellen-Rechner	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

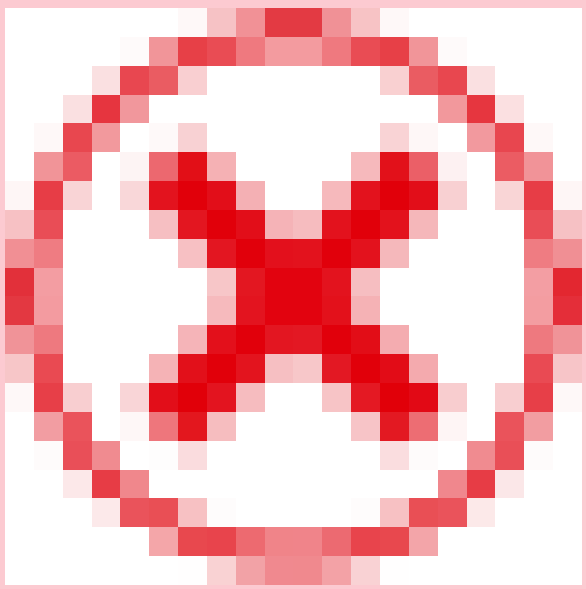
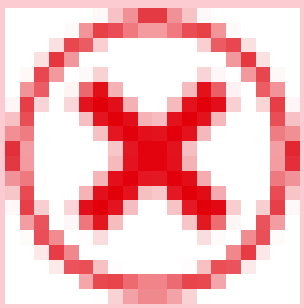
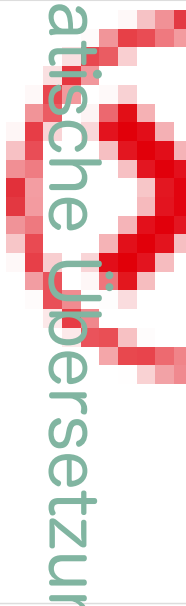
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Korrekturzielregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
VI-Granularität konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

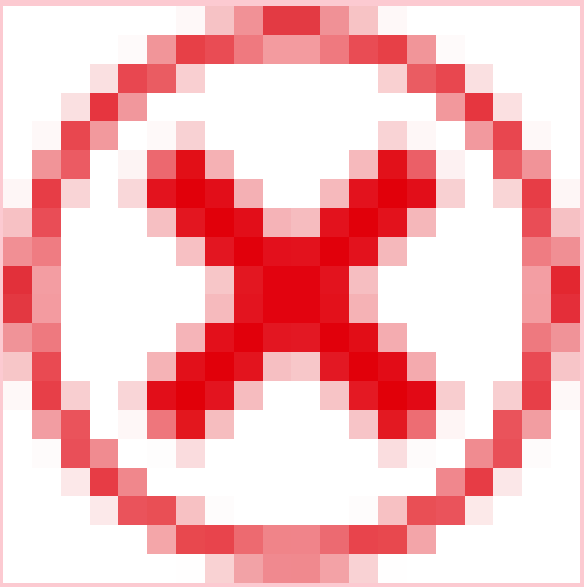
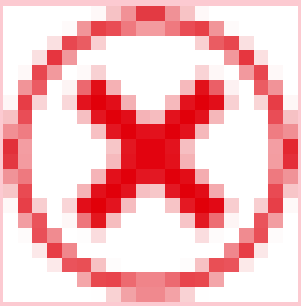
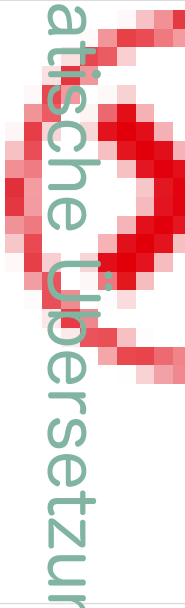
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Ausnahmeregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Genehmigungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Container-Sicherheitsintegrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

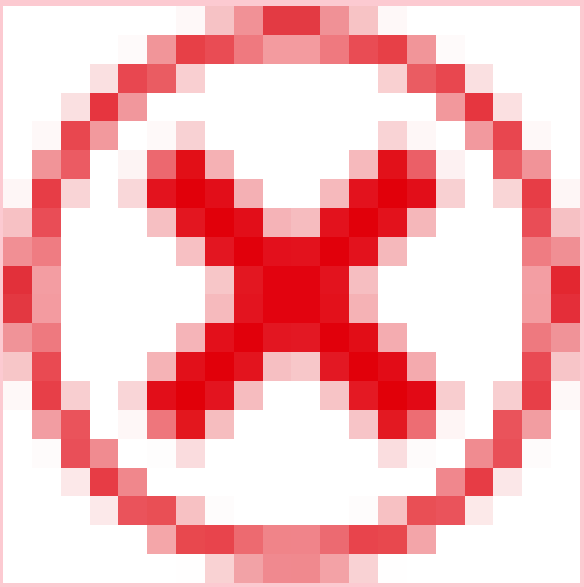
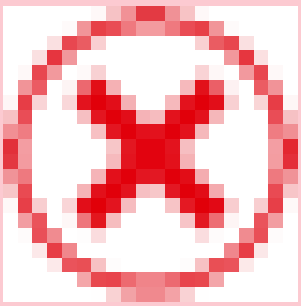
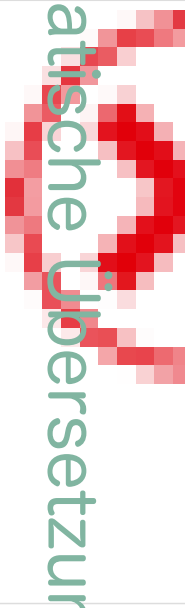
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Angreifbare Elemente automatisch schließen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Informationen für andere Rollen:

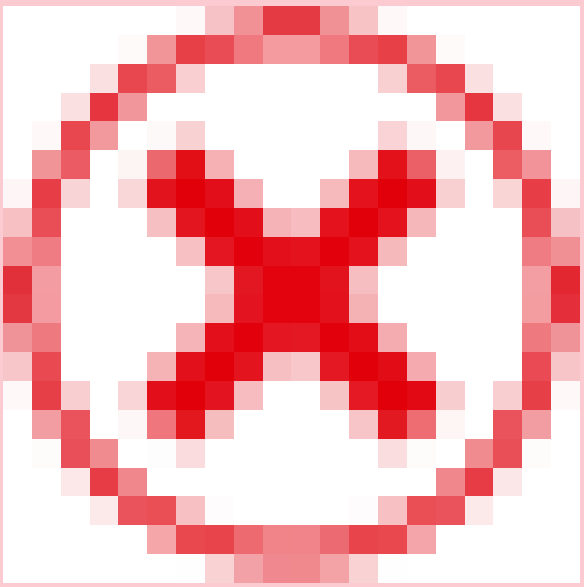
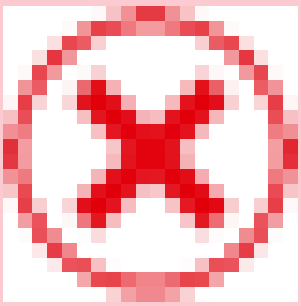
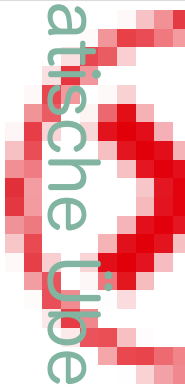
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

(Fortsetzung)

Modul	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_containe
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Modulzugriff für: sn_vul_container.read_auto_exception_rule

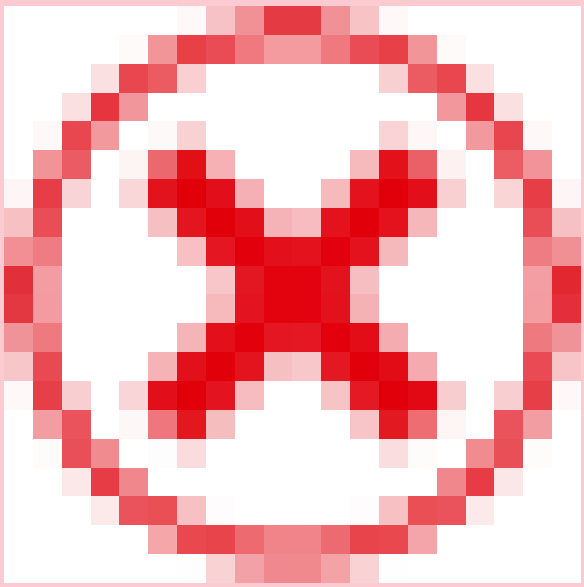
Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Modul	sn_vul_container.read_auto_exception_rule
(Haupt-App-Gruppe)	
Übersicht	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

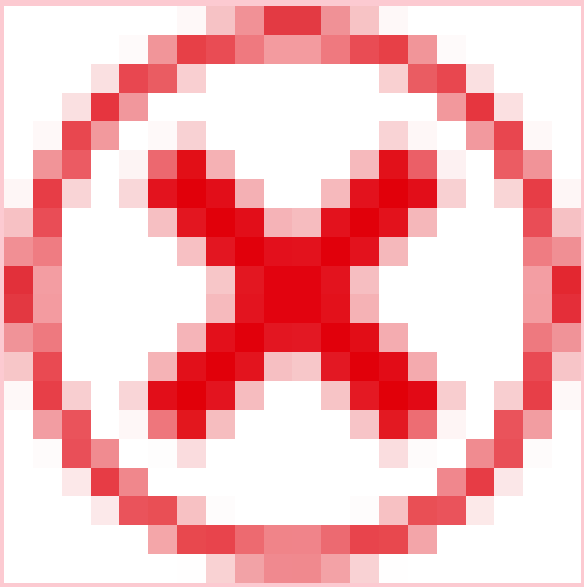
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Meine Genehmigungen	
Angreifbare Container-Elemente	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

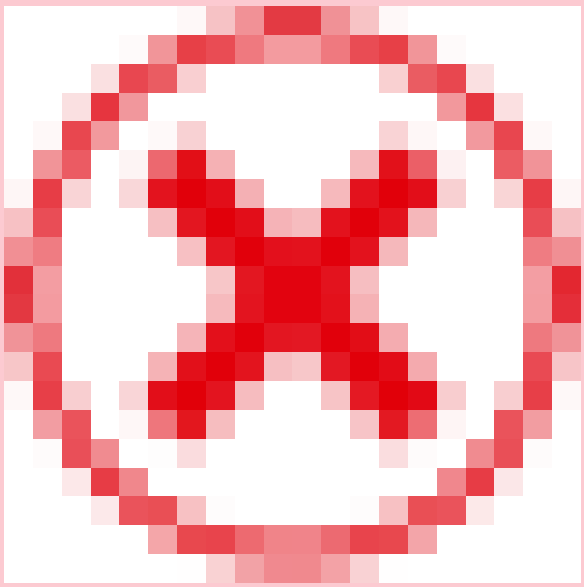
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Mir zugewiesen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

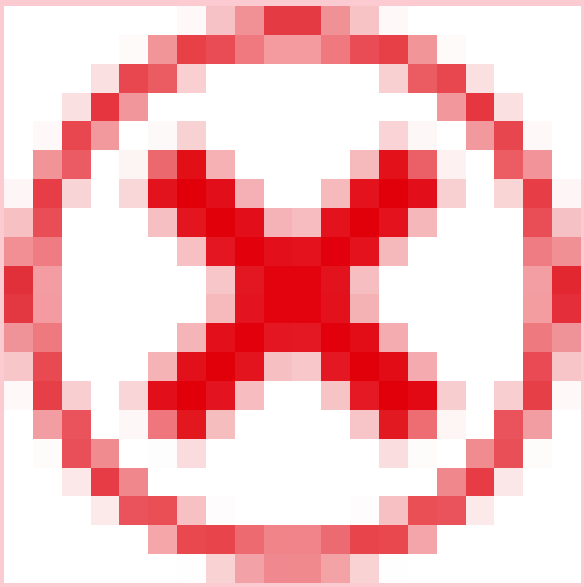
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Meinen Gruppen zugewiesen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

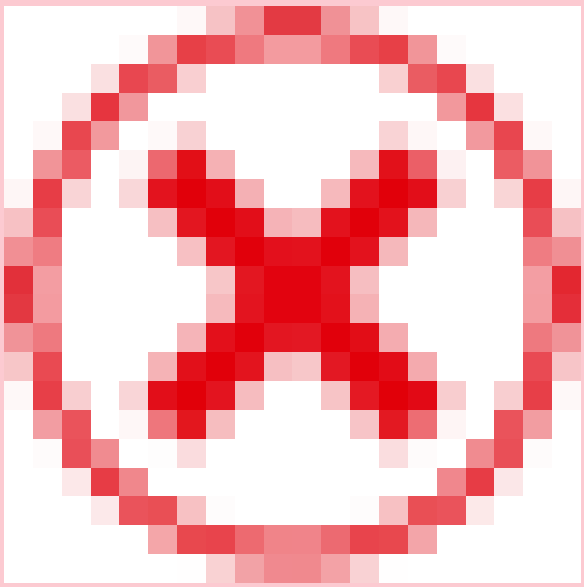
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Kritisches und hohes Risiko	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

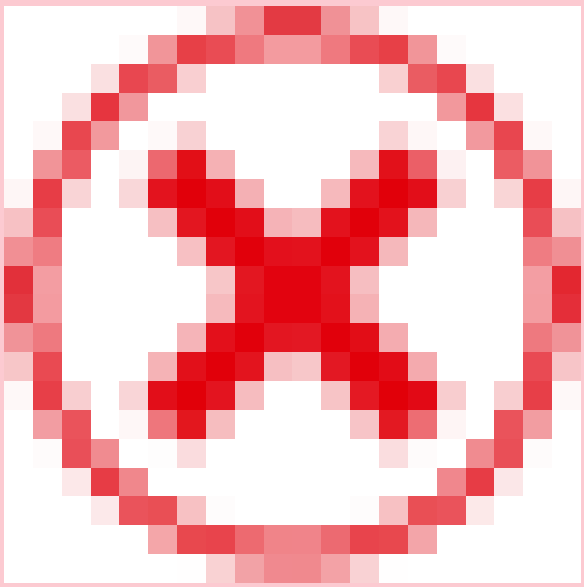
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Nutzbar	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

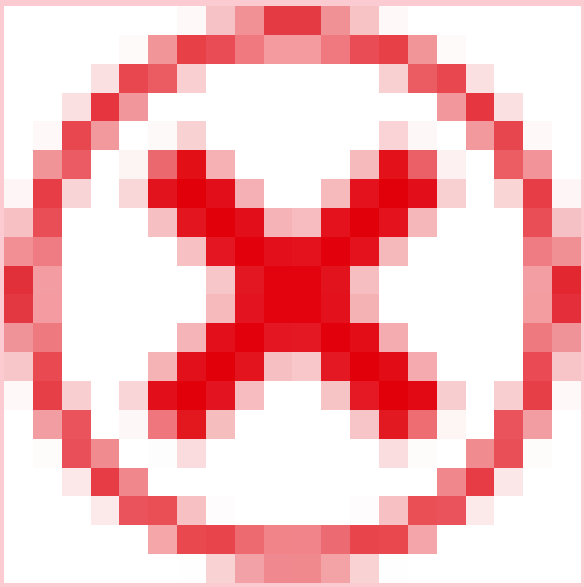
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Ziel rückt näher	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

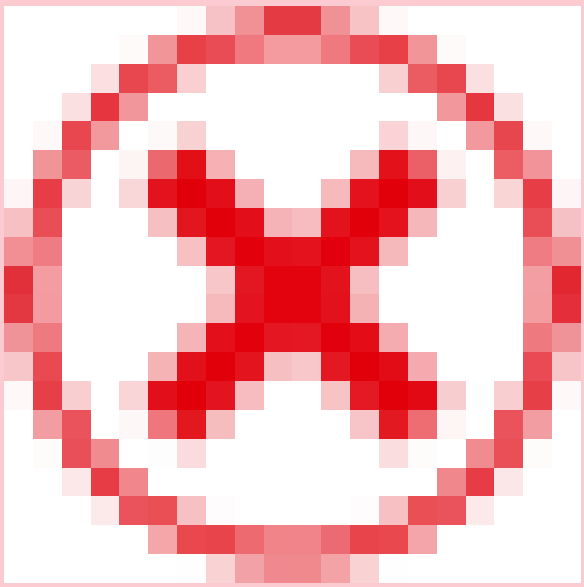
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Verfehltes Ziel	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

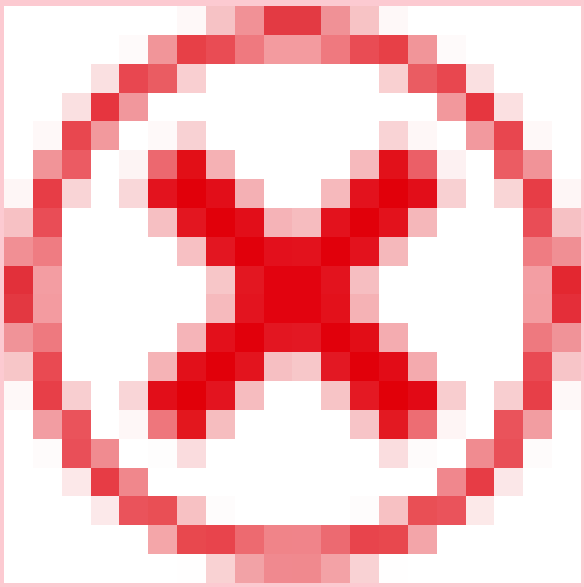
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Alle	
Bibliotheken	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

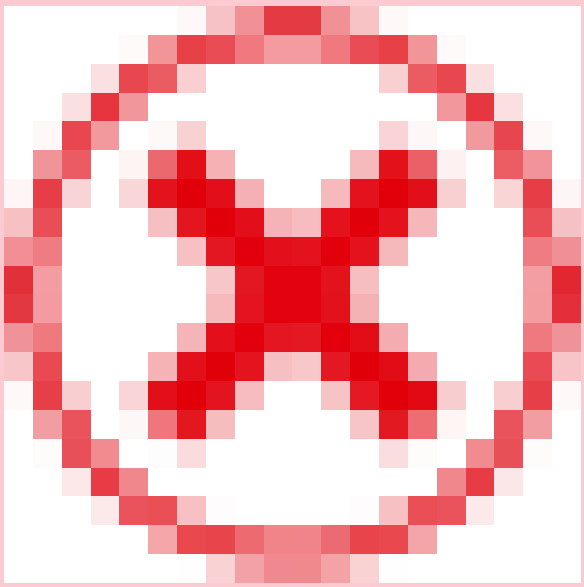
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
NVD	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

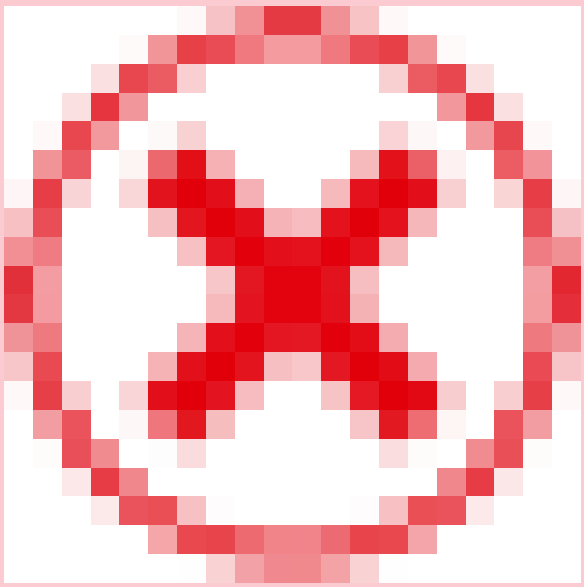
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Drittpartei	
Administration	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

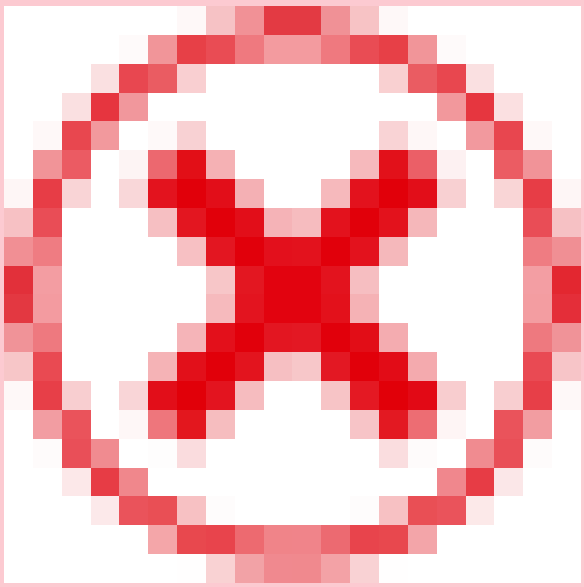
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Zuweisungsregeln	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

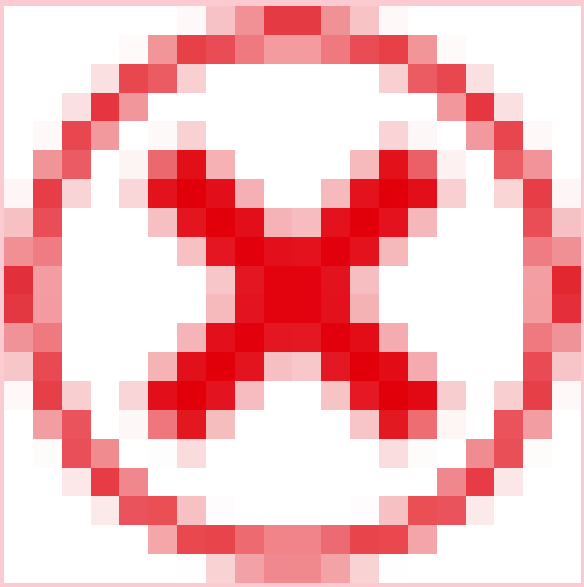
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Schwachstellen-Rechner	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

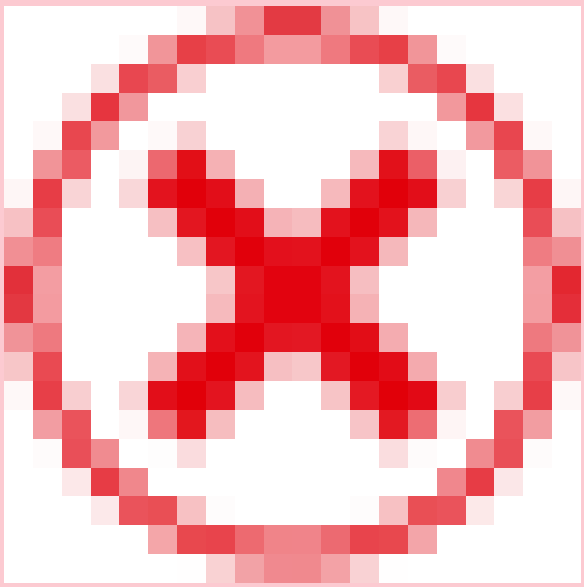
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Korrekturzielregeln	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

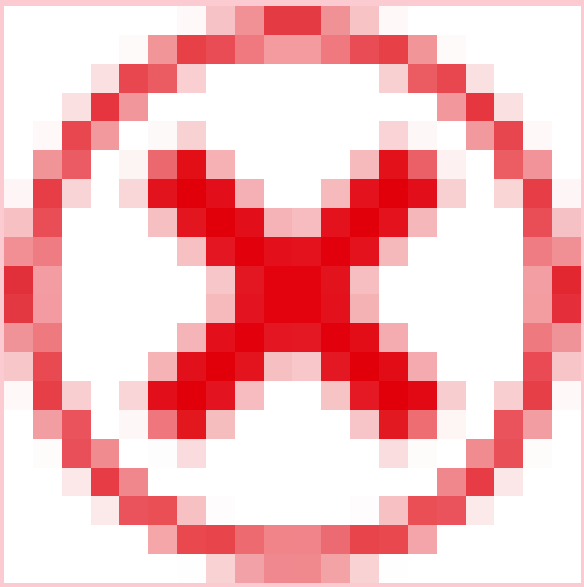
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
VI-Granularität konfigurieren	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

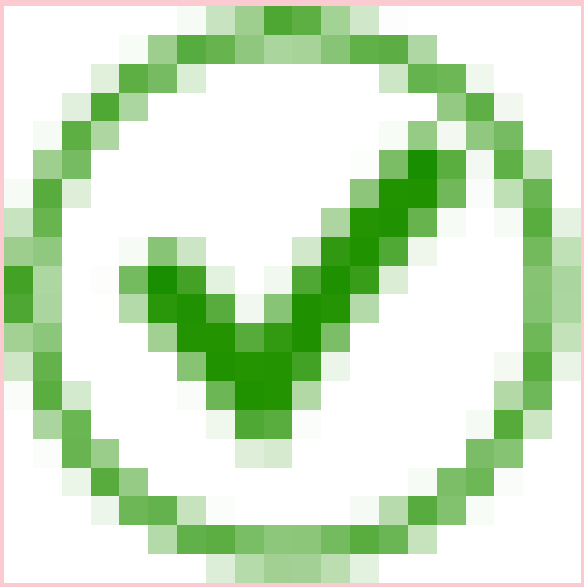
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Ausnahmeregeln	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

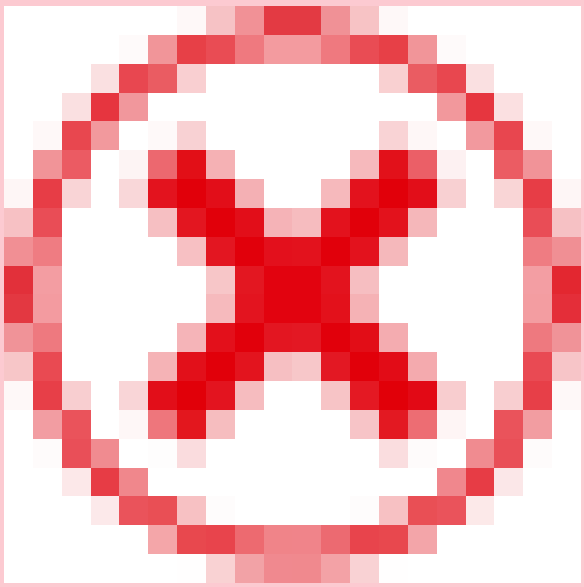
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Genehmigungsregeln	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

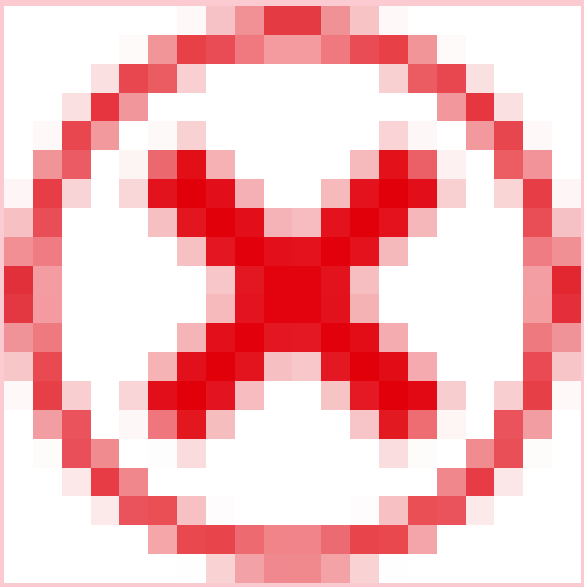
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Container-Sicherheitsintegrationen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

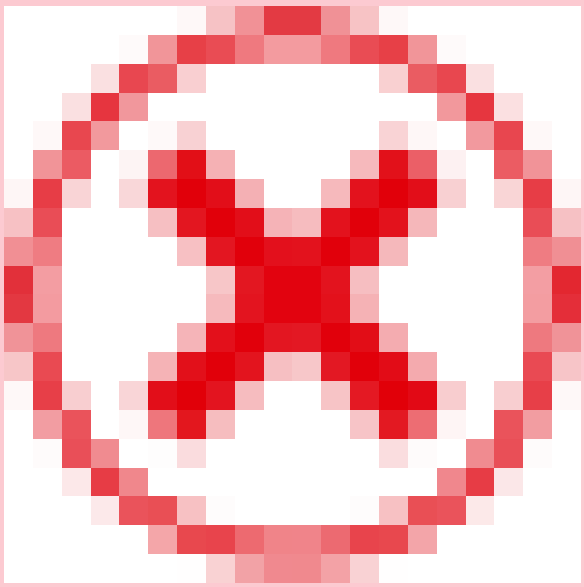
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Angreifbare Elemente automatisch schließen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_container.read_auto_exception_rule

Informationen für andere Rollen:

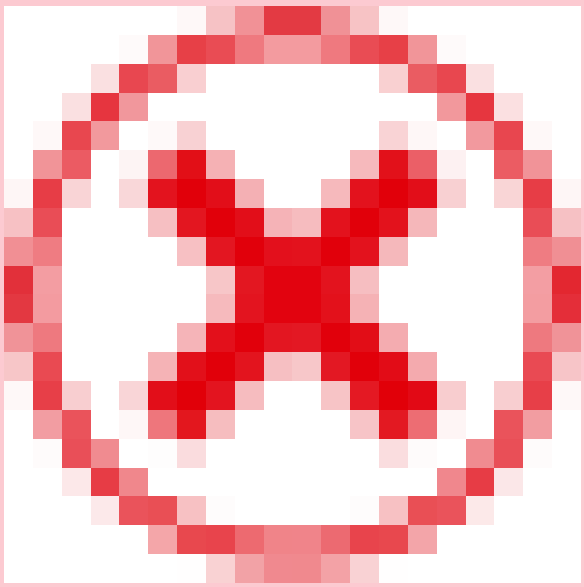
sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

(Fortsetzung)

Modul	sn_vul_container.read_auto_exception_rule
Normalisierte Schweregradzuordnungen	

[End]

[store-future: BEGIN review]

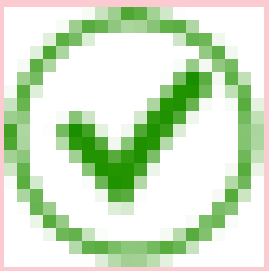
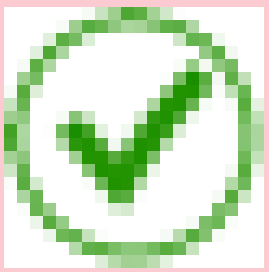
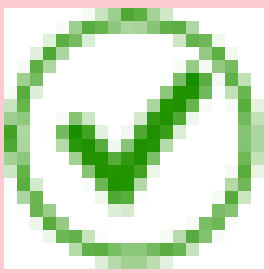
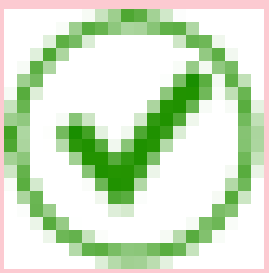
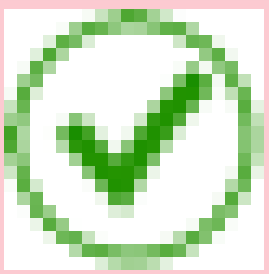
Modulzugriff nach Rolle für die DLP-Administration

Informationen zur DLP-Administration finden Sie in den Menüelementen, auf die mit einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_dlir.analyst
(Haupt-App-Gruppe)	

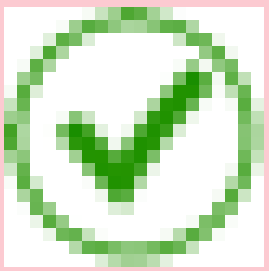
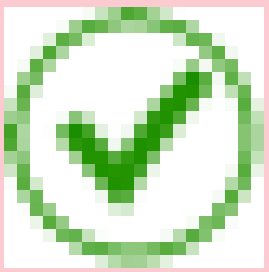
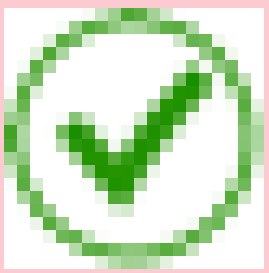
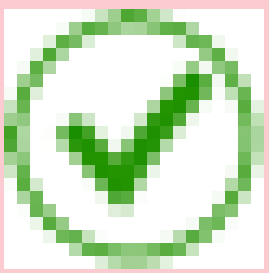
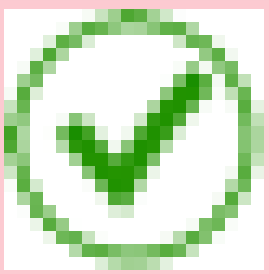
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_dlir.analyst
Standardkonfiguration	
Zuweisungsregeln	
Regeln für Fälligkeitsdatum der Antwort	
E-Mail-Vorlagen	
Bewertungen	
Optionen für die Reaktion auf Incidents	

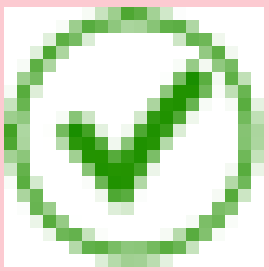
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_dlir.analyst
Konfiguration des Altersdiagramms	
Delegierten-Konfiguration	
Anwenderdefinierte Status	
Regeln zur Identifizierung von Wiederholungsvergehen	
Anwenderdefinierte Felder	
Erweiterte Einstellungen	
Incident-Zugriffsbeschränkungen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

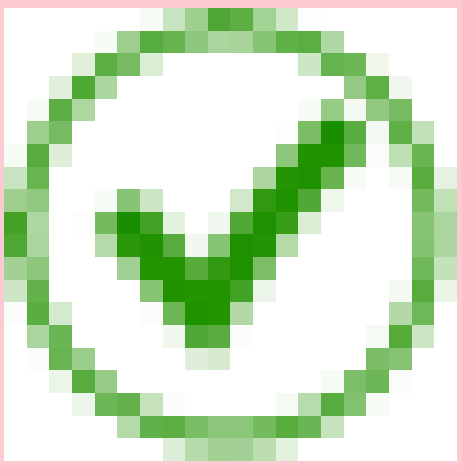
Modul	sn_dlir.analyst
Einschränkungen auf Datensatzebene	
Einschränkungen auf Feldebene	

[End]

[store-future: BEGIN review]

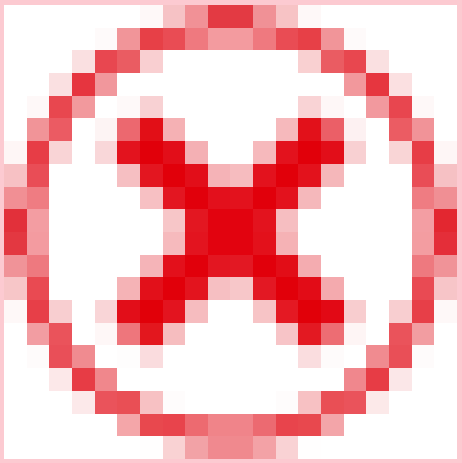
Modulzugriff nach Rolle für DLP-Incident-Management

Informationen zu DLP-Incident-Management finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Modul	sn_dlir.analyst
(Haupt-App-Gruppe)	
DLP-Vorgangsportal	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_dlir.analyst
DLP-Endanwenderportal	
DLP-Dashboard	

[End]

[store-future: BEGIN review]

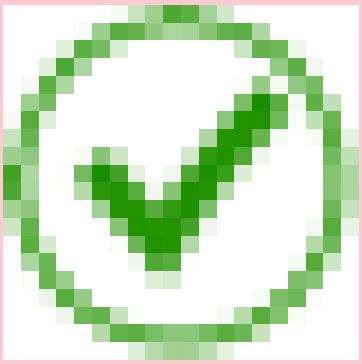
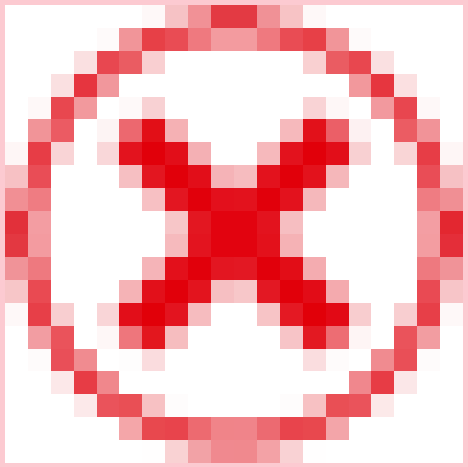
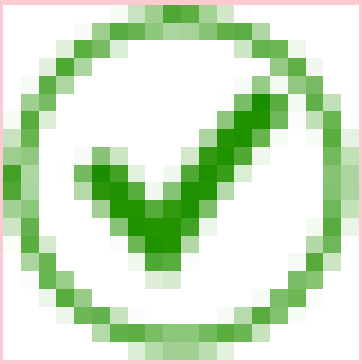
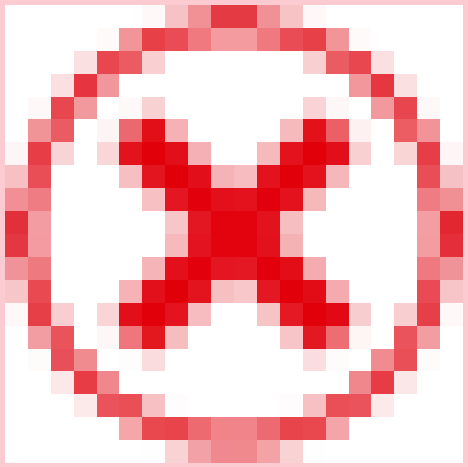
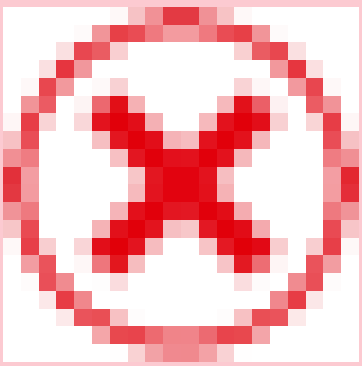
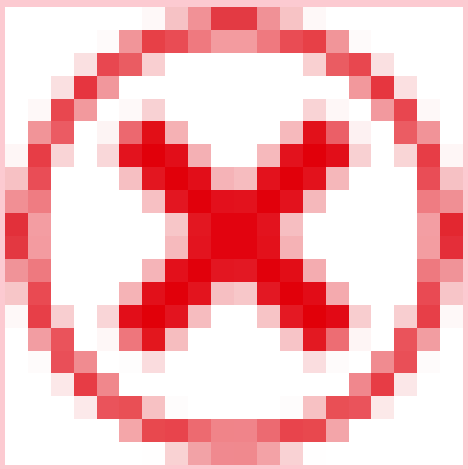
Modulzugriff nach Rolle für Datenzertifizierung

Informationen zur Datenzertifizierung finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	certification_admin	certification_filter_admin
(Haupt-App-Gruppe)		

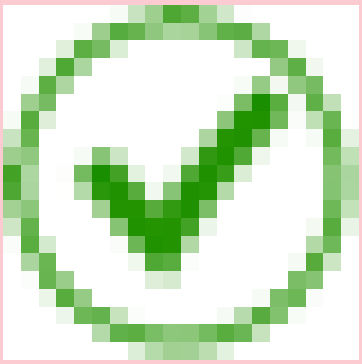
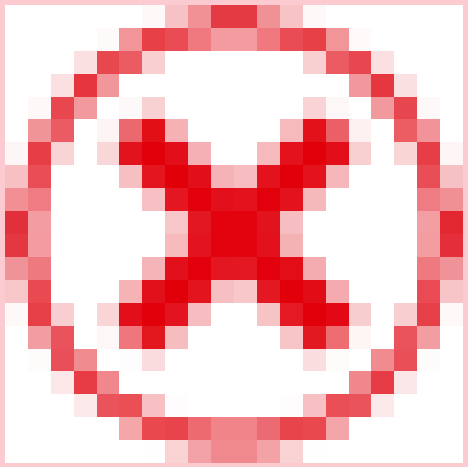
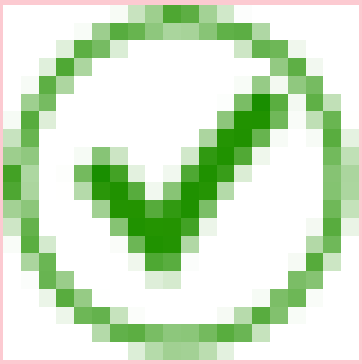
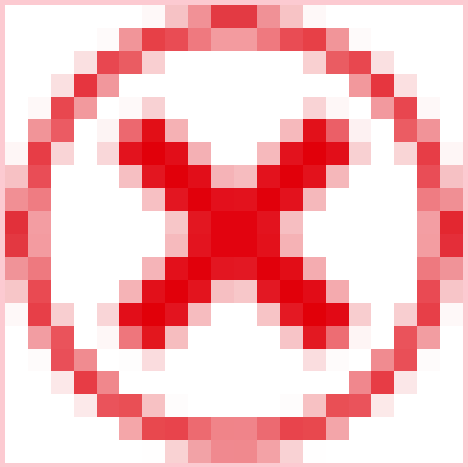
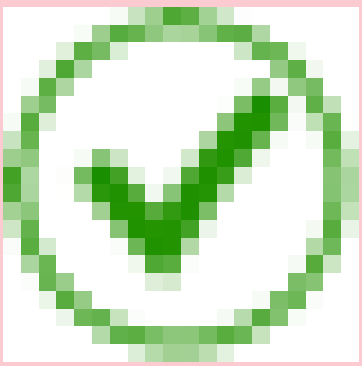
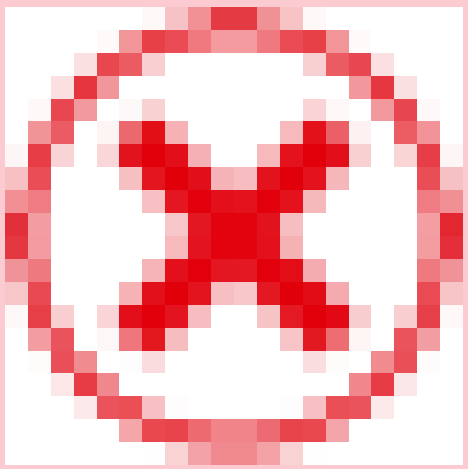
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Übersicht		
Erste Schritte		
Aufgaben		
Meine Aufgaben		

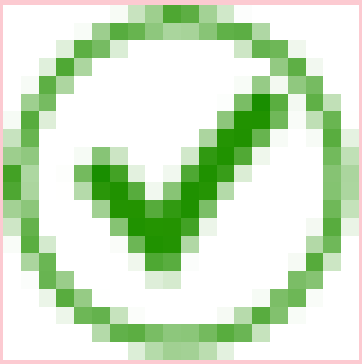
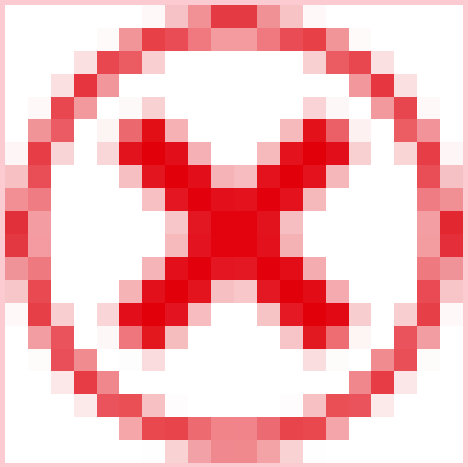
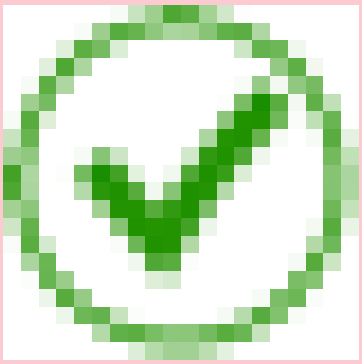
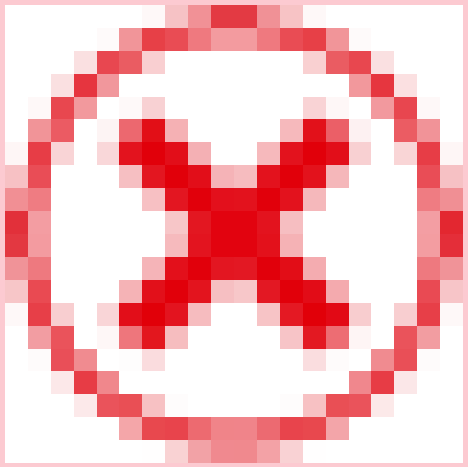
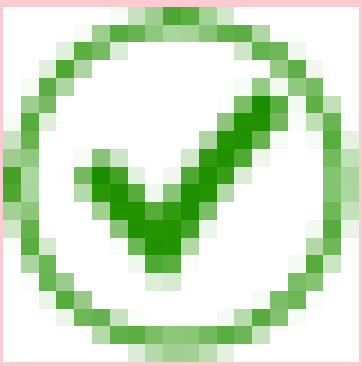
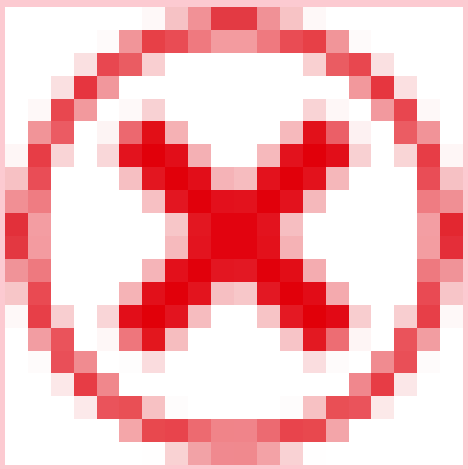
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Öffnen		
Alle Aufgaben		
Zertifizierungen		
Zertifiziert		

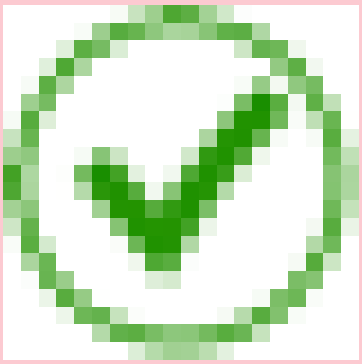
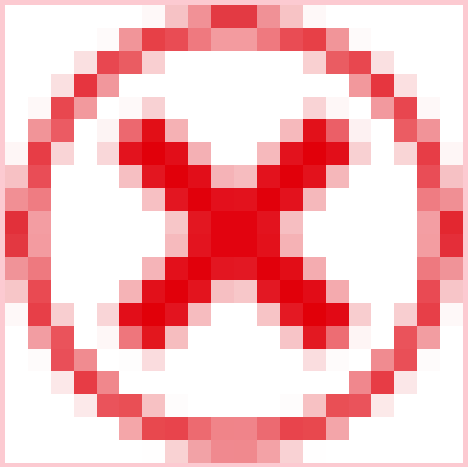
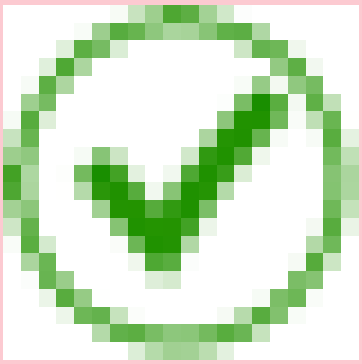
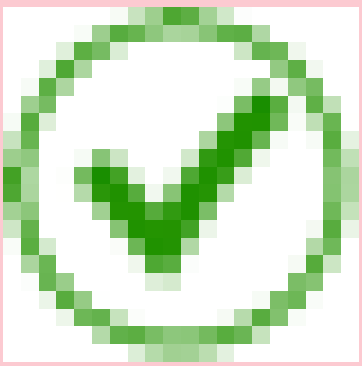
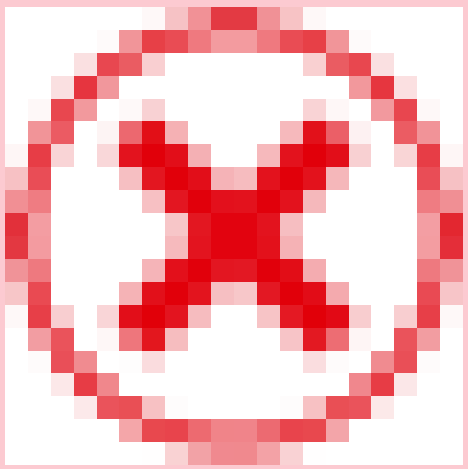
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Ausstehend		
Alle		
Zeitpläne		
Neu erstellen:		

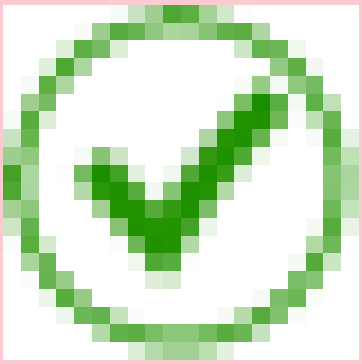
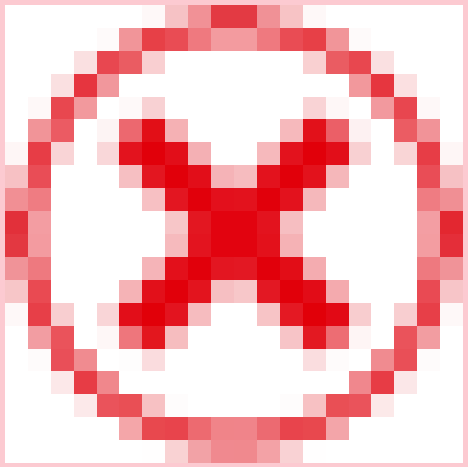
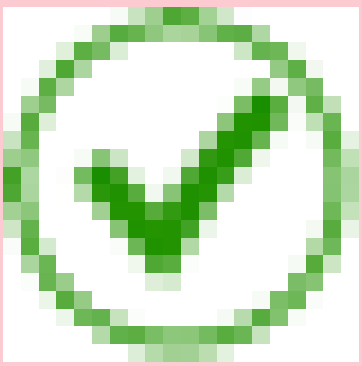
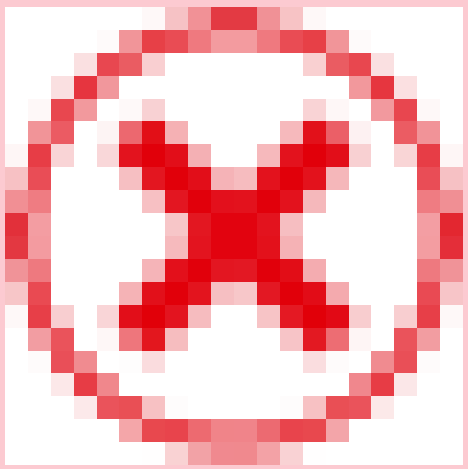
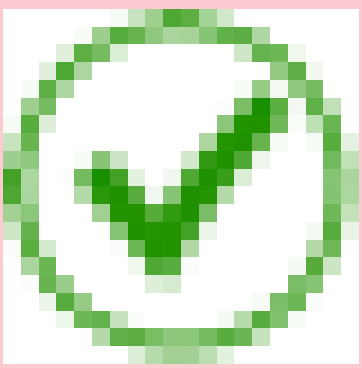
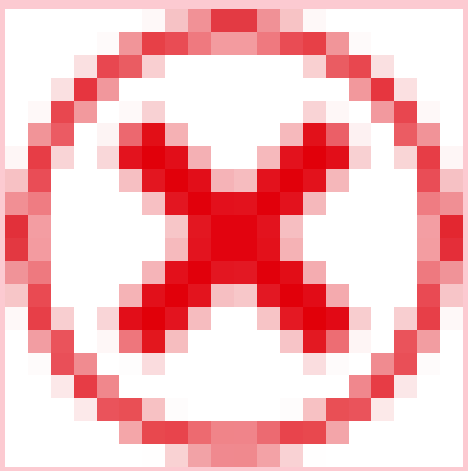
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Plandefinitionen		
Zertifizierungsfilter		
Instanzen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Audit-Ergebnisse		
Audits		
Auditdefinitionen		
Auditinstanzen		

[End]

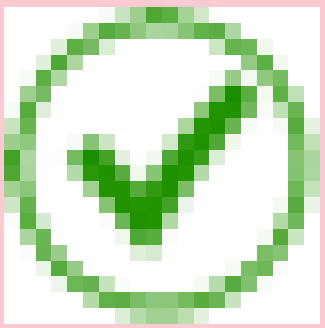
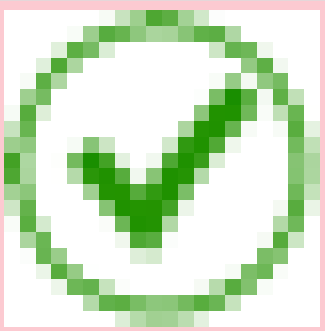
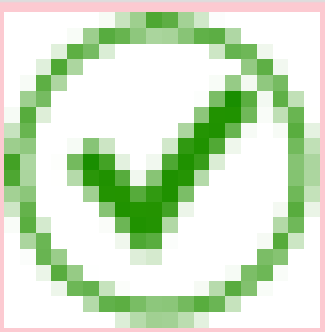
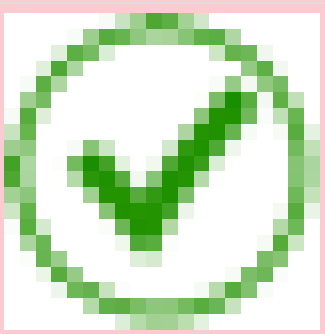
[store-future: BEGIN review]

Modulzugriff nach Rolle für IBM QRadar-Integration

Informationen zu IBM QRadar Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.analyst
(Haupt-App-Gruppe)	
IBM QRadar-Profil	
IBM QRadar Offense-Import	
IBM QRadar-Angriff auf Aufgabe	
IBM QRadar-Feldübersetzung	
IBM QRadar-Integrationseinstellungen	

Automatische Übersetzung

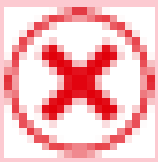
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für MISP-Integration

Informationen zur MISP-Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_si.admin	sn_si.analyst	sn_ti.admin	sn_ti.read	sn_ti.write
(Haupt-App-Gruppe)					
Integrationseinstellungen					
Sichtungssuche: Konfiguration					
Profile für die automatische Erstellung von Ereignissen					
Warteschlange für automatische Ereigniserstellung					
MISP-Ereignis-Daten					
Zugeordnete MISP-Ereignisse					
MISP-Anwenderinformationen					

[End]

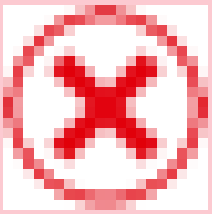
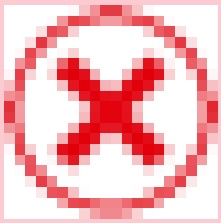
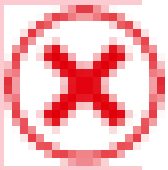
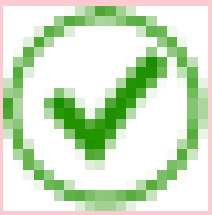
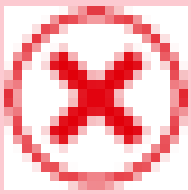
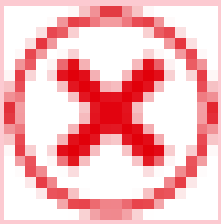
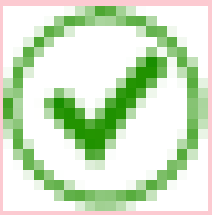
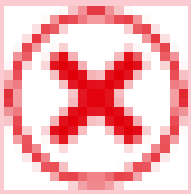
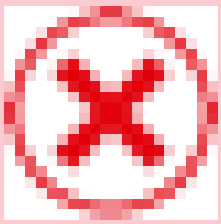
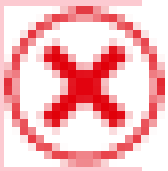
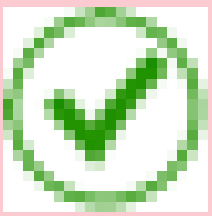
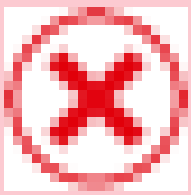
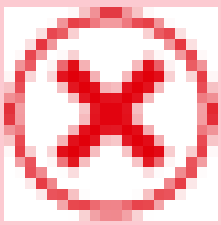
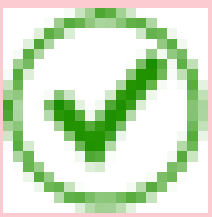
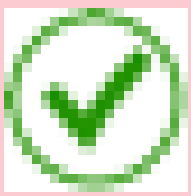
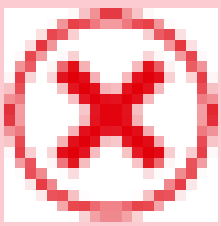
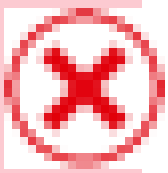
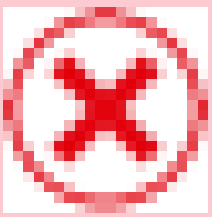
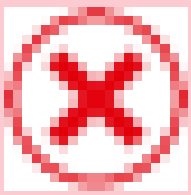
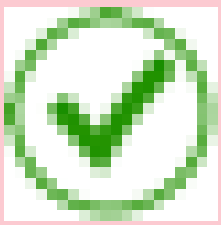
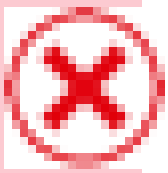
[store-future: BEGIN review]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

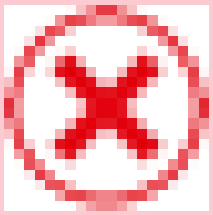
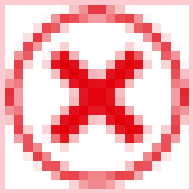
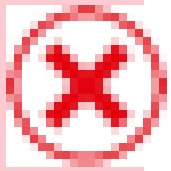
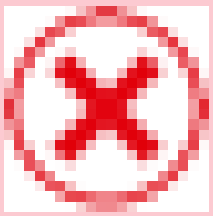
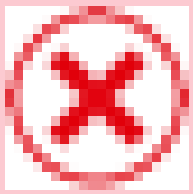
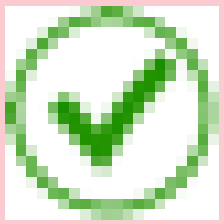
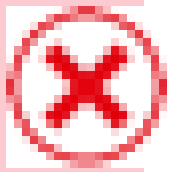
Modulzugriff nach Rolle für Microsoft Azure Defender for IoT

Sehen Sie sich für Microsoft Azure Defender for IoT die Menüelemente an, auf die eine bestimmte Rolle zugreifen kann.

Modul	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
(Haupt-App-Gruppe)				
Setup				
Datenquellen				
IntegrationHub ETL				
Zeitpläne importieren				
Eigenschaften				
Verbindungen und Anmeldeinformationen				
Aliasse für Verbindungsanmeldeinformationen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

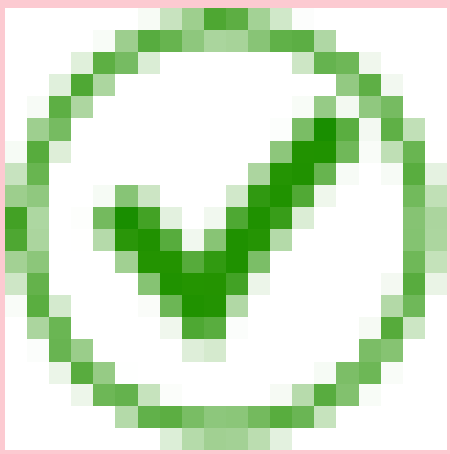
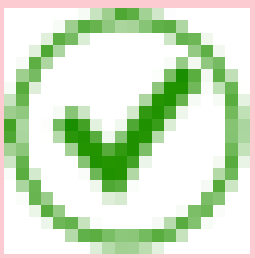
Modul	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
Anmeldeinformationen				
Verbindungen				

[End]

[store-future: BEGIN review]

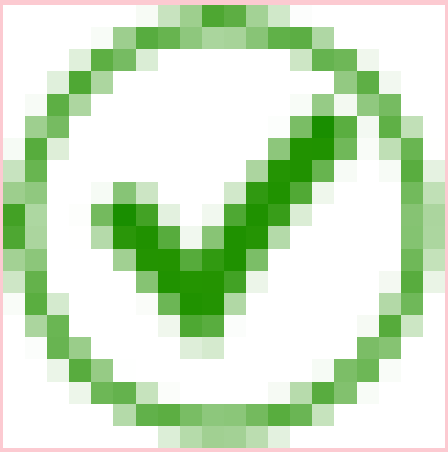
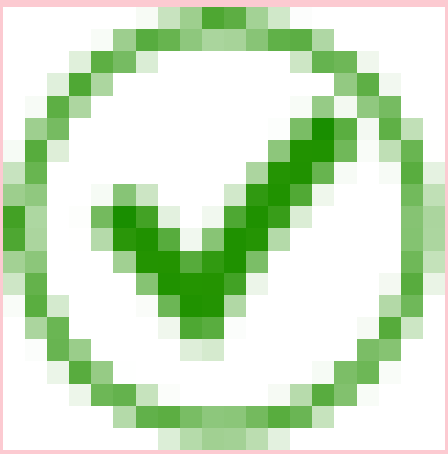
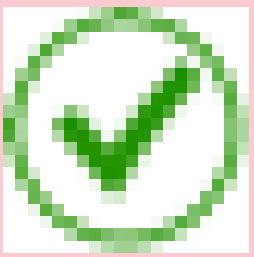
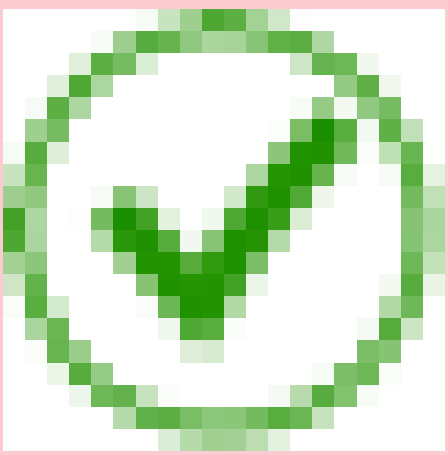
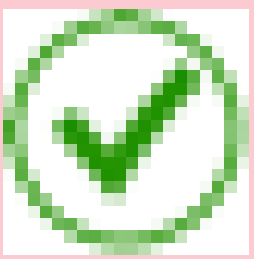
Modulzugriff nach Rolle für Qualys-Schwachstellenintegration

Informationen zu Qualys Vulnerability Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_vul.configure_qualys_integration	sn_vul_qualys.lesen
(Haupt-App-Gruppe)		
Übersicht		

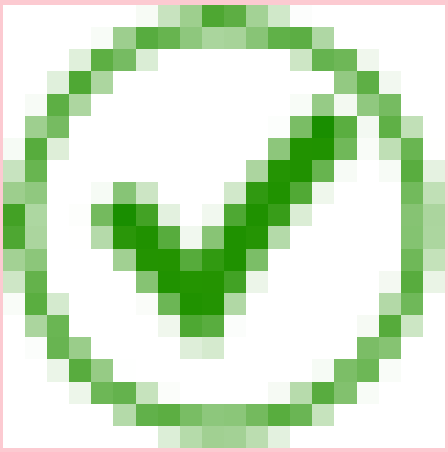
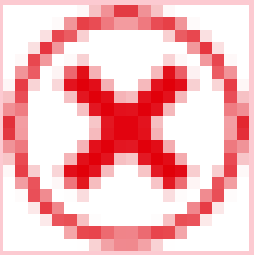
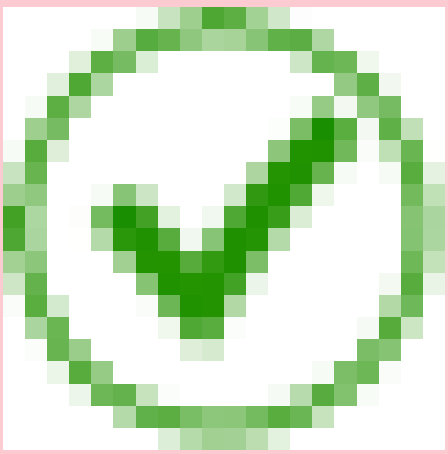
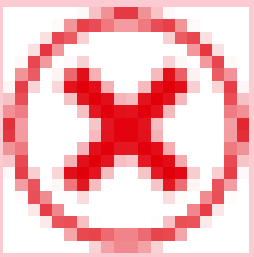
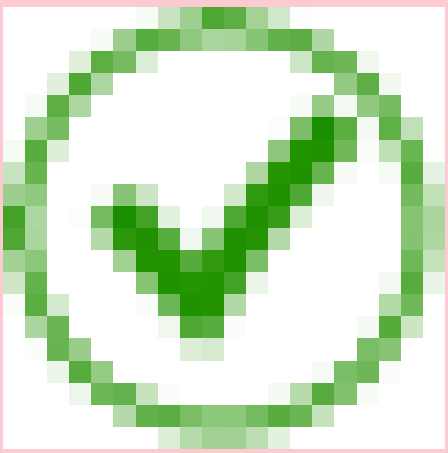
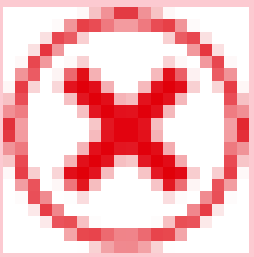
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul.configure_qualys_integration	sn_vul_qualys.lesen
Status der Integrationsausführung		
Scannergeräte		
Suchlisten		
Administration		

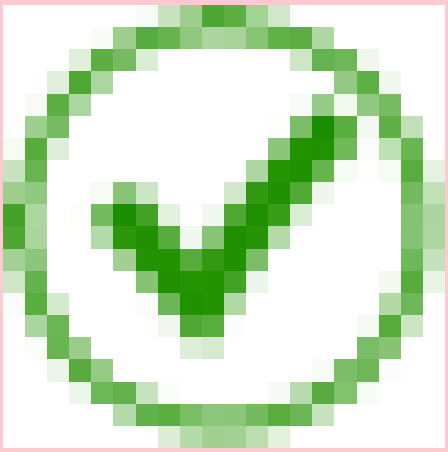
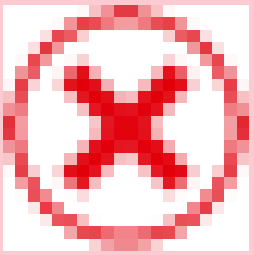
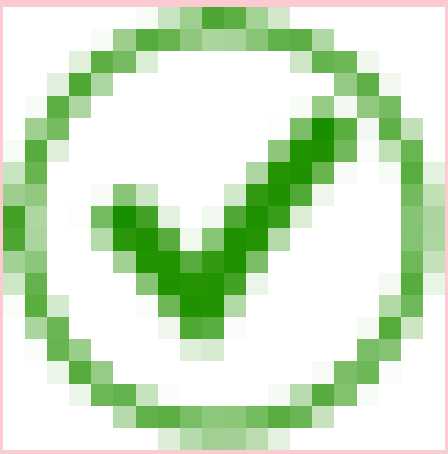
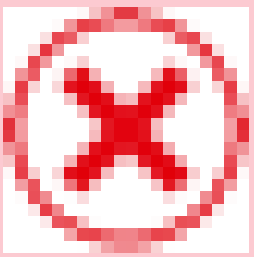
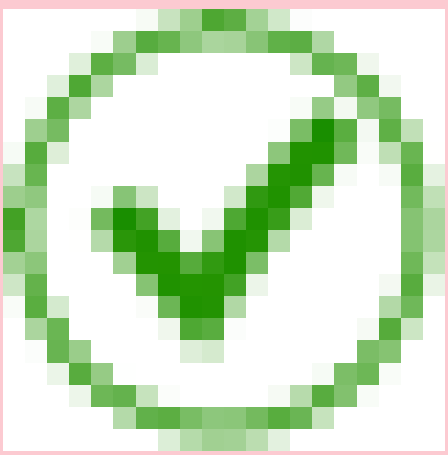
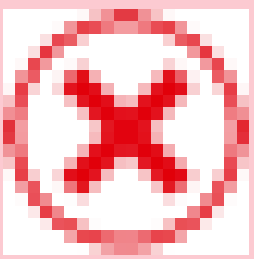
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul.configure_qualys_integration	sn_vul_qualys.lesen
Integrationsinstanzen		
Primäre Integrationen		
Unterstützende Integrationen		
Importsatztabellen		

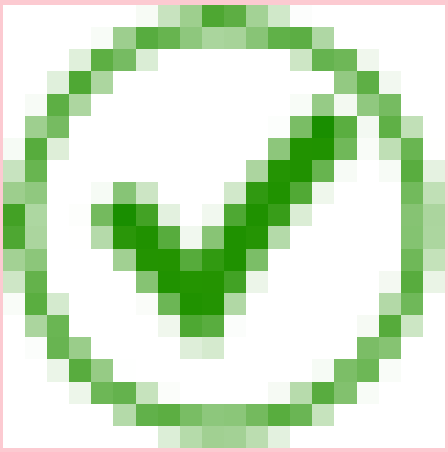
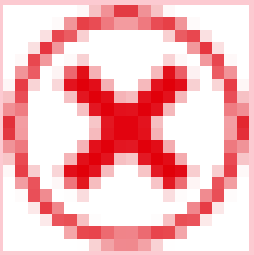
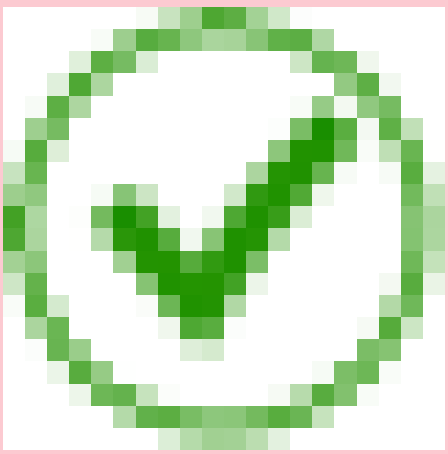
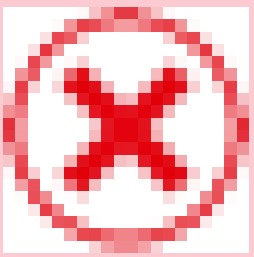
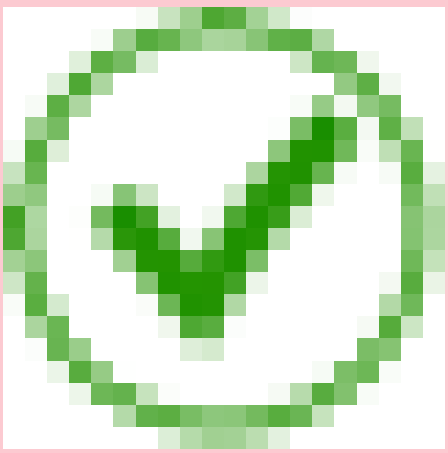
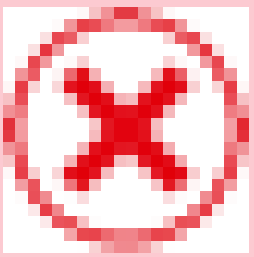
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul.configure_qualys_integration	sn_vul_qualys.lesen
Host-Import		
Import der Host-Erkennungsliste		
Wissensdatenbankimport		

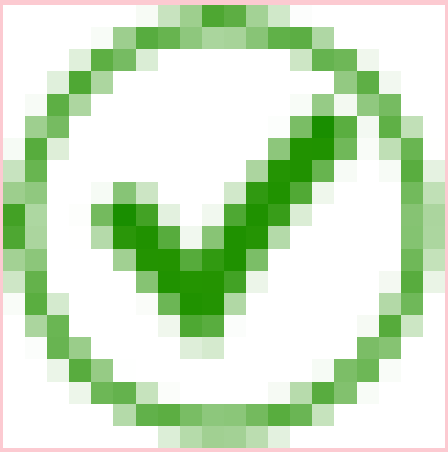
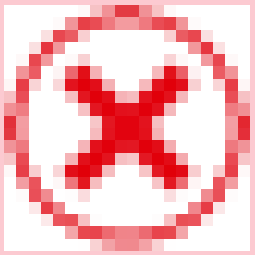
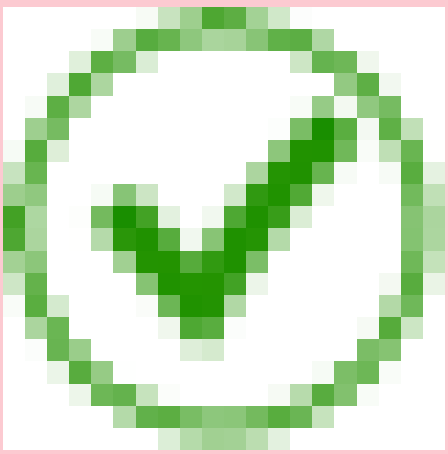
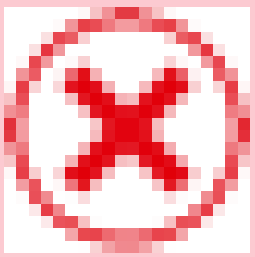
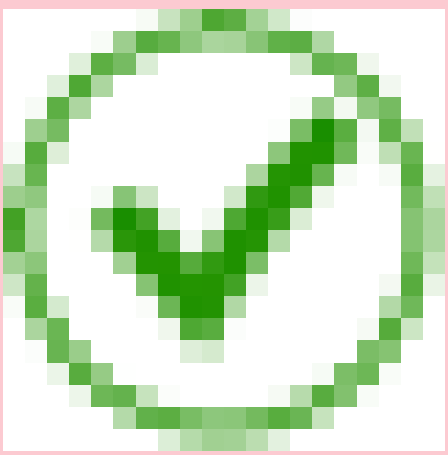
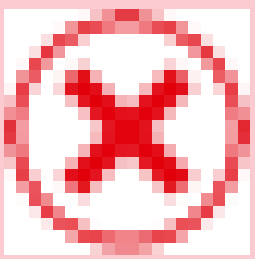
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul.configure_qualys_integration	sn_vul_qualys.lesen
Ticket-Listenimport		
Import dynamische Suchliste		
Import statische Suchliste		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul.configure_qualys_integration	sn_vul_qualys.lesen
Assetgruppenimport		
Appliance-Import		
Import der Host-Erkennungspaginierung		

[End]

[store-future: BEGIN review]

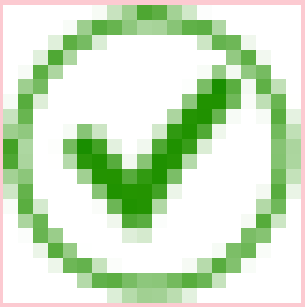
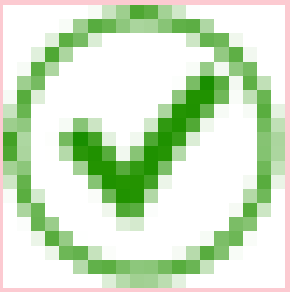
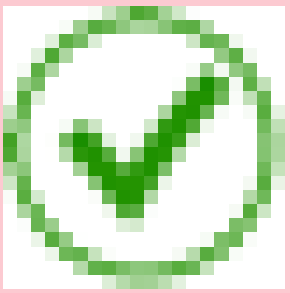
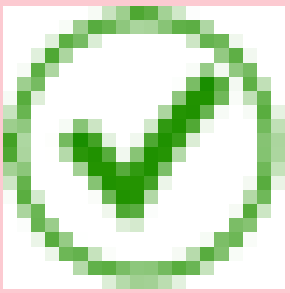
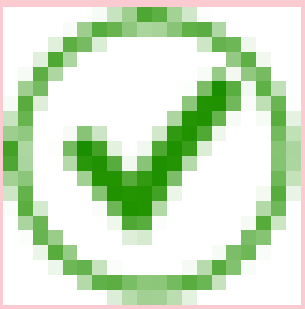
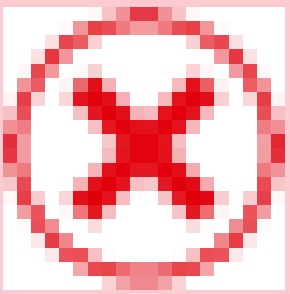
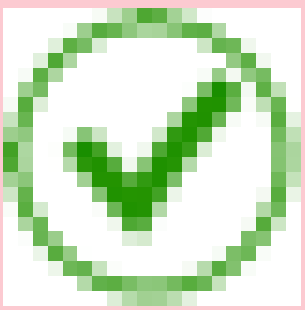
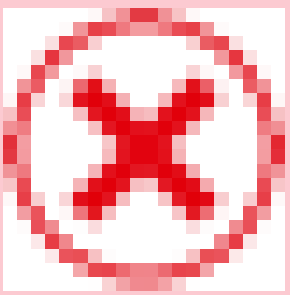
Modulzugriff nach Rolle für Rapid7 Vulnerability Integration

Informationen zu Rapid7 Vulnerability Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_vul_r7.admin	sn_vul_r7.lesen
(Haupt-App-Gruppe)		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul_r7.admin	sn_vul_r7.lesen
Status der Integrationsausführung		
Sites		
Lösungen		
Administration		
Integrationen		
Konfiguration		

[End]

[store-future: BEGIN review]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff nach Rolle für Security Incident

Beachten Sie bei Security Incident die Menüelemente, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
(Haupt-App-Gruppe)						
Incidents Neue UI	✗	✓	✓	✗	✗	
Serviceeinfluss	✗	✓	✗	✗	✗	
Übersicht	✗	✓	✓	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Echtzeit	✗	✓	✗	✗	✗	✗
Incidents						
Für mich sichtbar	✗	✗	✗	✗	✗	✗
Mir zugewiesen	✗	✓	✓	✓	✗	✓
Meine Arbeit	✗	✗	✗	✗	✓	✗

Automatische Übersetzung

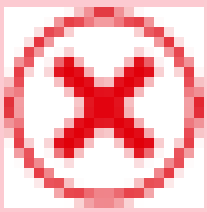
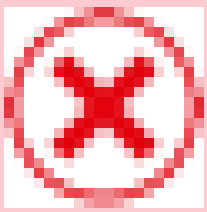
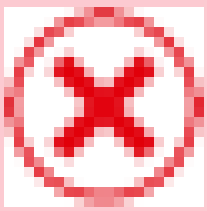
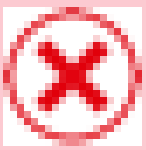
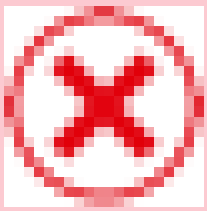
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Dem Team zugewiesen						
Offene Incidents anzeigen						
Alle Incidents anzeigen						
Nicht zugewiesene Incidents						
Antwortaufgaben						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Mir zugewiesen	✗	✓	✓	✓	✗	✓
Dem Team zugewiesen	✗	✓	✓	✓	✗	✓
Offene Aufgaben anzeigen	✗	✓	✓	✓	✗	✓
Alle Aufgaben anzeigen	✗	✓	✓	✓	✗	✓
Nicht zugewiesene Aufgaben	✗	✓	✓	✓	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Eingehende Anfragen						
Mir zugewiesen	✗	✓	✓	✓	✗	
Dem Team zugewiesen	✗	✓	✓	✓	✗	
Meine Genehmigungen	✗	✗	✗	✗	✗	
Offene Anfragen anzeigen	✗	✓	✓	✓	✗	

Automatische Übersetzung

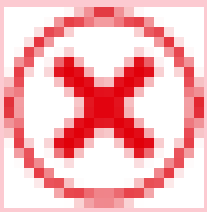
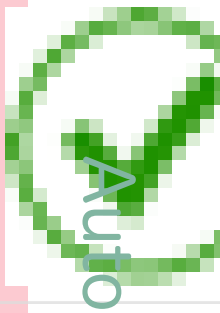
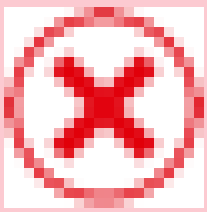
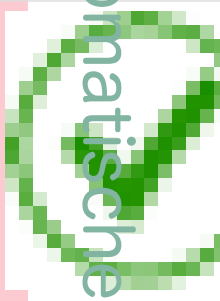
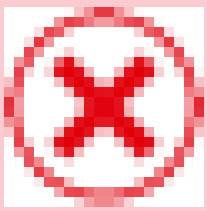
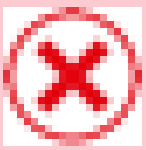
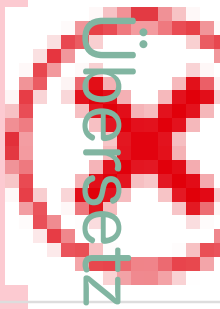
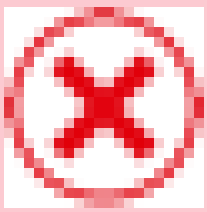
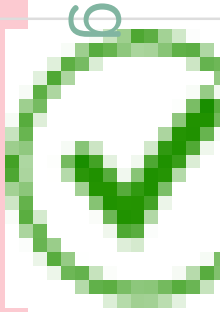
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Alle Anforderungen anzeigen						
Nicht zugewiesene Anfragen						
Meine Karte						
Warnungen und Ereignisse						
Überprüfung nach Incident						
Meine ausstehenden Überprüfungen						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Ausstehende Überprüfungen des Teams	✗	✓	✗	✗	✗	✗
Alle unvollständigen Überprüfungen	✗	✓	✗	✗	✗	✗
Setup						
Security Incident-Rechnergruppen	✗	✓	✗	✗	✗	✗
Schweregradrechner	✗	✓	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Risikopunktzahlkonfiguration	✓	✓	✓	✓	✗	✓
Nachrichtenfeed-Konfiguration	✗	✓	✓	✓	✗	✓
Gruppen	✗	✓	✗	✗	✗	✗
Rollen	✗	✓	✗	✗	✗	✗
SLAs	✗	✓	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Setup von Analyst Workspace (neue UI)						
Setup-Assistent	✗	✓	✗	✗	✗	✗
Konfiguration der Zielseitenfilter	✗	✓	✗	✗	✗	✗
Formular-UI-Aktionen	✗	✓	✗	✗	✗	✗
Konfigurationen zugehöriger Listen	✗	✓	✗	✗	✗	✗

Automatische Übersetzung

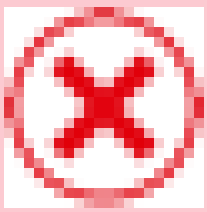
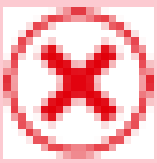
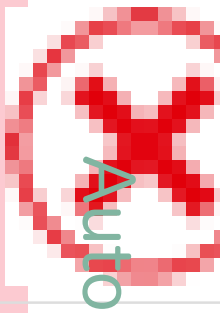
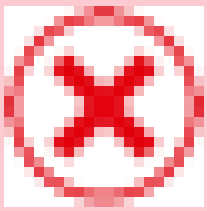
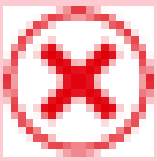
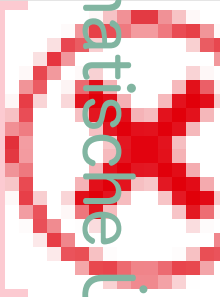
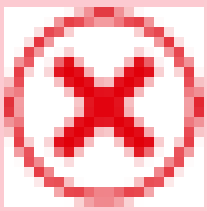
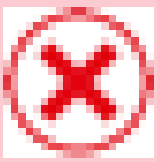
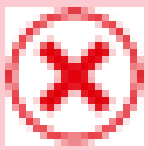
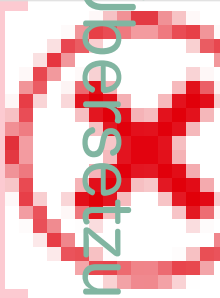
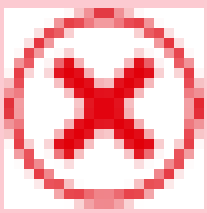
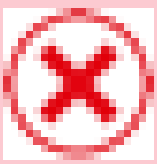
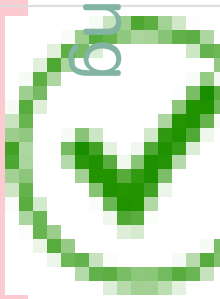
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Eigenschaften des Analystenarbeitsbereichs						
Katalog & Wissen						
Vorlagen für Security Incidents						
Katalogelemente pflegen						
Wissen						
Manuelles Runbook						

Automatische Übersetzung

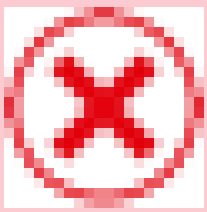
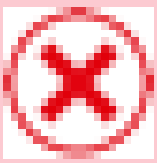
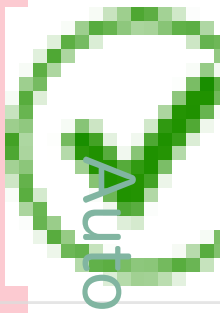
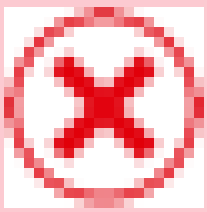
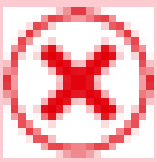
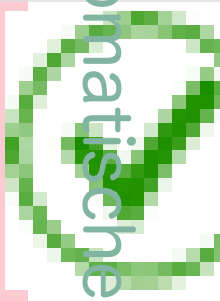
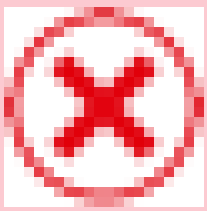
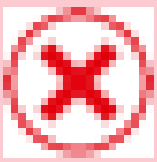
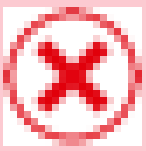
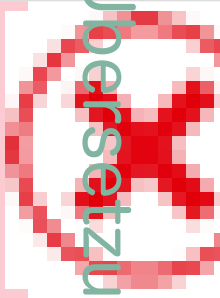
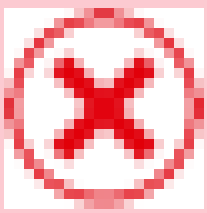
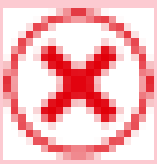
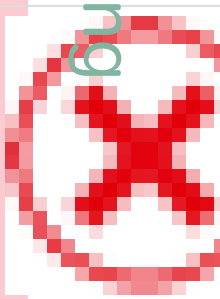
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Neues Runbook erstellen						
Runbook-Dokumente anzeigen						
Administration						
Eigenschaften						
Konfiguration						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Benachrichtigungen	✗	✓	✗	✗	✗	✗
Servicerelevanz-Reportingdefinition	✗	✓	✗	✗	✗	✗
Servicerelevanzdefinition	✗	✓	✗	✗	✗	✗
Serviceeinfluss-Definitionen	✗	✓	✗	✗	✗	✗
Bewertungen für Bewertungen der Überprüfung nach Incidents einrichten	✗	✓	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Setup des Berichts zur Überprüfung nach Incidents	✗	✓	✗	✗	✗	✗
Echtzeitdefinition	✗	✓	✗	✗	✗	✗
Prozessauswahl	✗	✓	✗	✗	✗	✗
Prozessdefinitionen	✗	✓	✗	✗	✗	✗
Vorlagenworkflow – Ergebnisauswertung	✗	✓	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informationen für andere Rollen:

sn_si.spezial_access, sn_si_approver_user

(Fortsetzung)

Modul	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.extern	sn_si.knowledge_a
Phishing-E-Mails						
Lizenzverwaltung	✗	✓	✗	✗	✗	✗
Phishing-E-Mail melden	✗	✓	✓	✗	✗	✗
Alle Phishing-E-Mails anzeigen	✗	✓	✓	✗	✗	✗

Automatische Übersetzung

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Modul	sn_si. special_access	sn_si_approver_user
(Haupt-App-Gruppe)		

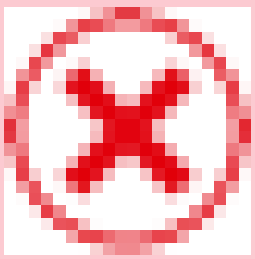
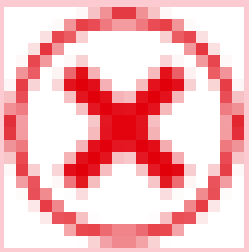
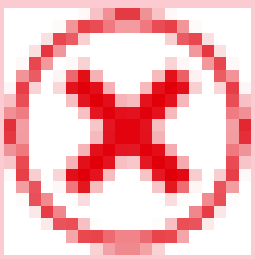
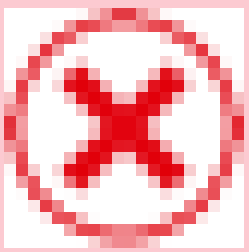
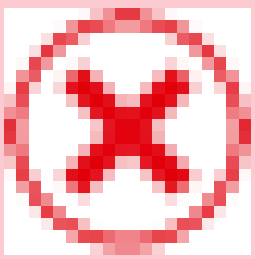
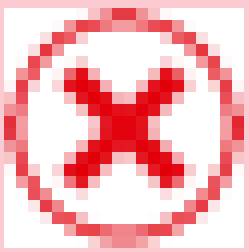
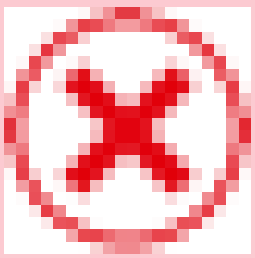
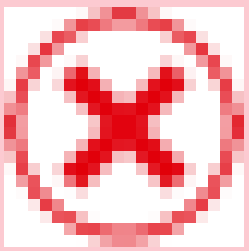
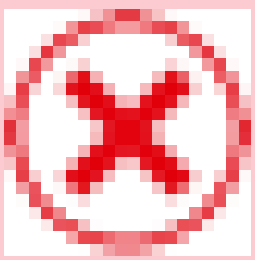
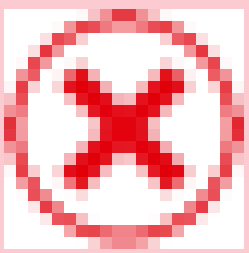
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Incidents Neue UI		
Serviceeinfluss		
Übersicht		
Echtzeit		
Incidents		
Für mich sichtbar		

Automatische Übersetzung

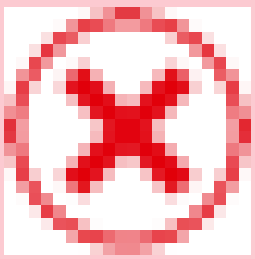
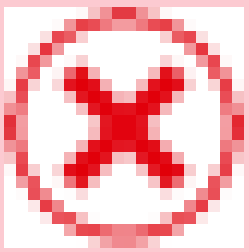
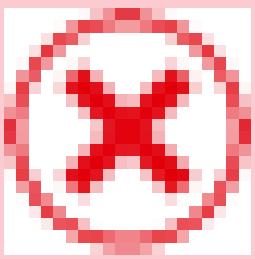
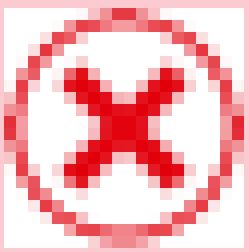
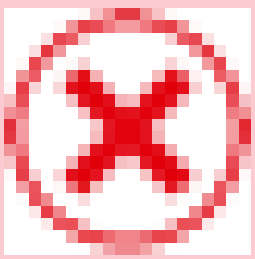
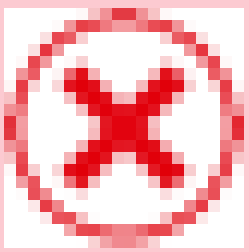
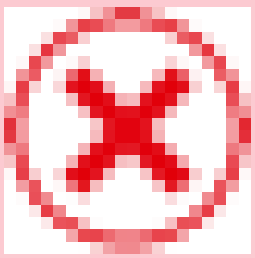
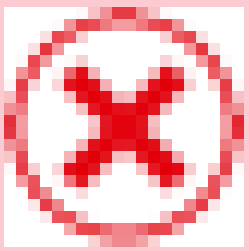
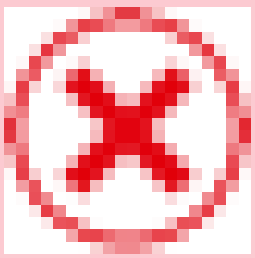
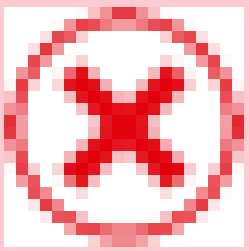
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Mir zugewiesen		
Meine Arbeit		
Dem Team zugewiesen		
Offene Incidents anzeigen		
Alle Incidents anzeigen		

Automatische Übersetzung

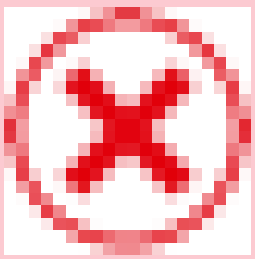
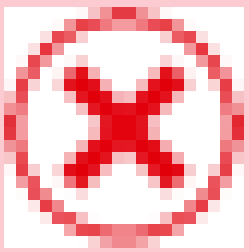
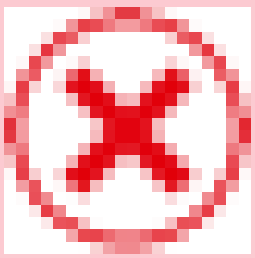
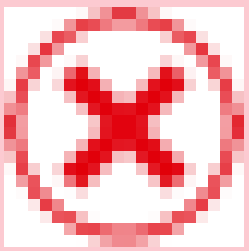
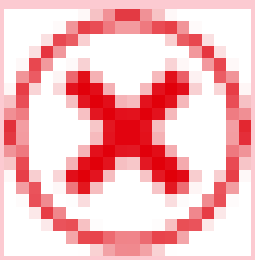
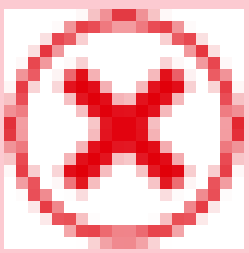
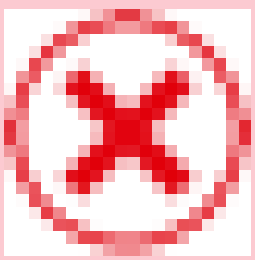
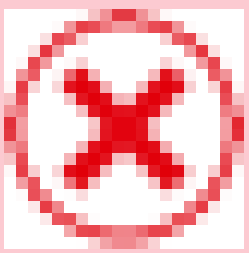
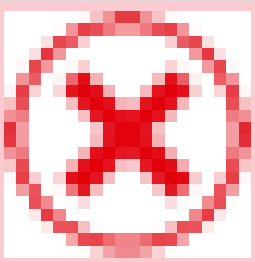
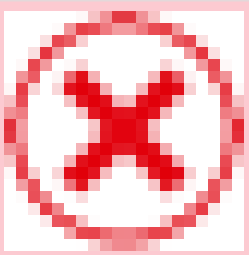
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Nicht zugewiesene Incidents		
Antwortaufgaben		
Mir zugewiesen		
Dem Team zugewiesen		
Offene Aufgaben anzeigen		
Alle Aufgaben anzeigen		

Automatische Übersetzung

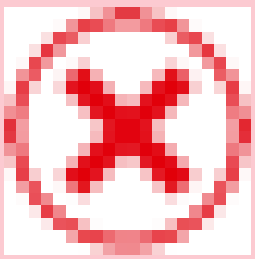
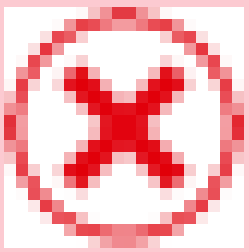
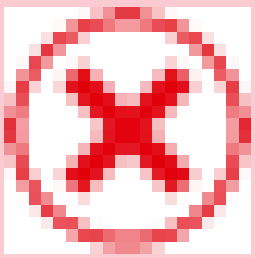
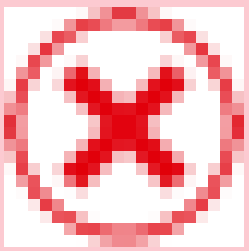
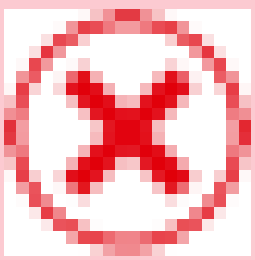
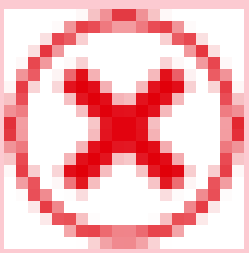
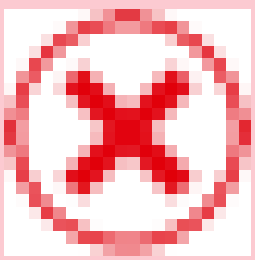
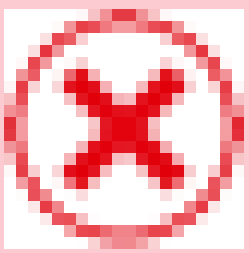
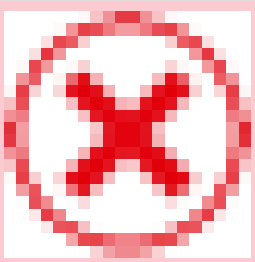
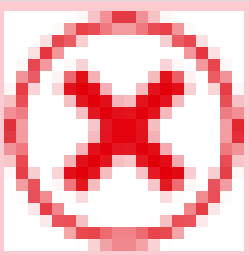
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Nicht zugewiesene Aufgaben		
Eingehende Anfragen		
Mir zugewiesen		
Dem Team zugewiesen		
Meine Genehmigungen		
Offene Anfragen anzeigen		

Automatische Übersetzung

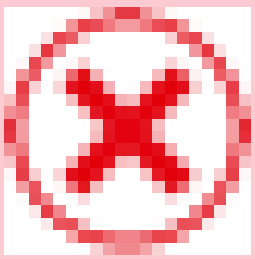
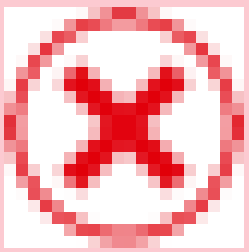
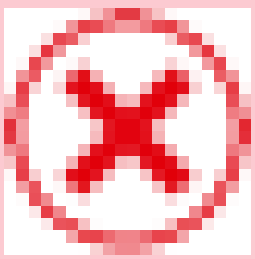
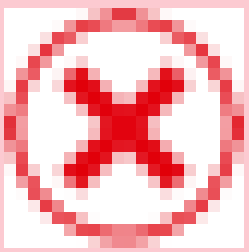
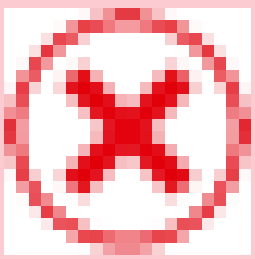
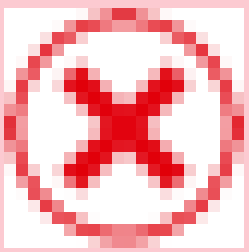
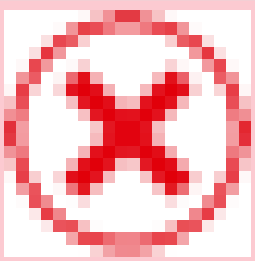
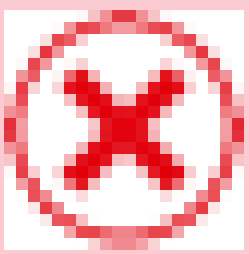
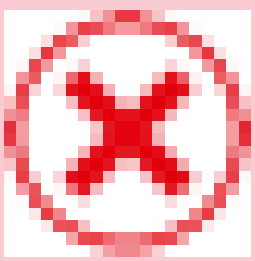
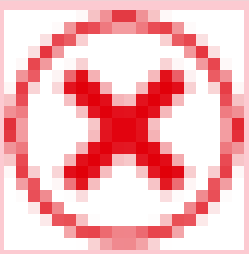
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Alle Anforderungen anzeigen		
Nicht zugewiesene Anfragen		
Meine Karte		
Warnungen und Ereignisse		
Überprüfung nach Incident		
Meine ausstehenden Überprüfungen		
Ausstehende Überprüfungen des Teams		

Automatische Übersetzung

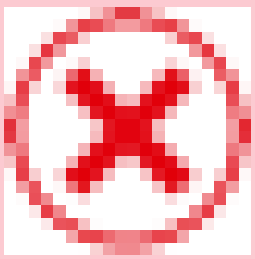
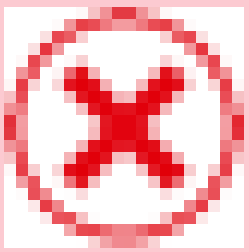
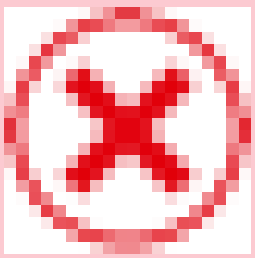
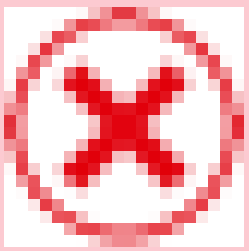
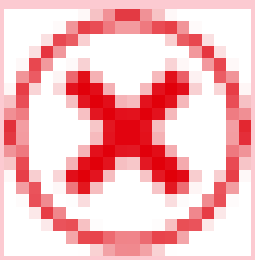
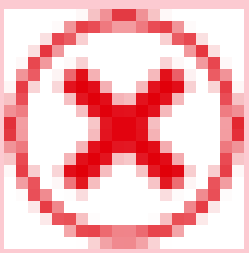
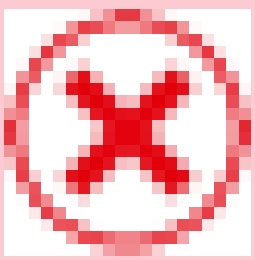
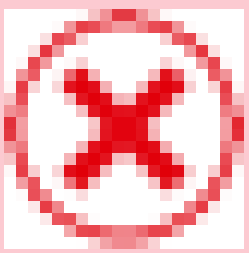
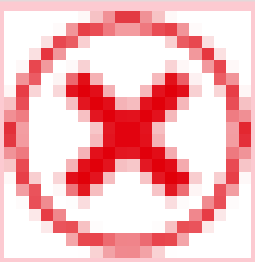
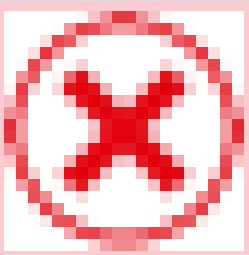
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Alle unvollständigen Überprüfungen		
Setup		
Security Incident-Rechnergruppen		
Schweregradrechner		
Risikopunktzahlkonfiguration		
Nachrichtenfeed-Konfiguration		

Automatische Übersetzung

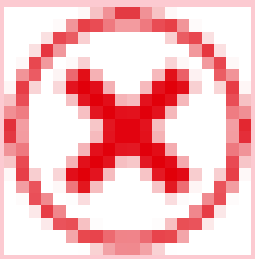
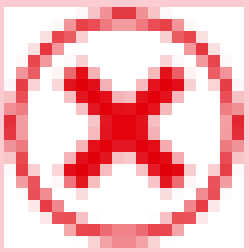
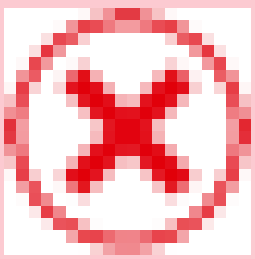
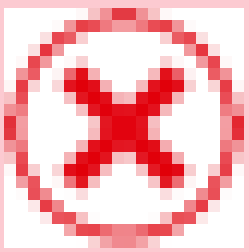
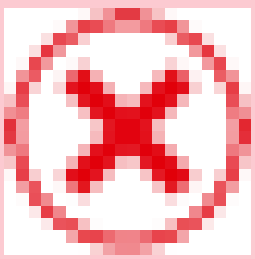
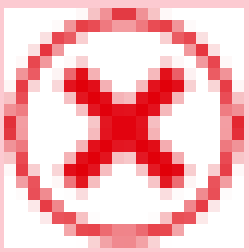
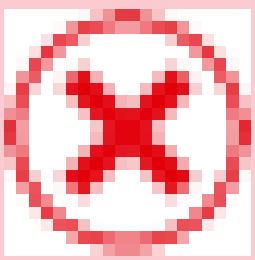
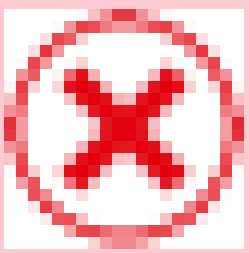
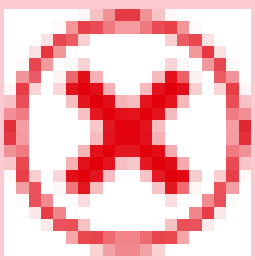
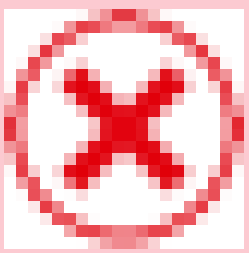
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Gruppen		
Rollen		
SLAs		
Setup von Analyst Workspace (neue UI)		
Setup-Assistent		
Konfiguration der Zielseitenfilter		

Automatische Übersetzung

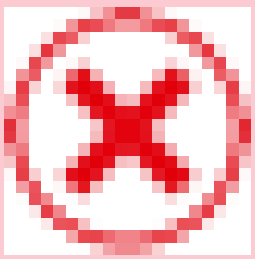
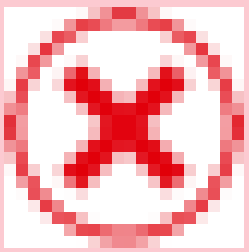
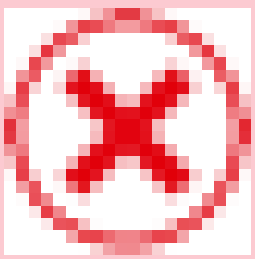
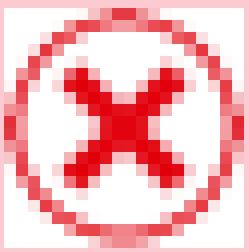
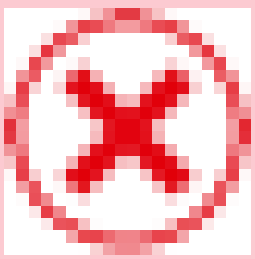
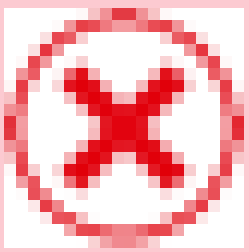
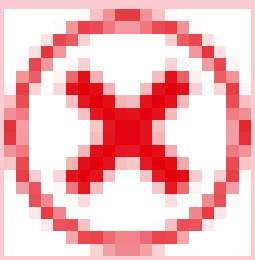
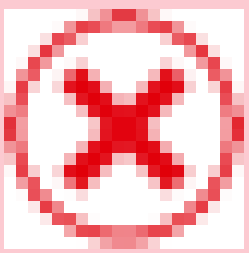
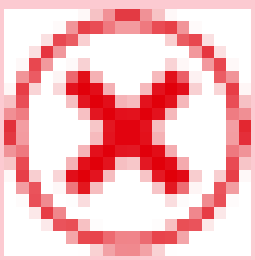
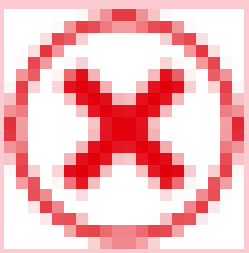
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Formular-UI-Aktionen		
Konfigurationen zugehöriger Listen		
Eigenschaften des Analystenarbeitsbereichs		
Katalog & Wissen		
Vorlagen für Security Incidents		
Katalogelemente pflegen		

Automatische Übersetzung

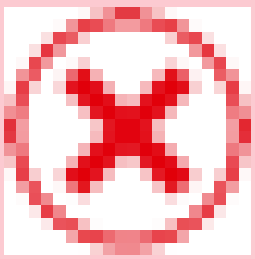
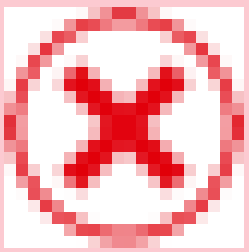
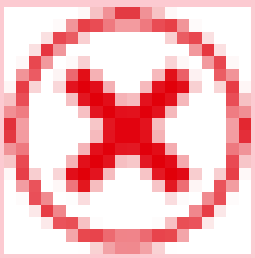
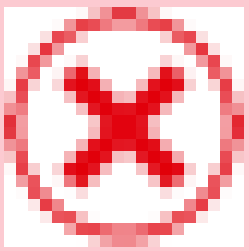
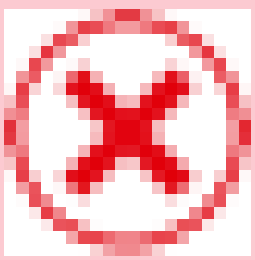
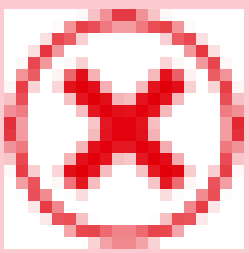
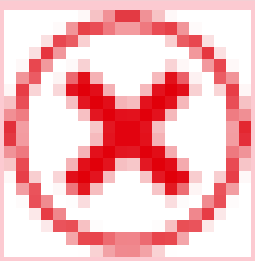
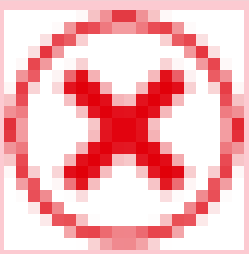
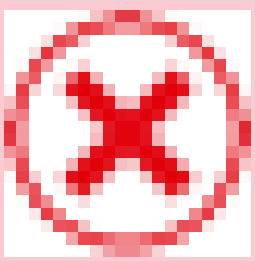
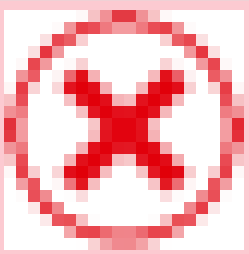
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Wissen		
Manuelles Runbook		
Neues Runbook erstellen		
Runbook-Dokumente anzeigen		
Administration		
Eigenschaften		
Konfiguration		

Automatische Übersetzung

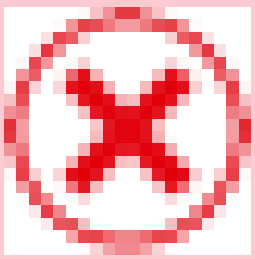
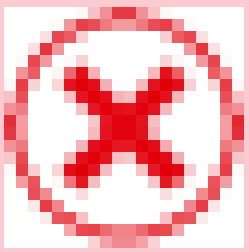
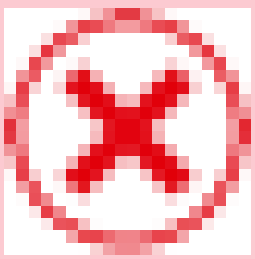
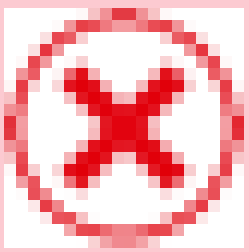
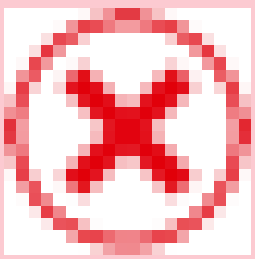
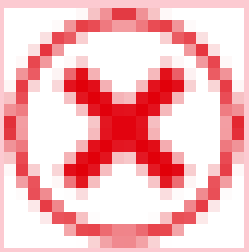
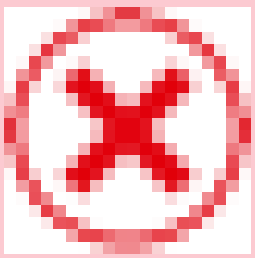
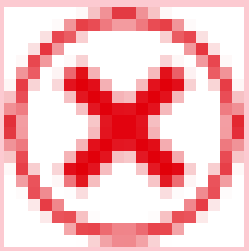
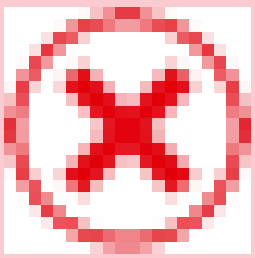
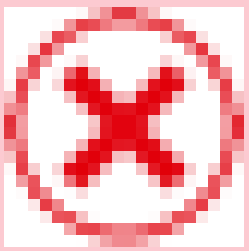
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Benachrichtigungen		
Servicerelevanz-Reportingdefinition		
Servicerelevanzdefinition		
Serviceeinfluss-Definitionen		
Bewertungen für Bewertungen der Überprüfung nach Incidents einrichten		

Automatische Übersetzung

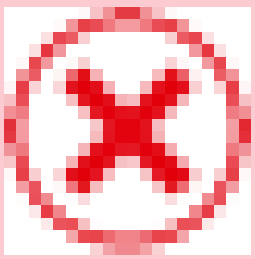
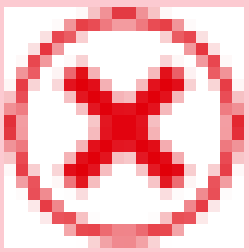
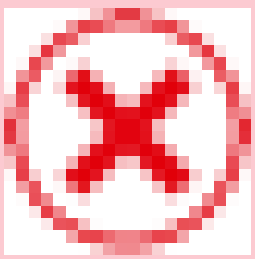
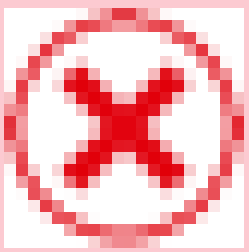
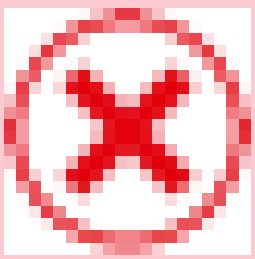
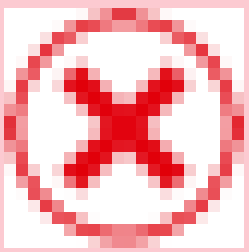
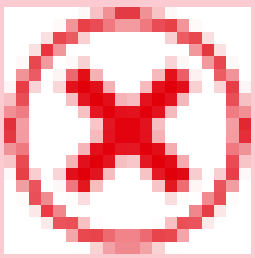
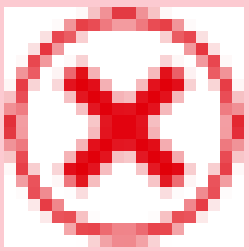
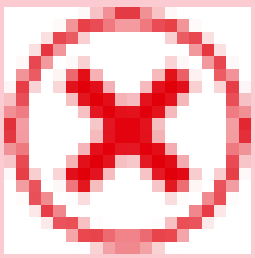
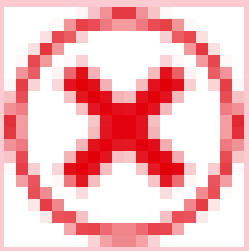
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Setup des Berichts zur Überprüfung nach Incidents		
Echtzeitdefinition		
Prozessauswahl		
Prozessdefinitionen		
Vorlagenworkflow – Ergebnisauswertung		
Phishing-E-Mails		

Automatische Übersetzung

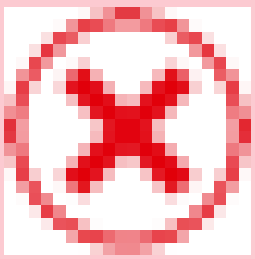
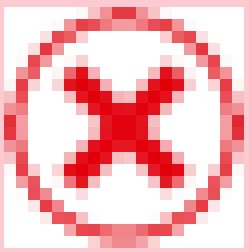
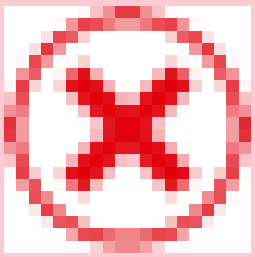
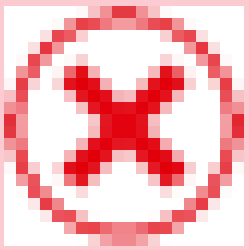
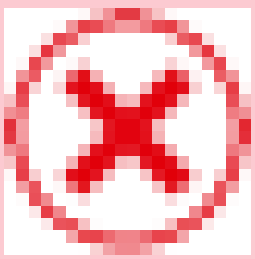
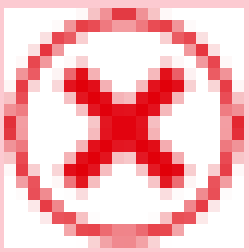
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si. special_access, sn_si_approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.cso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

(Fortsetzung)

Modul	sn_si. special_access	sn_si_approver_user
Lizenzverwaltung		
Phishing-E-Mail melden		
Alle Phishing-E-Mails anzeigen		

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Security Operations

Informationen zu Security Operations finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Automatische Übersetzung

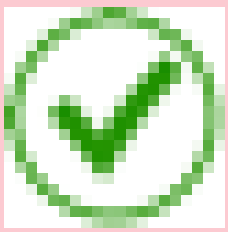
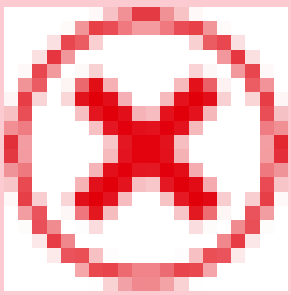
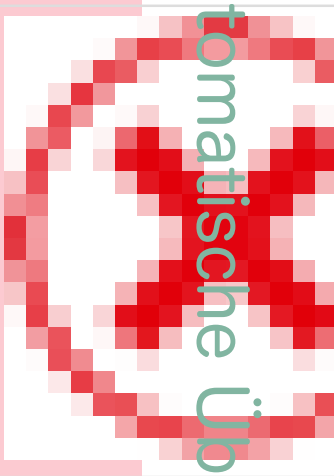
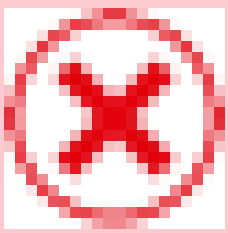
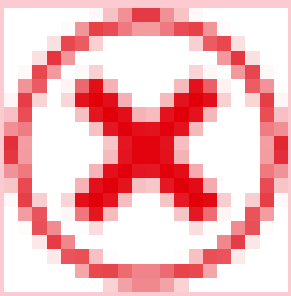
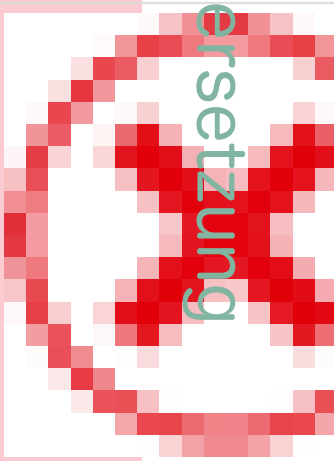
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
(Haupt-App-Gruppe)				
Integrationen				
Flows für Integrationsfähigkeiten				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Fähigkeitsausführungen	✓	✗	✗	✗
Ratenbegrenzung für Fähigkeitsimplementierungen	✓	✗	✗	✗
Integrationskonfigurationen	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Sichtungssuche – Konfiguration	✓	✓	✗	✗
Integrationsfunktionen	✓	✓	✗	✗
Integrationen				
Flows für Integrationsfähigkeiten	✓	✗	✗	✗

Automatische Übersetzung

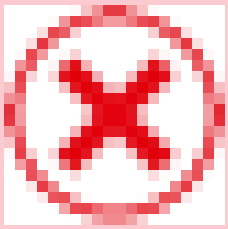
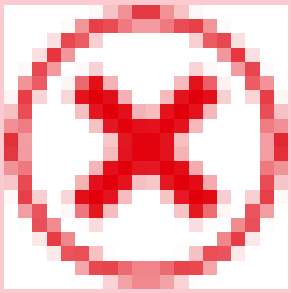
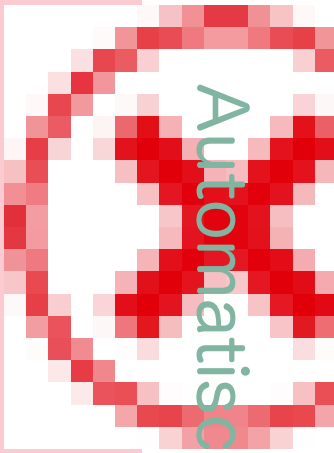
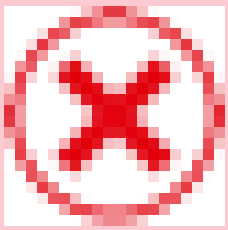
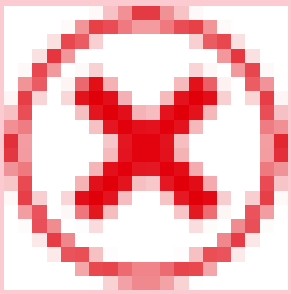
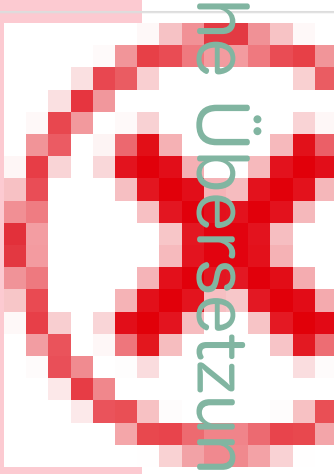
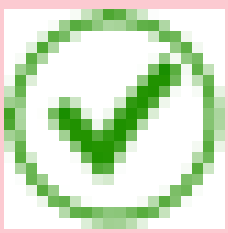
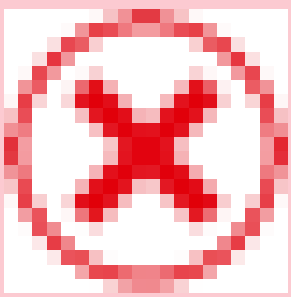
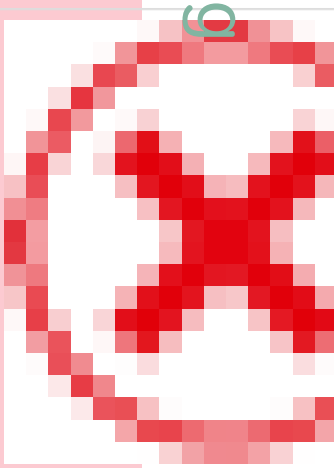
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Fähigkeitsausführungen				
Ratenbegrenzung für Fähigkeitsimplementierungen				
Integrationskonfigurationen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Sichtungssuche – Konfiguration	✓	✓	✗	✗
Integrationsfunktionen	✓	✓	✗	✗
E-Mail-Verarbeitung				
E-Mail-Analyse	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Duplizierungsregeln	✓	✓	✗	✗
Eigenschaften	✓	✓	✗	✗
Nicht übereinstimmende E-Mails	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Erfassungsregeln – Anwender hat Phishing gemeldet	✗	✗	✗	✗
Eigenschaften des vom Anwender gemeldeten Phishing	✓	✗	✗	✗
Gruppen				
Filtergruppen	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Eskalationen	✓	✓	✗	✗
Datenergänzungen				
Sicherheits-Tags				
Gruppen	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Tags	✓	✓	✗	✗
Workflows				
Ausführungsverfolgung	✓	✓	✗	✗
Sicherheitsworkflows anzeigen	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Workflow-Auslöser	✓	✓	✗	✗
Dienstprogramme				
Ergänzungsdatenzuordnung	✓	✓	✗	✗
Feldwertumwandlungen	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Feldzuordnung	✓	✓	✗	✗
Orchestration bei Bedarf	✓	✗	✗	✗
Betriebssystemgruppen	✓	✓	✗	✗

Automatische Übersetzung

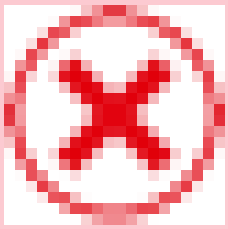
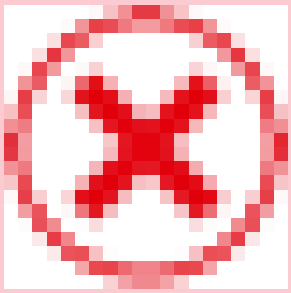
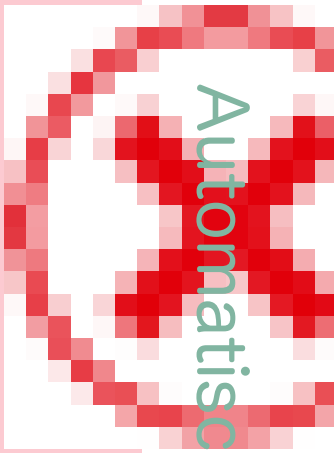
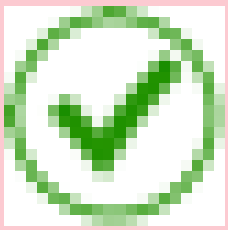
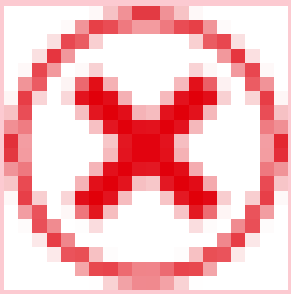
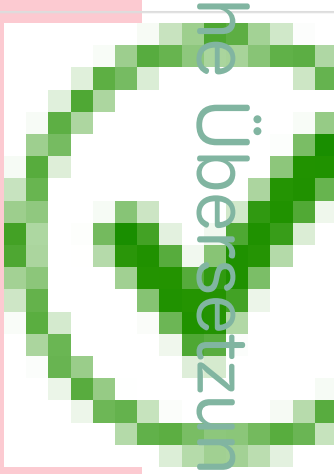
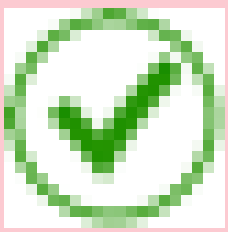
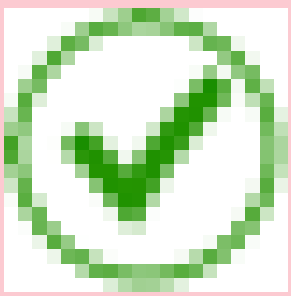
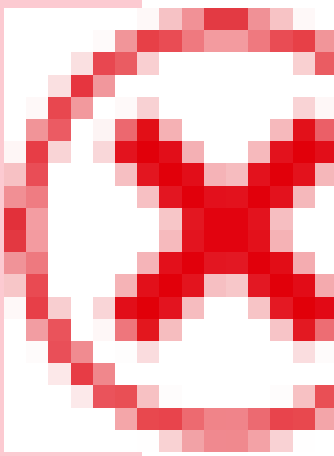
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
SecOps-Applikationsregistrierung				
Hintergrundauftrags-Konfiguration				
CMDB				
CI-Suchregeln				

Automatische Übersetzung

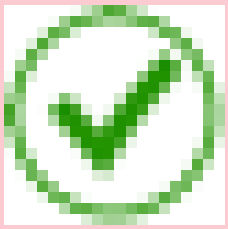
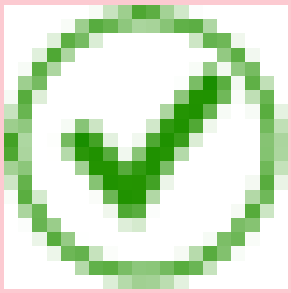
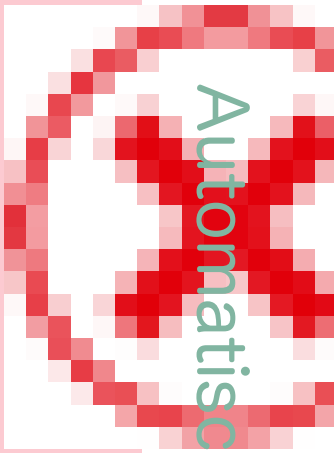
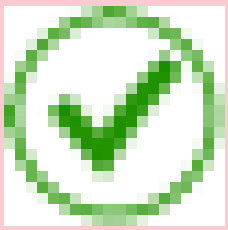
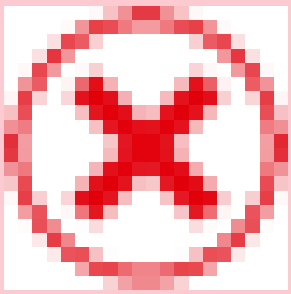
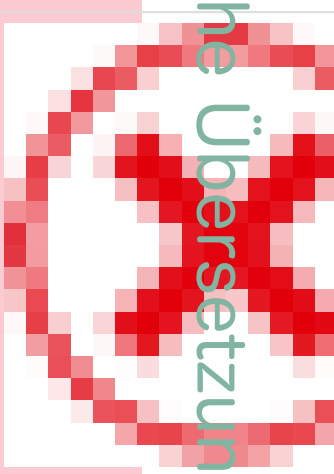
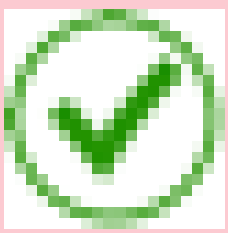
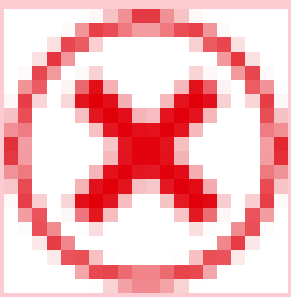
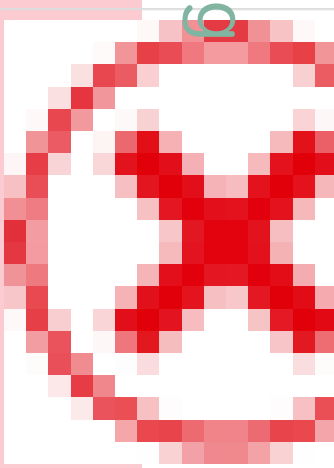
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Erkannte Elemente				
Nicht übereinstimmende erkannte Elemente abstimmen				
Erkannte Container-Images				
WatchDog				

Automatische Übersetzung

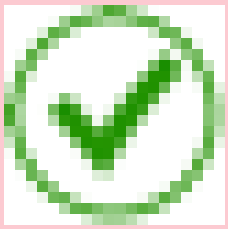
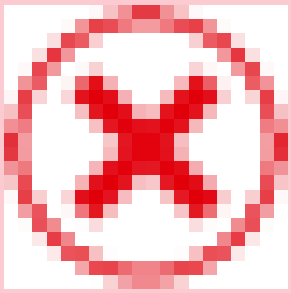
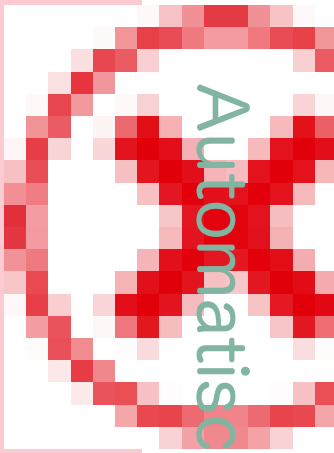
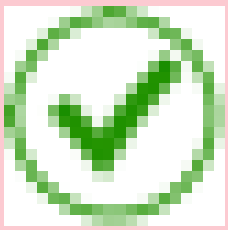
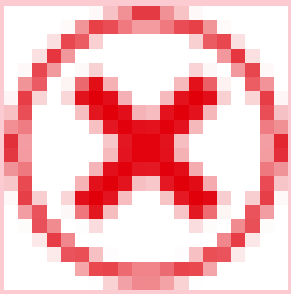
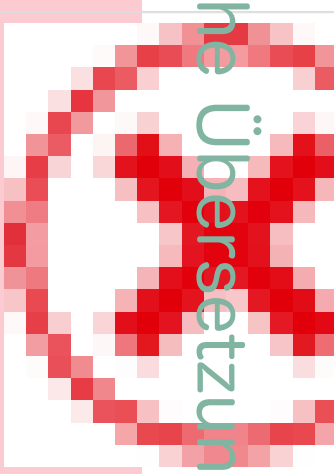
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_backgr
Konfiguration				
Übersicht				

Automatische Übersetzung

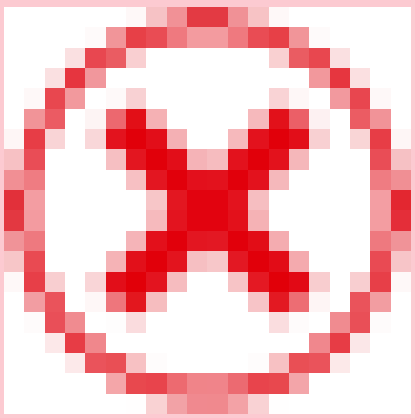
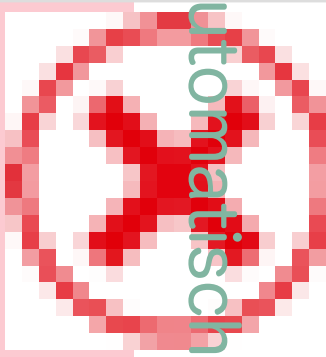
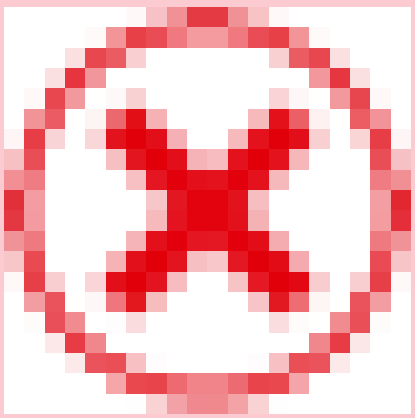
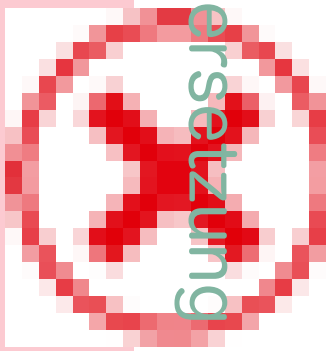
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
(Haupt-App-Gruppe)				
Integrationen				
Flows für Integrationsfähigkeiten				

Automatische Übersetzung

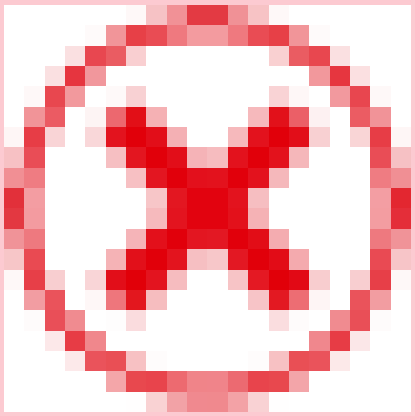
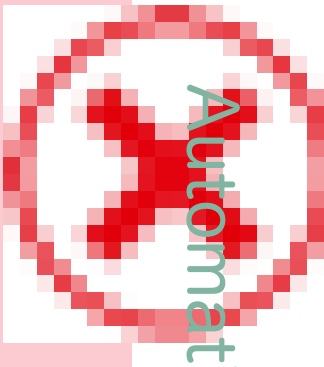
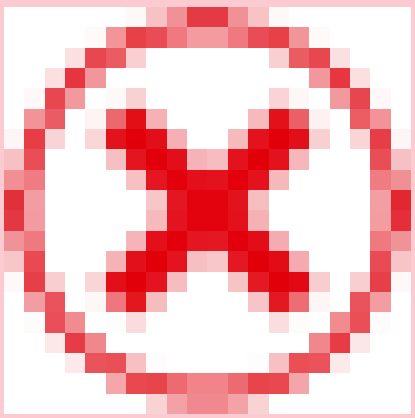
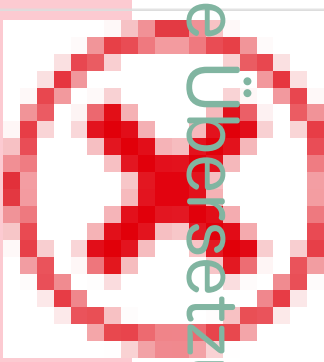
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Fähigkeitsausführungen				
Ratenbegrenzung für Fähigkeitsimplementierungen				

Automatische Übersetzung

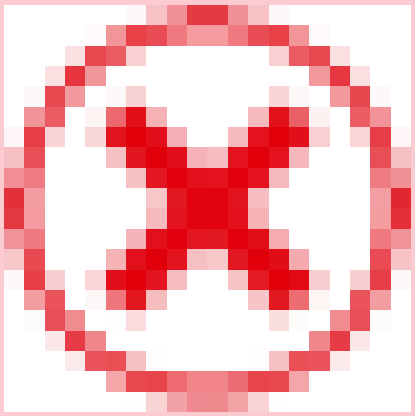
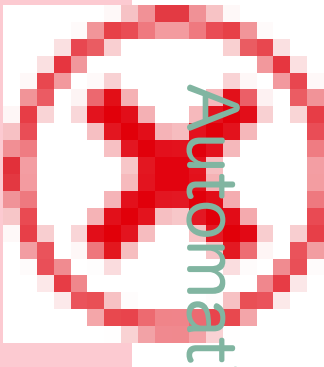
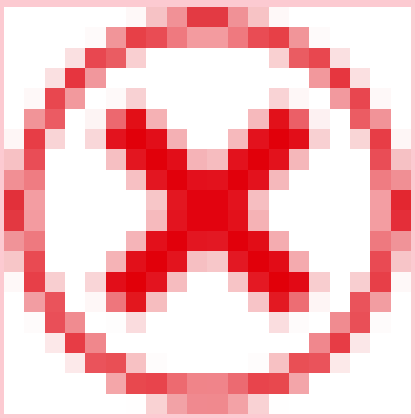
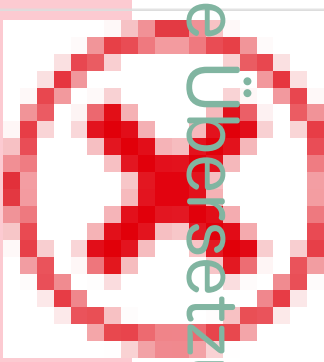
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Integrationskonfigurationen				
Sichtungssuche – Konfiguration				

Automatische Übersetzung

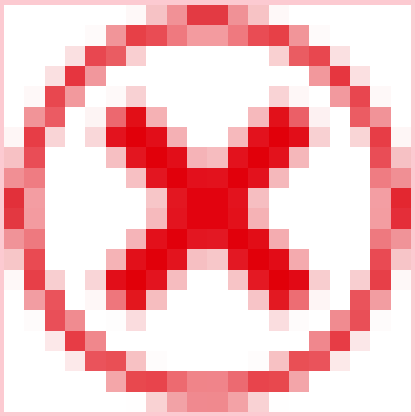
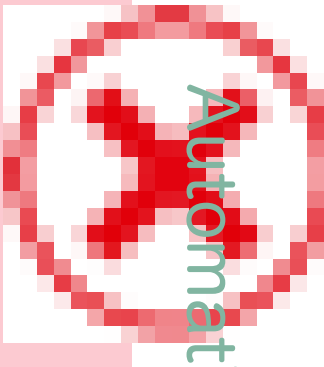
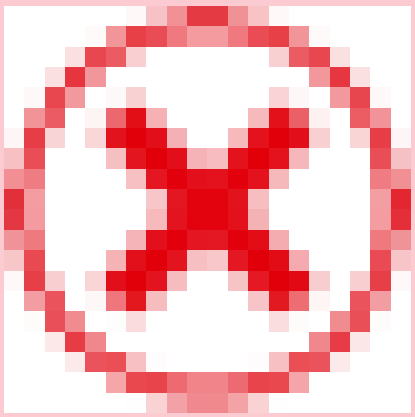
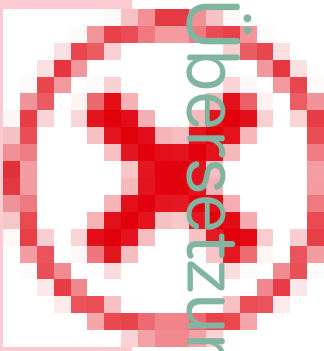
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Integrationsfunktionen				
Integrationen				
Flows für Integrationsfähigkeiten				

Automatische Übersetzung

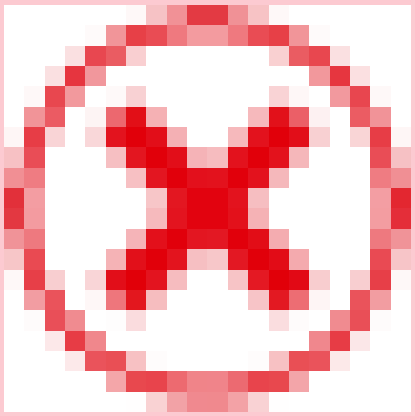
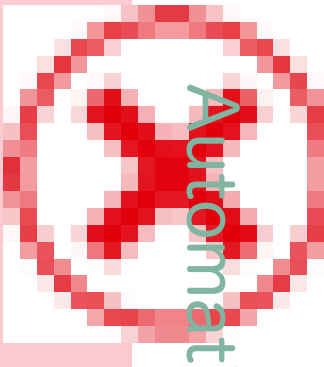
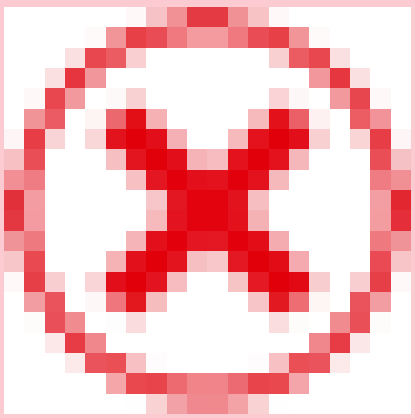
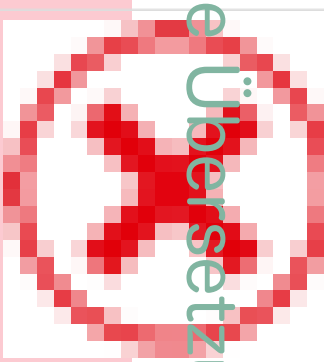
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Fähigkeitsausführungen				
Ratenbegrenzung für Fähigkeitsimplementierungen				

Automatische Übersetzung

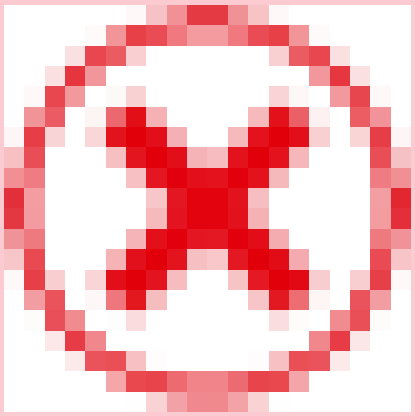
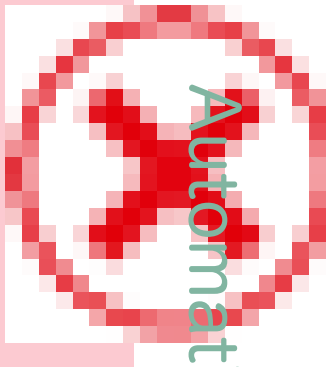
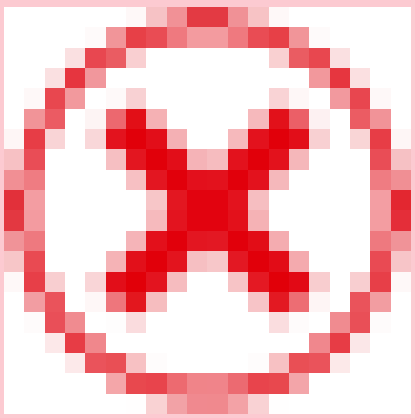
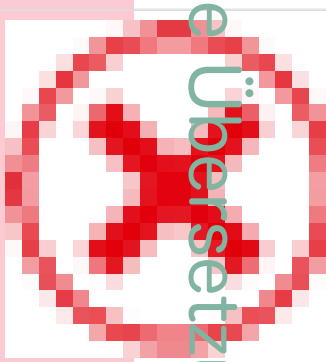
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Integrationskonfigurationen				
Sichtungssuche – Konfiguration				

Automatische Übersetzung

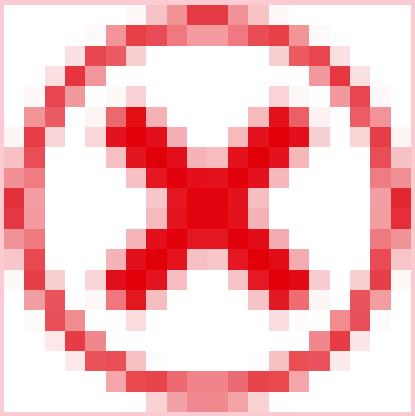
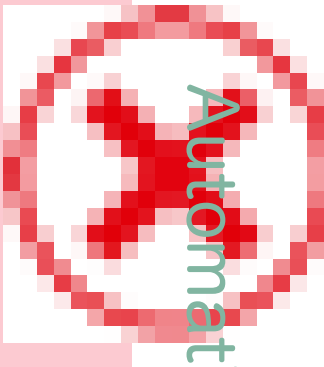
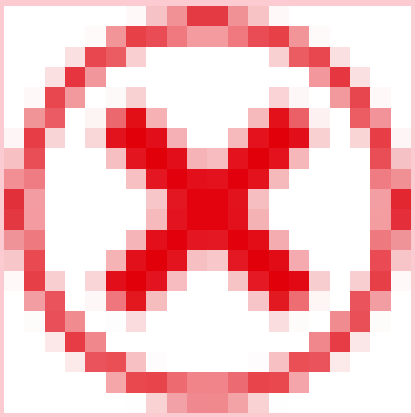
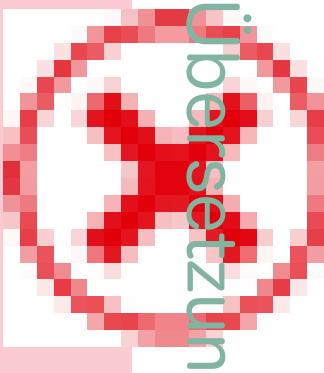
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Integrationsfunktionen				
E-Mail-Verarbeitung				
E-Mail-Analyse				

Automatische Übersetzung

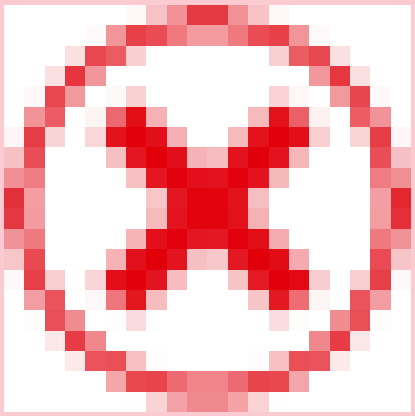
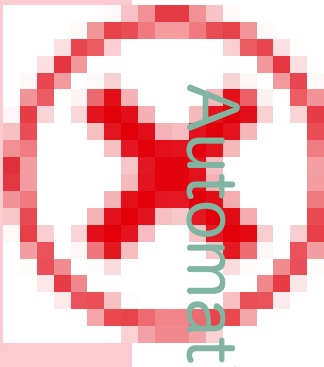
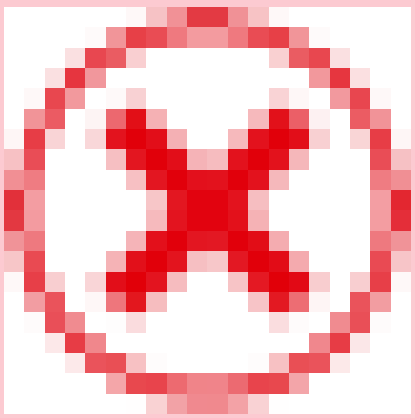
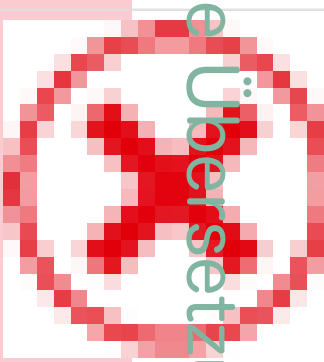
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Duplizierungsregeln				
Eigenschaften				

Automatische Übersetzung

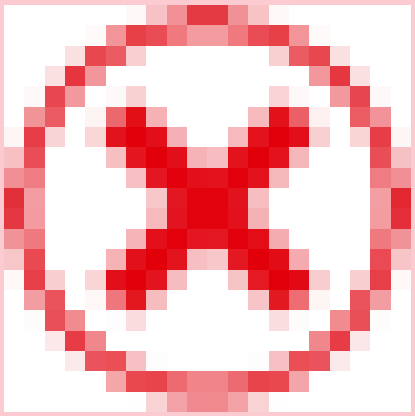
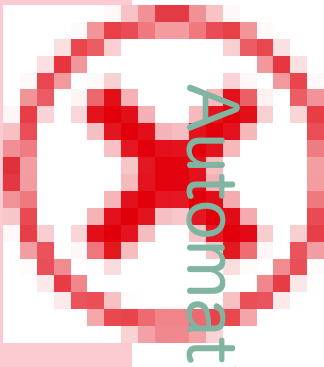
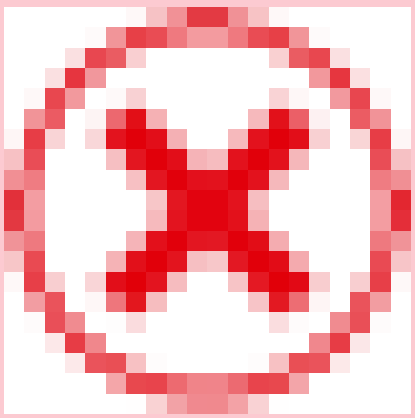
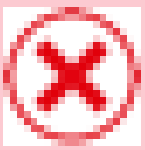
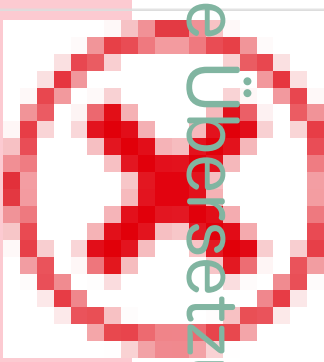
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Nicht übereinstimmende E-Mails				
Erfassungsregeln – Anwender hat Phishing gemeldet				

Automatische Übersetzung

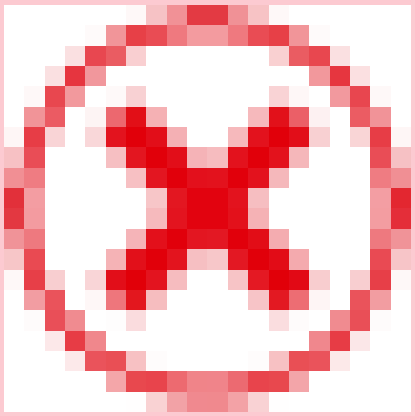
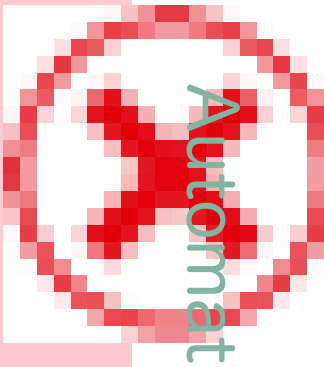
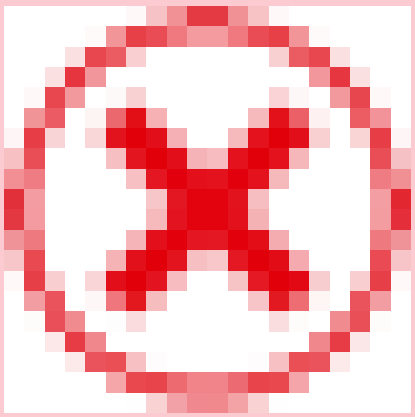
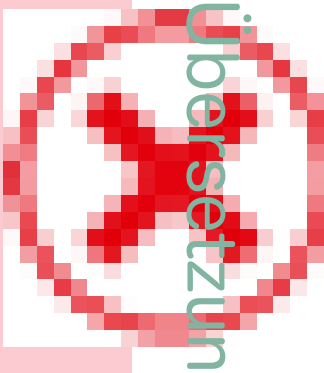
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Eigenschaften des vom Anwender gemeldeten Phishing				
Gruppen				
Filtergruppen				

Automatische Übersetzung

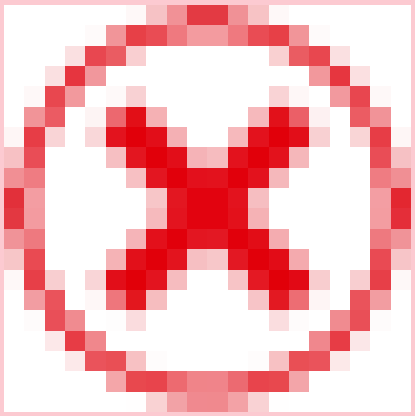
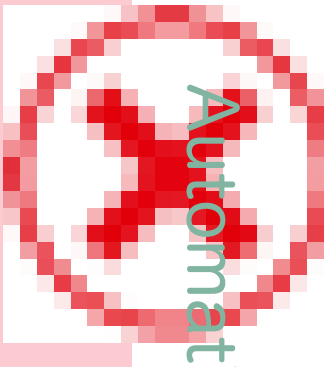
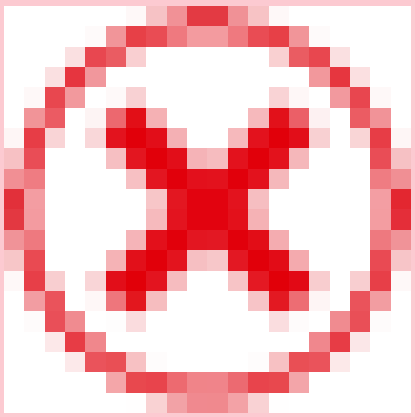
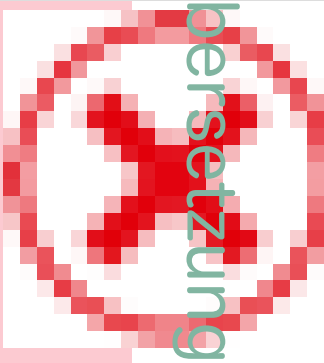
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Eskalationen				
Datenergänzungen				
Sicherheits-Tags				
Gruppen				

Automatische Übersetzung

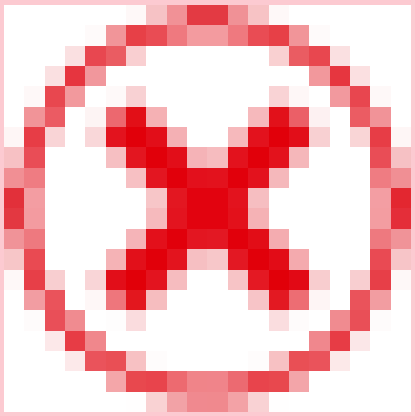
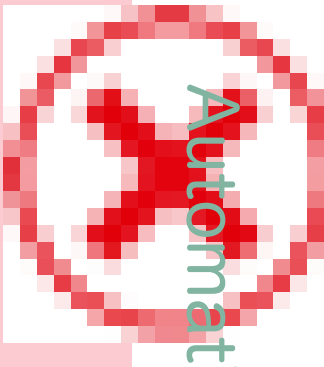
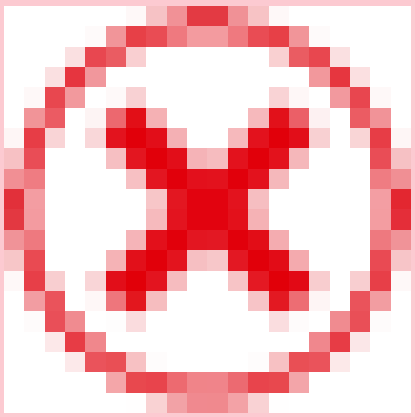
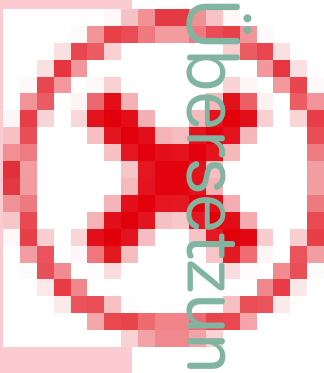
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Tags				
Workflows				
Ausführungsverfolgung				

Automatische Übersetzung

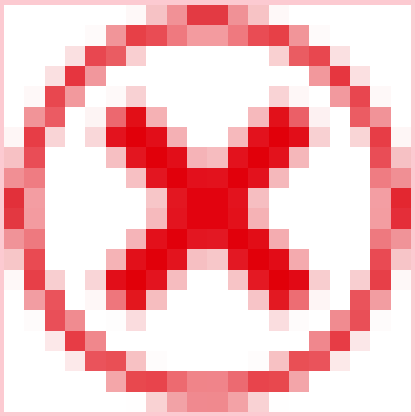
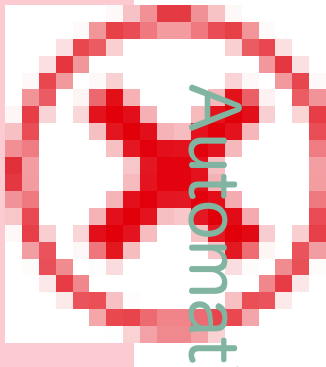
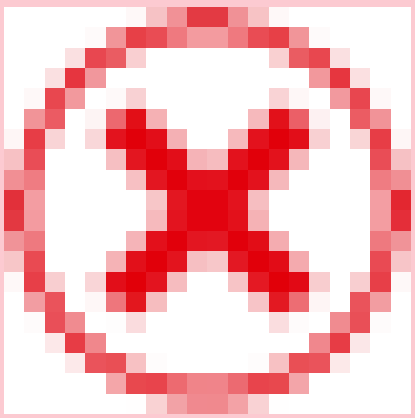
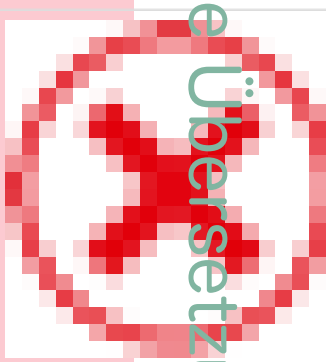
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Sicherheitsworkflows anzeigen				
Workflow-Auslöser				
Dienstprogramme				

Automatische Übersetzung

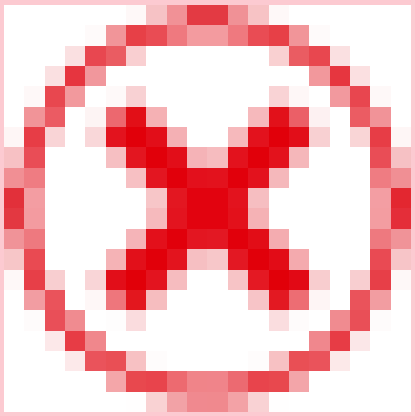
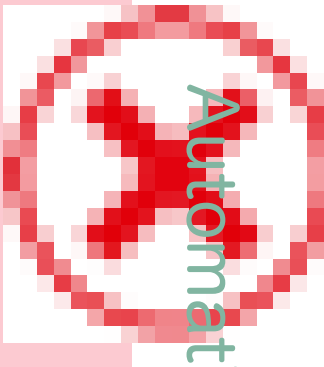
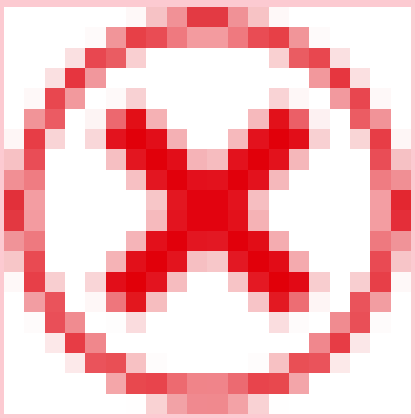
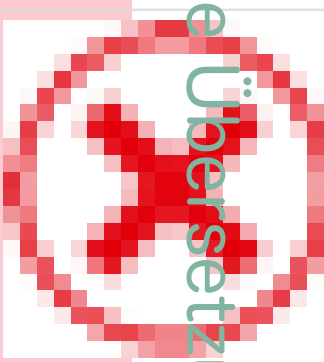
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Ergänzungsdatenzuordnung				
Feldwertumwandlungen				

Automatische Übersetzung

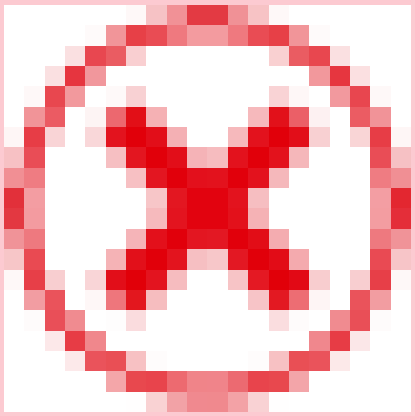
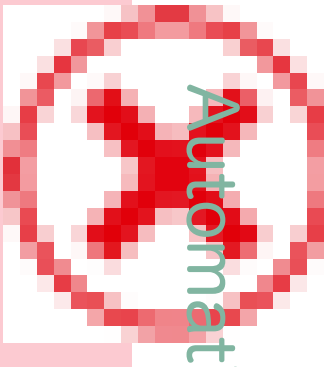
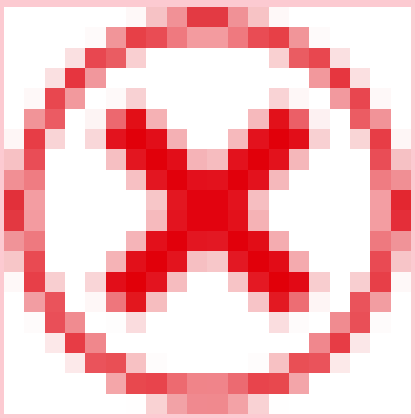
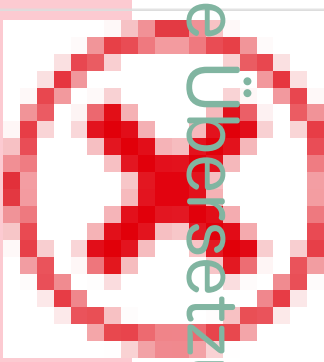
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Feldzuordnung				
Orchestration bei Bedarf				

Automatische Übersetzung

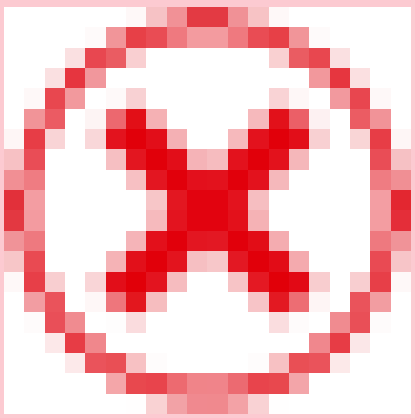
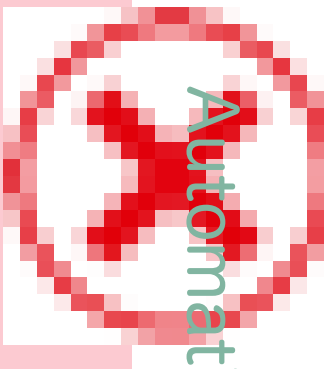
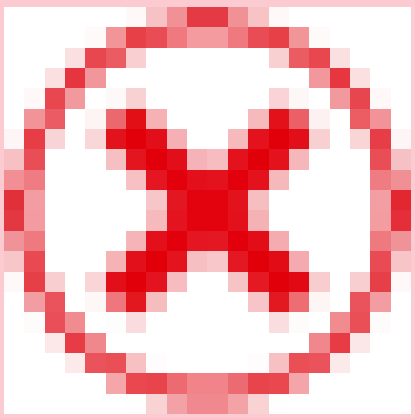
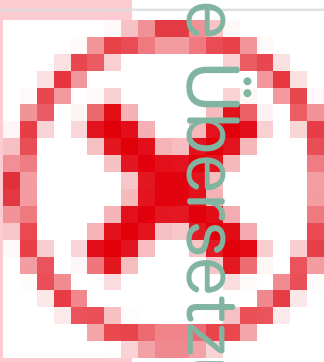
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Betriebssystemgruppen				
SecOps-Applikationsregistrierung				

Automatische Übersetzung

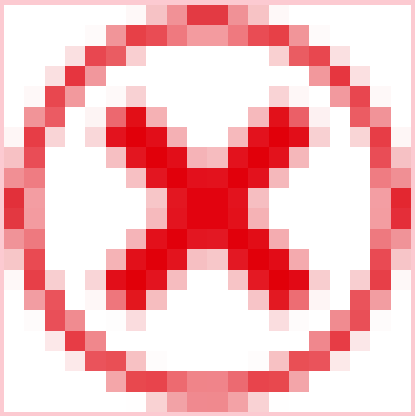
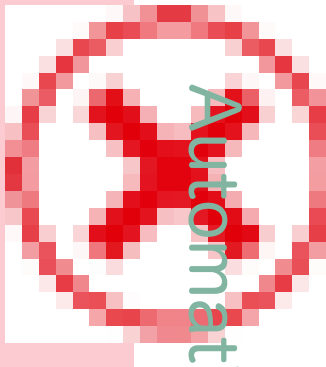
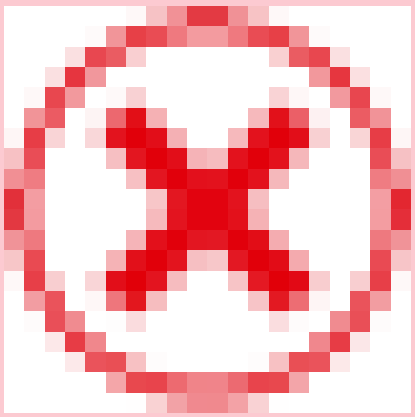
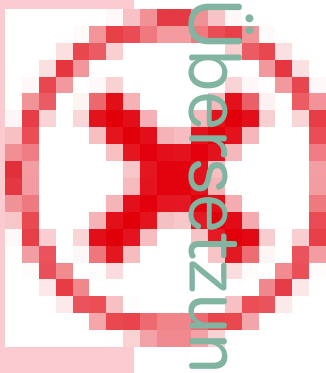
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Hintergrundauftrags-Konfiguration				
CMDB				
CI-Suchregeln				

Automatische Übersetzung

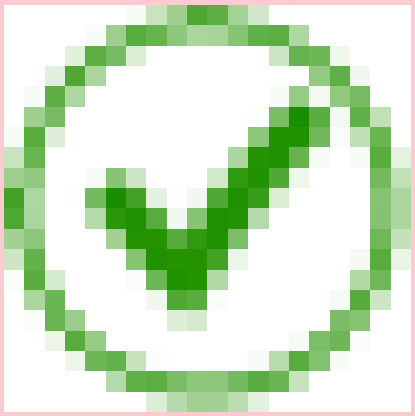
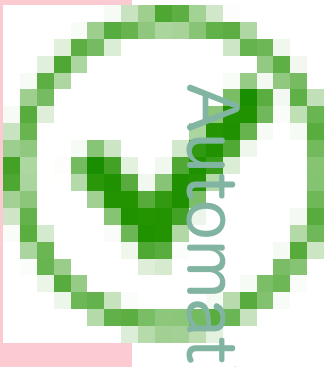
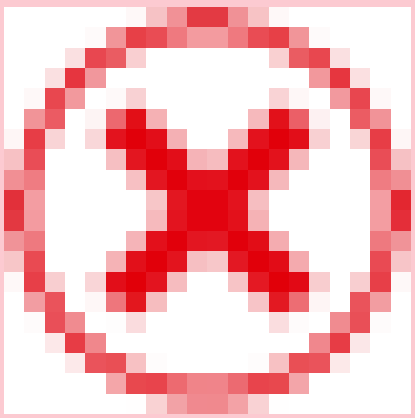
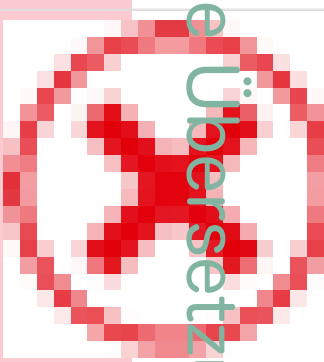
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Erkannte Elemente				
Nicht übereinstimmende erkannte Elemente abstimmen				

Automatische Übersetzung

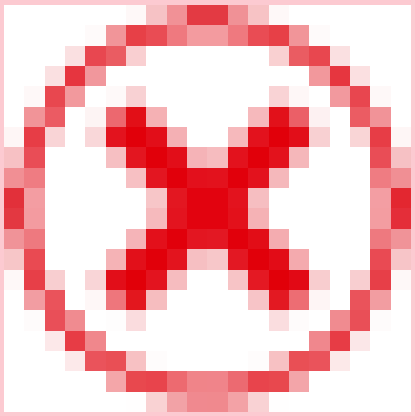
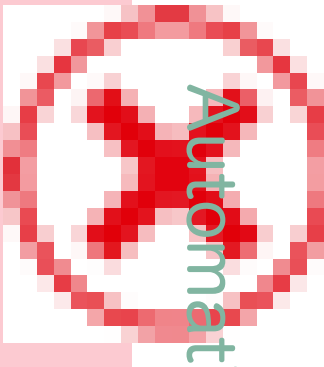
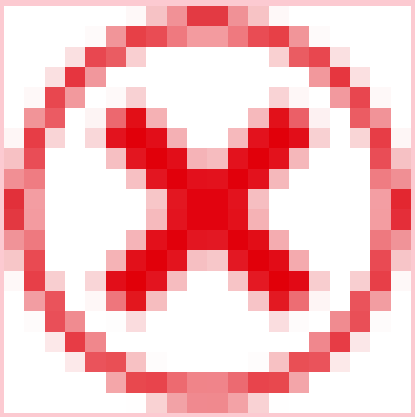
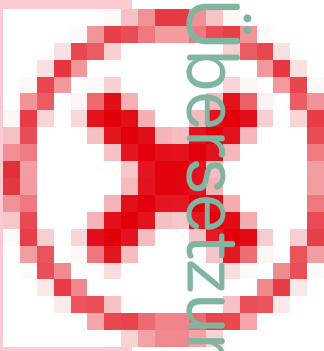
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Erkannte Container-Images				
WatchDog				
Konfiguration				

Automatische Übersetzung

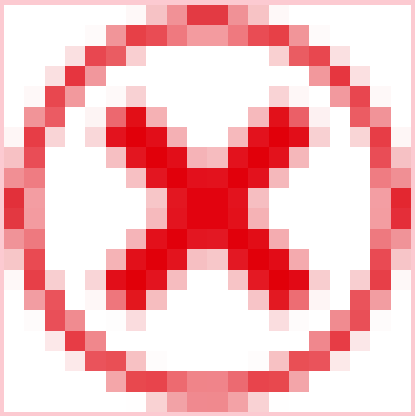
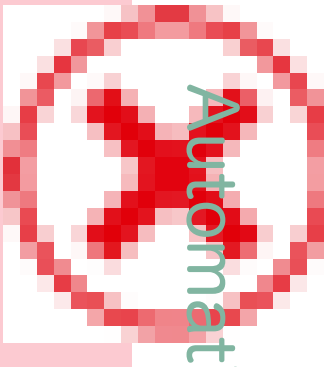
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informationen für andere Rollen:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

(Fortsetzung)

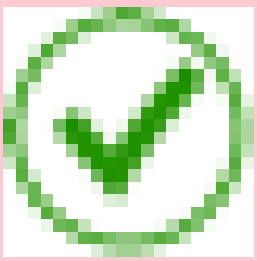
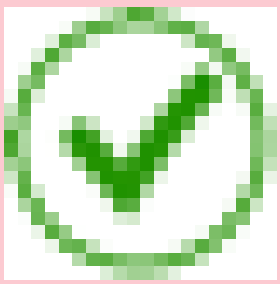
Modul	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_iter
Übersicht				

[End]

[store-future: BEGIN review]

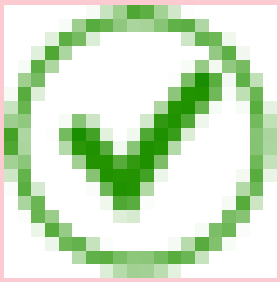
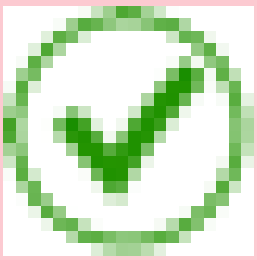
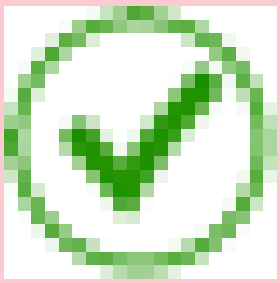
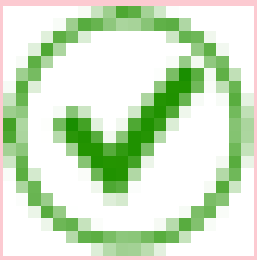
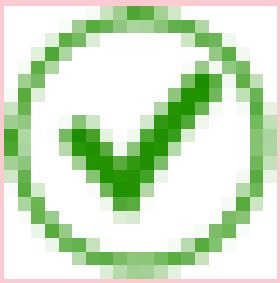
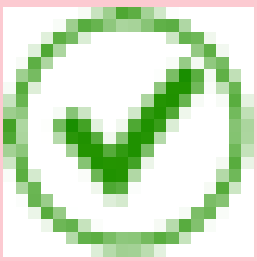
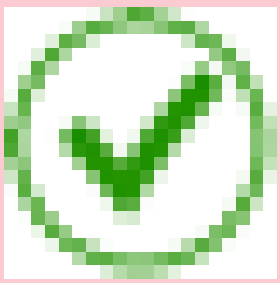
Modulzugriff nach Rolle für Splunk-Integration

Informationen zu Splunk Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_si.admin	sn_si.analyst
(Haupt-App-Gruppe)		
Splunk-Ereignisprofile		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst
Splunk-Feldübersetzungen		
Splunk-Ereignis für Aufgaben		
Splunk-Ereignisimport		
Splunk-Integrationseinstellungen		

[End]

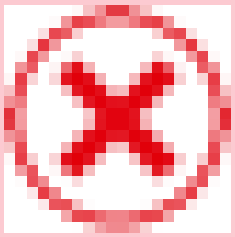
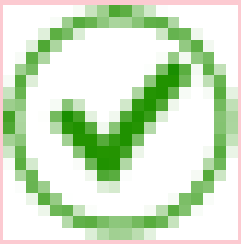
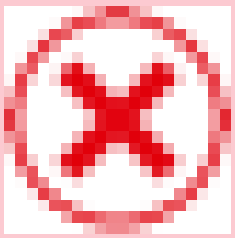
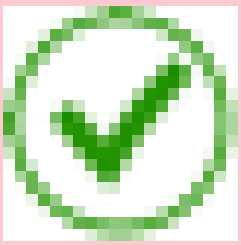
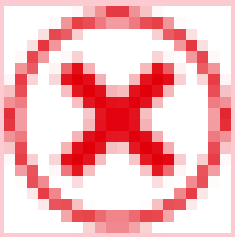
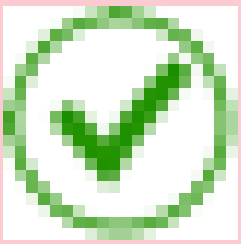
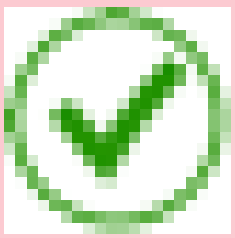
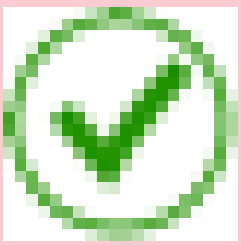
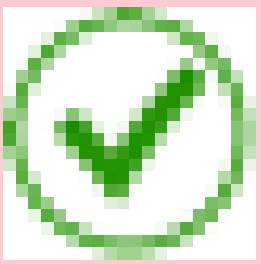
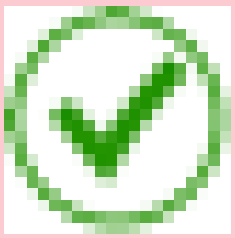
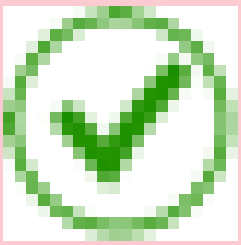
[store-future: BEGIN review]

Modulzugriff nach Rolle für Symantec DLP-Integration

Für Symantec DLP-Integration finden Sie die Menüelemente, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	agent_admin	sn_dlir.admin	sn_dlir.analyst
(Haupt-App-Gruppe)			

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	agent_admin	sn_dlir.admin	sn_dlir.analyst
Incident-Profil			
Incident-Statuszuordnung			
Einstellungen			
MID-Anwendung			
MID-Server			

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Threat Intelligence

Für Threat Intelligence sehen Sie sich die Menüelemente an, auf die eine bestimmte Rolle zugreifen kann.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
(Haupt-App-Gruppe)						

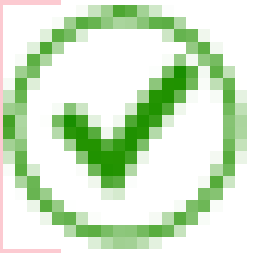
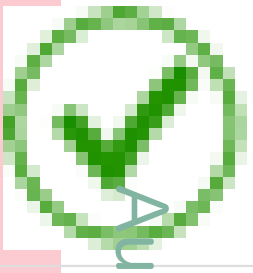
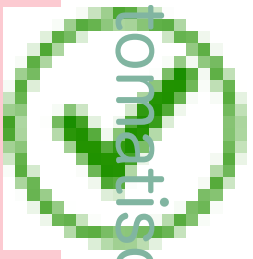
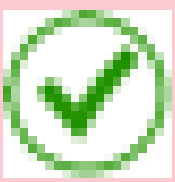
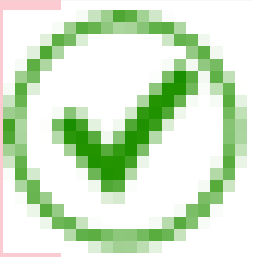
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Objekte	✗	✗	✗	✗	✗	✗
Objekte						
IoC-Repository						
AngriffsmodusMethoden	✓	✓	✓	✓	✓	✓
Indikatoren	✓	✓	✓	✓	✓	✓
Erkennbare Elemente	✓	✓	✓	✓	✓	✓
Angriffsmuster	✓	✓	✓	✓	✓	✓
Kampagnen	✓	✓	✓	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Vorgehensweisen						
Identitäten						
Infrastruktur						
Standorte						
Malware						
Angriffssatz						

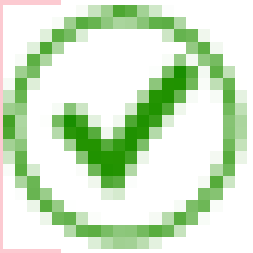
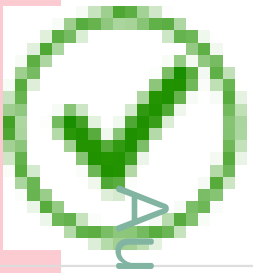
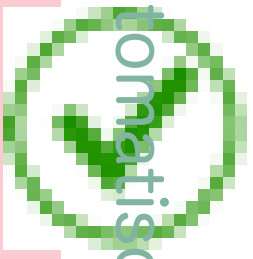
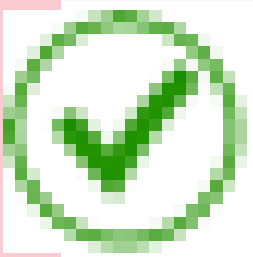
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Bedrohungsakteure	✓	✓	✓	✓	✓	✓
Malware-Analyse	✓	✓	✓	✓	✓	✓
Beobachtete Daten	✓	✓	✓	✓	✓	✓
Bedrohungsgruppierungen	✓	✓	✓	✓	✓	✓
Markierungsdefinitionen	✓	✓	✓	✓	✓	✓
Bedrohungshinweise	✓	✓	✓	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Bedrohungsmeinungen						
Bedrohungsberichte						
Indikatorsichtungen						
Objektsichtungen						
Schwachstellen						
Tools						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
ObjectObject-Beziehungen	✓	✓	✓	✓	✓	✓
ObjectIndicator-Beziehungen	✓	✓	✓	✓	✓	✓
Beziehungen erkennbarer Objekte	✓	✓	✓	✓	✓	✓
Quellen						
Bedrohungsquellen	✗	✗	✗	✗	✓	✗
TAXII-Profile	✗	✗	✗	✗	✓	✗
Externe Intelligenz						
Datenschutzverletzung – Bibliothek	✓	✓	✓	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
WHOIS-Bibliothek	✓	✓	✓	✓	✓	✓
Administration						
Eigenschaften	✗	✗	✗	✗	✓	✗
Angriffsmechanismen	✗	✗	✗	✗	✓	✗
Angriffsmotivationen	✗	✗	✗	✗	✓	✗
Discovery-Methoden	✗	✗	✗	✗	✓	✗
Feeds	✗	✗	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Indikatortypen	✗	✗	✗	✗	✓	✗
Infrastrukturtypen	✗	✗	✗	✗	✓	✗
Beabsichtigte Wirkungen	✗	✗	✗	✗	✓	✗
Malware-Fähigkeiten	✗	✗	✗	✗	✓	✗
Schadsoftwaretypen	✗	✗	✗	✗	✓	✗
Benachrichtigungen	✗	✗	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Erkennbare Typen	✗	✗	✗	✗	✓	✗
Quotengrenzdefinitionen	✗	✗	✗	✗	✓	✗
Berichtstypen	✗	✗	✗	✗	✓	✗
Bedrohungsakteurrollen	✗	✗	✗	✗	✓	✗
Bedrohungsakteurtypen	✗	✗	✗	✗	✓	✗
Tooltypen	✗	✗	✗	✗	✓	✗
Fallmanagement						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Alle Fälle	✗	✗	✗	✗	✗	✓
Offene Fälle	✗	✗	✗	✗	✗	✓
Meine Fälle	✗	✗	✗	✗	✗	✓
MITRE ATT&CK-Repository						
Übersicht	✓	✓	✓	✓	✓	✓
Matrizen	✓	✓	✓	✓	✓	✓
Techniken	✓	✓	✓	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Mitigationen	✓	✓	✓	✓	✓	✓
Gruppen	✓	✓	✓	✓	✓	✓
Malware	✓	✓	✓	✓	✓	✓
Tools	✓	✓	✓	✓	✓	✓
MITRE-Beziehungen	✓	✓	✓	✓	✓	✓
Heatmap und Navigator	✓	✓	✓	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Zuordnung der CVE-Techniken	✓	✓	✓	✓	✓	✓
MITRE ATT&CK-Administration						
Datenquellenzuordnung	✓	✓	✓	✓	✓	✓
Datenkomponentenzuordnung	✓	✓	✓	✓	✓	✓
Definition der Erkennungsabdeckung	✓	✓	✓	✓	✓	✓
Zuordnung der Abdeckung durch Erkennung	✓	✓	✓	✓	✓	✓
Definition der Abdeckung durch Risikominderung	✓	✓	✓	✓	✓	✓

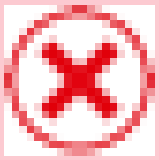
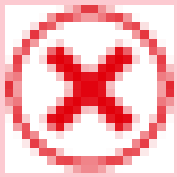
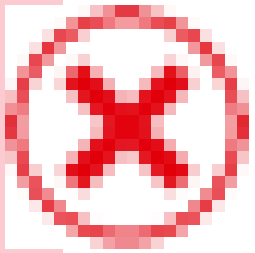
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Rechner für Abdeckung durch Risikominderung	✓	✓	✓	✓	✓	✓
Zuordnung der Abdeckung durch Risikominderung	✓	✓	✓	✓	✓	✓
Extraktionsregel für Technik	✓	✓	✓	✓	✓	✓
MITRE ATTCK-Zuordnung für Erkennungsregeln	✓	✓	✓	✓	✓	✓
Definition der Bedrohungsgruppentechnik-Heatmap	✓	✓	✓	✓	✓	✓
Bedrohungsgruppe – Zuordnung der MITRE ATTCK-Technik	✓	✓	✓	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read
Eigenschaften						

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Vulnerability Response

Informationen zu Vulnerability Response finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
(Haupt-App-Gruppe)				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
CISO-Dashboard	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Korrekturübersicht	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Arbeitsbereich des Schwachstellenmanagers	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Übersicht	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Arbeitsbereich für IT-Korrekturen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Genehmiger-Übersicht	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Übersicht	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Meine Genehmigungen	✗	✓	✗	
Korrekturaufgaben				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Aktiv	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Mir zugewiesen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Meinen Gruppen zugewiesen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Alle	✗	✓	✗	
Angreifbare Elemente				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Kritisches Risiko	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Hohes Risiko	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Nutzbar	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Ziel rückt näher	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Verfehltes Ziel	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Innerhalb der letzten 90 Tage	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Älter als 90 Tage	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Nicht zugewiesen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Nicht gruppiert	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Außer Betrieb genommen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Mehrere Zurückstellungen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Alle	✗	✓	✗	
Lösungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Alle	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Ersetzung mit höchster Priorität	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Mit angreifbaren Elementen	✗	✓	✗	
Bibliotheken				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
NVD	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
CWE	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Drittpartei	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

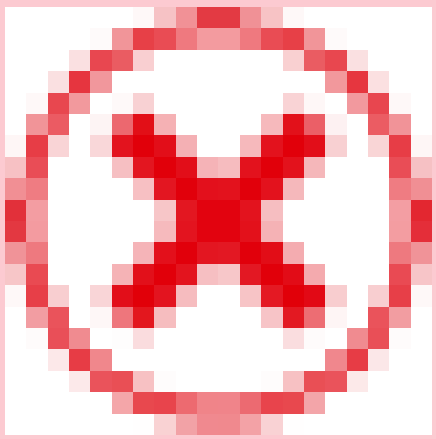
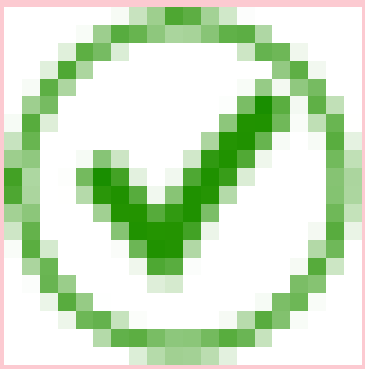
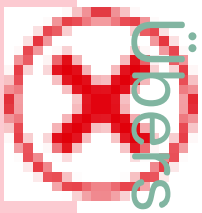
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Software mit Schwachstellen				
Schwachstellenscan				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Bewertung des Gefahrenpotenzials	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Scans	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Scanner	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Scan-Warteschlange	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Scannerquotengrenzen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Quotengrenzdefinitionen	✗	✓	✗	
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Setup-Assistent	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Überwachungsthemen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Zuweisungsregeln	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Regeln für Korrekturaufgaben	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Zuweisungsempfehlungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Schwachstellen-Rechner	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Rechner für Schwachstellen-Rollup	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Korrekturzielregeln	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Konfiguration für automatisches Schließen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Regeln für automatische Löschung	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Ausnahmeregeln	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Genehmigungsregeln	✓	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Klassifizierungsregeln	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Leistungskonfiguration	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
VI-Granularität konfigurieren	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Benachrichtigungen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
E-Mail-Vorlagen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Warteschlange importieren	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Integrationen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
SLA-Definitionen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
SAM-NVD konfigurieren	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Normalisierte Schweregradzuordnungen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Konfiguration der Scan-Abdeckung	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Ausnahmenverwaltung	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Verwendungsbericht	✗	✗	✗	
Diagnose				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_v
Überprüfungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
(Haupt-App-Gruppe)			
CISO-Dashboard	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Korrekturübersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Genehmiger-Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Meine Genehmigungen	✗	✗	✗
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Aktiv	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Mir zugewiesen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Meinen Gruppen zugewiesen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Alle			

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Kritisches Risiko	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Hohes Risiko	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Nutzbar	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Innerhalb der letzten 90 Tage	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Älter als 90 Tage	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Nicht zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Nicht gruppiert	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Außer Betrieb genommen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Mehrere Zurückstellungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Alle			

Lösungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Alle			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Ersetzung mit höchster Priorität			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Mit angreifbaren Elementen	✗	✗	✗
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
NVD	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
CWE			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Drittpartei	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Software mit Schwachstellen	✗	✗	✗
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Bewertung des Gefahrenpotenzials	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Scans	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Scanner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Scan-Warteschlange	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Scannerquotengrenzen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Überwachungsthemen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Regeln für Korrekturaufgaben	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Zuweisungsempfehlungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Schwachstellen-Rechner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Rechner für Schwachstellen-Rollup			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Korrekturzielregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Konfiguration für automatisches Schließen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Regeln für automatische Löschung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Ausnahmeregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Genehmigungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Klassifizierungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Leistungskonfiguration	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
VI-Granularität konfigurieren	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Benachrichtigungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
E-Mail-Vorlagen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Warteschlange importieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Integrationen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
SAM-NVD konfigurieren	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Normalisierte Schweregradzuordnungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Konfiguration der Scan-Abdeckung	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Ausnahmenverwaltung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Verwendungsbericht	✗	✗	✗
Diagnose			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_v
Überprüfungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
(Haupt-App-Gruppe)			
CISO-Dashboard	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Korrekturübersicht	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

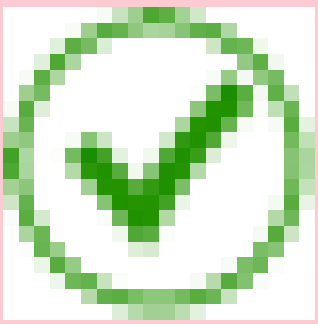
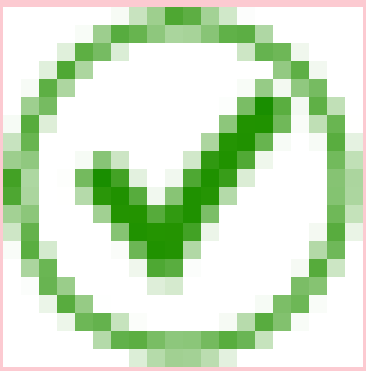
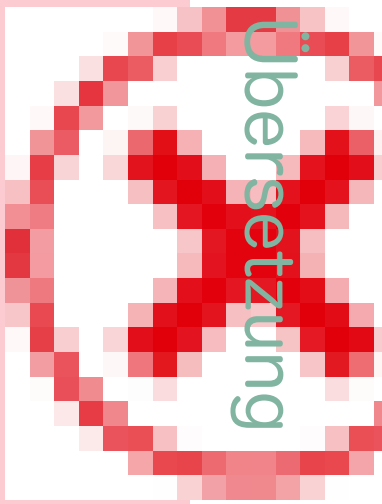
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Genehmiger-Übersicht	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

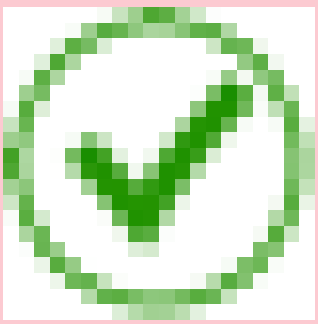
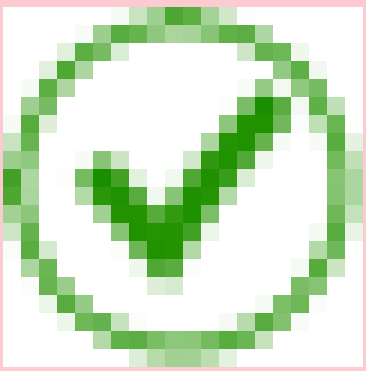
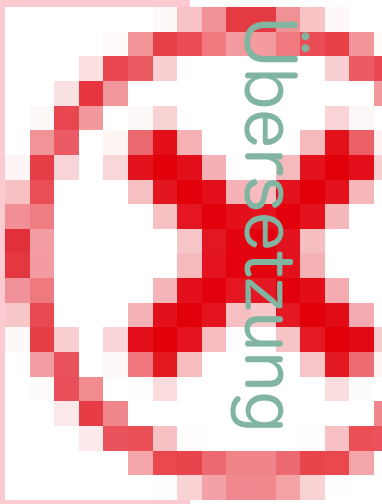
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Meine Genehmigungen	✓	✓	✗
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Aktiv	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Mir zugewiesen	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

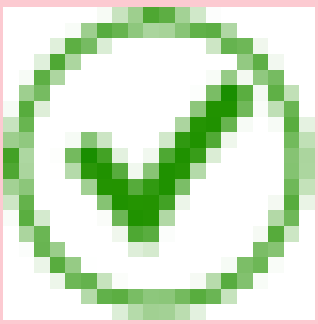
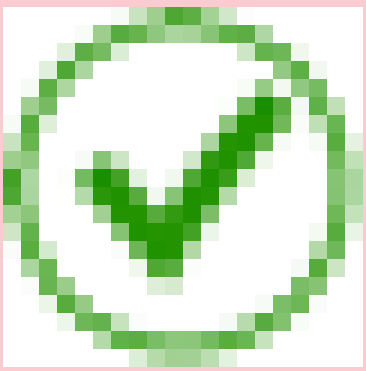
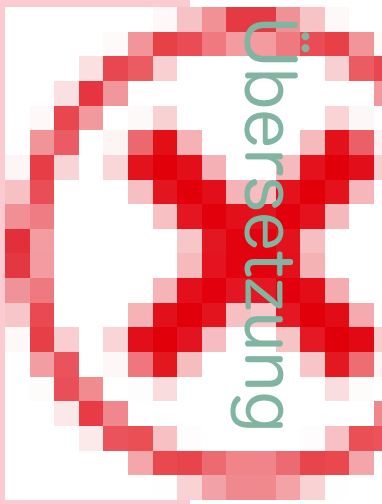
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Meinen Gruppen zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Alle	✓	✓	✗

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Kritisches Risiko	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Hohes Risiko	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Nutzbar	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

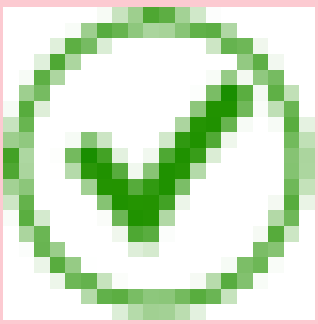
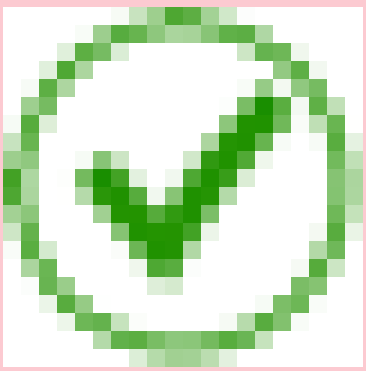
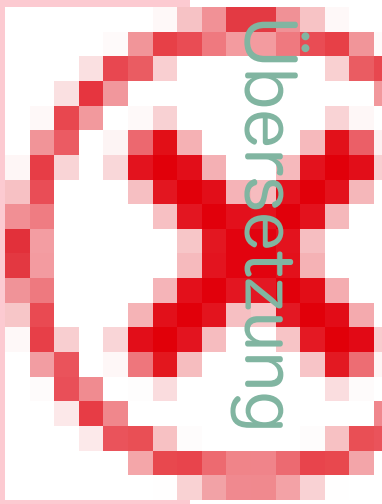
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Verfehltes Ziel	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Innerhalb der letzten 90 Tage	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Älter als 90 Tage	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

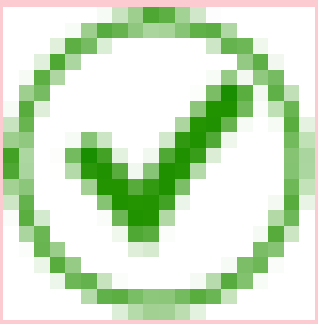
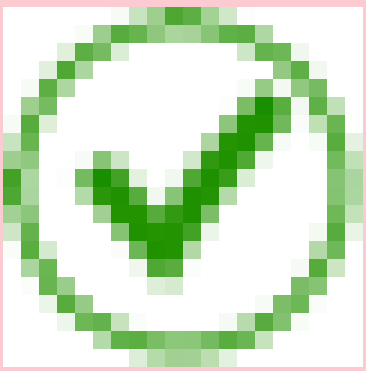
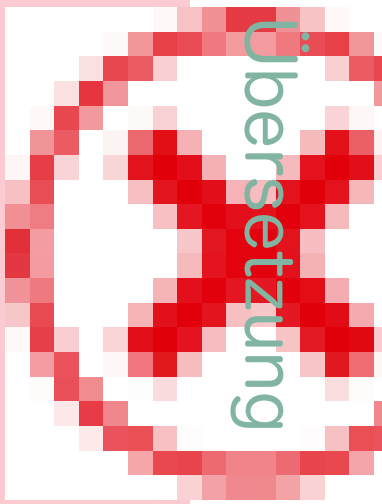
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Nicht zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Nicht gruppiert	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Außer Betrieb genommen	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Mehrere Zurückstellungen	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Alle	✓	✓	✗
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

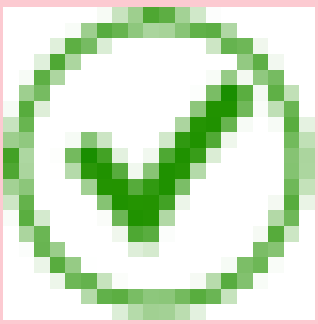
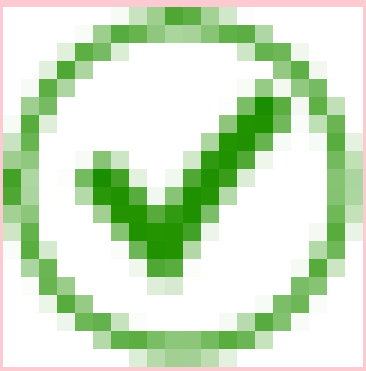
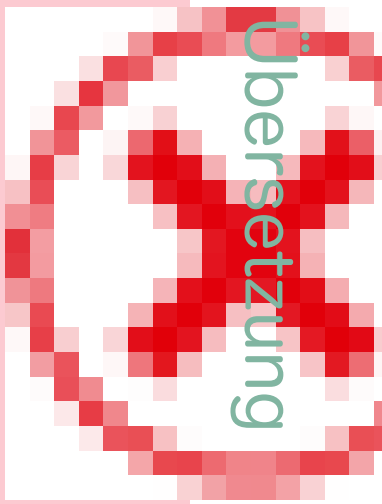
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Alle			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Ersetzung mit höchster Priorität	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Mit angreifbaren Elementen	✓	✓	✗
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
NVD	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
CWE	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Drittpartei	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Software mit Schwachstellen	✓	✓	✗
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Bewertung des Gefahrenpotenzials	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Scans	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

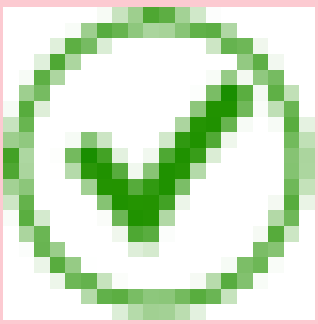
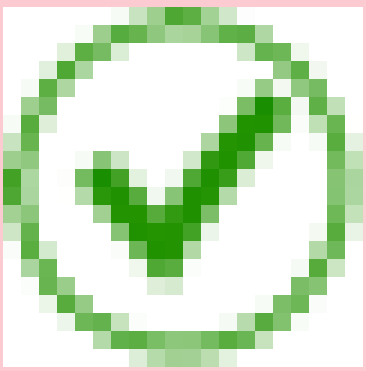
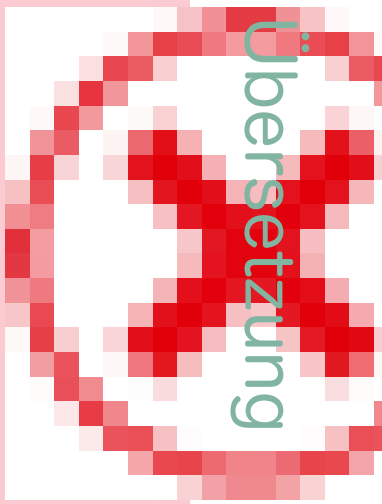
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Scanner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Scan-Warteschlange	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Scannerquotengrenzen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

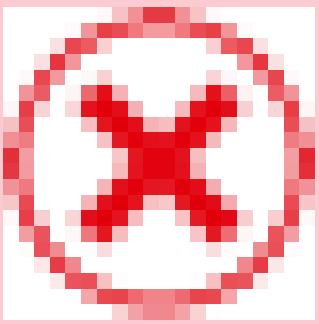
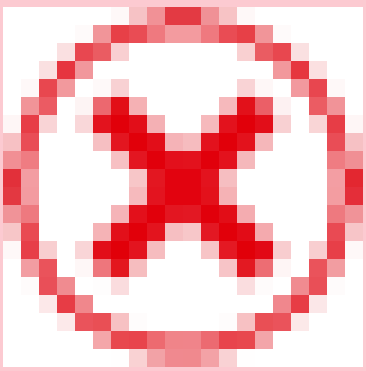
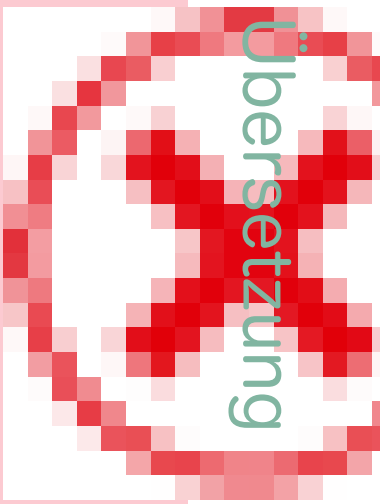
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Überwachungsthemen	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

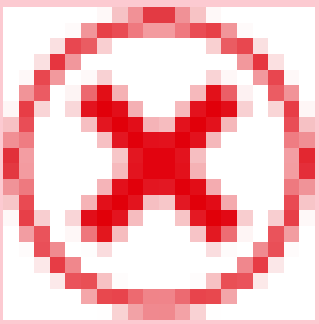
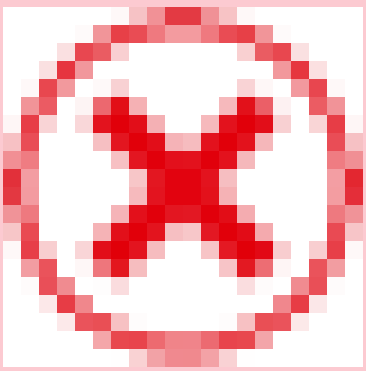
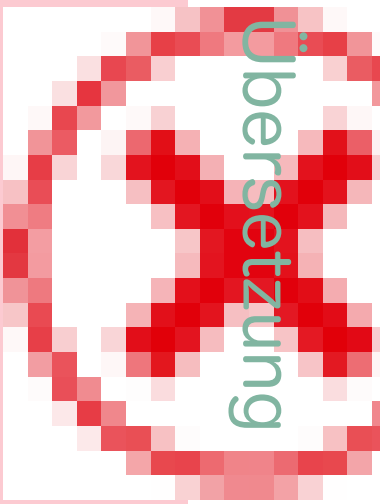
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Regeln für Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Zuweisungsempfehlungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Schwachstellen-Rechner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Rechner für Schwachstellen-Rollup	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Korrekturzielregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Konfiguration für automatisches Schließen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Regeln für automatische Löschung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Ausnahmeregeln	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Genehmigungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Klassifizierungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Leistungskonfiguration	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
VI-Granularität konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Benachrichtigungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
E-Mail-Vorlagen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Warteschlange importieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
SAM-NVD konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Normalisierte Schweregradzuordnungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Konfiguration der Scan-Abdeckung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Ausnahmenverwaltung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Verwendungsbericht	✗	✗	✗
Diagnose			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_reco
Überprüfungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
(Haupt-App-Gruppe)			
CISO-Dashboard	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificati
Korrekturübersicht	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Übersicht	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Genehmiger-Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Übersicht	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Meine Genehmigungen	✗	✗	✗
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Aktiv	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Mir zugewiesen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Meinen Gruppen zugewiesen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Alle	✗	✗	✓

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Kritisches Risiko	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Hohes Risiko	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Nutzbar	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Ziel rückt näher	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Verfehltes Ziel	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Innerhalb der letzten 90 Tage	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Älter als 90 Tage	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Nicht zugewiesen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Nicht gruppiert	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Außer Betrieb genommen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Mehrere Zurückstellungen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Alle	✗	✗	✓
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Alle	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Ersetzung mit höchster Priorität	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Mit angreifbaren Elementen	✗	✗	✓
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
NVD	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

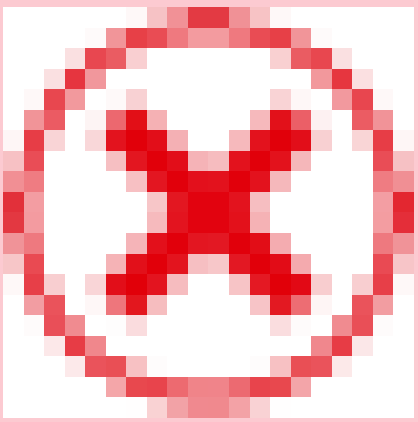
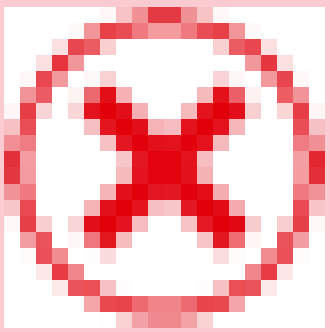
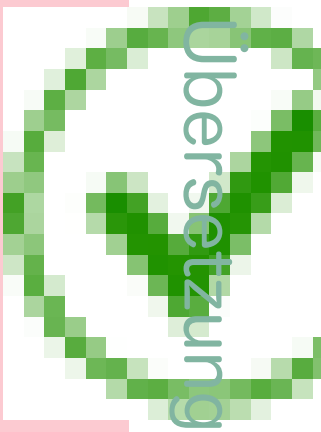
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
CWE			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Drittpartei	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Software mit Schwachstellen	✗	✗	✓
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Bewertung des Gefahrenpotenzials	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Scans	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Scanner	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Scan-Warteschlange	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Scannerquotengrenzen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Quotengrenzdefinitionen	✗	✗	✗
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Überwachungsthemen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Regeln für Korrekturaufgaben	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Zuweisungsempfehlungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Schwachstellen-Rechner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Rechner für Schwachstellen-Rollup	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Korrekturzielregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Konfiguration für automatisches Schließen	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Regeln für automatische Löschung	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Ausnahmeregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Genehmigungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Klassifizierungsregeln	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Leistungskonfiguration	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
VI-Granularität konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Benachrichtigungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
E-Mail-Vorlagen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Warteschlange importieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
SAM-NVD konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

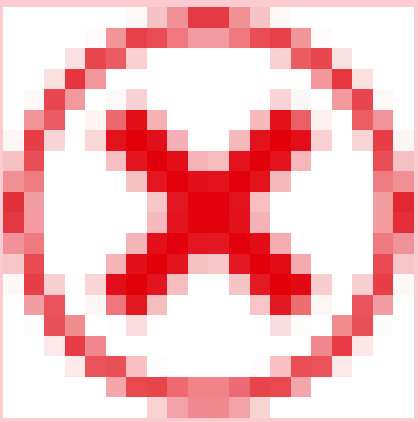
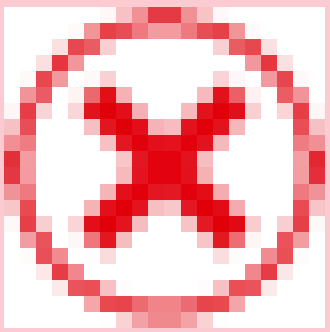
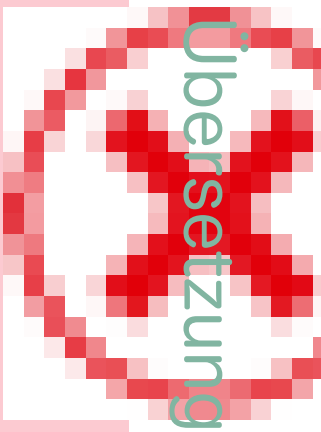
sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Konfiguration der Scan-Abdeckung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Ausnahmenverwaltung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Verwendungsbericht	✗	✗	✗
Diagnose			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classificatio
Überprüfungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notificat
(Haupt-App-Gruppe)			
CISO-Dashboard	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

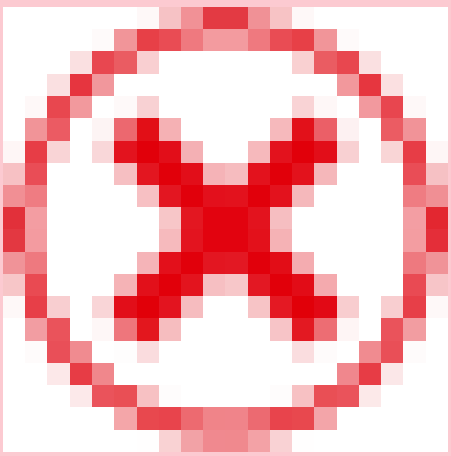
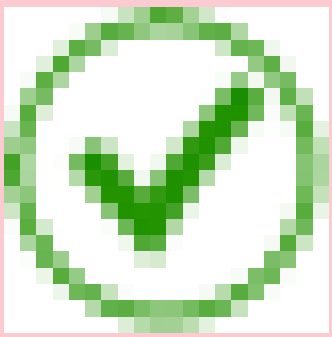
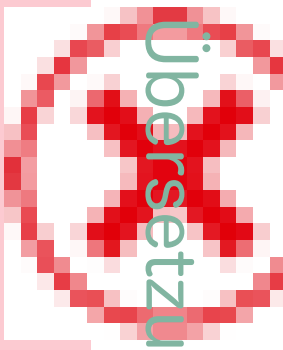
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Korrekturübersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

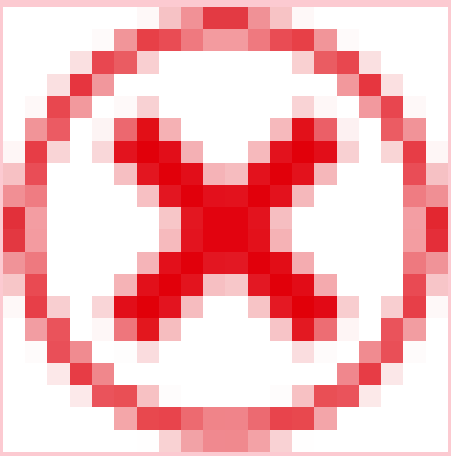
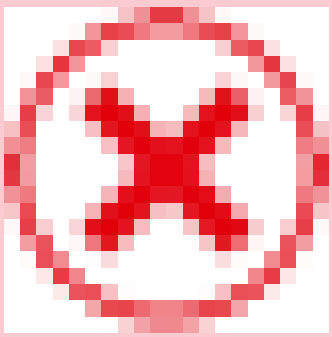
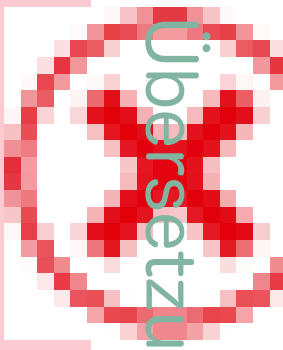
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Arbeitsbereich des Schwachstellenmanagers			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

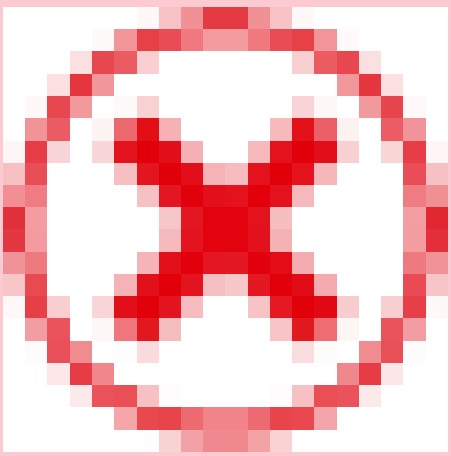
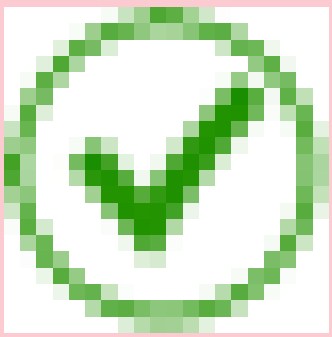
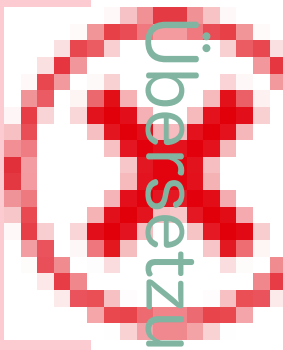
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

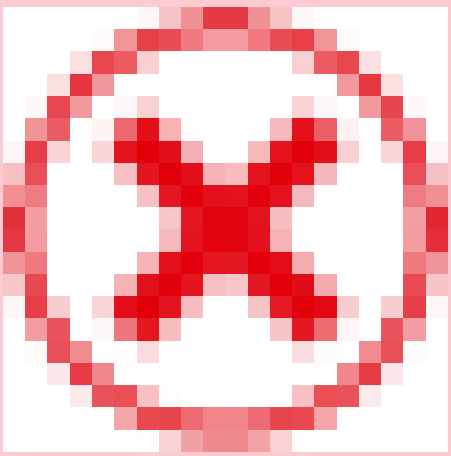
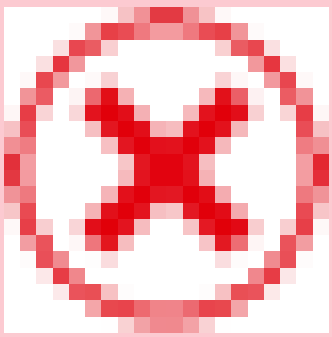
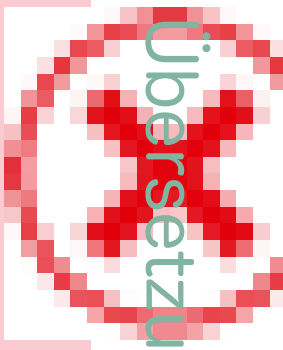
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Arbeitsbereich für IT-Korrekturen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

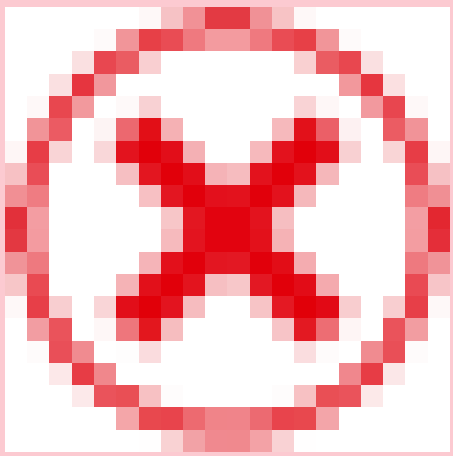
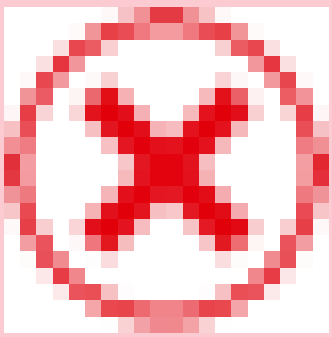
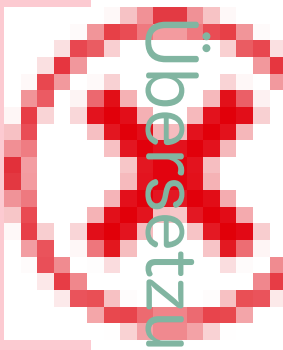
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Genehmiger-Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

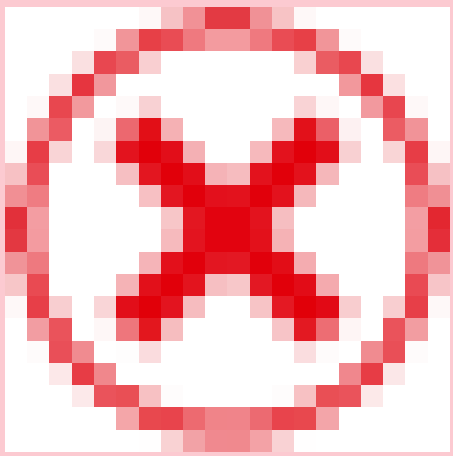
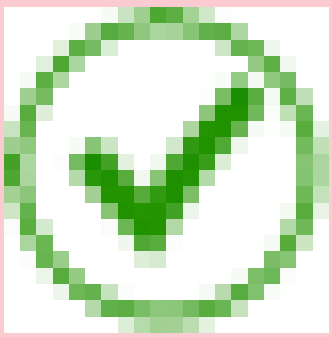
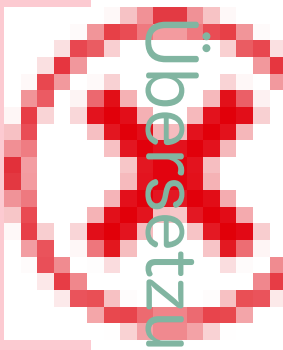
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

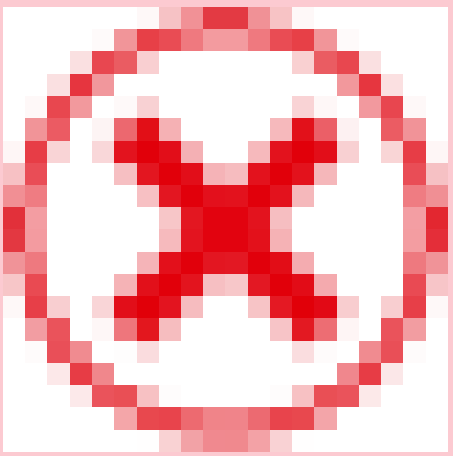
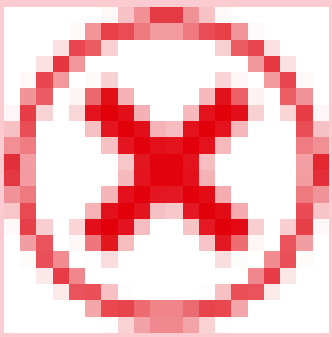
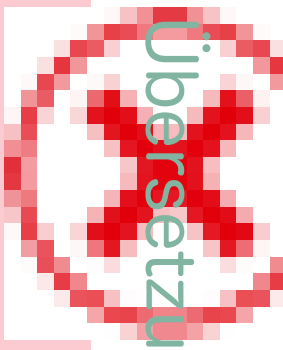
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Meine Genehmigungen			
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

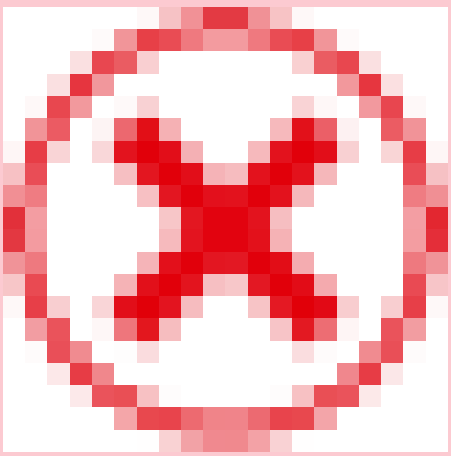
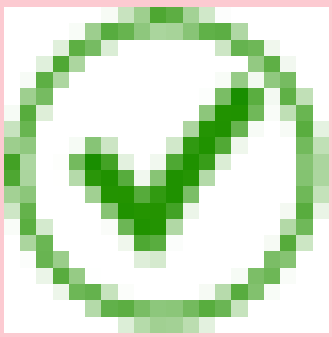
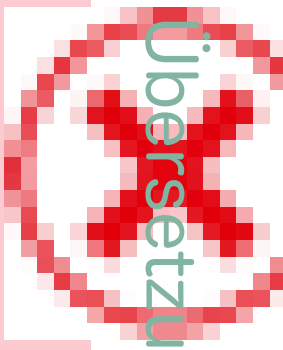
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Aktiv			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

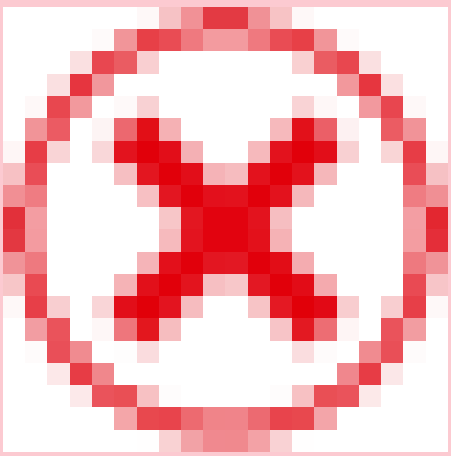
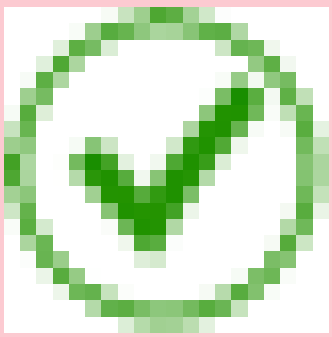
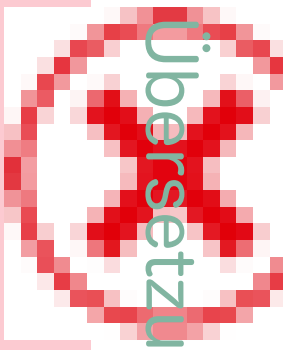
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Mir zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Meinen Gruppen zugewiesen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

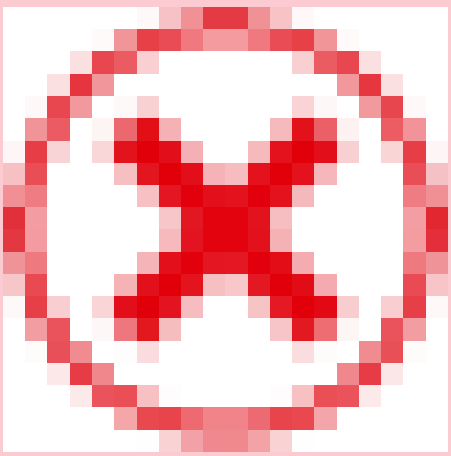
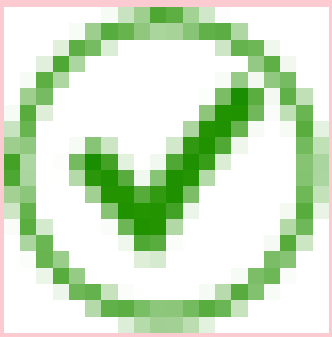
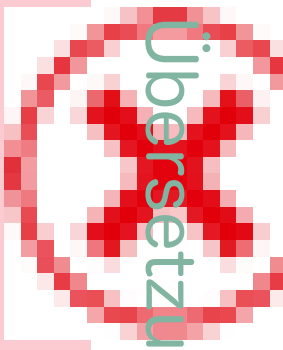
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Alle			

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

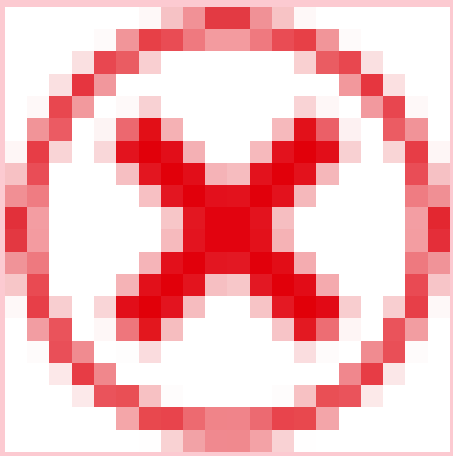
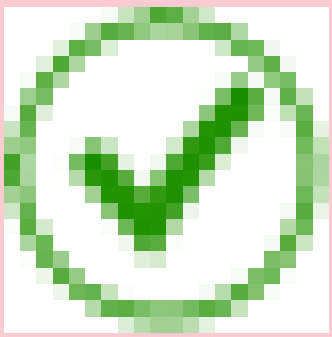
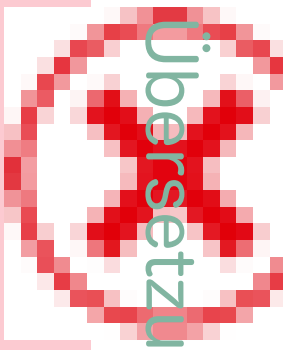
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Kritisches Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

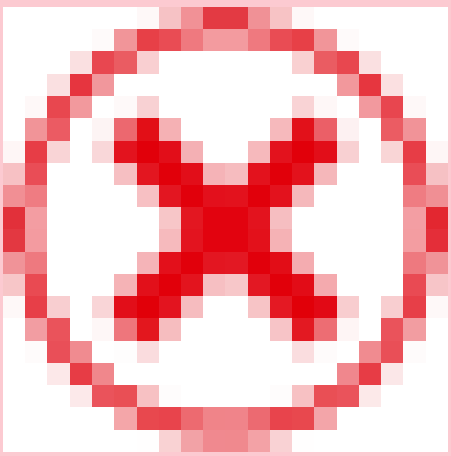
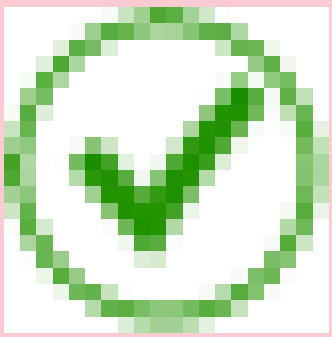
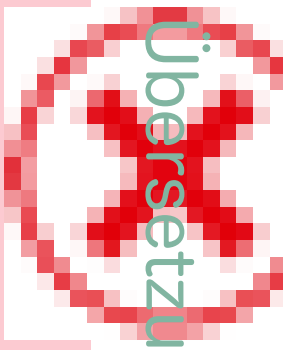
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Hohes Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

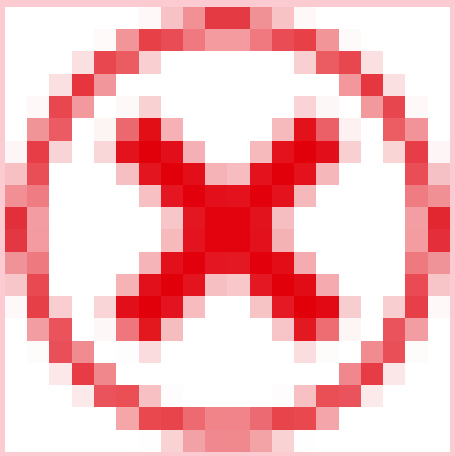
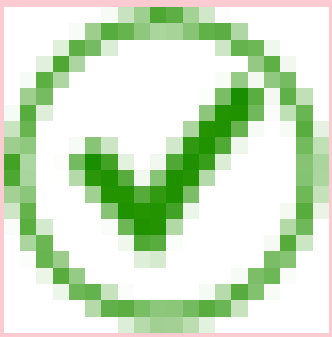
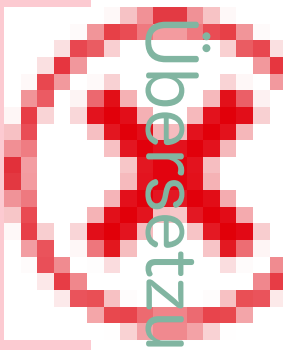
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Nutzbar			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

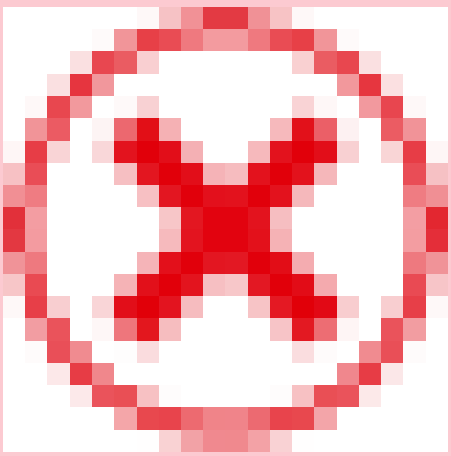
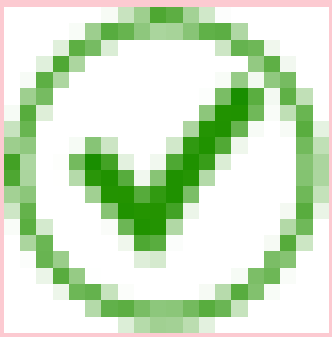
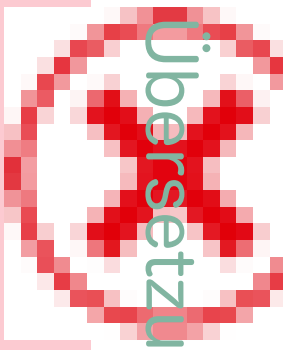
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

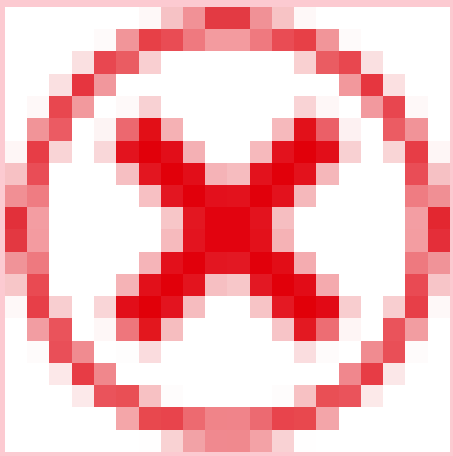
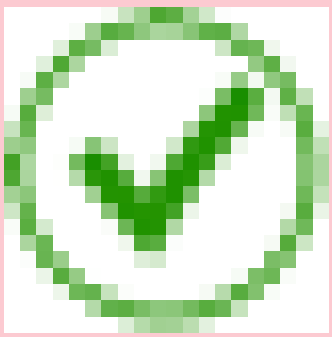
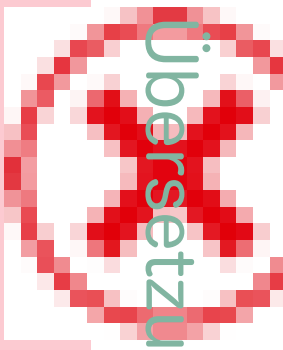
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

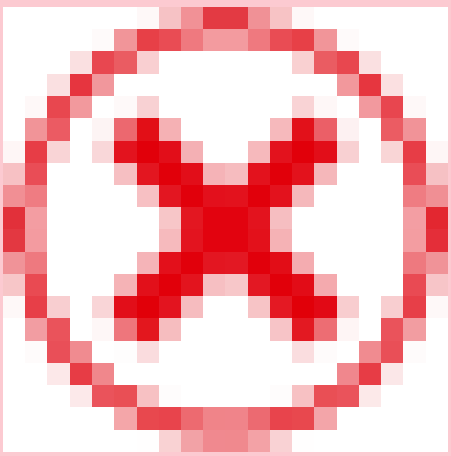
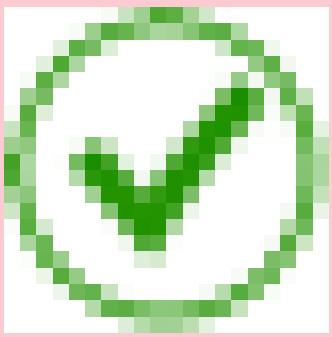
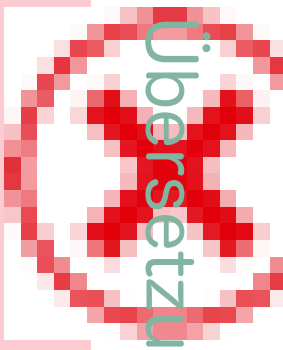
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Innerhalb der letzten 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

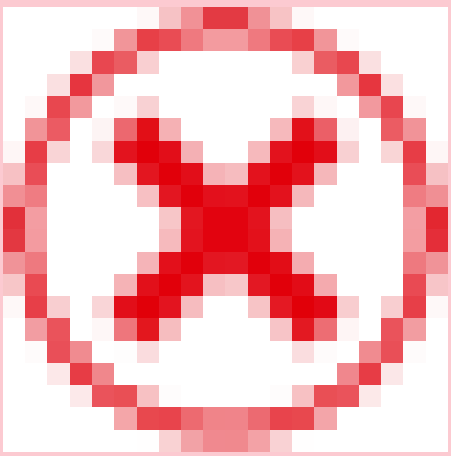
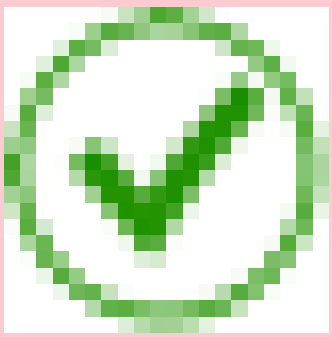
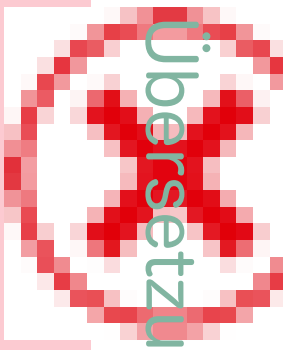
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Älter als 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

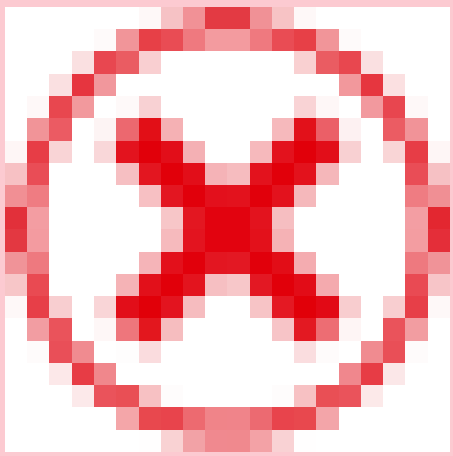
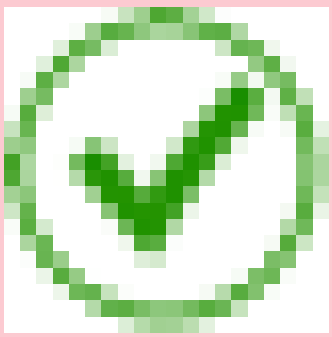
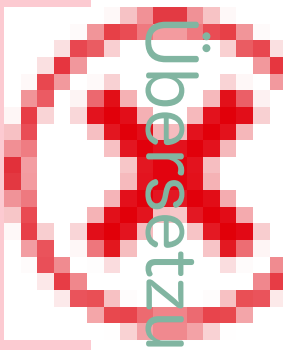
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Nicht zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

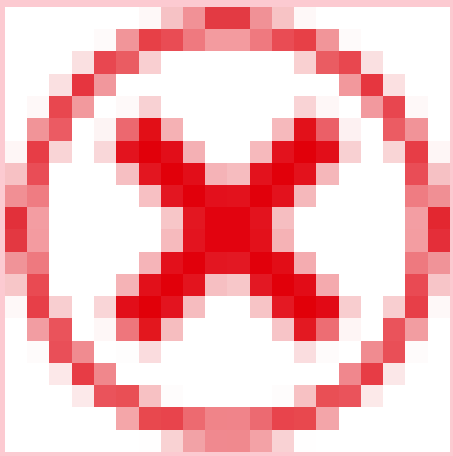
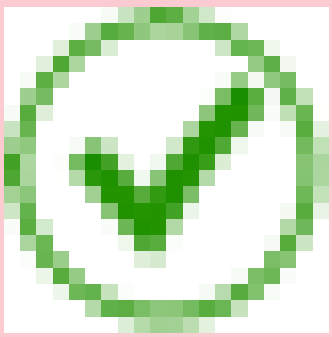
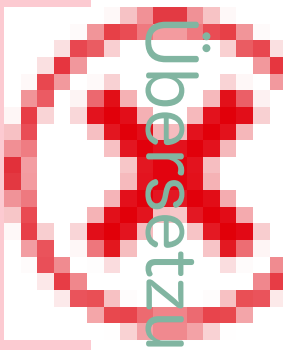
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Nicht gruppiert			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

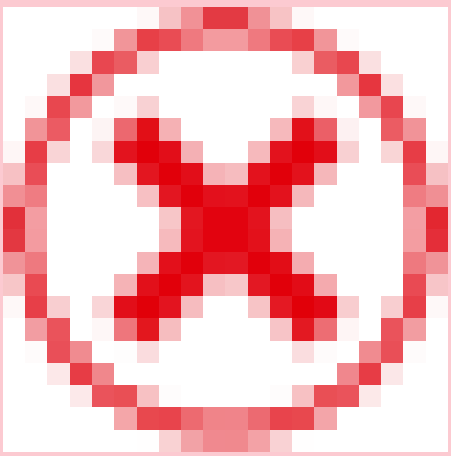
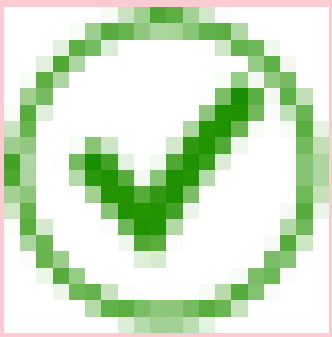
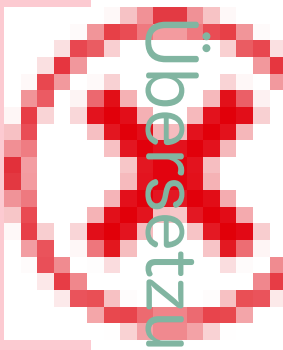
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Außer Betrieb genommen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Mehrere Zurückstellungen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

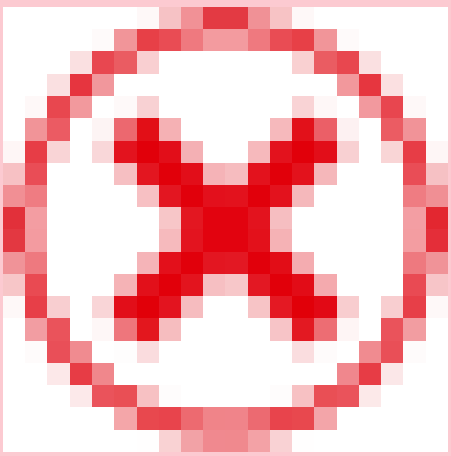
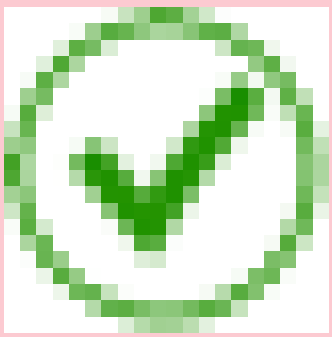
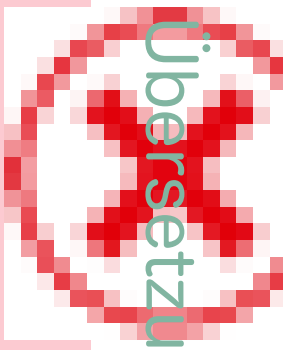
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Alle			
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

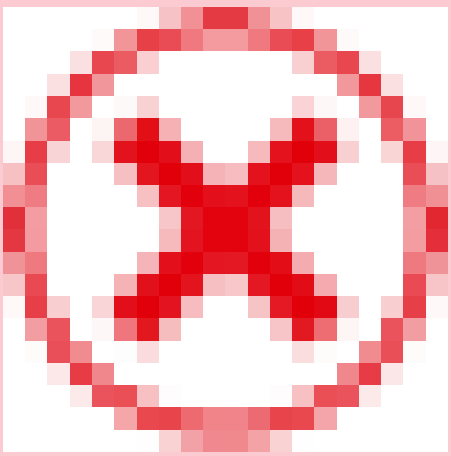
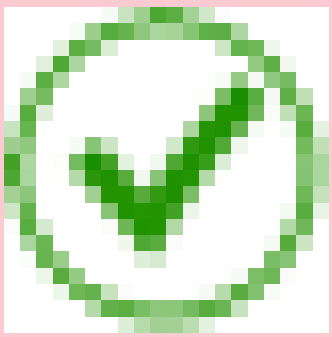
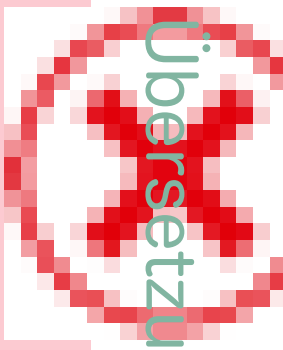
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Alle			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

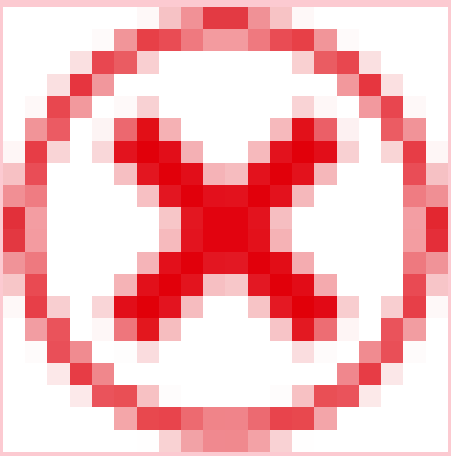
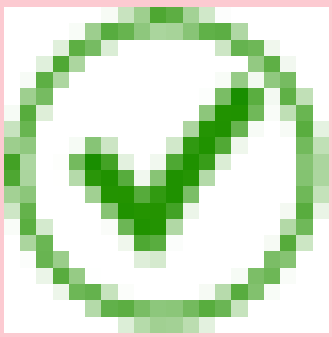
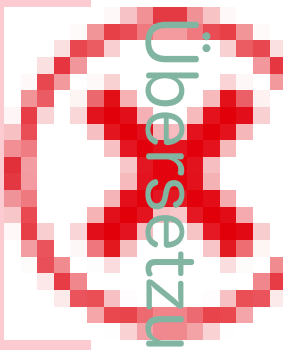
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Ersetzung mit höchster Priorität			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

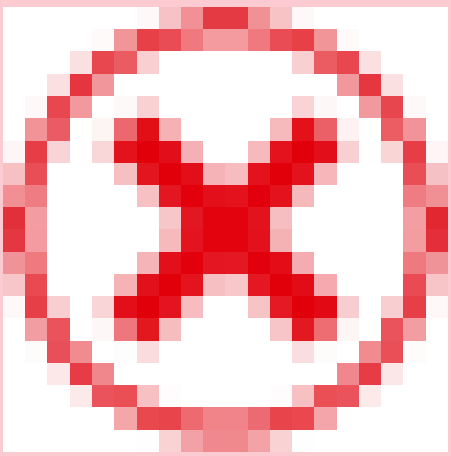
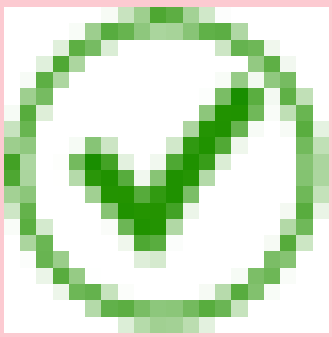
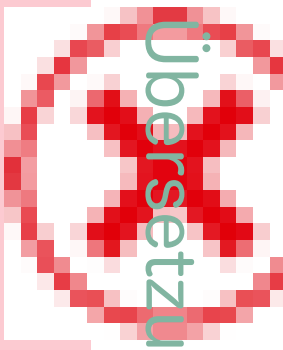
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Mit angreifbaren Elementen			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

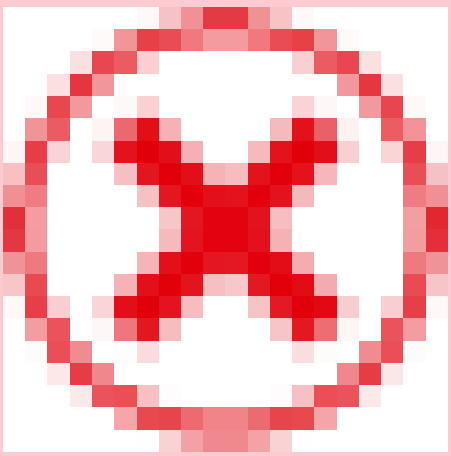
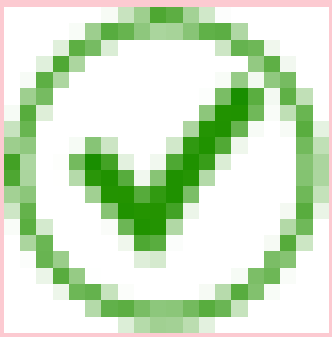
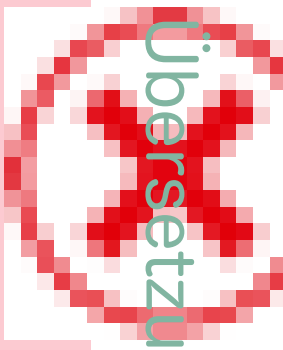
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
NVD			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

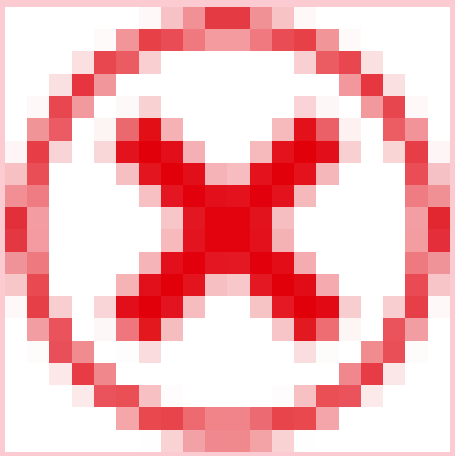
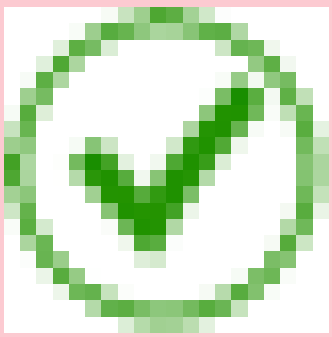
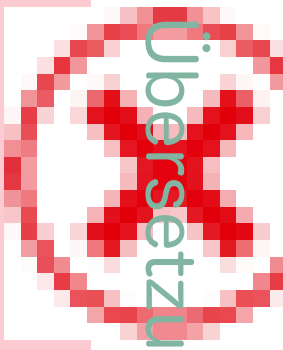
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
CWE			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

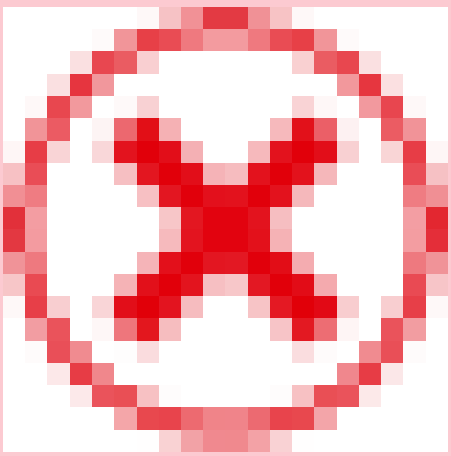
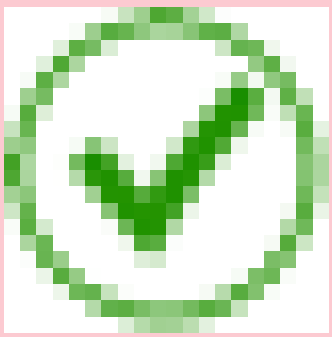
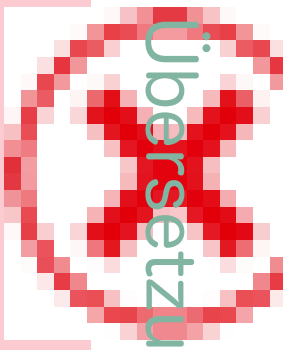
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Drittpartei			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

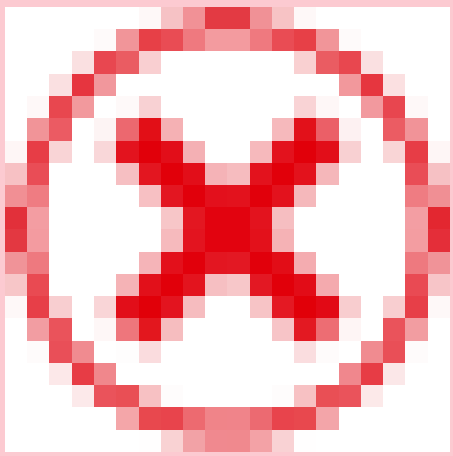
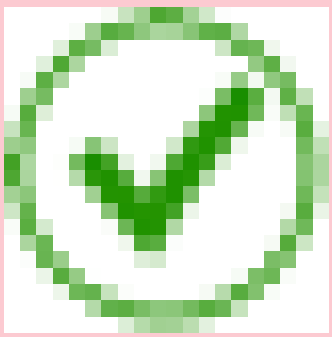
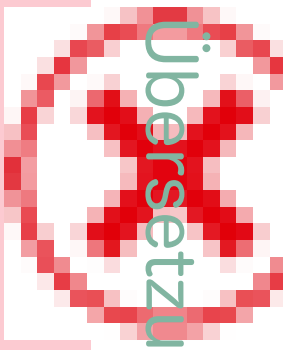
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Software mit Schwachstellen			
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

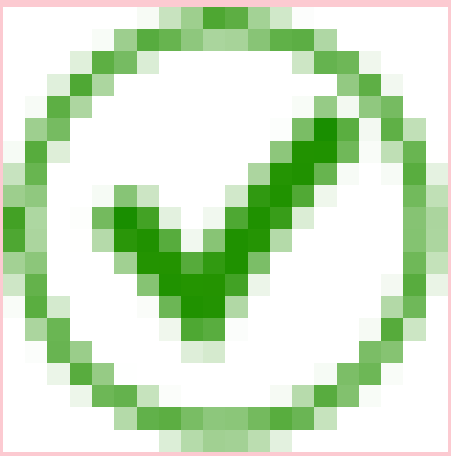
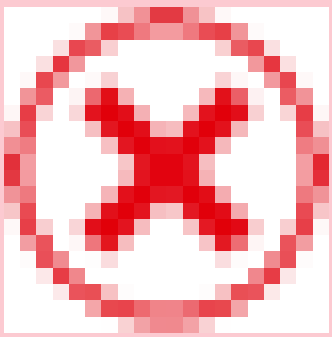
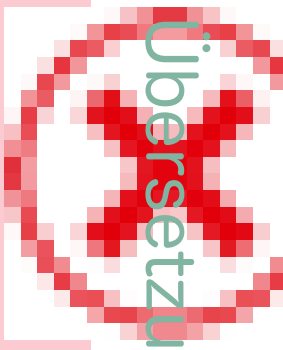
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Bewertung des Gefahrenpotenzials			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

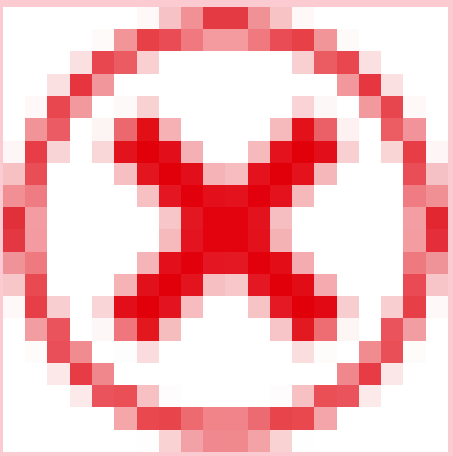
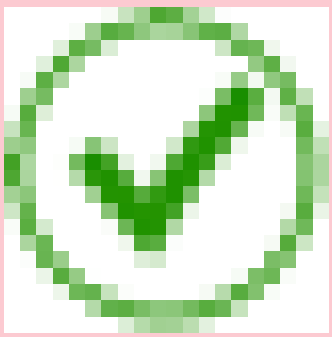
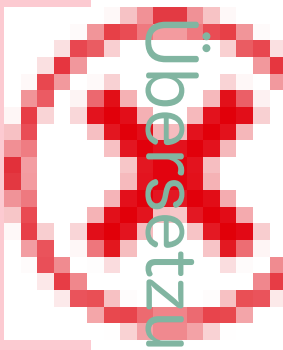
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Scans			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

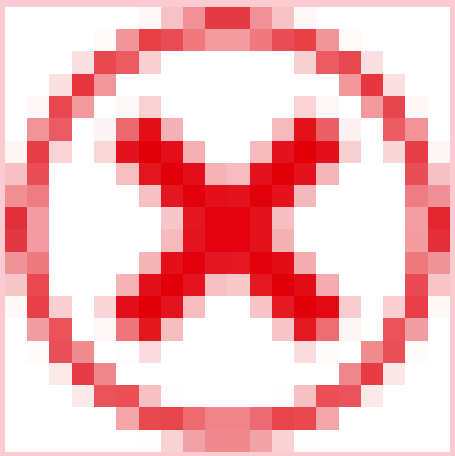
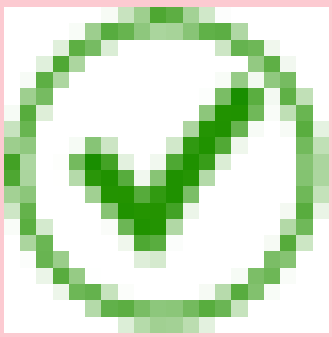
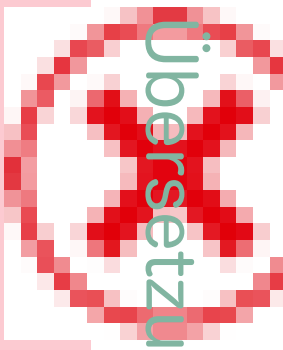
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Scanner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

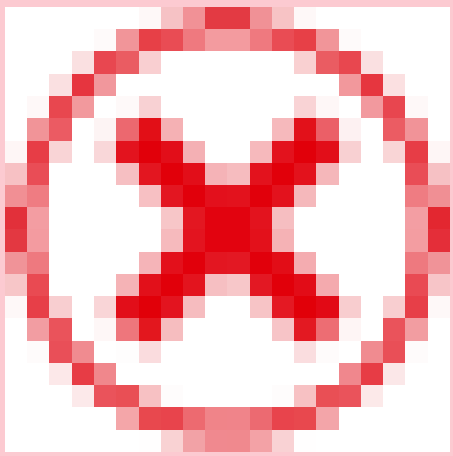
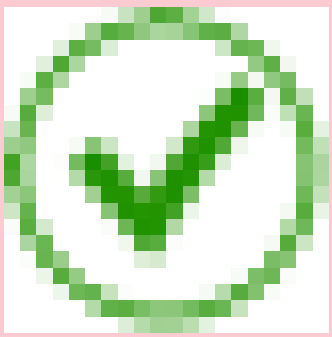
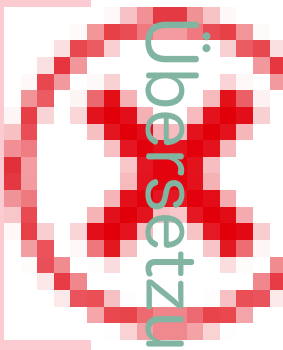
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Scan-Warteschlange			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

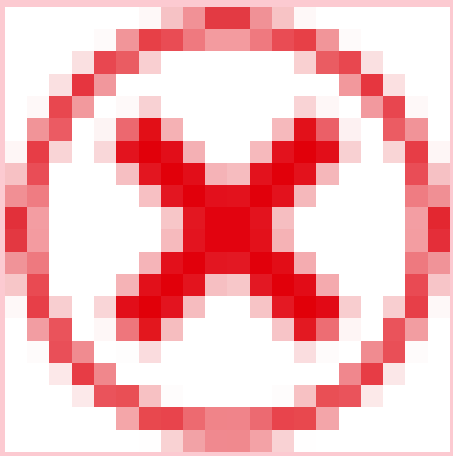
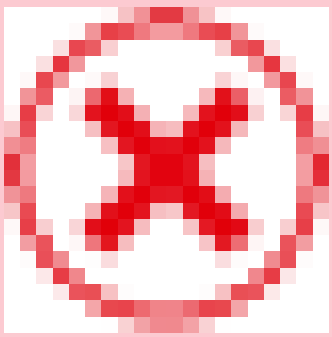
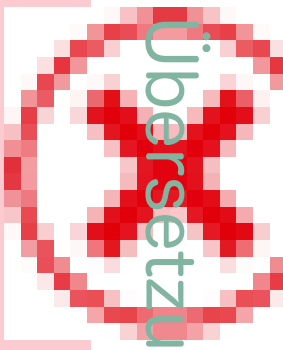
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Scannerquotengrenzen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

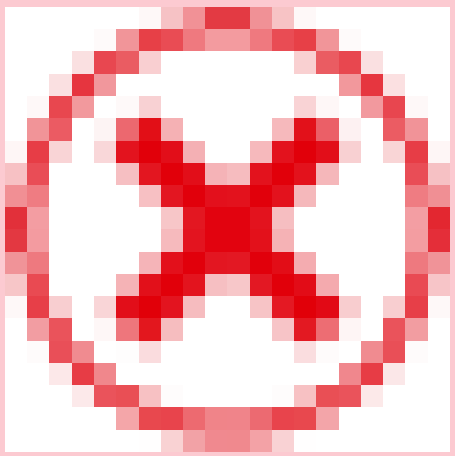
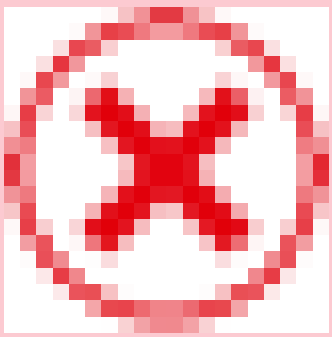
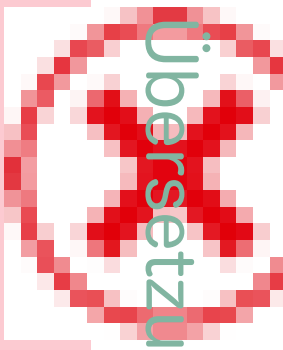
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

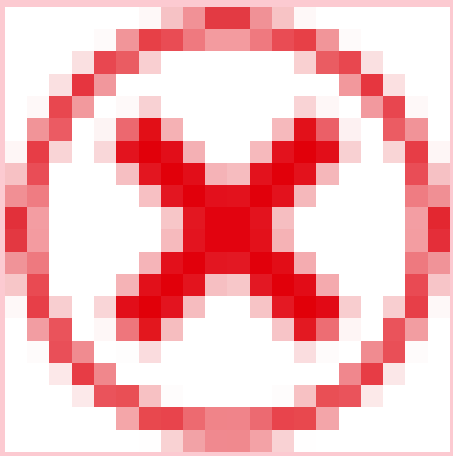
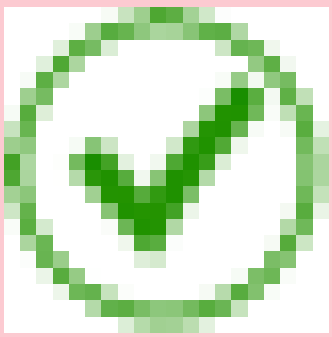
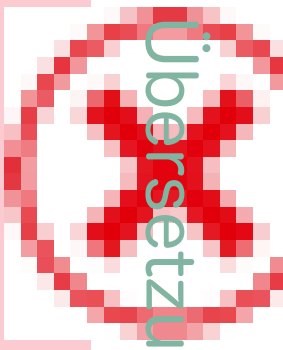
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Überwachungsthemen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

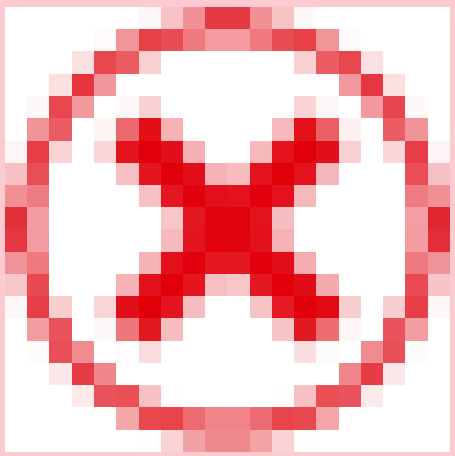
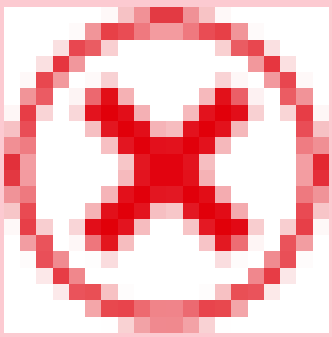
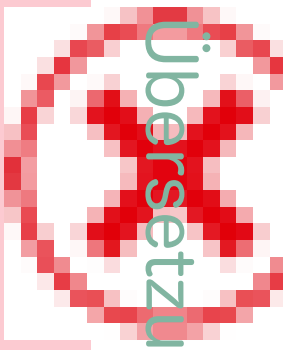
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Zuweisungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

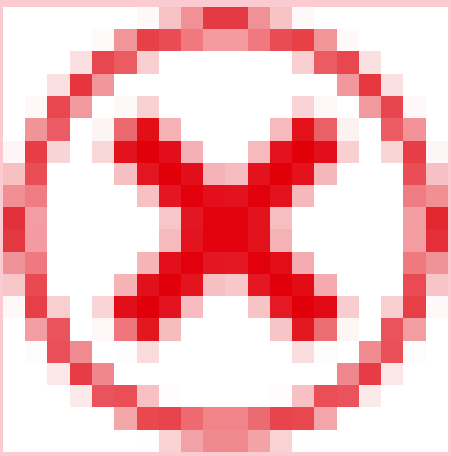
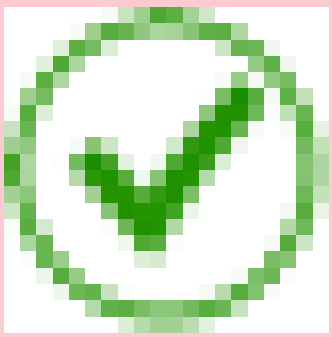
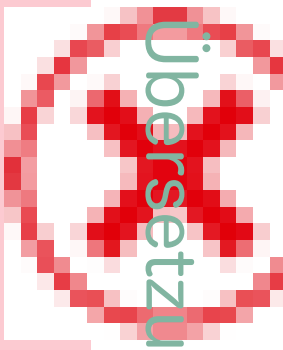
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Regeln für Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

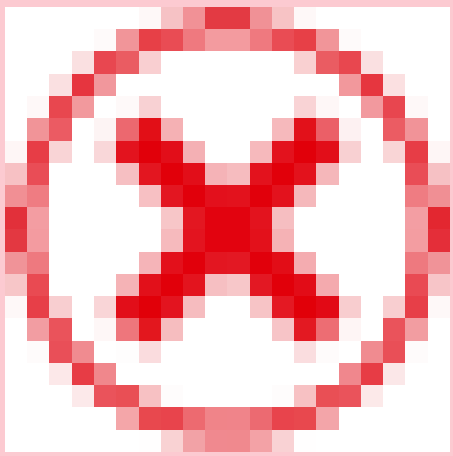
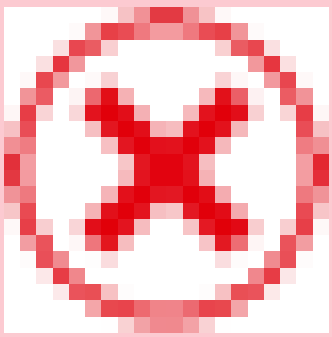
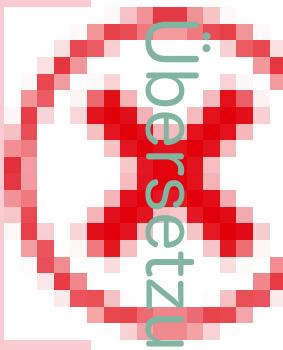
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Zuweisungsempfehlungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

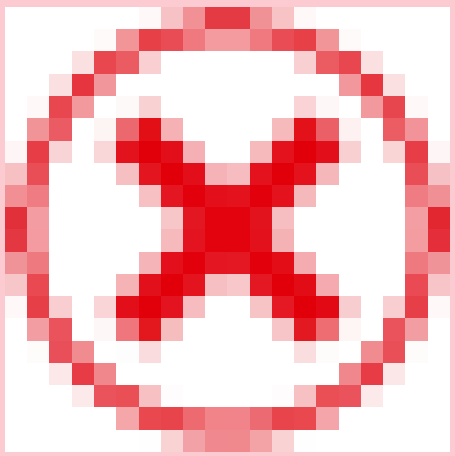
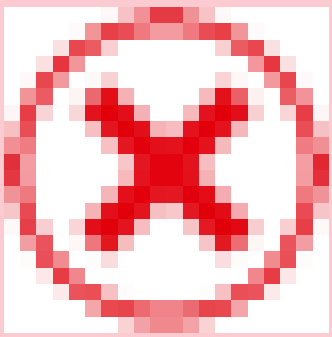
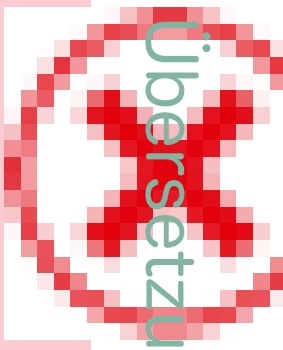
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Schwachstellen-Rechner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Rechner für Schwachstellen-Rollup	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

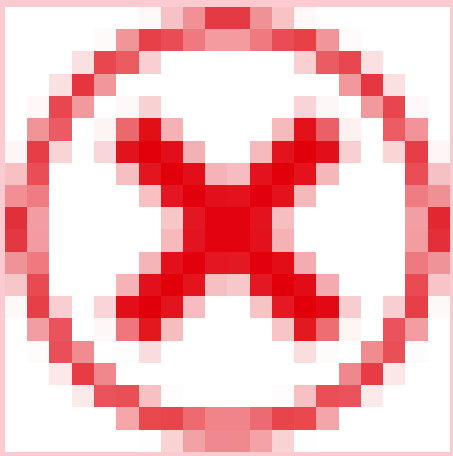
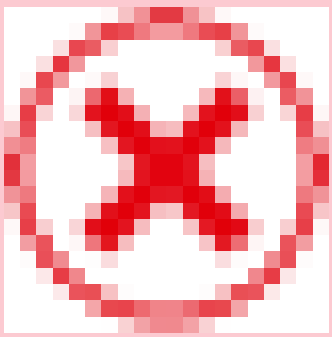
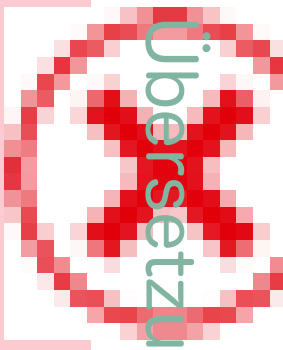
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Korrekturzielregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

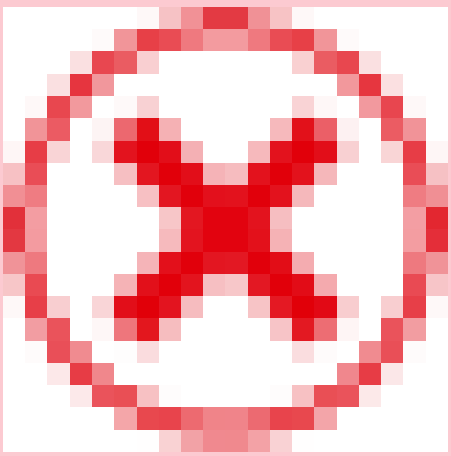
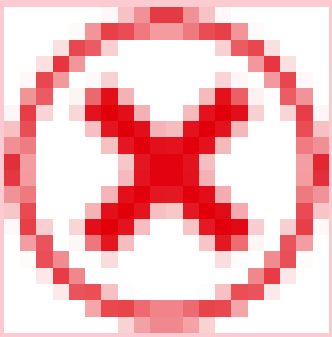
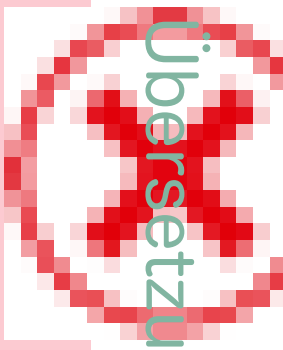
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Konfiguration für automatisches Schließen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Regeln für automatische Löschung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Ausnahmeregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

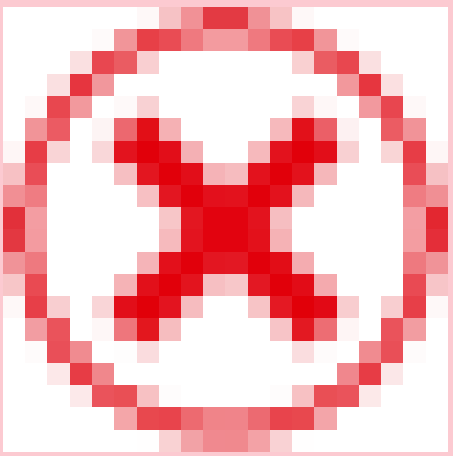
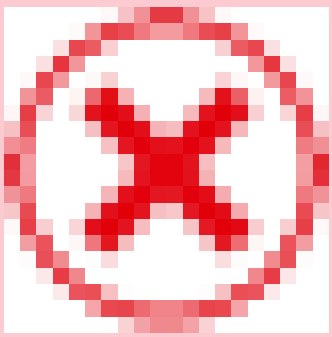
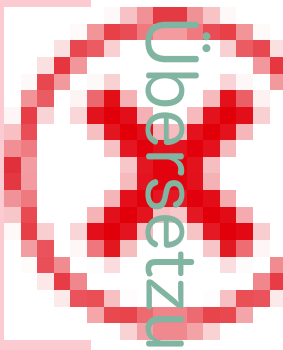
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

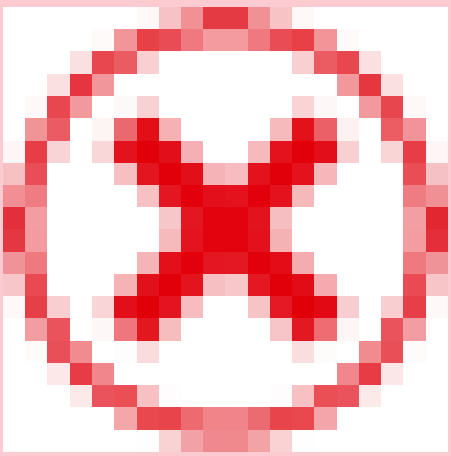
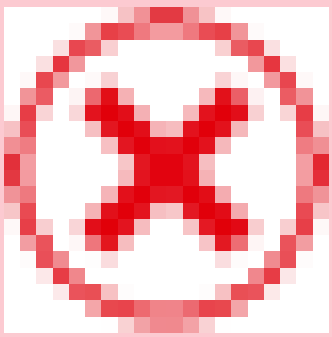
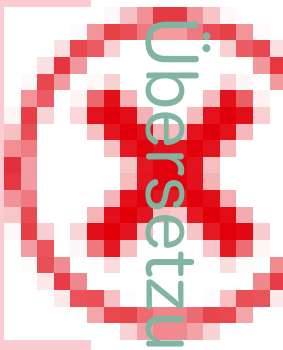
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Klassifizierungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

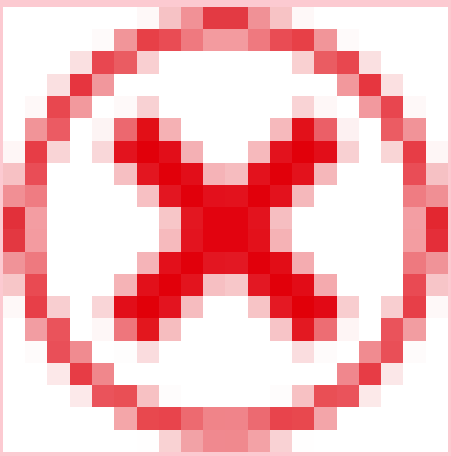
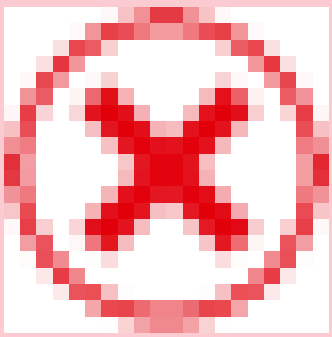
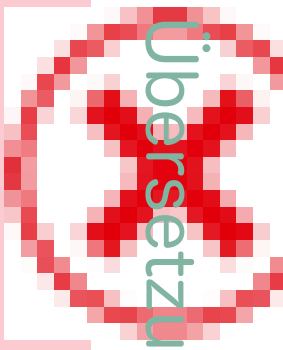
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Leistungskonfiguration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
VI-Granularität konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

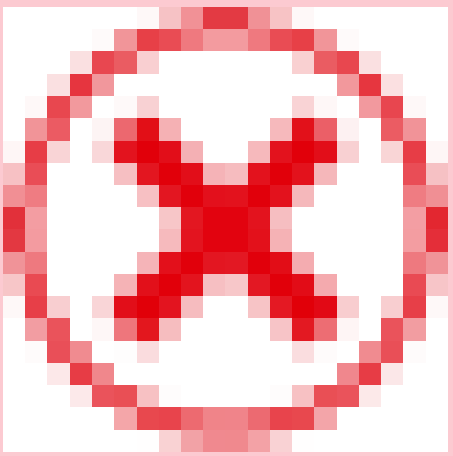
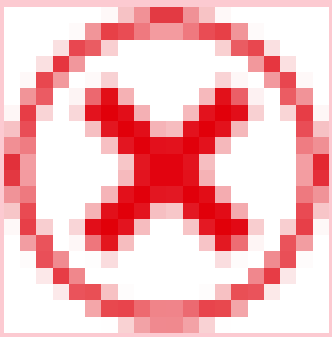
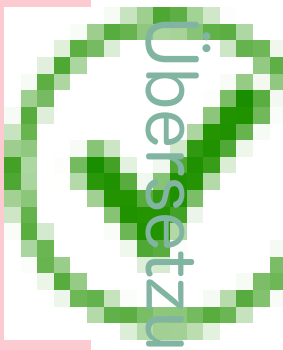
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Benachrichtigungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

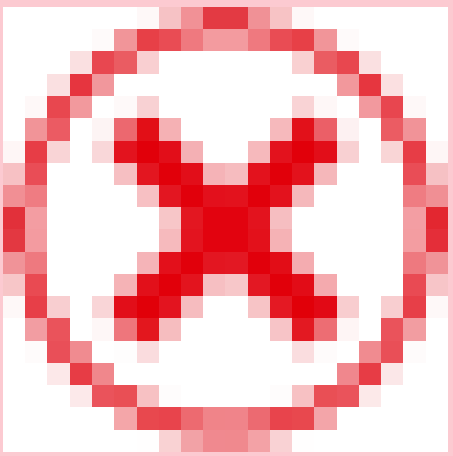
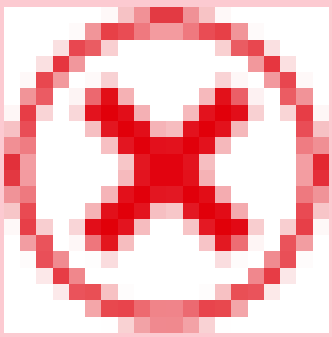
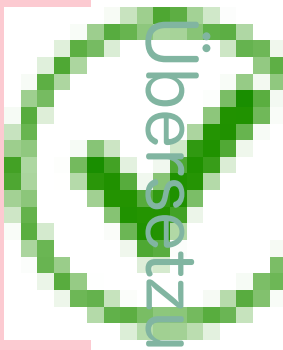
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
E-Mail-Vorlagen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

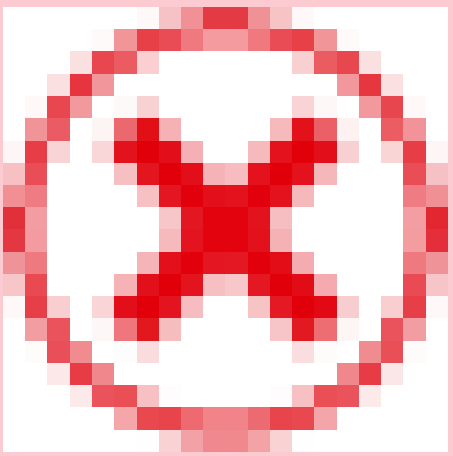
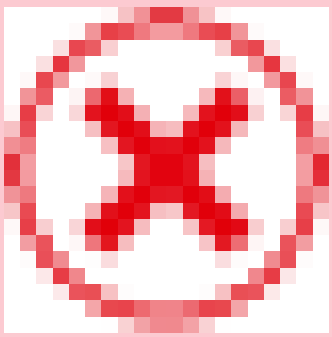
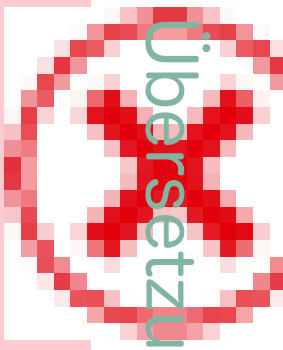
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Warteschlange importieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

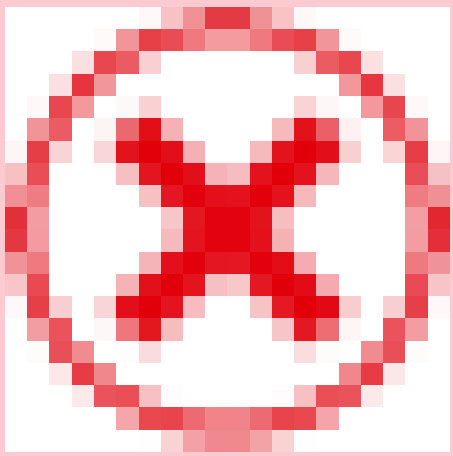
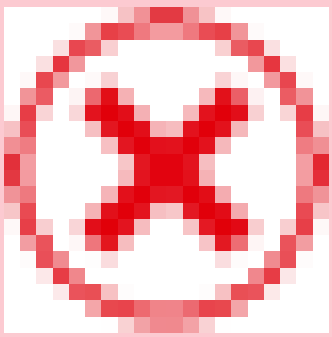
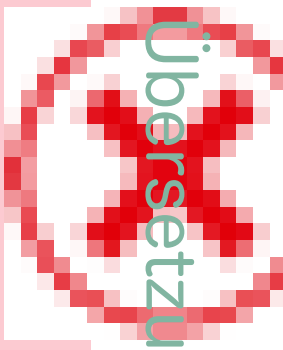
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
SAM-NVD konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

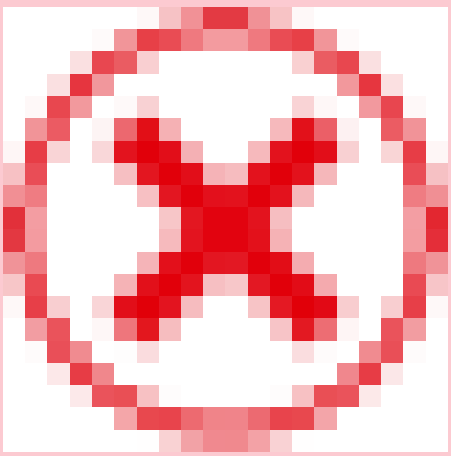
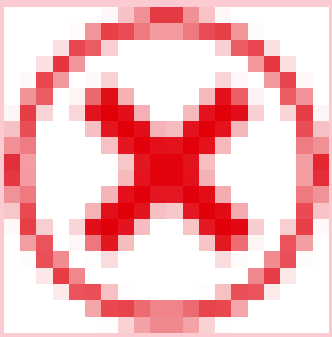
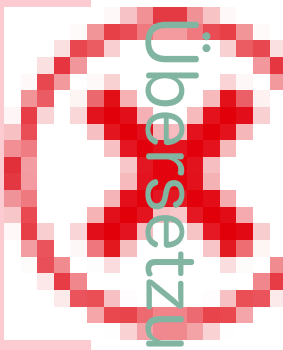
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Konfiguration der Scan-Abdeckung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

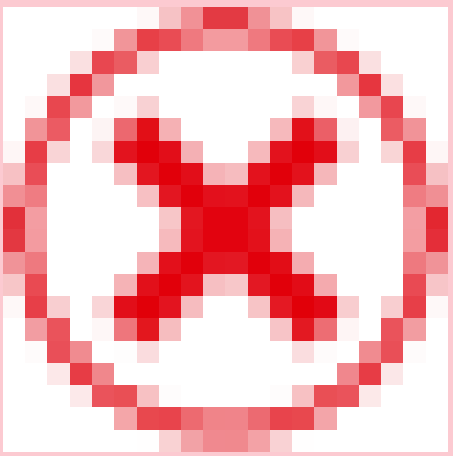
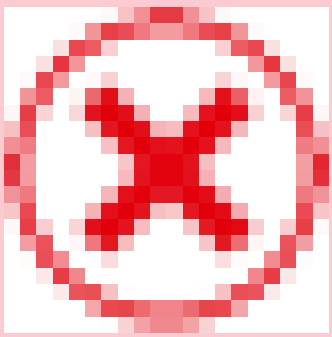
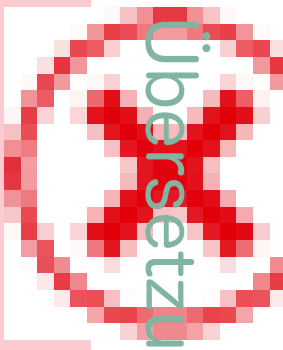
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Ausnahmenverwaltung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

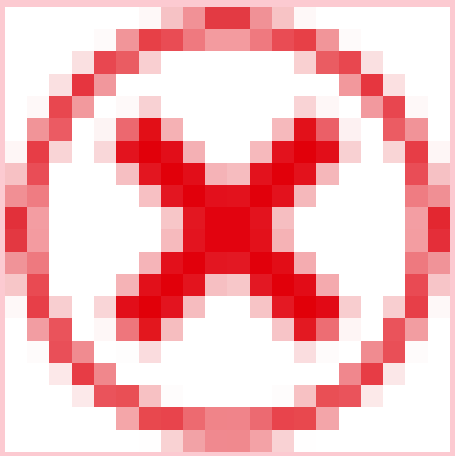
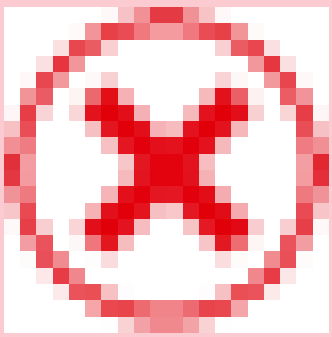
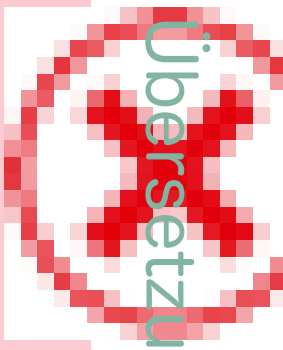
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Verwendungsbericht			
Diagnose			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

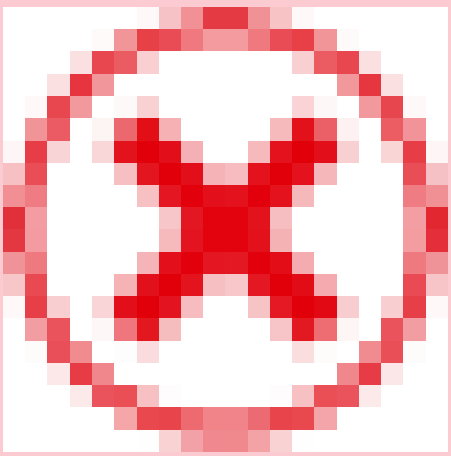
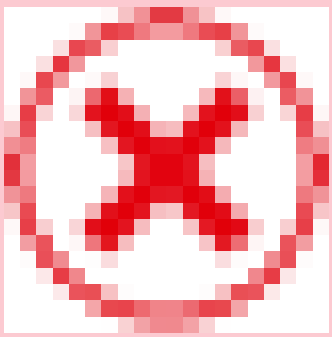
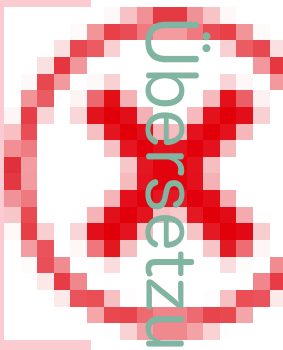
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifica
Überprüfungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
(Haupt-App-Gruppe)			
CISO-Dashboard	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Korrekturübersicht	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Übersicht	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Genehmiger-Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Übersicht	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Meine Genehmigungen	✗	✗	✗
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Aktiv	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Mir zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Meinen Gruppen zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

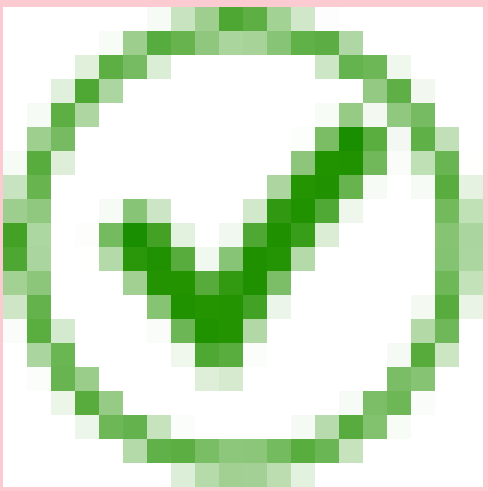
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Alle			
Angreifbare Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Kritisches Risiko	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Hohes Risiko	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Nutzbar	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Ziel rückt näher	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Verfehltes Ziel	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

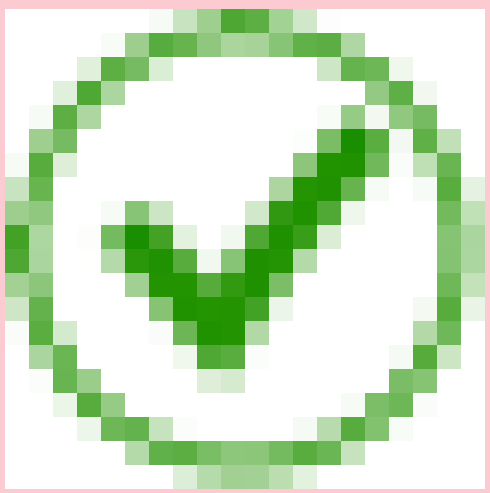
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Innerhalb der letzten 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Älter als 90 Tage	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Nicht zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Nicht gruppiert	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Außer Betrieb genommen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Mehrere Zurückstellungen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

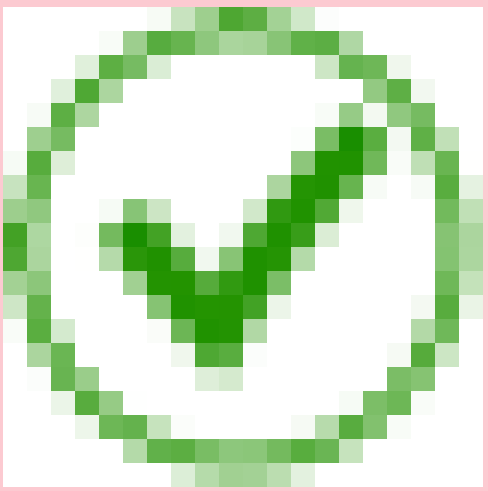
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Alle			
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Alle	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Ersetzung mit höchster Priorität	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

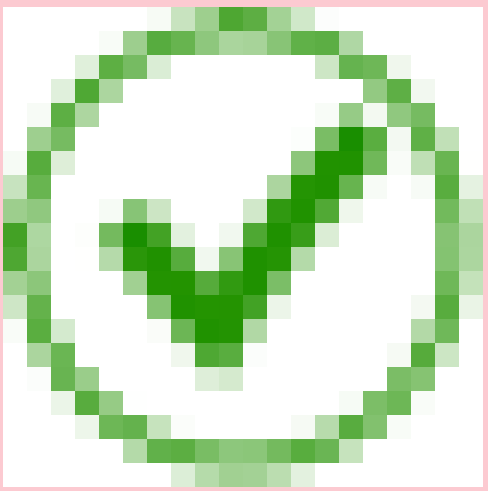
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Mit angreifbaren Elementen			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
NVD	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
CWE	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Drittpartei	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Software mit Schwachstellen	✓	✓	✓
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Bewertung des Gefahrenpotenzials	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Scans	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Scanner	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Scan-Warteschlange	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Scannerquotengrenzen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Überwachungsthemen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Regeln für Korrekturaufgaben	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

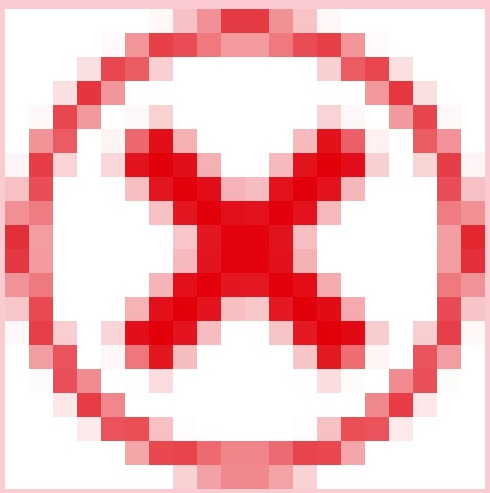
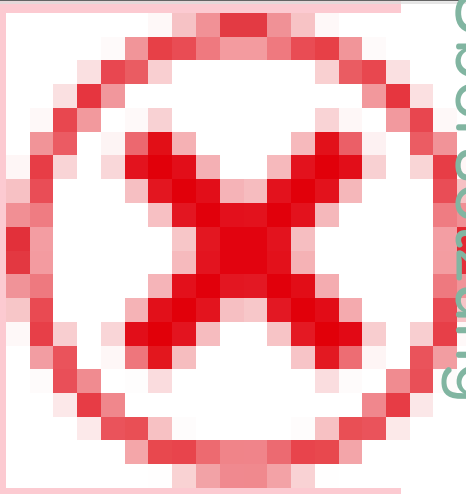
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Zuweisungsempfehlungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Schwachstellen-Rechner	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Rechner für Schwachstellen-Rollup	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Korrekturzielregeln	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Konfiguration für automatisches Schließen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Regeln für automatische Löschung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Ausnahmeregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Genehmigungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Klassifizierungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Leistungskonfiguration	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
VI-Granularität konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Benachrichtigungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
E-Mail-Vorlagen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Warteschlange importieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
SAM-NVD konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Normalisierte Schweregradzuordnungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Konfiguration der Scan-Abdeckung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Ausnahmenverwaltung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Verwendungsbericht	✗	✗	✗
Diagnose			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.r
Überprüfungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
(Haupt-App-Gruppe)				
CISO-Dashboard	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Korrekturübersicht	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Übersicht	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Arbeitsbereich für IT-Korrekturen	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Genehmiger-Übersicht	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Übersicht	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Meine Genehmigungen	✗	✗	✗	✓
Korrekturaufgaben				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Aktiv	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Mir zugewiesen	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Meinen Gruppen zugewiesen	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Alle	✗	✗	✗	✗

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Kritisches Risiko	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Hohes Risiko	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Nutzbar	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Ziel rückt näher	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Verfehltes Ziel				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Innerhalb der letzten 90 Tage	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Älter als 90 Tage	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Nicht zugewiesen	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Nicht gruppiert	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Außer Betrieb genommen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Mehrere Zurückstellungen	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Alle	✗	✗	✗	✗
Lösungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Alle	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Ersetzung mit höchster Priorität	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Mit angreifbaren Elementen	✗	✗	✗	✗
Bibliotheken				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
NVD	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
CWE	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Drittpartei	✗	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Software mit Schwachstellen	✗	✗	✗	✗
Schwachstellenscan				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Bewertung des Gefahrenpotenzials	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Scans	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Scanner	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Scan-Warteschlange	✓	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Scannerquotengrenzen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Quotengrenzdefinitionen	✗	✗	✗	✗
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Setup-Assistent	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Überwachungsthemen	✗	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Zuweisungsregeln	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Regeln für Korrekturaufgaben	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Zuweisungsempfehlungen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Schwachstellen-Rechner	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Rechner für Schwachstellen-Rollup	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Korrekturzielregeln	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Konfiguration für automatisches Schließen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Regeln für automatische Löschung	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Ausnahmeregeln	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Genehmigungsregeln	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Klassifizierungsregeln	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Leistungskonfiguration	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
VI-Granularität konfigurieren	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Benachrichtigungen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
E-Mail-Vorlagen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Warteschlange importieren	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Integrationen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
SLA-Definitionen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
SAM-NVD konfigurieren	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Normalisierte Schweregradzuordnungen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Konfiguration der Scan-Abdeckung	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Ausnahmenverwaltung	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Verwendungsbericht	✗	✗	✗	✗
Diagnose				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.Unassign_approver, sn_vul.view_enterprise_width_stats

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

(Fortsetzung)

Modul	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul. unass
Überprüfungen	✗	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

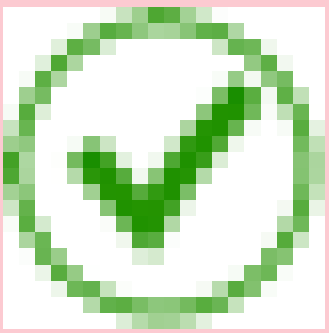
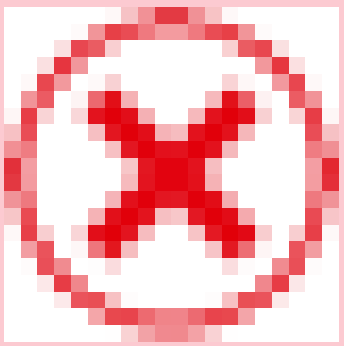
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
(Haupt-App-Gruppe)		
CISO-Dashboard		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

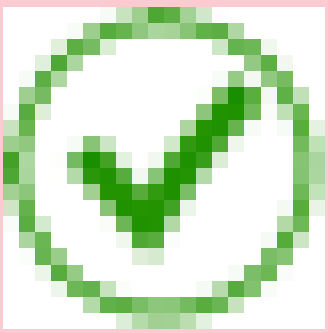
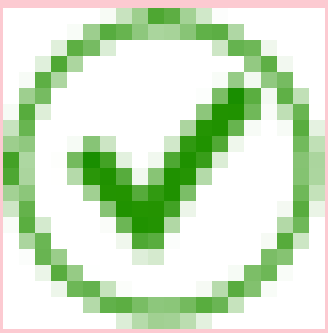
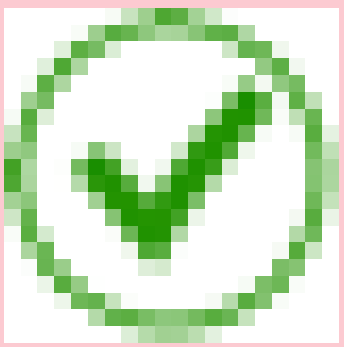
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Korrekturübersicht		
Arbeitsbereich des Schwachstellenmanagers		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

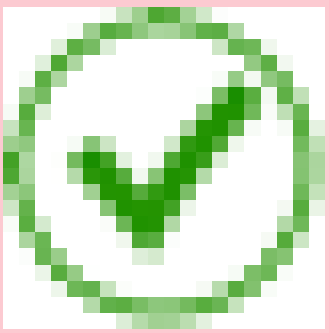
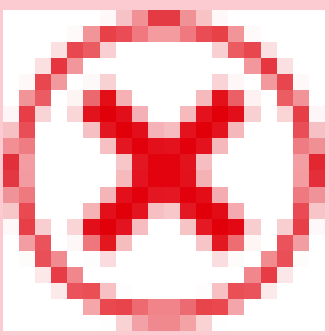
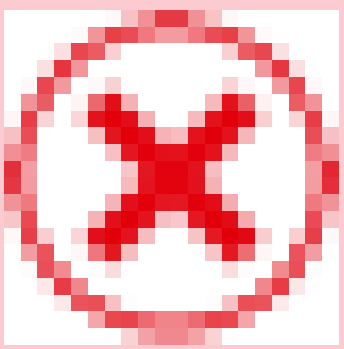
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Übersicht		
Arbeitsbereich für IT-Korrekturen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

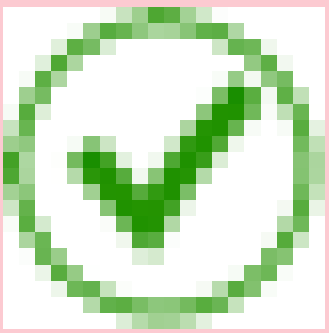
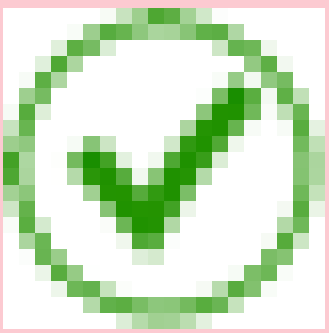
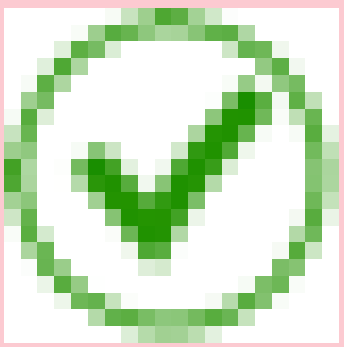
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Genehmiger-Übersicht		
Übersicht		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

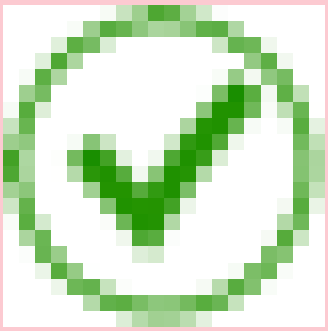
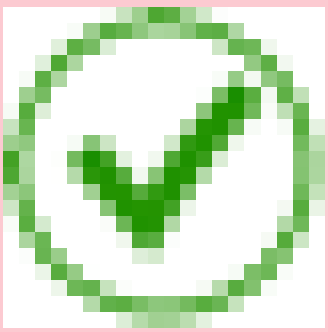
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Meine Genehmigungen		
Korrekturaufgaben		
Aktiv		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

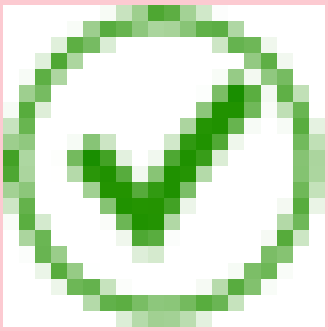
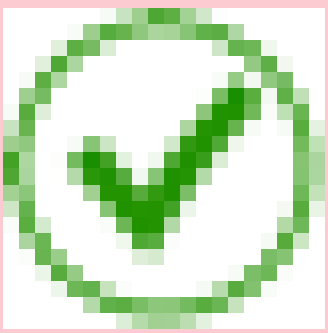
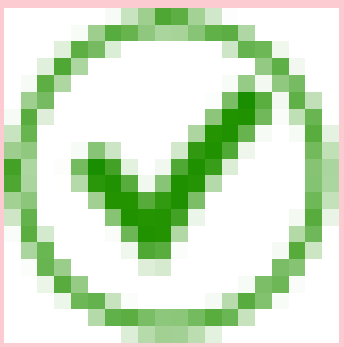
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Mir zugewiesen		
Meinen Gruppen zugewiesen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

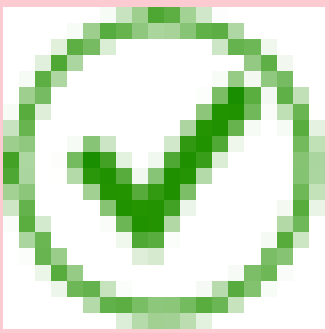
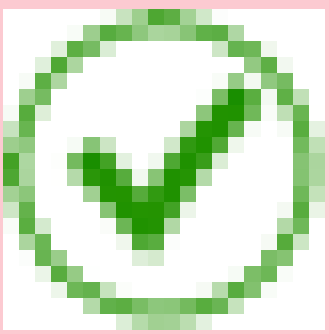
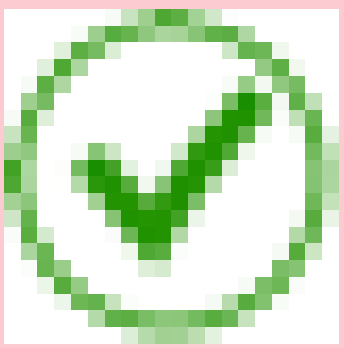
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Alle		
Angreifbare Elemente		
Kritisches Risiko		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

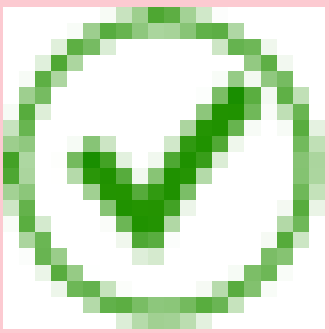
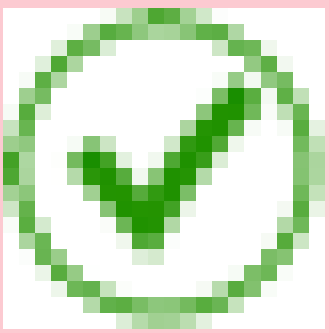
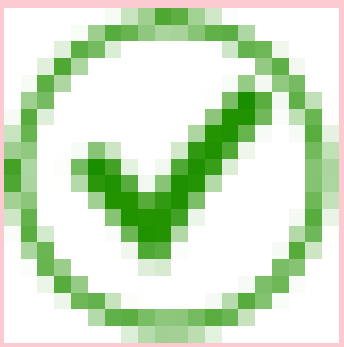
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Hohes Risiko		
Nutzbar		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

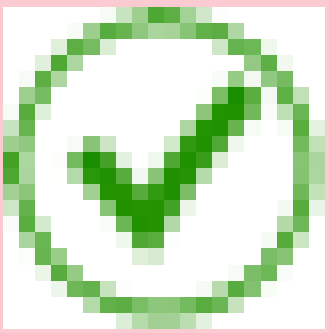
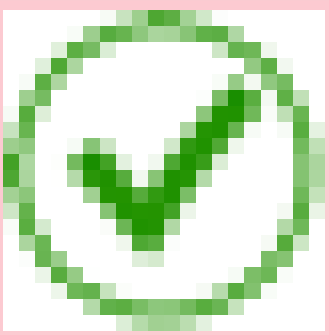
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Ziel rückt näher		
Verfehltes Ziel		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

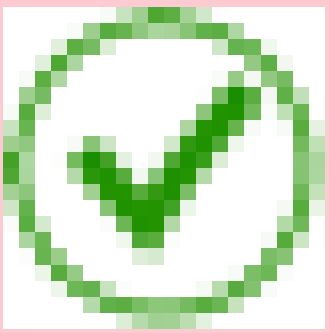
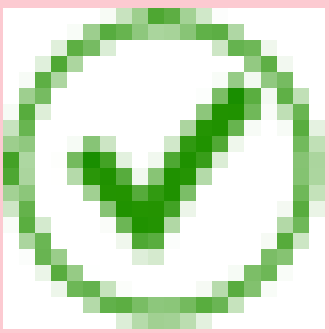
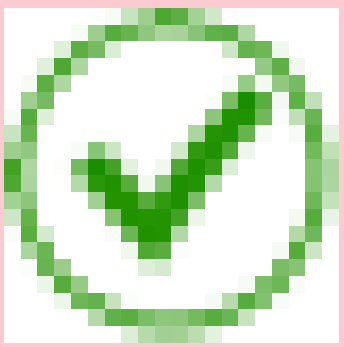
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Innerhalb der letzten 90 Tage		
Älter als 90 Tage		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

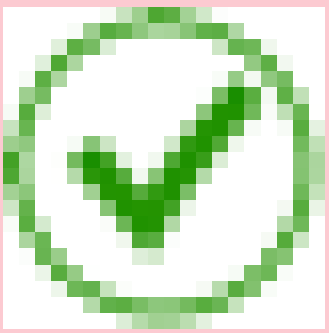
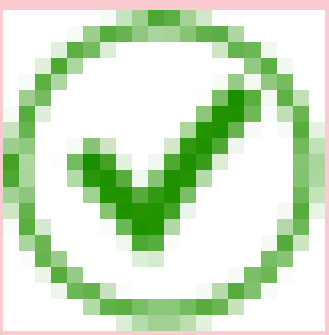
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Nicht zugewiesen		
Nicht gruppiert		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Außer Betrieb genommen	✓	✓
Mehrere Zurückstellungen	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Alle	✓	✓
Lösungen		
Alle	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

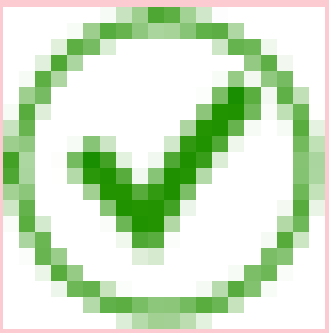
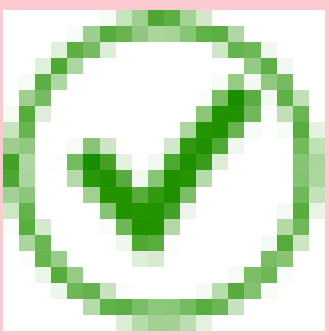
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Ersetzung mit höchster Priorität		
Mit angreifbaren Elementen		
Bibliotheken		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

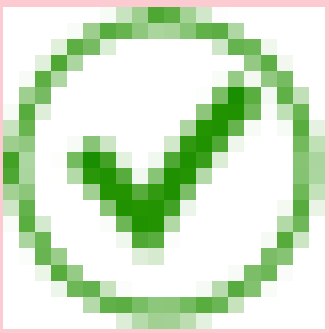
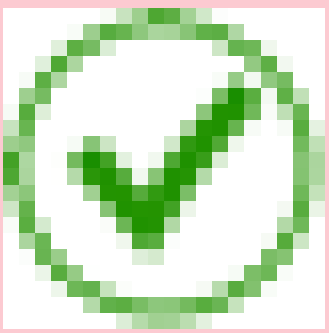
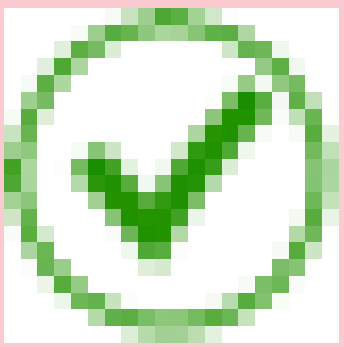
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
NVD		
CWE		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

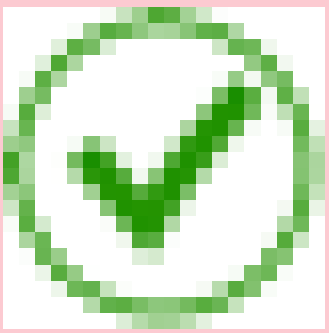
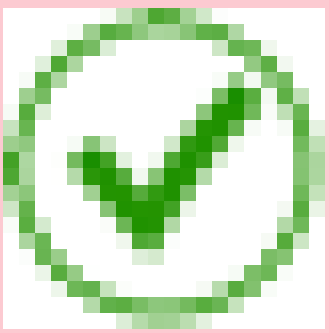
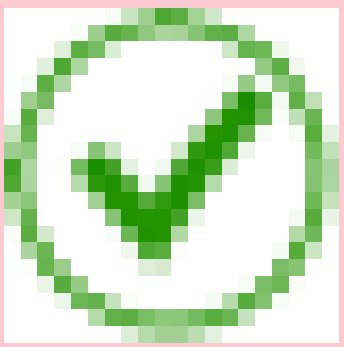
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Drittpartei		
Software mit Schwachstellen		
Schwachstellenscan		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

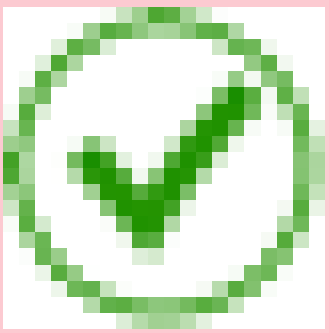
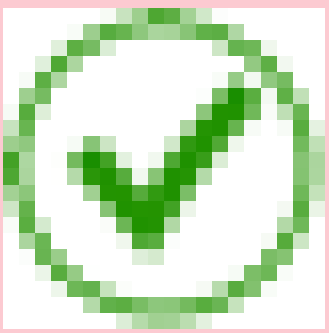
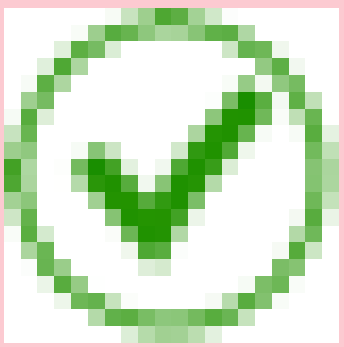
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Bewertung des Gefahrenpotenzials		
Scans		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

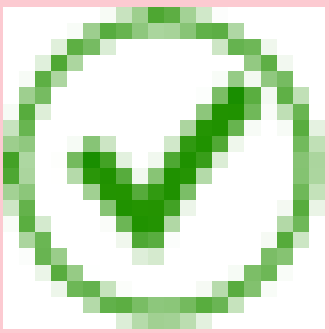
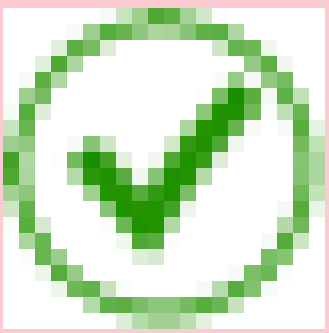
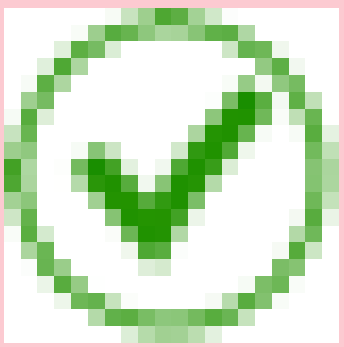
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Scanner		
Scan-Warteschlange		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

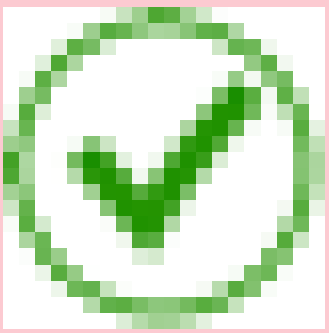
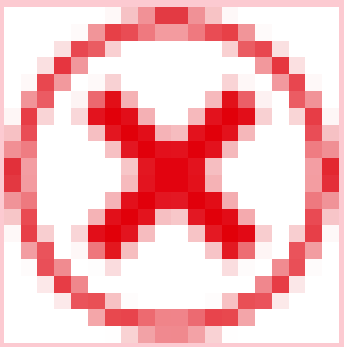
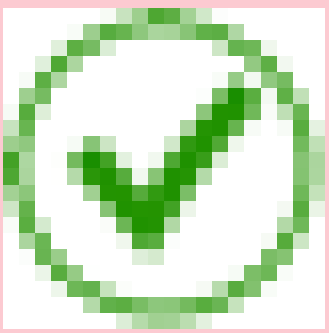
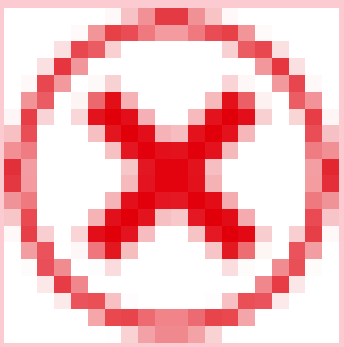
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Scannerquotengrenzen		
Quotengrenzdefinitionen		
Administration		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

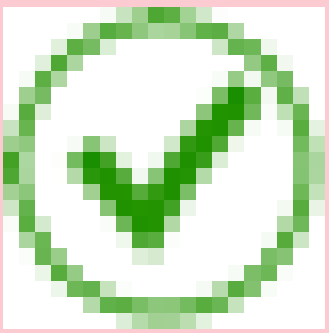
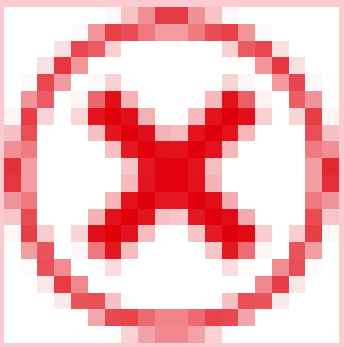
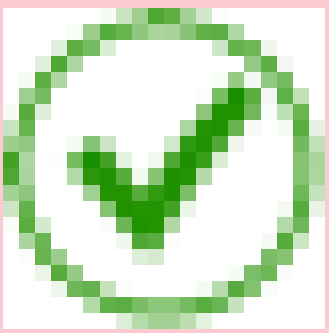
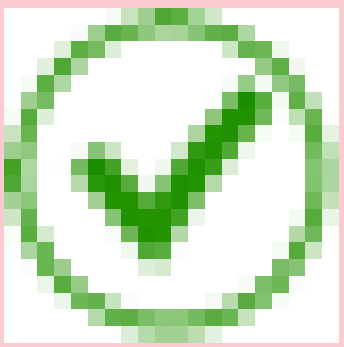
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Setup-Assistent		
Überwachungsthemen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

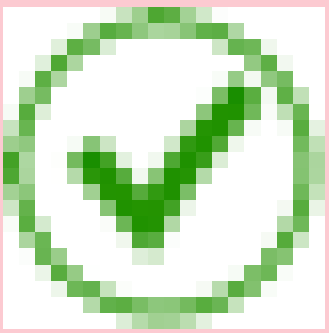
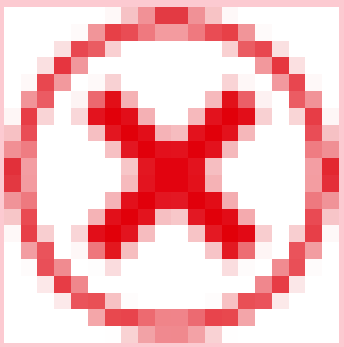
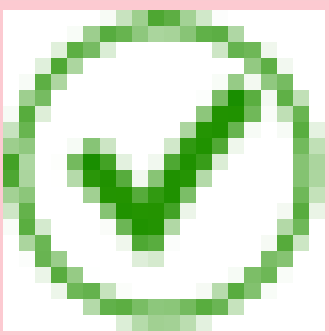
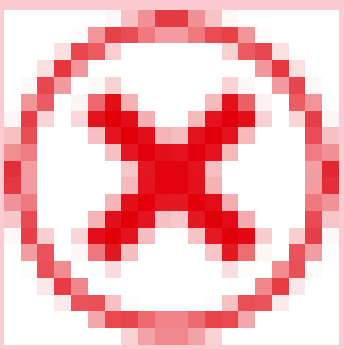
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Zuweisungsregeln		
Regeln für Korrekturaufgaben		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Zuweisungsempfehlungen	✗	✗
Schwachstellen-Rechner	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

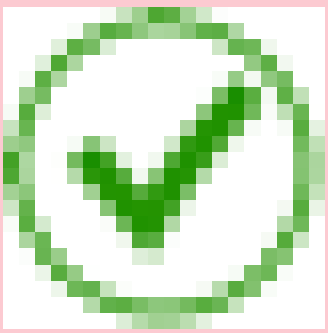
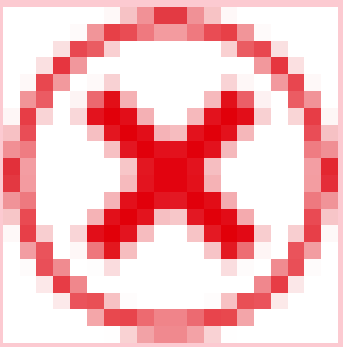
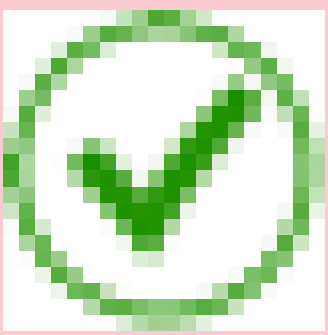
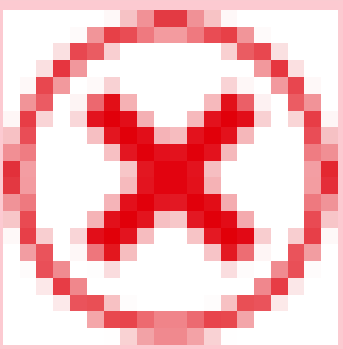
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Rechner für Schwachstellen-Rollup		
Korrekturzielregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

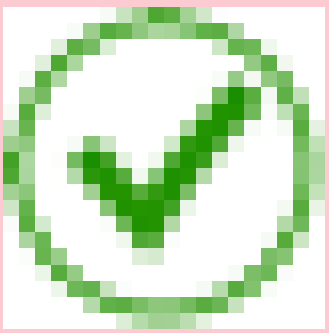
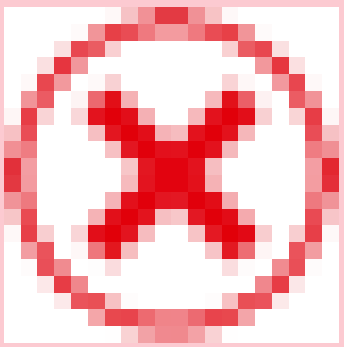
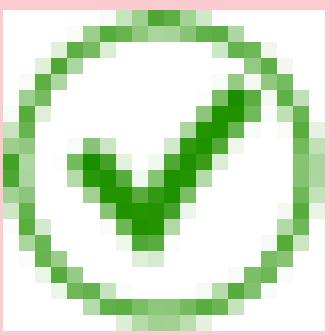
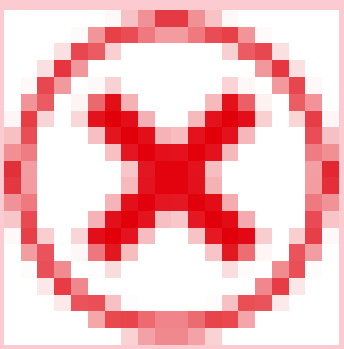
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Konfiguration für automatisches Schließen		
Regeln für automatische Löschung		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

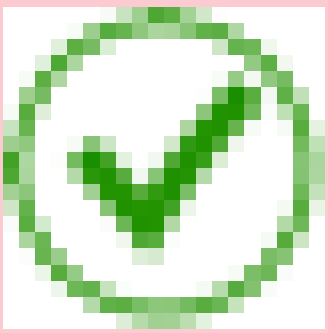
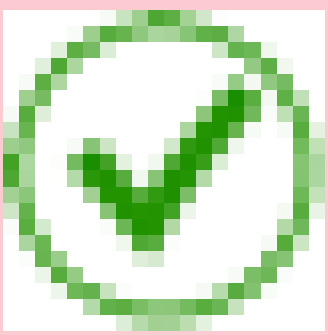
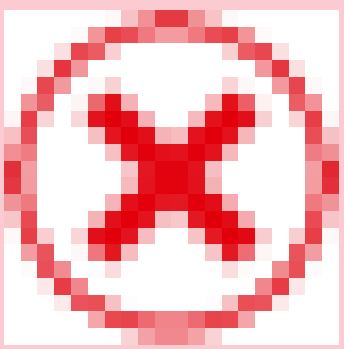
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Ausnahmeregeln		
Genehmigungsregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

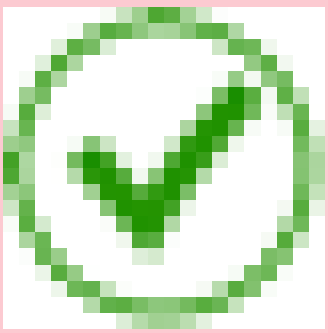
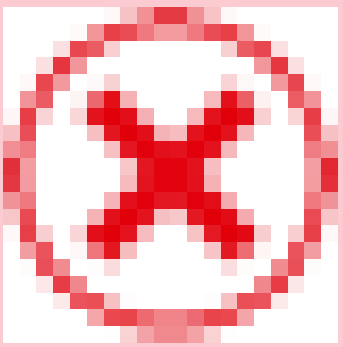
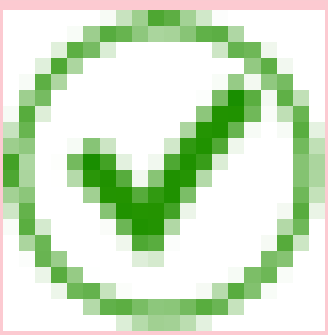
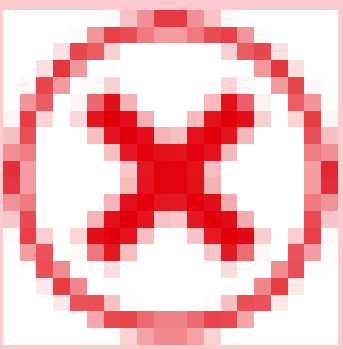
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Klassifizierungsregeln		
Leistungskonfiguration		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

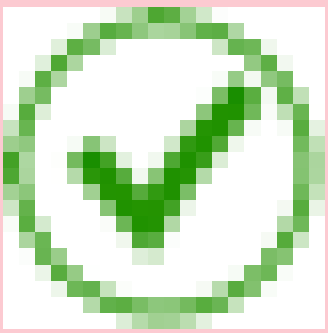
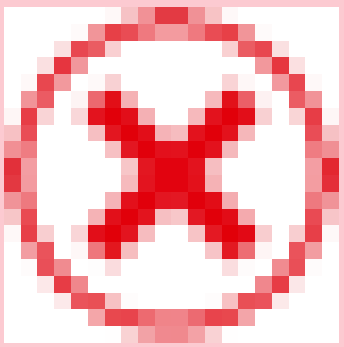
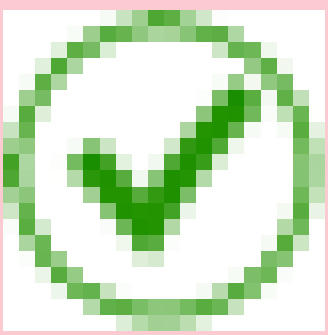
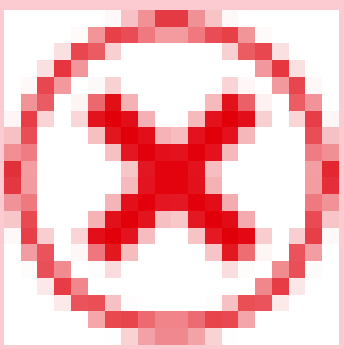
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
VI-Granularität konfigurieren		
Benachrichtigungen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

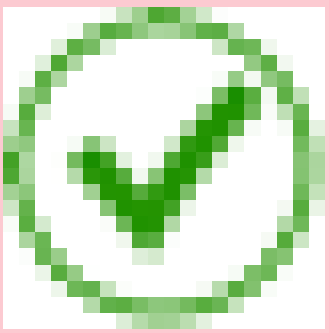
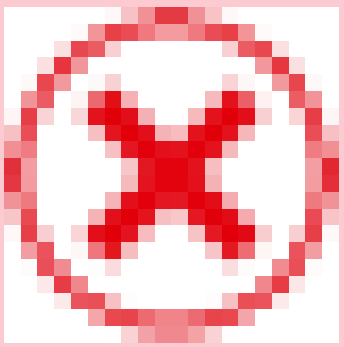
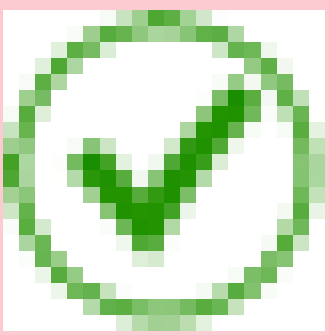
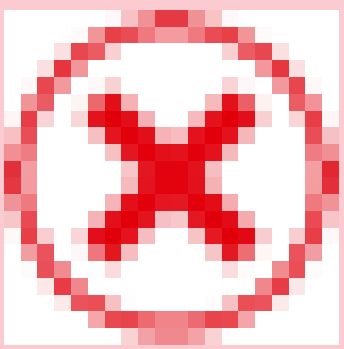
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
E-Mail-Vorlagen		
Warteschlange importieren		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

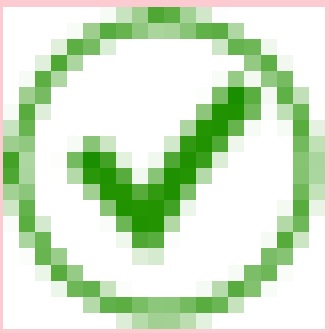
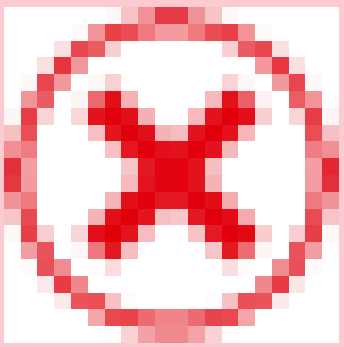
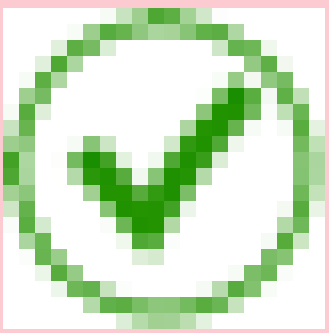
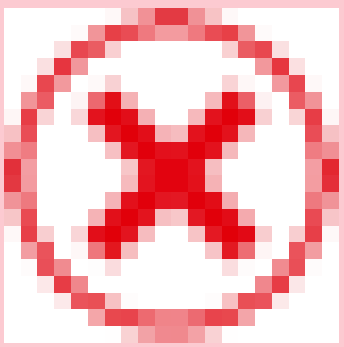
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Integrationen		
SLA-Definitionen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

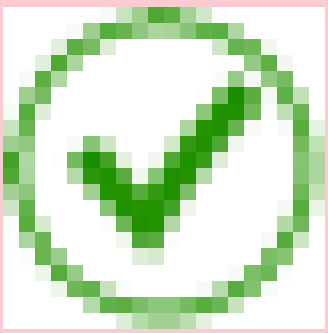
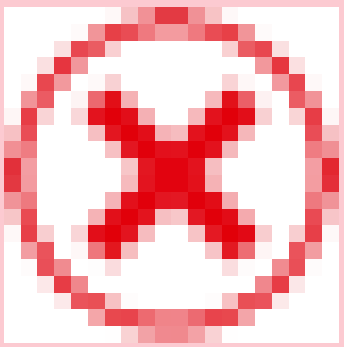
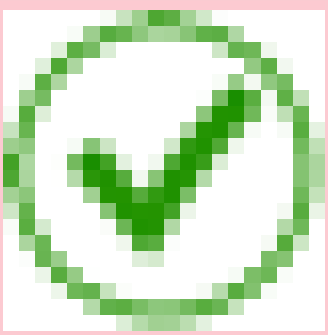
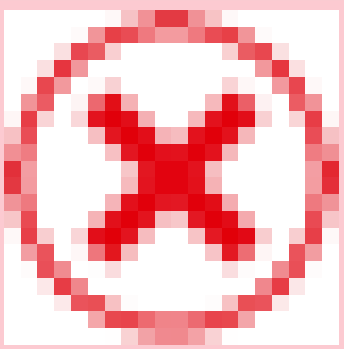
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
SAM-NVD konfigurieren		
Normalisierte Schweregradzuordnungen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Konfiguration der Scan-Abdeckung	✓	✓
Ausnahmenverwaltung	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informationen für andere Rollen:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.c iso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

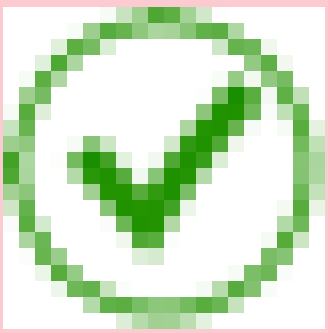
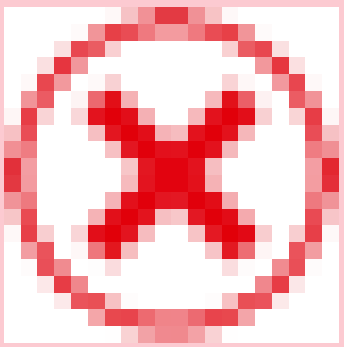
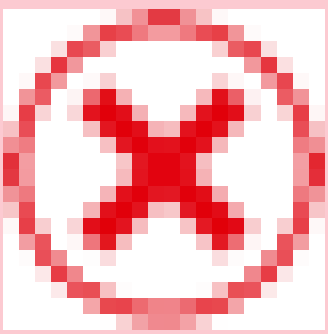
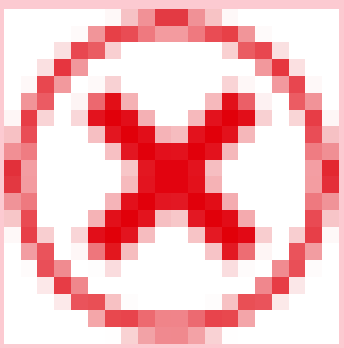
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

(Fortsetzung)

Modul	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Verwendungsbericht		
Diagnose		
Überprüfungen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

Security Operations durchsuchen

Über das Suchsymbol im Header des Bildschirms können Sie in jeder Anwendung Security Operations schnell Informationen finden. Zing ist die Textindizierungs- und Suchmaschine, die alle Textsuchen in Ihrer -Instanz durchführt.

Vorbereitungen

Erforderliche Rolle: sn_si.read oder höher

Prozedur

1. Klicken Sie auf das Suchsymbol ( ) in der oberen rechten Ecke des Bildschirms.
2. Geben Sie die Kriterien ein, nach denen Sie suchen möchten, und drücken Sie **die Eingabetaste**.
   Wenn Sie das Plugin Security Incident Response aktiviert haben, zeigen die von Ihnen eingegebenen Suchkriterien übereinstimmende Kurzbeschreibungstexte, CIs, IP-Adressen oder URLs in Ihren Security Incidents, Security Incident Response -Aufgaben oder Sicherheitsanforderungen an. Wenn Sie die Plugins Vulnerability Response oder Threat Intelligence aktiviert haben, umfassen die Suchergebnisse Schwachstellen, angreifbare Elemente, angreifbare Einträge, erkennbare Elemente, IoCs und Angriffsmodus/-methoden.

Zugehörige Informationen

Einführung in die Suche

Zing-Textsuche

Referenzen zur Integration mit Security Operations

Entwickler und ServiceNow-Partner können die Informationen in diesem Abschnitt verwenden, um sich ein Verständnis der zugrunde liegenden Funktionen von Drittanbieterintegrationen zu verschaffen, einschließlich Entwicklungsrichtlinien, Integrationsfunktionen und Workflows.

ServiceNow Security Operations Richtlinien für die Integrationsentwicklung

Die Plattform ServiceNow bietet mehrere Mechanismen für die Entwicklung von Integrationen mit externen Systemen. Die Produktsuite ServiceNow Security Operations fügt Integrationsfunktionen hinzu, die den Integrationsprozess in sicherheitsorientierte externe Systeme optimieren sollen.

Die meisten Konzepte in diesem Handbuch setzen eine gewisse Vertrautheit mit der Standardfunktionalität ServiceNow voraus. Für die Integration in die Suite Security Operations sind mindestens Kenntnisse der folgenden Konzepte von ServiceNow erforderlich:

- Skripteinbindungen
- Eingehende/ausgehende Webservices
- Datenquellen
- Importsätze
- Transformationszuordnungen

Technologiepartnerprogramm

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Anforderungen für die Anwendungszertifizierung oder Richtlinien, die in der Dokumentation zum Technologie-Partnerprogramm angegeben sind, haben Vorrang vor allen Informationen in diesem Leitfaden. Dieses Handbuch ist kein Ersatz für die Dokumentation zum Technologie-Partnerprogramm und dient lediglich als Ergänzung zur vorhandenen Dokumentation.

Weitere Informationen finden Sie im Blog-Beitrag zum Schulungskurs zum Technologie-Partnerprogramm .

Arten von ServiceNow Integrationen bereitgestellt

Die Security Operations -Anwendungen (Security Incident Response, Threat Intelligenceund Vulnerability Response) können nahtlos in andere ServiceNow -Anwendungen integriert werden, um deren Funktionalität zu erweitern.

Die folgenden Integrationen werden im Basissystem Security Operations bereitgestellt.

Security Incident Response – Ereignismanagement-Integration

Die Fähigkeiten der Anwendung Ereignismanagement wurden erweitert, um Security Incident Responsezu unterstützen. Das Support-Plugin Security Incident Response Ereignismanagement analysiert automatisch den Inhalt von Ereignissen in Ereignismanagement, um Felder in Security Incidents auszufüllen.

Abgedeckter Anwendungsfall:

Erstellung von Sicherheitsereignissen im System Ereignismanagement aus Sicherheitsinformationen und Ereignismanagement (SIEM-)Tools

Nützliche Fähigkeiten bereitgestellt:

- Ereignismanagement-Funktionalität: Ereigniskorrelation, Ereignisregeln und Warnungsregeln
- Automatische Zuordnung der Werte von „additional_information“ zum resultierenden Security Incident

Ressourcen:

Support-Dokumentation zur Verwaltung von Security Incident-Ereignissen

Dokumentation zu Event Management

Security Incident Response - Importsatz-API-Integration

Die Anwendung Security Incident Response verwendet nicht nur Ereignismanagement zum Übertragen von sicherheitsbezogenen Ereignissen, sondern stellt auch eine Importsatz-API bereit, mit der Security Incidents direkt erstellt werden können. Der REST-Endpunkt für den Importsatz für Security Incidents lautet http://localhost:8080/api/now/import/sn_si_incident_import.

Diese Integrationstechnik ist nützlich, wenn a) Ereignismanagement nicht installiert ist oder b) Security Incidents einfach erstellt werden sollen, ohne den Flow Ereignis > Warnung > Security Incident zu durchlaufen, der bei Verwendung von Ereignismanagementerforderlich ist.

Abgedeckter Anwendungsfall:

Erstellung von Security Incidents direkt mit SIEM-Tools.

Nützliche Fähigkeiten bereitgestellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatischer CI-Abgleich bei der Erstellung von Security Incidents basierend auf IP, NetBIOS oder vollqualifiziertem Domänennamen.

Ressourcen:

Dokumentation zur API des Plattform-Importsatzes

Dokumentation zum Webservice-Importsatz für Security Incidents

Threat Intelligence – Integration der Suchquelle

Suchquellen bieten die Möglichkeit, Daten an externe Suchquellen zu senden, um festzustellen, ob diese Daten schädlich sind. Im Allgemeinen sind diese Daten eine IP-Adresse, eine URL, eine Datei oder ein Datei-Hash.

Abgedeckter Anwendungsfall:

Suchen Sie mit einem externen Suchservice nach einer IP-Adresse, URL, Datei oder einem Hash.

Nützliche Fähigkeiten bereitgestellt:

- Einheitliche Methode zum Anfordern von Suchvorgängen in Katalogelementen und Security Incidents.
- Quotenbegrenzungs- und -drosselungsfunktionen mit wenig/keiner Codierung.
- Automatische Erstellung von Einträgen erkennbarer Indikatoren für Kompromittierungsindikatoren (IoC) für alle Probleme, die von Suchquellen gefunden wurden.

Threat Intelligence – Integration der Bedrohungsquelle

Bedrohungsquellen bieten die Möglichkeit, Daten aus externen Threat Intelligence-Repositorys abzurufen. Diese Daten werden dann in die verschiedenen Tabellen für Kompromittierungsindikatoren importiert, die im System vorhanden sind. TAXII-Sammlungen und einfache Sperrlisten werden nativ unterstützt. Um neue TAXII-Sammlungen (oder Profile basierend auf einem Discovery- oder Sammlungsverwaltungsservice) hinzuzufügen, fügen Sie ganz einfach einen Eintrag hinzu. Ebenso ist das Hinzufügen einer neuen einfachen, einspaltigen Sperrliste eine Angelegenheit der Eingabe eines neuen Datensatzes und der Angabe der URL der Sperrliste. Für komplexere Datensätze kann eine anwenderdefinierte Integration bereitgestellt werden, um eine URL aufzurufen und die Antwort zu analysieren.

Abgedeckter Anwendungsfall:

Rufen Sie Daten aus einer Threat Intelligence-Quelle ab, um sie in IoC-Tabellen zu laden.

Nützliche Fähigkeiten bereitgestellt:

- Unterstützung für einfache Sperrlisten und TAXII-Sammlungen ohne Codierung.
- Einfacher Mechanismus zum Ausführen von REST-Nachrichten zum Abrufen von Daten.
- Entkoppelter Datenabruf/-verarbeitung für die Wiederverwendbarkeit von Integrationskomponenten.
- Native Unterstützung für die Verarbeitung der Übergabe von Daten, die an Datenquellen (und Importsätze/Transformationszuordnungen) zurückgegeben werden.
- Unterstützt mehrere Datenanforderungen pro Integration (für paginierte Aufrufe) mit der Möglichkeit, Kontext an nachfolgende Aufrufe zu übergeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen:

Definieren Sie eine Bedrohungsquelle

Vulnerability Response – Integration des Scanneraufrufs

„Aufruf des Schwachstellenscanners“ ist ein schlanker Integrationseinstiegspunkt, der das Aufrufen von Schwachstellenscans aus der Instanz unterstützt. Der Schwachstellenscanner einer Drittpartei wird asynchron aufgerufen, um einen Scan auf Konfigurationselemente oder IP-Adressen zu planen.

Abgedeckter Anwendungsfall:

Fordern Sie den Scanner einer Drittpartei an, ein CI (mithilfe von aus dem CI abgeleiteten Hostinformationen) oder eine IP-Adresse/IP-Adressen zu scannen.

Nützliche Fähigkeiten bereitgestellt:

- Einfaches Framework zum Definieren von Scanner-Implementierungen.
- Einheitliche Methode zum Anfordern von Scans von Katalogelementen, Security Incidents und angreifbaren Elementen.
- Automatische Aktualisierung von Aufgaben mit Ergebnis des Scan-Aufrufs.

Vulnerability Response – Datenintegration

Schwachstellendaten-Integrationen sollen Schwachstellendaten aus Schwachstellensystemen von Drittanbietern abrufen. Die erwarteten Ausgaben dieser Integrationen sind Schwachstelleneinträge und angreifbare Elemente. Durch diese Integration können Schwachstellenscanner von Drittparteien unabhängig voneinander funktionieren, mit der Erwartung, dass Schwachstellen innerhalb der Instanz bearbeitet und nachverfolgt werden können.

Abgedeckte Anwendungsfälle:

- Rufen Sie Schwachstellenbibliotheken ab
- Rufen Sie Schwachstellen-/CI-Paare ab
- Synchronisieren Sie CIs mit dem Schwachstellenmanagementsystem

Nützliche Fähigkeiten bereitgestellt:

- Entkoppelter Datenabruf/-verarbeitung für die Wiederverwendbarkeit von Integrationskomponenten.
- Native Unterstützung für die Verarbeitung der Übergabe von Daten, die an Datenquellen (und Importsätze/Transformationszuordnungen) zurückgegeben werden.
- Unterstützt mehrere Datenanforderungen pro Integration (für paginierte Aufrufe) mit der Möglichkeit, Kontext an nachfolgende Aufrufe zu übergeben.

Ressourcen:

Dokumentation zur Schwachstellendaten-Integration

Security Operations Integrationskonfigurationen

Viele der im Basissystem enthaltenen Integrationen erfordern wenig oder kein Setup und funktionieren auf die gleiche Weise. Bestimmte Integrationen, z. B. Qualys Cloud Platform,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erfordern jedoch separate Schritte zum Einrichten der Integration. Andere unterstützen andere Sätze von Scan- und Suchtypen und andere Quotenbegrenzungen.

In diesem Abschnitt werden die Unterschiede zwischen den unterstützten Integrationen beschrieben und Sie werden bei Bedarf auf weitere Dokumentation verwiesen.

- Integration mit Carbon Black: ermöglicht Ihnen, Security Incidents zu untersuchen und darauf zu reagieren, indem Sie die Carbon Black-APIs verwenden, um Endpunkte im Zusammenhang mit Security Incidents abzufragen und mit ihnen zu interagieren.
- Integration mit Check Point Anti-Bot - Email Parser: verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von Check Point Anti-Bot verarbeitet, um Security Incidents zu erstellen.
- Integration mit Elasticsearch Incident Enrichment: durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Have I Been Pwned? Integration: Ermöglicht das schnelle Durchsuchen der Liste der verletzten Accounts (E-Mail-Adressen und Anwendernamen) über einen RESTful-Service.
- HPE Security ArcSight ESM – Integration mit E-Mail-Parser: verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von HPE ArcSight ESM verarbeitet, um Security Incidents zu erstellen.
- HPE ArcSight Logger Integration mit der Ergänzung von Incidents: durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- IBM QRadar – Integration zur Ergänzung von Incidents: durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- McAfee ESM – E-Mail-Parser-Integration: verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von McAfee ESM verarbeitet, um Security Incidents zu erstellen.
- McAfee ESM – Integration zur Ergänzung von Incidents: durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Integrationsüberblick OPSWAT Metadefender: ermöglicht das Herunterladen von Bedrohungsdaten, die vom Drittanbieter-Scanner Metadefender erkannt wurden, in die Anwendung Threat Intelligence zu Nachverfolgungs-, Priorisierungs- und Lösungszwecken.
- Palo Alto Networks – AutoFocus Integration: Palo Alto Networks AutoFocus, ein Cloud-Service für Bedrohungsinformationen, ermöglicht Ihnen die Suche nach Sitzungsinformationen im Zusammenhang mit erkennbaren Elementen von Security Incidents.
- Palo Alto Networks – Firewall Integration: Mit der Palo Alto Networks-Firewall können Sie Firewalls einrichten und verwalten, um bekannte und unbekannte Bedrohungen im Netzwerk, in der Cloud und an Endpunkten abzuwehren.
- Palo Alto Networks – WildFire Integration: Mit der WildFire-Integration können Sie Analyseaufträge in WildFire programmgesteuert abfragen und Verlaufsergebnisse über eine einfache XML-API-Schnittstelle abrufen.
- Qualys Vulnerability Integration verstehen: Qualys Cloud Platform wird in Vulnerability Responseverwendet.
- Integration mit Splunk - Incident Enrichment: durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Integration mit VirusTotal: verwendet in Threat Intelligence: Um diese Suchquelle zu verwenden, müssen Sie das Plugin „VirusTotal-Integration“ aktivieren.
- Setup der WhoisXML-API-Integration: liefert konsistente, gut strukturierte Daten aus einer Whois-Suche. Sorgt dafür, dass genaue Whois-Daten rund um die Uhr zugänglich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Drittanbieterintegrationen aktivieren und konfigurieren

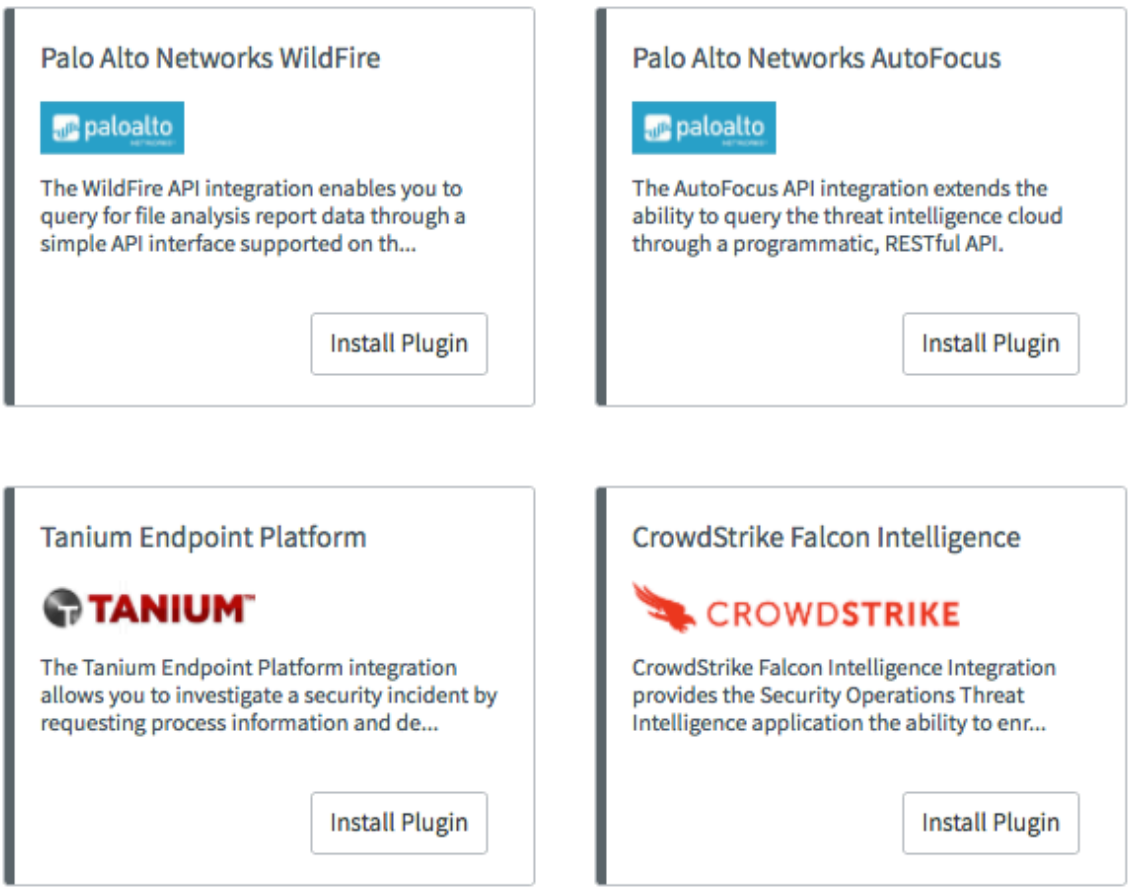
Sie können die Plugins für Drittanbieterintegrationen aktivieren und sie für die Verwendung im selben Bildschirm konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt, ähnlich der folgenden Gruppe von Karten. Sie können auf jede Karte zeigen, um eine Beschreibung der Integration zu erhalten.



2. Um das Plugin für eine bestimmte Integration zu installieren, klicken Sie auf **Plugin installieren**.

   a. Überprüfen Sie im Formular „System-Plugin“ die Plugin-Details, und klicken Sie auf den zugehörigen Link **Aktivieren/Upgrade**.

   b. Klicken Sie auf **Aktivieren**.
   Wenn die Aktivierung abgeschlossen ist, wird der Bildschirm „Security Integration“ erneut geöffnet, und die Schaltfläche für die von Ihnen aktivierte Integration trägt die Bezeichnung **Konfigurieren**.

3. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie Qualys Vulnerability Integrationkonfigurieren, lesen Sie unter Installation von Vulnerability Response und unterstützten Anwendungennach.

4. Geben Sie den **API-Schlüssel**ein.
5. Klicken Sie auf **Absenden**.

Erstellen Sie eine Integration

Sie können eine Integration erstellen und die zugehörige Integrationskarte zum Bildschirm „Security Integrations“ (Sicherheitsintegrationen) hinzufügen. Dieses Verfahren richtet sich an Partner, die Drittanbieterintegrationen erstellen.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Zielgruppe: Partner, die Integrationen von Drittparteien erstellen.

Prozedur

1. Geben Sie im Navigationsfilter sn_sec_core_integration_item.list ein, und drücken Sie die **Eingabetaste**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Integration.
Plugin-ID	Das Plugin, das zur Verwendung der Integration aktiviert werden muss.
Bestellung	Gibt den Reihenfolgewert an, in dem diese Integrationskarte angezeigt wird.
Banner-Text	Klicken Sie auf den Link, wählen Sie ein Bild oder Logo aus, das auf der Integrationskarte angezeigt werden soll, und klicken Sie auf **OK**.
Installiert	Schreibgeschütztes Feld, das angibt, ob das Plugin bereits installiert wurde.
Konfigurierbar	Gibt an, ob Sie die Integration konfigurieren können.
Kategorien	Wird zum Filtern der Integrationskarten verwendet.
Kurzbeschreibung	Eine Beschreibung der Integration, die im Tooltip-Hinweis für die Karte angezeigt wird.
Beschreibung	Eine längere Beschreibung der Integration.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die zugehörige Liste **Integrationen und Konfigurationen** wird angezeigt. Sie können diese zugehörige Liste verwenden, um Konfigurationsoptionen für die Integration zu definieren. Diese Optionen werden angezeigt, wenn Sie auf der zugehörigen Integrationskarte auf die Schaltfläche **Konfiguration** klicken.
5. Klicken Sie auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bezeichnung	Der Name des Integrationselements.
Name	Das Plugin, das zur Verwendung der Integration aktiviert werden muss.
Integration	Zeigt die Integration an, für die Sie Integrationselemente definieren
Bestellung	Gibt die Reihenfolge an, in der dieses Integrationselement angezeigt wird.
Typ	Wählen Sie in der Liste den Typ des Felds aus: ○ Zeichenfolge ○ Ganzzahl ○ Dezimalzahl ○ Datum ○ Boolean ○ Passwort ○ IPv4 ○ IPv6 ○ URL
Wert	Geben Sie den Wert ein, der dem ausgewählten **Typ** zugeordnet ist. Wenn ein Wert eingegeben wird, der für den ausgewählten **Typ** ungültig ist, werden bei Ausführung der Integration keine Datensätze abgerufen. Wenn Sie beispielsweise den URL-Typ auswählen und den Wert 12.32.23.10 eingeben, werden keine Datensätze abgerufen.

7. Klicken Sie auf **Absenden**.

Tipps zum Schreiben von Integrationen

Vermeiden Sie einige der Gefahren, die beim Schreiben eigener Integrationen auftreten können, indem Sie diese Richtlinien befolgen.

Verwenden Sie nach Möglichkeit die Funktionalität der Now Platform

Die in den Anwendungen Security Operations integrierten Integrationsfähigkeiten (Security Incident Response, Threat Intelligenceund Vulnerability Response) dienen hauptsächlich dazu, die vorhandenen Integrationsfunktionen der Plattform ServiceNow zu verbessern oder zu optimieren. Stellen Sie beim Schreiben von Integrationen immer sicher, dass Sie die Plattformfunktionalität verwenden, sofern vorhanden. Im Folgenden sind einige allgemeine ServiceNow -Funktionalitäten aufgeführt, die nicht „Rollen-Ihr-Eigentum rollen“ geändert werden können.

- Ausgehende Webservices: Bei den meisten Interaktionen mit Drittparteisystemen erfolgt die Kommunikation über Webservices. Verwenden Sie in diesen Fällen ausgehende Webservices der Plattform (REST und SOAP werden unterstützt).
- Datenquellen/Importsätze/Transformationszuordnung: Für die Verarbeitung von Daten und das Einfügen in Tabellen ServiceNow werden Datenquellen und zugehörige Komponenten bevorzugt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie nach Möglichkeit Security Operations-Integrationsframeworks

Da die Integrationsmechanismen Security Operations von viele häufige Probleme gelöst haben, ist es nicht erforderlich, grundlegende Funktionen für jede Integration neu zu implementieren. Beispielsweise unterstützen die Frameworks für Schwachstellendaten und Bedrohungsquellen die Verarbeitung mehrerer Seiten und die Übergabe dieser Daten an Datenquellen/Transformationen/Importsätze. In ähnlicher Weise bietet das Scan- oder Suchquell-Framework konfigurierbare Funktionen zur Quotenbegrenzung. Überprüfen Sie in der Regel bei der Implementierung einer Funktion oder einer Reihe von Funktionen, ob das vorhandene Security Operations -Integrations-Framework Ihren Anwendungsfall abdeckt. Wenn ja, verwenden Sie dieses Framework.

Erweitern Sie die vorhandenen Security Operations-Integrations-Frameworks nach Bedarf

Die meisten der von Security Operations -Integrations-Frameworks verwendeten Tabellen und Skripts sollten für zukünftige Anforderungen erweitert werden. Wenn beim Schreiben einer Integration ein Anwendungsfall auftritt, erweitern Sie eine Integrationstabelle oder ein Skript, um diesen Anwendungsfall besser anzupassen.

Geben Sie Feedback an ServiceNow zu Problemen, die während der Integration aufgetreten sind

Wenn eine Integration entwickelt oder getestet wird, geben Sie bei Problemen unbedingt Feedback. Selbst wenn ein Workaround erforderlich ist, können die Mitarbeiter von Kundenservice und Support in zukünftigen Releases eine Verbesserung bereitstellen, die das Problem für zukünftige Integrationen entschärft.

Unter angemessener Last testen

Ein häufiges Problem bei Integrationen ist, dass sie nicht für realistische Lasten geeignet sind. Da jede Integration eine bereichsbezogene Anwendung ist, gelten für die Systemstabilität je nach Plattform weitere Einschränkungen. Diese Einschränkungen können dazu führen, dass Aufträge mit langer Ausführungszeit oder API-Aufrufe beendet werden. Sie können sicherstellen, dass Prozesse mit langer Laufzeit oder Prozesse, die viele Daten verarbeiten, ordnungsgemäß gehandhabt werden, indem Sie die Zeit für jeden Aufruf oder Prozess reduzieren (normalerweise durch Bereitstellung einer Möglichkeit zur Paginierung von API-Anforderungen oder zur Blockierung großer Datenmengen).

Problembehandlung bei Integration

Diese Vorschläge zur Problembehandlung können Ihnen helfen, häufige Probleme zu beheben, die beim Einrichten oder Ausführen von Integrationen auftreten können.

Ersetzen Sie ein nicht vertrauenswürdiges oder abgelaufenes SSL-Zertifikat einer Drittpartei

Wenn in einer Integration eine SSL-Verbindung erforderlich ist, gibt es Fälle, in denen das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Sie können es ersetzen oder ein neues Zertifikat hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.write

Prozedur

1. Erwerben Sie das SSL-Zertifikat von einem Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) wie folgt von einem SSL-Endpunkt im Firefox-Browser importieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
Beispiel: `https://<3rdparty>/`.

b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

c. Klicken Sie auf **Weitere Informationen** und anschließend auf die Registerkarte **Sicherheit**.

d. Klicken Sie auf **Zertifikat anzeigen** und anschließend auf die Registerkarte **Detail**.

e. Klicken Sie auf **Export**, um die PEM-Datei in Ihrem lokalen Dateisystem zu speichern.

f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
Sie muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu** und Erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Klicken Sie auf **Speichern**.
Die anderen Felder im Datensatz werden automatisch generiert.

Framework für Integrationsfähigkeiten 2.0

Das neue Integration Capabilities Framework 2.0 wurde überarbeitet, um eine einfache und konsistente Implementierung von Integrationen zu ermöglichen. Dies stellt eine konsistente Experience für ähnliche Arten von Integrationen sicher (z. B. Reputationssuche erkennbarer Elemente).

Das neue -Framework verfügt über Funktionen, die mithilfe von Flows implementiert werden.

Zu den Vorteilen der Implementierung des erweiterten Frameworks gehören:

- Die Fähigkeits-Flows, die nur Komponenten auf Geschäftsebene ohne implementierte spezifische Logik enthalten.
- Die Fähigkeits-Flows akzeptieren jetzt eine breite Palette von Eingaben und Formaten für maximale Flexibilität (z. B. Referenzen erkennbarer Elemente, CI-Referenzen, Aufgaben, beliebige Tabellen- oder sys_id-Kombinationen).
- Quotenbegrenzung oder Drosselung bei Integrationsausführungen ist jetzt einfach zu konfigurieren (die Notwendigkeit, dies mit benutzerdefiniertem Code oder Änderungen an Implementierungs-Workflows zu tun, entfällt).
- Erweiterte Audit- und Ausführungsnachverfolgungsfunktionen ermöglichen jetzt eine bessere Berichterstellung und erleichtern die Problembehandlung.
- Robuste Fehlerbehandlungsfunktionen sind in die Fähigkeits-Flows integriert, um die Duplizierung von Implementierungsroutinen zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Möglichkeit zur Konfiguration der bedingten Auslösung der Fähigkeiten oder Integrationen. Dies bietet die Flexibilität, Automatisierungen automatisch basierend auf der Incident-Kategorie zu starten.
- Für alle Fähigkeiten wurde eine Standardfilterbedingung eingeführt, um auf der Zulassungsliste erkennbare Elemente zu filtern, bevor Eingaben für die Integrationen bereitgestellt werden.

Hinweis:
Dieses neue Fähigkeits-Framework aktualisiert das aktuelle Fähigkeits-Framework nicht. Beide Frameworks können parallel arbeiten. Anweisungen zur Nutzung des neuen Capability Framework finden Sie unter Mittels des neuen Fähigkeiten-Frameworks mit einer installierten Integration und Verwenden des neuen Fähigkeits-Frameworks mit einem Flow.

Unterstützte Integrationen und Komponenten

Das Security Incident Response-Plugin enthält alle in Integration Capabilities Framework 2.0 aufgeführten Fähigkeits-Flows sowie allgemeine Standardfilter, die Sie je nach Anforderung aktivieren oder deaktivieren können.

Hinweis:
Wenn Sie das neue Capability Integration Framework mit dem New York-Release verwenden möchten, müssen Sie das ServiceNow IntegrationHub Starter Pack Installer-Plugin installieren. Wenden Sie sich an den Kundensupport, um Unterstützung bei der Installation zu erhalten.

Unterstützte Anwendungsversionen

Ab Security Incident Response 10.0 werden die folgenden Integrationen unterstützt:

Anwendung	Mindestversion erforderlich
Integration der Hybridanalyse von Security Operations	10.0.0
PhishTank-Integration für Security Operations	10.0.0
Security Operations ThreatCrowd Integration	10.0.0
Integration von CrowdStrike Intelligence in Security Operations	10.0.0
Security Operations „Have I Been Pwned?“ Integration	10.0.0
Security Operations Metadefender Integration	10.0.0
Security Operations Recorded Future Integration	10.0.0
Security Operations VirusTotal-Integration	10.0.0
Security Operations – WhoIs-Integration umkehren	10.0.0

Ab Security Incident Response 10.4 werden die folgenden Integrationen unterstützt:

Anwendung	Mindestversion erforderlich
RiskIQ-Integration von Security Operations	10.0.0
Shodan-Integration für Security Operations	10.0.0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Mindestversion erforderlich
WhoIs-Integration von Security Operations	10.0.0
Security Operations Carbon Black Integration	10.3.1
Security Operations Splunk Search Integration	10.3.0
Integration der ArcSight-Protokollierung in Security Operations	10.3.0
Security Operations – McAfee ESM-Integration	10.3.0
Elasticsearch-Integration für Security Operations	10.3.0
Security Operations IBM QRadar Integration	10.3.1
CrowdStrike Falcon-Host für Security Operations	10.3.0

Enthaltene Komponenten

Das neue Framework für Fähigkeitsintegrationen enthält die folgenden Komponenten:

- **Fähigkeiten**: Alle der folgenden Fähigkeiten, die heute im Produkt als Workflows vorhanden sind, wurden mit Flows neu gestaltet:
  - **Anforderung blockieren**: Bietet eine Möglichkeit, erkennbare Elemente zu blockieren, die einem Security Incident an einer Firewall, einem Webproxy oder einem anderen Kontrollpunkt zugeordnet sind. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.
  - **E-Mails suchen und löschen**: Bietet eine Möglichkeit, einen E-Mail-Server während einer Sicherheitsuntersuchung zu durchsuchen und bei Bedarf E-Mails vom Server zu löschen.
  - **Configuration Item ergänzen**: Bietet eine allgemeine Möglichkeit, Configuration Items mit zusätzlichen Informationen aus verschiedenen Quellen zu ergänzen. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um die einem Security Incident zugeordneten Daten anzureichern.
  - **Erkennbares Element anreichern**: Bietet eine allgemeine Möglichkeit, erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen Quellen zu ergänzen. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.
  - **Ereigniserfassung**: Bietet eine allgemeine Möglichkeit, einen Security Incident zu erstellen, indem Ereignisse aus einer Integrationsquelle einem Security Incident zugeordnet werden.
  - **Netzwerkstatistiken abrufen**: Ruft eine Liste aktiver Netzwerkverbindungen von einem Endpunkt oder Host ab. Diese Funktion wird bei Untersuchungen für die Anreicherung von Incidents verwendet.
  - **Laufende Prozesse abrufen**: Ruft eine Liste laufender Prozesse von einem Endpunkt oder Host ab. Diese Funktion wird bei Untersuchungen für die Anreicherung von Incidents verwendet.
  - **Host isolieren**: Bietet eine Möglichkeit, einen Endpunkt oder Host zu isolieren, der einem Security Incident zugeordnet ist. „Host isolieren“ wird für ein Configuration Item (CI) ausgeführt.
  - **In Beobachtungsliste veröffentlichen**: Bietet eine Möglichkeit, erkennbare Elemente, die einem Security Incident zugeordnet sind, einer Beobachtungsliste hinzuzufügen, die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsereignisse überwacht und Warnungen generiert. Diese Fähigkeit wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.

- **Sichtungssuche**: Durchsucht verschiedene SIEMs oder andere Protokollspeicher nach Instanzen von erkennbaren Elementen. Diese Funktion wird verwendet, um das Vorhandensein schädlicher IoCs in Ihrer Umgebung festzustellen.
- **Bedrohungssuche**: Führt Threat Intelligence-Suchen durch, um zu bestimmen, ob ein bestimmtes erkennbares Element einer bekannten Sicherheitsbedrohung zugeordnet ist. Diese Fähigkeit wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.

- **Neue Tabellen**:
  - sn_sec_cmn_capability: Fähigkeit und Flow, die die Fähigkeit implementiert.
  - sn_sec_cmn_capability_implementation: Der tatsächliche Implementierungs-Flow, der die Services der Fähigkeit bereitstellt.
  - sn_sec_cmn_capability_execution: Der Ausführungsdatensatz für eine Fähigkeit zur Laufzeit.
  - sn_sec_cmn_capability_implementation_execution: Der Ausführungsdatensatz für eine Fähigkeitsimplementierung zur Laufzeit.
  - sn_sec_cmn_filter_condition: Die Filterbedingungen, die zur Laufzeit auf die Fähigkeit oder eine Fähigkeitsimplementierung angewendet werden können.
- **Skript einschließen**: CapabilityProcessor: Verarbeitet den gesamten Verarbeitungscode für das Framework.
- **Quotengrenze**: Max. gleichzeitige Anforderungen pro Zeitraum: Definiert, wie viele Integrationen parallel ausgeführt werden können.
- **Implementierung der Prozessfähigkeit für geplante Aufgaben**: Wird alle 15 Sekunden ausgeführt und kann auf der Seite mit den Sicherheitsadministrationseigenschaften deaktiviert werden (**Security Incident** > **Administration** > **Eigenschaften**.
  - Aktiviert oder deaktiviert die geplante Aufgabe Fähigkeitsimplementierungen verarbeiten: Diese Aufgabe plant und verwaltet automatisch Ausführungs-Flows für Fähigkeitsimplementierungen.
  - Aktiviert oder deaktiviert automatisierte Suchen oder Ergänzungen: Einstellung, mit der die geplante Aufgabe aktiviert oder deaktiviert wird, die die automatisierte Bedrohungssuche oder die Anreicherung von erkennbaren Elementen durchführt, wenn erkennbare Elemente zu Security Incidents im aktuellen Fähigkeits-Framework hinzugefügt werden.
  - Aktiviert oder deaktiviert die geplante Aufgabe „Nach erkennbaren Security Incident-Elementen suchen“: Diese Aufgabe plant automatisch eine Aufgabe für die Bedrohungssuche oder die Ergänzung erkennbarer Elemente, wenn erkennbare Elemente zu einem Security Incident hinzugefügt werden.

Konfigurationen im neuen Fähigkeiten-Framework

In diesem Abschnitt werden die im neuen -Framework verfügbaren Konfigurationen beschrieben.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, flow_designer, action_designer

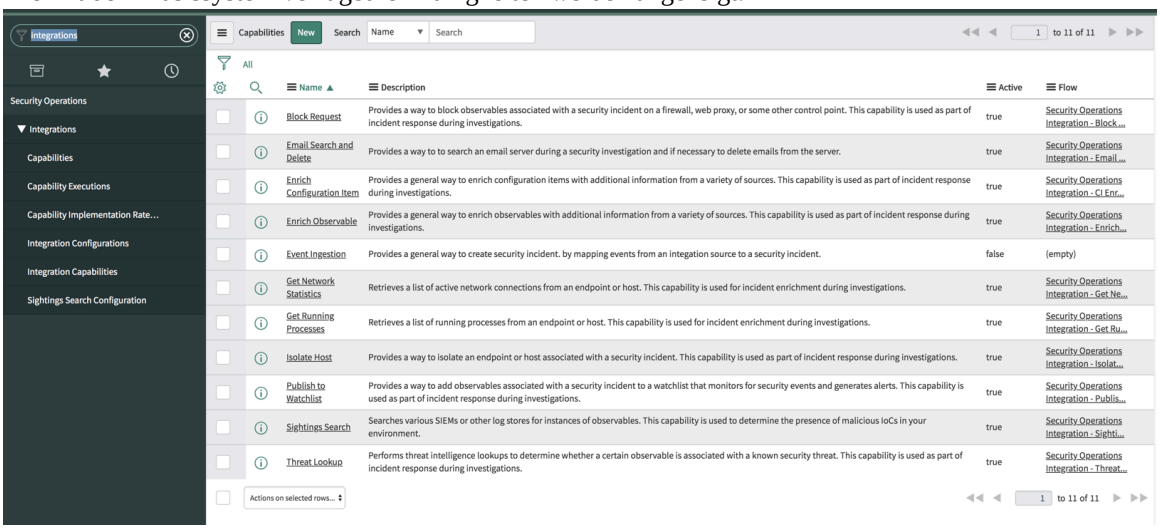
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Fähigkeiten**.

   Hinweis:
   Version 10.4: Ab Security Incident Response 10.4 wurde der Menüname **Fähigkeiten** in **Integrationsfähigkeiten (Flows)**geändert.

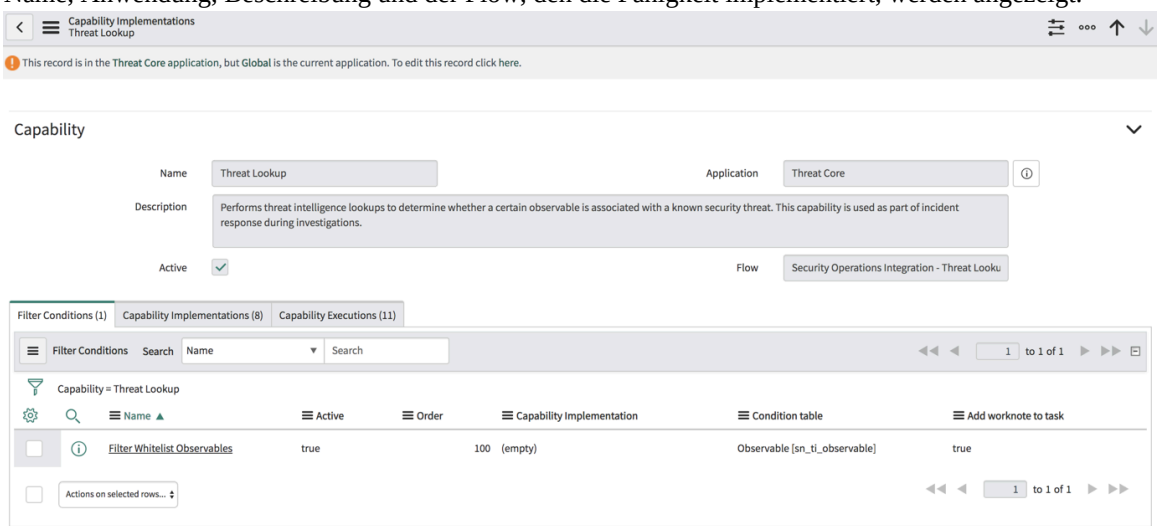
2. Die mit dem Basissystem verfügbaren Fähigkeiten werden angezeigt.



   Hinweis:

   Dies sind die mit dem Basissystem bereitgestellten Funktionen. Sie können die Fähigkeiten verwenden oder sie nach Bedarf anpassen. In den folgenden Schritten wird beschrieben, wie Sie eine Fähigkeit und die für die Fähigkeit implementierten Integrationen konfigurieren.

3. Klicken Sie auf den Link in der Spalte Name, um eine Fähigkeit zu konfigurieren.
   Name, Anwendung, Beschreibung und der Flow, den die Fähigkeit implementiert, werden angezeigt.



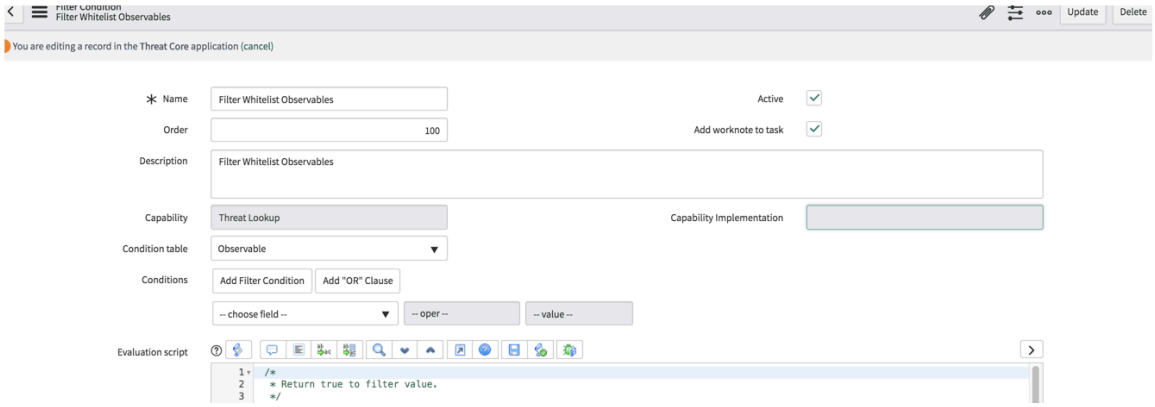
4. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Fähigkeit zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Filterbedingungen auf Fähigkeitsebene**: Wenn eine Integrationsfähigkeit einen Flow implementiert, werden die mit dem Flow verknüpften Filterbedingungen ausgeführt, bevor der Fähigkeits-Flow gestartet wird. Beispielsweise enthält die Fähigkeit „Bedrohungssuche“ wie oben dargestellt die Bedingung Filter Allowlisted Observables. Klicken Sie auf den Link Name, um die Filterbedingung zu bearbeiten.

  Hinweis:
  Aktivieren Sie das Kontrollkästchen **Arbeitsnotiz zu Aufgabe hinzufügen,** um Arbeitsnotizen hinzuzufügen und Informationen zu den verwendeten Filterbedingungen hinzuzufügen.



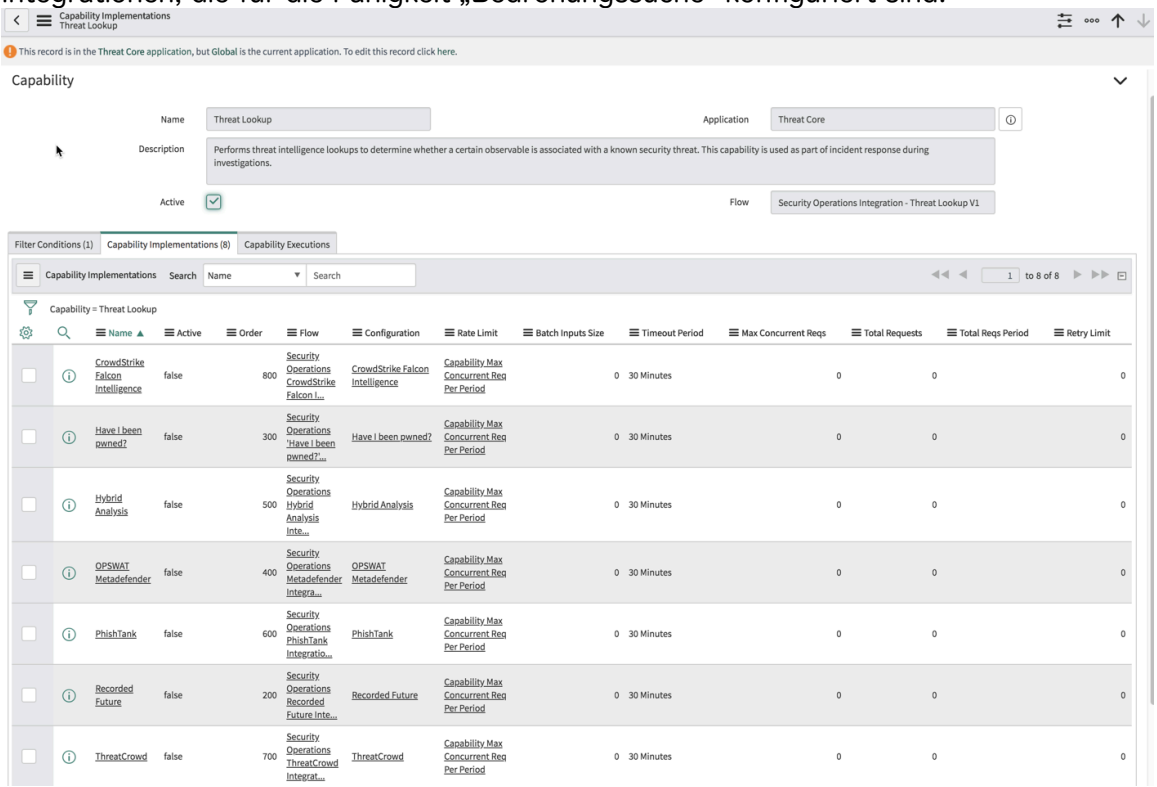
  Sie können entweder Filterbedingungen oder ein Skript oder eine Kombination aus beidem definieren. Im obigen Beispiel wird ein Skript verwendet, um die Filterbedingungen zu definieren. Wenn der Fähigkeits-Flow ausgeführt wird, sucht das Skript nach erkennbaren Elementen auf der Zulassungsliste und entfernt sie aus der Tabelle.

  Hinweis:
  Die hier festgelegten Filterbedingungen gelten für alle aktiven Integrationen, die auf der Registerkarte **Fähigkeitsimplementierungen** definiert sind.

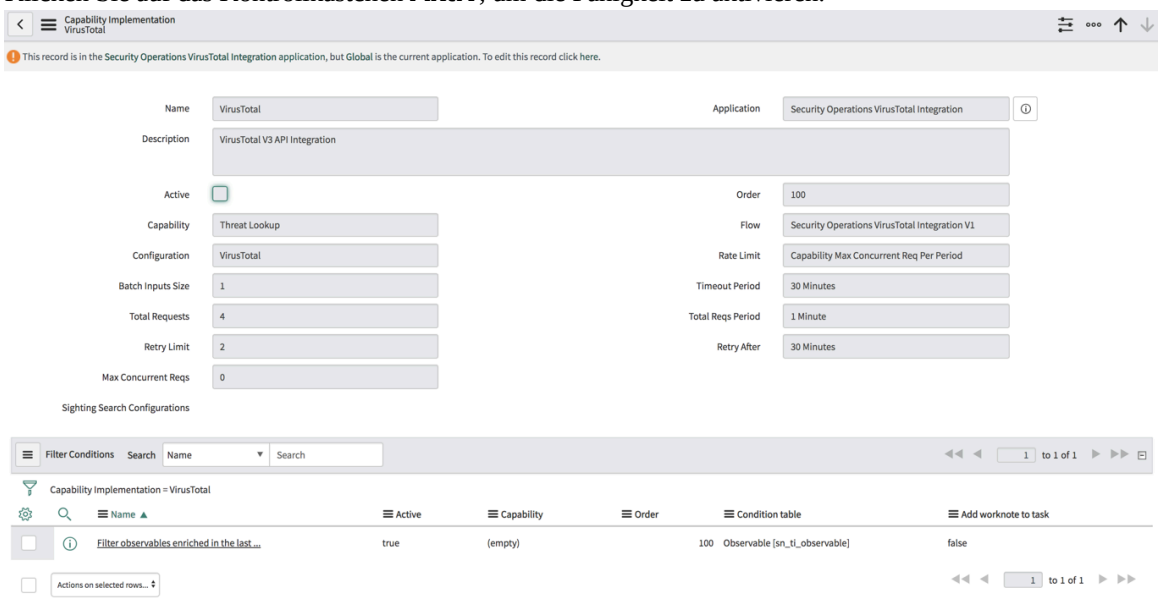
- **Fähigkeitsimplementierungen**: Klicken Sie auf die Registerkarte **Fähigkeitsimplementierungen**. Die Implementierungen (Integrationen), die für die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fähigkeit konfiguriert wurden, werden angezeigt. Das folgende Beispiel zeigt die Integrationen, die für die Fähigkeit „Bedrohungssuche“ konfiguriert sind:



5. Klicken Sie auf den Link Name, um die Fähigkeitsimplementierung anzuzeigen.
   Name, Anwendung, Beschreibung und der Flow, den die Fähigkeit implementiert, werden angezeigt.
6. Klicken Sie auf das Kontrollkästchen **Aktiv**, um die Fähigkeit zu aktivieren.



Sie können die folgenden Details angeben:

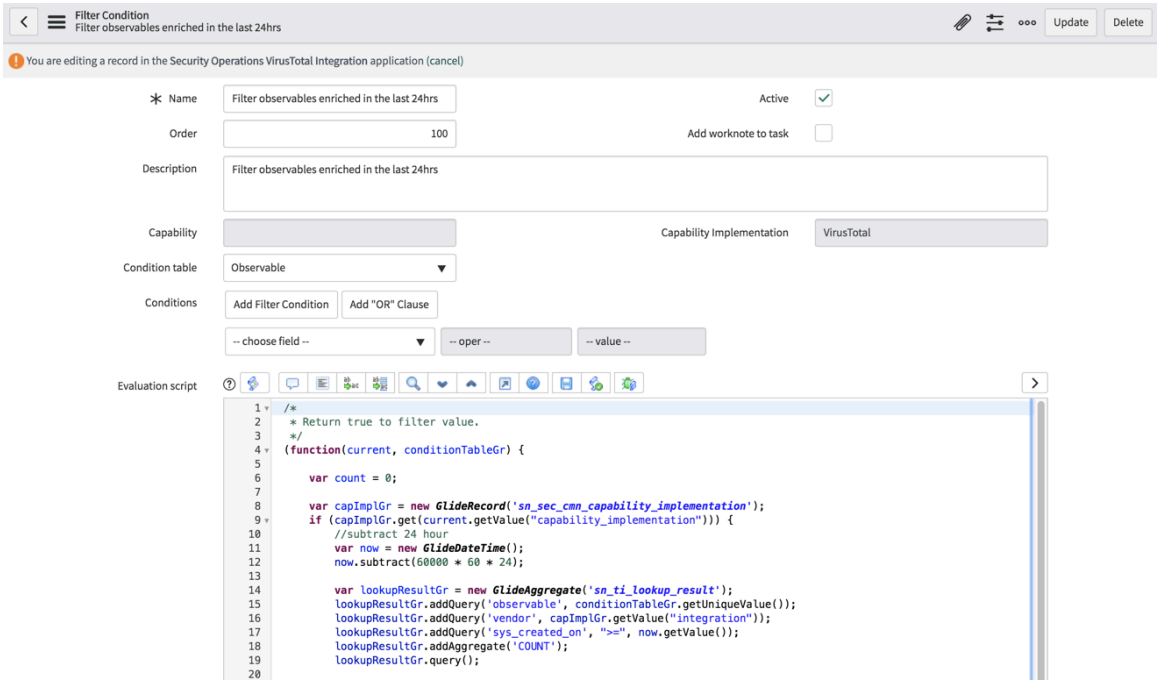
Feldname	Beschreibung
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese Integration zu deaktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
	Hinweis: Wenn Sie diese Integration mithilfe der Integrationskachel in konfigurieren, finden Sie in **Security Operations** > **Integrationen** > **Integrationskonfigurationen**Seite wird diese Kennzeichnung automatisch auf **Aktiv**gesetzt.
Bestellung	Gibt die Reihenfolge an, in der die Integrationen ausgeführt werden.
Fähigkeit	Die von dieser Integration implementierte Fähigkeit.
Flow	Der Subflow, der die Fähigkeit implementiert.
Konfiguration	Die Integrationskonfiguration für diese Fähigkeit. **Hinweis:** Dies ist anfänglich auf die mit dem Basissystem bereitgestellte Standardkonfiguration festgelegt. Wenn eine Integration mithilfe der Integrationskachel auf der Seite **„Integrationskonfigurationen“** konfiguriert wird, wird dieser Wert automatisch auf die neu erstellte Konfiguration zurückgesetzt.
Quotengrenze	Gibt die Anzahl der Integrationen an, die zur Laufzeit ausgeführt werden können (parallel oder pro Zeiteinheit).
Batch-Eingabegröße	Die Batch-Eingabegröße für jede Ausführung. Beispielsweise können Sie für eine Sichtungssuche-Integration die erkennbaren Elemente in Batches von 50 gruppieren, damit die generierten Abfragen nicht zu groß werden. 0 gibt an, dass es keine Begrenzung gibt.
Zeitüberschreitungszeitraum	Die maximale Dauer, bevor der Fähigkeitsimplementierungs-Flow abgebrochen wird. 0 gibt an, dass es keine Zeitüberschreitung gibt.
Anforderungen insgesamt	Die Gesamtzahl der Anforderungen zur Implementierungsausführung. Dieses Feld kann in Verbindung mit dem Feld Gesamtanforderungszeitraum verwendet werden, um die Anzahl der Anforderungen an den Service zu begrenzen. Sie können beispielsweise die Anzahl auf 4 Anforderungen pro Minute begrenzen.
Anforderungen insgesamt im Zeitraum	Die Gesamtzahl der pro Zeitraum zulässigen Ausführungsanforderungen.
Wiederholungsbegrenzung	Die Anzahl der zulässigen Wiederholungen für eine fehlgeschlagene Ausführungsanforderung. Dieser Grenzwert gilt, wenn in Ihrer Integration die **Wiederholungskennzeichnung** festgelegt ist, um eine Ausführungsanforderung zu wiederholen, wenn eine Bedingung erfüllt ist. Eine Wiederholungsanforderung wird beispielsweise gestellt, wenn Sie Ihr Lizenzlimit für diesen Service für einen bestimmten Zeitraum überschritten haben oder der Service ausgefallen ist.
Wiederholen nach	Der Zeitraum, nach dem versucht wird, eine fehlgeschlagene Ausführungsanforderung zu wiederholen.
Max. gleichzeitige Anforderungen	Die maximale Anzahl gleichzeitiger Anforderungen zur Implementierungsausführung. 0 bedeutet keine Begrenzung.
Sichtungssuchkonfigurationen	Die standardmäßigen Sichtungssuchabfragen, die ausgeführt werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie auf den Link Name im Abschnitt Filterbedingungen, um die für die Implementierung definierten Bedingungen zu konfigurieren. Fügen Sie Filterbedingungen hinzu, oder löschen Sie sie, ändern Sie das Skript bei Bedarf, und aktualisieren Sie den Datensatz.



Mittels des neuen Fähigkeiten-Frameworks mit einer installierten Integration

In diesem Abschnitt wird beschrieben, wie Sie das neue -Framework für eine vorhandene -Integration verwenden.

Führen Sie die folgenden Schritte aus, um eine bereits installierte und konfigurierte Integration (siehe Liste der unterstützten Integrationen in Unterstützte Integrationen und Komponenten) für die Verwendung des neuen Fähigkeits-Frameworks zu aktivieren.

Hinweis:
Das mit Security Incident Response 10.0.2 verfügbare Integration Capability Framework 2.0 unterstützt Implementierungen der Fähigkeiten **„Bedrohungssuche“** und **„Erkennbares Element anreichern“**. Implementierungen für andere Fähigkeiten werden in einem zukünftigen Release verfügbar gemacht.

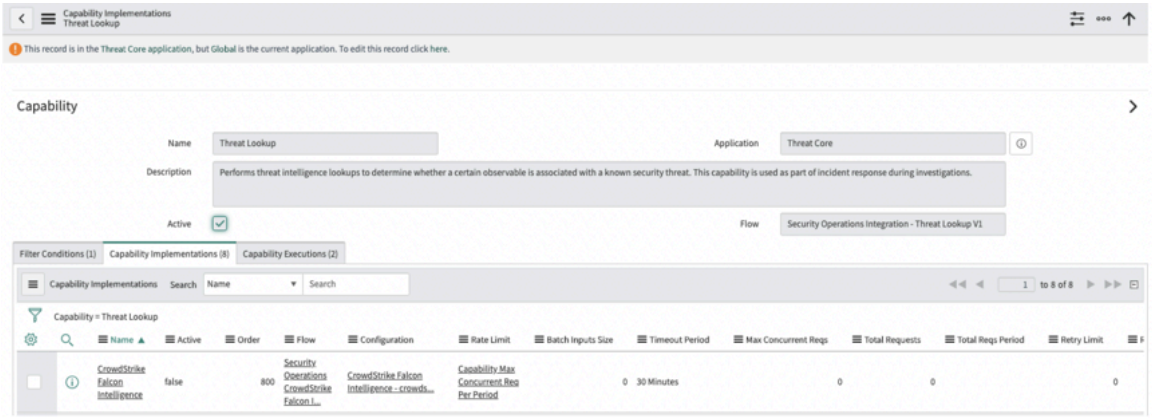
Bevor Sie beginnen

- Erforderliche Rolle: sn_si.admin
- Security Incident Response 10.0.2

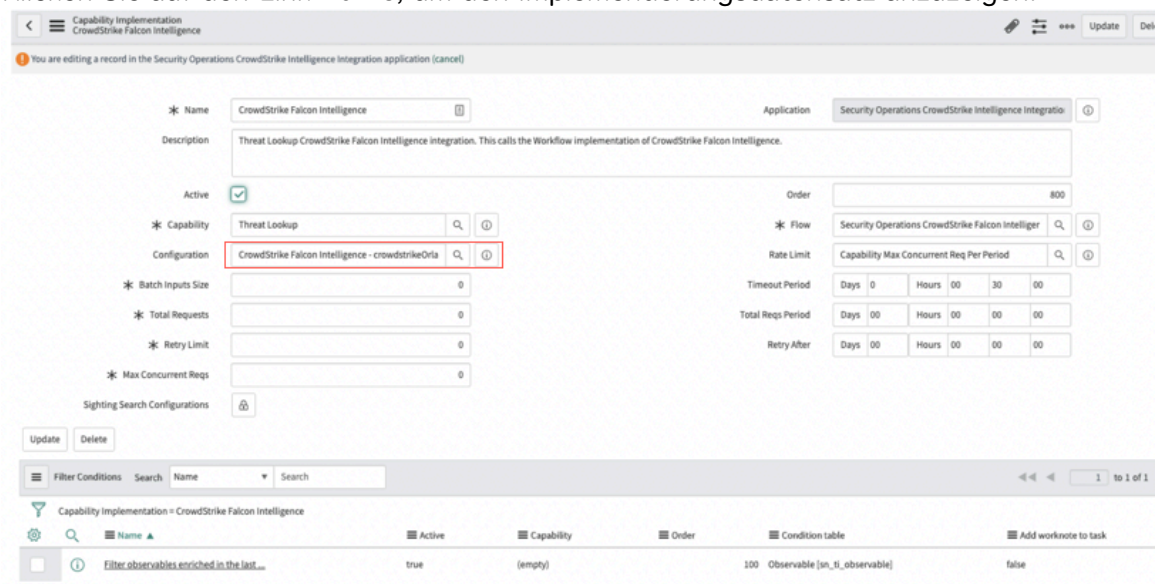
1. Navigieren zu **Security Operations** > **Integrationen** > **Fähigkeiten**.
2. Klicken Sie auf die Fähigkeit **zur Bedrohungssuche**.
3. Klicken Sie auf die Registerkarte Fähigkeiten-Implementierung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

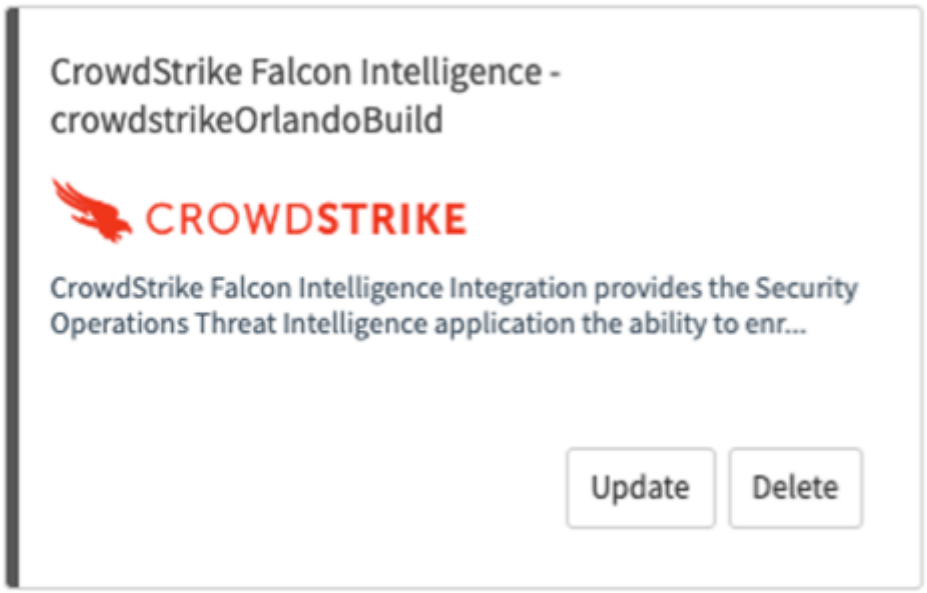


4. 4. Zeigen Sie den Datensatz „Fähigkeitsimplementierung“ für die Integration an, die Sie interessiert (Beispiel: Crowdstrike Falcon Intelligence). Die Spalte **„Aktiv“** muss den Wert **False**aufweisen.
5. Klicken Sie auf den Link **Name**, um den Implementierungsdatensatz anzuzeigen.



6. Aktivieren Sie die Checkbox **Aktiv**.
7. Stellen Sie sicher, dass der Implementierungsdatensatz auf den richtigen Konfigurationsdatensatz (den Kachelnamen für die Integration in) verweist **Integrationskonfigurationen** > **Konfigurationen anzeigen (Ja)**) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Die Implementierung von ist für die Verwendung mit dem neuen -Framework aktiviert.

Hinweis:
Alle unterstützten Integrationen werden bei der Installation mit Security Incident Response 10.0.2 automatisch unter dem neuen Integration Capability Framework aktiviert.

Verwenden des neuen Fähigkeits-Frameworks mit einem Flow

Führen Sie die folgenden Schritte aus, um einen Flow zu erstellen und den vom neuen Fähigkeits-Framework bereitgestellten Subflow aufzurufen.

Vorbereitungen

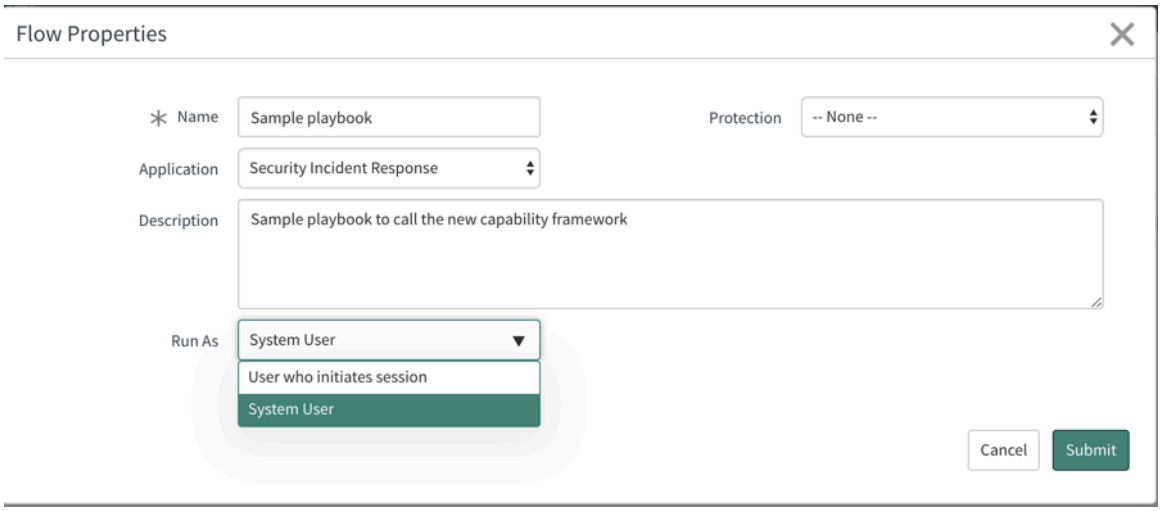
- Erforderliche Rolle: sn_si.admin, flow_designer, action_designer
- Installieren Sie eine der unterstützten Integrationen (siehe Unterstützte Integrationen und Komponenten).

In den folgenden Schritten wird beschrieben, wie Sie einen Beispiel-Flow erstellen und einen der mit dem neuen Fähigkeits-Framework bereitgestellten Subflows aufrufen.

Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer**.
2. Klicken Sie auf **Neu**, um einen neuen Flow zu erstellen und die erforderlichen Informationen für die Eigenschaften anzugeben.

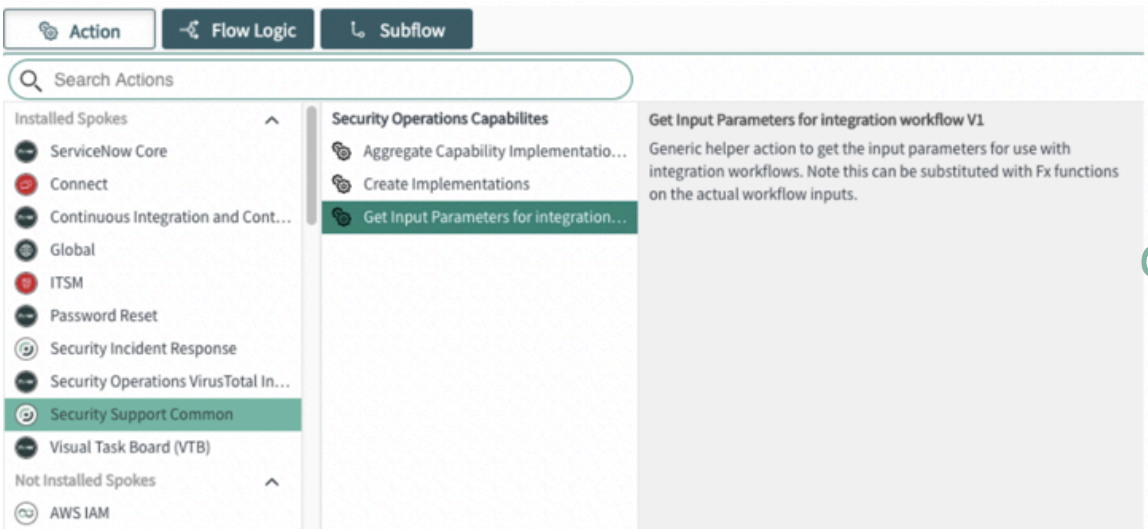
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wählen Sie in der Auswahlliste Ausführen als die Option **Systemanwender** aus (siehe Abbildung oben).

3. Wählen Sie eine Auslöserbedingung für den Flow aus (ein häufiger Auslöser ist die Erstellung eines Security Incident-Datensatzes für eine bestimmte Incident-Kategorie).

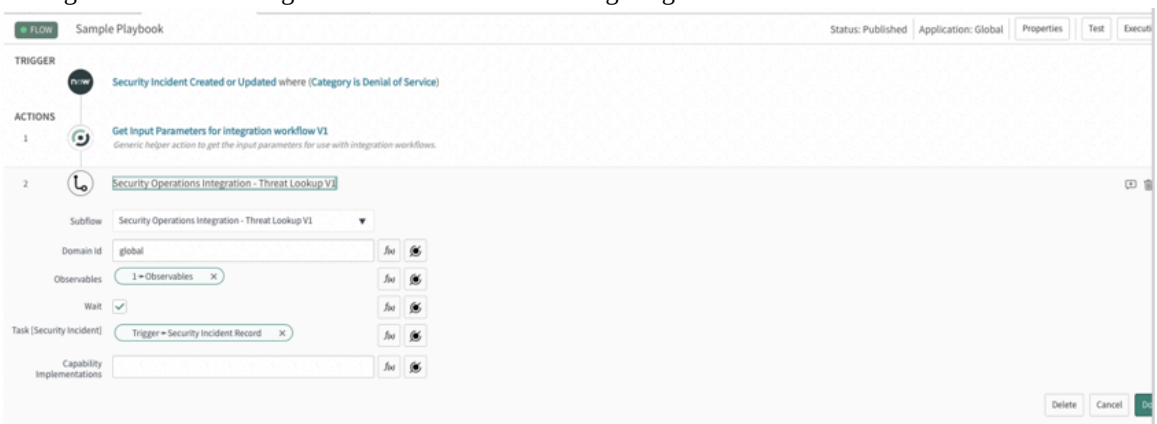
4. Wählen Sie in Schritt 1 des Flows eine Aktion aus, um Eingaben aus dem Security Incident zu erhalten (z. B. erkennbare Elemente).
Mit der Security Support Common Spoke können Sie eine Aktion aus den im Basissystem bereitgestellten Aktionen auswählen.



5. Wählen Sie in Schritt 2 einen Subflow aus (z. B. Bedrohungssuche).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Konfigurieren Sie den ausgewählten Subflow wie unten gezeigt:



7. Speichern und veröffentlichen Sie den Flow.

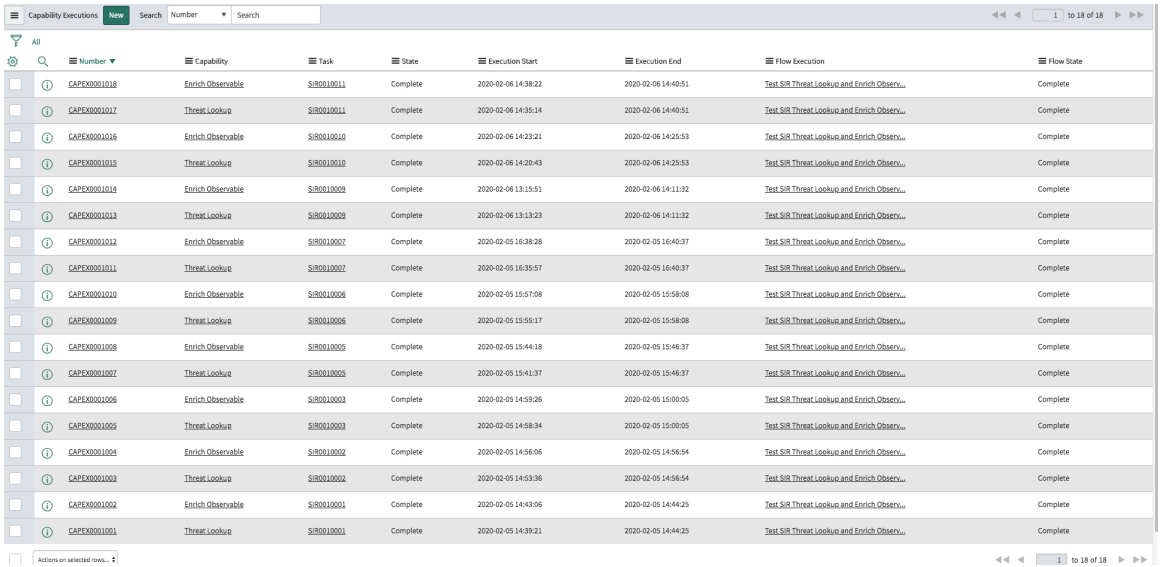
Flows zur Problembehandlung bei Integrationsfähigkeiten

Die Option Fähigkeitsausführungen bietet detaillierte Informationen zu jeder ausgeführten Fähigkeit.

Hinweis:
Abgeschlossene Ausführungen werden nach 30 Tagen archiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Security Operations** > **Integrationen** > **Fähigkeitsausführungen**.



2. Klicken Sie auf den Link Fähigkeitsausführungen, um zusätzliche Details anzuzeigen.

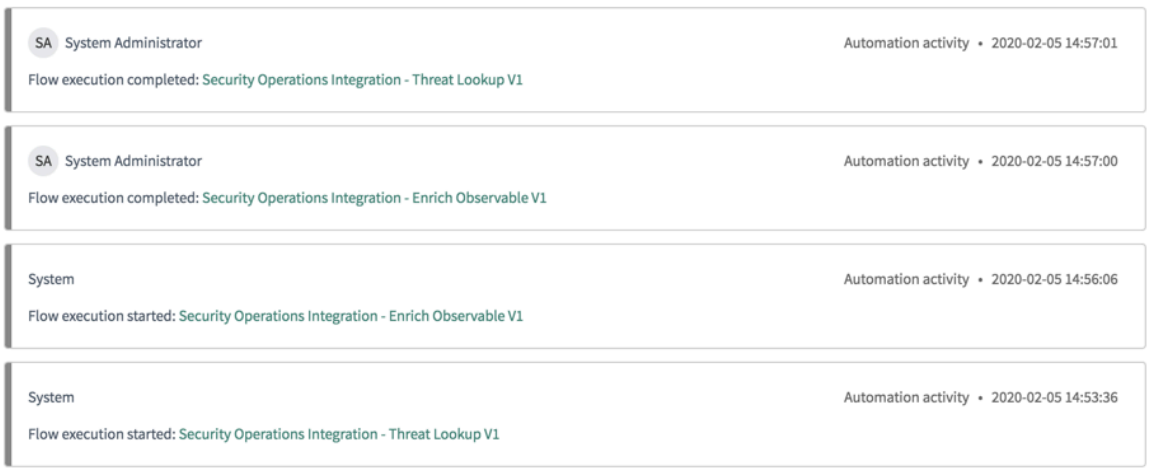
`Arbeitsnotizen zu Security Incident-Datensatz`

Wenn einem Security Incident erkennbare Elemente hinzugefügt wurden und die Auslöserbedingung für den Flow erfüllt ist, werden die Subflows „Bedrohungssuche“ und „Erkennbares Element ergänzen“ initiiert, und die folgenden Arbeitsnotizen werden dem Security Incident hinzugefügt:

- Flow-Ausführung gestartet: Security Operations Integration – Erkennbares Element ergänzen V1
- Flow-Ausführung abgeschlossen: Security Operations Integration - Enrich Observable V1
- Flow-Ausführung gestartet: Security Operations Integration – Bedrohungssuche V1
- Flow-Ausführung abgeschlossen: Security Operations Integration – Bedrohungssuche V1

Um diese Arbeitsnotizen anzuzeigen, melden Sie sich als Benutzer mit den Rollen *`sn_si.admin`* oder *`sn_si.analyst`*, *`flow_designer`*und *`action_designer`* an.

Navigieren Sie zur Datensatzseite des Security Incidents, und klicken Sie auf diese Arbeitsnotizen, um die Details zur Flow-Ausführung anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST APIs für die Integration von Drittparteien in Security Operations

Das Basissystem Security Operations enthält eine Reihe von REST APIs mit Skript, mit denen Kunden und Partner problemlos eine Integration in eine vorhandene Security Operations -Bereitstellung durchführen können. Die APIs ermöglichen es Ihnen, Daten von außerhalb Ihres Systems zu sammeln (z. B. wird ein Python-Skript verwendet, um Daten von VirusTotal zu empfangen) und an Ihre -Instanz zurückzusenden.

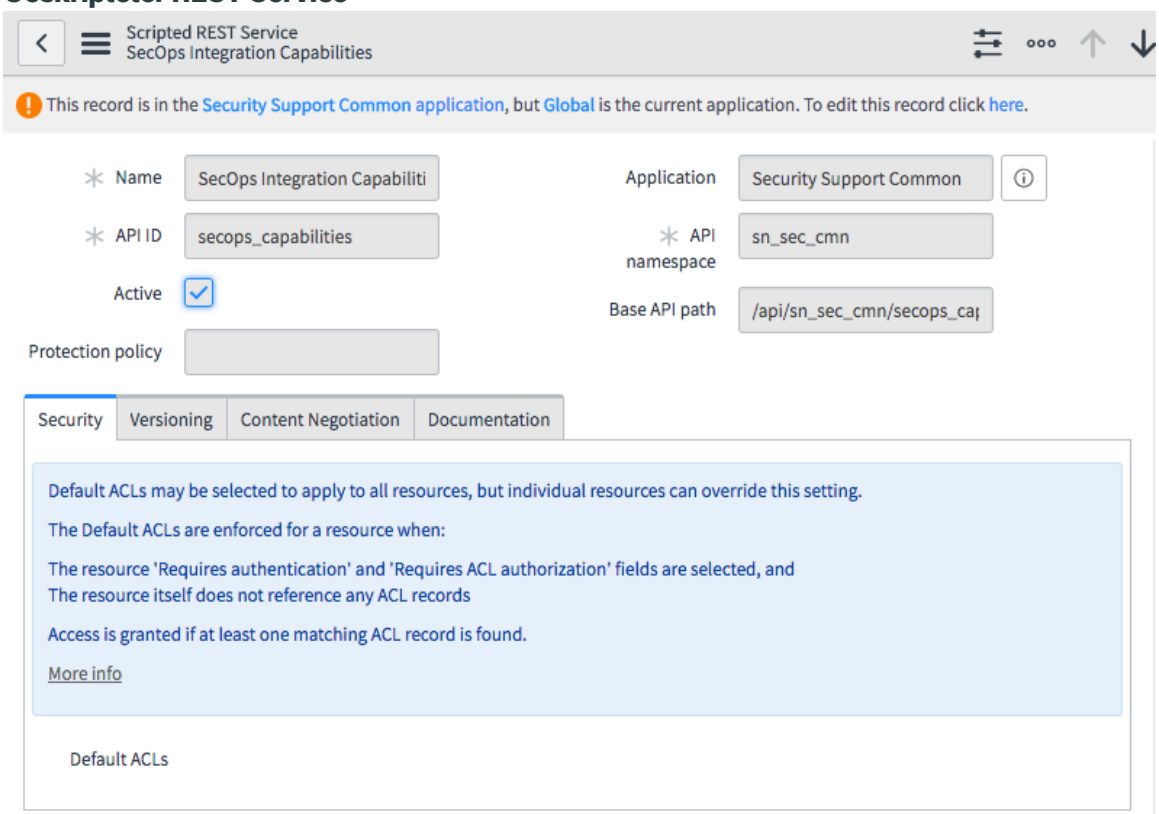
Skripts, die in fast jeder Sprache (z. B. Python) geschrieben sind, können mit den APIs verwendet werden, um kundenspezifische Prozesse auszuführen. Die Skripts müssen in einer Sprache geschrieben sein, die einen externen HTTP-Post-Aufruf durchführen kann. Wenn Sie beispielsweise eine Java-Anwendung haben, müssen Sie eine Bibliothek wie das Paket `java.net.HttpUrlConnection` verwenden, um einen HTTP-Aufruf zu erstellen und eine JSON-Zeichenfolge als Textkörper für die Nachricht zu übergeben.

Die API wird ausschließlich zum Hinzufügen von Daten verwendet, die außerhalb unseres Systems erfasst wurden. Wenn Sie beispielsweise ein VT-Python-Skript eingegeben und Daten von VT erhalten haben, können Sie diese Daten zurück an die SN-Instanz senden.

Authentifizierung

Alle Vorgänge innerhalb der API-Definitionen verwenden die von bereitgestellte Plattformauthentifizierung Funktion für den Betriebvon geskripteten REST APIs. Um darauf zuzugreifen, navigieren Sie zu **System-Webservices** > **Scripted Web Services** > **Scripted REST APIs** und suchen Sie die **SecOps Integration Capabilities** API.

Geskripteter REST-Service



Der Benutzer und die Domäne des Benutzers sind im Kontext der API sofort verfügbar. Datensätze können an einen Benutzer gebunden, ein Audit-Pfad eingerichtet und Domänentrennung erreicht werden. Da Sie als bestimmter Benutzer authentifiziert sind, können Sie außerdem verwenden GlideRecordSecure verwenden, um jeden nicht autorisierten Zugriff auf Daten zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autorisierung

Um den Datensatzerstellungsprozess für Benutzer außerhalb der Anwendung Security Operations zu schützen, benötigen Sie die Rolle sn_sec_cmn.api_write. Nur Benutzer mit dieser Rolle können auf die APIs zugreifen.

Konfigurationsanforderungsparameter

Die folgenden Anforderungsparameter sind verfügbar.

Name	Standard	Beschreibung
ignorieren_obligatorische_Felder	falsch	Bei Festlegung auf „wahr“ wird der Datensatz beibehalten, auch wenn Pflichtfelder nicht ausgefüllt sind.
„include_wrap“	falsch	Bei Festlegung auf „wahr“ enthält die Antwort den von der Instanz bereitgestellten Standard-Wrapper für geskriptete REST APIs.
simple_response	falsch	Bei Festlegung auf wahr gibt die Antwort nur an, ob der Vorgang erfolgreich war.

Fehlerantworten

Die folgenden Fehlerantworten können auftreten.

Fehlermeldung	Wann tritt es auf?	Lösung
Ungenügender Zugriff	Anwender verfügt nicht über die Rolle sn_sec_cmn.api_write.	Fügen Sie dem Anwender die Rolle hinzu.
Ungültiger Beitragstext	Anforderungstext ist leer oder ein leeres Objekt.	Entsprechen der API-Definition.
Keine Felder angegeben	Zum Beibehalten bereitgestellte Datenfelder sind leer.	Entsprechen der API-Definition.
Pflichtfelder fehlen: x, y, z	Pflichtfelder fehlen.	Passen Sie sich an die Tabellendefinition der Zieltabelle an, oder setzen Sie **„ignore_mandtory_fields“** auf „wahr“.
Datensatz kann nicht beibehalten werden	Analysierter Datensatz kann nicht beibehalten werden.	GlideRecord-Einfügung () fehlgeschlagen, weitere Analyse ist erforderlich.
Unbekannter Fehler	Tritt auf, wenn kein bekannter Fehlerpfad verfolgt wurde.	Weitere Analysen sind erforderlich.

Anwendungsfall für CI-Ergänzung

Mit Ihren Drittanbieterskripts können Sie zur CI-Ergänzung in die Tabelle „Configuration Item Enrichment“ [sn_sec_cmn_ci_enrichment_result] schreiben. Die Ergänzungsdatensätze basieren auf vorhandenen Funktionen, die detaillierte Informationen zu einem Datensatz aus einer Drittparteiquelle bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hier werden Beispiele für Anforderungen und Antworten für den Anwendungsfall „CI-Ergänzung“ angezeigt.

Erstellungsanforderung für CI-Ergänzung

```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```

Erstellungsantwort für CI-Ergänzung

```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```

Anwendungsfall für Ergänzung erkennbarer Elemente

Mit Ihren Drittanbieterskripts können Sie zur Anreicherung erkennbarer Elemente in die Tabelle „Ergebnis für Ergänzung erkennbarer Elemente “ [sn_ti_observable_enrichment_result] schreiben. Die Ergänzungsdatensätze basieren auf vorhandenen Funktionen, die detaillierte Informationen zu einem Datensatz aus einer Drittparteiquelle bereitstellen.

Beispielanforderungen und -antworten für den Anwendungsfall Ergänzung erkennbarer Elemente werden hier angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellungsanforderung zur Ergänzung erkennbarer Elemente

```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```

Erstellen-Antwort für Anreicherung erkennbarer Elemente

```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```

Automatische Übersetzung

Hinweis:

Zusätzlich zur Anreicherung vorhandener Datensätze können Sie auch Security Operations Zuordnung von Ergänzungsdaten verwenden, um Tabellen neue Datensätze hinzuzufügen, indem Sie eine **„richment_mapping_id“** für eine vorhandene Ergänzungszuordnung und eine entsprechende **„raw_data“** -Zeichenfolge übergeben, die vom Zuordnungsprozess analysiert werden kann.

Anwendungsfall für die Bedrohungssuche

Mithilfe von Drittanbieterskripts können Sie in die Tabelle „Ergebnis der Bedrohungssuche“ [sn_ti_lookup_result] schreiben, um Ergebnisse der Bedrohungssuche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu erhalten. Die Suchdatensätze basieren auf vorhandenen Funktionen, die detaillierte Informationen zu einem Datensatz aus einer Drittanbieterquelle bereitstellen.

Beispielanforderungen und -antworten für den Anwendungsfall „Bedrohungssuche“ werden hier angezeigt.

Erstellungsanforderung für Bedrohungssuchen

```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellungsantwort für Bedrohungssuchen


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Integrationsfähigkeiten

Das Integrationsfunktionen -Framework bietet eine konsistente -Architektur zur Unterstützung der Interoperabilität mit Drittanbieterintegrationen. Diese abstrahierte Schnittstelle und dieses Datenmodell isolieren Integrationen von Änderungen an der Kernanwendung und stellen eine konsistente Experience für ähnliche Arten von Integrationen sicher.

Alle Integrationsfähigkeiten werden in der Tabelle „Integrationsfähigkeit “ [sn_sec_cmn_integration_capability] beibehalten. Integrationsfähigkeits-Flows können nicht einzeln ausgeführt werden und erfordern den Start eines Implementierungs-Flows. Jedes Plugin, das eine Implementierung der Fähigkeit bereitstellt, fügt seine Implementierung der untergeordneten Tabelle Integration Capability Implementation [sn_sec_cmn_integration_capability_implementation]hinzu.

Die -Implementierung gibt den auszuführenden Flow, die zugehörige Integration (Plugin-ID) und die von ihr implementierte Fähigkeit an. Diese Flows können mit dem Startprogramm für parallele Flows parallel ausgeführt werden. Im Basissystem ist jedoch die sequenzielle Ausführung der Standard. Bei Bedarf können Sie die Reihenfolge der Ausführung ändern.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Security Operations-Integration: Blockierungsanforderungsfunktion

Die Fähigkeit „Aktion blockieren“ blockiert erkennbare Elemente, die einem Security Incident zugeordnet sind, an einer Firewall, einem Webproxy oder einem anderen Kontrollpunkt mithilfe von Implementierungs-Flows. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Fähigkeit „Anforderung blockieren“ hat den Flow Security Operations Integration – Anforderungs-Flow blockieren, der die zu blockierende Anforderung ausführt. Dieser Flow akzeptiert eine Liste von erkennbaren Elementen, findet implementierende Fähigkeiten und führt die Anforderung basierend auf dem konfigurierten Flow aus.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Blockierungsanforderung ausführen

Blockiert die Kommunikation mit erkennbaren Elementen, die einem Security Incident zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

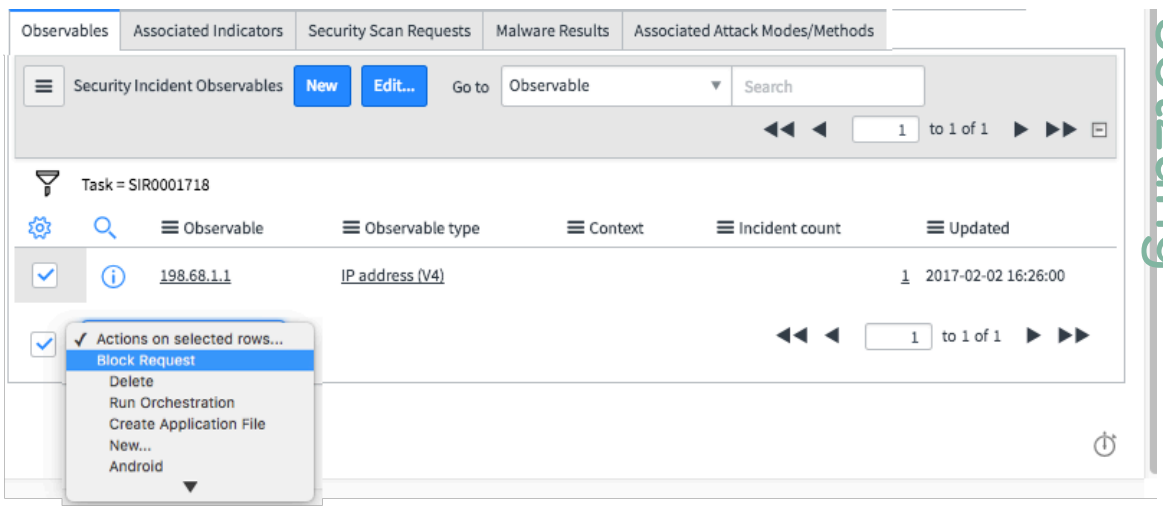
Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Der Flow **„Security Operations Integration – Block Request“** kann von einem Formular für erkennbare Elemente oder von der zugehörigen Liste „ **Erkennbare Elemente des Security Incident“** in einem Security Incident ausgelöst werden.

Dieses Beispiel zeigt eine Sperranforderung aus einem Security Incident.

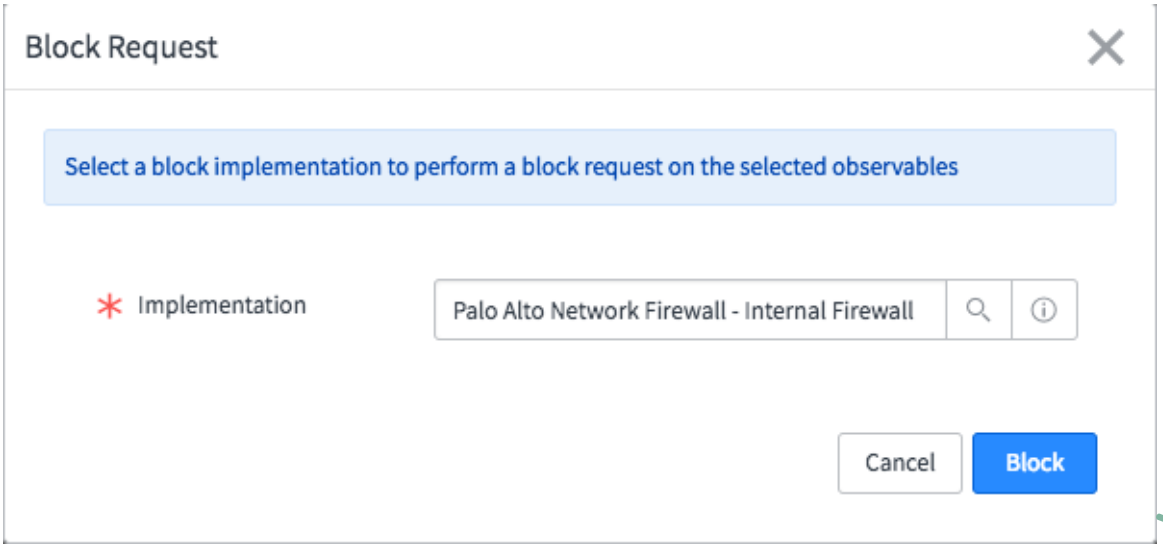
Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie erkennbare Elemente auf der Registerkarte **Zugehörige Liste** aus.
3. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen...** auf **Anforderung blockieren**.

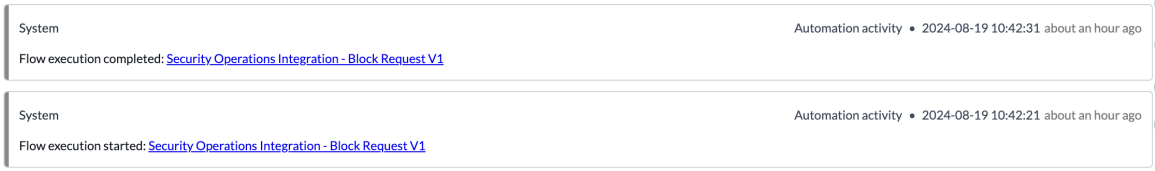


Das Dialogfeld wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Implementierung aus.
5. Klicken Sie auf **Block**.
   Das Audit der Flow-Ausführung wird im Abschnitt „Arbeitsnotizen“ angezeigt.



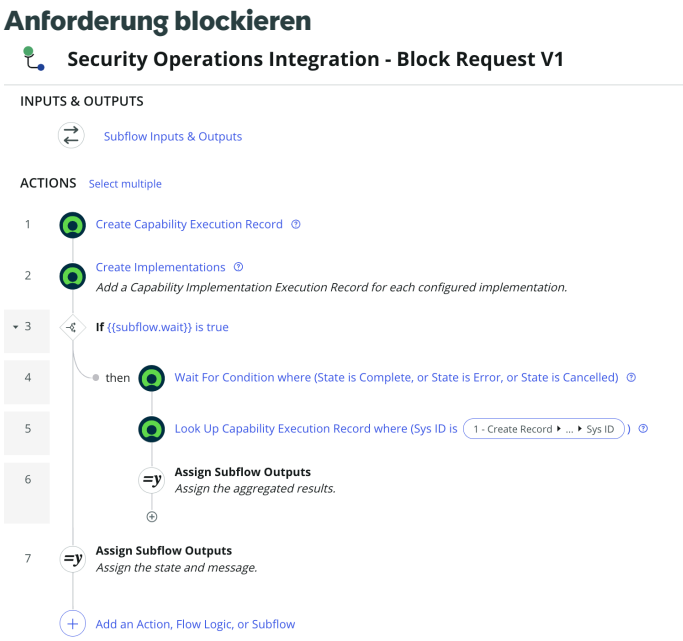
Security Operations Integration – Anforderungs-Flow blockieren

Der Flow „Security Operations Integration – Block Request“ ist ein allgemeiner Flow, der von Integrationen unabhängig ist. Es blockiert erkennbare Elemente, die einem Security Incident zugeordnet sind. Verwenden Sie diese, um eine Integration wie Palo Alto Networks – Firewallzu erfüllen.

Der Flow **„Security Operations Integration – Block Request“** kann auf einem Formular für erkennbare Elemente oder über die zugehörige Liste „ **Erkennbare Elemente des Security Incident“** in einem Security Incident ausgelöst werden. In einer Liste befindet sie sich im Dropdown-Aktionsmenü. Bei einem Formular handelt es sich um einen zugehörigen Link. Das Blockieren einer Anforderung ist nur verfügbar, wenn Sie eine Implementierung für die Funktion zum Blockieren von Anforderungen installiert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Security Operations-Integration – Funktion zum Suchen und Löschen von E-Mails

Die Fähigkeit „E-Mails suchen und löschen“ gibt die Anzahl der Bedrohungs-E-Mails aus einer E-Mail-Serversuche und optional Details für jede gefundene E-Mail zurück. Nachdem die E-Mail-Suche abgeschlossen ist, können Sie die E-Mails löschen.

Die Fähigkeit „E-Mails suchen und löschen“ hat einen Flow, der die Prozesse zum Suchen und Löschen von E-Mails ausführt.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt. Wenn keine der Implementierungen der Funktionen **„E-Mails suchen“ und „Löschen“** aktiv ist, wird der zugehörige Link **„E-Mail-Suche“** für einen Security Incident nicht angezeigt.

Security Operations Integration - Flow zum Suchen und Löschen von E-Mails

Der Flow „Security Operations Integration – E-Mails suchen und löschen“ gibt die Anzahl der Bedrohungs-E-Mails aus einer E-Mail-Serversuche und optional Details für jede gefundene E-Mail zurück. Nachdem die E-Mail-Suche abgeschlossen ist, können Sie die E-Mails löschen.

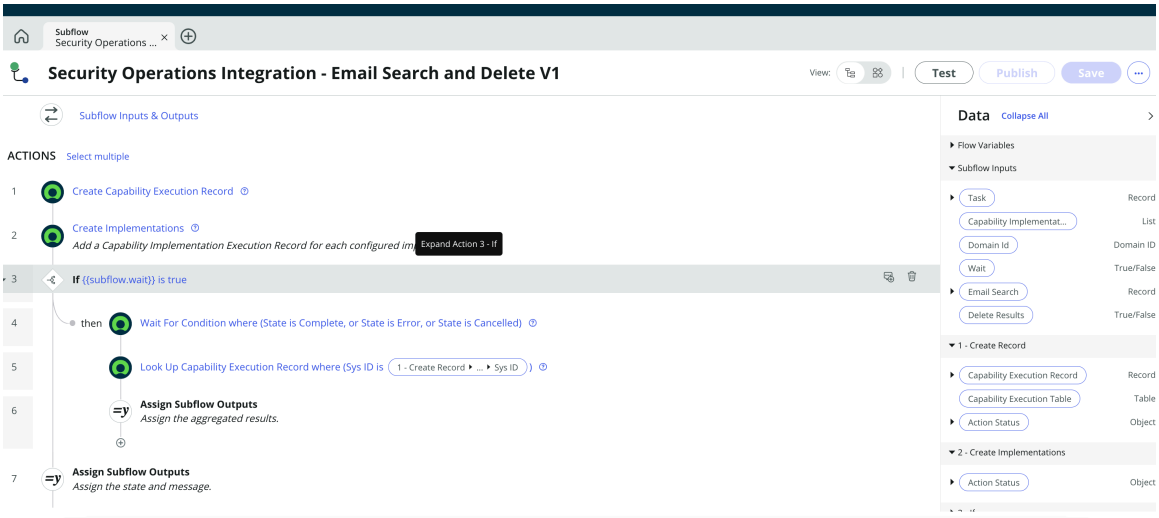
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Die Suchabfrage kann einige Zeit in Anspruch nehmen. Nachdem die Anzahl empfangen wurde, ist eine Genehmigung erforderlich, um E-Mails von einem E-Mail-Server zu löschen.

Dieser Flow wird durch die Schaltflächen **Von E-Mail-Servern löschen** und **Auf E-Mail-Servern suchen** im Formular **„E-Mail-Suche“** in einem Security Incident ausgelöst. Weitere Informationen finden Sie unter Suchen und löschen Sie Phishing-E-Mails.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mails suchen und löschen



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Die Flow-Prozessaktivitäten umfassen:

Aktion „Beginn der Ausführungsnachverfolgung (E-Mail-Suche)“.

Die Ausführungsaktion der Fähigkeit „Ausführungsnachverfolgung – Begin (E-Mail-Suche)“ erstellt einen Ausführungsnachverfolgungsdatensatz und markiert den Datensatzstatus als „Gestartet“. Diese Aktion wird von allen Fähigkeits- und Implementierungs-Flows verwendet, um ihren Status nachzuverfolgen.

Ergebnisse

Mögliche Ergebnisse für diese Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ausführungsnachverfolgungsdatensatz wurde erstellt.
Fehler	Ausführungsnachverfolgungsdatensatz konnte nicht erstellt werden.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
capabilityId	System-ID der ausgeführten Integrationsfunktionalität
Implementierungs-ID	System-ID der ausgeführten Implementierung der Integrationsfähigkeit.
Aufgaben-ID	System-ID für jede Aufgabe, die dem Flow zugeordnet ist.
flowContextId	Systembezeichner des zugeordneten Flow-Kontextdatensatzes. Wird vom System bereitgestellt.
FlowName	Name des Flows. Wird vom System bereitgestellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
parentCapabilityExcutionId	Systembezeichner des Audit-Datensatzes, von dem der Implementierungs-Flow gestartet wurde. Nur für Implementierungs-Flows für Integrationsfähigkeiten erforderlich, z. B. Splunk, Elasticsearch.
emailsearchId	Die sysid des E-Mail-Suchdatensatzes in der Tabelle „E-Mail-Suche“ [sn_sec_cmn_email_search].

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
capabilityExecutionId	System-ID des Ausführungsnachverfolgungsdatensatzes.

- Aktion „Unterstützte Sicherheitsfähigkeiten abrufen“.
- Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.

Security Operations-Integration: CI-Fähigkeit ergänzen

Mit der Fähigkeit „CI ergänzen“ können Sie Daten für Configuration Items ergänzen, die einem Security Incident zugeordnet sind.

Die Fähigkeit **„CI ergänzen“** hat den Flow Security Operations-Integration – Flow zur CI-Ergänzung. Wenn der Fähigkeits-Flow ausgeführt wird, werden zusätzliche Flows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die für die Anreicherung der ausgewählten CIs verwendet werden soll, oder Sie können die Anreicherung mit allen Implementierungen durchführen.

Hinweis:
Diese angereicherten Daten sind nicht der Typ von Daten, die Sie in Ihrer CMDB speichern möchten, da es sich um forensische Daten handelt, die für eine bestimmte Untersuchung spezifisch sind, z. B. die Durchführung eines Memdump-Vorgangs von einem CI. Stattdessen werden die Daten in der Tabelle „Configuration Item Enrichment“ [sn_sec_cmn_ci_enrichment_result] gespeichert.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Security Operations-Integration – Flow zur CI-Ergänzung

Mit dem Flow Security Operations-Integration – CI-Ergänzung können Sie Daten in Konfigurationselementen (Configuration Items, CI) ergänzen, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird von Security Incident Response auf zwei Arten ausgelöst.

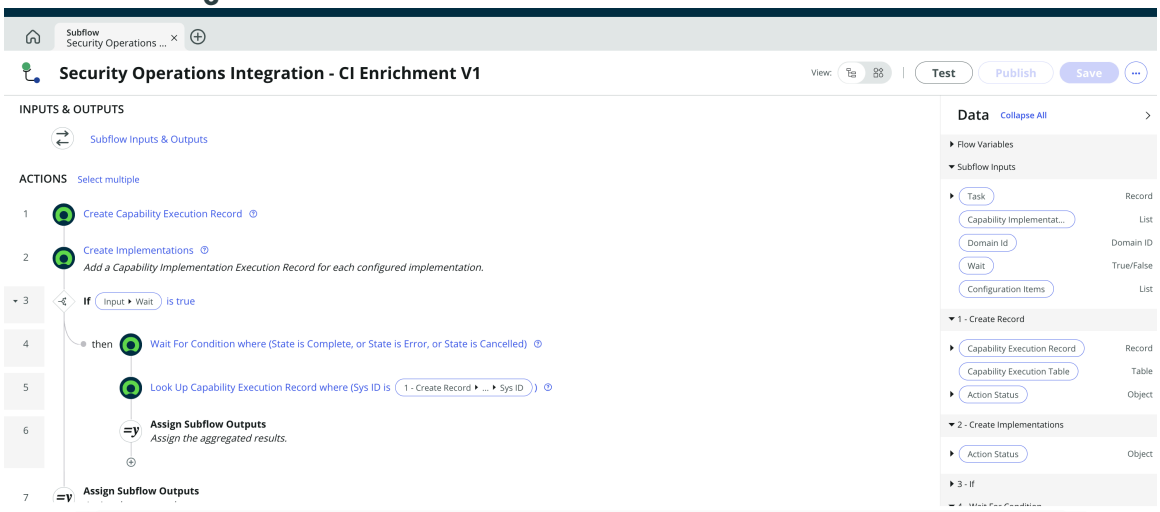
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- durch Auswahl eines oder mehrerer CIs auf der Registerkarte **Konfigurationselemente** (unter dem zugehörigen Link **Betroffene Elemente**) und Auswahl von **CI-Ergänzung ausführenin der Auswahlliste Aktionen für ausgewählte Zeilen**.
- indem Sie einen CI-Datensatz öffnen und auf den zugehörigen Link **CI-Ergänzung ausführen** klicken.

Anschließend können Sie mit beiden Methoden angeben, welche Implementierungen die ausgewählten CIs ergänzen sollen. Die zugehörigen Implementierungs-Flows werden ausgeführt, um die Anreicherung durchzuführen.

Hinweis:
Das Basissystem enthält keinen Implementierungs-Flow für diese Fähigkeit. Um CIs anzureichern, müssen Sie Ihren eigenen Implementierungs- Flow erstellen.

CI-Anreicherung



Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Zu den Flow-Prozessaktionen gehören:

- Ausführungsnachverfolgung: Flow-Aktion beginnen
- Security Operations-Integration – Flow zur CI-Ergänzung
- Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.
- Aktion „Unterstützte Sicherheitsfähigkeiten abrufen“.

Security Operations-Integration: Fähigkeit „Erkennbares Element ergänzen“.

Mit der Fähigkeit „Erkennbares Element anreichern“ können Sie erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen Quellen mithilfe von Implementierungs-Flows anreichern. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.

Die Fähigkeit „Erkennbares Element anreichern“ hat den Flow Security Operations-Integration – Flow „Erkennbares Element anreichern“.. Wenn der Fähigkeits-Flow ausgeführt wird, werden zusätzliche Flows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die zur Ergänzung der ausgewählten erkennbaren Elemente verwendet wird, oder Sie können die Ergänzung mit allen Implementierungen durchführen, die den unterstützten erkennbaren Elementen entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Security Operations-Integration – Flow „Erkennbares Element anreichern“.

Mit dem Subflow „Security Operations Integration – Erkennbares Element anreichern“ können Sie erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen Quellen mithilfe des Implementierungs-Flow Designers anreichern.

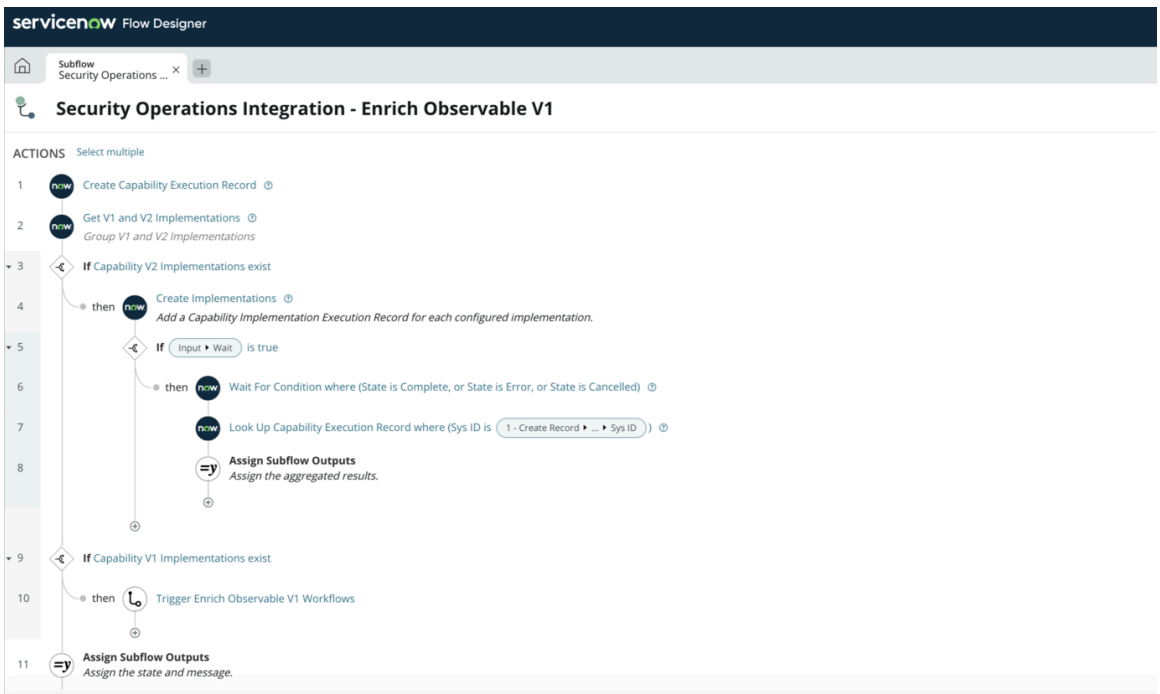
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow kann auf zwei Arten über Security Incident Response oder Threat Intelligence ausgelöst werden.

- durch Auswahl eines oder mehrerer erkennbarer Elemente in der Liste „Erkennbare Elemente“ und Auswahl von **Ergänzung erkennbarer Elemente ausführenin der Auswahlliste Aktionen für ausgewählte Zeilen**.
- indem Sie einen Datensatz eines erkennbaren Elements öffnen und auf den zugehörigen Link **Ergänzung erkennbarer Elemente ausführen** klicken.

Anschließend können Sie mit beiden Methoden angeben, welche Implementierungen zum Anreichern der ausgewählten erkennbaren Elemente verwendet werden sollen. Die zugehörigen Implementierungs-Flows werden ausgeführt, um die Anreicherung durchzuführen.

Erkennbares Element ergänzen



Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Zu den Flow-Prozessaktionen gehören:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.
- Aktion „Unterstützte Sicherheitsfähigkeiten abrufen“.Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.

Security Operations-Integration: Funktion zum Abrufen von Netzwerkstatistiken

Mit der Fähigkeit „Netzwerkstatistiken abrufen“ wird eine Liste der aktiven Netzwerkverbindungen von einem Host oder Endpunkt abgerufen. Es kann bei Untersuchungen zur Anreicherung von Incidents verwendet werden. Diese Fähigkeit wird automatisch ausgelöst, wenn einem Security Incident ein Konfigurationselement hinzugefügt wird.

Die Fähigkeit **„Netzwerkstatistiken abrufen“** besitzt den Flow Flow für Security Operations-Integrationen – Netzwerkstatistiken abrufen, der mindestens ein CI und mindestens eine Aufgabe akzeptiert. Der Flow wird für jede Implementierung und jedes CI durchlaufen und ruft den Implementierungs-Flow erneut auf.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

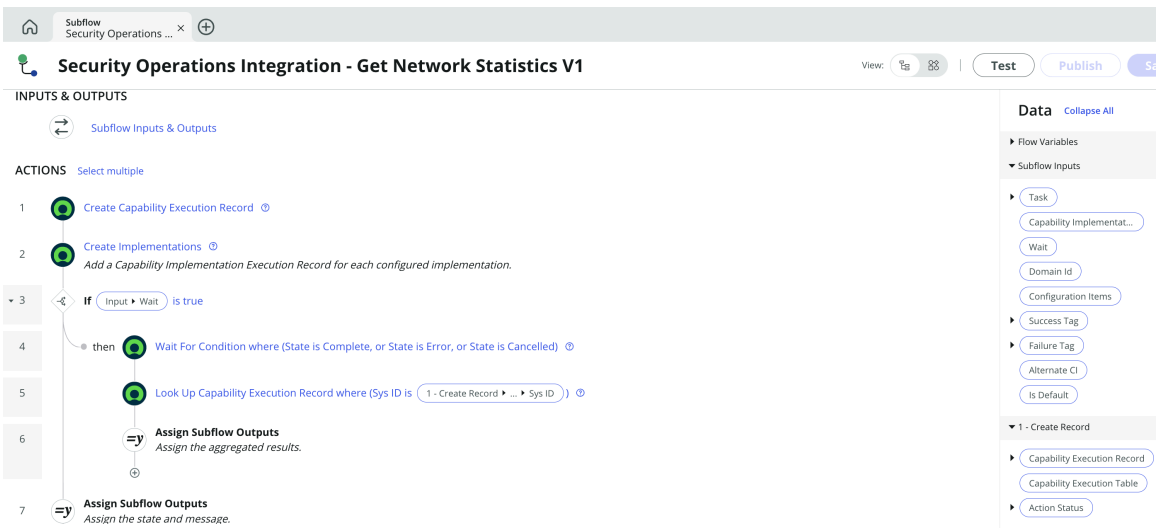
Flow für Security Operations-Integrationen – Netzwerkstatistiken abrufen

Der Flow „Security Operations Integrations – Netzwerkstatistiken abrufen“ ruft eine Liste aktiver Netzwerkverbindungen von einem Host oder Endpunkt ab.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird automatisch ausgeführt, wenn einem Security Incident ein Konfigurationselement hinzugefügt wird.

Netzwerkstatistiken abrufen



Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Die Flow-Aktionen umfassen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fähigkeit – Aktivität „CIs bestimmen“.
-

.

Ausführungsnachverfolgung – Flow-Aktion „Beginn (CIs)

Die Flow-Aktion **„Ausführungsnachverfolgung – Begin (CIs)“** startet den Auditing-Prozess für einen Security Operations Integration-Flow, der für Configuration Items (CIs) ausgeführt wird.

Die Flow-Aktion **„Ausführungsnachverfolgung – Begin (CIs)“** kann mit jedem CI-Flow verwendet werden, um mit der Aufzeichnung des Flow-Fortschritts in einem Audit zu beginnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ein Audit-Datensatz wird erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
capabilityId	System-ID der ausgeführten Integrationsfunktionalität
istImpl	Kennzeichnung, die angibt, ob das Audit für einen Integrationsfähigkeits-Flow oder einen Integrationsfähigkeits-Implementierungs-Flow durchgeführt wird. Mögliche Werte: • „falsch“ - bedeutet Auditing für einen abstrakten Integrationsfähigkeits-Flow wie z. B. Sichtungssuche. (Standard) • wahr – bezeichnet Auditing in einem Implementierungs-Flow für eine Integrationsfähigkeit. Zum Beispiel Splunk oder Elasticsearch.
Aufgaben-ID	System-ID für jede Aufgabe, die dem Flow zugeordnet ist.

ciList	Mindestens ein Configuration Item (CI) für die Ausführung der gewünschten Aktion im folgenden Format:
	`["sysId", "sysId"]`
	oder
	`"sysId"`
	Wird als Flow-Eingabe verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
flowContextId	Systembezeichner des zugeordneten Flow-Kontextdatensatzes. Wird vom System bereitgestellt.
FlowName	Name des Flows. Wird vom System bereitgestellt.
parentCapabilityExcutionId	Systembezeichner des Audit-Datensatzes, von dem der Implementierungs-Flow gestartet wurde. Nur erforderlich für Implementierungs-Flows für Integrationsfähigkeiten wie Splunk, Elasticsearch.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
capabilityExecutionId	Systembezeichner des Audit-Datensatzes.

Zu den Flow-Prozessaktionen gehören:

- Aktion „Unterstützte Sicherheitsfähigkeiten abrufen“.
- Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.

Security Incident Response – Flow zum Abrufen von Netzwerkstatistiken

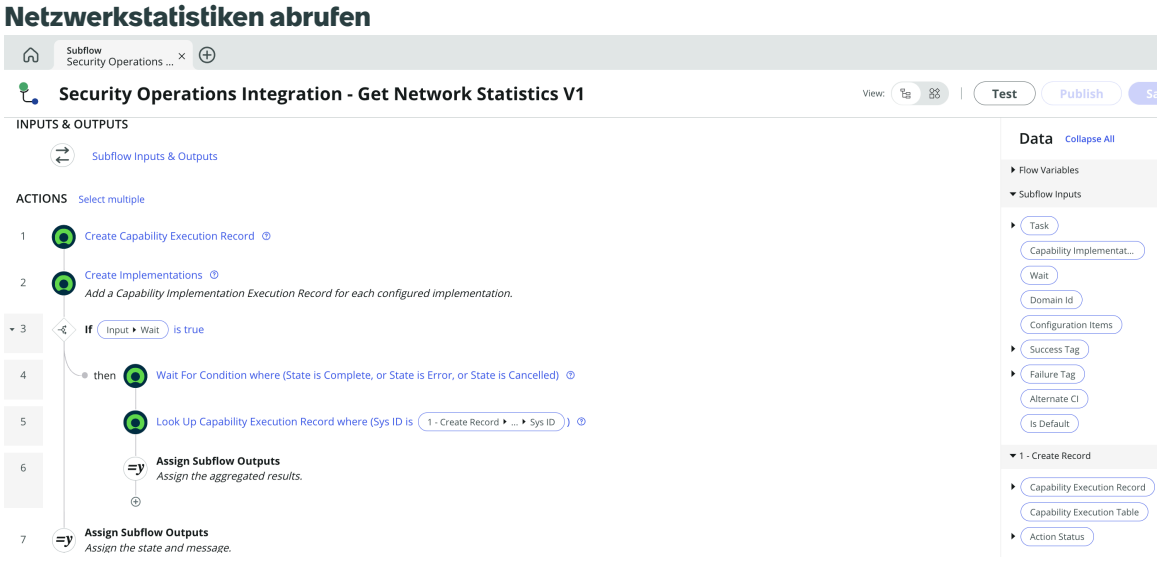
Die zugehörigen Listen namens **Security Incident Response** > **Netzwerkstatistiken abrufen** -Flow ruft die Netzwerkstatistiken für eine betroffene Windows-basierte Ressource ab, wenn sie einem Security Incident im **Analysestatus** hinzugefügt wird.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Bei neuen Security Incidents, die Konfigurationselemente enthalten, wird der Flow automatisch ausgeführt, wenn sich der Status in **Analyse**ändert.

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich im Status **„Analyse** “ befinden und ein neues Configuration Item hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zu den Flow-Prozessaktionen gehören:

FQDN-Flow-Aktion für Konfigurationselement abrufen

Shell-Skript nach Betriebssystem bestimmen

Die If-Anweisung wird von PowerShell ausgeführt

Ausführungsnachverfolgung: Flow-Aktion beginnen

Flow-Aktion „Netzwerkstatistiken über Netstat“ abrufen

Nachverfolgung der Fähigkeitsausführung: Fehler-Flow-Aktion

Flow-Aktion zum Erstellen von Datensätzen mit Ergänzungsdaten

Nachverfolgung der Fähigkeitsausführung: Fehler-Flow-Aktion Gibt die Ergänzungs-ID zurück.

Nachverfolgung der Fähigkeitsausführung – Flow-Aktion abschließen

Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie bei Bedarf den **Status** auf **Analyse**.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration stellt Netzwerkstatistikinformationen im bereit **Zugehörige Links** > **Ergänzungen zu Security Incidents** Registerkarte Weitere Informationen finden Sie unter Security Operations Zuordnung von Ergänzungsdaten.

   Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Security Operations-Integration: Fähigkeit zum Abrufen laufender Prozesse

Mit der Fähigkeit „Laufende Prozesse abrufen“ wird eine Liste der laufenden Prozesse für ein Configuration Item (CI) von einem Host oder Endpunkt abgerufen. Diese Funktion wird bei Untersuchungen für die Anreicherung von Incidents verwendet.

Die Fähigkeit „Laufende Prozesse abrufen“ hat zwei Implementierungs -[]- Flows:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Operations Carbon Black-Integration – Flow zum Abrufen laufender Prozesse
- Security Operations-Systembefehlsintegration: Flow zum Abrufen laufender Prozesse

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

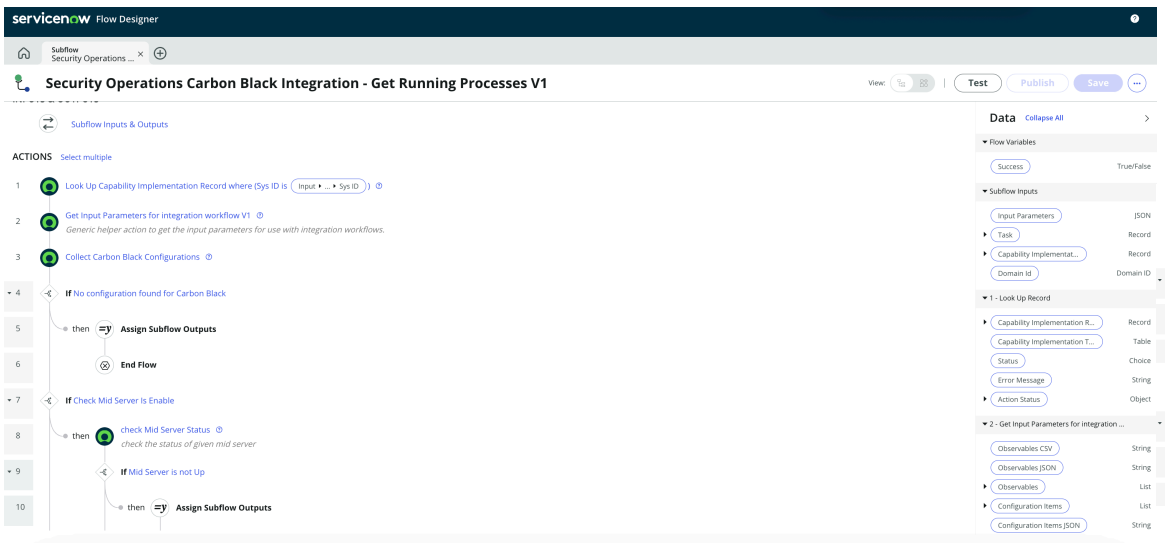
Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Security Operations Carbon Black-Integration – Flow zum Abrufen laufender Prozesse

„Security Operations Carbon Black Integration – Get Laufende Prozesse“ ist die Implementierung für die Carbon Black-Integration, die durch den Flow „Security Operations Integration – Get Laufende Prozesse“ gestartet wird.

Erforderliche Rolle: sn_si.analyst

Carbon Black ruft laufende Prozesse ab



Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Flow-Aktion zum Sammeln von Carbon Black-Konfigurationen

Mit der Flow-Aktion Carbon Black-Konfigurationen erfassen werden Konfigurationsinformationen gesammelt, die im Flow verwendet werden sollen.

Mit der Flow-Aktion Carbon Black-Konfigurationen sammeln sammeln Sie Carbon Black-Konfigurationsinformationen, die im Flow verwendet werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Konfiguration erfolgreich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse (Fortsetzung)

Ergebnis	Beschreibung
Fehler	Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Für diese Flow-Aktion sind keine Eingabevariablen vorhanden.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
endpoint_base	Basis-URL der API der Drittpartei-Integration.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
api_token	API-Schlüssel für die Drittpartei-Integration.

Überprüfen Sie den MID-Server-Status

Bestimmt, ob der im Feld **MID-Server-Host** der Konfiguration der Integration angegebene MID-Server aktiv ist und ausgeführt wird. Wenn das Feld auf **Beliebig**festgelegt ist, überprüft die Flow-Aktion, ob ein MID Server aktiv ist und ausgeführt wird.

Die Flow-Aktion MID-Server-Status überprüfen kann mit jedem Flow verwendet werden, um zu überprüfen, ob ein aktiver MID-Server innerhalb des Flows vorhanden ist.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzungsstatus zurückgegeben.
Fehler	Sitzungsstatusfehler. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
capabilityExecutionId	Die ID der ausgeführten Fähigkeit.
FlowName	Der Name des ausgeführten Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
mid_server_host	Der in der Konfiguration der Integration identifizierte MID Server, i

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
mid_server_live	Gibt an, ob der im Feld **„MID-Server-Host“** der Konfiguration der Integration angegebene MID-Server aktiv ist und ausgeführt wird. Wenn das Feld auf **Beliebig**festgelegt ist, überprüft die Flow-Aktion, ob ein MID Server aktiv ist und ausgeführt wird.

Flow-Aktion „Sensor-ID abrufen“.

Mit der Flow-Aktion Sensor-ID abrufen werden Sensor-Bezeichner gesammelt, die im Flow verwendet werden sollen.

Die Flow-Aktion Sensor-ID abrufen kann mit jedem Flow verwendet werden, um Sensorinformationen zu sammeln, die im Flow verwendet werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sensorbezeichner gefunden.
Fehler	Keine Sensoren gefunden. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
endpoint_base	Basis-URL der Carbon Black-API.
ci_ip_address	IP-Adresse des Konfigurationselements.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.
Elementtyp „Array“.	API-Variablen
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Flow-Aktion für Sitzung erstellen

Mit der Flow-Aktion Sitzung erstellen wird eine Carbon Black-Sitzung zur Verwendung im Flow eingerichtet.

Die Flow-Aktion „Sitzung erstellen“ kann mit jedem Flow verwendet werden, um eine Carbon Black-Sitzung innerhalb des Flows zu erstellen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzung erstellt.
Fehler	Sitzung nicht erstellt. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
sensor_id	Sensor-Bezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
Ausgabe	API-Variablen

Flow-Aktion zum Überprüfen des Sitzungsstatus

Bestimmt den Status einer Carbon Black-Sitzung innerhalb des Flows.

Die Flow-Aktion Sitzungsstatus überprüfen kann mit jedem Flow verwendet werden, um den Status der Carbon Black-Sitzung innerhalb des Flows zu überprüfen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzungsstatus zurückgegeben.
Fehler	Sitzungsstatusfehler. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.
Ausgabe	Informationen zu laufenden Carbon Black-Prozessen.

Erstellen Sie eine Flow-Aktion des Befehlsprozesses

Mit der Flow-Aktion Befehlsprozess erstellen wird ein Carbon Black-Befehlsprozess erstellt, der im Flow verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Flow-Aktion Befehlsprozess erstellen kann mit jedem Flow verwendet werden, um einen Carbon Black-Befehlsprozess innerhalb des Flows zu erstellen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Befehlsprozess erstellt.
Fehler	Befehlsprozess nicht erstellt. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
command_id	Befehlsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.
Ausgabe	API-Variablen

Überprüfen Sie den Befehlsstatus, und rufen Sie die Prozess-Flow-Aktion ab

Überprüft den Status des Carbon Black-Befehls und ruft Prozesse ab, die im Flow verwendet werden sollen.

Die Aktionen zum Überprüfen des Befehlsstatus und zum Abrufen der Prozess-Flow-Aktion können mit jedem Flow verwendet werden, um den Status eines Carbon Black-Befehls zu überprüfen und Prozesse innerhalb des Flows abzurufen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Befehlsstatus zurückgegeben und Prozesse erstellt.
Fehler	Befehlsstatus oder Prozessfehler. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
command_id	Befehlsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.
Ausgabe	API-Variablen

Flow-Aktion für Prozessdaten zuordnen

Mit der Flow-Aktion „Prozessdaten zuordnen“ werden Carbon Black-Prozessdaten innerhalb des Flow zugeordnet.

Die Flow-Aktion „Prozessdaten zuordnen“ kann mit jedem Flow verwendet werden, um Carbon Black-Prozesse zuzuordnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Zugeordnete Prozesse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse (Fortsetzung)

Ergebnis	Beschreibung
Fehler	Prozesse nicht zugeordnet. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
impacted_ci	Betroffenes Konfigurationselement.
Implementation_id	Implementierungsbezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ausgabe	Formatierte Rückgabedaten zu laufenden Prozessen, die vom abstrakten Workflow verwendet werden.
Prozesse	Liste der Prozesse in einem Array.

Nachverfolgung der Fähigkeitsausführung – Flow-Aktion abschließen

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Nachverfolgung von“ aktualisiert den Audit-Datensatz, wenn der Flow abgeschlossen ist.

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Abschließen“ kann mit jedem Flow verwendet werden, um den Abschluss des Flows aufzuzeichnen.

Hinweis:
Das **Rückgabewert-** Array aus der Core-Flow-Aktion **des parallelen Startprogramms** enthält ein Array von Ergebnissen aus allen ausgeführten Integrations-Flows und zeigt den erfolgreichen Abschluss der Ausführungsnachverfolgung an.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Audit-Datensatzes wird auf **Abgeschlossen**aktualisiert.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
capabilityExecutionId	Systembezeichner für den Audit-Datensatz. Dieses Feld war die Ausgabe einer der Aktivitäten für „Auditing beginnen“.
FlowName	Name des Flows. Wird vom System bereitgestellt.
Nachricht	Abschlussmeldung.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

Flow-Aktion zum Schließen der Sitzung

Schließt eine Carbon Black-Sitzung innerhalb des Flows.

Die Aktivität „Sitzung schließen“ kann mit jedem Flow verwendet werden, um eine Carbon Black-Sitzung zu schließen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzung geschlossen.
Fehler	Sitzung nicht geschlossen. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.
Ausgabe	API-Variablen

Security Operations-Systembefehlsintegration: Flow zum Abrufen laufender Prozesse

Der Flow „Security Operations-Systembefehlsintegration – Get Laufende Prozesse“ ruft die laufenden Prozesse eines Configuration Item ab, wenn es einem Windows- oder Unix-basierten Security Incident im Status **„Analyse“**hinzugefügt oder aktualisiert wird.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Bei neuen Security Incidents wird der Flow automatisch ausgeführt, wenn Sie den Incident mit einem ausgewählten Configuration Item übermitteln, wenn der Status automatisch in **Analyse**geändert wird. Wenn er im Status **Entwurf** bleibt, wird er nicht ausgeführt.

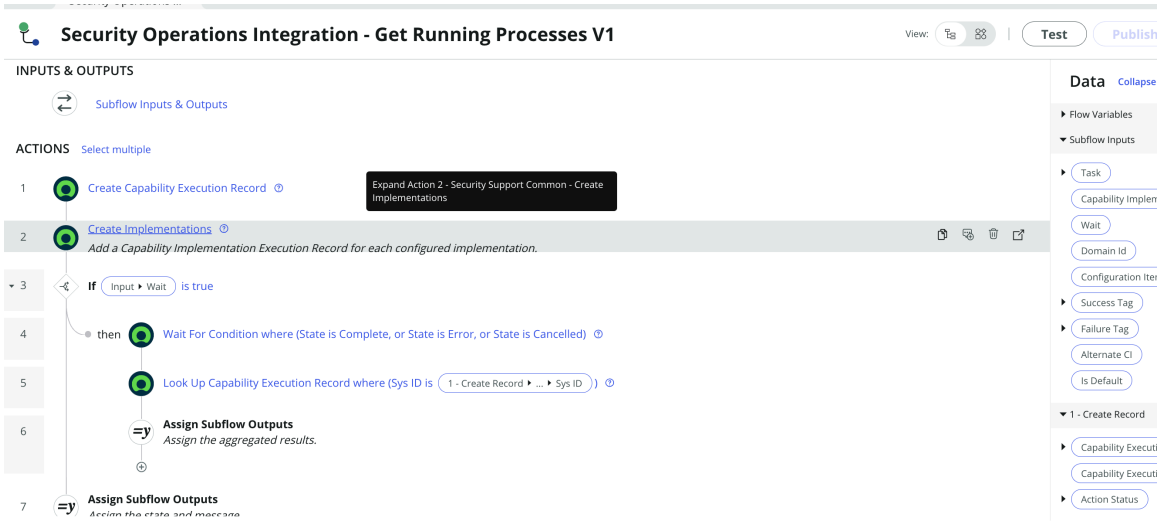
Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich im Status **„Analyse** “ befinden und ein neues Configuration Item hinzufügen.

Zu den Flow-Prozessaktionen gehören:

- FQDN-Flow-Aktion für Konfigurationselement abrufen
- Bestimmen Sie das Shell-Skript anhand der Betriebssystemaktivität
- Ausführungsnachverfolgung: Flow-Aktion beginnen
- Laufende Prozesse über PowerShell abrufen
- Aktivität „Shell-Skript ausführen“.
- Nachverfolgung der Fähigkeitsausführung: Fehler-Flow-Aktion
- Aktivität „Shell-Skript aus MID-Skript extrahieren“.
- Kombinieren Sie Ergebnisse und Rückgabewerte in einem Array
- Flow-Aktion zum Erstellen von Datensätzen mit Ergänzungsdaten
- Nachverfolgung der Fähigkeitsausführung – Flow-Aktion abschließen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laufende Prozesse abrufen



Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie bei Bedarf den **Status** auf **Analyse**.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration stellt Informationen zum laufenden Prozess in bereit **Zugehöriger Link** > **Ergänzungen zu Security Incidents**Registerkarte Weitere Informationen finden Sie unter Security Operations Zuordnung von Ergänzungsdaten.

   Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Aktivität „Ergebnisse kombinieren“.

Mit der Workflow-Aktivität „Ergebnisse kombinieren“ werden die Ergebnisse aus Drittanbieterintegrationen zur Verwendung im Workflow zusammengeführt.

Die Aktivität Ergebnisse kombinieren kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript im Workflow auszuführen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ergebnisse zusammengefasst.
Fehler	Kombination fehlgeschlagen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
inputA	Ergebnissatz A
inputB	Ergebnissatz B
Implementation_id	Implementierungsbezeichner.
impacted_ci	Konfigurationselement

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis	Ergebnissatz A oder Ergebnissatz B, je nachdem, welcher Wert ausgefüllt ist.

Aktivität „Shell-Skript ausführen“.

Die Workflow-Aktivität Shell-Skript ausführen führt ein MID-Server-Shell-Skript innerhalb des Workflows aus.

Die Aktivität „Shell-Skript ausführen“ kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript im Workflow auszuführen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Shell-Skript gefunden
Fehler	Kein Shell-Skript gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Ziel	IP oder vollqualifizierter Domänenname (FQDN) des Ziel-CI.
scriptValue	Skript als Zeichenfolgenwert, das auf einem Unix-System ausgeführt wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
response	Rohausgabe Daten laufender Prozesse.

Aktivität „Shell-Skript aus MID-Skript extrahieren“.

Mit der Workflow-Aktivität „Shell-Skript aus MID-Skript extrahieren“ wird ein MID-Server-Shell-Skript zur Verwendung mit im Workflow abgerufen.

Die Aktivität Shell-Skript aus MID-Skript extrahieren kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript zu extrahieren und in den Workflow aufzunehmen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Shell-Skript gefunden
Fehler	Kein Shell-Skript gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
sysId	Systembezeichner

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
scriptValue	Skript als Zeichenfolgenwert, das auf einem Unix-System ausgeführt wird.

Aktivität „Laufende Prozesse über PowerShell abrufen“.

Die Workflow-Aktivität „Sensor-ID abrufen“ sammelt laufende Prozesse mithilfe von PowerShell, um sie im Workflow zu verwenden.

Die Workflow-Aktivität „Laufende Prozesse über PowerShell abrufen“ kann mit jedem Workflow verwendet werden, um Prozesse abzurufen, die in den Workflow aufgenommen werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Prozesse gefunden
Fehler	Keine Prozesse gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Ziel	IP oder vollqualifizierter Domänenname (FQDN) des Ziel-CI.
Verarbeitungsskript	ECC-Skript wird auf einem Windows-basierten System ausgeführt.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

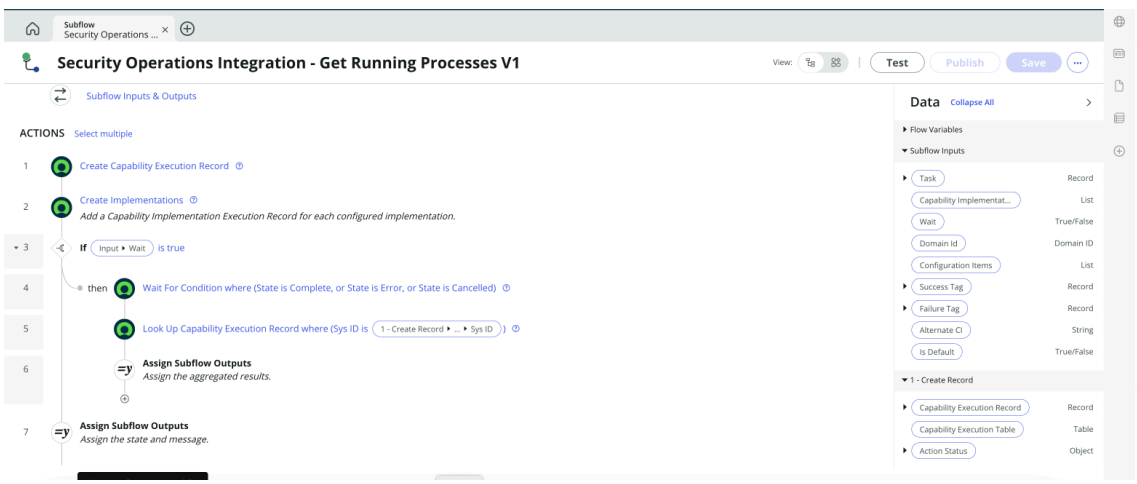
Variable	Beschreibung
response	Rohausgabe Daten laufender Prozesse.

Security Operations – Flow für laufende Prozesse abrufen

Der Flow „Security Operations – Laufende Prozesse abrufen“ ist ein allgemeiner Flow, der von Integrationen unabhängig ist. Ruft eine Liste der laufenden Prozesse für ein Configuration Item (CI) von einem Host ab. Verwenden Sie diese Liste, um eine Integration wie Carbon Black oder einen Windows-basierten Security Incident zu erfüllen.

Erforderliche Rolle: sn_si.analyst

Laufende Prozesse abrufen



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations-Integration: Fähigkeit „Host isolieren“.

Die Fähigkeit **„Host isolieren“** schränkt Systemverbindungen mit anderen Geräten ein. „Host isolieren“ wird für ein Configuration Item (CI) ausgeführt.

Die Fähigkeit **„Host isolieren“** besitzt den Flow Security Operations – Flow zum Isolieren von Hosts, der mindestens ein CI und optional eine Implementierung akzeptiert. Sie können eine Implementierung angeben, die zum Isolieren des Hosts verwendet wird, oder für den Flow versuchen, den Host mithilfe aller Implementierungen zu isolieren.

Hinweis:
Security Operations Carbon Black Integration: Flow zum Entfernen der Hostisolierung ist zwar nicht mit einer Fähigkeit integriert, aber mit einem Flow, der für die Orchestrierung verfügbar ist, um die Kommunikation mit einem isolierten Host wiederherzustellen.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Führen Sie „Host isolieren“ aus

„Host isolieren“ schränkt Systemverbindungen mit anderen Geräten ein.

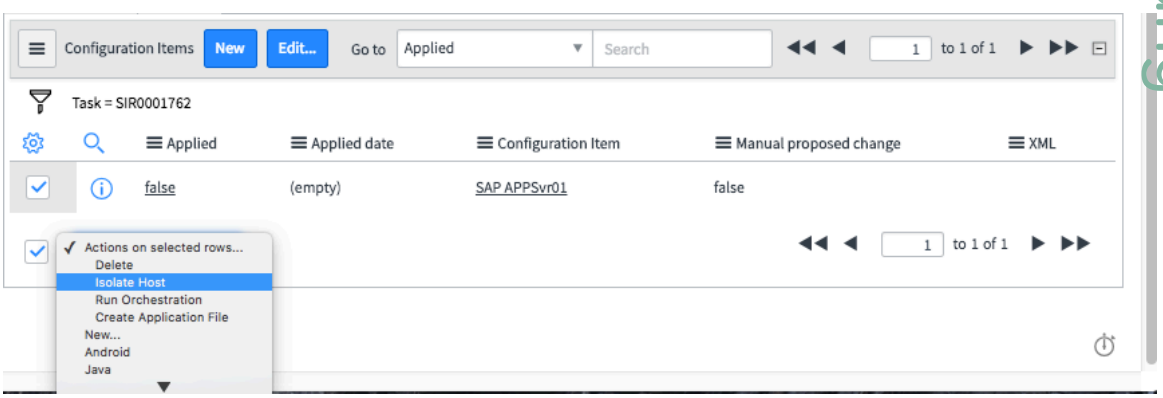
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Der Flow **„Security Operations Integration – Host oder Endpunkt isolieren“** kann über die zugehörige Liste in einem Security Incident ausgelöst werden.

Prozedur

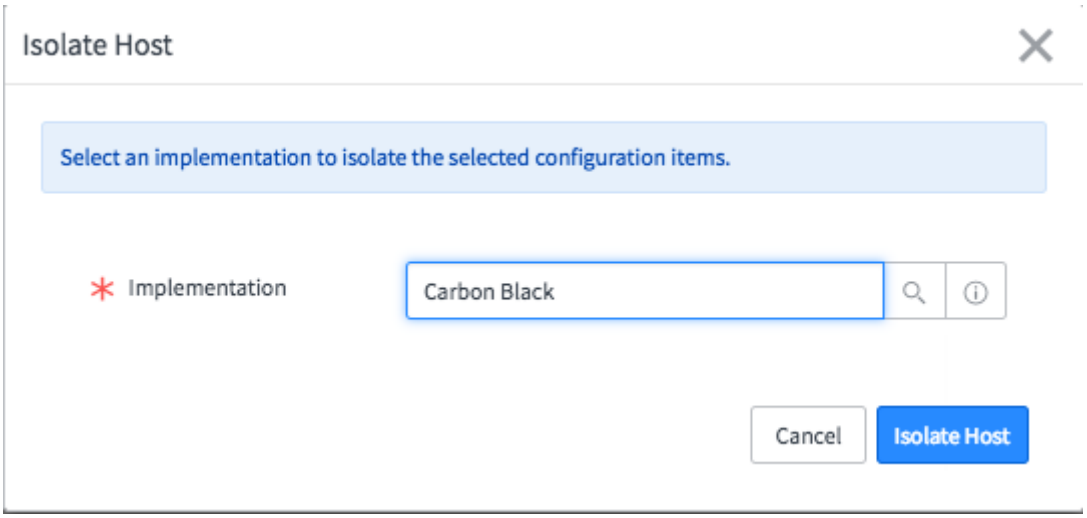
1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie **Configuration Items** auf der Registerkarte **Zugehörige Liste** aus.
3. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen...** auf **Host isolieren**.



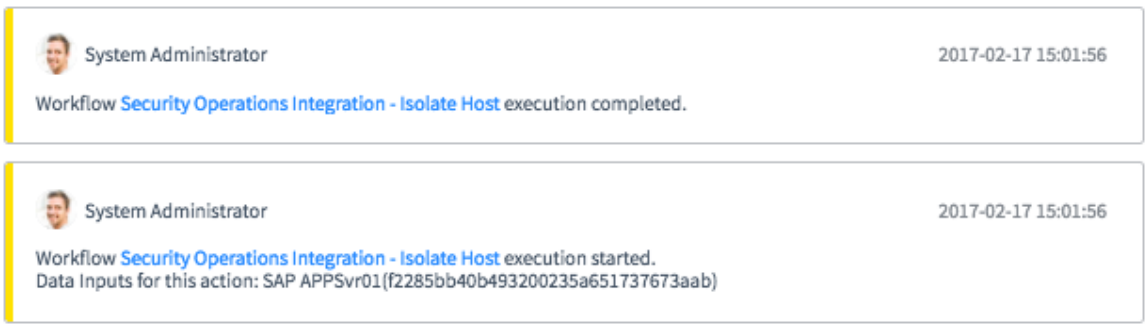
Das Dialogfeld wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Implementierung aus.
5. Klicken Sie auf **Host isolieren**.
   Das Audit der Flow-Ausführung wird im Abschnitt „Arbeitsnotizen“ angezeigt.



Security Operations – Flow zum Isolieren von Hosts

Der Flow **„Security Operations – Host isolieren“** ist ein allgemeiner Flow, der von Integrationen unabhängig ist. Es verwendet die konfigurierten Abfragen, um nach einer Reihe von Configuration Items zu suchen. Verwenden Sie sie, um eine -Integration zu erfüllen, z. B. Carbon Black.

Vorbereitungen

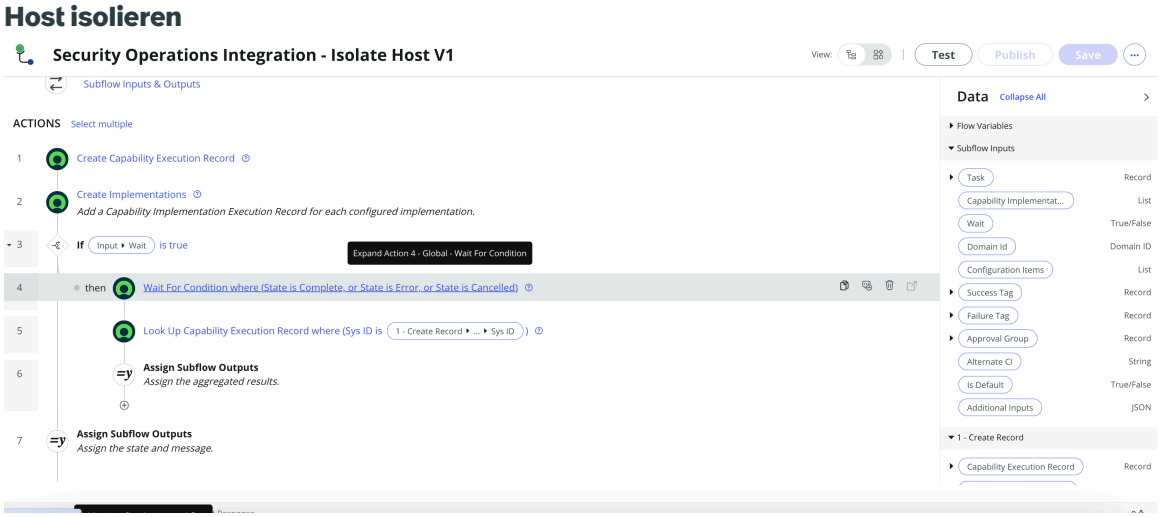
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird über die Registerkarte **„Konfigurationselemente“** in einer zugehörigen Liste für Security Incidents ausgelöst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Security Operations Carbon Black Integration – Flow zum Isolieren von Hosts

Die Security Operations Carbon Black-Integration – Host isolieren ist die Implementierung für die Carbon Black-Integration, die durch den Flow Security Operations Integration – Host isolieren gestartet wird.

Vorbereitungen

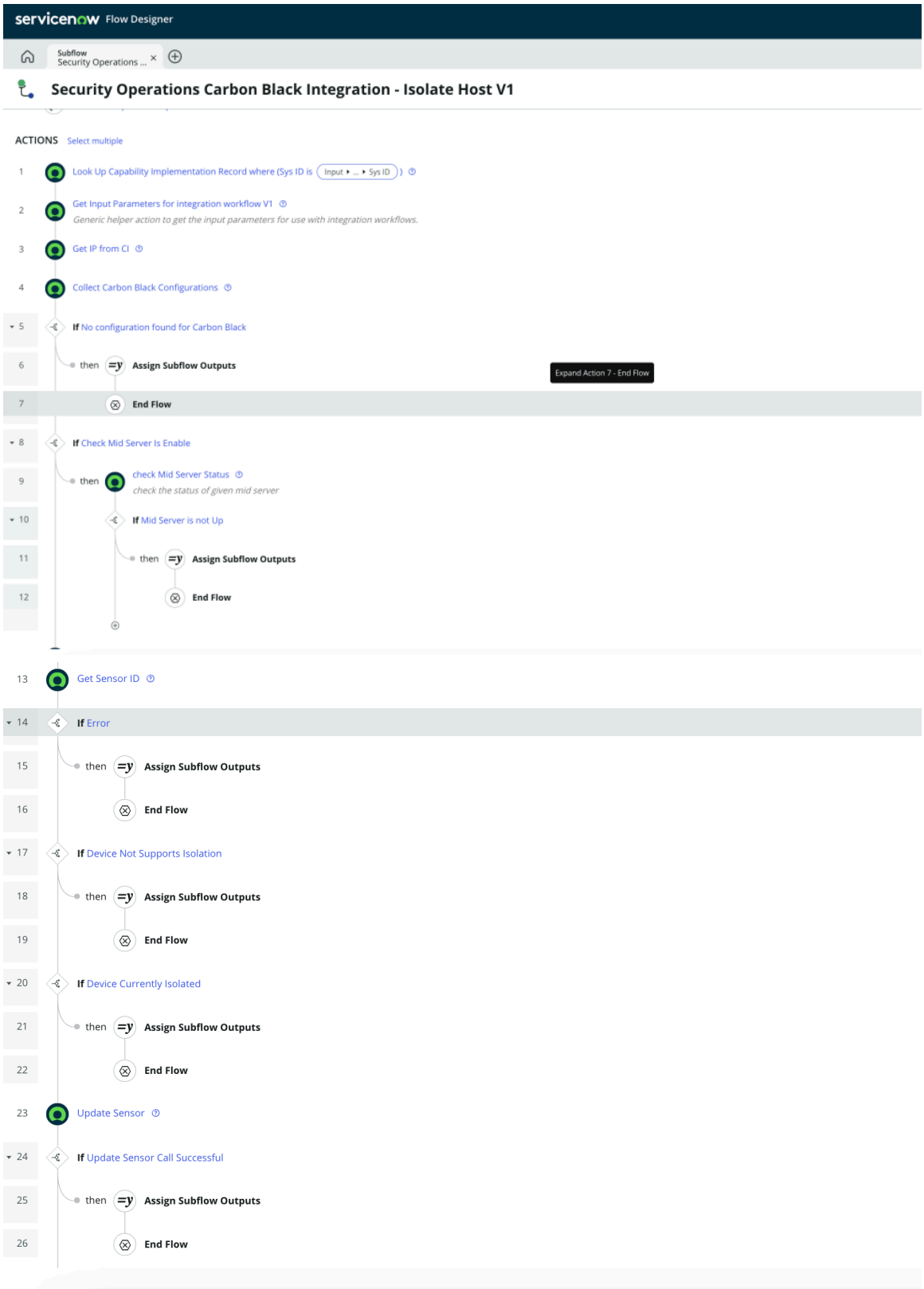
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

Die Flow-Prozessaktivitäten umfassen:

- Ausführungsnachverfolgung – Flow-Aktion „Beginn (CIs)
- IP von CI abrufen
- Erfassen Sie Carbon Black-Konfigurationen
- Nachverfolgung der Fähigkeitsausführung: Fehler-Flow-Aktion
- Sensor-ID abrufen
- Legen Sie die Aktivität „Netzwerkisolierung aktiviert“ fest
- Sensor aktualisieren : gibt das Ergebnis „Host isolieren“ zurück.
- Nachverfolgung der Fähigkeitsausführung – Flow-Aktion abschließen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Flow-Aktion „Sensor-ID abrufen“.

Mit der Flow-Aktion Sensor-ID abrufen werden Sensor-Bezeichner gesammelt, die im Flow verwendet werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Flow-Aktion Sensor-ID abrufen kann mit jedem Flow verwendet werden, um Sensorinformationen zu sammeln, die im Flow verwendet werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sensorbezeichner gefunden.
Fehler	Keine Sensoren gefunden. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
endpoint_base	Basis-URL der Carbon Black-API.
ci_ip_address	IP-Adresse des Konfigurationselements.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.
Elementtyp „Array“.	API-Variablen
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Legen Sie die Aktivität „Netzwerkisolierung aktiviert“ fest

Mit der Workflow-Aktivität „Netzwerkisolierung auf Aktiviert festlegen“ wird die Netzwerkisolierung aktiviert.

Die Aktivität „Netzwerkisolierung auf Aktiviert festlegen“ kann mit jedem Workflow verwendet werden, um die Netzwerkisolierung zu aktivieren.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Netzwerkisolierung aktiviert.
Fehler	Netzwerkisolierung kann nicht aktiviert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.
Deaktivieren	Bestimmt, ob der Host isoliert ist, oder entfernt die Hostisolierung. Wahr = Isolation deaktivieren False = Isolierung bleibt aktiviert

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Aktualisieren Sie die Sensoraktivität

Die Workflow-Aktivität „Sensor aktualisieren“ aktualisiert den Sensor, um Hosts oder Endpunkte zu isolieren.

Die Aktivität „Sensor aktualisieren“ kann mit jedem Workflow verwendet werden, um Hosts oder Endpunkte zu isolieren.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Aktualisierter Sensor.
Fehler	Sensor kann nicht aktualisiert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
endpoint_base	Basis-URL der Carbon Black-API.
sensor_id	Sensor-Bezeichner.
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Gibt an, ob die Anforderung erfolgreich war. Andernfalls werden ein HTTP-Fehlercode und eine entsprechende Meldung angezeigt.

Security Operations Carbon Black Integration: Flow zum Entfernen der Hostisolierung

Der Flow **„Security Operations Carbon Black Integration – Hostisolierung entfernen“** entsperrt die Kommunikation mit einem angegebenen Host oder Endpunkt in einem Carbon Black-System.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

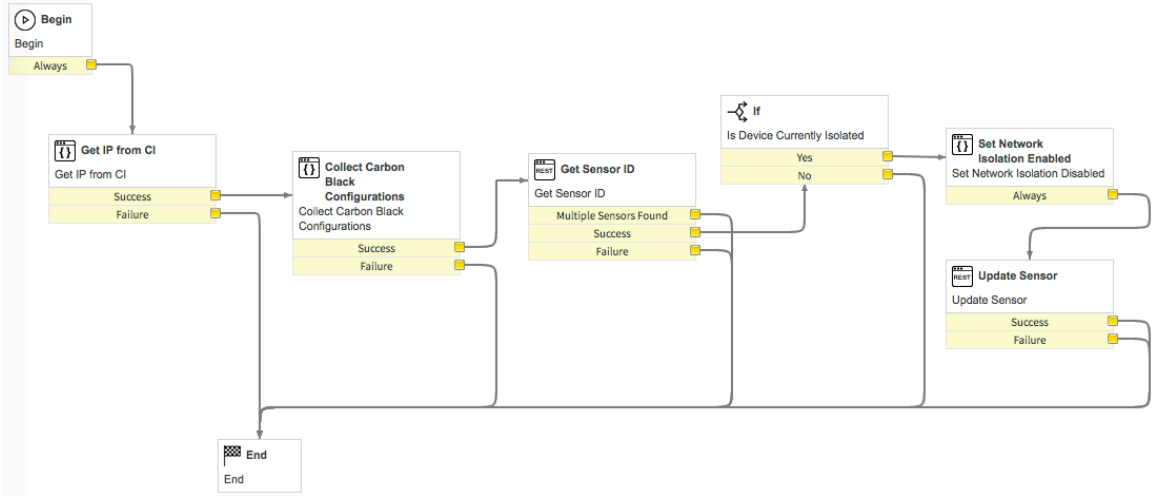
Dieser Flow ist nicht Teil einer Fähigkeit und benötigt eine anwenderdefinierte Orchestrierung, um ausgeführt zu werden.

Die Flow-Prozessaktivitäten umfassen:

- Rufen Sie die IP aus der CI-Aktivität ab
- Bei Erfolg: Flow-Aktion zum Sammeln von Carbon Black-Konfigurationen
- Flow-Aktion „Sensor-ID abrufen“.Sensor-ID abrufen
- Wenn: Gerät die Isolation unterstützt und Gerät nicht isoliert bis deaktiviert ist.
- Aktualisieren Sie die SensoraktivitätGibt das Ergebnis „Host isolieren“ zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Carbon Black-Integration: Hostisolierung entfernen



Security Operations-Integration: Fähigkeit „In Beobachtungsliste veröffentlichen“.

Die Fähigkeit „In Beobachtungsliste veröffentlichen“ fügt erkennbare Elemente und Indikatoren, die einem Security Incident zugeordnet sind, einer Drittanbieter-Beobachtungsliste hinzu, die Sicherheitsereignisse überwacht und Warnungen generiert. Diese Fähigkeit wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

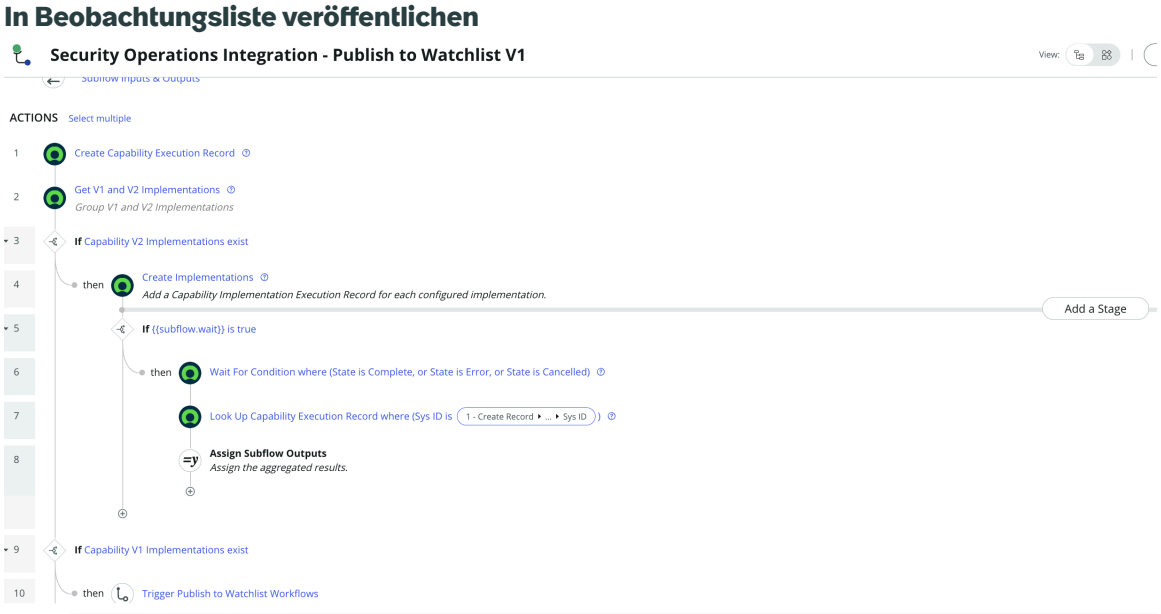
Security Operations-Integration – Flow zur Veröffentlichung in der Beobachtungsliste

Der Flow „ **Security Operations Integrations – In Beobachtungsliste veröffentlichen“** ist ein allgemeiner Flow, der von Integrationen unabhängig ist. Es fügt der Beobachtungsliste von Drittparteien erkennbare Elemente hinzu, die die Fähigkeit unterstützen. Verwenden Sie diese Liste, um eine Integration zu erfüllen.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow ist sichtbar und wird nur ausgeführt, wenn eine Integration verfügbar ist. Sie wird über die Registerkarte **Erkennbare Elemente** oder **Zugeordnete Indikatoren** in einem Security Incident ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Security Operations-Integration – Fähigkeit zur Sichtungssuche

Die Fähigkeit **„Sichtungssuche“** akzeptiert eine Reihe von erkennbaren Elementen, findet alle Integrationen, die eine Sichtungssuche unterstützen, und führt diese Suchen dann aus.

Die Fähigkeit „Sichtungssuche“ verfügt über den Workflow Security Operations Integration - Sichtungssuche-Flow, der die Sichtungssuche ausführt. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, findet implementierte Fähigkeiten, erstellt die Abfragen basierend auf Sichtungssuchkonfigurationen und führt die Suchvorgänge basierend auf dem konfigurierten Workflow aus. Sobald die Suche abgeschlossen ist, wird den Incident-Arbeitsnotizen eine Notiz hinzugefügt, in der angegeben wird, ob und wie viele Sichtungen gefunden wurden.

Um Konfigurationen für die Sichtungssuche anzuzeigen, navigieren Sie zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfigurationen**.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

Erstellen Sie mehrere Konfigurationsdatensätze für die Sichtungssuche, und verwenden Sie sie, wenn Sie mehrere Protokollspeicher abfragen oder die Suchparameter variieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

- Das CIM-Add-on muss auf der Splunk-Instanz installiert sein.
- Gespeicherte Suchen und Inplace-Abfragen werden nur für die Splunk-Integration unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch Konfigurationsdatensätze für Sichtungssuchen erstellen, um gespeicherte Suchen im Splunk-Enterprise-Protokollspeicher aufzurufen.

Hinweis:
Die Suchkonfigurationsabfragen beruhen darauf, dass Splunk-Protokolldaten konform mit dem Splunk Common Information Model (CIM) sind.

Mit gespeicherten Suchkonfigurationen können Sie:

- Erstellen Sie anwenderdefinierte Suchen, die mehrere Ereignisdatensätze kombinieren.
- Designeffiziente und effektive Suche.
- Verwenden Sie parametrisierte Eingaben in der gespeicherten Splunk-Suche.

Das -Basissystem enthält die in der folgenden Abbildung gezeigten Beispielkonfigurationen:

Gespeicherte Suchkonfigurationen

Name	Observable type	Search	Is saved search
Search	Search	Search	Search
Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

Die gespeicherte Suche und die Inplace-Konfigurationsabfragen sind Beispielabfragen und können durch entsprechende Parameter für Ihre Umgebung ersetzt werden. Erstellen Sie nach Bedarf zusätzliche gespeicherte Suchkonfigurationen. Wenn Sie eine gespeicherte Suchkonfiguration definieren, müssen der Name und die Parameter in der Suchabfrage mit der in Ihrer Splunk-Instanz definierten gespeicherten Konfiguration übereinstimmen. Wenn der Name und die Parameter nicht identisch sind, werden bei einer Sichtungssuche möglicherweise keine genauen Ergebnisse angezeigt.

Hinweis:
Navigieren Sie in Ihrer Splunk-Instanz zur Seite Suchen, Berichte und Warnungen, und suchen Sie nach Ihrer gespeicherten Suchabfrage. Klicken Sie auf den Link **Berechtigungen**, um zur Seite „Berechtigungen“ zu navigieren. Wählen Sie das Optionsfeld **Alle Apps** aus, und aktivieren Sie die Option **Leseberechtigung** für **Jeder**. Dadurch wird der Spaltenwert „Freigabe“ für Ihre gespeicherte Suchabfrage von „Privat“ in „App“ geändert. Wenn dies nicht festgelegt ist, gibt die gespeicherte Suchabfrage möglicherweise keine Ergebnisse zurück.

So überprüfen Sie, ob die gespeicherte Suchkonfiguration mit der in Ihrer Splunk-Instanz definierten Konfiguration übereinstimmt:

1. Navigieren zu **Einstellungen** > **Suchen, Berichte und Warnungen**.
2. Ändern Sie **den App-Kontext** in **Alle**.

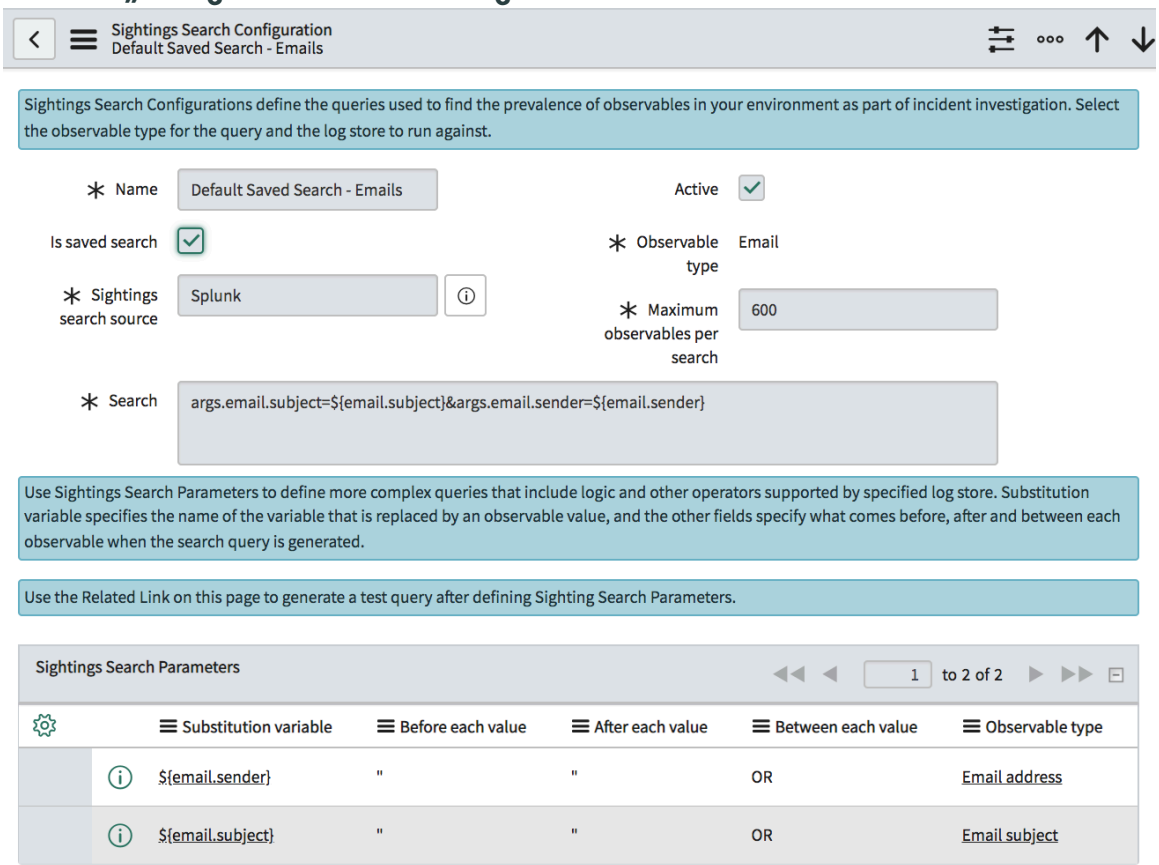
   Eine Liste der Suchberichte wird angezeigt.
3. Bestätigen Sie, dass die gespeicherte Suchabfrage in der Liste vorhanden ist.

Das Formular „Konfigurationen für die Sichtungssuche“ enthält beispielsweise die E-Mail-Adresse und den E-Mail-Absender als Suchparameter:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Konfigurationen für Sichtungssuche“.



Definieren Sie in Ihrer Splunk-Instanz die gespeicherte Suche mit demselben Namen, Standardmäßige gespeicherte Suche – E-Mails, und denselben Suchparametern für die E-Mail-Adresse und den E-Mail-Betreff. Wenn der Name und die Suchparameter nicht identisch sind, generiert die Sichtungssuche kein genaues Ergebnis.

Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfiguration** und erstellen Sie einen neuen Datensatz (Feldbeschreibungen finden Sie in der Tabelle).

Formular „Konfigurationen für Sichtungssuche“.

Feld	Beschreibung
Name	Name der Konfiguration
Ist gespeicherte Suche	Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt.
Sichtungssuchquelle	Die Quelle für die Sichtungssuche. Wählen Sie den Splunk-Protokollspeicher als Quelle aus.
Aktiv	Option für den gespeicherten Suchstatus. Nur aktive Suchkonfigurationen können verwendet werden, um eine Sichtungssuche durchzuführen.
Erkennbarer Typ	Der erkennbare Elementtyp kann ein beliebiger erkennbarer Elementtyp wie IP, Hash-Wert, URL, Domänenname usw. sein.
Maximale erkennbare Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die von der Suche zurückgegeben werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchen	Die Standardsuchzeichenfolge ist `$(observable)`, Sie können jedoch Ihre eigene Suchabfrage definieren, indem Sie Parameter angeben, die vom Splunk-Protokollspeicher unterstützt werden.

2. Klicken Sie auf **Absenden**.

Ergebnisse
Sie haben einen Konfigurationsdatensatz für die Sichtungssuche erstellt.

Nächste Maßnahme
Nachdem Sie die Suchabfrage definiert haben, klicken Sie auf **Testabfrage für Sichtungssuche generieren**und geben eine Liste erkennbarer Elemente an, um eine Testabfrage basierend auf dieser gespeicherten Suchkonfiguration zu generieren.

Führen Sie eine Sichtungssuche aus

Ermitteln Sie die Verbreitung einer Bedrohung im Laufe der Zeit, oder testen Sie Korrektur- oder Beseitigungsmaßnahmen. Sie können einzelne oder mehrere erkennbare Elemente und den Datumsbereich für Ihre Suche aus einem Security Incident auswählen. Ergebnisse sind in der zugehörigen Liste **„Erkennbare Elemente des Security Incident“** enthalten.

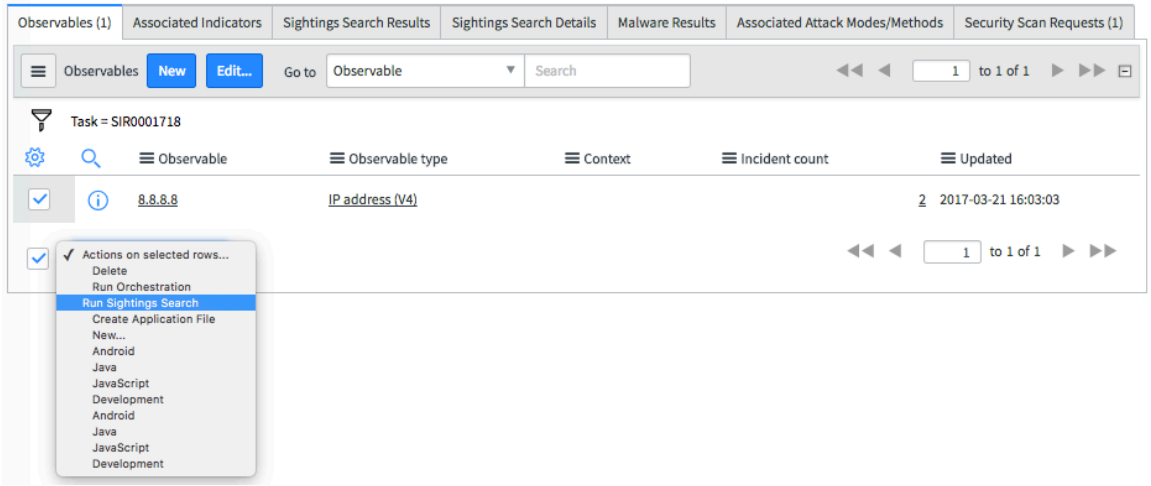
Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Die Fähigkeit „Sichtungssuche“ hat den Flow Security Operations Integration - Sichtungssuche-Flow, der die Sichtungssuche ausführt. Dieser Flow akzeptiert eine Liste von erkennbaren Elementen, findet implementierte Fähigkeiten, erstellt die Abfragen basierend auf Sichtungssuchkonfigurationen und führt die Suchvorgänge basierend auf dem konfigurierten Flow aus.

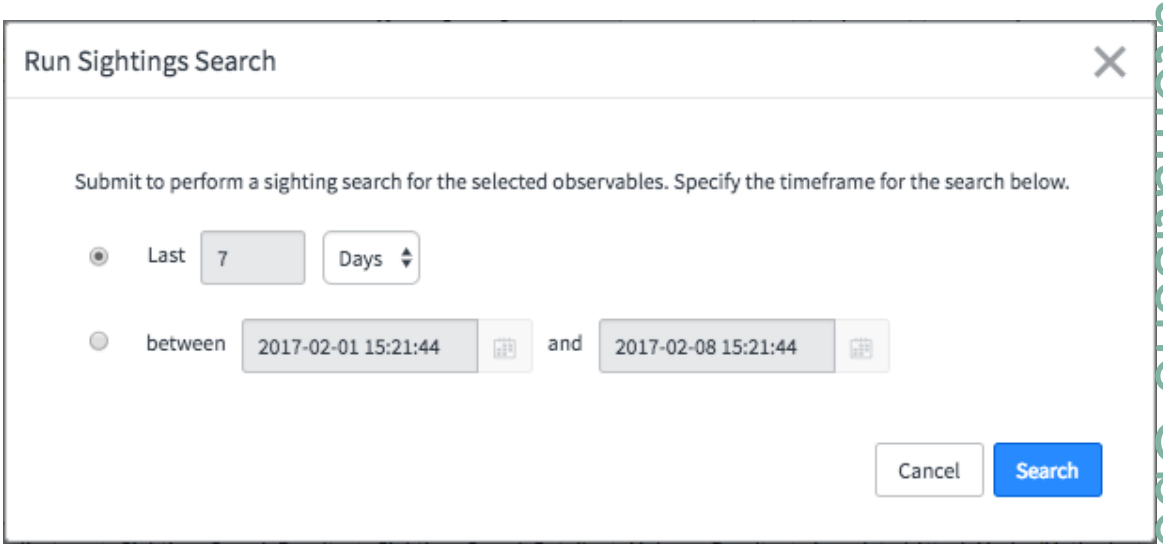
Hinweis:
Eine aktive Implementierung muss konfiguriert sein. Die Sichtungssuche unterstützt Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger und QRadar Incident Enrichment. Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen, wie z. **B. Sichtungssuche ausführen**, nicht in Produktmenüs angezeigt.

Prozedur
1. Navigieren Sie zu einem Security Incident.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.
3. Wählen Sie auf der Registerkarte Zugehörige Liste **die Option Erkennbare Elemente** aus.
4. Wählen Sie die erkennbaren Elemente aus, für die Sie eine Sichtungssuche durchführen möchten.
5. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen...** auf **Sichtungssuche ausführen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Dialogfeld „Sichtungssuche ausführen“ wird geöffnet.



Hinweis:
Die im Dialogfeld eingegebenen Werte überschreiben die Fähigkeitskonfigurationswerte für diese Ausführung.

6. Wählen Sie die Anzahl der Tage oder einen Datumsbereich für die Suche nach Daten.

Option	Bezeichnung
Letzter	Anzahl der Stunden oder Tage vor der Erstellung des zu durchsuchenden Incidents. Der Standardwert ist 7 Tage. Das Limit beträgt 99 Stunden oder Tage.
zwischen	Datumsbereich für die Suche. Standarddaten sind: Datum und Uhrzeit der Öffnung des incident. Datum und Uhrzeit sieben Tage vor Eröffnung des Incidents

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Letzte ist die Anzahl der Stunden oder Tage vor der Erstellung des zu durchsuchenden Incidents. Der Standardwert ist 7 Tage. Das Limit beträgt 99 Stunden oder Tage.

7. Klicken Sie auf **Suche**.
Ein Datensatz für die Sichtungssuche wird erstellt. Aggregierte und zugehörige Sichtungsdaten werden im Security Incident auf den **Registerkarten Ergebnisse der Sichtungssuche** und **Details der Sichtungssuche** angezeigt.

Hinweis:
Sichtungssuchergebnisdaten können mit Trusted Security Circlegeteilt werden, mit Ausnahme von Rohdaten bei Implementierungen, die für die Einbeziehung von Rohdaten konfiguriert sind.

Ergebnisse der Sichtungssuche

Ergebnis	Beschreibung
Nummer	Der Bezeichner für die Sichtungssuche.
Anzahl der erkennbaren Elemente	Anzahl der anhand der Abfrage gesuchten erkennbaren Elemente.
Interne Sichtungen	Anzahl der internen Sichtungen.
Externe Sichtungen	Anzahl der externen Sichtungen. (Erhalten aus der Bedrohungsfreigabe.)
Übereinstimmende Konfigurationselemente	Anzahl der Konfigurationselemente, die für jedes in Ihrer Umgebung gefundene erkennbare Element mit einem vorhandenen Datensatz in Ihrer CMDB übereinstimmen.
Startdatumsbereich	Zeit, mit der Suche nach Sichtungen zu beginnen
Enddatumsbereich	Zeit, die Suche nach Sichtungen zu beenden.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

Hinweis: Wenn die für die Sichtungssuche verwendete Implementierung so konfiguriert ist, dass Rohdaten einbezogen werden und mindestens eine Sichtung gefunden wird, wird oben im Security Incident ein Anhang mit Rohdatenbeispielen angezeigt.

Details der Sichtungssuche

Detail	Beschreibung
Sichtungssuche	Der Bezeichner für die Sichtungssuche.
Erkennbares Element	Über die Abfrage gesuchtes erkennbares Element.
Erkennbarer Typ	Typ des erkennbaren Elements, nach dem die Abfrage gesucht hat.
Interne Sichtungen	Aggregierte Anzahl interner Sichtungen.
Externe Sichtungen	Aggregierte Anzahl externer Sichtungen. (Erhalten aus der Bedrohungsfreigabe.)
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

Security Operations Integration - Sichtungssuche-Flow

Der Flow**Security Operations-Integration – Sichtungssuche** ist ein allgemeiner Flow, der von Integrationen unabhängig ist. Sie verwendet die konfigurierten Abfragen, um basierend auf den konfigurierten Integrationen, die diese Fähigkeit unterstützen, nach einer Reihe von

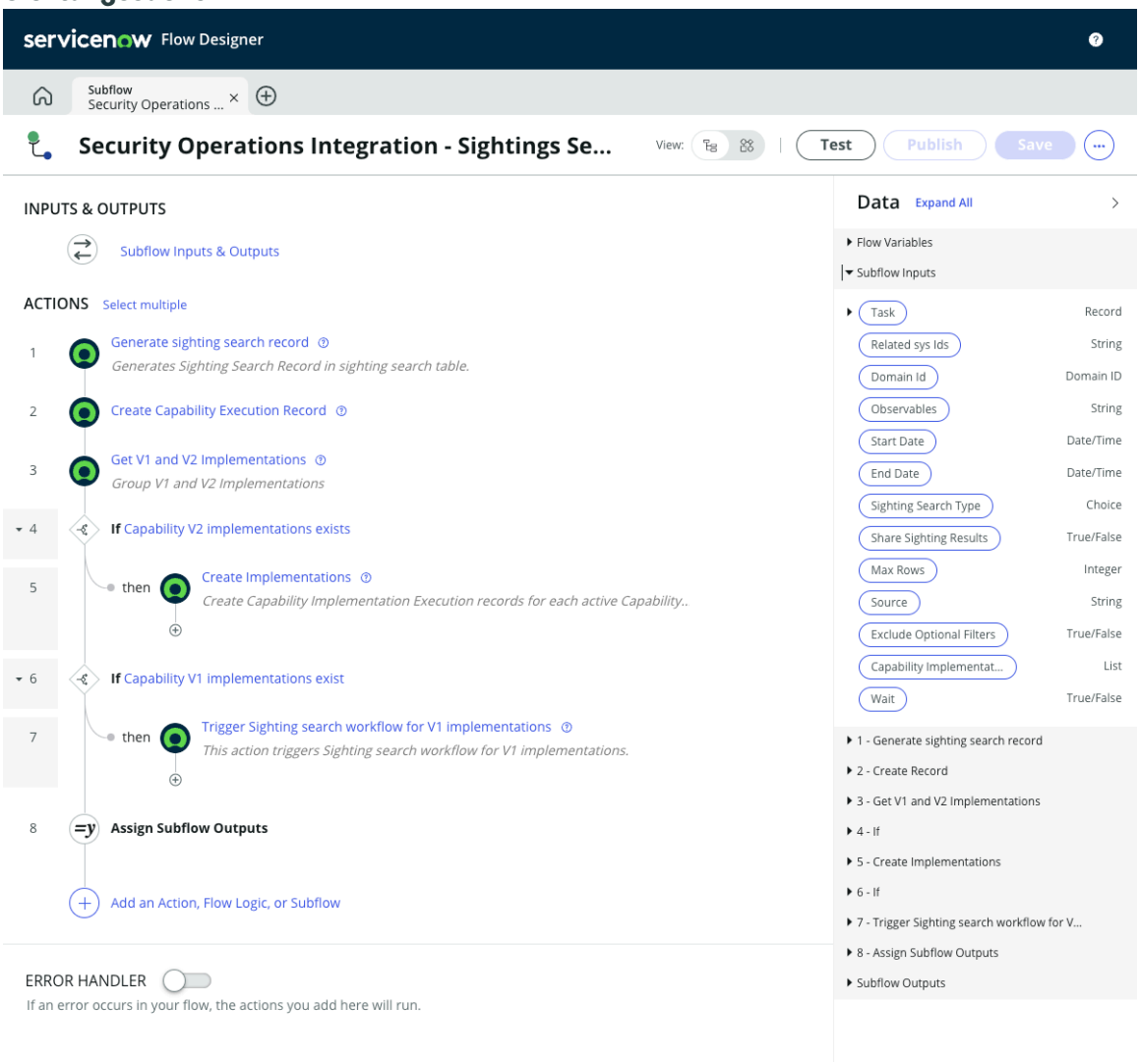
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erkennbaren Elementen zu suchen. Verwenden Sie es, um eine -Integration wie Splunk oder Elasticsearch zu erfüllen.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
Wenn einem Security Incident ein erkennbares Element angehängt ist, wird dieser Flow ausgelöst, wenn Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen...** auf der Registerkarte **Erkennbare Elemente des Security Incident** auf **Sichtungssuche ausführen** klicken.

Sichtungssuche



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Sichtungssuche – Aktivität „Erkennbare Elemente bestimmen“.

Die Workflow-Aktivität **„Sichtungssuche – Bestimmen erkennbarer Elemente“** bestimmt, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität **„Sichtungssuche – erkennbare Elemente bestimmen“** kann mit jedem Workflow verwendet werden, um zu bestimmen, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Erkennbare Elemente gefunden
Fehler	Keine erkennbaren Elemente gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
task_sys_id	Aufgabenbezeichner (ordnet Security Incident erkennbaren Elementen zu).
Erkennbare Elemente	IP-Adressen, Hash, URLs, Domänennamen.
workflow_current_sys_id	Systembezeichner des aktuellen Datensatzes. (Wird nur verwendet, wenn `task_sys_id`, Eingaben für erkennbare Elemente sind nicht verfügbar.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Erkennbare Elemente	Gefilterte erkennbare Elemente

Aktivität „Sichtungen von persistenten erkennbaren Elementen“.

Die Workflow-Aktivität **„Persistent Observable Sightings“** ruft erkennbare Elemente aus der Drittanbieterintegration ab.

Die Aktivität **„Persistent Observable Sightings“** kann mit jedem Workflow verwendet werden, um in der Drittparteiintegration gefundene erkennbare Elemente aufzuzeichnen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Erkennbare Elemente abgerufen.
Fehler	Beim Versuch, erkennbare Elemente zu sammeln, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
SichtungenAntwort	
Aufgaben-ID	Aufgabenbezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	

Aktivität „Sichtungsabfragen für erkennbares Element abrufen“.

Die Workflow-Aktivität **„Abfragen von erkennbaren Elementen abrufen“** ruft Abfragen aus der Integrationskonfiguration ab.

Die Aktivität **„Abfragen zu Sichtungen von erkennbaren Elementen abrufen“** kann mit jedem Workflow verwendet werden, um Abfragen abzurufen, die mit dem **Startprogramm für parallele Flows**an die angegebene Implementierung gesendet werden.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Abfragen gefunden.
Fehler	Beim Versuch, Abfragen abzurufen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
Erkennbare Elemente	Liste der gefilterten erkennbaren Elemente.
capabilities	Liste der unterstützten Fähigkeiten.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
queries	Suchzeichenfolge.
Abfrageanzahl	Anzahl der auszuführenden Abfragen.

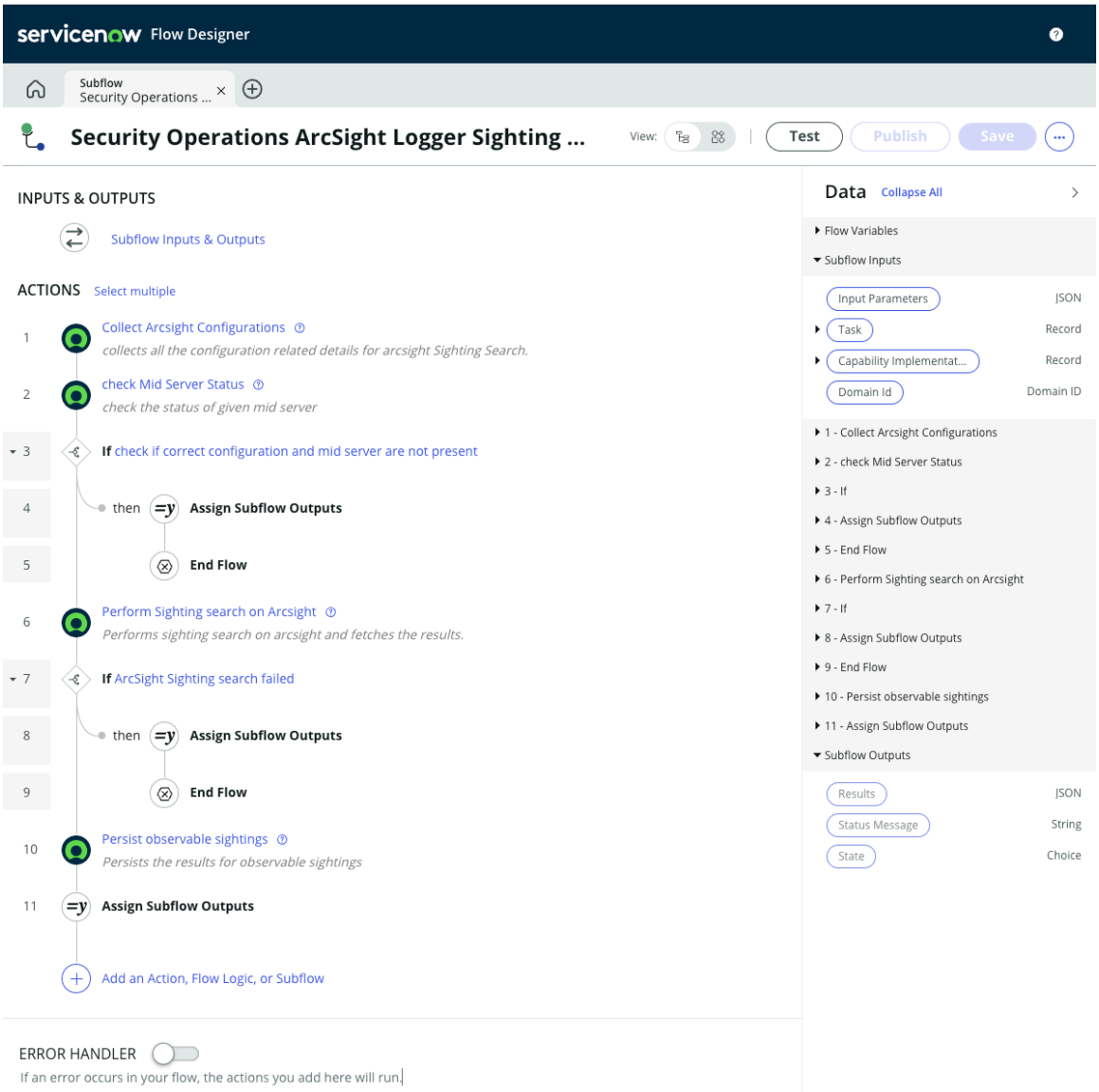
Security Operations: Sichtungssuch-Flow für Arcsight Logger

Der Flow**„Security Operations – ArcSight Logger Sightings Search“** ist die Implementierung für die Splunk-Integration, die durch die **Security Operations-Integration – Sightings-Such-Flow**gestartet wird.

Erforderliche Rolle: sn_si_analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichtungssuche in Arcsight Logger



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Security Operations – Elasticsearch Sightings-Such-Flow

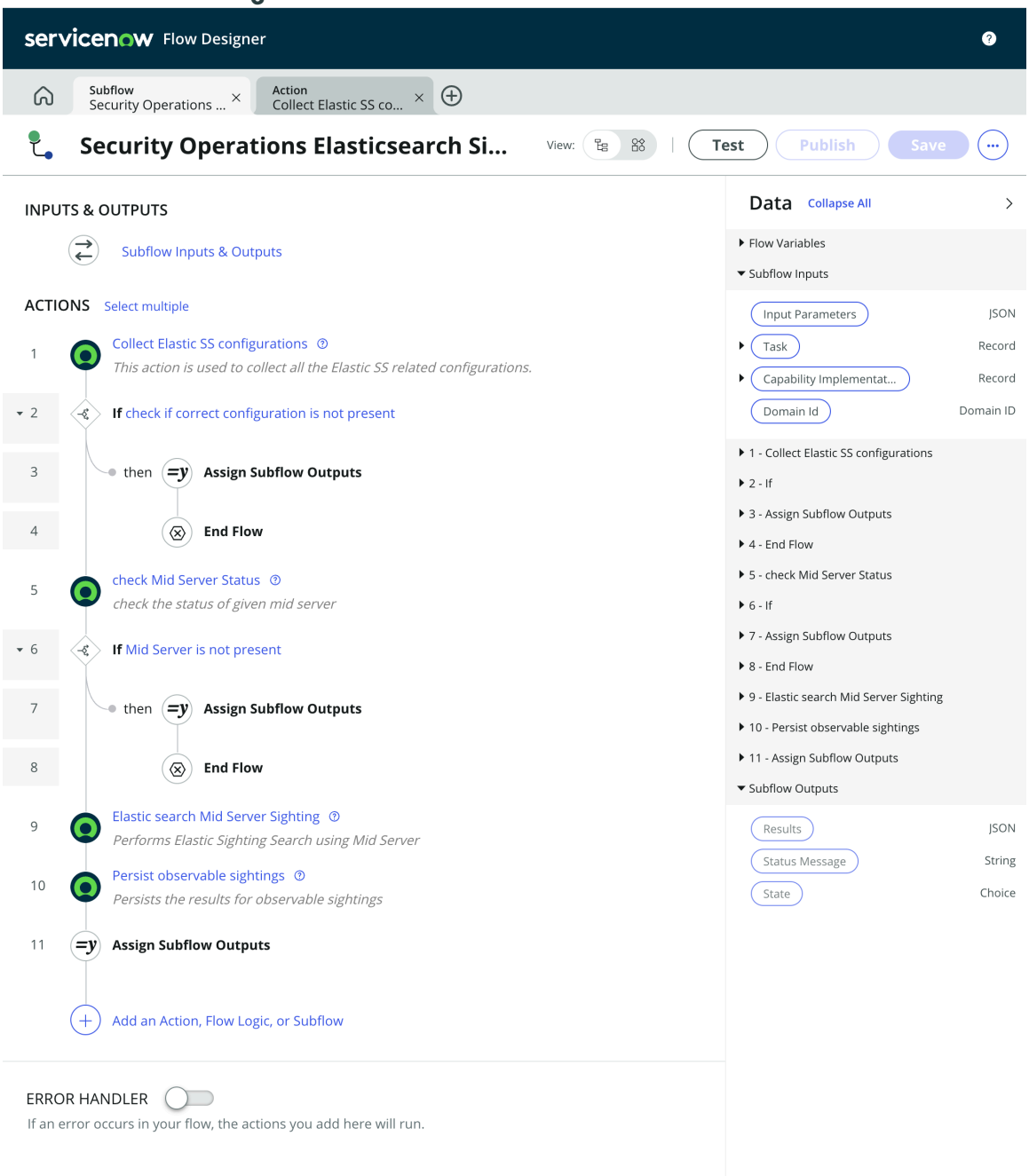
Der Flow**„Security Operations - Elasticsearch Sightings Search“** ist die Elasticsearch-Implementierung, die vom Flow „ **Security Operations Integration – Sightings Search“** gestartet wird.

Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elasticsearch Sichtungssuche



Automatische Übersetzung

Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

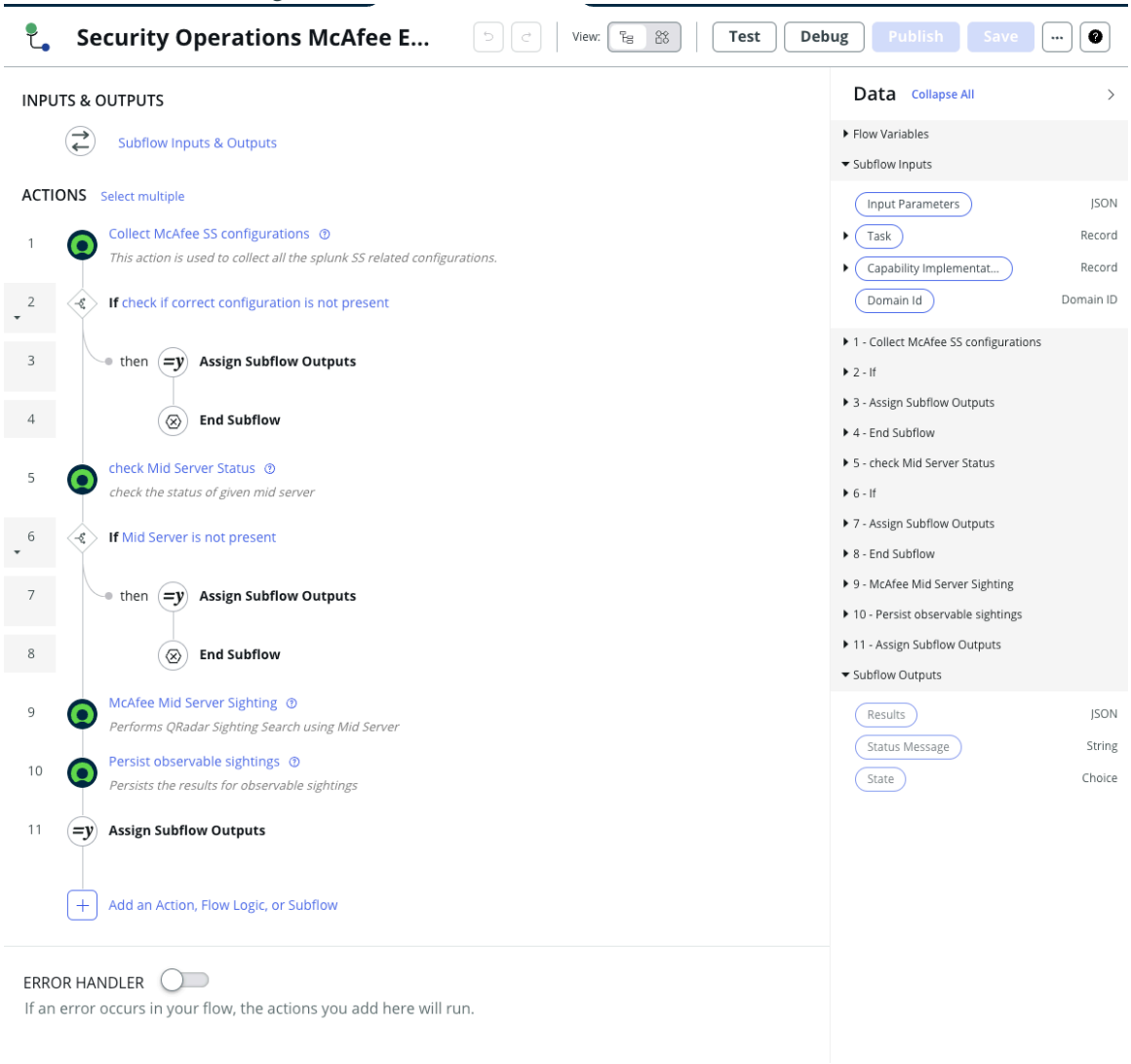
Security Operations – McAfee ESM-Sichtungssuch-Flow

Der Flow**„Security Operations – McAfee ESM-Sichtungssuche“** ist die Implementierung für die Implementierung der McAfee-Sichtungssuche, die durch **Security Operations-Integration – Flow für die Sichtungssuche**gestartet wird.

Erforderliche Rolle: sn_si_analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

McAfee ESM Sichtungssuche



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

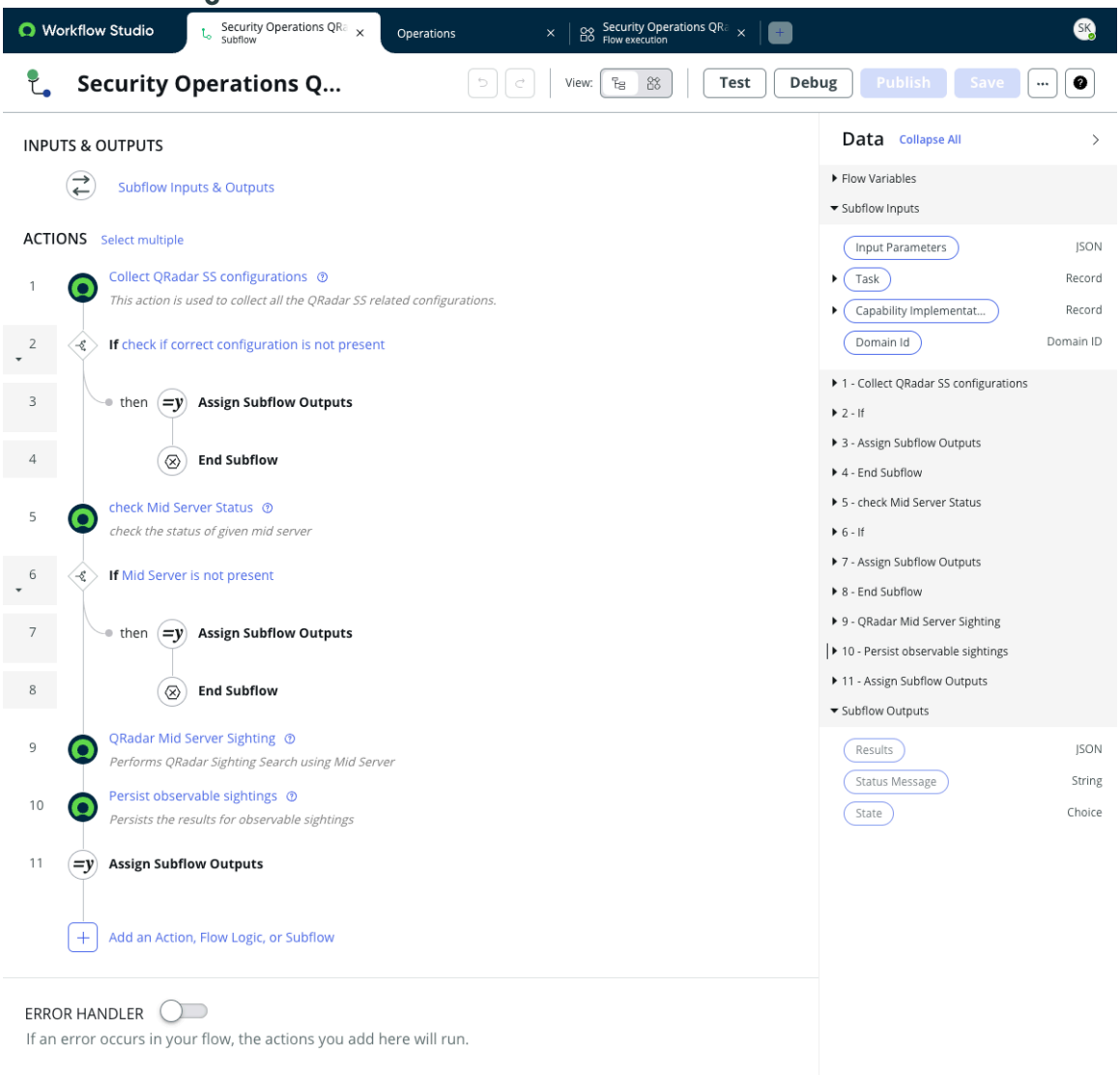
Security Operations – QRadar-Sichtungssuch-Flow

Der Flow**„Security Operations – QRadar-Sichtungssuche“** ist die Implementierung für die IBM QRadar-Integration, die durch den **Flow „Security Operations Integration – Sichtungssuche“**gestartet wird.

Erforderliche Rolle: sn_si_analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

QRadar-Sichtungssuche



Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Security Operations Integration - Splunk Sightings Search Flow

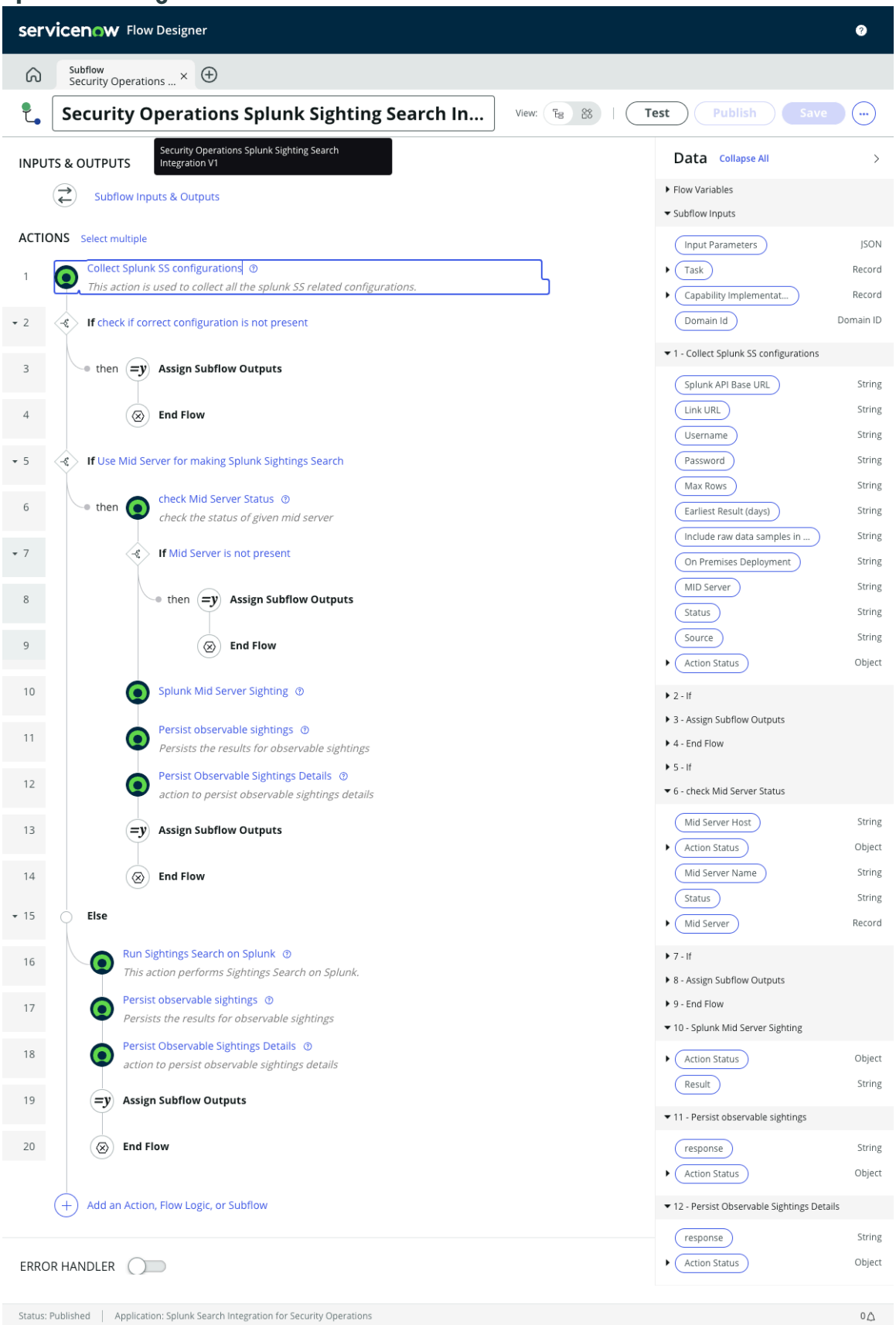
Der Flow**„Security Operations – Splunk-Sichtungssuche“** ist die Implementierung für die Splunk-Integration, die durch den **Flow „Security Operations Integration – Sichtungssuche“**gestartet wird.

Erforderliche Rolle: sn_si_analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunk-Sichtungssuche



Automatische Übersetzung

Spezifische Aktivitäten für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichtungssuchergebnisse anzeigen

Sie können Ergebnisse der Sichtungssuche für interne und externe schädliche Indikatoren überprüfen.

Vorbereitungen

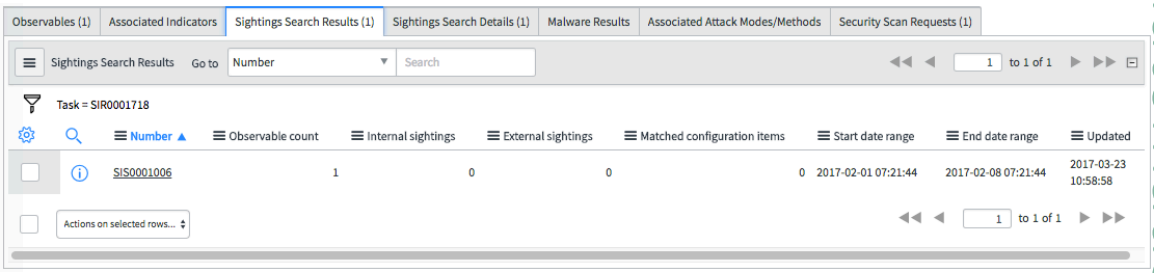
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

.

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie die Registerkarte **Sichtungssuchergebnisse** in der Gruppe „Zugehörige **IoC-Liste anzeigen“** aus, um die Liste der Sichtungssuchen anzuzeigen.



Hinweis:
Diese Daten können für Trusted Security Circlefreigegeben werden.

Ergebnisse der Sichtungssuche

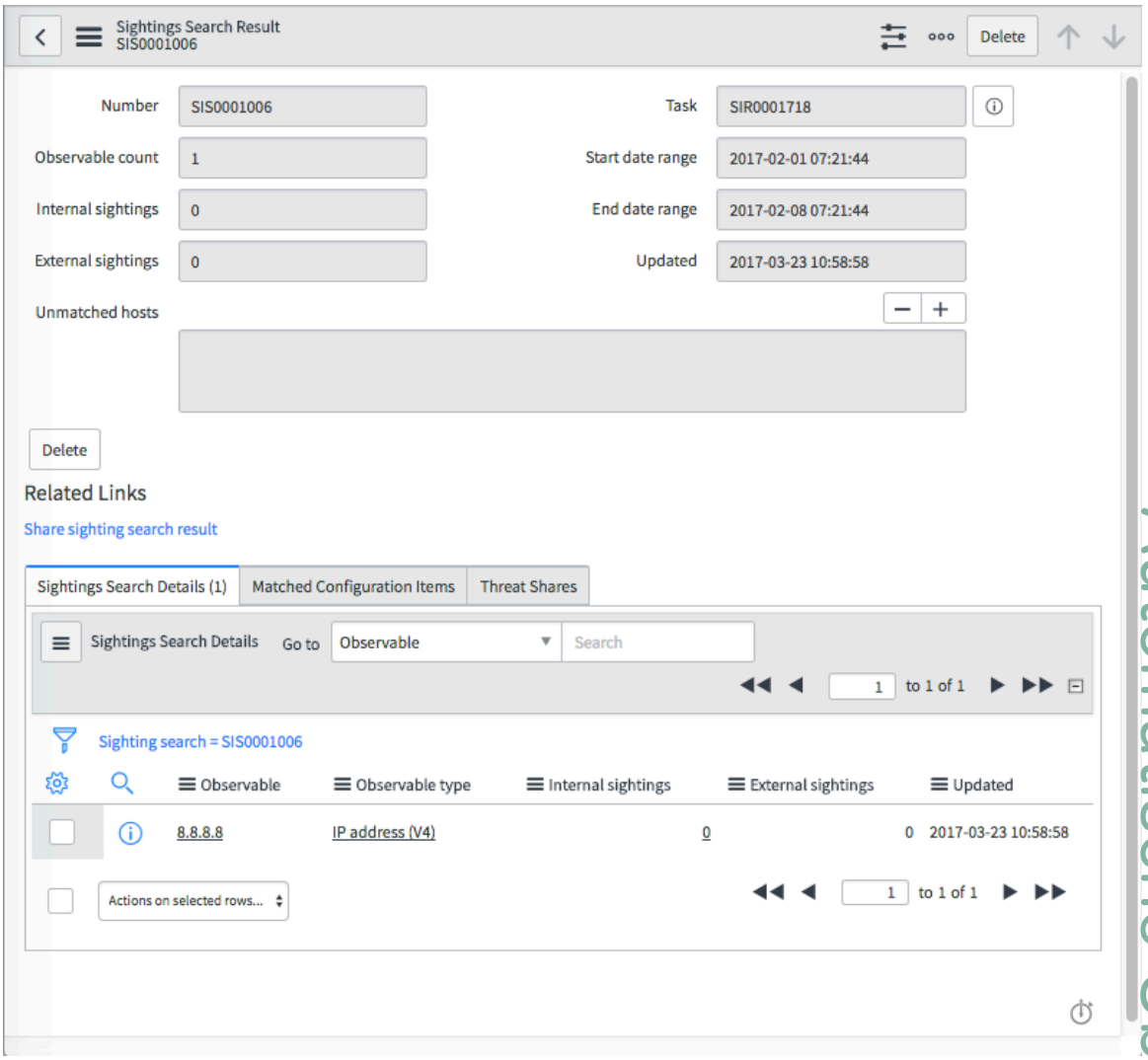
Ergebnis	Beschreibung
Nummer	Bezeichner für die Sichtungssuche.
Anzahl der erkennbaren Elemente	Anzahl der gesuchten erkennbaren Elemente.
Interne Sichtungen	Aggregierte Anzahl interner Sichtungen.
Externe Sichtungen	Aggregierte Anzahl externer Sichtungen. (Erhalten aus der Bedrohungsfreigabe.)
Übereinstimmende Konfigurationselemente	Aggregierte Anzahl der Konfigurationselemente, die einem vorhandenen Datensatz in Ihrer CMDBentsprechen.
Startdatumsbereich	Zeit, mit der Suche nach Sichtungen zu beginnen
Enddatumsbereich	Zeit, die Suche nach Sichtungen zu beenden.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

So zeigen Sie die Details einer einzelnen Suche an:

3. Klicken Sie auf eine Sichtungssuche in der Liste mit **den Suchergebnissen für Sichtungen**.
Das Formular „Suchergebnis für Sichtungen“ wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Formular „Sichtungssuchergebnisse“.

Detail	Beschreibung
Nummer	Bezeichner für interne Sichtungssuche.
Anzahl der erkennbaren Elemente	Anzahl der erkennbaren Elemente, nach denen diese Abfrage gesucht hat.
Interne Sichtungen	Anzahl der internen Sichtungen für diese Suche.
Externe Sichtungen	Anzahl der externen Sichtungen für diese Suche. (Erhalten von Trusted Security Circle.)
Nicht übereinstimmende Hosts	Liste potenzieller Konfigurationselemente für diese Suche, die keinen Datensätzen in Ihrer CMDBzugeordnet wurden.
Aufgabe	Bezeichner der Security Incident-Aufgabe.
Startdatumsbereich	Startzeit der Sichtungssuche.
Enddatumsbereich	Zeitpunkt, zu dem die Sichtungssuche beendet wurde.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detail	Beschreibung
Details einer Sichtungssuche	Typ, Anzahl der Sichtungen und Änderungsdatum.
Übereinstimmende Configuration Items	Anzahl der Konfigurationselemente, die mit einem vorhandenen Datensatz in Ihrer CMDBübereinstimmen. Listet das CI und die Sichtung auf.
Bedrohungsfreigaben	Liste der für Trusted Security Circlefreigegebenen Bedrohungen.

Teilen Sie Ergebnisse von Sichtungssuchen

Sie können lokale Sichtungsdetails oder Ergebnisse, die einer bestimmten Suche zugeordnet sind, für Ihren Trusted Security Circle freigeben.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird

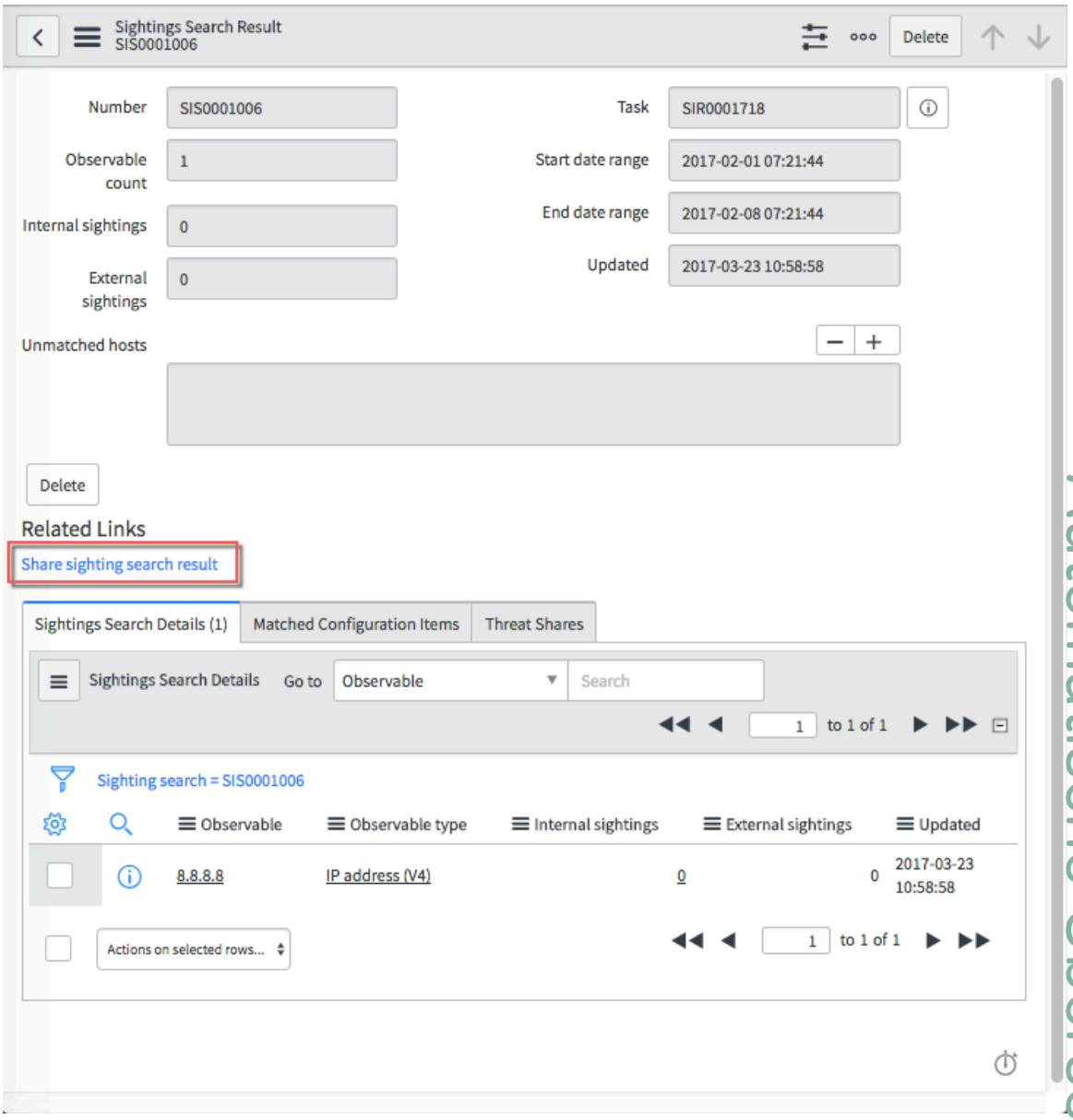
Die Freigabe kann mithilfe der folgenden Security Incident Response- **Eigenschaften**automatisiert werden.

- Gibt die Ergebnisse einer Sichtungssuche automatisch für den standardmäßigen vertrauenswürdigen ServiceNow-Kreis frei
- Schließen Sie erkennbare Elemente ohne lokale Sichtungen ein, wenn Sie Ergebnisse der Sichtungssuche automatisch freigeben
- Reagieren Sie mit lokalen Sichtungen, wenn von einem vertrauenswürdigen Kreis eine Bedrohungsfreigabe empfangen wird

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Klicken Sie auf die zugehörige Liste **IoC anzeigen**, und wählen Sie die Registerkarte **Sichtungssuchergebnisse** aus, um die Liste der Sichtungssuchen anzuzeigen.
3. Klicken Sie auf ein Sichtungssuchergebnis.

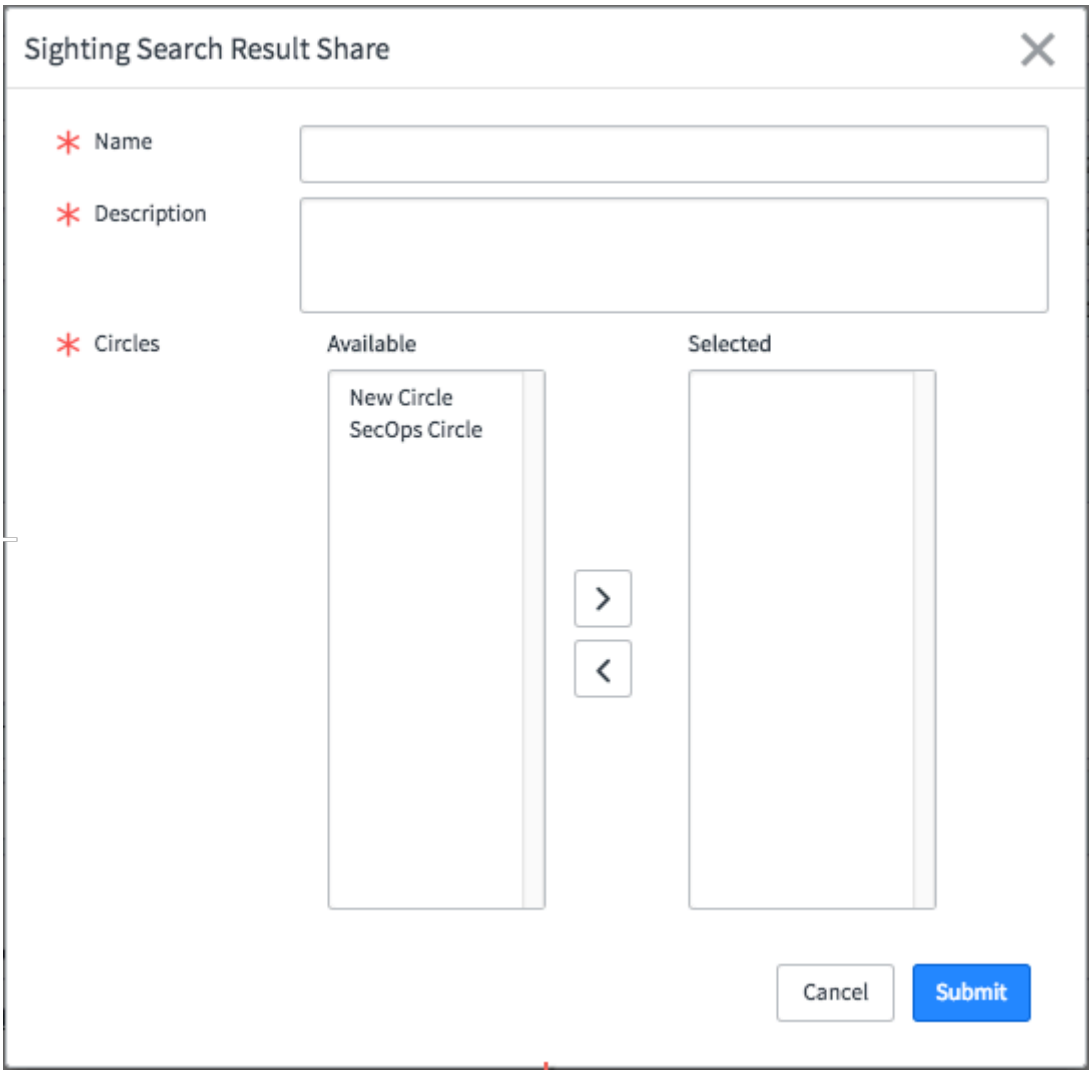
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie im Formular **„Sichtungssuchergebnis“**auf den zugehörigen Link **Sichtungssuchergebnis teilen**.
   Das Dialogfeld „Freigabe des Sichtungssuchergebnisses“ wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Geben Sie einen **Namen** für diesen freigegebenen Datensatz des erkennbaren Elements ein.
6. Geben Sie eine **Beschreibung**der freizugebenden erkennbaren Elemente ein.
7. Wählen Sie **Kreise** aus, für die Sie die erkennbaren Elemente freigeben möchten.
8. Klicken Sie auf **Absenden**.
   Die erkennbaren Elemente werden für den angegebenen vertrauenswürdigen Kreis freigegeben.

Geben Sie erkennbare Elemente aus einem Security Incident frei

Erkennbare Elemente können aus einem Security Incident in Security Incident Response für Mitglieder in Ihrem vertrauenswürdigen Kreis freigegeben werden.

Vorbereitungen

Erforderliche Rolle: sn_si.analyst

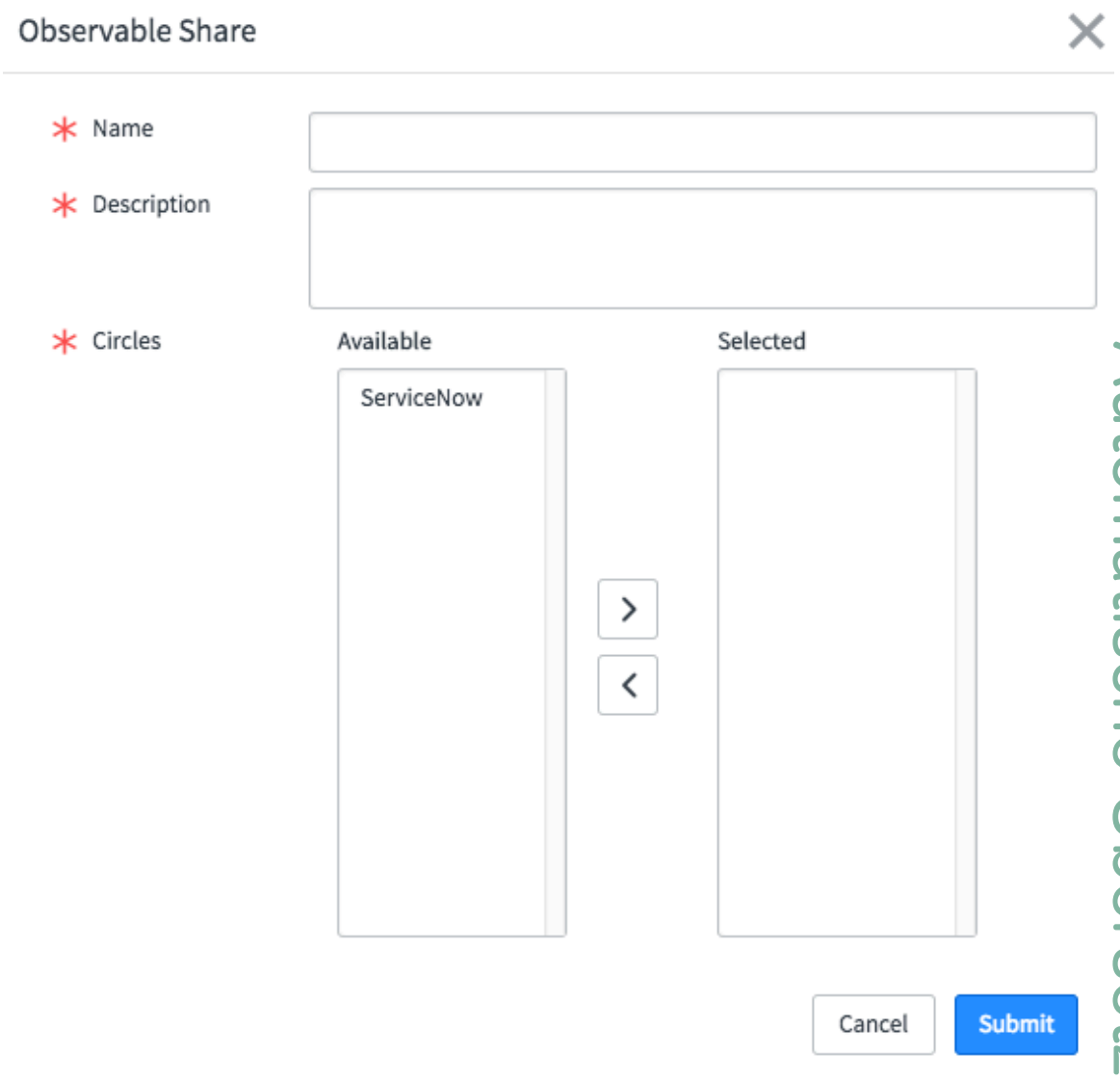
Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie die Registerkarte **Erkennbare Elemente** in der Gruppe Zugehörige **IoC-Liste anzeigen aus**.
3. Klicken Sie auf ein erkennbares Element.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie im Formular **„Erkennbares Element** “ auf den zugehörigen Link **Erkennbares Element freigeben**.
   Das Dialogfeld „Freigabe erkennbarer Elemente“ wird angezeigt.



5. Geben Sie einen **Namen** für diesen Bedrohungsfreigabedatensatz ein.
6. Geben Sie eine **Beschreibung**der ausgewählten erkennbaren Elemente ein.
7. Wählen Sie **Kreise** aus, für die Sie die erkennbaren Elemente freigeben möchten.
8. Klicken Sie auf **Absenden**.
   Die erkennbaren Elemente werden für den angegebenen vertrauenswürdigen Kreis freigegeben.
9. Sie können die Datensätze für die Bedrohungsfreigabe anzeigen, indem Sie auf die Registerkarte **Bedrohungsfreigaben** klicken.
10. Wenn eines der freigegebenen erkennbaren Elemente Sichtungen enthält, werden die Sichtungen ebenfalls freigegeben und können durch Klicken auf die Registerkarte **Sichtungen** angezeigt werden.

Zeigen Sie Details der Sichtungssuche an

Überprüfen Sie die zusammengefassten Details aller Sichtungssuchen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.analyst

Warum und wann dieser Vorgang ausgeführt wird
.

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie die Registerkarte **Details der Sichtungssuche** in der Gruppe „Zugehörige **IoC-Liste anzeigen"** aus, um die Liste der Sichtungssuchen anzuzeigen.

Hinweis:
Diese Daten können für Trusted Security Circlefreigegeben werden.

Details einer Sichtungssuche

Detail	Beschreibung
Erkennbares Element	Liste aller erkennbaren Elemente, nach denen die Abfrage gesucht hat.
Erkennbarer Typ	
Interne Sichtungen	Anzahl der internen Sichtungen für alle Suchen.
Externe Sichtungen	Anzahl der externen Sichtungen für alle Suchen. (Erhalten aus der Bedrohungsfreigabe.)
Sichtungssuche	Bezeichner für die Sichtungssuche.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

Automatische Übersetzung

Security Operations-Integration – Funktionalität zur Bedrohungssuche

Die Fähigkeit **„Bedrohungssuchen" führt Threat** Intelligence-Suchen durch, um zu bestimmen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsrisiken zugeordnet sind.

Die Fähigkeit **„Bedrohungssuchen"** verfügt über den Workflow Security Operations Integration – Flow zur Bedrohungssuche. Wenn der Fähigkeits-Workflow ausgeführt wird, werden zusätzliche Workflows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die für die Suche nach den ausgewählten erkennbaren Elementen verwendet werden soll, oder Sie können die Suche mit allen Implementierungen durchführen.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden in Produktmenüs keine Fähigkeitsaktionen angezeigt.

Security Operations Integration – Flow zur Bedrohungssuche

Der Flow der Funktionalität **„Security Operations Integration – Threat Lookup"** greift auf verfügbare Implementierungen der Bedrohungssuche zu und führt die jeweils zugehörigen Implementierungs-Flows aus, um Bedrohungssuchen für ausgewählte erkennbare Elemente durchzuführen.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

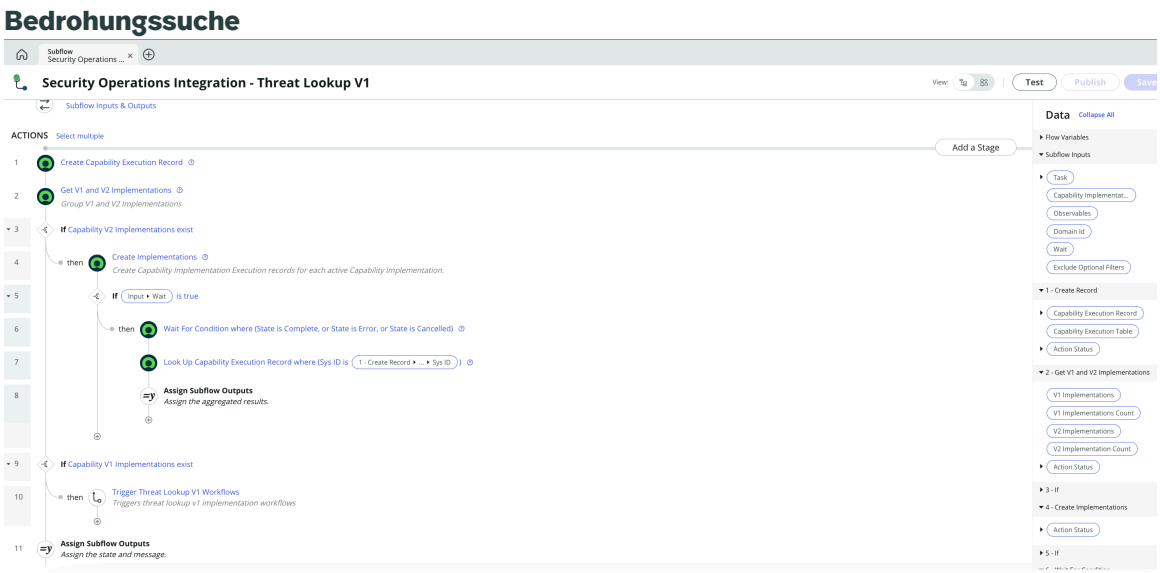
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow kann auf folgende Weise ausgelöst werden.

- indem Sie ein oder mehrere erkennbare Elemente in der Liste „Erkennbare Elemente“ auswählen und in der Auswahlliste **Aktionen für ausgewählte Zeilen** die **Option Bedrohungssuche ausführen** auswählen.
- indem Sie einen Datensatz eines erkennbaren Elements öffnen und auf den zugehörigen Link **Bedrohungssuche ausführen** klicken.
- Aus der zugehörigen Liste „Erkennbare Elemente“ in einem Security Incident

Anschließend können Sie mit jeder Methode angeben, welche Suchimplementierungen zum Scannen der ausgewählten erkennbaren Elemente verwendet werden sollen. Die zugehörigen Implementierungs-Flows werden ausgeführt, um die Suchvorgänge durchzuführen.



Spezifische Aktionen für diesen Flow werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations.

Zu den Flow-Prozessaktionen gehören:

- Aktion „Unterstützte Sicherheitsfähigkeiten abrufen“.
- Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.

Ändern Sie die Reihenfolge der Flow-Ausführung

Implementierungen der Integrationsfähigkeit geben den auszuführenden Flow an. Im Basissystem werden Flows nacheinander in der in der Implementierung angegebenen Reihenfolge ausgeführt. Sie können die Reihenfolge nach Bedarf ändern.

Vorbereitungen

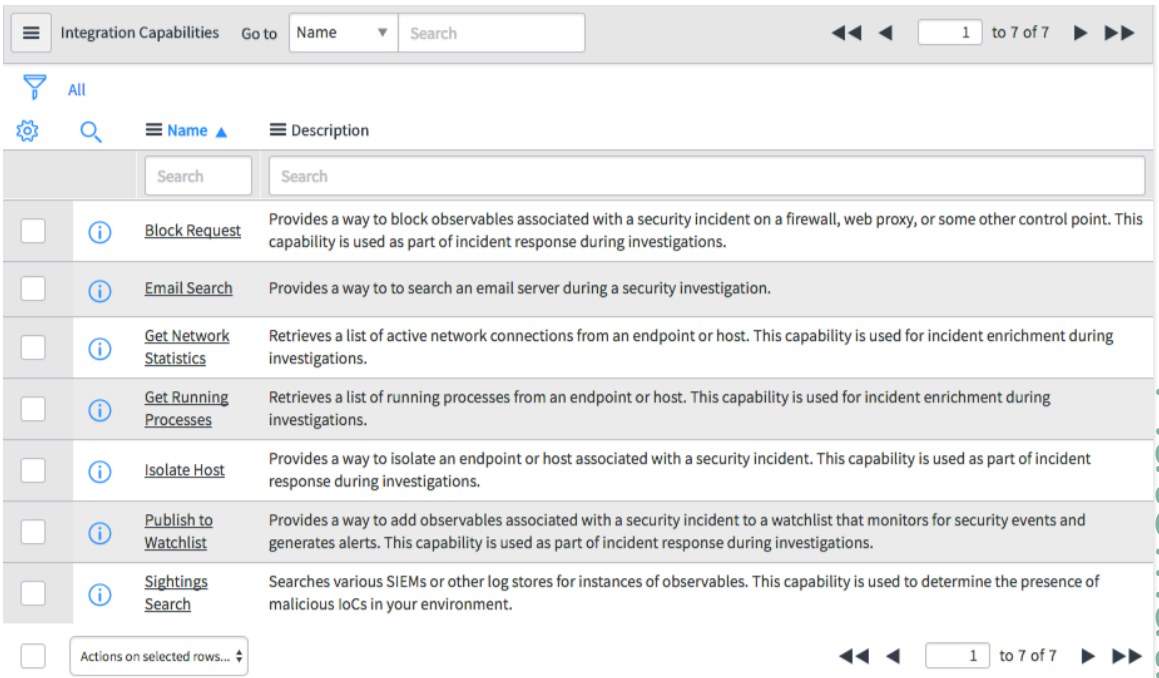
Erforderliche Rolle: sn_sec_cmn.write

Automatische Übersetzung

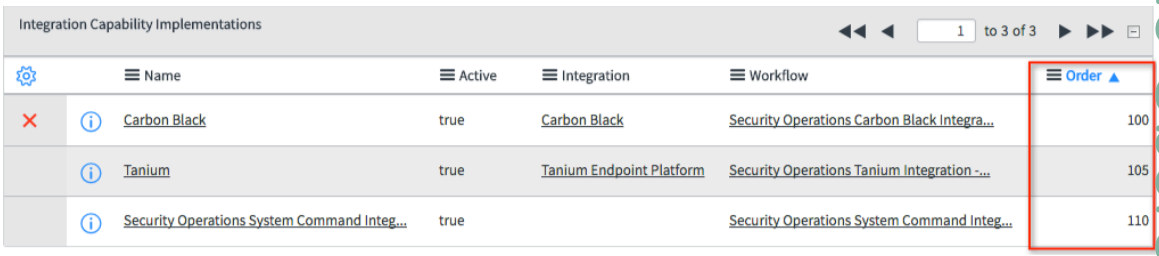
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

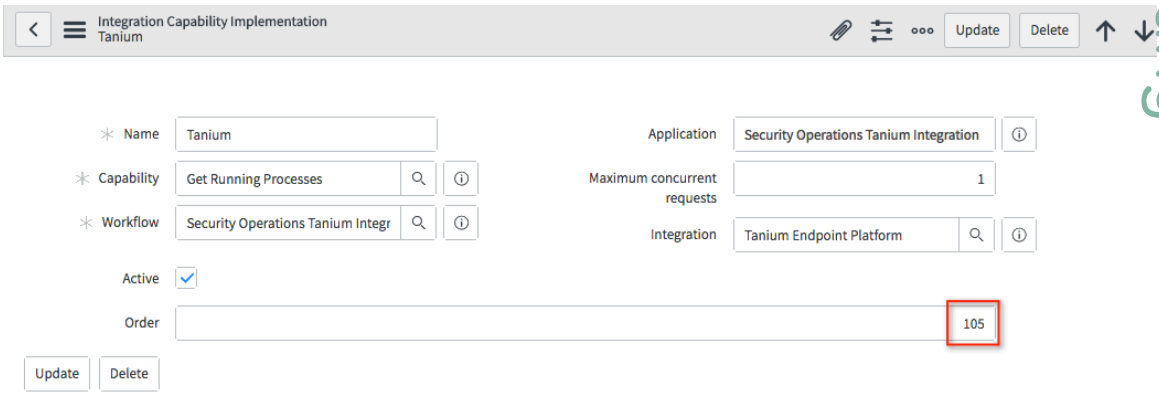
1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationsfunktionen**.



2. Wählen Sie die Integrationsfähigkeit aus, für die Sie die Ausführungsreihenfolge ändern möchten.



3. Wählen Sie die Implementierung aus, die Sie ändern möchten.



4. Ändern Sie den **Auftrag** in eine höhere oder niedrigere Zahl.
   Niedrigere Zahlen bedeuten eine höhere Ausführungspriorität.
5. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrations-Flows und Orchestration-Aktivitäten von Common Security Operations

Viele der Flows, die Drittanbieterintegrationen zugeordnet sind, beinhalten dieselben Aktivitäten. Zum Beispiel Aktivitäten zum Starten und Abschließen der Verarbeitung.

Ausführungsnachverfolgung: Flow-Aktion beginnen

Mit der Flow-Aktion „Ausführungsnachverfolgung - Begin“ wird der Auditing-Prozess für einen Security Operations Integration-Flow gestartet, der für erkennbare Elemente ausgeführt wird.

Die Aktion „Ausführungsnachverfolgung – Flow beginnen“ kann mit jedem Flow verwendet werden, um mit der Aufzeichnung des Flow-Fortschritts in einem Audit zu beginnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ein Audit-Datensatz wird erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
capabilityId	System-ID der ausgeführten Integrationsfunktionalität
istImpl	Kennzeichnung, die angibt, ob das Audit für einen Integrationsfähigkeits-Flow oder einen Integrationsfähigkeits-Implementierungs-Flow durchgeführt wird. Mögliche Werte: • „falsch“ - bedeutet Auditing für einen abstrakten Integrationsfähigkeits-Flow wie z. B. Sichtungssuche. (Standard) • wahr – bezeichnet Auditing in einem Implementierungs-Flow für eine Integrationsfähigkeit. Zum Beispiel Splunk oder Elasticsearch.
Aufgaben-ID	System-ID für jede Aufgabe, die dem Flow zugeordnet ist.
observableList	Eine oder mehrere erkennbare SysIDs zum Ausführen der gewünschten Aktion Wird als Flow-Eingabe verwendet.
flowContextId	Systembezeichner des zugeordneten Flow-Kontextdatensatzes. Wird vom System bereitgestellt.
FlowName	Name des Flows. Wird vom System bereitgestellt.
parentCapabilityExcutionId	Systembezeichner des Audit-Datensatzes, von dem der Implementierungs-Flow gestartet wurde. Nur erforderlich für Implementierungs-Flows für Integrationsfähigkeiten wie Splunk, Elasticsearch und VirusTotal.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
capabilityExecutionId	Systembezeichner des Audit-Datensatzes.

- Aktion „Unterstützte Sicherheitsfähigkeiten abrufen“.
- Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.

Nachverfolgung der Fähigkeitsausführung – Flow-Aktion abschließen

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Nachverfolgung von“ aktualisiert den Audit-Datensatz, wenn der Flow abgeschlossen ist.

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Abschließen“ kann mit jedem Flow verwendet werden, um den Abschluss des Flows aufzuzeichnen.

Hinweis:
Das **Rückgabewert-** Array aus der Core-Flow-Aktion **des parallelen Startprogramms** enthält ein Array von Ergebnissen aus allen ausgeführten Integrations-Flows und zeigt den erfolgreichen Abschluss der Ausführungsnachverfolgung an.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Audit-Datensatzes wird auf **Abgeschlossen**aktualisiert.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
capabilityExecutionId	Systembezeichner für den Audit-Datensatz. Dieses Feld war die Ausgabe einer der Aktivitäten für „Auditing beginnen“.
FlowName	Name des Flows. Wird vom System bereitgestellt.
Nachricht	Abschlussmeldung.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachverfolgung der Fähigkeitsausführung: Fehler-Flow-Aktion

Mit der Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Fehler“ wird ein Fehler im Audit-Datensatz aufgezeichnet.

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Fehler“ kann mit jedem Flow verwendet werden, um eine Fehlerbedingung aufzuzeichnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Audit-Datensatzes wird auf **„Fehler“** festgelegt, und eine Meldung mit einem entsprechenden Fehler wird aufgezeichnet.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
capabilityExecutionId	Systembezeichner für den Audit-Datensatz. Dies ist die Ausgabe einer der Begin-Auditing-Aktivitäten.
errorMessage	Meldung, die den Grund für den Fehler angibt.
FlowName	Name des Flows. Wird vom System bereitgestellt.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

Fähigkeit – Aktivität „CIs bestimmen“.

Die Workflow-Aktivität Funktionalität – CIs bestimmen bestimmt, welche Configuration Items (CIs) in den Workflow aufgenommen werden sollen.

Die Aktivität Fähigkeit – CIs bestimmen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche CIs in den Workflow aufgenommen werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Konfigurationselemente gefunden.
Fehler	Keine CIs gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
task_sys_id	Aufgabenbezeichner (ordnet Security Incidents CIs zu).
cis_affected	Configuration Items

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
cis_affected	Gefilterte CIs
task_sys_id	Aufgabenbezeichner (ordnet Security Incidents CIs zu).

Flow-Aktion zum Erstellen von Datensätzen mit Ergänzungsdaten

Mit der Flow-Aktion **„Ergänzungsdatensätze erstellen“** werden Ergänzungsdatensätze erstellt oder aktualisiert, die im Flow verwendet werden sollen.

Die Flow-Aktion **„Ergänzungsdatensätze erstellen“** kann mit jedem Flow verwendet werden, um Ergänzungsdatensätze im Flow zu aktualisieren.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ergänzungsdatensatz aktualisiert.
Fehler	Ergänzungsdatensatz nicht aktualisiert. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
task_id	Aufgabenbezeichner.
Content	Rohinhalt (Daten der laufenden Prozesse).
„richment_mapping_id“	Bezeichner der Ergänzungszuordnung.
ci_id	Bezeichner des Konfigurationselements.
Referenzwert	Nicht verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis	Mit dem Skript „enrichmentUtils“ erstellte GlideRecords.

FQDN-Flow-Aktion für Konfigurationselement abrufen

Die zugehörigen Listen namens **Security Common Orchestration** > **FQDN für Konfigurationselement abrufen** Die Flow-Aktion ruft den vollqualifizierten Domänennamen (FQDN) eines Konfigurationselements ab. Diese Flow-Aktion kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Flow-Aktion Konfigurationselement-FQDN abrufen kann mit jedem Flow verwendet werden, um den vollqualifizierten Domänennamen (FQDN) eines Konfigurationselements abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Eingabevariablen

Variable	Beschreibung
cmdb_ci.id [Zeichenfolge]	Der Systembezeichner (sys_id) eines Configuration Item-Datensatzes.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
fqdn [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) des Konfigurationselements.

Zusätzliche Hinweise

Das Feld „fqdn“ im Konfigurationselement muss ausgefüllt sein.

Aktivität „Erkennbare Elemente“ bestimmen

Die Workflow-Aktivität **„Erkennbare Elemente bestimmen“** bestimmt, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen

Die Aktivität **„Erkennbare Elemente bestimmen“** kann mit jedem Workflow verwendet werden, um zu bestimmen, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Erkennbare Elemente gefunden
Fehler	Keine erkennbaren Elemente gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
task_sys_id	Aufgabenbezeichner (ordnet Security Incident erkennbaren Elementen zu).
Erkennbare Elemente	IP-Adressen, Hash, URLs, Domänennamen.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Erkennbare Elemente	Gefilterte erkennbare Elemente

Aktion „Unterstützte Sicherheitsfähigkeiten abrufen“.

Mit der Flow-Aktion „Unterstützte Fähigkeiten abrufen“ werden der Name und die Anzahl der Integrationen abgerufen, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktion Unterstützte Fähigkeiten abrufen kann mit jedem Flow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

Ergebnisse

Mögliche Ergebnisse für diese Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Integration, die die gefundene Fähigkeit unterstützt.
Fehler	Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktionsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
capabilityName	Name der Fähigkeit.
Aufgaben-ID	System-ID für jede Aufgabe, die dem Flow zugeordnet ist.
domainId	System-ID für eine beliebige Domäne, die dem Flow zugeordnet ist.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
unterstützte Funktionen	Liste der Integrationen, die diese Fähigkeit unterstützen.
capabilityCount	Anzahl der Integrationen, die diese Fähigkeit unterstützen.

Nachverfolgung der Fähigkeitsausführung: Aktion „Keine Implementierungen“.

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktion „Nachverfolgung der Fähigkeitsausführung – Keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Flow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

Ergebnisse

Mögliche Ergebnisse für diese Aktion sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **„Fehler“** festgelegt, und eine Meldung mit einem entsprechenden Fehler wird aufgezeichnet.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
capabilityExecutionId	Systembezeichner für den Audit-Datensatz. Ausgabe der Aktion, die zum Starten der Ausführungsnachverfolgung verwendet wird.
FlowName	Name des Flows. Wird vom System bereitgestellt.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Compliance-Suchaktion

Mit der Aktion „Compliance-Suche erstellen“ wird mithilfe der definierten Suchabfragen eine Compliance-Suche für E-Mails auf den angegebenen Exchange-Servern erstellt. Außerdem wird der Name der erstellten Compliance-Suche zurückgegeben.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
search_query	Obligatorische Suchabfrage, die verwendet wird, um in Exchange Server in allen Postfächern E-Mails zu finden.
Exchange-Standort	Obligatorisches Standortfeld, das für die Suche im definierten Standort verwendet wird. Werte sind: • Alle • Name eines bestimmten Postfachs
targetId	Pflichtfeld für den Zielhostbezeichner, an dem sich der Exchange-Server befindet.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Name der erstellten Compliance-Suche.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Fehler beim Erstellen der Suche	Wenn die Suche aufgrund einer Ausnahme in Exchange Server fehlschlägt.
Suche erfolgreich erstellt	Wenn die Suche erfolgreich erstellt wurde.
Fehler beim Erstellen der Suche aufgrund eines Analysefehlers	Wenn die Suche aufgrund eines Parsing-Problems fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Rufen Sie die IP aus der CI-Aktivität ab

Diese Workflow-Aktivität bestimmt die IPV4-Adresse, die einem Configuration Item (CI) zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität **IP von CI abrufen** kann mit jedem Workflow verwendet werden, um die IPv4-Adresse eines CI abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
ci_sys_id [Zeichenfolge]	Systembezeichner des Konfigurationselements

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ip_addr [Zeichenfolge]	IPv4-Adresse. Wenn die IP-Adresse nicht bestimmt werden kann, ist dieser Wert leer.

Austrittsbedingungen

Mögliche Ergebnisse für diese Aktivität sind:

Bedingungen

Bedingung	Beschreibung
Erfolg	Es wurde eine IPv4-Adresse zurückgegeben.
Fehler	Es konnte keine IPv4-Adresse ermittelt werden.

Flow-Aktion „Netzwerkstatistiken über Netstat“ abrufen

Mit der Flow-Aktion „Security Common Orchestration – Netzwerkstatistiken über Netstat abrufen“ werden die Netzwerkstatistiken für eine betroffene Ressource in einem Windows-basierten System abgerufen. Diese Flow-Aktion kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Flow-Aktion „Netzwerkstatistiken über netstat abrufen“ kann mit jedem Flow verwendet werden, um Netzwerkstatistiken aus einem Windows-basierten System abzurufen. Der Computer wird mit dem Befehl **netstat** einschließlich der Parameter **„-a“** und **„-o“** abgefragt. Um die Ausgabedaten zu verbessern, wird auch der Befehl **„get-process“** aufgerufen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Netzwerkstatistiken wurden im JSON-Format abgerufen.
Fehler	Beim Versuch, Netzwerkstatistiken abzurufen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Variable	Beschreibung
Ziel [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des Zielsystems.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Antwort [Zeichenfolge]	Eine JSON-Zeichenfolge, die die aktuell auf dem Zielcomputer laufenden Prozesse darstellt. JSON-Daten enthalten: **pid** Prozessbezeichner **local _port** Lokaler Port für die Netzwerktransaktion **state** Status der TCP-Verbindung. **Hinweis:** Dieses Feld ist für UDP-Verbindungen null. **local_address** Lokaler vollqualifizierter Domänenname (FQDN) oder IP-Adresse **remote_address** Vollqualifizierter Remote-Domänenname (FQDN) oder IP-Adresse **protocol** TCP oder UDP **remote_port** Remote-Port der Netzwerktransaktion **path** Der Dateipfad der ausführbaren Prozessdatei **hash**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
	Der Hash-Wert der ausführbaren Prozessdatei. Der Hashwert ist SHA-256 für PowerShell V4 oder höher. Andernfalls befindet sich der Hash in MD5.

Beschränkungen

Der MID Server muss PowerShellunterstützen.

SHA-256-Hash erfordert PowerShell V4.

Rufen Sie laufende Prozesse über die WMI-Aktivität ab

Die Workflow-Aktivität**„Laufende Prozesse abrufen“** ruft die laufenden Prozesse eines Configuration Item in einem Windows-basierten System ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität **„Laufende Prozesse über WMI abrufen“** kann mit jedem Workflow verwendet werden, um laufende Prozesse in einem Windows-basierten System abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Ziel [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des Zielsystems.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Antwort [Zeichenfolge]	Eine JSON-Zeichenfolge, die die aktuell auf dem Zielsystem laufenden Prozesse darstellt. JSON-Daten enthalten: **pid** Der Prozessbezeichner **name** Der Name des Prozesses Außerdem, falls verfügbar: **Besitzer** Der Name des Prozessverantwortlichen **owner_sid**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
	Der Systembezeichner des Prozessverantwortlichen **owner_domain** Die Domäne des Prozessverantwortlichen **path** Der Dateipfad der ausführbaren Prozessdatei **hash** Der Hash-Wert der ausführbaren Prozessdatei. Der Hashwert ist SHA-256 für PowerShell V4 oder höher. Andernfalls befindet sich der Hash in MD5.

Beschränkungen

Der MID Server muss **PowerShell**unterstützen.

SHA-256-Hash erfordert PowerShell V4.

Aktion zum Überprüfen des Compliance-Suchstatus

Mit der Aktion Compliance-Suchstatus überprüfen wird der Status der erstellten Compliance-Suche auf dem Exchange-Server überprüft. Wenn der Status abgeschlossen ist, werden die Informationen zur E-Mail-Suche zurückgegeben, die für die Compliance-Suche gefunden wurde.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Pflichtfeld für den Zielhostbezeichner, an dem sich der Exchange-Server befindet.
searchName	Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Enthält den Status der Compliance-Suche und die Anzahl der auf dem Exchange-Server gefundenen E-Mails für die Compliance-Suche.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Austrittsbedingungen

Variable	Beschreibung
Suche in Bearbeitung	Wenn der Status der Compliance-Suche ausgeführt wird.
Suche abgeschlossen – keine Bedrohungs-E-Mails gefunden	Wenn der Status der Compliance-Suche abgeschlossen ist und keine E-Mails als Teil der Compliance-Suche gefunden wurden.
Suche abgeschlossen – Bedrohungs-E-Mails gefunden	Wenn der Status der Compliance-Suche abgeschlossen ist und E-Mails als Teil der Compliance-Suche gefunden werden.
Fehler beim Überprüfen des Status	Wenn die Statusüberprüfung aufgrund einer Ausnahme in Exchange Server fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Aktivität „Arbeitsnotizen zur Aufgabe aktualisieren“.

Die Workflow-Aktivität **„Security Common Orchestration – Aufgaben-Arbeitsnotizen aktualisieren“** aktualisiert den Abschnitt **„Aktivität** “ (Arbeitsnotizen) eines Aufgabendatensatzes. Dies ist nützlich für die Protokollierung von Informationen.

Die Aktivität **Aufgaben-Arbeitsnotizen aktualisieren** kann mit jedem Workflow verwendet werden, um die Arbeitsnotizen eines Aufgabendatensatzes zu aktualisieren.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
task_id [Zeichenfolge]	Der Systembezeichner (sys_id) eines Aufgabendatensatzes.
Inhalt [Zeichenfolge]	Die Daten, die in die Arbeitsnotizen einer Aufgabe geschrieben werden.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Gibt an, ob das Update erfolgreich war.

Rollup der Suchinformationen über die Aktivität „Security Incident“.

Die Aktivität **„Suchinformationen zu Security Incident aufrollen“** kann mit jedem Workflow verwendet werden, um Informationen aus einer Bedrohungssuche zu sammeln und eine Zusammenfassung des Inhalts sowie die ID des ursprünglichen Security Incidents in Arbeitsnotizen zur Aufgabe auszugeben.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Zusammenfassung des Suchberichts für Security Incident zusammengefasst.
Fehler	Ursprungsaufgabe und Suchzusammenfassungsbericht sind leer.

Eingabevariablen

Variable	Beschreibung
scanID[Zeichenfolge]	Suchbezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
siId[Zeichenfolge]	Bezeichner des Security Incidents.
Antwort [Zeichenfolge]	Zusammenfassung der Suchergebnisse, einschließlich IoC-Wert, Ergebnis, Fehlergrund, Suchreferenz usw.

Aktualisieren Sie den Security Incident mit dem Workflow für Suchergebnisse

Der Workflow **„Security Incident mit Suchergebnissen aktualisieren“** aktualisiert vorhandene Security Incidents mit Suchergebnissen.

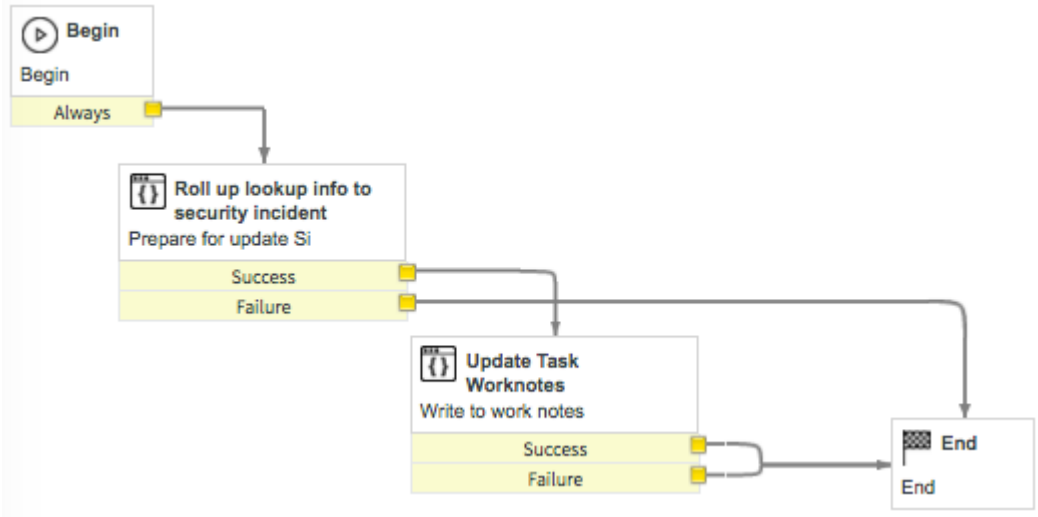
Vorbereitungen
Erforderliche Rolle: sn_si.basic

Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird von einer Geschäftsregel in der Suchtabelle ausgelöst, die überwacht, wenn das Feld **Ergebnis** in Fehlgeschlagen wechselt.

Zu den Workflow-Prozessaktivitäten gehören:

- Rollup der Suchinformationen über die Aktivität „Security Incident“.
- Aktivität „Arbeitsnotizen zur Aufgabe aktualisieren“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aktivität „Erkennbare Elemente auf der Zulassungsliste filtern“.

Mit der Workflow-Aktivität „Gefilterte erkennbare Elemente auf der zulässigen Liste“ werden erkennbare Elemente entfernt, die aus der Liste der erkennbaren Elemente ignoriert werden können. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „Erkennbare Elemente auf der zulässigen Liste filtern“ kann mit jedem Workflow verwendet werden, um erkennbare Elemente zu filtern, bevor eine Aktion ausgeführt wird.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Filterliste erstellt.
Fehler	Beim Versuch, die erkennbaren Elemente zu filtern, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Erkennbare Elemente	Liste der verfügbaren erkennbaren Elemente.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
gefilterteErkennbareElemente	Gefilterte erkennbare Elemente.

Schreiben Sie Inhalt, um ihn als Anhangaktivität aufzuzeichnen

Diese Aktivität schreibt den Inhalt, der aus einer Eingabe übergeben wurde, und erstellt einen festgelegten Anhang zu einem bestimmten Datensatz.

Die Aktivität **Inhalt an Datensatz als Anhang schreiben** kann mit jedem Workflow verwendet werden, um Inhalt zu schreiben und an einen Datensatz anzuhängen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Tabellenname [Zeichenfolge]	Der Tabellenname für den Datensatz. Dieses Eingabefeld ist ein Pflichtfeld.
sysid [Zeichenfolge]	Der Systembezeichner (sys_id) eines Aufgabendatensatzes. Dieses Eingabefeld ist ein Pflichtfeld.
Nutzlast	Der Nur-Text-Inhalt, der als Anhang geschrieben werden soll. Dieses Eingabefeld ist ein Pflichtfeld.
filename	Der Name der Anhangdatei.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Gibt an, ob das Update erfolgreich war.

Rufen Sie die IP aus der CI-Aktivität ab

Mit der Flow-Aktivität IP aus CI abrufen wird die IP-Adresse aus Configuration Items (CIs) erfasst, die im Flow verwendet werden sollen.

Die Aktivität IP von CI abrufen kann mit jedem Flow verwendet werden, um IP-Adressen für Konfigurationselemente (CI) zur Verwendung im Flow zu sammeln.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	IP-Adressen gefunden.
Fehler	Keine IP-Adressen gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
ci_sys_id	Bezeichner des Konfigurationselements.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ip_addr	IP-Adressen.

Security Operations Workflow-Auslöser

Security Operations Workflow-Auslöser enthalten eine Bedingung in einer Tabelle. Alle an den Workflow-Auslöserdatensatz angehängten Workflows werden ausgeführt, wenn die Bedingung erfüllt ist.

Erstellen Sie Workflow-Auslöser Security Operations .

Erstellen Sie einen Workflow-Auslöser, der eine Bedingung in einer Tabelle enthält.

Vorbereitungen

Security Operations enthält mehrere Workflow-Auslöser im Basissystem:

Konfigurationselement-Changes bei einem aktiven Security Incident

Nutzt die Integration, um CI-bezogene Daten anzureichern, wenn sich Konfigurationselemente ändern.

Angreifbare Gruppe erneut scannen

Scannt eine angreifbare Gruppe erneut mit Workflow zum Scannen auf Schwachstellen, wenn Sie die Gruppe **schließen/ignorieren**.

Scannen Sie das angreifbare Element erneut

Scannt ein angreifbares Element erneut, indem Workflow zum Scannen von angreifbaren Elementen verwendet wird, wenn Sie das Element **schließen/Ignorieren**.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zum Lesen von: sn_sec_cmn.read
- Zum Erstellen oder Aktualisieren: sn_sec_cmn.write
- Zu Löschen: sn_sec_cmn.admin

Prozedur

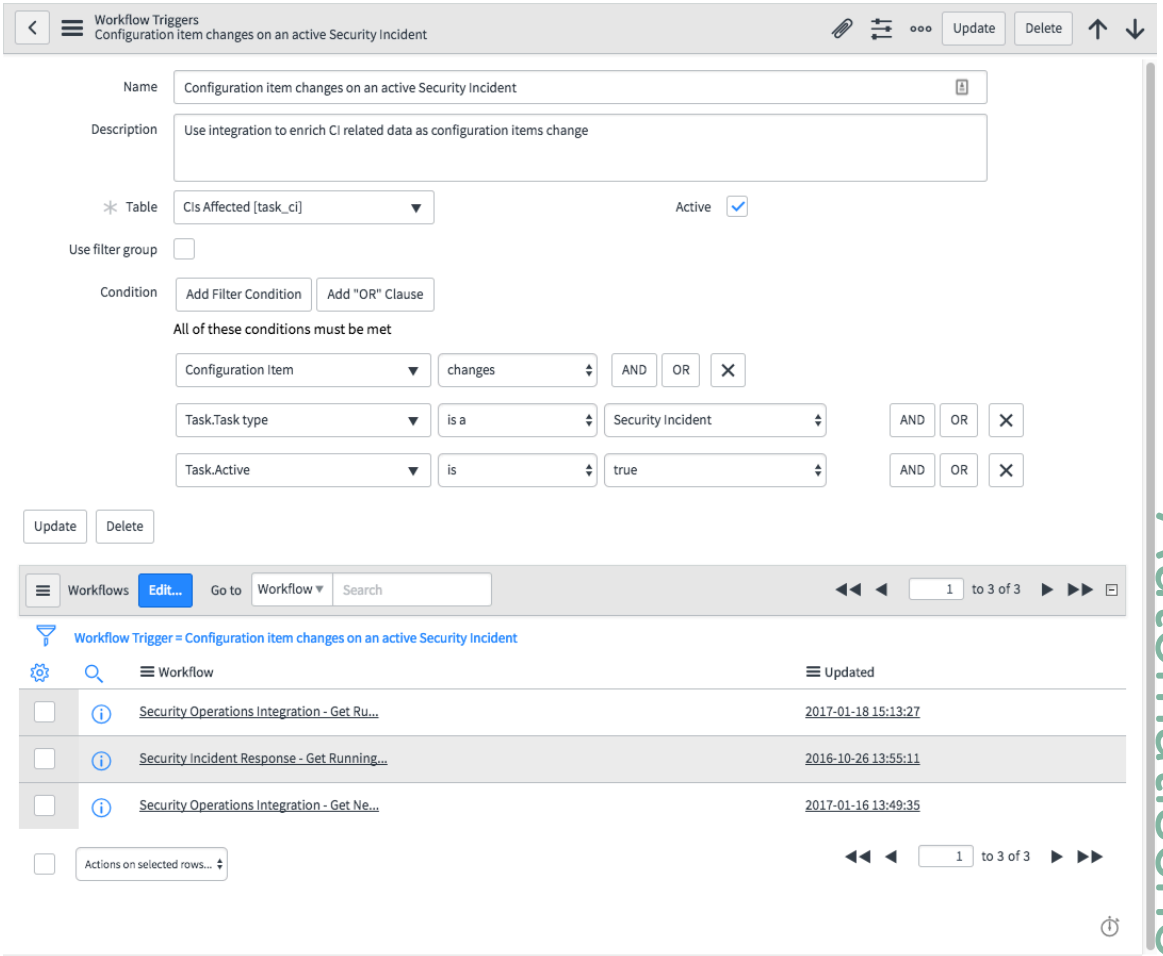
1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Workflow-Auslöser**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Workflow-Auslöser

Feld	Beschreibung
Name	Der Name des Workflow-Auslösers.
Beschreibung	Geben Sie eine Beschreibung für den Workflow-Auslöser ein.
Tabelle	Die Tabelle, die den Workflow-Auslöser enthält. Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert und eine Filtergruppe ausgewählt haben, wird in diesem Feld standardmäßig die Tabelle verwendet, die der ausgewählten Filtergruppe zugeordnet ist.
Bedingung	Verwenden Sie den Bedingungsgenerator , um die Kriterien für den Workflow-Auslöser zu definieren. Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** und eine Filtergruppe ausgewählt haben, werden die Felder **Bedingung** nicht angezeigt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den Workflow-Auslöser zu aktivieren.
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine vordefinierte Filtergruppe zu verwenden oder eine neue Filtergruppe zu erstellen, um die Workflow-Auslösekriterien zu definieren.
Filtergruppe	Wählen Sie die Filtergruppe aus, die zum Definieren von Workflow-Auslösern verwendet werden soll. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Filtergruppen verwenden** aktiviert ist.

4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie **Speichern**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Registerkarte **Workflows** wird angezeigt. Enthält Workflows, die ausgeführt werden, wenn alle Filterbedingungen oder Filtergruppenbedingungen erfüllt sind.

5. Führen Sie die folgenden Schritte aus, um Workflows hinzuzufügen.
   a. Klicken Sie auf der Registerkarte **Workflowsauf Bearbeiten**.
   b. Verwenden Sie bei Bedarf den Bedingungsgenerator, um die Workflows zu finden, die Sie auswählen möchten, oder verwenden Sie den Slushbucket, um Workflows auszuwählen und in die Workflows-Liste zu verschieben.
   c. Klicken Sie auf **Speichern**.
   Die ausgewählten Workflows werden hinzugefügt.
6. Klicken Sie auf **Aktualisieren**.

Orchestration für Security Operations

Benutzer können mithilfe von Aktivitätenpaketen und Workflows in Security Operations Orchestrationmit Daten aus Windows- oder UNIX-basierten Systemen und Umgebungen interagieren und Daten abrufen.

Security Operations Orchestration spart Zeit, indem es manuelle Prozesse eliminiert und kontextbezogene Informationen zur Behebung von Incidents erhält. Die -Produkte Security Operations verfügen über Standard-Aktivitätenpakete und -Workflows, die in den einzelnen Plugins enthalten und darin aktiviert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um zusätzliche Orchestration-Aktivitäten zu erstellen und darauf zuzugreifen, die mit den Produkten des Standardangebots Security Operations nicht verfügbar sind, erwerben Sie eine vollständige Orchestration-Lizenz.

- Security Incident Response Orchestration -Workflows:
  - Security Incident Response – Flow zum Abrufen von Netzwerkstatistiken
  - Security Operations-Systembefehlsintegration: Flow zum Abrufen laufender Prozesse
  - Workflow „Suchanforderung für IoC-Changes erstellen“.
  - Security Operations Integration - Flow zum Suchen und Löschen von E-Mails
- Threat Intelligence Orchestration -Workflows:
  - Threat Intelligence - IoC-Such-Workflow ausführen
  - Aktualisieren Sie den Security Incident mit dem Workflow für Suchergebnisse
- Vulnerability Response Orchestration -Workflows:
  - Workflow zum Scannen auf Schwachstellen
  - Workflow zum Scannen von angreifbaren Elementen

[store-future: BEGIN review]

Security Operations Szenarien und Beispiele

Die ServiceNow® Security Operations -Produkte können anhand einiger Szenarien leicht verstanden werden. Diese Szenarien stellen Funktionen dar, die Sie bei der Verwendung der -Produkte einsetzen können. Sie sollen Sie über die Leistungsfähigkeit und Flexibilität dieser Produkte informieren.

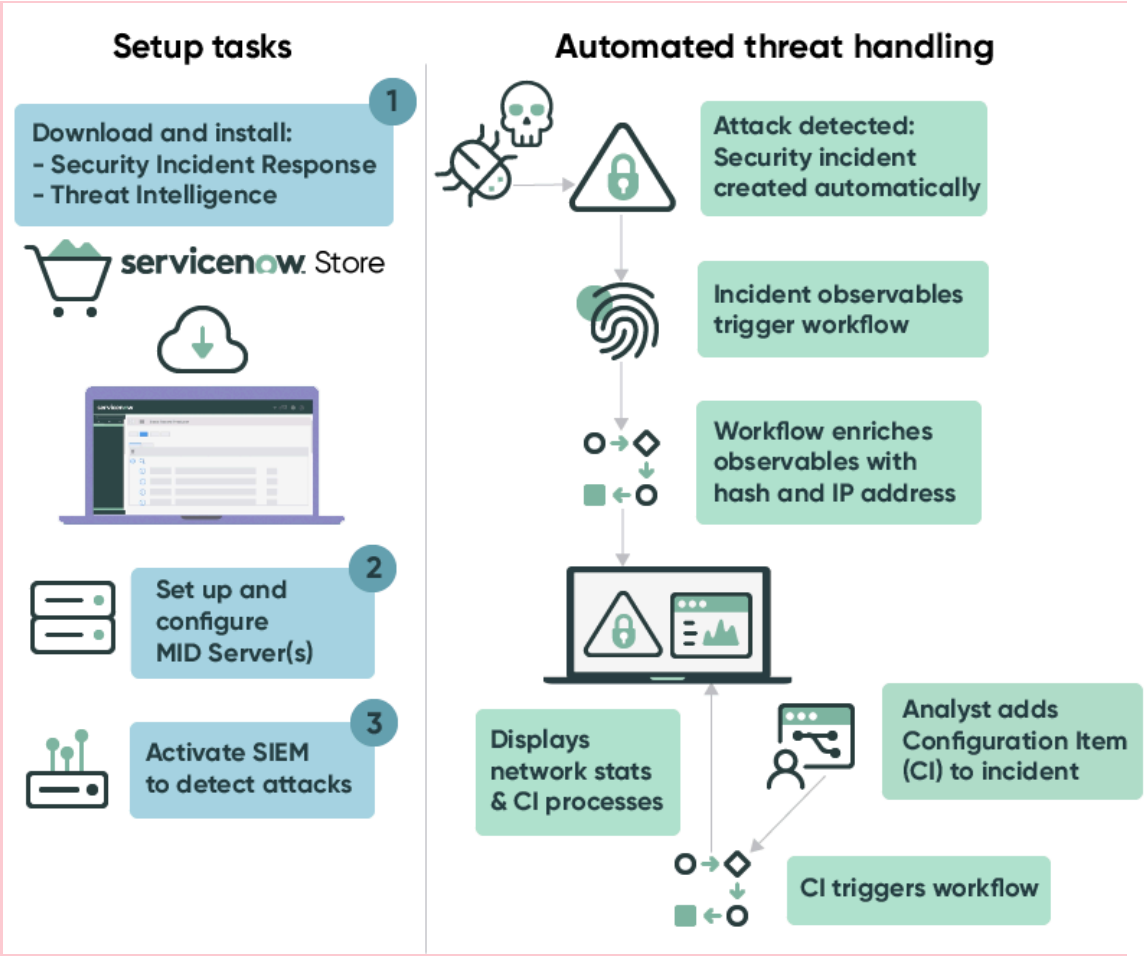
[End]
[store-future: BEGIN review]

Reduzieren Sie die Zeit für Bedrohungsanalysen durch Automatisierung

Die Selektierung und Analyse von Security Incidents sind notwendige Schritte, um während des Prozesses der Reaktion auf Bedrohungen Falschmeldungen auszusortieren und zu bestimmen, wie Sie Sicherheitsbedrohungen am besten identifizieren, eindämmen und beseitigen können.

Selektierung kann manuelle Schritte zum Aufspüren der Ursachen und Auswirkungen von Bedrohungen umfassen. Durch die Automatisierung vieler Schritte können Sie den Zeit- und Arbeitsaufwand für die Analyse und Eindämmung von Bedrohungen erheblich reduzieren. Nachdem Sie die Automatisierung in Ihrer ServiceNow® Security Operations -Software eingerichtet haben, können Sie verschiedene Arten der Automatisierung ausführen. Beispielsweise können Sie Daten erkennbarer Elemente automatisch ergänzen, wenn sie einem Security Incident hinzugefügt werden. Oder Sie können laufende Prozesse anzeigen oder Netzwerkstatistiken abrufen, wenn ein CI in Ihrer CMDB zu einem Security Incident hinzugefügt wird. Diese unten dargestellten Prozesse können Ihnen bei der Bedrohungsanalyse wertvolle Zeit sparen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In diesem Szenario wurde eine schädliche Datei von dem SIEM-Tool (Security Information and Event Management) erkannt, das Ihr Unternehmen zur Bedrohungserkennung verwendet. Die Integration Security Operations von mit dem SIEM bewirkt, dass automatisch ein Security Incident basierend auf dem Typ der erkannten Bedrohung erstellt wird. Wenn die schädliche Datei bereits erkennbare Elemente enthielt oder der Sicherheitsanalyst nachträglich neue, nicht abgelaufene erkennbare Elemente hinzugefügt hat, wird automatisch ein Workflow ausgelöst, der die Datensätze der erkennbaren Elemente anreichert. Der Workflow bewirkt, dass die erkennbaren Elemente gescannt werden und der Hash und die IP-Adresse der Partei, die die Datei gesendet hat, dem Security Incident hinzugefügt werden.

Während der Selektierung kann der Analyst feststellen, dass in der CMDB des Unternehmens enthaltene Configuration Items (CI) von dem Angriff betroffen waren. Daher fügt der Analyst dem Security Incident die CIs hinzu. Beim Speichern des Security Incident werden zwei weitere Workflows ausgeführt, und Netzwerkstatistiken und laufende Prozesse im Zusammenhang mit den CIs werden dem Security Incident sofort hinzugefügt.

[End]

Bereiten Sie die Automatisierung von Threat Intelligence vor

Bevor die Automatisierung Threat Intelligence von im Bedrohungsantwortprozess verwendet werden kann, müssen Sie einige vorläufige Setupschritte ausführen. Wenn das Setup abgeschlossen ist, werden die Workflows automatisch mit geringer oder keiner Benutzerunterstützung ausgeführt.

Vorbereitungen

Erforderliche Rolle: Administrator

Automatische Übersetzung

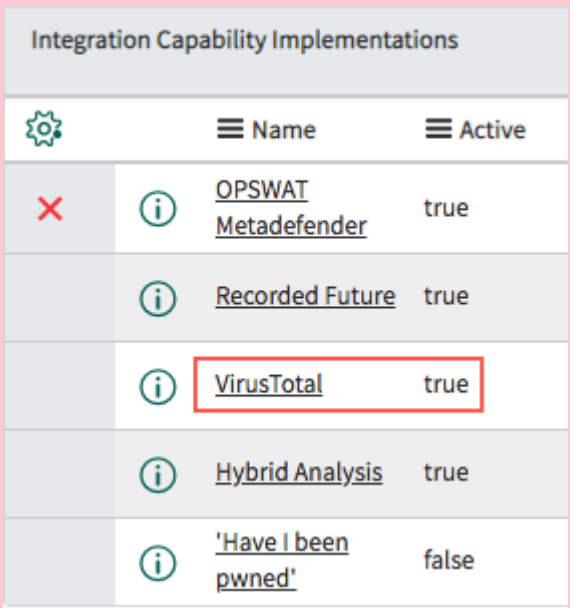
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie die herunter Security Incident Response und Threat Intelligence Anwendungen aus dem ServiceNow Store.
2. Installieren Sie einen oder mehrere MID Server , und konfigurieren Sie für jeden die Serviceanmeldeinformationen .
3. Wenn die MID-Server in Betrieb sind, vergewissern Sie sich, dass die Implementierung der Integrationsfunktion, die Sie verwenden (z. B. VirusTotal), für die Fähigkeit „Bedrohungssuche“ aktiv ist. Die Fähigkeit „Bedrohungssuche“ führt Suchvorgänge durch, um zu bestimmen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsrisiken zugeordnet sind.

   a. Navigieren zu **Security Operations** > **Integrationen** > **Integrationsfunktionen**.

   b. Klicken Sie auf **Bedrohungssuche**, und scrollen Sie nach unten zur zugehörigen Liste „Implementierung der Integrationsfähigkeit“.



   c. Suchen Sie die Implementierung, die Sie verwenden möchten, und vergewissern Sie sich, dass in der Spalte **Aktivtrue**angezeigt wird.

   d. Wenn die Implementierung nicht aktiv ist, klicken Sie auf den **Implementierungsnamen**, aktivieren Sie das Kontrollkästchen **Aktiv**, und klicken Sie auf **Aktualisieren**.

Daten zu erkennbaren Elementen automatisch ergänzen

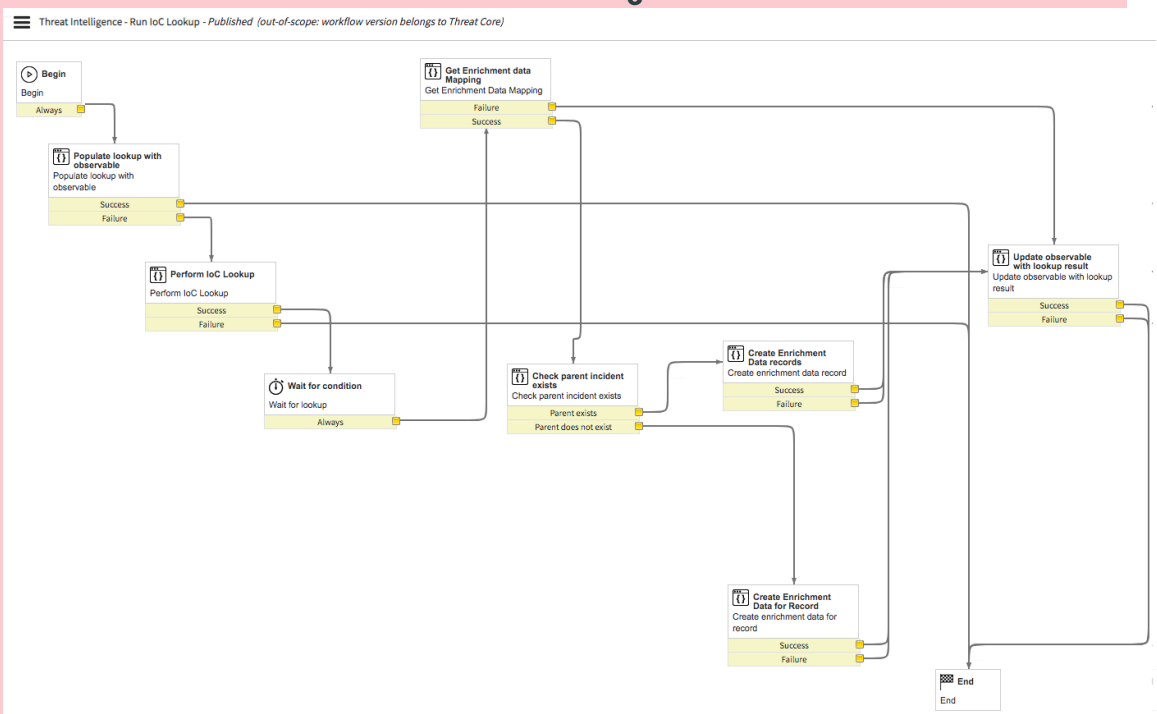
Nachdem Sie die Automatisierung von Threat Intelligence vorbereitet haben und einem Security Incident neue oder nicht abgelaufene Kompromittierungsindikatoren (IoC) hinzugefügt haben, wird der Workflow Threat Intelligence – IoC-Suche ausführen automatisch ausgeführt.

Die Workflow-Aktivitäten extrahieren Informationen aus den IoCs, einschließlich des Hashes der verdächtigen Datei und der ursprünglichen IP-Adresse, ohne dass der Benutzer eingreifen muss.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten zu erkennbaren Elementen automatisch ergänzen



Hinweis:

Sie können die Suche auch manuell ausführen, indem Sie mindestens ein erkennbares Element auswählen, das bereits an den Security Incident angehängt ist, und in der Auswahlliste **Aktionen für ausgewählte Zeilen** die **Option Bedrohungssuche ausführen** auswählen.

Der -Workflow führt die folgenden Aktivitäten aus:

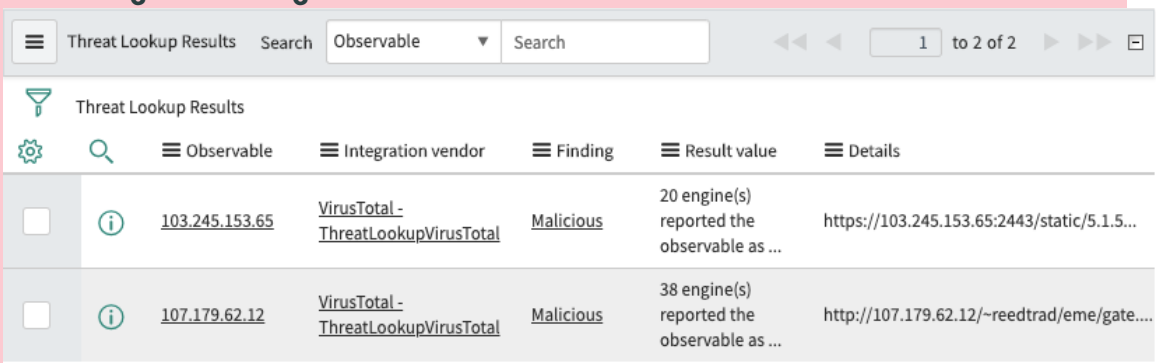
1. Die Aktivität **„Suche mit erkennbarem Element füllen“** versucht, ein vorhandenes erkennbares Element für eine Suche zu finden, das dem Wert und Typ der Suche entspricht, die der Aktivität als Eingabe bereitgestellt wurde.
   a. Wenn ein erkennbares Element gefunden wird, das den Eingaben entspricht, bewirkt die Aktivität **IoC-Suche durchführen**, dass eine Suche für die ScanID des Datensatzes durchgeführt wird.
   b. Wenn ein erkennbares Element gefunden wird und nicht abgelaufen ist, wird die Suche nicht durchgeführt, und die Suchergebnisse im Security Incident werden mit Informationen aus dem erkennbaren Element aktualisiert. Weitere Informationen finden Sie unter Füllen Sie die Suche mit der Aktivität erkennbarer Elemente aus.
2. Wenn eine IoC-Suche ausgeführt wird, rufen die folgenden vier Aktivitäten zuerst Informationen aus der Ergänzungsdatenzuordnung ab. Die Ergänzungsdatenzuordnung wandelt Daten aus XML-, JSON- oder Eigenschaftsdateien in ServiceNow-Datensätze um. Als Nächstes überprüfen sie, ob ein übergeordneter Security Incident vorhanden ist. Wenn dies der Fall ist, wird ein erkennbares Element erstellt und angereichert. Andernfalls wird das vorhandene erkennbare Element angereichert. Weitere Informationen finden Sie unter Erkennbares Element mit Suchergebnisaktivität aktualisieren.
   - **Ruft die Zuordnung von Ergänzungsdaten ab**
   - **Überprüft, ob der übergeordnete Incident vorhanden ist**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Ergänzungsdatensätze erstellen**
- **Ergänzungsdaten für Datensatz erstellen**

3. Nach Abschluss der Datenanreicherung **aktualisiert die Aktivität „Erkennbares Element mit Suchergebnissen** aktualisieren“ die erkennbaren Elemente im Security Incident und schreibt die Ergebnisse in die zugehörige Liste **„Ergebnisse der Bedrohungssuche“**.

Bedrohungssuche – Ergebnisse



Ruft automatisch Netzwerkstatistiken und laufende Prozesse ab

Wenn Sie einem Security Incident ein in der CMDB gefundenes Configuration Item (CI) mit einem vollqualifizierten Windows-Domänennamen (FQDM) hinzufügen, werden zusätzliche Workflows ausgeführt, um Netzwerkstatistiken und laufende Prozesse bereitzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

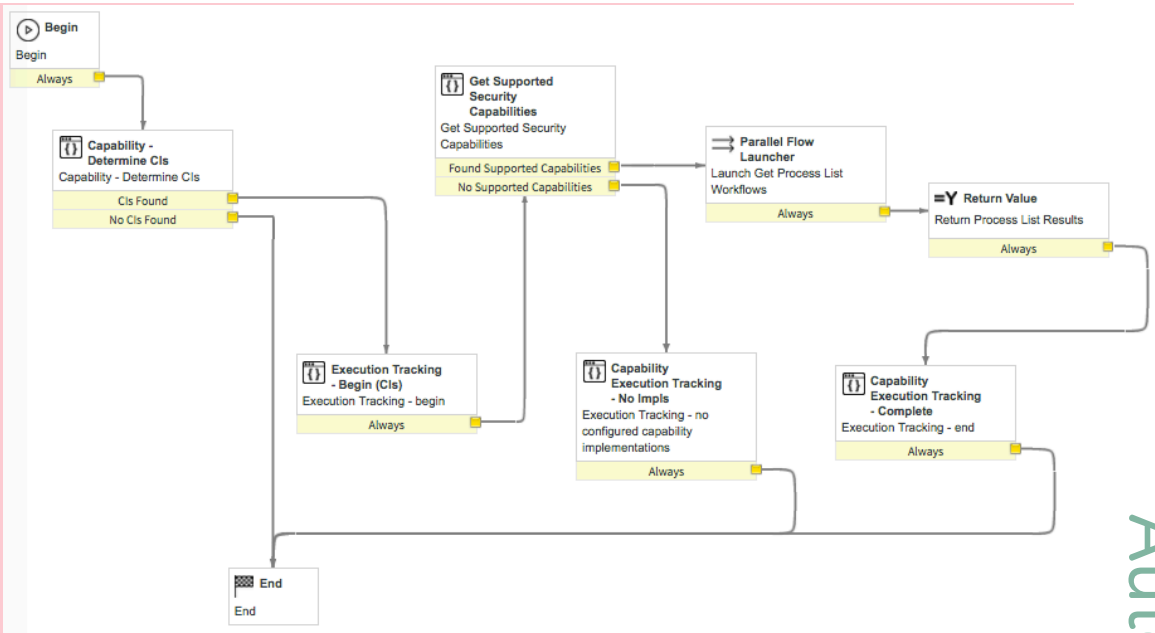
Prozedur

1. Füllen Sie die CMDB mit dem Discovery -Modul mit Windows-Domänennamen aus.

> **Hinweis:**
> Wenn Sie das ServiceNow Discovery- Modul nicht abonnieren, müssen Sie Ihre CMDB manuell füllen oder ein Discovery-Produkt einer Drittpartei verwenden.

2. Fügen Sie dem Security Incident ein CI hinzu.
   Die folgenden beiden Workflows werden parallel ausgeführt.
   - Security Operations – Flow für laufende Prozesse abrufen: Dieser Workflow ruft eine Liste der laufenden Prozesse für ein Configuration Item (CI) von einem Host ab. Verwenden Sie diese Liste, um eine Integration wie Carbon Black oder einen Windows-basierten Security Incident zu erfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn der Workflow abgeschlossen ist, werden die laufenden Prozesse in der zugehörigen Liste **„Laufende Prozesse“** im Security Incident angezeigt.

Laufende Prozesse

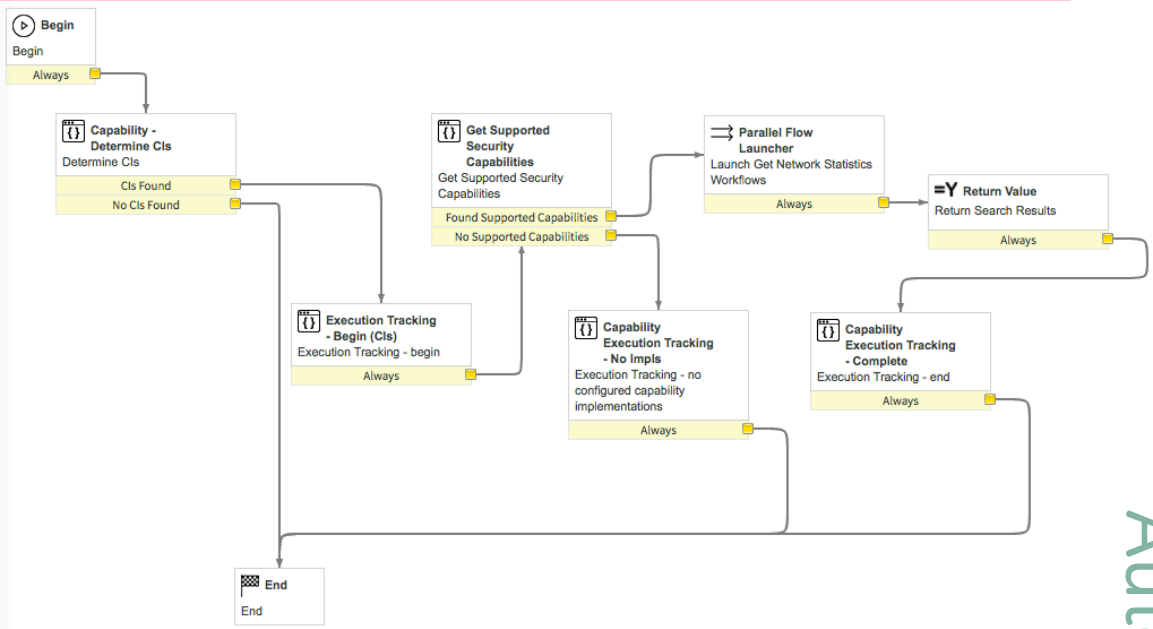
Running Processes

Path	Command ...	Owner	PID	Parent PID	Security Tags
C:\Windows\syste...	C:\Windows\syste...	SYSTEM	456	368	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	LOCAL SERVICE	856	456	UNKNOWN
C:\Windows\syste...	\??\C:\Windows\sy...	SYSTEM	1748	320	UNKNOWN
C:\Windows\Syste...	C:\Windows\Syste...	NETWORK SERVICE	3676	456	UNKNOWN
C:\Windows\syste...	\	Administrator	2400	1056	UNKNOWN
C:\demo\agent\jre\...	\	SYSTEM	6932	2540	UNKNOWN
C:\Windows\syste...	\	SYSTEM	6720	2968	UNKNOWN
		SYSTEM	4	0	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	SYSTEM	472	368	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	NETWORK SERVICE	964	456	UNKNOWN

1 to 10 of 50

- Flow für Security Operations-Integrationen – Netzwerkstatistiken abrufen: Dieser Workflow ruft eine Liste aktiver Netzwerkverbindungen von einem Host oder Endpunkt ab. Wann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn der Workflow abgeschlossen ist, werden Netzwerkstatistiken in der zugehörigen Liste **„Netzwerkstatistiken“** im Security Incident angezeigt.

Netzwerkstatistiken

Workflow Activity History | Search | Started | Search | 1 to 8 of 8

Context = Security Operations Integration - Get Network Statistics

Started	Activity	State	Ended	Result	Fault Description
2019-05-13 13:28:38	Execution Tracking - begin	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Get Supported Security Capabilities	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:39	Execution Tracking - end	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	End	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	Return Search Results	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:38	Determine CIs	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Launch Get Network Statistics Workflows	Finished	2019-05-13 13:28:39	success	
2019-05-13 13:28:38	Begin	Finished	2019-05-13 13:28:38		

Priorisieren Sie Schwachstellen mit hohem Profil

Wenn Ihr Netzwerk angegriffen wird, werden folgende typische Fragen gestellt: „Wie bestimmen wir unser Risiko?“ Und was noch wichtiger ist: „Wie bestimmen wir, welche Systeme zuerst behandelt werden sollen?“

Anfang 2018 wurden zwei kritische Schwachstellen entdeckt: **Kernelemente Kernel** und **Spezifisch**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Priorisieren Sie Schwachstellen mit hohem Profil

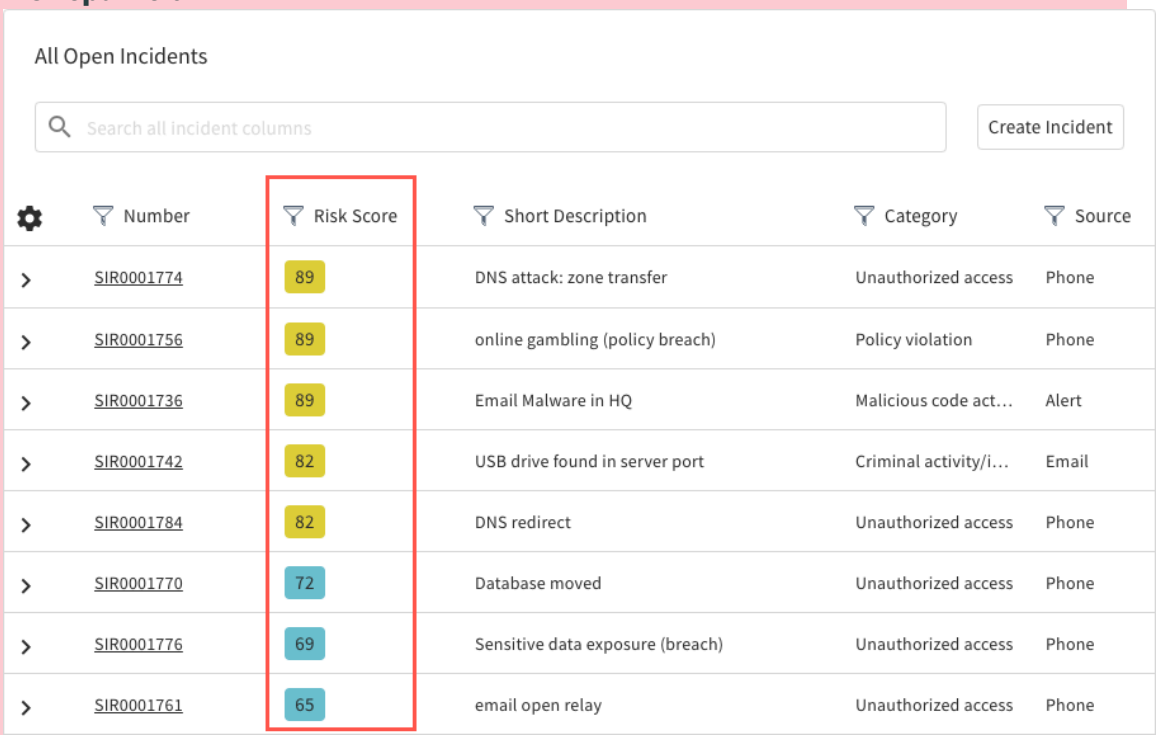
Schädliche Programme können „Meltdown“ und „Spectre“ ausnutzen, um sich Zugriff auf Geheimnisse zu verschaffen, die im Arbeitsspeicher anderer laufender Programme gespeichert sind. Weltweit waren fast drei Milliarden Systeme potenziell von den Schwachstellen betroffen, da sowohl Hardware- als auch Softwareanbieter versuchten, Patches für ihre Kunden bereitzustellen.

Rangfolge der Bedrohungen anhand gescannter Daten in Vulnerability Response

Mit der Anwendung Security Operations Vulnerability Response stehen zahlreiche Methoden zur Durchführung von Schwachstellen-Scanszur Verfügung. Wenn die Anwendung Security Incident Response aktiviert ist, können Sie Scans auch aus dem Security Incident-Katalog, einem Security Incident-Datensatz oder einer Sicherheitsscan-Anforderung initiieren.

Je nachdem, welche Drittanbieterintegration Sie verwenden, werden Schwachstellendaten gescannt und mithilfe von APIs in die Anwendung Vulnerability Response importiert. Anschließend wird es mit Ihren Assets in ServiceNow Configuration Management Database (CMDB)abgeglichen. Den resultierenden angreifbaren Elementen wird eine Risikopunktzahl zugewiesen, die auf mehreren Faktoren basiert, einschließlich des Schweregrads der Schwachstelle und der Bedeutung des betroffenen Asset.

Risikopunktzahl

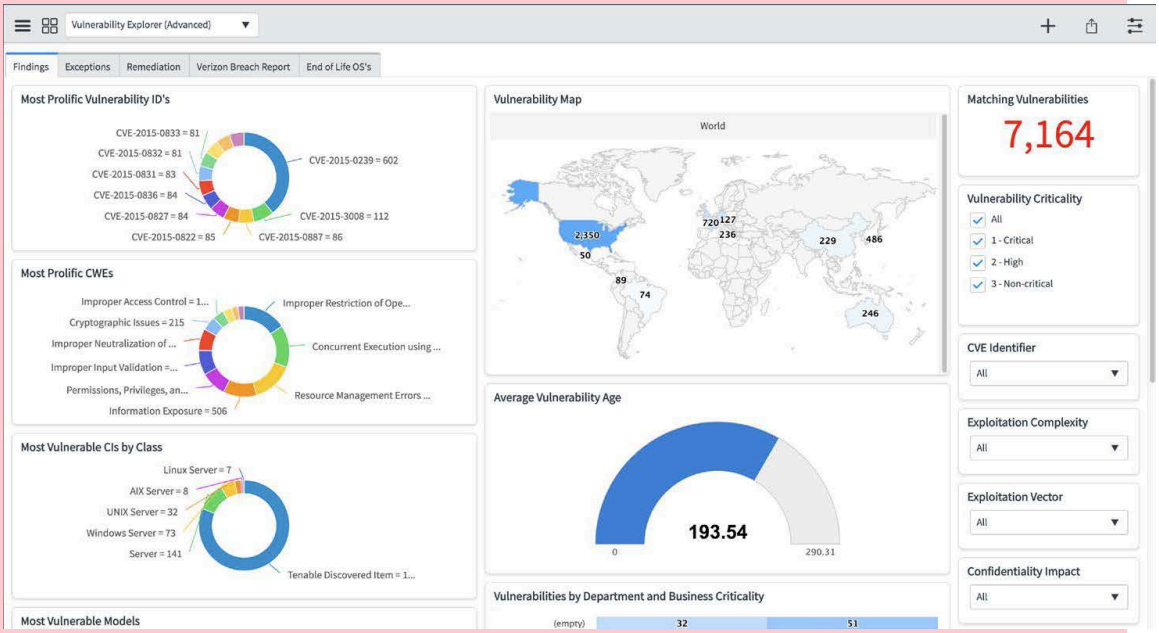


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Risikopunktzahl ist konfigurierbar und ermöglicht eine schnelle Priorisierung. Alle Informationen über die Schwachstelle (z. B. was es ist, wie sie ausgenutzt wurde und wie die Bedrohung behoben werden kann) werden automatisch aus der National Vulnerability Database (NVD) in Vulnerability Response abgerufen, sodass keine manuelle Suche erforderlich ist. Die konfigurierbaren Dashboards der Lösung zeigen sofort das allgemeine Schwachstellenrisiko Ihrer Organisation an.

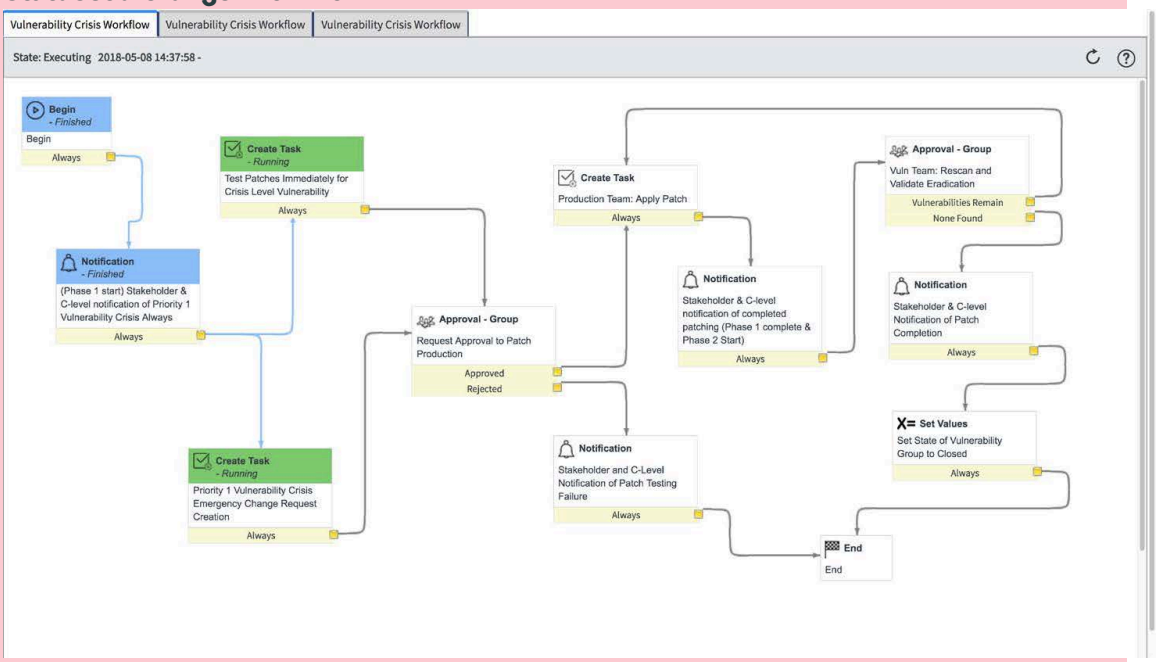
VR-Dashboard



Die nächsten Schritte werden automatisiert

Nachdem Sie die kritischsten angreifbaren Elemente identifiziert und priorisiert haben, automatisieren Security Operations -Workflows mehrere der nächsten Schritte.

Statuscodierungs-Workflow



Für geschäftskritische angreifbare Elemente werden Anforderungen zur Genehmigung des automatischen Patchens gesendet, und die entsprechenden Besitzer werden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

benachrichtigt. Dadurch entfällt die Suche nach dem Bereitschaftsanalysten oder die manuelle Entscheidung, welche Elemente als „kritisch“ gelten.

Nach Genehmigung und Abschluss des Patches wird automatisch ein zweiter Scan ausgeführt, um die Korrektur zu überprüfen. Mithilfe von Priorisierung, Workflows und Automatisierung werden die kritischsten Elemente zuerst behandelt.

Security Operations und ServiceNow Store

Ab Madrid können alle Security Operations -Anwendungen und -Integrationen von ServiceNow Storeheruntergeladen werden. Auf diese Weise können Sie neue und aktualisierte Funktionen schneller abrufen. Bevor Sie Security Operations -Anwendungen verwenden können, müssen Sie überprüfen, ob Sie berechtigt sind (d. h. gültige Lizenzen für ihre Verwendung besitzen), sie von ServiceNow Storeherunterladen und aktivieren.

Die Liste der zum Download verfügbaren Security Operations -Anwendungen wird ständig erweitert:

- Security Incident Response (und unterstützte Integrationen)
- Vulnerability Response (und unterstützte Integrationen)
- Threat Intelligence (und unterstützte Integrationen)
- Konfigurations-Compliance
- Trusted Security Circle
- Data Loss Prevention Incident Response

Sehen Sie sich dieses fünfminütige Video an, um mehr über das Herunterladen von Security Operations- und GRC-Anwendungen aus dem ServiceNow Storezu erfahren. In diesem 5-minütigen Video wird beschrieben, wie Security Operations- und GRC-Anwendungen aus dem ServiceNow Store heruntergeladen werden

Der Prozess zum Abrufen von Security Operations -Anwendungen und -Integrationen hängt davon ab, ob Sie eine Anwendung zum ersten Mal herunterladen, eine zuvor aus ServiceNow Storeheruntergeladene Anwendung aktualisieren oder ein Upgrade von einem Familien-Release auf das nächste durchführen.

Laden Sie eine Anwendung zum ersten Mal von ServiceNow Store herunter

Das erstmalige Herunterladen einer Anwendung von ServiceNow Store umfasst mehrere einfache Schritte. Einige der Schritte werden in der Instanz ServiceNow Store ausgeführt, andere in Ihrer -Instanz.

Mit ServiceNow Store können Sie Kernprodukte und -anwendungen herunterladen. Ein Produkt enthält eine oder mehrere Anwendungen, die als Gruppe lizenziert sind. Beispiel: Security Incident Response ist ein Produkt. Der -Prozess umfasst die folgenden Schritte:

Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In ServiceNow Storemüssen Sie sicherstellen, dass Sie über Berechtigungen (oder Lizenzen) für die Anwendung und die abhängigen Anwendungen verfügen.

  Hinweis:
  Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

- Abschließend können Sie die Anwendung aktivieren und in Ihrer -Instanz ausführen.

Hinweis:
Ab früheren Versionen von Rome und späteren Releases werden Abhängigkeits-Plugins automatisch aktiviert, wenn Sie eine Kernanwendung aktivieren. Wenn Sie beispielsweise die Anwendung Vulnerability Response aktivieren, wird auch das Plugin Vulnerability Response „ Dependencies“ aktiviert. Weitere Informationen finden Sie unter Aktivieren Sie eine ServiceNow Store -Anwendung.

Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung Security Operations der ab

Der erste Schritt bei der Installation einer Anwendung Security Operations besteht darin, sicherzustellen, dass die Anwendung bzw. das Produkt und die zugehörigen Anwendungen gültige Berechtigungen ServiceNow besitzen.

Vorbereitungen

Erforderliche Rolle: Administrator

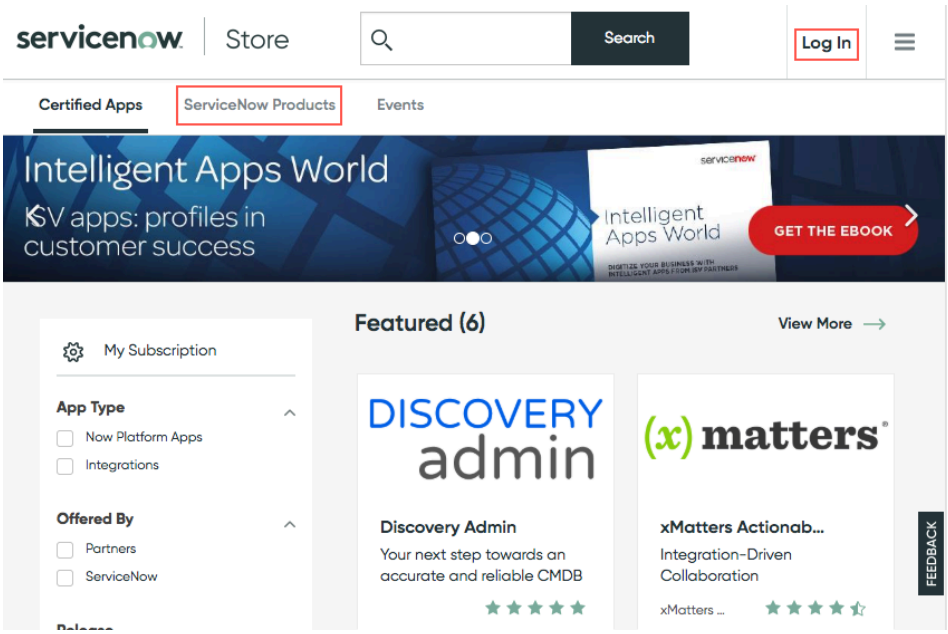
Personen, die die Berechtigung erfüllen, müssen über ein Konto Now Support verfügen und berechtigt sein, Anwendungen für die betreffenden Instanzen anzufordern.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen wurden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, müssen keine Berechtigungen erworben werden. Fahren Sie mit Aktivieren Sie eine ServiceNow Store -Anwendungfort.

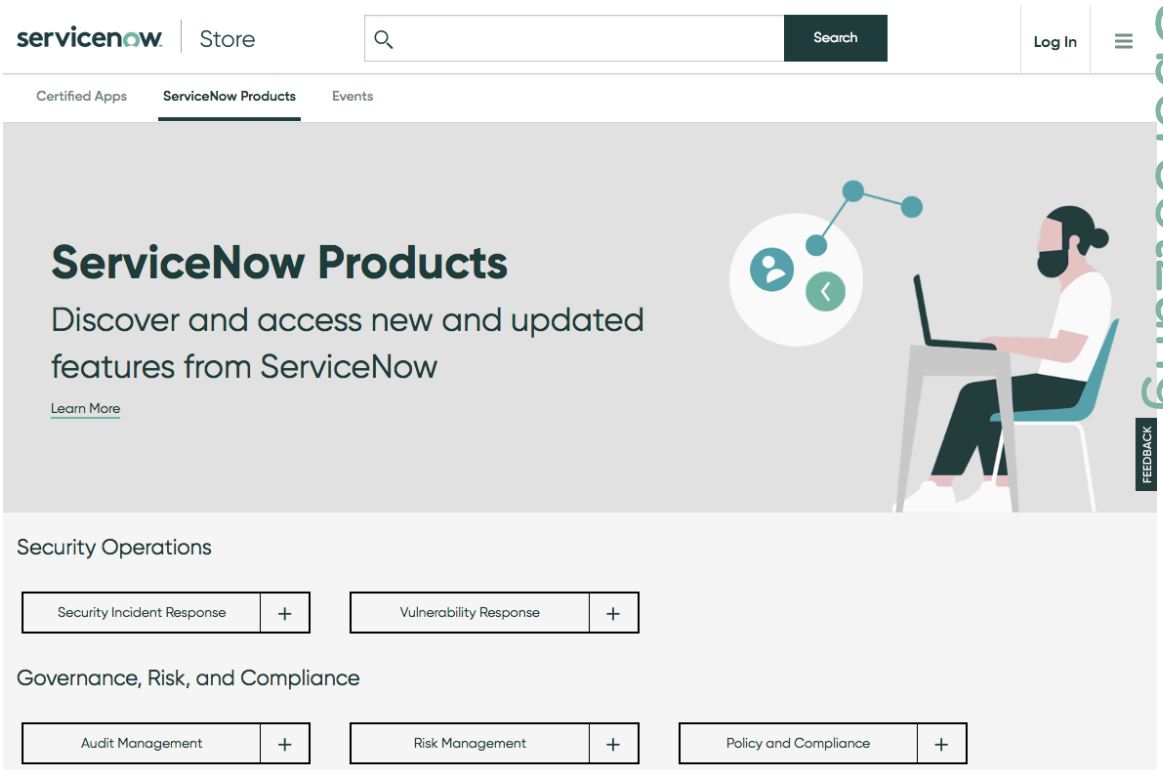
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu ServiceNow Store .



2. Klicken Sie auf **Anmelden**, und melden Sie sich mit Ihren HI -Anmeldeinformationen an.
3. Klicken Sie auf die Registerkarte **ServiceNow-Produkte**, um alle verfügbaren ServiceNow -Produkte anzuzeigen.
   Integrationen und andere Inhaltstypen werden auf der Registerkarte **Zertifizierte Apps** angezeigt.



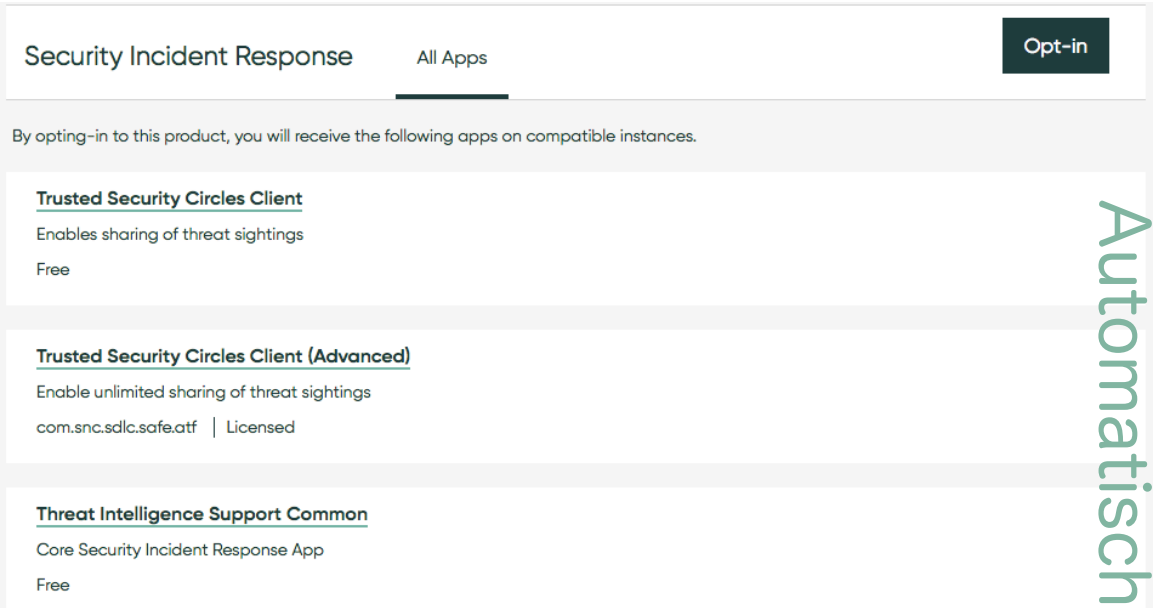
Hinweis:
Für dieses Beispiel nehmen wir an, Sie erwerben die Berechtigung für das Produkt Security Incident Response.

Automatische Übersetzung

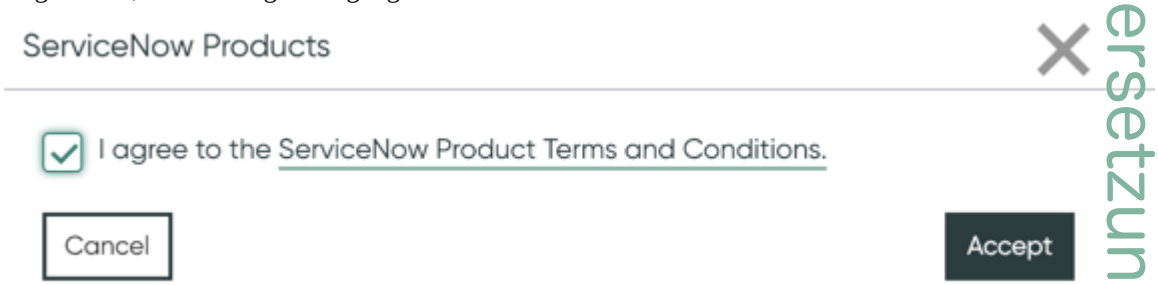
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf das Pluszeichen (+) neben dem Namen des Produkts, für das Sie berechtigt sind.
   Alle Anwendungen, die dem Produkt zugeordnet sind, für das Sie Berechtigungen erteilen, werden aufgelistet. Wenn Sie die Berechtigung für das Kernprodukt erworben haben, sind die darunter aufgeführten Anwendungen ebenfalls berechtigt.

   Hinweis:
   Sie können auch auf den Produktnamen klicken, um weitere Informationen zum Produkt und den zugehörigen Anwendungen anzuzeigen.



5. Klicken Sie **auf Aktivieren,** um zu überprüfen, ob Sie für das Produkt und die aufgeführten Anwendungen berechtigt sind.
   Sie werden aufgefordert, die Nutzungsbedingungen ServiceNow von zu lesen und zu



   akzeptieren.

6. Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.

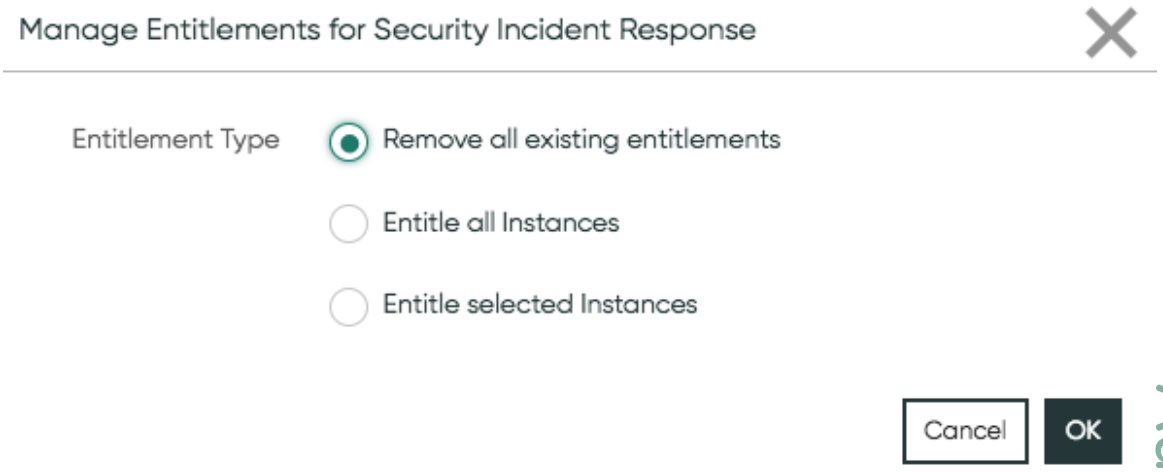
7. Beachten Sie, dass neben dem Produktnamen ein Häkchen angezeigt wird und die Schaltfläche Berechtigungen verwalten angezeigt wird.

   Das Häkchen zeigt an, dass Sie das Produkt und die zugehörigen Anwendungen abonniert haben. Es ist an der Zeit, Ihre Berechtigungen zu verwalten. Dies ist ein einmaliger Vorgang für dieses Produkt und alle anderen Produkte, die Sie in Zukunft installieren möchten.

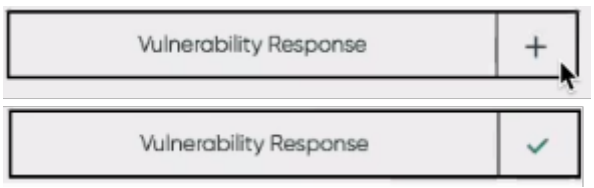
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. **Wahlweise:** Sie können **auf Berechtigungen verwalten** klicken, um die Instanzen zu ändern, die von den Anwendungen betroffen sind, für die Sie berechtigt sind.



9. Nachdem Sie den Nutzungsbedingungen ServiceNow zugestimmt und Berechtigungen verwaltet haben, können Sie mit einem einzigen Klick andere -Produkte berechtigen.



Hinweis:
Sie können das Produkt jetzt aktivieren.

Aktivieren Sie eine ServiceNow Store -Anwendung

Nachdem einer Anwendung die Berechtigung erteilt wurde, müssen Sie das Plugin für Abhängigkeiten aktivieren und die Anwendung aktivieren. Dieser Prozess gilt auch für Anwendungen, die auf Test- und Entwicklungsumgebungsinstanzen heruntergeladen wurden.

Vorbereitungen

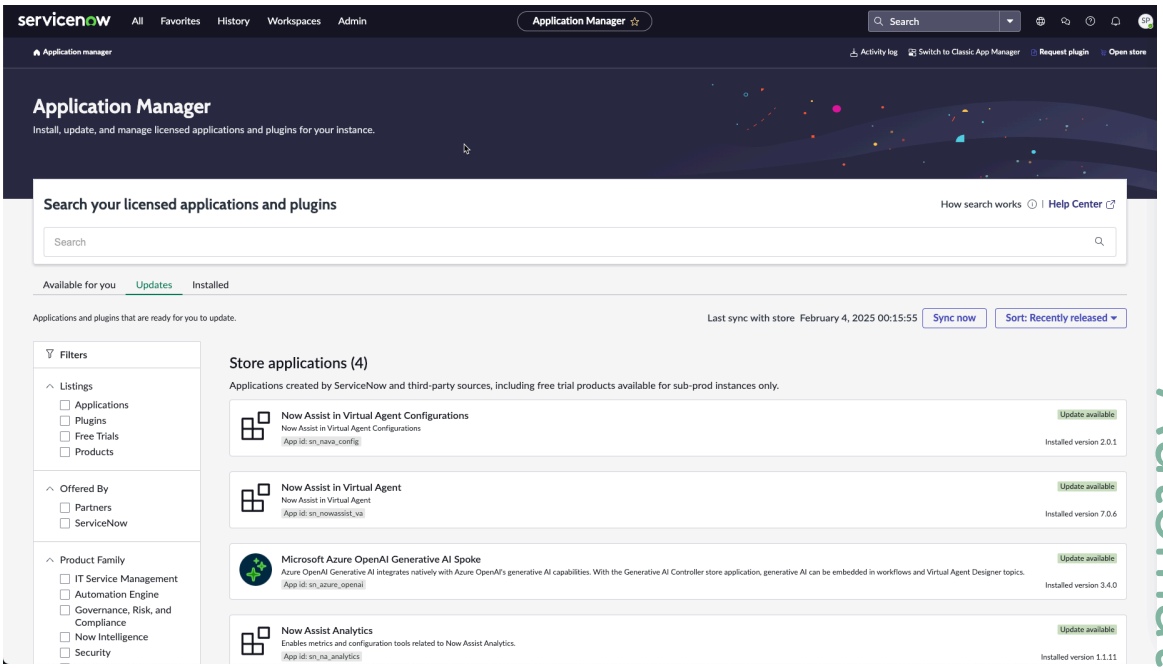
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

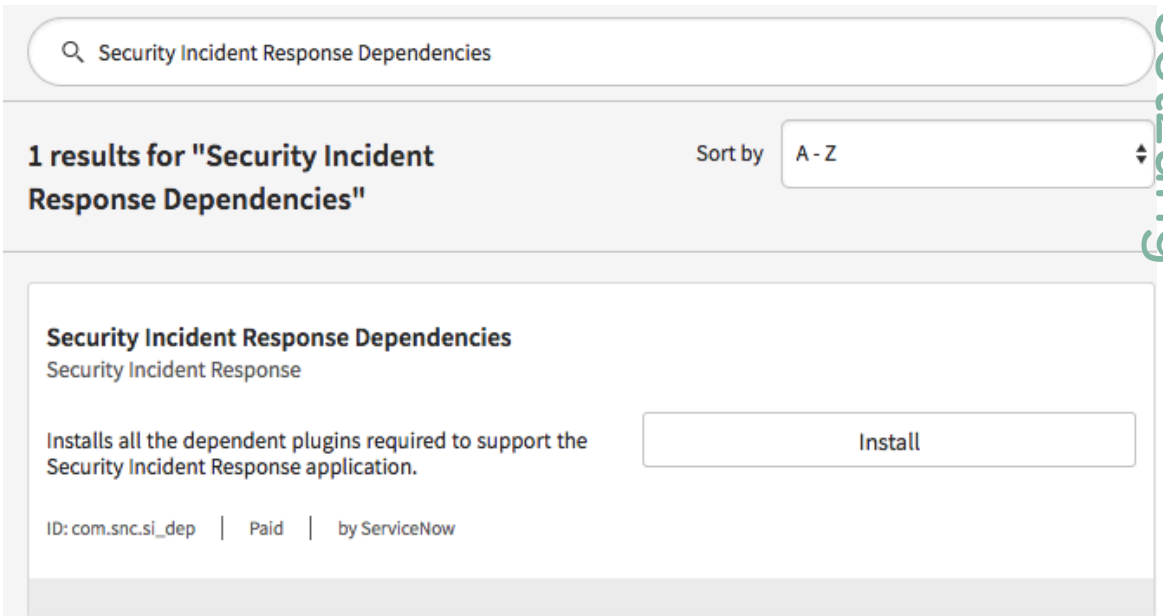
Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



Hinweis:
Ab Orlando werden Abhängigkeits-Plugins automatisch aktiviert, wenn Sie eine Kernanwendung aktivieren. Wenn Sie beispielsweise die Anwendung Vulnerability Response aktivieren, wird auch das Plugin Vulnerability Response „ Dependencies“ aktiviert. Daher sind die Schritte 2 bis 5 optional.

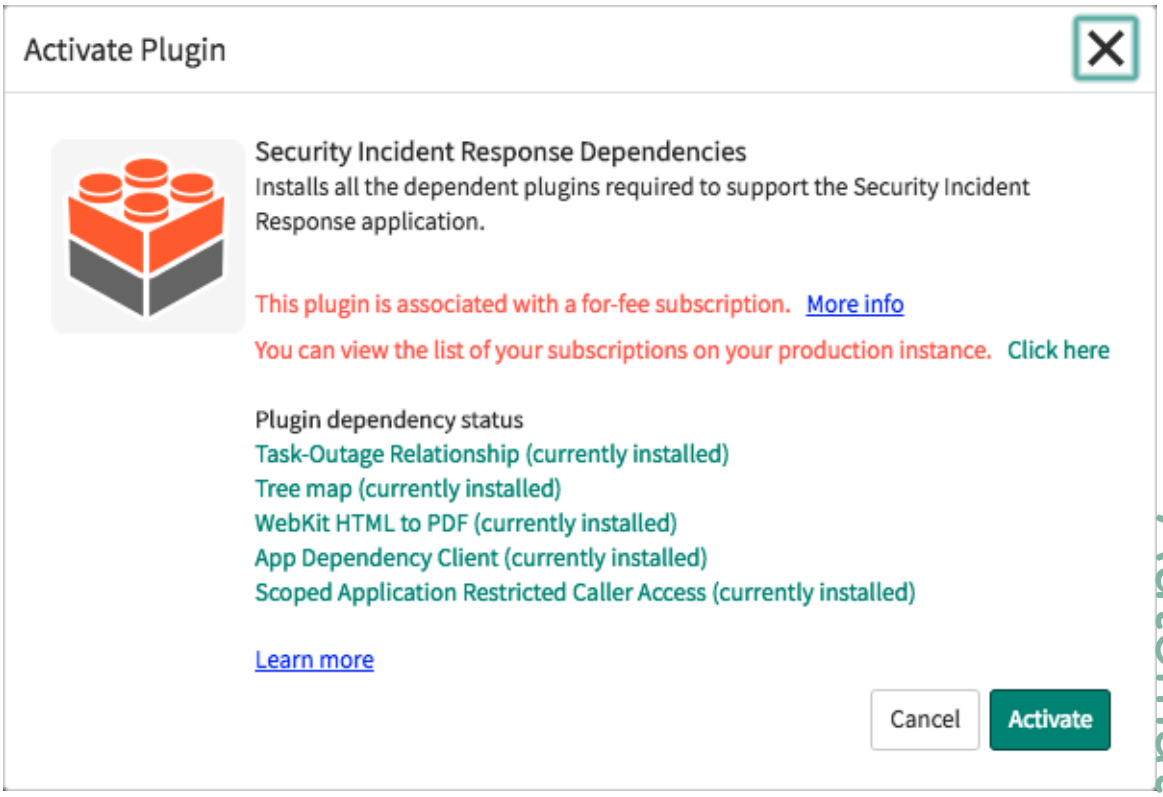
2. Suchen Sie nach dem Plugin für Abhängigkeiten für die Anwendung, die Sie aktivieren möchten.
Wenn Sie beispielsweise Security Incident Responseaktivieren, suchen Sie das Plugin Security Incident Response Dependencies.



3. Klicken Sie auf **Installieren**.
Das Dialogfeld Plugin aktivieren wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie im Dialogfeld **„Plugin aktivieren“** auf **Aktivieren**.
5. Klicken Sie nach Abschluss der Aktivierung **auf Formular schließen und neu laden**.
6. Suchen Sie nun das Kernprodukt, das Sie aktivieren, aktivieren Sie das Kontrollkästchen **Mit Demodaten installieren,** wenn Sie Demodaten laden möchten, und klicken Sie auf **Installieren**.
   Die Anwendung wird automatisch in Ihrer Instanz von installiert.

> **Hinweis:**
> Wenn Sie das Kontrollkästchen **Mit Demodaten installieren** nicht aktivieren, können die Demodaten später nicht über den **Anwendungsmanager** installiert werden. Informationen zur Installation oder erneuten Installation von Demodaten nach der Erstinstallation finden Sie im Artikel Problemumgehung zur Installation von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] in der Knowledge Base HI.

Installieren Sie eine Security Operations -Integration

Alle ServiceNow -Integrationen sind unter ServiceNow Storeverfügbar. Kernanwendungen wie Security Incident Response werden auf der Registerkarte **ServiceNow-Produkte** im Store angezeigt. Integrations-Add-Ons werden auf der Registerkarte **Zertifizierte Apps** angezeigt.

Vorbereitungen

Erforderliche Rolle: Administrator
Store-Installationen erfordern einen Account Now Support und die Berechtigung zum Anfordern von -Anwendungen für die betreffenden Instanzen.

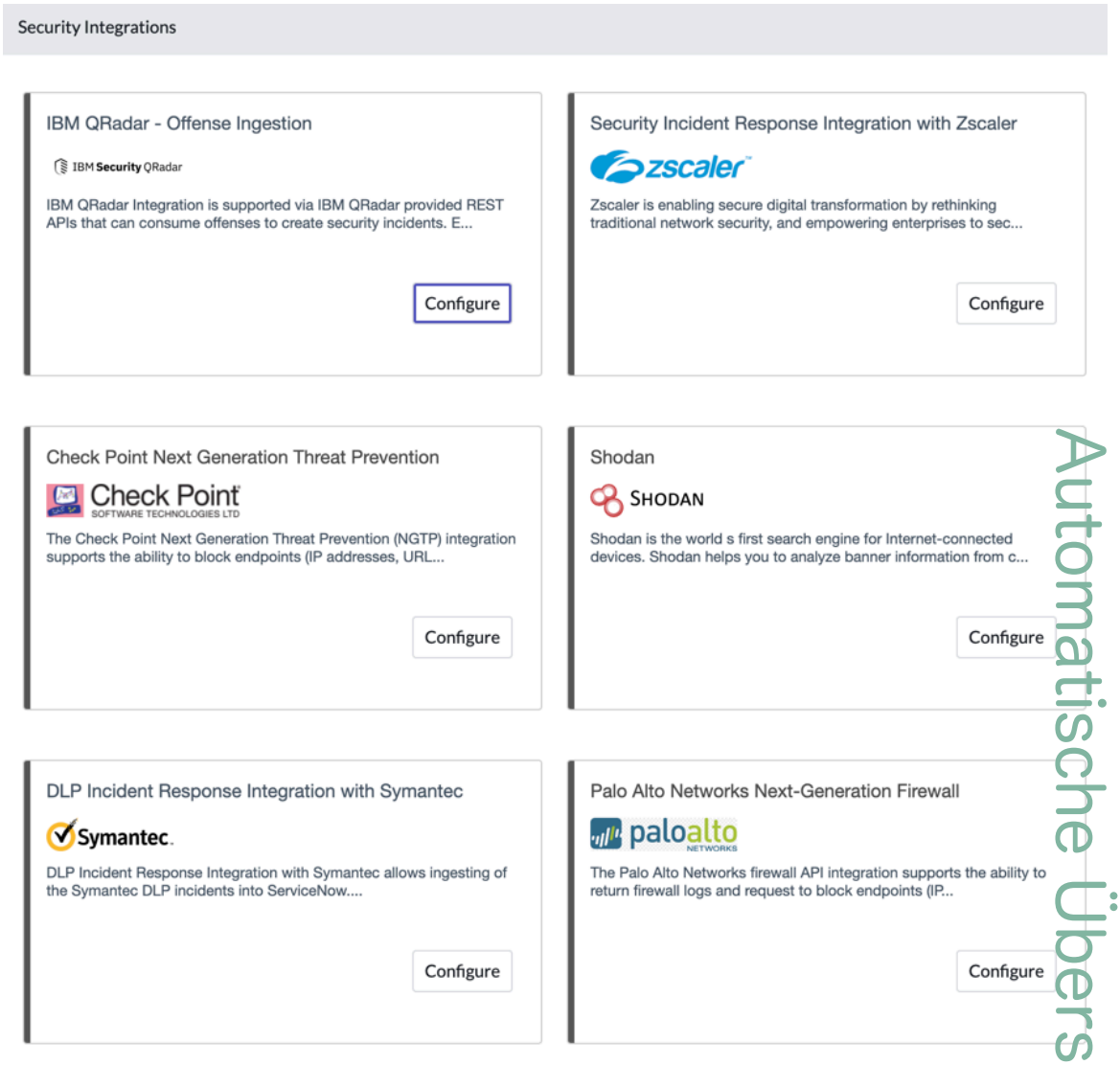
Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen** nachdem Sie die Anwendung aus dem ServiceNow Store installiert haben.
   Konfigurationskacheln für die Integrationen werden angezeigt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

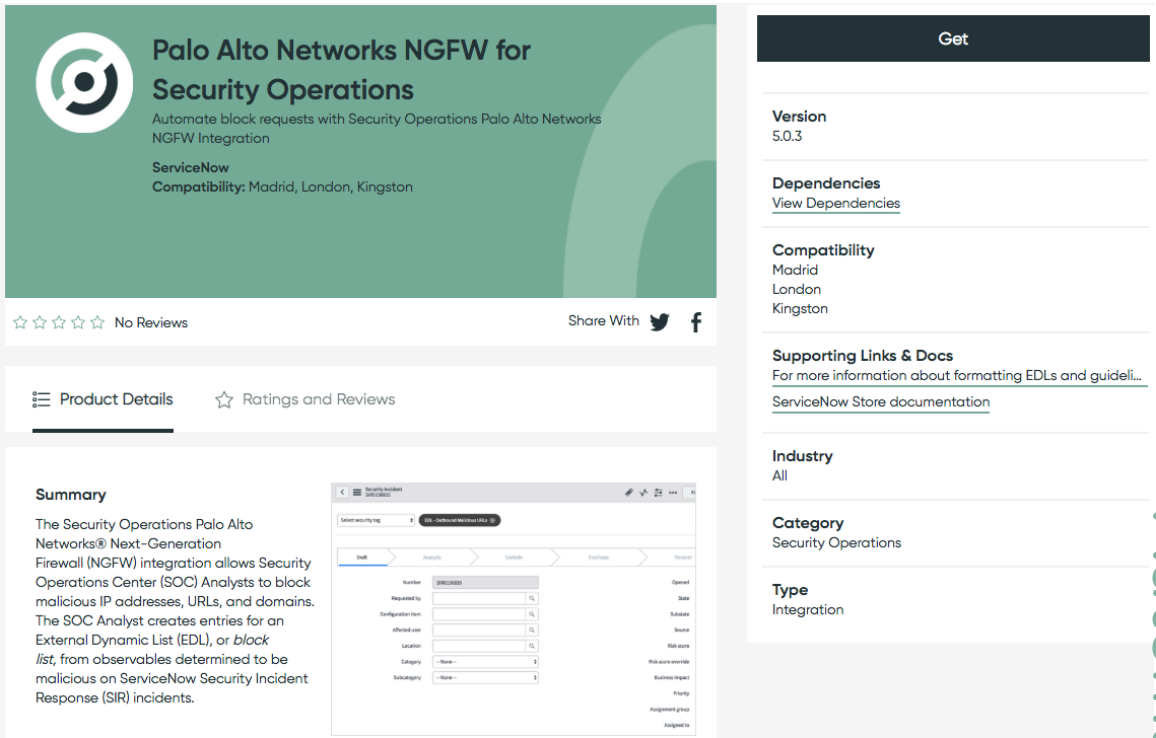
Hinweis:



2. Suchen Sie die Integration, die Sie installieren möchten, und klicken Sie auf **Konfigurieren**.
   Die ausgewählte Integration wird in angezeigt ServiceNow Store

Automatische Übersetzung

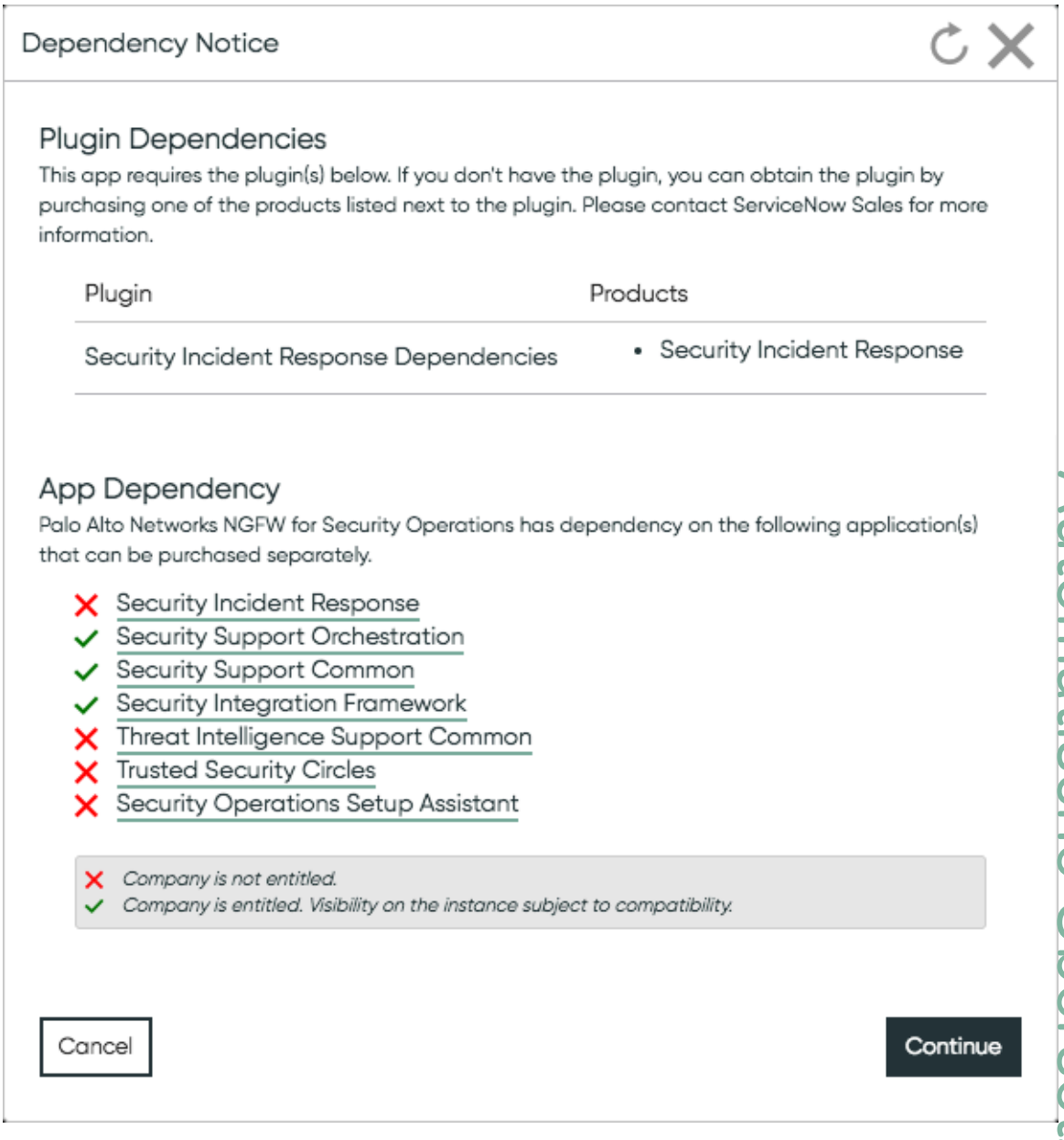
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Abhängigkeiten anzeigen**, und überprüfen Sie die aufgelisteten App-Abhängigkeiten.

Automatische Übersetzung

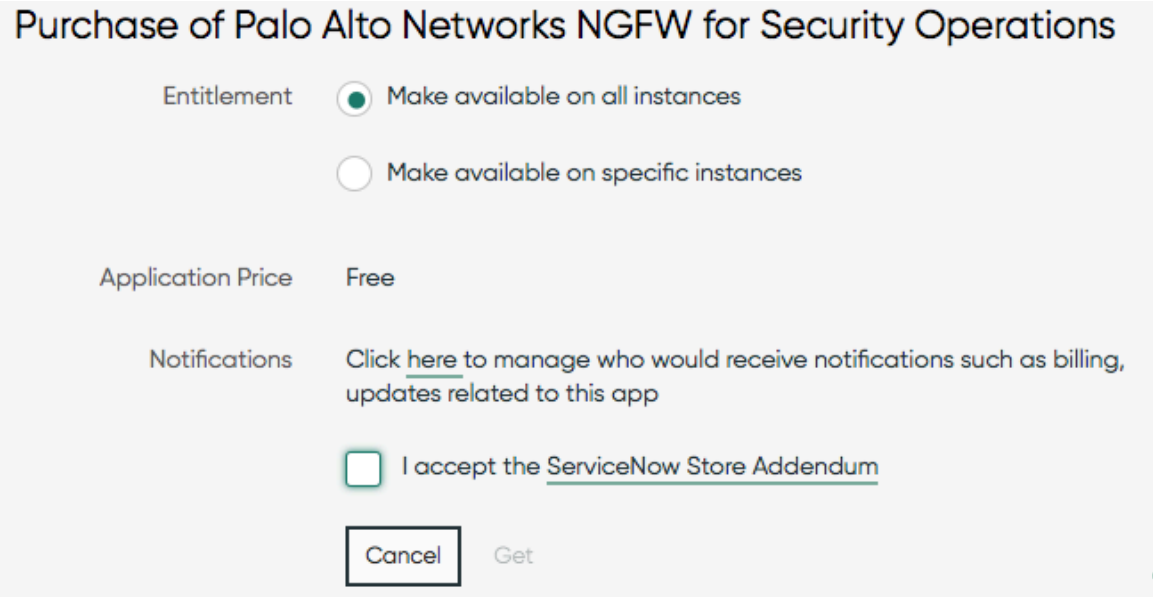
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wenn die Integration Kernanwendungsabhängigkeiten aufweist, z. B. Security Incident Response, für die Ihr Unternehmen noch nicht berechtigt ist:
   a. Befolgen Sie diese Anweisungen, um Berechtigungen zu erhalten, Abhängigkeits-Plugins herunterzuladen und die -Anwendungen zu aktivieren.
   b. Kehren Sie zu diesem Verfahren zurück.
   c. Klicken Sie auf **Fortsetzen**.
5. Klicken Sie auf **Abrufen**.
   Die ServiceNow-Nutzungsbedingungen werden angezeigt.
6. Klicken Sie auf **Fortsetzen**.
   Es öffnet sich ein Bildschirm für den Einkauf, der dem folgenden ähnelt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Geben Sie an, auf welchen Instanzen die Integration verfügbar sein soll, verwalten Sie Ihre Benachrichtigungen, und aktivieren Sie das Kontrollkästchen **ServiceNow Store Addendum**.
8. Klicken Sie auf **Abrufen**.

> **Hinweis:**
> Wenn Sie eine Anwendung zum Kauf herunterladen, klicken Sie auf **Kaufen**. Wenn Sie eine Anwendung herunterladen, für die Sie vorab die Genehmigung des Lieferanten einholen müssen, klicken Sie auf **App anfordern**.

9. Geben Sie den Instanznamen und einen Grund für die Anforderung ein, und klicken Sie dann auf **Anfordern**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
10. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
    Eine Liste der für die Installation verfügbaren Anwendungen wird angezeigt.
11. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Integration wird automatisch in Ihrer Instanz von installiert.

Aktualisiert eine zuvor aus dem heruntergeladene Anwendung ServiceNow Store

Wenn Sie zuvor eine Anwendung von ServiceNow Store heruntergeladen haben und eine neue Version verfügbar ist, können Sie sie in Ihrer Instanz aktualisieren.

Vorbereitungen

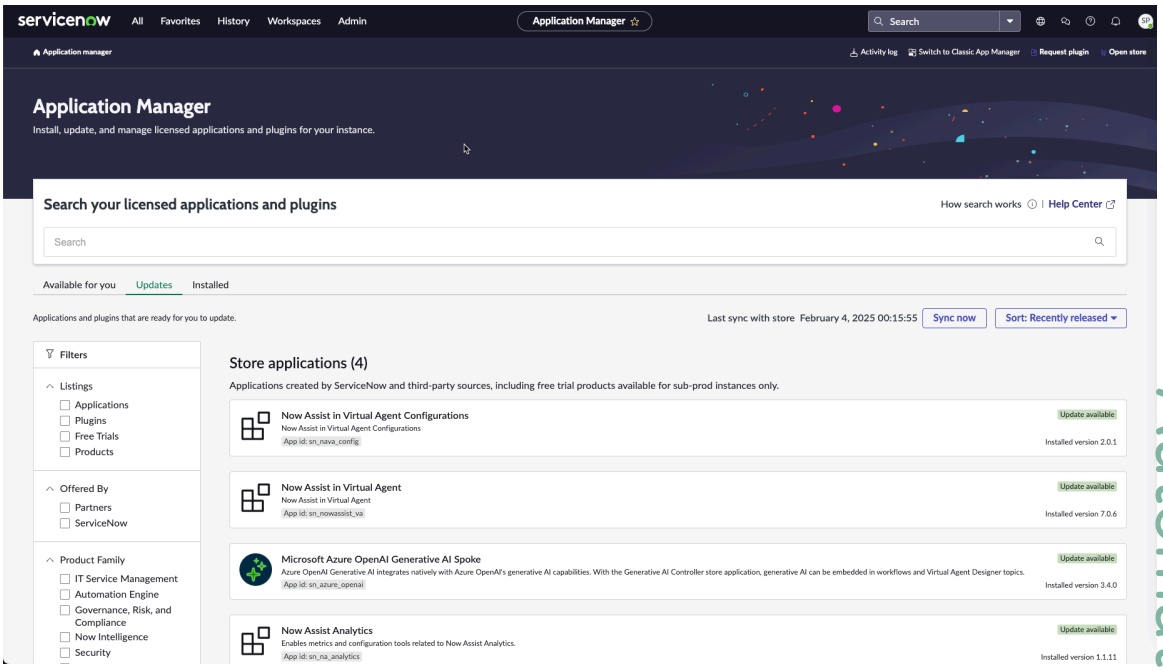
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie nach der Anwendung, die Sie aktualisieren möchten.
3. Wählen Sie die Version aus, auf die Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.
   Die Anwendung wird automatisch in Ihrer Instanz von installiert.

Aktualisieren Sie Ihre Instanz von auf das nächste Familien-Release

Wenn Sie derzeit ein Familien-Release verwenden (z. B. London) und auf das nächste Release upgraden möchten, müssen Sie die -Anwendungen nicht von ServiceNow Storeerwerben. Die Anwendung wird automatisch aktualisiert, wenn die Plattform auf die erforderliche Mindestversion aktualisiert wird.

Vorbereitungen

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.